# 6 Ideal norms and the Dedekind-Kummer theorem

In order to better understand how ideals split in Dedekind extensions we want to extend our definition of the norm map to ideals. Recall that for a ring extension $B/A$ in which $B$ is a free $A$-module of finite rank, we defined the norm map $\mathrm{N}_{B/A}\colon B \to A$ as

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

the determinant of the multiplication-by-$b$ map with respect to an $A$-basis for $B$. If $B$ is a free $A$-module we could define the norm of a $B$-ideal to be the $A$-ideal generated by the norms of its elements, but in the case we are most interested in (our "$AKLB$" setup) $B$ is typically *not* a free $A$-module (even though it is finitely generated as an $A$-module).

To get around this limitation, we introduce the notion of the *module index*, which we will use to define the norm of an ideal. In the special case where $B$ is a free $A$-module, the norm of a $B$-ideal will be equal to the $A$-ideal generated by the norms of elements.

## 6.1 The module index

Our strategy is to define the norm of a $B$-ideal as the intersection of the norms of its localizations at maximal ideals of $A$ (note that $B$ is an $A$-module, so we can view any ideal of $B$ as an $A$-module). Recall that by Proposition 2.6 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 ideals (and 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 [3].

Recall that an $A$-lattice $M$ in a $K$-vector space $V$ is a finitely generated $A$-submodule of $V$ that spans $V$ as a $K$-vector space (Definition 5.9). If $M$ is a free $A$-module, then any $A$-basis for $M$ is also a $K$-basis for $V$, and we must have $M \simeq A^n$, where $n = \dim_K V$. If $A$ is a Dedekind domain, even when $M$ is not free, its localization $M_\mathfrak{p}$ at any prime $\mathfrak{p}$ of $A$ will be a free $A_\mathfrak{p}$-module. This follows from the following facts: (a) $A_\mathfrak{p}$ is a DVR and therefore a PID, (b) $M_\mathfrak{p}$ is a torsion-free $A_\mathfrak{p}$-module, since it lies in a $K$-vector space and $A_\mathfrak{p} \subseteq K$, and (c) any finitely generated torsion-free module over a PID is free.

**Definition 6.1.** Let $A$ be a Dedekind domain with fraction field $K$, let $V$ be an $n$-dimensional $K$-vector space, let $M$ and $N$ be $A$-lattices in $V$, and let $\mathfrak{p}$ be a prime of $A$. Then $A_\mathfrak{p}$ is a PID and we must have $M_\mathfrak{p} \simeq A_\mathfrak{p}^n \simeq N_\mathfrak{p}$, as explained above. 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 principal 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 $A_\mathfrak{p}$-module automorphisms $\phi_1\colon M_\mathfrak{p} \xrightarrow{\sim} M_\mathfrak{p}$ and $\phi_2\colon N_\mathfrak{p} \xrightarrow{\sim} N_\mathfrak{p}$ that necessarily have unit determinants. The *module index* $[M : N]_A$ is the $A$-module

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

where $\mathfrak{p}$ ranges over primes of $A$ and the intersection takes place in $K$. Each $[M_\mathfrak{p}\colon N_\mathfrak{p}]_{A_\mathfrak{p}}$ is an $A$-submodule of $K$ (which need not be finitely generated), so their intersection is clearly an $A$-submodule of $K$, but it is not immediately clear that it finitely generated (or nonzero).

We claim that in fact $[M : N]_A$ is a nonzero fractional ideal of $A$ whose localizations agree with all the local module indexes, that is for every prime $\mathfrak{p}$ of $A$ we have

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

This is obvious when $M$ and $N$ are free $A$-modules: fix a global $A$-module isomorphism $\phi\colon M \xrightarrow{\sim} N$ so that $(\det \hat{\phi})_{\mathfrak{p}} = (\det \hat{\phi}_{\mathfrak{p}})$ for all primes $\mathfrak{p}$ (where $\phi_{\mathfrak{p}}$ is just the $A_{\mathfrak{p}}$-module isomorphism induced by $\phi$). To prove the general case we apply a standard "gluing" argument that will be familiar to those who have studied algebraic geometry.

**Proposition 6.2.** *Let $A$ be a Dedekind domain with fraction field $K$ and let $M$ and $N$ be $A$-lattices in a $K$-vector space of finite dimension. The module index $[M : N]_A$ is a nonzero fractional ideal of $A$ whose localization at each prime $\mathfrak{p}$ of $A$ is equal to the local module index $[M_{\mathfrak{p}} : N_{\mathfrak{p}}]_{A_{\mathfrak{p}}}$.*

*Proof.* The finitely generated $A$-module $M$ is locally free in the sense that the module $M_{\mathfrak{p}}$ is a free $A_{\mathfrak{p}}$-module for every prime $\mathfrak{p}$. It follows from [2, Thm. 19.2] that there exist nonzero $a_1, \dots, a_r \in A$ generating the unit ideal such that each $M[1/a_i]$ is a free $A[1/a_i]$-module (here $M[1/a_i]$ denotes the localization of $M$ with respect to the multiplicative set $\{a_i^n : n \in \mathbb{Z}_{\geq 0}\}$). We similarly have nonzero $b_1, \dots, b_s \in A$ generating the unit ideal such that each $N[1/b_j]$ is a free $A[1/b_j]$-module. For any pair $a_i$ and $b_j$, if we localize at the multiplicative set $S_{ij} \coloneqq \{a_i^m b_j^n : m, n \in \mathbb{Z}_{\geq 0}\}$ then $S_{ij}^{-1}M$ and $S_{ij}^{-1}N$ will both be free $S_{ij}^{-1}A$-modules and we will have

$$\Big([S_{ij}^{-1}M : S_{ij}^{-1}N]_{S_{ij}^{-1}A}\Big)_{\mathfrak{p}} = [M_{\mathfrak{p}} : N_{\mathfrak{p}}]_{A_{\mathfrak{p}}},$$

for all primes $\mathfrak{p}$ of $A$ that do not contain either $a_i$ or $b_j$, since we can fix a global $S_{ij}^{-1}A$-module isomorphism $\phi\colon S_{ij}^{-1}M \to S_{ij}^{-1}N$ that induces $A_{\mathfrak{p}}$-module isomorphisms $\phi_{\mathfrak{p}}\colon M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ with $(\det \hat{\phi})_{\mathfrak{p}} = (\det \hat{\phi}_{\mathfrak{p}})$; note that if $\mathfrak{p}$ contains either $a_i$ or $b_j$ then $\mathfrak{p}S_{ij}^{-1}A$ is the unit ideal (not a prime ideal of $S_{ij}^{-1}A$), thus $[S_{ij}^{-1}M : S_{ij}^{-1}N]_{S_{ij}^{-1}A}$ is equal to the intersection $\cap_{\mathfrak{p}}[M_{\mathfrak{p}} : N_{\mathfrak{p}}]_{A_{\mathfrak{p}}}$ over primes $\mathfrak{p}$ that do not contain $a_i$ or $b_j$.

We now observe that since the sets $\{a_i\}$ and $\{b_j\}$ both generate the unit ideal, for every prime $\mathfrak{p}$ there is a choice of $a_i$ and $b_j$ that do not lie in $\mathfrak{p}$. It follows that

$$[M : N]_A = \bigcap_{\mathfrak{p}} [M_{\mathfrak{p}} : N_{\mathfrak{p}}]_{A_p} = \bigcap_{ij} [S_{ij}^{-1}M : S_{ij}^{-1}N]_{S_{ij}^{-1}A}.$$

Moreover, $[M : N]_A$ is a nonzero fractional ideal. To see this, let $I_{ij} \coloneqq [S_{ij}^{-1}M : S_{ij}^{-1}N]_{S_{ij}^{-1}A}$. Each $I_{ij}$ is a nonzero principal fractional $S_{ij}^{-1}A$-ideal, and we can choose a single $\alpha \in K^\times$ so that each $\alpha I_{ij}$ is an $S_{ij}^{-1}A$-ideal. The intersection of the $\alpha I_{ij}$ lies in $\cap_{ij} S_{ij}^{-1}A = A$ and is thus an $A$-submodule of $A$, hence an ideal, and finitely generated because $A$ is noetherian. It follows that $[M : N]_A$ is a fractional ideal of $A$, and it is nonzero, since it contains the product of the generators of the $I_{ij}$, for example. The localization of the intersection of a finite set of $A$-modules is equal to the intersection of their localizations, thus

$$([M : N]_A)_{\mathfrak{p}} = \Big(\cap_{ij} [S_{ij}^{-1}M : S_{ij}^{-1}N]_{S_{ij}^{-1}A}\Big)_{\mathfrak{p}} = \cap_{ij} \Big([S_{ij}^{-1}M : S_{ij}^{-1}N]_{S_{ij}^{-1}A}\Big)_{\mathfrak{p}} = [M_{\mathfrak{p}} : N_{\mathfrak{p}}]_{A_{\mathfrak{p}}}$$

as claimed. □

Proposition 6.2 implies that the module index $[M : N]_A$ is 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 6.3.** 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 $\pi$ 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-$\pi^{n-m}$ 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 6.4.** *Let $A$ be a Dedekind domain with fraction field $K$, and let $N \subseteq M$ be $A$-lattices in a $K$-vector space $V$ 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 nonzero ideals of $A$. Then*

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

*Proof.* Let $\mathfrak{p}$ be a prime of $A$, let $\pi$ 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 $U, V \in \mathrm{GL}_r(A_\mathfrak{p})$ and $D = \operatorname{diag}(\pi^{d_1}, \dots, \pi^{d_r})$ for some uniquely determined nonnegative integers $d_1 \le \cdots \le d_r$. We then have

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

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

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

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

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

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

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 6.7.** *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 $(\alpha)$ 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. 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

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

**Corollary 6.9.** *Assume AKLB and let $I$ be a fractional ideal of $B$. The ideal norm of $I$ is the fractional ideal of $A$ generated by the image of $I$ 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

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

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.

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

**Theorem 6.10.** *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 6.4. Thus $N_{B/A}(\mathfrak{q}) = [B : \mathfrak{q}]_A = \mathfrak{p} \cdots \mathfrak{p} = \mathfrak{p}^{f_\mathfrak{q}}$. $\square$

**Corollary 6.11.** *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

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

## 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.[1] 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 $\phi$ 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 $\phi$, 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 $e_Q$ 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 $\phi$, which is defined by

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

[1] 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.

where $f_Q$ counts the number of $\bar{k}$-points in the $\mathrm{Gal}(\bar{k}/k)$-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 5.35). It is a weighted measure of the cardinality of the fibers of $\phi$ 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 $\phi$).

## 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 6.10 implies

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

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

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

*Proof.* The ring $\mathcal{O}_L$ is a free $\mathbb{Z}$ module of rank $n := [L : \mathbb{Q}]$. It is free because it is torsion-free and $\mathbb{Z}$ is a PID, and it has rank $n$ because it contains a $\mathbb{Q}$-basis for $L$, by Proposition 5.17. The same is true of any nonzero fractional ideal of $\mathcal{O}_L$: it is a torsion-free $\mathbb{Z}$-module, hence free, and it has the same rank $n$ as $\mathcal{O}_L$ because it contains some nonzero principal fractional ideal $\alpha\mathcal{O}_L$: the fact that $\mathcal{O}_L$ spans $L$ implies that $\alpha\mathcal{O}_L$ spans $L$, because the multiplication-by-$\alpha$ map $L \overset{\times\alpha}{\to} L$ is an invertible $\mathbb{Q}$-linear transformation.

Let us now fix $\mathbb{Z}$-bases for $\mathcal{O}_L$ and the nonzero $\mathcal{O}_L$-ideal $\mathfrak{a}$. Let $\Phi \in \mathbb{Z}^{n\times n}$ be the matrix whose columns express each basis element for $\mathfrak{a}$ in terms of our basis for $\mathcal{O}_L$. Multiplication by $\Phi$ defines a $\mathbb{Z}$-module isomorphism from $\mathcal{O}_L$ to $\mathfrak{a}$, since it maps our basis for $\mathcal{O}_L$ to our basis for $\mathfrak{a}$. It follows that $[\mathcal{O}_L : \mathfrak{a}]_{\mathbb{Z}} = (\det \Phi)$: for every prime $p \in \mathbb{Z}$ we can use the

matrix $\Phi$ to define a $\mathbb{Z}_{(p)}$-module isomorphism $\phi_{(p)}\colon (\mathcal{O}_L)_{(p)} \to \mathfrak{a}_{(p)}$ with $\det \hat{\phi}_{(p)} = \det \Phi$ (any $\mathbb{Z}$-basis for a free $\mathbb{Z}$-module $M$ is also a $\mathbb{Z}_{(p)}$-basis for the free $\mathbb{Z}_{(p)}$-module $M_{(p)}$).

We now observe that the absolute value of the determinant of $\Phi$ is equal to the index of $\mathfrak{a}$ in $\mathcal{O}_L$: indeed, if we identify $\mathcal{O}_L$ with $\mathbb{Z}^n$ then $|\det \Phi|$ is the volume of a fundamental parallelepiped for $\mathfrak{a}$, viewed as a sublattice of $\mathbb{Z}^n$. We thus have

$$([\mathcal{O}_L : \mathfrak{a}]) = (\det \Phi) = [\mathcal{O}_L : \mathfrak{a}]_{\mathbb{Z}} = \mathrm{N}(\mathfrak{a}),$$

which proves the first 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 6.8, proving the second claim. □

**Remark 6.13.** Since $\mathbb{Z}$ is a principal ideal domain whose only units are $\pm 1$, 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 $\mathrm{N}(a) := \mathrm{N}((a)) = |\mathrm{N}_{L/\mathbb{Q}}(a)|$; this is a positive rational number, and for $a \in \mathcal{O}_L$, 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 5.17. 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* $\{\beta_1, \dots, \beta_n\}$ 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 $\{1, \alpha, \dots, \alpha^{n-1}\}$. 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 section we will address the general case.

**Theorem 6.14** (Dedekind-Kummer). *Assume AKLB with $L = K(\alpha)$ and $\alpha \in B$. Let $f \in A[x]$ be the minimal polynomial of $\alpha$, let $\mathfrak{p}$ be a prime of $A$, 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, let us give an example to illustrate its utility.

**Example 6.15.** 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

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

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

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

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, and we must then have $e_i \geq e_{\mathfrak{q}_i}$ and $\{\mathfrak{q}|\mathfrak{p}\} \subseteq \{\mathfrak{q}_i\}$ in order for $\prod_i \mathfrak{q}_i^{e_i}$ to be divisible by $\mathfrak{p}B$; we already showed that each $\mathfrak{q}_i$ is a prime above $\mathfrak{p}$, so we must have $\{\mathfrak{q}_i\} = \{\mathfrak{q}|\mathfrak{p}\}$. 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 6.14. 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 6.16.** 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 6.17.** 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 $\mathbb{Z}$; note that $(2, 1+\sqrt{-3}) = 2\mathbb{Z}[\zeta_3]$ is principal in $\mathbb{Z}[\zeta_3]$ but not in $\mathbb{Z}[\sqrt{-3}]$).

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

**Lemma 6.18.** *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 2.14. □

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 6.19.** 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.[2]

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 [5, 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 5.22), hence over every intermediate ring between $A$ and $B$, including all those whose integral

[2] Not all authors require an order to have nonzero conductor (e.g. Neukirch [6, §I.12]), but nearly all of the interesting theorems about orders require this assumption, so we include it in the definition.

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. Recall that an $A$-lattice in a $K$-vector space $L$ is a finitely generated $A$-submodule of $L$ that spans $L$ as a $K$-vector space.

**Definition 6.20.** 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.

**Remark 6.21.** In general the $K$-algebra $L$ (and the order $\mathcal{O}$) in Definition 6.20 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; see Theorem 13.17 and Corollary 13.20 in [7].

**Proposition 6.22.** *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. 10.28], 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 6.23.** 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 not finitely generated over $A$. But its integral closure is not $B$ (indeed, $\mathcal{O} \not\subseteq B$).

**Remark 6.24.** 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 5.28. 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 $\mathfrak{c} \subseteq \mathcal{O}$), and conversely. It follows that the map is $\operatorname{Spec} B \to \operatorname{Spec} \mathcal{O}$ 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 6.25.** *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 $\operatorname{Spec} B \to \operatorname{Spec} \mathcal{O}$ becomes a bijection.

**Lemma 6.26.** *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 $\mathcal{O}_\mathfrak{p} \subseteq B_\mathfrak{q}$, 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 6.27.** *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 6.28.** *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 3. □

**Remark 6.29.** 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 2.6 and Lemma 3.1. 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 6.30.** 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 6.31.** *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 6.27; 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 $\mathcal{O} = A[\alpha]$, where $L = K(\alpha)$ with $\alpha \in B$, as in the Dedekind-Kummer Theorem. Theorem 6.31 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 $\mathfrak{p}$ are all prime to $\mathfrak{c}$ and hence to the conductor, so the factorizations of $\mathfrak{p}B$ and $\mathfrak{p}\mathcal{O}$ will match up. In order to complete the picture, we now show that the residue field degrees of the primes in these factorizations also match.

**Proposition 6.32.** *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 $[B/\mathfrak{q} : A/\mathfrak{p}] = [\mathcal{O}/\mathfrak{q}' : A/\mathfrak{p}]$.*

*Proof.* We first note that $(\mathfrak{c}' \cap A)\mathcal{O} \subseteq \mathfrak{c}'$, so $\mathfrak{c} = (\mathfrak{c}' \cap A)B \subseteq \mathfrak{c}'B = \mathfrak{c}'$, thus $\mathfrak{c}$ is contained in the conductor of $\mathcal{O}$. That $\mathcal{O}$ is an $A$-lattice in $L$ follows from Proposition 6.22. Let $\mathfrak{q}$ be a prime of $B$ that does not contain $\mathfrak{c}$, and define $\mathfrak{q}' \coloneqq \mathfrak{q} \cap \mathcal{O}$ and $\mathfrak{p} \coloneqq \mathfrak{q} \cap A$. 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 6.26 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

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

The proof that $N_{B/A}(\mathfrak{q}) = \mathfrak{p}^{f_{\mathfrak{q}}}$ in Theorem 6.10 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 6.33.** *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 $B$.*

**Remark 6.34.** In the special case where $A = \mathbb{Z}$ and $L = \mathbb{Q}(\alpha)$ is a number field generated by an algebraic integer $\alpha$, for any prime number $p$, the ideal $p\mathcal{O}_L$ is prime to the conductor of $A[\alpha]$ if and only if $p$ does not divide the index $n$ of $A[\alpha]$ in $\mathcal{O}_L$, as we now explain. The conductor $\mathfrak{c}$ is an $\mathcal{O}_L$-ideal with absolute norm $[\mathcal{O}_L : \mathfrak{c}]$, and it is also an $A[\alpha]$-ideal, hence contained in $A[\alpha]$, so $[\mathcal{O}_L : \mathfrak{c}] = [\mathcal{O}_L : A[\alpha]][A[\alpha] : \mathfrak{c}]$ is divisible by $n = [\mathcal{O}_L : A[\alpha]]$. If $p|n$ then $p|[\mathcal{O}_L : \mathfrak{c}]$ and $p\mathcal{O}_L$ must have a prime of $\mathcal{O}_L$ above $p$ that divides $\mathfrak{c}$. Conversely if $p\mathcal{O}_L$ is not prime to $\mathfrak{c}$ then there is a prime $\mathfrak{q}$ of $\mathcal{O}_L$ above $p$ that divides $\mathfrak{c}$, and it follows that $p = [\mathcal{O}_L : \mathfrak{q}]$ divides $[\mathcal{O}_L : \mathfrak{c}]$, hence $p$ divides either $\mathcal{O}_L : A[\alpha]]$ or $[A[\alpha] : \mathfrak{c}]$. The latter cannot hold because it would imply that $\mathfrak{q}$ is an $A[\alpha]$-ideal, hence divisible by the conductor $\mathfrak{c}$ (and therefore equal to $\mathfrak{c}$), but then $[\mathcal{O}_L : \mathfrak{c}] = [\mathcal{O}_L : \mathfrak{q}]$ and $[\mathcal{O}_L : A[\alpha]] = 1$ which is impossible when $A[\alpha]$ has nontrivial conductor $\mathfrak{c} = \mathfrak{q}$.

**Remark 6.35.** For number fields $L = \mathbb{Q}[x]/(x^n + ax^m + b)$ with $m|n$, the article [4] gives a precise characterization of the primes $p$ dividing $[\mathcal{O}_L : A[\alpha]]$ (equivalently, dividing the conductor of $A[\alpha]$, as argued above), including necessary and sufficient criteria for $L$ to be monogenic.

**Remark 6.36.** In Lecture 12 we will define the *discriminant* of an $A$-order, and for orders of the form $A[\alpha]$ this is just the principal $A$-ideal generated by the discriminant of the minimal polynomial $f \in A[x]$ of $\alpha$. In Problem Set 6 you will prove that this discriminant is equal to the product of the norm of the conductor of $A[\alpha]$ and the discriminant of the $A$-order $B$. An immediate practical consequence is that the Dedekind-Kummer theorem always holds for primes $\mathfrak{p}$ of $A$ that do not contain the discriminant of $f$, equivalently, primes for which the reduction of $f$ modulo $\mathfrak{p}$ is separable, which is useful because it is an easy condition to check. But we should note that this sufficient condition is not necessary.

## References


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

[2] David Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Springer, 1995.

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

[4] Anuj Jakhar, Sudesh K. Khanduja, Neraj Sangwan, *On prime divisors of the index of an algebraic integer*, J. Number Theory **2016** (166), 47–61.

[5] Masayoshi Nagata, *Local rings*, John Wiley & Sons, 1962.

[6] Jürgen Neukirch, *Algebraic number theory*, Springer, 1999.

[7] Andrew V. Sutherland, *18.783 Elliptic curves, Lecture 13: Endomorphism algebras*, Spring 2019, MIT OpenCourseWare.

18.785 Number Theory I
Fall 2021