6 Ideal norms and the Dedekind-Kummer theorem

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

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

the determinant of the multiplication-by-b map with respect to any A-basis for B. We want to extend our notion of norm to fractional ideals of B. 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 (our "$AKLB$" setup), the Dedekind domain B is typically *not* a free A-module, even though it is finitely generated as an A-module, by Proposition 5.19.

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 in our setting because B is always torsion-free (it is an integral domain containing A).[1]

This necessarily applies when A is a DVR (which is a special case of a Dedekind domain), and even if A is not a DVR, as a Dedekind domain, its localization at any prime[2] $\mathfrak{p}$ will be a DVR (this was one of our two equivalent definitions of a Dedekind domain). Thus if we localize the A-module B at a prime $\mathfrak{p}$ of A then the module $B_\mathfrak{p}$ will be a free $A_\mathfrak{p}$-module; in other words, B is a *locally free* A-module (this applies to any A-module).

6.1 The module index

Out strategy is to define the norm of an ideal as the intersection of the norms of all its localizations. Recall that by Proposition 2.7 any A-module M in a K-vector space is equal to the intersection of its localizations at primes of A; this applies, in particular, to fractional ideals of A and B. In order to do this we first define the *module index* of two A-lattices, as originally introduced by Fröhlich [2]. Recall that an A-lattice M in a K-vector space V is a finitely generated A-submodule of V that contains a K-basis for V. If M is free, then any A-basis for M is necessarily a K-basis for V, and we must have $M \simeq A^n$; if M is not free we can apply this to its localizations $M_\mathfrak{p}$ at primes $\mathfrak{p}$ of A, each of which is an $A_\mathfrak{p}$-lattice.

Definition 6.1. 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. Then $A_\mathfrak{p}$ is a PID and we necessarily have $M_\mathfrak{p} \simeq A^n \simeq N_\mathfrak{p}$. Let us choose an $A_\mathfrak{p}$-module isomorphism $\phi_\mathfrak{p}\colon M_\mathfrak{p} \xrightarrow{\sim} N_\mathfrak{p}$ and let $\hat\phi_\mathfrak{p}$ denote the unique K-linear map $V \to V$ extending $\phi_\mathfrak{p}$. The linear map $\hat\phi_\mathfrak{p}$ is an isomorphism and therefore has nonzero determinant. The *module index* $[M_\mathfrak{p} : N_\mathfrak{p}]_{A_\mathfrak{p}}$ is the fractional $A_\mathfrak{p}$-ideal generated by $\det\hat\phi_\mathfrak{p}$:

$$[M_\mathfrak{p} : N_\mathfrak{p}]_{A_\mathfrak{p}} := \big(\det\hat\phi_\mathfrak{p}\big).$$

This ideal does not depend on our choice of $\phi_\mathfrak{p}$ because any other choice can be written as $\phi_1\phi_\mathfrak{p}\phi_2$ for some A-module automorphisms $\phi_1\colon M \xrightarrow{\sim} M$ and $\phi_2\colon N \xrightarrow{\sim} N$ that necessarily

[1] Of course 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 by a "prime" of a Dedekind domain A (or of its fraction field K) we mean a nonzero prime ideal of A.

have unit determinants (each corresponds to a change of basis). The *module index* $[M:N]_A$ is the 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.

We observe that

$$([M:N]_A)_{\mathfrak{p}} = [M_{\mathfrak{p}}:N_{\mathfrak{p}}]_{A_{\mathfrak{p}}},$$

since for any prime $\mathfrak{q} \neq \mathfrak{p}$ the A-module $[M_{\mathfrak{q}}:N_{\mathfrak{q}}]_{A_{\mathfrak{q}}} = \det(\hat{\phi}_q)A_{\mathfrak{q}} \subseteq K$ contains elements of every possible $\mathfrak{p}$-adic valuation (because $A_{\mathfrak{q}}$ does); if we localize it at $\mathfrak{p}$ we will just get $K \supseteq [M_{\mathfrak{p}}:N_{\mathfrak{p}}]_{A_{\mathfrak{p}}}$. This implies, in particular, that the module index $[M:N]_A$ is always nonzero, hence an element of the ideal group $\mathcal{I}_A$. If M, N, P are A-lattices in V then

$$[M:N]_A[N:P]_A = [M:P]_A, \tag{1}$$

since for each prime $\mathfrak{p}$ we can write any isomorphism $M_{\mathfrak{p}} \xrightarrow{\sim} P_{\mathfrak{p}}$ as a composition of isomorphisms $M_{\mathfrak{p}} \xrightarrow{\sim} N_{\mathfrak{p}} \xrightarrow{\sim} P_{\mathfrak{p}}$; we then note that the determinant map is multiplicative with respect to composition and multiplication of fractional ideals is compatible with localization. Taking $P = M$ yields the identity

$$[M:N]_A[N:M]_A = [M:M]_A = A, \tag{2}$$

thus $[M:N]_A$ and $[N:M]_A$ are inverses in the ideal group $\mathcal{I}_A$. We note that when $N \subseteq M$ the module index $[M:N]_A \subseteq A$ is actually an ideal (not just a fractional ideal), since in this case we can express a basis for $N_{\mathfrak{p}}$ as $A_{\mathfrak{p}}$-linear combinations of a basis for $M_{\mathfrak{p}}$, and the matrix for $\hat{\phi}_{\mathfrak{p}}$ will then have entries (and determinant) in $A_{\mathfrak{p}}$.

Remark 6.2. In the special case $V = K$, an A-lattice in V is simply a fractional ideal of A. In this setting each module index $[M:N]_A$ corresponds to a colon ideal

$$[M:N]_A = (N:M). \tag{3}$$

Note that the order of M and N is **reversed**. This unfortunate conflict of notation arises from the fact that the module index is generalizing the notion of an index (for example, $[\mathbb{Z}:2\mathbb{Z}]_{\mathbb{Z}} = ([\mathbb{Z}:2\mathbb{Z}]) = (2)$), whereas colon ideals are generalizing the notion of a ratio (for example, $(\mathbb{Z}:2\mathbb{Z}) = (1:2) = (1/2)$). To see why (3) holds, let π be a uniformizer for $A_{\mathfrak{p}}$. Then $M_{\mathfrak{p}} = (\pi^m)$ and $N_{\mathfrak{p}} = (\pi^n)$ for some $m, n \in \mathbb{Z}$, and we may take $\phi_{\mathfrak{p}}$ to be the multiplication-by-π^{n-m} map. We then have

$$[M_{\mathfrak{p}}:N_{\mathfrak{p}}]_{A_{\mathfrak{p}}} = (\det \hat{\phi}_{\mathfrak{p}}) = (\pi^{n-m}) = (\pi^n/\pi^m) = (N_{\mathfrak{p}}:M_{\mathfrak{p}}).$$

It follows from the remark that if M and N are nonzero fractional ideals of A then

$$M[M:N]_A = M(N:M) = N.$$

(note we are using the fact that A is a Dedekind domain; we always have $M(N:M) \subseteq N$ but equality does not hold in general), and if $N \subseteq M$ then $I := [M:N]_A \subseteq A$ is an ideal and we have $MI = N = NA$ and therefore $M/N \simeq A/I$ as quotients of A-modules. It follows that $I = \{a \in A : aM \subseteq N\}$ is the *annihilator* of M/N, which is a *cyclic* A-module (has a single generator), since A/I is clearly cyclic (generated by the image of 1). Conversely, if we know that $M/N \simeq A/I$ for nonzero fractional ideals $N \subseteq M$, then we necessarily have $I = [M:N]_A$. The following theorem generalizes this observation.

Theorem 6.3. *Let A be a Dedekind domain with fraction field K, and let $N \subseteq M$ be A-lattices in a K-vector space V of dimension r for which the quotient module M/N is a direct sum of cyclic A-modules:*

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

where $I_1, \ldots, I_n$ are ideals of A. Then

$$[M : N]_A = I_1 \cdots I_n.$$

Proof. Let $\mathfrak{p}$ be a prime of A, let π be a uniformizer for $A_\mathfrak{p}$, and let $e_j = v_\mathfrak{p}(I_j)$ for $1 \le j \le n$. Pick a basis for $M_\mathfrak{p}$ and an isomorphism $\phi_\mathfrak{p} \colon M_\mathfrak{p} \to N_\mathfrak{p}$ so that $M_\mathfrak{p}/N_\mathfrak{p} = \operatorname{coker} \phi_\mathfrak{p}$. The matrix of $\phi_\mathfrak{p}$ is an $r \times r$ matrix over the PID $A_\mathfrak{p}$ with nonzero determinant. It therefore has Smith normal form UDV, with $U, V \in \operatorname{GL}_r(A_\mathfrak{p})$ and $D = \operatorname{diag}(\pi^{d_1}, \ldots, \pi^{d_r})$ for some uniquely determined nonnegative integers $d_1 \le \cdots \le d_r$. We then have

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

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 therefore have $\sum_{j=1}^n e_j = \sum_{i=1}^r d_i$, and applying the definition of the module index yields

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

It follows that $[M : N]_A = I_1 \cdots I_n$, since the localizations $([M : N]_A)_\mathfrak{p} = [M_\mathfrak{p} : N_\mathfrak{p}]_{A_\mathfrak{p}}$ and $(I_1 \cdots I_n)_\mathfrak{p}$ coincide for every prime $\mathfrak{p}$. □

6.2 The ideal norm

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. As we proved in the previous lecture, every fractional B-ideal I is an A-lattice in L, so let us consider

$$\begin{aligned} \mathcal{I}_B &\to I_A \\ I &\mapsto [B : I]_A. \end{aligned}$$

Definition 6.4. 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 extend $N_{B/A}$ to the zero ideal by defining $N_{B/A}((0)) = (0)$.

We now show that the ideal norm $N_{B/A}$ is compatible with the field norm $\mathrm{N}_{L/K}$.

Proposition 6.5. *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. □

Proposition 6.6. *Assume AKLB. The map $N_{B/A}\colon \mathcal{I}_B \to \mathcal{I}_A$ is a group 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

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

□

Corollary 6.7. *Assume AKLB. For all $I, J \in \mathcal{I}_B$ we have*

$$[I : J]_A = N_{B/A}(I^{-1}J) = N_{B/A}((J : I))$$

Proof. The second equality is immediate: $(J : I) = I^{-1}J$ (because B is a Dedekind domain). The first follows from (1), (2), and the previous proposition. Indeed, we have

$$[I : J]_A = [I : A]_A[A : J]_A = [A : I]_A^{-1}[A : J]_A = N_{B/A}(I^{-1})N_{B/A}(J) = N_{B/A}(I^{-1}J).$$

□

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

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

□

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.

$$\begin{tikzcd}
K^\times \arrow[r, hook] \arrow[d, "(x)"] & L^\times \arrow[d, "(y)"] \\
\mathcal{I}_A \arrow[r, "I \mapsto IB"] & \mathcal{I}_B
\end{tikzcd}
\qquad
\begin{tikzcd}
L^\times \arrow[r, "N_{L/K}"] \arrow[d, "(y)"] & K^\times \arrow[d, "(x)"] \\
\mathcal{I}_B \arrow[r, "N_{B/A}"] & \mathcal{I}_A
\end{tikzcd}$$

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 $f_{\mathfrak{q}}$ (by definition); as a quotient of A-modules, we have $B/\mathfrak{q} \simeq A/\mathfrak{p} \oplus \cdots \oplus A/\mathfrak{p}$, an $f_{\mathfrak{q}}$-fold direct sum of cyclic A-modules $A/\mathfrak{p}$, and we may apply Theorem 6.3. 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

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

6.3 The ideal norm 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 (while glossing over some details).

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.[3] 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, which is called the *generic point*). When the field of constants k is algebraically closed, Hilbert's Nullstellensatz gives a one-to-one 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 $\operatorname{Gal}(\bar{k}/k)$-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

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

where e_Q is the ramification index (one then extends $\mathbb{Z}$-linearly: $\phi^*(\sum n_P P) = \sum n_P \phi^*(P)$). Geometrically we think of e_Q as the "multiplicity" of Q in the fiber above P, although e_Q

[3] 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 function field of X, not just those arising from primes. This distinction does not affect our discussion here but will become relevant in later lectures.

is typically defined algebraically as the ramification index of the prime Q in the Dedekind extension B/A as we have done (alternatively, as we shall see in later lectures, it can be defined in terms of valuations on $k(X)$ and $k(Y)$ associated to P and 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 by

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

where f_Q counts the number of $\bar{k}$-points in the $\operatorname{Gal}(\bar{k}/k)$-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). This is precisely the residue field degree of Q as a prime in the Dedekind extension B/A. Note that when $k = \bar{k}$ we always have $f_Q = 1$ (so over algebraically closed fields one typically omits f_Q from the pushforward map and the degree formula below).

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 (by Theorem 5.31). It is a weighted measure of the cardinality of the fibers of ϕ that reflects both the ramification and degree of each closed point in the fiber (and as a consequence, it is the same for every fiber and is an invariant of ϕ).

6.4 The ideal norm in number fields

We now consider the special case $A = \mathbb{Z}$, $K = \mathbb{Q}$, where $B = \mathcal{O}_L$ 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 Theorem 6.9 implies

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

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

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

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 $\mathrm{N}(\mathfrak{a}) = \big([\mathcal{O}_L : \mathfrak{a}]\big)$, and if $\mathfrak{b} \subseteq \mathfrak{a}$ are nonzero fractional ideals, then*

$$[\mathfrak{a} : \mathfrak{b}]_\mathbb{Z} = ([\mathfrak{a} : \mathfrak{b}]).$$

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 $[\mathcal{O}_L : \mathfrak{a}] = \prod_i [\mathcal{O}_L : \mathfrak{q}_i^{e_i}]$. It thus suffices to consider the case where $\mathfrak{a}$ a prime power $\mathfrak{q}^e$, since N is a group homomorphism. For $0 \le i < e$ each quotient $\mathfrak{q}^i/\mathfrak{q}^{i+1}$ is both an $(\mathcal{O}_L/\mathfrak{q})$-vector space and a ring with maximal ideal (0) (there are no ideals properly between $\mathfrak{q}^e$ and $\mathfrak{q}^{e+1}$), hence 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 $\mathrm{N}(\mathfrak{q}) = (p)^f = (p^f)$, and $\mathrm{N}(\mathfrak{q}^e) = (p^{ef})$, 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 $[\mathfrak{a} : \mathfrak{b}]_{\mathbb{Z}} = [\alpha\mathfrak{a} : \alpha\mathfrak{b}]_{\mathbb{Z}}$, so we can assume without loss of generality that $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in $\mathcal{O}_L$. 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

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

and therefore $([\mathfrak{a} : \mathfrak{b}]) = \mathrm{N}(\mathfrak{a}^{-1}\mathfrak{b}) = [\mathfrak{a} : \mathfrak{b}]_{\mathbb{Z}}$, by Corollary 6.7. □

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 $\mathrm{N} \colon \mathcal{I}_{\mathcal{O}_L} \to \mathcal{I}_{\mathbb{Z}}$ as a homomorphism $\mathrm{N} \colon \mathcal{I}_{\mathcal{O}_L} \to \mathbb{Q}^\times_{>0}$ from ideal group of $\mathcal{O}_L$ to the multiplicative group of positive rational numbers. If we write $\mathrm{N}(\mathfrak{a})$ in contexts where an element of $\mathbb{Z}$ or $\mathbb{Q}$ (or $\mathbb{R}$) is expected, it is always with this understanding. When $\mathfrak{a} = (a)$ is a nonzero principal fractional ideal we may also write $\mathrm{N}(a) \coloneqq \mathrm{N}((a)) = |\mathrm{N}_{L/\mathbb{Q}}(a)|$; this is a positive rational number, and for $a \in \mathcal{O}_K$, a positive integer.

6.5 The Dedekind-Kummer theorem

We now give a theorem that provides a practical method for factoring primes in Dedekind 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 are a finite separable extensions L/K (the $AKLB$ setup).

The primitive element theorem implies when L/K is a finite separable extension we can always write $L = K(\alpha)$ for some $\alpha \in L$, and in the $AKLB$ setup we can assume $\alpha \in B$, by Proposition 5.15. This does **not** imply that $B = A[\alpha]$; indeed, it may very will 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* $\{\beta_1, \ldots, \beta_n\}$ that is both an A-basis for B and a K-basis for L. But monogenicity is a much stronger condition: it implies that B has an *integral power basis*, one of the form $\{1, \alpha, \ldots, \alpha^{n-1}\}$. When $A = \mathbb{Z}$ every B has an integral basis, but very few have an integral power basis. Examples of monogenic extensions include quadratic and cyclotomic number fields (as extensions of $\mathbb{Q}$); see Problem Set 3 for proofs of these facts and some examples of non-monogenic number fields.

We will first prove the Dedekind-Kummer theorem assuming we have a monogenic extension; in the next lecture we will address the general case.

Theorem 6.13 (Dedekind-Kummer). *Assume $AKLB$ with $L = K(\alpha)$ and $\alpha \in B$. Let $f \in A[x]$ be the minimal polynomial of α and let*

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

be its factorization into monic irreducibles in $(A/\mathfrak{p})[x]$. Let $\mathfrak{q}_i := (\mathfrak{p}, g_i(\alpha))$, where $g_i \in A[x]$ is any lift of $\bar{g}_i$ in $(A/\mathfrak{p})[x]$ under the reduction map $A[x] \to (A/\mathfrak{p})[x]$. If $B = A[\alpha]$ 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 field degree of $\mathfrak{q}_i$ is $\deg \bar{g}_i$.

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 $\alpha = \zeta_5$ is a primitive 5th root of unity with minimal polynomial $f(x) = x^4 + x^3 + x^2 + x + 1$. Then $B = \mathcal{O}_L = \mathbb{Z}[\zeta_5]$ and we can use the theorem to factor any prime of $\mathbb{Z}$ in $\mathcal{O}_L$:

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

The four cases above 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, thus $(\bar{g}_i(x))$ is a maximal ideal (because $(A/\mathfrak{p})[x]$ is a UFD of dimension 1), so the quotient $(A/\mathfrak{p})[x]/(\bar{g}_i(x))$ is a field; indeed, it is an extension of the residue field $A/\mathfrak{p}$ of degree $\deg g_i$. It follows that $\mathfrak{q}_i$ is a prime above $\mathfrak{p}$ with residue field degree $f_{\mathfrak{q}_i} = \deg \bar{g}_i$ as claimed.

The ideal $\prod_i \mathfrak{q}_i^{e_i} = \prod_i (\mathfrak{p}, g_i(\alpha))^{e_i} = \prod_i (\mathfrak{p}B + (g_i(\alpha))^{e_i}$ is divisible by $\mathfrak{p}B$, since if we expand the ideal product every term is clearly divisible by $\mathfrak{p}B$, including

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

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

$$N_{B/A}\left(\prod_i \mathfrak{q}_i^{e_i}\right) = \prod_i N_{B/A}(\mathfrak{q}_i)^{e_i} = \prod_i (\mathfrak{p}^{f_{\mathfrak{q}_i}})^{e_i} = \mathfrak{p}^{e_i \deg \bar{g}_i} = \mathfrak{p}^{\deg f} = \mathfrak{p}^{[L:K]},$$

so $\sum_i e_i f_{\mathfrak{q}_i} = [L:K] = \sum_{\mathfrak{q}|\mathfrak{p}} e_{\mathfrak{q}} f_{\mathfrak{q}}$. We must have $e_i = e_{\mathfrak{q}_i}$ and the theorem follows. □

We now want to remove the monogenic hypothesis from Theorem 6.13 We can always write $L = K(\alpha)$ for some $\alpha \in B$ (since L/K is separable), but in general the ring $A[\alpha]$ may be a proper subring of B. The relationship between $A[\alpha]$ and B is characterized by the *conductor* of the extension $B/A[\alpha]$.

6.6 The conductor of a ring

We first give the general definition then specialize to subrings of Dedekind domains.

Definition 6.15. Let S/R be an extension of commutative rings. The *conductor of R in S* is the largest S-ideal that is also an R-ideal; equivalently, it is the largest ideal of S contained in R. It can be written as

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

If R is an integral domain, the *conductor of R* is the conductor of R in its integral closure.

Example 6.16. The conductor of $\mathbb{Z}$ in $\mathbb{Z}[i]$ is (0). The conductor of $\mathbb{Z}[\sqrt{-3}]$ in $\mathbb{Z}[\zeta_3]$ is $(2, 1+\sqrt{-3})$ (these may be viewed as generators over $\mathbb{Z}[\sqrt{-3}]$ or $\mathbb{Z}[\zeta_3]$, or even just $\mathbb{Z}$).

We are interested in the case where R is a noetherian domain.

Lemma 6.17. *Let R be a noetherian domain. The conductor of R in its integral closure S is nonzero if and only if S is finitely generated as an R-module.*

Proof. This is a special case of Lemma 3.3. □

Recall that we defined a fractional ideal of a noetherian domain R as a finitely generated R-submodule of its fraction field. If R has nonzero conductor then its integral closure S is a fractional ideal of R that is also a ring. This means we can write S as $\frac{1}{r}I$ for some $r \in R$ and R-ideal I, and the conductor $\mathfrak{c}$ is precisely the set of denominators $r \in R$ for which $S = \frac{1}{r}I$ for some R-ideal I (note that the representation $\frac{1}{r}I$ is far from unique).

6.7 Orders in Dedekind domains

We now introduce the notion of an *order* (in a Dedekind domain). This should not be confused with the notion of a reflexive, transitive, antisymmetric relation on a set, rather it is a literal translation of the German *Ordnung*, which refers to a ring of algebraic integers.

Definition 6.18. An *order* $\mathcal{O}$ is a noetherian domain of dimension one whose conductor is nonzero, equivalently, whose integral closure is finitely generated as an $\mathcal{O}$-module.[4]

Every Dedekind domain that is not a field is also an order. The integral closure of an order is always a Dedekind domain, but not every ring whose integral closure is a Dedekind domain is an order: as shown by Nagata [3, p. 212], one can construct noetherian domains of dimension one with zero conductor. But in the case of interest to us the conductor is automatically nonzero: in the $AKLB$ setup B is finitely generated over A (by Proposition 5.19), hence over every intermediate ring between A and B, including all those whose integral closure is B. In particular, if $A[\alpha]$ and B have the same fraction field (so $L = K(\alpha)$), then $A[\alpha]$ is an order in B (assuming $B \neq L$).

There is an alternative definition of an order that coincides with our definition in the case of interest to us.

Definition 6.19. Let A be a noetherian domain with fraction field K, and let L be a (not necessarily commutative) K-algebra of finite dimension. An A-*order* in L is an A-lattice that is also a ring (recall that an A-lattice is a finitely generated A-submodule that spans).

[4] Not all authors require an order to have nonzero conductor (e.g. Neukirch [4, §I.12]), but nearly all of the interesting theorems about orders require this assumption, so we include it in the definition.

Remark 6.20. In general the K-algebra L (and the order $\mathcal{O}$) in Definition 6.19 need not be commutative (even though A necessarily is). For example, the endomorphism ring of an elliptic curve is isomorphic to a $\mathbb{Z}$-order in a $\mathbb{Q}$-algebra L of dimension 1, 2, or 4. This $\mathbb{Z}$-order is necessarily commutative in dimensions 1 and 2, where L is either $\mathbb{Q}$ or an imaginary quadratic field, but it is non-commutative in dimension 4, where L is a quaternion algebra.

Proposition 6.21. *Assume $AKLB$ and let $\mathcal{O}$ be a subring of L. Then $\mathcal{O}$ is an A-order in L if and only if it is an order with integral closure B.*

Proof. We first recall that under our $AKLB$ assumption, $\dim A = 1$, hence $\dim B = 1$, since $A = B \cap K$, and $\mathcal{O} \subseteq L$ is an A-module containing 1, so it contains A.

Suppose $\mathcal{O}$ is an A-order in L. Then $\mathcal{O}$ is an A-lattice, hence finitely generated as an A-module, and therefore integral over A (see [1, Thm. 10.8], for example). Thus $\mathcal{O}$ lies in the integral closure B of A in L. The fraction field of $\mathcal{O}$ is a K-vector space spanning L, hence equal to L, so $\mathcal{O}$ and B have the same fraction field and B is the integral closure of $\mathcal{O}$. Thus $\mathcal{O}$ is a domain of dimension 1 (since B is), and it is noetherian because it is a finitely generated over the noetherian ring A. The integral closure B of $\mathcal{O}$ is finitely generated over A, hence over $\mathcal{O}$; therefore $\mathcal{O}$ is an order.

Now suppose $\mathcal{O}$ is an order with integral closure B. It is an A-submodule of the noetherian A-module B, hence finitely generated over A. It contains a K-basis for L because L is its fraction field (take any K-basis for L written as fractions over $\mathcal{O}$ and clear denominators). Thus $\mathcal{O}$ is an A-lattice in L that is also a ring, hence it is an A-order in L. □

Remark 6.22. There may be subrings $\mathcal{O}$ of L that are orders but not A-orders in L, but these do not have B as their integral closure. Consider $A = B = \mathbb{Z}$, $K = L = \mathbb{Q}$, and $\mathcal{O} = \mathbb{Z}_{(2)}$, for example. In this case $\mathcal{O}$ is a DVR, hence a Dedekind domain, hence an order, but it is not an A-order in L, because it is is not finitely generated over A. But its integral closure is not B (indeed, $\mathcal{O} \not\subseteq B$).

Remark 6.23. An A-order in L is a *maximal order* if it is not properly contained in any other A-order in L. When A is a Dedekind domain one can show that every A-order in L lies in a maximal order. Maximal orders are not unique in general, but in the $AKLB$ setup B is the unique maximal order.

As with Dedekind domains, we call a nonzero prime ideal $\mathfrak{p}$ in an order $\mathcal{O}$ a *prime* of $\mathcal{O}$, and if $\mathfrak{q}$ is a prime of the integral closure B of $\mathcal{O}$ lying above $\mathfrak{p}$ (dividing $\mathfrak{p}B$) then we may write $\mathfrak{q}|\mathfrak{p}$ to indicate this. As in the $AKLB$ setup, we have $\mathfrak{q}|\mathfrak{p}$ if and only if $\mathfrak{q} \cap \mathcal{O} = \mathfrak{p}$, by Lemma 5.25. The fact that B is integrally closed ensures that every prime $\mathfrak{p}$ of $\mathcal{O}$ has at least one prime $\mathfrak{q}$ lying above it (this is a standard fact of commutative algebra). We thus have a surjective map

$$\begin{aligned} \operatorname{Spec} B &\twoheadrightarrow \operatorname{Spec} \mathcal{O} \\ \mathfrak{q} &\mapsto \mathfrak{q} \cap \mathcal{O} \end{aligned}$$

If a prime $\mathfrak{q}$ of B contains the conductor $\mathfrak{c}$, then so does $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}$ (since $\mathfrak{c} \subseteq \mathbb{P}$), and conversely. It follows that the map is $\operatorname{Spec} B \to \operatorname{Spec} O$ is still well-defined if we restrict to primes that do not contain $\mathfrak{c}$. In B we can factor $\mathfrak{c}$ into a product of powers of finitely many primes $\mathfrak{q}$; it follows that only finitely many primes $\mathfrak{p}$ of $\mathcal{O}$ contain $\mathfrak{c}$.

Proposition 6.24. *In any order $\mathcal{O}$, only finitely many primes contain the conductor.*

We now show that when we restrict to primes that do not contain the conductor the map $\operatorname{Spec} B \to \operatorname{Spec} O$ becomes a bijection.

Lemma 6.25. *Let $\mathcal{O}$ be an order with integral closure B and conductor $\mathfrak{c}$ and let $\mathfrak{p}$ be a prime of $\mathcal{O}$ not containing $\mathfrak{c}$. Then $\mathfrak{p}B$ is prime of B.*

Proof. Let $\mathfrak{q}$ be a prime of B lying above $\mathfrak{p}$, so that $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}$, and pick an element $s \in \mathfrak{c}$ not in $\mathfrak{p}$ (and hence not in $\mathfrak{q}$). Claim: $\mathcal{O}_\mathfrak{p} = B_\mathfrak{q}$. To see that $\mathcal{O}_p \subseteq B_\mathfrak{q}$, note that if $a/b \in \mathcal{O}_\mathfrak{p}$ with $a \in \mathcal{O}$ and $b \in \mathcal{O} - \mathfrak{p}$, then $b \in B - \mathfrak{q}$, so $a/b \in B_\mathfrak{q}$. Conversely, if $a/b \in B_\mathfrak{q}$ with $a \in B$ and $b \in B - \mathfrak{q}$ then $sa \in \mathcal{O}$ and $sb \in \mathcal{O} - \mathfrak{p}$, so $(sa)/(sb) = a/b \in \mathcal{O}_p$; here we have used that $sB \subseteq \mathcal{O}$ (since $s \in \mathfrak{c}$) and $sb \notin \mathfrak{q}$ (since $s, b \notin \mathfrak{q}$), so $sb \notin \mathfrak{p}$.

We now note that $\mathfrak{q}'|\mathfrak{p} \Rightarrow B_{\mathfrak{q}'} = \mathcal{O}_\mathfrak{p} = B_\mathfrak{q} \Rightarrow \mathfrak{q}' = \mathfrak{q}$, so there is only one prime $\mathfrak{q}$ lying above $\mathfrak{p}$. It follows that $\mathfrak{p}B = \mathfrak{q}^e$ for some $e \geq 1$, and we claim that $e = 1$. Indeed, we must have $\mathfrak{p}\mathcal{O}_\mathfrak{p} = \mathfrak{q}B_\mathfrak{q}$ (this is the unique maximal ideal of the local ring $\mathcal{O}_\mathfrak{p} = B_\mathfrak{q}$ written in two different ways), so $\mathfrak{q}^e B_\mathfrak{q} = \mathfrak{q}B_\mathfrak{q}$ and therefore $e = 1$. □

Corollary 6.26. *Let $\mathcal{O}$ be an order with integral closure B and conductor $\mathfrak{c}$. The restriction of the map $\operatorname{Spec} B \to \operatorname{Spec} \mathcal{O}$ defined by $\mathfrak{q} \mapsto \mathfrak{q} \cap \mathcal{O}$ to prime ideals not containing $\mathfrak{c}$ is a bijection with inverse $\mathfrak{p} \mapsto \mathfrak{p}B$.*

We now note several conditions on primes of $\mathcal{O}$ that are equivalent to not containing the conductor; these notably include the property of being invertible.

Theorem 6.27. *Let $\mathcal{O}$ be an order with integral closure B and conductor $\mathfrak{c}$, and let $\mathfrak{p}$ be a prime of $\mathcal{O}$. The following are equivalent:*

(a) *$\mathfrak{p}$ does not contain $\mathfrak{c}$;*

(b) *$\mathcal{O} = \{x \in B : x\mathfrak{p} \subseteq \mathfrak{p}\}$;*

(c) *$\mathfrak{p}$ is invertible;*

(d) *$\mathcal{O}_\mathfrak{p}$ is a DVR;*

(e) *$\mathfrak{p}\mathcal{O}_\mathfrak{p}$ is principal.*

If any of these equivalent properties hold, then $\mathfrak{p}B$ is a prime of B.

Proof. See Problem Set 4. □

Remark 6.28. Orders in Dedekind domains also have a geometric interpretation. If $\mathcal{O}$ is an order, the curve $X = \operatorname{Spec} \mathcal{O}$ will have a singularity at each closed point P corresponding to a maximal ideal of $\mathcal{O}$ that contains the conductor. Taking the integral closure B of $\mathcal{O}$ yields a smooth curve $Y = \operatorname{Spec} B$ with the same function field as X and a morphism $Y \to X$ that looks like a bijection above non-singular points (a dominant morphism of degree 1). The curve Y is called the *normalization* of X.

Recall that two ideals I and J in a ring A are said to be *relatively prime* or *coprime* if $I + J = A$; we may also say that I is *prime to* J. When A is a noetherian domain this is equivalent to requiring that $I_\mathfrak{p} + J_\mathfrak{p} = A_\mathfrak{p}$ for every prime ideal $\mathfrak{p}$ of A; this follows from Proposition 2.7 and Lemma 3.13. For prime ideals $\mathfrak{p}$ that do not contain J, we have $J_\mathfrak{p} = A_\mathfrak{p}$, in which case $I_\mathfrak{p} + J_\mathfrak{p} = A_\mathfrak{p}$ certainly holds, so we only need to consider the case where $\mathfrak{p}$ contains J. In this case $J_\mathfrak{p}$ is contained in $\mathfrak{p}A_\mathfrak{p}$ and $I_\mathfrak{p} + J_\mathfrak{p} = A_\mathfrak{p}$ if and only if $I_\mathfrak{p} \not\subseteq \mathfrak{p}A_\mathfrak{p}$, in which case $I_\mathfrak{p} = A_\mathfrak{p}$, equivalently, $IA_\mathfrak{p} = A_\mathfrak{p}$. This leads to the following definition.

Definition 6.29. Let A be a noetherian domain and let J be an ideal of A. A fractional ideal I of A is *prime to* J if $IA_\mathfrak{p} = A_\mathfrak{p}$ for all prime ideals $\mathfrak{p}$ that contain J. The set of invertible fractional ideals prime to J is denoted $\mathcal{I}_A^J$; it is a subgroup of the ideal group $\mathcal{I}_A$.

To check that $\mathcal{I}_A^J$ is in fact a subgroup, we note that if $\mathfrak{p}$ is any prime containing J then (a) $(1)A_\mathfrak{p} = A_\mathfrak{p}$, (b) if $IA_\mathfrak{p} = A_\mathfrak{p}$ then $I^{-1}A_\mathfrak{p} = I^{-1}IA_\mathfrak{p} = A_\mathfrak{p}$ (c) if $I_1A_\mathfrak{p} = A_\mathfrak{p}$ and $I_2A_\mathfrak{p} = A_\mathfrak{p}$ then $I_1I_2A_\mathfrak{p} = I_2A_\mathfrak{p} = A_\mathfrak{p}$.

Theorem 6.30. *Let $\mathcal{O}$ be an order with integral closure B. Let $\mathfrak{c}$ be any ideal of B contained in the conductor of $\mathcal{O}$. The map $\mathfrak{q} \mapsto \mathfrak{q} \cap \mathcal{O}$ induces a group isomorphism from $\mathcal{I}_B^\mathfrak{c}$ to $\mathcal{I}_\mathcal{O}^\mathfrak{c}$ and both groups are isomorphic to the free abelian group generated by their prime ideals. In particular, every fractional ideal of $\mathcal{O}$ prime to the conductor has a unique factorization into prime ideals $\prod \mathfrak{p}_i^{e_i}$ which matches the factorization $IB = \prod \mathfrak{q}_i^{e_i}$ with $\mathfrak{p}_i = \mathfrak{q}_i \cap \mathcal{O}$.*

Proof. The B-ideal $\mathfrak{c}$ lies in the conductor of $\mathcal{O}$ and is therefore also an $\mathcal{O}$-ideal, so the subgroups $\mathcal{I}_B^\mathfrak{c}$ and $\mathcal{I}_\mathcal{O}^\mathfrak{c}$ are well defined and the map $\mathfrak{q} \to \mathfrak{q} \cap \mathcal{O}$ gives a bijection between the sets of prime ideals contained in these subgroups, by Corollary 6.26; the theorem follows. □

We now return to the $AKLB$ setup. Let $\mathcal{O}$ be an order in B with conductor $\mathfrak{c}$. For example, we could take $\mathcal{O}[\alpha]$ where $L = K(\alpha)$ and $\alpha \in B$, as in the Dedekind-Kummer Theorem. Theorem 6.30 implies that we can determine how primes of A split in B by looking at their factorizations in $\mathcal{O}$, provided we restrict to primes $\mathfrak{p}$ that do not contain $\mathfrak{c} \cap A$. This restriction ensures that the primes $\mathfrak{q}$ of B and $\mathfrak{q}' = \mathfrak{q} \cap \mathcal{O}$ lying above $\mathfrak{p}$ will all be prime to $\mathfrak{c}$ and hence to the conductor and the factorizations of $\mathfrak{p}B$ and $\mathfrak{p}\mathcal{O}$ will match. In order to complete the picture, we now show that the residue field degrees of the primes in these factorizations also match.

Proposition 6.31. *Assume $AKLB$ and let $\mathcal{O}$ be an order with integral closure B. Let $\mathfrak{c} = (\mathfrak{c}' \cap A)B$, where $\mathfrak{c}'$ is the conductor of $\mathcal{O}$. Then $\mathcal{O}$ is an A-lattice in L and the restrictions of the norm maps $N_{B/A}$ and $N_{\mathcal{O}/A}$ to $I_B^\mathfrak{c}$ and $\mathcal{I}_\mathcal{O}^\mathfrak{c}$ commute with the isomorphism $\mathcal{I}_B^\mathfrak{c} \to \mathcal{I}_\mathcal{O}^\mathfrak{c}$ defined by $\mathfrak{q} \mapsto \mathfrak{q} \cap \mathcal{O}$. If $\mathfrak{q}$ is a prime of B that does not contain $\mathfrak{c}$ and $\mathfrak{q}' = \mathfrak{q} \cap \mathcal{O}$ and $\mathfrak{p} = \mathfrak{q} \cap A$, then $N_{B/A}(\mathfrak{q}) = N_{\mathcal{O}/A}(\mathfrak{q}') = \mathfrak{p}^{f_\mathfrak{q}}$ and $[B/\mathfrak{q}B : A/\mathfrak{p}] = [\mathcal{O}/\mathfrak{q}' : A\mathfrak{p}]$.*

Proof. That $\mathcal{O}$ is an A-lattice in L follows from Proposition 6.21. Let $\mathfrak{q}$ be a prime of B that does not contain $\mathfrak{c}$, and define $\mathfrak{q}' := \mathfrak{q} \cap \mathcal{O}$ and $\mathfrak{p} := \mathfrak{q} \cap A$. If $\mathfrak{p}'$ is any prime of A other than $\mathfrak{p}$, then the localization of $\mathfrak{q}$ at $\mathfrak{p}'$ contains B and the localization of $\mathfrak{q}'$ at $\mathfrak{p}$ contains $\mathcal{O}$ (pick $a \in \mathfrak{p} - \mathfrak{p}'$ and note that $a/a = 1$ lies in both $\mathfrak{q}$ and $\mathfrak{q}'$); we thus have

$$N_{B/A}(\mathfrak{q})_{\mathfrak{p}'} = [B_{\mathfrak{p}'} : \mathfrak{q}_{\mathfrak{p}'}]_{A_{\mathfrak{p}'}} = [B_{\mathfrak{p}'} : B_{\mathfrak{p}'}]_{A_{\mathfrak{p}'}} = A_{\mathfrak{p}'} = [\mathcal{O}_{\mathfrak{p}'} : \mathcal{O}_{\mathfrak{p}'}]_{A_{\mathfrak{p}'}} = [\mathcal{O}_{\mathfrak{p}'} : \mathfrak{q}'_{\mathfrak{p}'}]_{A_{\mathfrak{p}'}} = N_{\mathcal{O}/A}(\mathfrak{q}')_{\mathfrak{p}'}$$

For the prime $\mathfrak{p}$ we proceed as in the proof of Lemma 6.25 and pick $s \in (\mathfrak{c} \cap A) - \mathfrak{p}$. We then find that $B_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$ and $\mathfrak{q}_\mathfrak{p} = \mathfrak{q}'_\mathfrak{p}$, and therefore

$$N_{B/A}(\mathfrak{q})_\mathfrak{p} = [B_\mathfrak{p} : \mathfrak{q}_\mathfrak{p}]_{A_\mathfrak{p}} = [\mathcal{O}_\mathfrak{p} : \mathfrak{q}'_\mathfrak{p}]_{A_\mathfrak{p}} = N_{\mathcal{O}/A}(\mathfrak{q}')_\mathfrak{p}.$$

Thus $N_{B/A}(\mathfrak{q})_\mathfrak{p} = N_{B/A}(\mathfrak{q}')_\mathfrak{p}$ for all primes $\mathfrak{p}$ of A, and

$$N_{B/A}(\mathfrak{q}) = \cap_\mathfrak{p} N_{B/A}(\mathfrak{q})_\mathfrak{p} = \cap_\mathfrak{p} N_{B/A}(\mathfrak{q}')_\mathfrak{p} = N_{\mathcal{O}/A}(\mathfrak{q}').$$

The proof that $N_{B/A}(\mathfrak{q}) = \mathfrak{p}^{f_\mathfrak{q}}$ in Theorem 6.9 does not depend on the fact that B is a Dedekind domain and applies equally to the order $\mathcal{O}$. Thus $N_{\mathcal{O}/A}(\mathfrak{q}') = \mathfrak{p}^{f_{\mathfrak{q}'}}$, where $f_{\mathfrak{q}'} := [\mathcal{O}/\mathfrak{q}' : A/\mathfrak{p}]$. We therefore have $f_{\mathfrak{q}'} = f_\mathfrak{q}$ and $[B/\mathfrak{q} : A/\mathfrak{p}] = [\mathcal{O}/q' : A/\mathfrak{p}]$ as claimed. □

Corollary 6.32. *The assumption $B = A[\alpha]$ in the Dedekind-Kummer theorem can be replaced with the assumption that $\mathfrak{p}B$ is prime to the conductor of $A[\alpha]$ in B.*

References

[1] Allen Altman and Steven Kleiman, *A term of commutative algebra*, Worldwide Center of Mathematics, 2013.

[2] Albrecht Fröhlich, *Ideals in an extension field as modules over the algebraic integers in a finite number field*, Math. Z. **74** (1960), 29–38.

[3] M. Nagata, *Local rings*, John Wiley & Sons, 1962.

[4] J. Neukirch, *Algebraic number theory*, Springer, 1999.

18.785 Number Theory I
Fall 2016