6 Ideal norms and the Dedekind-Kummer thoerem

6.1 The ideal norm

Recall that for a ring extension B/A in which B is a free A-module of finite rank, we defined the (relative) norm $\mathrm{N}_{B/A}\colon B \to A$ as

$$\mathrm{N}_{B/A}(b) := \det(L \xrightarrow{\times b} L),$$

the determinant of the multiplication-by-b map with respect to some A-basis for B. We now want to extend our notion of norm to ideals, and to address the fact that in the case we are most interested in, in which B is the integral closure of a Dedekind domain A in a finite separable extension L of its fraction field K (the "$AKLB$ setup"), the Dedekind domain B is typically *not* a free A-module, even though it is finite generated as an A-module (see Proposition 4.60).

There is one situation where B is guaranteed to be a free A-module: if A is a PID then it follows from the structure theorem for finitely generated modules over PIDs, that $B \simeq A^r \oplus T$ for some torsion A-module T which must be trivial because B is torsion-free (it is a domain containing A).[1] This necessarily applies when A is a DVR, so if we localize the A-module B at a prime[2] $\mathfrak{p}$ of A, the module $B_\mathfrak{p}$ will be a free $A_\mathfrak{p}$-module.[3] Thus B is *locally free* as an A-module. We will use this fact to generalize our definition of $N_{B/A}$, but first we recall the notion of an *A-lattice* and define the *module index*.

Definition 6.1. Let A be a domain with fraction field K and let V be a K-vector space of finite dimension. An *A-lattice in V* is a finitely generated A-submodule $M \subseteq V$ that spans V as a K-vector space.

In the $AKLB$ setting, B is an A-lattice in the K-vector space L (see Proposition 4.55).

Definition 6.2. Let A be a Dedekind domain with fraction field K, let V be an n-dimensional K-vector space, and let M and N be A-lattices in V. Let $\mathfrak{p}$ be a prime of A, and let $\phi\colon M_\mathfrak{p} \xrightarrow{\sim} N_\mathfrak{p}$ be an isomorphism of $M_\mathfrak{p}$ and $N_\mathfrak{p}$ as free A_p-modules of rank n (note that $A_\mathfrak{p}$ is a PID and $M_\mathfrak{p}$ and $N_\mathfrak{p}$ are $A_\mathfrak{p}$-modules that span V, so they are both isomorphic to $A_\mathfrak{p}^n$). Now let ϕ_K be the unique K-linear map $V \to V$ extending ϕ, and define the (generalized) *module index* $(M_\mathfrak{p} : N_\mathfrak{p})_{A_\mathfrak{p}}$ is defined as the nonzero principal fractional A-ideal

$$(M_\mathfrak{p} : N_\mathfrak{p})_{A_\mathfrak{p}} := \big(\det(\phi_K)\big).$$

Finally, we define the *module index* $(M : N)_A$ to be the nonzero fractional A-ideal

$$(M : N)_A := \bigcap_\mathfrak{p} (M_\mathfrak{p} : N_\mathfrak{p})_{A_\mathfrak{p}}.$$

where $\mathfrak{p}$ ranges over primes of A (nonzero prime ideals, equivalently, maximal ideals); note that the localization of $(M : N)_A$ is $(M_\mathfrak{p} : N_\mathfrak{p})_{A_\mathfrak{p}}$, so we can recover $(M_\mathfrak{p} : N_\mathfrak{p})_{A_\mathfrak{p}}$ from $(M : N)_A$ (in other words, the module index respects localization).

[1] B may be a free A-module even when A is not a PID, but this is the exception, not the rule.

[2] Recall that a "prime of A" is a nonzero prime ideal, equivalently, a maximal ideal.

[3] Note that $B_\mathfrak{p}$ is the localization of B as an A-module, not as a ring (the latter doesn't even make sense: $\mathfrak{p}$ is not a prime ideal of B (unless $B = A$), and $\mathfrak{p}B$ need not be a prime ideal of B in any case).

Note that the module M need not contain N (this is why it is sometimes called the *generalized* module index), but when it does the module index $(M : N)_A$ is an actual ideal, not just a fractional ideal (to see this, apply Theorem 6.4 below locally and choose each uniformizer π to lie in A).

Some authors use the notation $[M : N]_A$, but we prefer $(M : N)_A$ because the module index should really be viewed as a generalization of colon ideals. Indeed, it follows immediately from the definition that

$$(M : N)_A(N : M)_A = A,$$

so $(M : N)_A$ and $(N : M)_A$ are inverse fractional ideals of A. Moreover, if I and J are nonzero fractional ideals of A, then I and J are both A-lattices in $V = K$ and the module index $(I : J)_A$ is precisely the colon ideal $(I : J)$. To see this, note that if π is a uniformizer for $\mathfrak{p}A_\mathfrak{p}$, then $I_\mathfrak{p} = (\pi^i)$ and $J_\mathfrak{p} = (\pi^j)$ for some $i, j \in \mathbb{Z}$, and up to a unit the determinant of ϕ_K is π^{j-i}. Thus $(I_\mathfrak{p} : J_\mathfrak{p})_{A_\mathfrak{p}} = (\pi^{j-i}) = (I_\mathfrak{p} : J_\mathfrak{p})$, and therefore $(I : J)_A = (I : J)$.

Example 6.3. If $A = \mathbb{Z}$ and $N \subseteq M$ then $(M : N)_\mathbb{Z}$ is the principal $\mathbb{Z}$-ideal generated by the index $[M : N]$ of additive groups, equivalently, the cardinality of the finite quotient M/N. For example, if $M = 3\mathbb{Z}$ and $N = 6\mathbb{Z}$ then $(6\mathbb{Z} : 3\mathbb{Z})_\mathbb{Z} = (2)$. Note that $(N : M)_\mathbb{Z}$ is also defined: it is the principal fractional $\mathbb{Z}$-ideal generated by the reciprocal of $[M : N]$. For $M = 3\mathbb{Z}$ and $N = 6\mathbb{Z}$ we have $(3\mathbb{Z} : 6\mathbb{Z})_\mathbb{Z} = (\frac{1}{2})$.

More generally, we have the following theorem, which applies whenever $N \subseteq M$ and the quotient M/N is isomorphic to a direct sum of cyclic modules (always the case when A is a PID). Recall that a *cyclic module* is a module generated by a single element $x \in M$ and is canonically isomorphic to A/I where $I = \{a \in A : ax = 0 \text{ (in } M)\}$ is the annhilator of x (when M is a nonzero principal fractional ideal of A this is just saying that $M \simeq A/(A : M)$).

Theorem 6.4. *Let A be a Dedekind domain with fraction field K, and let $N \subseteq M$ be A-lattices in a K-vector space V for which the quotient module M/N is a direct sum of cyclic A-modules:*

$$M/N \simeq A/I_1 \oplus \cdots \oplus A/I_n,$$

for some A-ideals $I_1, \ldots, I_n$. Then

$$(M : N)_A = I_1 \cdots I_n.$$

Proof. Let $\mathfrak{p}$ be a maximal ideal of A. Then $M_\mathfrak{p}$ and $N_\mathfrak{p}$ are both free $A_\mathfrak{p}$-modules of rank $n = \dim V$, and the localization of each I_j at $\mathfrak{p}$ is a principal ideal (π^{e_j}), where π is a uniformizer for $\mathfrak{p}A_\mathfrak{p}$. Fix an $A_\mathfrak{p}$-module basis for $M_\mathfrak{p}$ and use is to identify $A_\mathfrak{p}^n$ with $M_\mathfrak{p}$. Write down an $A_\mathfrak{p}$-module basis for $N_\mathfrak{p}$ in terms of the basis for $M_\mathfrak{p}$, and let $\phi\colon A_\mathfrak{p}^n \to A_\mathfrak{p}^n$ be the corresponding map that sends basis elements of $M_\mathfrak{p}$ to basis elements of $N_\mathfrak{p}$, so that $M_\mathfrak{p}/N_\mathfrak{p} = \operatorname{coker}\phi$. Write the matrix of ϕ in Smith normal form UDV with $U, V \in \mathrm{GL}_n(A)$ and $D = \operatorname{diag}(\pi_\mathfrak{p}^{d_1}, \ldots, \pi_\mathfrak{p}^{d_r})$ an $n \times n$ diagonal matrix. Then

$$A_\mathfrak{p}/(\pi^{e_1}) \oplus \cdots \oplus A_\mathfrak{p}/(\pi^{e_n}) \simeq M_\mathfrak{p}/N_\mathfrak{p} = \operatorname{coker}\phi \simeq A_\mathfrak{p}/(\pi^{d_1}) \oplus \cdots \oplus A/(\pi^{d_r}).$$

It follows from the structure theorem for modules over a PID that the non-trivial summands on each side are precisely the invariant factors of $M_\mathfrak{p}/N_\mathfrak{p}$, possibly in different orders. We must have $\sum_{j=1}^n e_j = \sum_{i=1}^r d_i$, and since we may also view $\phi\colon A_\mathfrak{p}^n \to A_\mathfrak{p}^n$ as the isomorphism $\phi\colon M_\mathfrak{p} \to N_\mathfrak{p}$ used to define the module index, we have

$$(M_\mathfrak{p} : N_\mathfrak{p})_{A_\mathfrak{p}} = (\det\phi) = (\det D) = (\pi_\mathfrak{p}^{\sum d_i}) = (\pi_\mathfrak{p}^{\sum e_j}) = (\pi_\mathfrak{p}^{e_1}) \cdots (\pi_\mathfrak{p}^{e_n}) = (I_1 \cdots I_n)_\mathfrak{p}.$$

We then note that

$$(M : N) = \bigcap_{\mathfrak{p}} (M_{\mathfrak{p}} : N_{\mathfrak{p}})_{A_{\mathfrak{p}}} = \bigcap_{\mathfrak{p}} (I_1 \cdots I_n)_{\mathfrak{p}} = I_1 \cdots I_n. \qquad \square$$

In the $AKLB$ setup the inclusion $A \subseteq B$ induces a homomorphism of ideal groups:

$$\begin{aligned} \mathcal{I}_A &\to \mathcal{I}_B, \\ I &\mapsto IB. \end{aligned}$$

We wish define a homomorphism $N_{B/A} \colon \mathcal{I}_B \to \mathcal{I}_A$ in the reverse direction. Every fractional B-ideal is an A-lattice in the finite-dimensional K-vector space L, so we may define

$$\begin{aligned} \mathcal{I}_B &\to I_A, \\ I &\mapsto (B : I)_A \end{aligned}$$

Definition 6.5. Assume $AKLB$. The *ideal norm* $N_{B/A} \colon \mathcal{I}_B \to \mathcal{I}_A$ is the map $I \mapsto (B : I)_A$. We may extend $N_{B/A}$ to (0) by defining $N_{B/A}((0)) = (0)$.

We now show that the ideal norm $N_{B/A}$ is compatible with the field norm $\mathrm{N}_{L/K}$ (and with $\mathrm{N}_{B/A}$, which is just the restriction of $\mathrm{N}_{L/K}$ to B).

Proposition 6.6. *Assume $AKLB$ and let $\alpha \in L$. Then $N_{B/A}((\alpha)) = \big(\mathrm{N}_{L/K}(\alpha)\big)$.*

Proof. The case $\alpha = 0$ is immediate, so assume $\alpha \in L^\times$. We have

$$N_{B/A}((\alpha)) = (B : \alpha B)_A = \bigcap_{\mathfrak{p}} (B_{\mathfrak{p}} : \alpha B_{\mathfrak{p}})_{A_{\mathfrak{p}}} = \Big(\det(L \xrightarrow{\times\alpha} L)\Big) = \big(\mathrm{N}_{L/K}(\alpha)\big),$$

since each $B_{\mathfrak{p}} \xrightarrow{\times\alpha} \alpha B_{\mathfrak{p}}$ is an isomorphism of free $A_{\mathfrak{p}}$-modules that are $A_{\mathfrak{p}}$-lattices in L. $\square$

Proposition 6.7. *Assume $AKLB$. The map $N_{B/A} \colon \mathcal{I}_B \to \mathcal{I}_A$ is a homomorphism.*

Proof. Let $\mathfrak{p}$ be a maximal ideal of A. Then $A_{\mathfrak{p}}$ is a DVR and $B_{\mathfrak{p}}$ is a semilocal Dedekind domain, hence a PID. Thus every element of $\mathcal{I}_{B_{\mathfrak{p}}}$ is a principal ideal (α) for some $\alpha \in L^\times$, and the previous proposition implies that $N_{B_{\mathfrak{p}}/A_{\mathfrak{p}}} \colon \mathcal{I}_{B_{\mathfrak{p}}} \to \mathcal{I}_{A_{\mathfrak{p}}}$ is a group homomorphism, since $N_{L/K}$ is. For any $I, J \in \mathcal{I}_B$ we then have

$$N_{B/A}(IJ) = \bigcap_{\mathfrak{p}} N_{B_{\mathfrak{p}}/A_{\mathfrak{p}}}(I_{\mathfrak{p}} J_{\mathfrak{p}}) = \bigcap_{\mathfrak{p}} N_{B_{\mathfrak{p}}/A_{\mathfrak{p}}}(I_{\mathfrak{p}}) N_{B_{\mathfrak{p}}/A_{\mathfrak{p}}}(J_{\mathfrak{p}}) = N_{B/A}(I) N_{B/A}(J). \qquad \square$$

Corollary 6.8. *Assume $AKLB$ and let I be a factional ideal of B. The ideal norm of B is the fractional ideal of A generated by the image of B under the field norm $N_{L/K}$, that is,*

$$N_{B/A}(I) = \big(\mathrm{N}_{L/K}(\alpha) : \alpha \in I\big).$$

Proof. Let J denote the RHS. For any nonzero prime $\mathfrak{p}$ of A, the localization of the ideal $N_{B/A}(I) = (B : I)_A$ at $\mathfrak{p}$ is $(B_{\mathfrak{p}} : I_{\mathfrak{p}})_{A_{\mathfrak{p}}} = N_{B_{\mathfrak{p}}/A_{\mathfrak{p}}}(I_{\mathfrak{p}})$. The fractional ideal $N_{B_{\mathfrak{p}}/A_{\mathfrak{p}}}(I_{\mathfrak{p}})$ of $A_{\mathfrak{p}}$ is principal, so $N_{B_{\mathfrak{p}}/A_{\mathfrak{p}}}(I_{\mathfrak{p}}) = J_{\mathfrak{p}}$ follows from the proposition, and

$$N_{B/A}(I) = \bigcap_{\mathfrak{p}} N_{B_{\mathfrak{p}}/A_{\mathfrak{p}}}(I_{\mathfrak{p}}) = \bigcap_{\mathfrak{p}} J_{\mathfrak{p}} = J. \qquad \square$$

The corollary gives us an alternative definition of the ideal norm in terms of the field norm. In view of this we extend our definition of the field norm $N_{L/K}$ to fractional ideals of B, and we may write $N_{L/K}(I)$ instead of $N_{B/A}(I)$. We have the following pair of commutative diagrams, in which the downward arrows map nonzero field elements to the principal fractional ideals they generate. We know that composing the maps $K^\times \to L^\times \to K^\times$ along the top corresponds to exponentiation by $n = [L : K]$ (see Problem Set 2); we now show that this is also true for the composition of the bottom maps.

$$\begin{array}{ccc} K^\times & \xrightarrow{\subseteq} & L^\times \\ \downarrow{\scriptstyle (a)} & & \downarrow{\scriptstyle (y)} \\ \mathcal{I}_A & \xrightarrow{I\mapsto IB} & \mathcal{I}_B \end{array} \qquad \begin{array}{ccc} L^\times & \xrightarrow{N_{L/K}} & K^\times \\ \downarrow{\scriptstyle (y)} & & \downarrow{\scriptstyle (x)} \\ \mathcal{I}_B & \xrightarrow{N_{B/A}} & \mathcal{I}_A \end{array}$$

Theorem 6.9. *Assume AKLB and let $\mathfrak{q}$ be a prime lying above $\mathfrak{p}$. Then $N_{B/A}(\mathfrak{q}) = \mathfrak{p}^{f_\mathfrak{q}}$, where $f_\mathfrak{q} = [B/\mathfrak{q} : A/\mathfrak{p}]$ is the residue field degree of $\mathfrak{q}$.*

Proof. The $(A/\mathfrak{p})$-vector space $B/\mathfrak{q}$ has dimension $f_\mathfrak{q}$. The A-module $B/\mathfrak{q} \simeq A/\mathfrak{p} \oplus \cdots \oplus A/\mathfrak{p}$ is thus an $f_\mathfrak{q}$-fold direct sum of cyclic A-modules $A/\mathfrak{p}$, and we may apply Theorem 6.4. Thus $N_{B/A}(\mathfrak{q}) = (B : \mathfrak{q})_A = \mathfrak{p} \cdots \mathfrak{p} = \mathfrak{p}^{f_\mathfrak{q}}$. □

Corollary 6.10. *Assume AKLB. For $I \in \mathcal{I}_A$ we have $N_{B/A}(IB) = I^n$, where $n = [L : K]$.*

Proof. Since $N_{B/A}$ and $I \mapsto IB$ are group homomorphisms, it suffices to consider the case were $I = \mathfrak{p}$ is a nonzero prime ideal. We then have

$$N_{B/A}(\mathfrak{p}B) = N_{B/A}\left(\prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}_\mathfrak{q}^e\right) = \prod_{\mathfrak{q}|\mathfrak{p}} N_{B/A}(\mathfrak{q})^{e_\mathfrak{q}} = \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{p}^{e_\mathfrak{q} f_\mathfrak{q}} = \mathfrak{p}^{\sum_{\mathfrak{q}|\mathfrak{p}} e_\mathfrak{q} f_\mathfrak{q}} = \mathfrak{p}^n. \qquad \square$$

6.2 Dedekind domains in algebraic geometry

The maps $i\colon \mathcal{I}_A \to \mathcal{I}_B$ and $N_{B/A}\colon \mathcal{I}_B \to \mathcal{I}_A$ have a geometric interpretation that will be familiar to those who have studied algebraic geometry: they are the pushforward and pullback maps on divisors associated to the morphism of curves $Y \to X$ induced by the inclusion $A \subseteq B$, where $X = \operatorname{Spec} A$ and $Y = \operatorname{Spec} B$. For the benefit of those who have not seen this before, let us briefly explain the connection.

Dedekind domains naturally arise in algebraic geometry as coordinate rings of smooth curves (which for the sake of this discussion one can take to mean geometrically irreducible algebraic varieties of dimension one with no singularities). In order to make this explicit, let us fix a perfect field k and a polynomial $f \in k[x, y]$ that we will assume is irreducible in $\bar{k}[x, y]$. The ring $A = k[x, y]/(f)$ is a noetherian domain of dimension 1, and if we further assume that the algebraic variety X defined by $f(x, y) = 0$ has no singularities, then A is also integrally closed and therefore a Dedekind domain.[4] We call A the *coordinate ring* of X, denoted $k[X]$, and its fraction field is the *function field* of X, denoted $k(X)$.

Conversely, given a Dedekind domain A, we can regard $X = \operatorname{Spec} A$ as a smooth curve whose *closed points* are the maximal ideals of A (all of $\operatorname{Spec} A$ except the zero ideal). When the field of constants k is algebraically closed, Hilbert's Nullstellensatz gives a one-to-one

[4] If A is not integrally closed, we can replace it by its integral closure, thereby obtaining the *normalization* of the curve X. One typically also takes the projective closure of X in order to obtain a *complete* curve; this corresponds to considering all absolute values (*places*) of the fraction field of A, not just those arising from primes. This distinction does not affect our discussion here but will become relevant in later lectures.

correspondence between maximal ideals $(x - x_0, y - y_0)$ and points (x_0, y_0) in the affine plane, but in general closed points correspond to $\mathrm{Gal}(\bar{k}/k)$-orbits of $\bar{k}$-points.

Recall that the ideal group $\mathcal{I}_A$ is isomorphic to the free abelian group generated by the nonzero prime ideals $\mathfrak{p}$ of A. The corresponding object in algebraic geometry is the *divisor group* $\operatorname{Div} X$, the free abelian group generated by the closed points P of X. The group $\operatorname{Div} X$ is written additively, so its elements have the form $D = \sum n_P P$ with all but finitely many of the integers n_P equal to 0.

A finite extension of Dedekind domains B/A induces a surjective morphism $\phi\colon Y \to X$ of the corresponding curves $X = \operatorname{Spec} A$ and $Y = \operatorname{Spec} B$. Primes $\mathfrak{q}$ of B in the fiber above a prime $\mathfrak{p}$ of A correspond to closed points Q of Y in the fiber of ϕ above a closed point P of X. The map $\mathcal{I}_A \to \mathcal{I}_B$ defined by $\mathfrak{p} \mapsto \mathfrak{p}B = \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{e_\mathfrak{q}}$ corresponds to the *pullback* map $\phi^*\colon \operatorname{Div} X \to \operatorname{Div} Y$ induced by ϕ, which is defined by

$$\phi^*(P) := \sum_{\phi(Q)=P} e_Q Q.$$

In the other direction, the norm map $N_{B/A}\colon \mathcal{I}_B \to \mathcal{I}_A$, which sends $\mathfrak{q}$ to $N_{B/A}(\mathfrak{q}) = \mathfrak{p}^{f_\mathfrak{q}}$, corresponds to *pushforward* map $\phi_*\colon \operatorname{Div} Y \to \operatorname{Div} X$ induced by ϕ, which is defined

$$\phi_*(Q) := f_Q \phi(Q) = f_Q P.$$

It weights the image $P = \phi(Q)$ by the number of $\bar{k}$-points in the Galois orbit corresponding to the closed point Q, equivalently, the degree of the field extension of k needed to split Q into f_Q distinct closed points after base extension (here we are using our assumption that k is perfect). If we compose the pushforward and pullback maps we obtain

$$\phi_*\phi^*(P) = \sum_{\phi(Q)=P} e_Q f_Q P = \deg(\phi) P.$$

Here $\deg(\phi)$ is the *degree* of the morphism $\phi\colon Y \to X$, which is typically defined as the degree of the function field extension $[k(Y) : k(X)]$, but one can take the above formula as an alternative definition. It is a weighted measure of the cardinality of the fibers of ϕ that reflects both the ramification and degree of each closed point Q in the fiber (and as a consequence, is the same for every fiber).

6.3 The ideal norm in number fields

We now specialize to the case $A = \mathbb{Z}$, $K = \mathbb{Q}$, and $B = \mathcal{O}_L$ is the ring of integers of the number field L. In this situation we may simply write N in place of $N_{B/A}$ and call it the *absolute norm*. If $\mathfrak{q}$ is a nonzero prime ideal of $\mathcal{O}_L$ then

$$N(\mathfrak{q}) = (p^{f_\mathfrak{q}}),$$

where $p \in \mathbb{Z}$ is the unique prime in $\mathfrak{q} \cap \mathbb{Z}$, and f is the degree of the finite field $B/\mathfrak{q}$ as an extension of $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$. The absolute norm

$$N(\mathfrak{q}) = (\mathcal{O}_L : \mathfrak{q})_\mathbb{Z}$$

is the principal ideal generated by the (necessarily finite) index $[\mathcal{O}_L : \mathfrak{q}] \in \mathbb{Z}$ of $\mathfrak{q}$ in $\mathcal{O}_L$ as free $\mathbb{Z}$-modules of equal rank; this is just the index of $\mathfrak{q}$ in $\mathcal{O}_L$ as additive groups. More generally, we have the following.

Proposition 6.11. *Let L be a number field with ring of integers $\mathcal{O}_L$. For any nonzero $\mathcal{O}_L$-ideal $\mathfrak{a}$ we have $N(\mathfrak{a}) = \big([\mathcal{O}_L : \mathfrak{a}]\big)$, and if $\mathfrak{b} \subseteq \mathfrak{a}$ are nonzero fractional ideals, then*

$$\big([\mathfrak{a} : \mathfrak{b}]\big) = N(\mathfrak{a}^{-1}\mathfrak{b}).$$

Proof. Let $\mathfrak{a} = \prod_i \mathfrak{q}_i^{e_i}$ by the factorization of $\mathfrak{a}$ into prime ideals $\mathfrak{q}_i$. By the Chinese remainder theorem, $\mathcal{O}_L/\mathfrak{a} \simeq \prod \mathcal{O}_L/\mathfrak{q}_i^{e_i}$, so $(\mathcal{O}_L : \mathfrak{a}) = \prod_i (\mathcal{O}_L : \mathfrak{q}_i^{e_i})$, and since N is a group homomorphism, it suffices to consider $\mathfrak{a} = \mathfrak{q}^e$ a prime power. Each quotient $\mathfrak{q}^{e+1}/\mathfrak{q}^e$ is both an $(\mathcal{O}_L/\mathfrak{q})$-vector space and a ring that has no non-trivial ideals (there are no ideals properly between $\mathfrak{q}^e$ and $\mathfrak{q}^{e+1}$), hence a field, and therefore isomorphic to the finite field $\mathcal{O}_L/\mathfrak{q}$. It follows that $\mathcal{O}_L/\mathfrak{q}^e$ is an e-dimensional $(\mathcal{O}_L/\mathfrak{q})$-vector space, thus $[\mathcal{O}_L : \mathfrak{q}^e] = [\mathcal{O}_L : \mathfrak{q}]^e = p^{ef}$, where $p = \mathfrak{q} \cap \mathbb{Z}$ and $f = [\mathcal{O}_L/\mathfrak{q} : \mathbb{Z}/p\mathbb{Z}]$. By Theorem 6.9 we have $N(\mathfrak{q}) = (p)^f = (p^f)$, and $N(\mathfrak{q}^e) = (p^{ef})$, which proves the first claim.

We now prove the second claim. For any $\alpha \in L^\times$ we have $[\mathfrak{a} : \mathfrak{b}] = [\alpha\mathfrak{a} : \alpha\mathfrak{b}]$ and $N([(\alpha\mathfrak{a})^{-1}\alpha\mathfrak{b}]) = N(\mathfrak{a}^{-1}\mathfrak{b})$, so we can assume without loss of generality that $\mathfrak{a}$ and $\mathfrak{b}$ are integral ideals. We then have a tower of free $\mathbb{Z}$-modules $\mathfrak{b} \subseteq \mathfrak{a} \subseteq \mathcal{O}_L$, and therefore

$$[\mathcal{O}_L : \mathfrak{a}][\mathfrak{a} : \mathfrak{b}] = [\mathcal{O}_L : \mathfrak{b}].$$

Replacing both sides with the $\mathbb{Z}$-ideals they generate, we have

$$N(\mathfrak{a})\big((\mathfrak{a} : \mathfrak{b})\big) = N(\mathfrak{b}),$$

thus $\big((\mathfrak{a} : \mathfrak{b})\big) = N(\mathfrak{a}^{-1}\mathfrak{b})$, since $N\colon \mathcal{I}_L \to \mathcal{I}_\mathbb{Z}$ is a group homomorphism. □

Remark 6.12. Since $\mathbb{Z}$ is a principal ideal domain whose only units are ± 1, we can unambiguously identify each fractional ideal with a positive rational number and view the absolute norm $N\colon \mathcal{I}_L \to \mathcal{I}_\mathbb{Z}$ as a homomorphism $N\colon \mathcal{I}_L \to \mathbb{Q}^\times_{>0}$ from $\mathcal{I}_L$ to the multiplicative group of positive rational numbers. If we write $N(\mathfrak{a})$ in contexts where an element of $\mathbb{Z}$ or $\mathbb{Q}$ (or $\mathbb{R}$) is expected, it is always with this understanding.

6.4 The Dedekind-Kummer theorem

We now give a theorem that provides a practical method for factoring primes in extensions. This result was proved by Dedekind for number fields, building on earlier work of Kummer, but we will give a version that works for arbitrary extensions of Dedekind domains B/A whose fraction fields form a finite separable extension L/K (the usual $AKLB$ setup).

Recall that the primitive element theorem implies that if L/K is a finite separable extension then we can always write $L = K(\alpha)$ for some $\alpha \in L$, and in the $AKLB$ setup we can assume $\alpha \in B$ (see Proposition 4.55). This does not imply that $B = A[\alpha]$; indeed, it may happen that there is no $\alpha \in B$ for which $B = A[\alpha]$. Extensions L/K for which $B = A[\alpha]$ for some $\alpha \in B$ are said to be *monogenic*. This necessarily implies that B is a free A-module, hence it has an *integral basis* $\{\beta_1, \dots, \beta_n\}$, but monogenicity is a stronger condition, since it implies that B has an *integral power basis*, one of the form $\{1, \alpha, \dots, \alpha^{n-1}\}$. Examples of monogenic extensions include all quadratic and cyclotomic extensions, but most extensions are not monogenic, (even when B is a free A-module).

Let us first prove the Dedekind-Kummer theorem assuming $B = A[\alpha]$, then address the general case, in which we do not assume B is monongenic or even free over A.

Theorem 6.13 (Dedekind-Kummer Theorem)**.** *Assume $AKLB$ with $L = K(\alpha)$ and $\alpha \in B$, let $f \in A[x]$ be the minimal polynomial of α and assume $B = A[\alpha]$. Suppose $g_1, \dots, g_r \in A[x]$ are monic polynomials for which*

$$\bar{f} = \bar{g}_1^{e_1} \cdots \bar{g}_r^{e_r}$$

is a complete factorization of $\bar{f} \in (A/\mathfrak{p})[x]$, where $\bar{\cdot}$ denotes reduction modulo $\mathfrak{p}$, and let $\mathfrak{q}_i := (\mathfrak{p}, g_i(\alpha))$ be the B-ideal generated by $\mathfrak{p}$ and $g_i(\alpha)$. Then

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

is the prime factorization of $\mathfrak{p}B$ in B and the residue degree of $\mathfrak{q}_i$ is $f_i := \deg g_i$.

Before proving the theorem, last us give an example to illustrate its utility.

Example 6.14. Let $A = \mathbb{Z}$, $K = \mathbb{Q}$, and $L = \mathbb{Q}(\zeta_5)$, where $\alpha = \zeta_5$ be a primitive 5th root of unity with minimal polynomial $f(x) = x^4 + x^3 + x^2 + x + 1$. Then $B = \mathcal{O}_L = \mathbb{Z}[\zeta_5]$ (see Problem Set 3), and we have $(B : A[\alpha])_A = (1)$ so the theorem applies to every prime (p).

- (2): $f(x)$ is irreducible modulo 2, so $2\mathbb{Z}[\zeta_5]$ is prime and (2) is inert in $\mathbb{Q}(\zeta_5)$.
- (5): $f(x) \equiv (x-1)^4 \bmod 5$, so $5\mathbb{Z}[\zeta_5] = (5, \zeta_5 - 1)^4$ and (5) is totally ramified in $\mathbb{Q}(\zeta_5)$.
- (11): $f(x) \equiv (x-4)(x-9)(x-5)(x-3) \bmod 11$, so

  $$11\mathbb{Z}[\zeta_5] = (11, \zeta_5 - 4)(11, \zeta_5 - 9)(11, \zeta_5 - 5)(11, \zeta_5 - 3),$$

  and (11) splits completely in $\mathbb{Q}(\zeta_5)$.
- (19): $f(x) \equiv (x^2 + 5x + 1)(x^2 - 4x + 1) \bmod 19$, so

  $$19\mathbb{Z}[\zeta_5] = (19, \zeta_5^2 + 5\zeta_5 + 11)(19, \zeta_5^2 - 4\zeta_5 + 1).$$

The four cases above actually cover every possible prime factorization pattern in the cyclotomic extension $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ (see Problem Set 3 for a proof).

Proof of the Dedekind-Kummer theorem. We have $B = A[\alpha] \simeq A[x]/(f(x))$ and therefore

$$\frac{A[\alpha]}{(\mathfrak{p}, g_i(\alpha))} \simeq \frac{A[x]}{(f(x), \mathfrak{p}, g_i(x))} \simeq \frac{(A/\mathfrak{p})[x]}{(\bar{f}(x), \bar{g}_i(x))} \simeq \frac{(A/\mathfrak{p})[x]}{(\bar{g}_i(x))}.$$

The polynomial $\bar{g}_i(x)$ is by assumption irreducible in the one-dimensional UFD $(A/\mathfrak{p})[x]$, thus $(\bar{g}_i(x))$ is a maximal ideal and the quotient $(A/\mathfrak{p})[x]/(\bar{g}_i(x))$ is a field; indeed, it is an extension of the field $(A/\mathfrak{p})$ of degree $\deg g_i$. It follows that $\mathfrak{q}_i$ is a prime above $\mathfrak{p}$ with residue degree $f_i := \deg g_i$ as claimed.

The ideal $\prod_i \mathfrak{q}_i^{e_i} = \prod_i (\mathfrak{p}, g_i(\alpha))^{e_i}$ lies in $\mathfrak{p}B$, because it is generated by elements of $\mathfrak{p}B$ together with the element

$$\prod_i g_i(\alpha)^{e_i} \equiv f(\alpha) \equiv 0 \bmod \mathfrak{p}B.$$

The $\bar{g}_i(x)$ are distinct as elements of $(A/\mathfrak{p})[x]/(f(x)) \simeq A[x]/(\mathfrak{p}, f(x)) \simeq A[\alpha]/\mathfrak{p}$, and it follows that the $g_i(\alpha)$ are distinct modulo $\mathfrak{p}$. Therefore the prime ideals $\mathfrak{q}_i$ are distinct and we must have $e_i \geq e_{\mathfrak{q}_i}$ in order for $\prod_i \mathfrak{q}_i^{e_i}$ to lie in $\mathfrak{p}B$. We also have

$$N_{B/A}\left(\prod_i \mathfrak{q}_i^{e_i}\right) = \prod_i N_{B/A}(\mathfrak{q}_i)^{e_i} = \prod_i (\mathfrak{p}^{f_i})^{e_i} = \mathfrak{p}^{\deg f} = p^n,$$

so in fact $e_i = e_{\mathfrak{q}_i}$ is the ramification index of $\mathfrak{q}_i$. The theorem follows. □

In order to generalize the Dedekind-Kummer theorem to handle cases where L/K is not monogenic we introduce the notion of the *conductor* of a ring extension.

Definition 6.15. Let S/R be an extension of rings. The *conductor* $\mathfrak{c}$ of R in S is the largest S-ideal that is also an R-ideal;

$$\mathfrak{c} := \mathfrak{c}_{S/R} := \{\alpha \in S : \alpha S \subseteq R\} = \{\alpha \in R \colon \alpha S \subseteq R\}.$$

The equality of the two sets follows from the fact that $1 \in S$.

We say that an ideal $\mathfrak{a}$ of R or S is *prime to the conductor* if $\mathfrak{a} + \mathfrak{c} = (1)$.

Proposition 6.16. *The assumption $B = A[\alpha]$ in the Dedekind-Kummer theorem can be replaced with the assumption that $\mathfrak{p}A[\alpha]$ is prime to the conductor of $A[\alpha]$ in B.*

Proof. We will prove in the next lecture that there is a bijection between prime ideals of $A[\alpha]$ that do not contain $\mathfrak{c}$ and prime ideals of B that do not contain $\mathfrak{c}$. The proof of the Dedekind-Kummer theorem is then the same: whether we view them as $A[\alpha]$-ideals or B-ideals, the ideals $\mathfrak{q}_i = (\mathfrak{p}, g_i(\alpha))$ are precisely the primes above $\mathfrak{p}$ and their ramification indices and residue degrees are e_i and $f_i = \deg g_i$ respectively. □

18.785 Number Theory I
Fall 2015