4 Étale algebras, norm and trace, Dedekind extensions

4.1 Separability

We recall some standard facts about separable and inseparable field extensions and define the more general notion of an *étale algebra* (or separable algebra). This is optional background material that may be skipped by those already familiar with it.

Definition 4.1. A nonzero polynomial f over a field K is *separable* if the zeros of f are distinct in every extension of K; equivalently, $\gcd(f, f') = 1$.[1]

Warning 4.2. Older texts (such as Bourbaki) define a polynomial in $K[x]$ to be separable if all of its irreducible factors are separable (under our definition); so $(x-1)^2$ is separable under this definition but not under ours. The older definition has the disadvantage that it is not preserved under field extension (for example, a polynomial that is inseparable as an element of $K[x]$ becomes separable when viewed as an element of $\overline{K}[x]$, since it splits into linear factors in $\overline{K}[x]$ and every linear polynomial is separable). This discrepancy does not impact the definition of separable element or field extensions.

Definition 4.3. Let L/K be an algebraic field extension. An element $\alpha \in L$ is *separable over* K if it is the root of a separable polynomial in $K[x]$ (in which case its minimal polynomial is separable). The extension L/K is *separable* if every $\alpha \in L$ is separable over K; otherwise it is *inseparable*.

Lemma 4.4. *Let K be a field. If $f \in K[x]$ is irreducible but not separable then $f' = 0$.*

Proof. Let $f \in K[x]$ be irreducible, and let L be its splitting field over K. If f is not separable then f and f' have a common root $\alpha \in L$. The minimal polynomial $g \in K[x]$ of α over K divides f, but f is irreducible and nonzero, so $\deg g = \deg f$. But g also must divide f', and $\deg f' < \deg f$, so $f' = 0$. □

Corollary 4.5. *Let p be the characteristic of the field K and let $f \in K[x]$ be irreducible. If $p = 0$ then f is separable, and if $p > 0$ then f is not separable if and only if it is of the form $f = g(x^p)$, where the polynomial $g \in K[x]$ is uniquely determined by f.*

Proof. Easy exercise. □

Corollary 4.6. *If* $\operatorname{char} K = 0$ *then every algebraic extension of K is separable.*

Corollary 4.7. *Let K be a field of characteristic $p \geq 0$. Every irreducible $f \in K[x]$ is of the form $g(x^{p^n})$ for some irreducible separable polynomial $g \in K[x]$ and integer $n \geq 0$ that are uniquely determined by f.*

Proof. We proceed by induction on $\deg f$. If f is separable the corollary holds with $g = f$ and $n = 0$. Otherwise $p > 0$ and $f = g(x^p)$ for some unique irreducible $g \in K[x]$ with $\deg g < \deg f$. By induction on $n = \deg f$, we have $g = h(x^{p^n})$ for some unique irreducible separable polynomial $h \in K[x]$ and integer $n \geq 0$ and then $f = h(x^{p^{n+1}})$. □

[1] Here f' denotes the formal derivative of f in $K[x]$ and the gcd is defined only up to a unit.

Lecture by Andrew Sutherland

Lemma 4.8. *Let $L = K(\alpha)$ be an algebraic extension contained in an algebraic closure $\overline{K}$ of K and let $f \in K[x]$ be the minimal polynomial of α over K. Then*

$$\#\operatorname{Hom}_K(L, \overline{K}) = \#\{\beta \in \overline{K} : f(\beta) = 0\} \leq [L : K],$$

with equality if and only if α is separable over K.

Proof. Each element of $\operatorname{Hom}_K(L, \overline{K})$ is uniquely determined by the image of α, which must be a root β of $f(x)$ in $\overline{K}$. The number of these roots is equal to $[L : K] = \deg f$ precisely when f and therefore α is separable over K. □

Definition 4.9. Let L/K be a finite extension. The *separable degree* of L/K is

$$[L : K]_s := \#\operatorname{Hom}_K(L, \overline{K}).$$

The *inseparable degree* of f is

$$[L : K]_i := [L : K]/[L : K]_s$$

We will shortly show that $[L : K]_i$ is always a positive integer (in fact a power of the characteristic of K), but it follows immediately from the definition that

$$[L : K] = [L : K]_s[L : K]_i.$$

Remark 4.10. As with the degree of a field extension (defined as the dimension of a vector space), one can define the separable degree of an arbitrary algebraic extension as the cardinality of the set $\operatorname{Hom}_K(L, \overline{K})$. Multiplication of degrees is then multiplication of cardinals (if S and T are sets the product of their cardinalities is the cardinality of the set $\operatorname{Hom}(S, T) = \{f : S \to T\}$).

Lemma 4.8 implies that for simple algebraic extensions $L = K(\alpha)$ we always have $[L : K]_s \leq [L : K]$, with equality if and only if α is separable (which we will shortly show is equivalent to L/K being separable).

Theorem 4.11. *Let $\phi_K : K \to \Omega$ be a homomorphism from a field K to an algebraically closed field Ω, and let L/K be algebraic. Then ϕ_K extends to a homomorphism $\phi_L : L \to \Omega$.*

Proof. We use Zorn's lemma. Define a partial ordering on the set $\mathcal{F}$ of pairs (F, ϕ_F) for which F/K is a subextension of L/K and $\phi_F : F \to \Omega$ extends ϕ_K by defining

$$(F_1, \phi_{F_1}) \leq (F_2, \phi_{F_2})$$

whenever F_2 contains F_1 and ϕ_{F_2} extends ϕ_{F_1}. Given any totally ordered subset $\mathcal{C}$ of $\mathcal{F}$, let $E = \bigcup\{F : (F, \phi_F) \in \mathcal{C}\}$ and define $\phi_E : E \to \Omega$ by $\phi_E(x) = \phi_F(x)$ for $x \in F \subseteq E$ (this does not depend on the choice of F because $\mathcal{C}$ is totally ordered). Then (E, ϕ_E) is a maximal element of $\mathcal{C}$, and by Zorn's lemma, $\mathcal{F}$ contains a maximal element (M, ϕ_M).

We claim that $M = L$. If not, then pick $\alpha \in L - M$ and consider the field $F = M[\alpha] \subseteq L$ properly containing M, and extend ϕ_M to $\varphi_F : F \to \Omega$ be letting $\phi_F(\alpha)$ by any root of $\alpha_M(f)$ in Ω, where $f \in M[x]$ is the minimal polynomial of α over M and $\alpha_M(f)$ is the image of f in $\Omega[x]$ obtained by applying φ_M to each coefficient. Then (M, ϕ_M) is strictly dominated by (F, ϕ_F), contradicting its maximality. □

Lemma 4.12. *Let $L/F/K$ be a tower of finite extensions. Then*

$$\#\operatorname{Hom}_K(L,\overline{K}) = \#\operatorname{Hom}_K(F,\overline{K})\#\operatorname{Hom}_F(L,\overline{K}).$$

Proof. We decompose $L/F/K$ into a tower of simple extensions and proceed by induction. The result is trival if $L=K$ and otherwise it suffices to consider $K\subseteq F\subseteq F(\alpha)=L$, where $K=F$ in the base case. Theorem 4.11 allows us to define a bijection

$$\operatorname{Hom}_K(F,\overline{K})\times\operatorname{Hom}_F(F(\alpha),\overline{K})\to\operatorname{Hom}_K(F(\alpha),\overline{K})$$

that sends (ϕ_1,ϕ_2) to $\phi\colon L\to\overline{K}$ defined by $\phi|_F=\phi_1$ and $\phi(\alpha)=(\hat{\phi}_1\hat{\phi}_2\hat{\phi}_1^{-1})(\alpha)$, where $\hat{\phi}_1,\hat{\phi}_2\in\operatorname{Aut}(\overline{K})$ denote arbitrary extensions of ϕ_1,ϕ_2 to $\overline{K}$; note that $\phi(\alpha)$ does not depend on these choices and is a root of $\phi(f)$, where $f\in F[x]$ is the minimal polynomial of α and $\phi(f)$ is its image in $\phi(F)[x]$. The inverse bijection is $\phi_1=\phi_F$ and $\phi_2(\alpha)=(\hat{\phi}_1^{-1}\hat{\phi}\hat{\phi}_1)(\alpha)$. □

Corollary 4.13. *Let $L/F/K$ be a tower of finite extensions. Then*

$$[L:K]_s=[L:F]_s[F:K]_s$$
$$[L:K]_i=[L:F]_i[F:K]_i$$

Proof. The first equality follows from the lemma and the second follows from the identities $[L:K]=[L:F][F:K]$ and $[L:K]=[L:K]_s[L:K]_i$. □

Corollary 4.14. *Let $L=K(\alpha)$ be an algebraic extension. Then L/K is separable if and only if α is separable over K, equivalently, if and only if $[L:K]_s=[L:K]$.*

Proof. If L/K is separable then α is separable over K and $[L:K]_s=[L:K]$, by Lemma 4.8.

Now suppose α is separable; then $[L:K]_s=[L:K]$, by Lemma 4.8. For any $\beta\in L$ we can write $L=K(\beta)(\alpha)$, and note that α is separable over $K(\beta)$, since its minimal polynomial over $K(\beta)$ divides it minimal polynomial over K, which is separable. So we also have $[L:K(\beta)]_s=[L:K(\beta)]$. The equalities

$$[L:K]=[L:K(\beta)][K(\beta):K]$$
$$[L:K]_s=[L:K(\beta)]_s[K(\beta):K]_s$$

then imply $[K(\beta):K]_s=[K(\beta):K]$, so β is separable over K, by Lemma 4.8. □

Corollary 4.15. *Let L/K be a finite extension. Then $[L:K]_s\le[L:K]$ with equality if and only if L/K is separable.*

Proof. We have alredy established this for simple extensions, and otherwise we my decompose L/K into a finite tower of simple extensions and proceed by induction on the number of extensions, using the previous two corollaries at each step. □

Corollary 4.16. *If $L/F/K$ is a tower of finite extensions with L/F and F/K separable then L/K is separable.*

Proof. This follows from Corollaries 4.13 and 4.15. □

Corollary 4.17. *If $L/F/K$ is a tower of algebraic extensions with L/F and F/K separable, then L/K is separable.*

Proof. Let $\beta \in L$. If $\beta \in F$ the β is separable over K, since F/K is separable. Otherwise, β is separable over F and we may consider the subextension M/K of F/K generated by the coefficients of the minimal polynomial $f \in F[x]$ of β over F. This is a finite separable extension of K, and $M(\beta)$ is also a finite separable extension of M, since the minimal polynomial of β over $M(\beta)$ is f, which is separable. By the previous corollary, $M(\beta)$, and therefore β, is separable over K. □

Corollary 4.18. *Let L/K be an algebraic extension, and let*

$$F = \{\alpha \in L : \alpha \textit{ is separable over } K\}.$$

Then F is a separable field extension of K.

Proof. This is clearly a field, since if α and β are both separable over K then $K(\alpha)$ and $K(\alpha, \beta)$ are separable extensions of K (by the previous corollary), thus every element of $K(\alpha, \beta)$, including $\alpha\beta$ and $\alpha + \beta$, is separable over K and lies in F. The field F is then separable by construction. □

The field F in the corollary is the *maximal separable extension* of K in L. When $L = \overline{K}$ it is called a *separable closure* of K and denoted K^{sep}. If K has characteristic zero then $K^{\text{sep}} = \overline{K}$ is algebraically closed. This also holds when K is a perfect field.

Definition 4.19. A field K is *perfect* if every algebraic extension of K is separable.

All fields of characteristic zero are perfect, as are all finite fields.

Theorem 4.20. *Every finite field is a perfect field.*

Proof. It suffices to consider a finite field of prime order $\mathbb{F}_p$, since every finite field is an algebraic extension of its prime field, and any algebraic extension of a perfect field is perfect. Let $f \in \mathbb{F}_p[x]$ be irreducible, and use Corollary 4.7 to write $f(x) = g(x^{p^n})$ with $g \in \mathbb{F}_p[x]$ irreducible and separable, and $n \geq 0$. If $n > 0$ then

$$f(x) = g(x^{p^n}) = g(x^{p^{n-1}})^p,$$

since $h(x^p) = h(x)^p$ for any $h \in \mathbb{F}_p[x]$, but this contradicts the irreducibility of f. So $n = 0$ and $f = g$ is separable. □

Definition 4.21. A field K is *separably closed* if K has no nontrivial finite separable extensions. Equivalently, K is equal to its separable closure in any algebraic closure.

Definition 4.22. An algebraic extension L/K is *purely inseparable* if $[L : K]_s = 1$.

Remark 4.23. The trivial extension K/K is both separable and purely inseparable.

Example 4.24. If $K = \mathbb{F}_p(t)$ and $L = \mathbb{F}_p(t^{1/p})$ then L/K is a purely inseparable extension of degree p.

Proposition 4.25. *Let K be a field of characteristic $p > 0$. If L/K is purely inseparable of degree p then $L = K(a^{1/p})$ for some $a \in K \backslash K^p$; equivalently, $L \simeq K[x]/(x^p - a)$.*

Proof. Every $\alpha \in L \backslash K$ is inseparable over K, and by Corollary 4.5 its minimal polynomial over K is of the form $f(x) = g(x^p)$ with f monic. We have $1 < \deg f \leq [L : K] = p$, so $g(x)$ must be a monic polynomial of degree 1, which we can write as $g(x) = x - a$. Then $f(x) = x^p - a$, and we must have $a \notin K^p$ since f is irreducible. We have $[L : K(\alpha)] = 1$, so $L = K(\alpha) \simeq K[x]/(x^p - a)$ as claimed. □

Theorem 4.26. *Let L/K be an algebraic extension and let F be the maximal separable extension of K in L. Then L/F is purely inseparable.*

Proof. If $L = F$ the theorem holds, so we assume otherwise and let $p > 0$ be the characteristic of K. Fix an algebraic closure $\overline{K}$ of K that contains L. Let α be an element of L that is not in F and let f be its minimal polynomial over F. Use Corollary 4.7 to write $f(x) = g(x^{p^n})$ with $g \in F[x]$ irreducible and separable, and $n \geq 0$. We must have $\deg g = 1$, since otherwise the roots of g would be separable over F and therefore over K but not in F. Thus $f(x) = x^{p^n} - c$ for some $c \in F$ (since f is monic and $\deg g = 1$). Since we are in characteristic $p > 0$, we can factor f in $F(\alpha)[x]$ as

$$f(x) = x^{p^n} - \alpha^{p^n} = (x - \alpha)^{p^n}.$$

There is thus only one F-homomorphism from $F(\alpha)$ to $\overline{K}$. The same statement applies to any extension of F obtained by adjoining any set of elements of L (even an infinite set). Therefore $\#\operatorname{Hom}_F(L, \overline{K}) = 1$, so $[L : F]_s = 1$ and L/F is purely inseparable. □

Corollary 4.27. *Every algebraic extension L/K can be decomposed into a tower of extensions $L/F/K$ with F/K separable and L/F purely inseparable.*

Corollary 4.28. *The inseparable degree of any finite extension is a power of the characteristic.*

Proof. This follows from the proof of the theorem above. □

4.2 Étale algebras

Definition 4.29. An *étale K-algebra* is a (necessarily commutative) K-algebra that is isomorphic to a finite product of separable extensions of K. A *finite étale K-algebra* is a K-algebra that is isomorphic to a finite product of finite separable extensions of K. By the *dimension* of an étale K-algebra we mean its dimension as a K-vector space.

Every separable field extension L/K is an étale K-algebra, and if an étale K-algebra L is a field, then it is necessarily isomorphic to a separable extension of K. An étale K-algebra L need not be a field, but every $\alpha \in L$ is separable (note that when L is not a field the minimal polynomial of α need not be irreducible, but it will be separable).

Example 4.30. If K is a separably closed field then every étale K-algebra of dimension n is isomorphic to $K^n = K \times \cdots \times K$.

Our main interest in étale algebras is that they naturally arise via *base change*, a notion we now recall (this is not the most general definition but suffices for our purposes).

Definition 4.31. Let $\varphi\colon A \to B$ be a ring homomorphism (so B is an A-module), and let M be an A-module. The tensor product of A-modules $M \otimes_A B$ is a B-module (with multiplication defined by $b(m \otimes b') := m \otimes bb'$) called the *base change* (or *extension of scalars*) of M from A to B. If M is an A-algebra then its base change to B is a B-algebra.

Remark 4.32. Each $\varphi\colon A \to B$ determines a functor from the category of A-modules to the category of B-modules via base change. It has an adjoint functor called *restriction of scalars* which, given a B-module M turns it into an A-module by the rule $am = \varphi(a)m$.

The ring homomorphism $\varphi\colon A \to B$ will often be an inclusion, in which case we have a ring extension B/A (we may also take this view in whenever φ is injective, which is necessarily the case if A is a field). We are specifically interested in the case where B/A is a field extension M is a finite étale A-algebra. We first recall the primitive element theorem.

Theorem 4.33. *Let L/K be a finite separable extension. Then $L = K(\alpha)$ for some $\alpha \in L$; equivalently $L \simeq K(x)/(f)$ for some monic, irreducible, separable $f \in K[x]$.*

Proof. See [1, §15.8] or [4, §V.7.4]. □

Proposition 4.34. *Suppose L is a finite étale K-algebra and K'/K is any field extension. Then $L \otimes_K K'$ is a finite étale K'-algebra of the same dimension as L.*

Proof. Without loss of generality we assume that L is actually a field; if not apply the following argument to each factor of L.

By the primitive element theorem, $L \simeq K[x]/(f)$ for some irreducible separable polynomial $f \in K[x]$. Suppose $f = f_1 f_2 \cdots f_m$ is the irreducible factorization of f in $K'[x]$. Each f_i is necessarily separable (no repeated roots over any extension), since f is. We have an isomorphism of K'-algebras $L \otimes_K K' \simeq K'[x]/(f)$, and by the Chinese Remainder Theorem, $K'[x]/(f) \simeq \prod_i K'[x]/(f_i)$. Each field $K'[x]/(f_i)$ is a finite separable extension of K', thus $L \otimes_K K'$ is a finite étale algebra over K'. We have $\dim L = \deg f = \dim K'[x]/(f)$, so the dimension is clearly preserved. □

Example 4.35. Any finite dimensional real vector space V is a finite étale $\mathbb{R}$-algebra (with coordinate-wise multiplication with respect to some basis); the complex vector space $V \otimes_{\mathbb{R}} \mathbb{C}$ is then a finite étale $\mathbb{C}$-algebra of the same dimension.

Note that even when an étale K-algebra L is a field, the base change $L \otimes_K K'$ will often not be a field. For example, if $K = \mathbb{Q}$ and $L \neq \mathbb{Q}$ is a number field, then the base $L \otimes_K \mathbb{C}$ will never be a field, it will be isomorphic to a $\mathbb{C}$-vector space of dimension $[L : K] > 1$.

We record the following corollary of Proposition 4.34, which is implied by its proof.

Corollary 4.36. *Let $L \simeq K[x]/(f)$ be a finite separable extension of a field K defined by an irreducible separable polynomial $f \in K[x]$. Let K'/K be any field extension, and let $f = f_1 \cdots f_m$ be the factorization of f into distinct irreducible polynomials $f_i \in K'[x]$. We have an isomorphism of étale K'-algebras*

$$L \otimes_K K' \simeq \prod_i K'[x]/(f_i)$$

where each $K'[x]/(f_i)$ is a finite separable field extension of K'.

Proposition 4.37. *Suppose L is a finite étale K-algebra and Ω is a separably closed field extension of K.Then*

$$L \otimes_K \Omega \quad \simeq \prod_{\sigma \in \operatorname{Hom}_K(L,\Omega)} \Omega.$$

In particular, the map $L \otimes_K \Omega \to \prod \Omega$ sends $y \otimes 1$ to $(\sigma(y))_\sigma$ for each $y \in L$.

Proof. Without loss of generality we may assume $L = K[x]/(f)$ is a simple field extension. Then f factors as $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ over Ω, with the α_i are distinct. We have a bijection between $\operatorname{Hom}_K(K[x]/(f), \Omega)$ and the set $\{\alpha_i\}$: each $\sigma \in \operatorname{Hom}_K(K[x]/(f), \Omega)$

is determined by $\sigma(x) \in \{\alpha\}$, and for each α_i, the map $x \mapsto \alpha_i$ determines a K-algebra homomorphism $\sigma_i \in \operatorname{Hom}_K(K[x]/(f), \Omega)$. As in the proof of Proposition 4.34 we have Ω-algebra homomorphisms

$$\frac{K[x]}{(f)} \otimes_K \Omega \simeq \frac{\Omega[x]}{(f)} \simeq \prod_{\alpha_i} \frac{\Omega[x]}{(x-\alpha_i)} \simeq \prod_{\sigma_i} \Omega_i.$$

given by the maps

$$x \otimes 1 \mapsto x \mapsto (\alpha_i)_i \mapsto (\sigma_i(x))_i.$$

The element $x \otimes 1$ generates $L \otimes_K \Omega$ as an Ω-algebra, and has image $(\sigma_i(x))_i$ in $\prod_{\sigma_i}$. It follows that $y \otimes 1 \mapsto (\sigma_i(y))_i$ for every $y \in L$. □

Remark 4.38. The proof of Proposition 4.37 does not actually require Ω to be separably closed, we only needed $f(x)$ to split into linear factors in $\Omega[x]$. Thus the proposition holds whenever all the irreducible polynomials $f \in K[x]$ for which the field $K[x]/(f)$ is a isomorphic to one of the finite separable field extensions of K whose product is L split completely in $\Omega[x]$ (for example, when L is a field, one could take Ω to be its normal closure).

Example 4.39. Let $L/K = \mathbb{Q}(i)/\mathbb{Q}$ and $\Omega = \mathbb{C}$. We have $\mathbb{Q}(i) \simeq \mathbb{Q}[x]/(x^2+1)$ and

$$\mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{C} \simeq \frac{\mathbb{Q}[x]}{x^2+1} \otimes_{\mathbb{Q}} \mathbb{C} \simeq \frac{\mathbb{C}[x]}{x^2+1} \simeq \frac{\mathbb{C}[x]}{x-i} \times \frac{\mathbb{C}[x]}{x+i} \simeq \mathbb{C} \times \mathbb{C}.$$

As $\mathbb{C}$-algebra isomorphisms, the corresponding maps are determined by

$$i \otimes 1 \mapsto x \otimes 1 \mapsto x \mapsto (x, x) \equiv (i, -i) \mapsto (i, -i).$$

Taking the base change of $\mathbb{Q}(i)$ to $\mathbb{C}$ lets us see the two distinct embeddings of $\mathbb{Q}(i)$ in $\mathbb{C}$, which are determined by the image of i. Note that $(i \otimes 1)^2 = i^2 \otimes 1^2 = -1 \otimes 1 = -(1 \otimes 1)$ and $(i, -i)^2 = (-1, -1) = -(1, 1)$, so we also have $1 \otimes 1 \mapsto (1, 1)$. Thus as an isomorphism of $\mathbb{C}$-vector spaces, the $\mathbb{C}$-basis $(1 \otimes 1, 1 \otimes i)$ for $\mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{C}$ is mapped to the $\mathbb{C}$-basis $\big((1,1),(i,-i)\big)$ for $\mathbb{C} \times \mathbb{C}$. It follows that for any $(\alpha, \beta) \in \mathbb{C} \times \mathbb{C}$, the inverse image of

$$(\alpha, \beta) = \frac{\alpha+\beta}{2}(1,1) + \frac{\alpha-\beta}{2i}(i,-i)$$

in $\mathbb{Q}(i) \otimes \mathbb{C}$ under this isomorphism is

$$\frac{\alpha+\beta}{2}(1 \otimes 1) + \frac{\alpha-\beta}{2i}(i \otimes 1) = 1 \otimes \frac{\alpha+\beta}{2} + i \otimes \frac{\alpha-\beta}{2i}.$$

Now $\mathbb{R}/\mathbb{Q}$ is an extension of rings, so we can also consider the base change of the $\mathbb{Q}$-algebra $\mathbb{Q}(i)$ to $\mathbb{R}$. But note that $\mathbb{R}$ is not separably closed and in particular, it does not contain a subfield isomorphic to $\mathbb{Q}(i)$, thus Proposition 4.37 does not apply. Indeed, as an $\mathbb{R}$-module, we have $\mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R}^2$, but as an $\mathbb{R}$-algebra, $\mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{C} \not\simeq \mathbb{R}^2$.

4.3 Norms and traces

We now introduce the norm and trace of a finite extension B/A. These are often defined only for field extensions, but in fact the same definition works without modification whenever B is a free A-module of finite rank. One can generalize further to projective modules (with some restrictions), but this is somewhat more involved and not needed here.

Definition 4.40. Let B/A be ring extensions in which B is a free A-module of finite rank. The (relative) *norm* $\mathrm{N}_{B/A}(b)$ and *trace* $\mathrm{T}_{B/A}(b)$ of b (down to A) are the determinant and trace of the A-linear multiplication-by-b map $B \to B$ defined by $x \mapsto bx$.

As a special case, note that if B/A is a finite extension of fields, then B is an A-vector space of finite dimension, hence a free A-module of finite rank. In practice one computes the norm and trace by picking a basis for B as an A-module and computing the matrix of the multiplication-by-b map with respect to this basis; this is an $n \times n$ matrix with entries in A whose determinant and trace do not depend on the choice of basis. It follows immediately from the definition that $\mathrm{N}_{B/A}$ is multiplicative and $\mathrm{T}_{B/A}$ is additive. Moreover, the norm map $\mathrm{N}_{B/A}$ defines a group homomorphism from $B^\times$ to $A^\times$ and the trace map $T_{B/A}$ defines a group homomorphism from B to A (as additive groups).

Example 4.41. Consider $A = \mathbb{R}$ and $B = \mathbb{C}$, which has the A-module basis $\{1, i\}$. For $b = 2 + 3i$ the matrix of $B \overset{\times b}{\to} B$ with respect to this basis can be written as $\left(\begin{smallmatrix} 2 & -3 \\ 3 & 2 \end{smallmatrix}\right)$, thus

$$\begin{aligned} \mathrm{N}_{\mathbb{C}/\mathbb{R}}(2+3i) &= \det \begin{pmatrix} 2 & -3 \\ 3 & 2 \end{pmatrix} = 13, \\ \mathrm{T}_{\mathbb{C}/\mathbb{R}}(2+3i) &= \operatorname{tr} \begin{pmatrix} 2 & -3 \\ 3 & 2 \end{pmatrix} = 4. \end{aligned}$$

Warning 4.42. Note that in order to write down the matrix of an A-linear transformation $B \to B$ with respect to basis for B as a free A-module of rank n, one not only needs to pick a basis, one needs to order this basis and decide whether to represent elements of $B \simeq A^n$ as row vectors with linear transformations acting via matrix multiplication on the right, or as column vectors with linear transformations acting via matrix multiplication on the left. The latter convention is often implicitly assumed in the literature (as in the example above), but the former is often used in computer algebra systems.

We now verify that the norm and trace are well behaved under base change.

Lemma 4.43. *Let B/A be ring extension with B free of rank n over A, and let $\varphi\colon A \to A'$ be a ring homomorphism. The base change $B' = B \otimes_A A'$ of B to A' is a free A'-module of rank n and we for every $b \in B$*

$$\varphi(\mathrm{N}_{B/A}(b)) = \mathrm{N}_{B'/A'}(b \otimes 1) \qquad \text{and} \qquad \varphi(\mathrm{T}_{B/A}(b) = \mathrm{T}_{B'/A'}(b \otimes 1).$$

Proof. Let $b \in B$, let $(b_1, \ldots, b_n)$ be a basis for B as an A-module, and let $M = (m_{ij}) \in A^{n \times n}$ be the matrix of $B \overset{\times b}{\to} B$ with respect to this basis. Then $(b_1 \otimes 1, \ldots, b_n \otimes 1)$ is a basis for B' as an A'-module (thus B' is free of rank n over A') and $M' = (\varphi(m_{ij})) \in A'^{n \times n}$ is the matrix of $B' \overset{\times b \otimes 1}{\to} B'$, and we have

$$\begin{aligned} \varphi(\mathrm{N}_{B/A}(b) &= \varphi(\det M) = \det(M')) = \mathrm{N}_{B'/A'}(b \otimes 1) \\ \varphi(\mathrm{T}_{B/A}(b) &= \varphi(\mathrm{T} M) = \varphi(\mathrm{T}(M')) = \mathrm{N}_{B'/A'}(b \otimes 1) \end{aligned}$$

□

Theorem 4.44. *Let K be a field with separable closure Ω and let L be a finite étale K-algebra. Then for all $\alpha \in L$ we have*

$$\mathrm{N}_{L/K}(\alpha) \;=\; \prod_{\sigma \in \mathrm{Hom}_K(L,\Omega)} \sigma(\alpha) \qquad \text{and} \qquad \mathrm{T}_{L/K}(\alpha) \;=\; \sum_{\sigma \in \mathrm{Hom}_K(L,\Omega)} \sigma(\alpha).$$

Proof. Let n be the rank of L as a K-module. By the previous lemma and Proposition 4.37.

$$\mathrm{N}_{L/K}(\alpha)=\mathrm{N}_{L\otimes_K\Omega/\Omega}(\alpha\otimes 1)=\mathrm{N}_{\Omega^n/\Omega}((\sigma_1(\alpha),\ldots,\sigma_n(\alpha))=\prod_{i=1}^n\sigma_i(\alpha).$$

The isomorphism $L\otimes_K\Omega\to\prod_\sigma\Omega=\Omega^n$ of Prop. 4.37 sends $\alpha\otimes 1$ to $(\sigma_1(\alpha),\ldots,\sigma_n(\alpha))$. Using the standard basis for Ω^n, the matrix of multiplication-by-$(\sigma_1(\alpha),\ldots,\sigma_n(\alpha))$ is just the diagonal matrix with $\sigma_i(\alpha)$ in the ith diagonal entry. Similarly,

$$\mathrm{T}_{L/K}(\alpha)=\mathrm{T}_{L\otimes_K\Omega/\Omega}(\alpha\otimes 1)=\mathrm{T}_{\Omega^n/\Omega}((\sigma_1(\alpha),\ldots,\sigma_n(\alpha))=\sum_{i=1}^n\sigma_i(\alpha).\qquad\square$$

The proof above demonstrates a useful trick: when working over a field that is not algebraically/separably closed, base change to an algebraic/separable closure. This often turns separable field extensions into étale algebras that are no longer fields.

Proposition 4.45. *Let L/K be a finite extension. Let $\alpha\in L^\times$, let $f\in K[x]$ be its minimal polynomial over K, let $\alpha_1,\ldots,\alpha_d$ be the roots of $f(x)$ in an algebraic closure of K that contains L, and let $e=[L:K(\alpha)]$. Then*

$$\mathrm{N}_{L/K}(\alpha)=\prod_{i=1}^d\alpha_i^e\qquad\textit{and}\qquad\mathrm{T}_{L/K}(\alpha)=e\sum_{i=1}^d\alpha_i,$$

In particular, if $f(x)=\sum_{i=0}^d a_ix^i$, then $\mathrm{N}_{L/K}(\alpha)=a_0^e$ and $\mathrm{T}_{L/K}(\alpha)=-ea_{d-1}$.

Proof. This follows immediately from Theorem 4.44 when L/K is separable, but to prove the general case, let M_α be the matrix of the multiplication-by-α map $T_\alpha\colon L\to L$. It follows from the Cayley-Hamilton theorem that T_α satisfies the characteristic polynomial $g\in K[x]$ of M_α, thus α is a root of g, which must be a multiple of f. If we pick a K-basis $u_1,\ldots,u_d$ for $K(\alpha)/K$ and a $K(\alpha)$-basis $v_1,\ldots,v_e$ for $L/K(\alpha)$, then $(u_iv_j)_{ij}$ is a K-basis for L/K, and if we order this basis appropriately, the matrix M_α is block diagonal with e copies of the $d\times d$ matrix of the restriction of T_α to $K(\alpha)$ along the diagonal and zeros elsewhere. The characteristic polynomial of the restriction of T_α to $K(\alpha)$ is necessarily $f(x)$, and the characteristic polynomial of T_α is then $g(x)=f(x)^e$. The proposition follows. $\square$

Corollary 4.46. *Let $M/L/K$ be a tower of finite extensions. Then*

$$\mathrm{N}_{M/K}=\mathrm{N}_{L/K}\circ\mathrm{N}_{M/L}\qquad\textit{and}\qquad\mathrm{T}_{M/K}=\mathrm{T}_{L/K}\circ\mathrm{T}_{M/L}.$$

Proof. Fix a separable closure Ω of K that contains M. As in the proof of Lemma 4.12, each $\sigma\in\mathrm{Hom}_K(M,\Omega)$ can be identified with a pair (σ_1,σ_2) with $\sigma_1\in\mathrm{Hom}_L(M,\Omega)$ and $\sigma_2\in\mathrm{Hom}_K(L,\Omega)$. We then note that for any $\alpha\in M^\times$,

$$\mathrm{N}_{M/K}(\alpha)=\prod_{\sigma\in\mathrm{Hom}_K(M,\Omega)}\sigma(\alpha)=\prod_{\sigma_2\in\mathrm{Hom}_K(L,\Omega)}\sigma_2\left(\prod_{\sigma_1\in\mathrm{Hom}_L(M,\Omega)}\sigma_1(\alpha)\right)=N_{L/K}(N_{M/L}(\alpha)),$$

and $\mathrm{T}_{M/K}(\alpha)=\mathrm{T}_{L/K}(\mathrm{T}_{M/L}(\alpha))$ follows similarly by replacing products with sums. $\square$

Corollary 4.46 actually holds in greater generality.

Theorem 4.47 (Transitivity of Norm and Trace). *Let $A \subseteq B \subseteq C$ be rings with C free of finite rank over B and B free of rank over A. Then C is free of finite rank over A and*

$$\mathrm{N}_{C/A} = \mathrm{N}_{B/A} \circ \mathrm{N}_{C/B} \qquad \text{and} \qquad \mathrm{T}_{C/A} = \mathrm{T}_{B/A} \circ \mathrm{T}_{C/B}.$$

Proof. See [3, §III.9.4]. □

4.4 Bilinear pairings and discriminants

Definition 4.48. Let V be a finite dimensional K-vector space. A *bilinear pairing* on V is a map $\langle\cdot,\cdot\rangle\colon V \times V \to K$ that satisfies

$$\begin{aligned} \langle u+v, w\rangle &= \langle u,w\rangle + \langle v,w\rangle, \\ \langle u, v+w\rangle &= \langle u,v\rangle + \langle u,w\rangle, \\ \langle \lambda u, v\rangle &= \langle u, \lambda v\rangle = \lambda\langle u,v\rangle. \end{aligned}$$

If $\langle v,w\rangle = \langle w,v\rangle$ then $\langle\cdot,\cdot\rangle$ is *symmetric*, and if $\langle v,w\rangle = -\langle w,v\rangle$ then $\langle\cdot,\cdot\rangle$ is *skew-symmetric*.

Definition 4.49. Let $\mathbf{e} := (e_1,\ldots,e_n)$ be a basis for a vector space V. The *discriminant* of a bilinear pairing $\langle\cdot,\cdot\rangle$ on V with respect to the basis $\mathbf{e}$ is

$$\operatorname{disc}(\langle\cdot,\cdot\rangle;\mathbf{e}) := \det\left((\langle e_i, e_j\rangle)_{ij}\right).$$

If $T\colon V \to V$ is an invertible linear transformation (change of basis) then

$$\operatorname{disc}(\langle\cdot,\cdot\rangle; T\mathbf{e}) = (\det T)^2 \operatorname{disc}(\langle\cdot,\cdot\rangle;\mathbf{e}),$$

thus $\operatorname{disc}(\langle\cdot,\cdot\rangle;\mathbf{e})$ depends on the choice $\mathbf{e}$. But note that whether $\operatorname{disc}(\langle\cdot,\cdot\rangle;\mathbf{e})$ is zero or not does not depend on $\mathbf{e}$.

Any bilinear pairing induces a map $V \to V^* := \operatorname{Hom}_K(V,K)$ that sends each $v \in V$ to the linear functional $w \mapsto \langle v,w\rangle$ in V^*; this map need not be an isomorphism, but we are particularly interested in the case where it is.

Definition 4.50. The *left kernel* of a bilinear pairing $\langle\cdot,\cdot\rangle$ is the vector space

$$\{v \in V\colon \langle v,w\rangle = 0,\ \forall w \in V\},$$

and the *right kernel* is similarly defined by $\{w \in V\colon \langle v,w\rangle = 0,\ \forall v \in V\}$. If $\langle\cdot,\cdot\rangle$ is symmetric then its left and right kernels coincide.

Proposition 4.51. *Let $\langle\cdot,\cdot\rangle$ be a bilinear pairing on a finite dimensional vector space V. The following are equivalent:*

1. *the map $V \to V^*$ induced by $\langle\cdot,\cdot\rangle$ is an isomorphism;*
2. *the left kernel of $\langle\cdot,\cdot\rangle$ is $\{0\}$;*
3. *the discriminant of $\langle\cdot,\cdot\rangle$ is nonzero.*

Proof. This is just linear algebra, the equivalences (1) ⇔ (2) ⇔ (3) are all immediate. □

Definition 4.52. A bilinear pairing with any of the three equivalent properties of Proposition 4.51 is said to be *nondegenerate* or *perfect*.

Remark 4.53. One can define bilinear pairings more generally for the case where K is a ring and V is a free K-module of finite rank. In this more general setting the three properties of Proposition 4.51 are not necessarily equivalent; one calls pairings that satisfy (1) perfect and those that satisfy (2) and (3) non-degenerate.

Recall from linear algebra that each basis (e_i) for V uniquely determines a dual basis (f_i) for V^* that satisfies

$$f_j(e_i) = \delta_{ij} := \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

Here δ_{ij} is the Kronecker delta function and the linear functional $f_j \colon V \to K$ is uniquely determined by its action on the basis (e_i) for V, which is given above.

If $\langle \cdot, \cdot \rangle$ is nondegenerate then applying the inverse of the isomorphism $V \to V^*$ it induces to the basis (f_i) uniquely determines a basis (e_i') for V that satisfies

$$\langle e_i', e_j \rangle = \delta_{ij},$$

since the inverse image e_i' of f_i under the induced map $V \to V^*$ satisfies $f_i(e_j) = \langle e_i', e_j \rangle$. We record this fact in the following proposition.

Proposition 4.54. *Let K be a field and let V a K-vector space of dimension n with a nondegenerate pairing $\langle \cdot, \cdot \rangle$. Associated to each basis $e_1, \ldots, e_n$ for V there is a unique basis $e_1', \ldots, e_n'$ for V such that $\langle e_i', e_j \rangle = \delta_{ij}$.*

4.5 Extensions of Dedekind domains

We now want to prove that the ring of integers of a number field is a Dedekind domain. We will use following setup: let A be a Dedekind domain with fraction field K, let L/K be a finite extension, and let B be the integral closure of A in L. To avoid trivialities, we will assume that A is not a field (this would mean $A = K$ and $L = B$), so A is a Dedekind domain of dimension one. Note that $B \cap K = A$, since A is integrally closed. We now show that $L = \operatorname{Frac} B$.

Proposition 4.55. *Let A be a Dedekind domain with fraction field K, let L/K be a finite extension, and let B be the integral closure of A in L. Every element of L can be written as $\frac{b}{a}$ with $a \in A$ and $b \in B$. In particular, the K-vector space $K \cdot B$ spanned by B is equal to L and L is the fraction field of B.*

Proof. Let $\alpha \in L$. The minimal polynomial of α over K is a monic irreducible polynomial in $K[x]$, and since $K = \operatorname{Frac} A$, we can multiply it by a nonzero element of A so that α is a root of the irreducible polynomial

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

with $a_n \neq 0$. We can make this polynomial monic by replacing x with x/a_n and multiplying by a_n^{n-1} to obtain

$$a_n^{n-1} f(x/a_n) = x^n + a_{n-1} x^{n-1} + a_n a_{n-2} x^{n-2} \cdots + a_n^{n-2} a_1 x + a_n^{n-1} a_0.$$

This is a monic polynomial with coefficients in A, so its roots, including $a_n \alpha$, all lie in B, the integral closure of A in L; thus $\alpha = b/a_n$ for some $b \in B$.

It follows that $K \cdot B = L$, and that L lies in the fraction field of B. We now note that since $B \subseteq L \subseteq \operatorname{Frac} B$ and L is a field, we must have $L = \operatorname{Frac} B$. □

Proposition 4.56. *Let A be a Dedekind domain with fraction field K, let L/K be a finite extension, and let B be the integral closure of A in L. Then $\mathrm{N}_{L/K}(b) \in A$ and $\mathrm{T}_{L/K}(b) \in A$ for all $b \in B$.*

Proof. The minimal polynomial $f = \sum_{i=0}^{d} a_i x^i \in K[x]$ of b has coefficients in A, by Proposition 2.1, and it then follows from Proposition 4.45 that $N_{L/K}(b) = a_0^e \in A$ and $T_{L/K}(b) = -ea_{d-1} \in A$ (where $e = [L : K(b)] \in \mathbb{Z}$). □

Definition 4.57. Let L/K be a finite extension of fields. The *trace pairing* is the map $L \times L \to K$ defined by

$$\langle x, y\rangle_{L/K} := \mathrm{T}_{L/K}(xy).$$

Proposition 4.58. *Let L/K be a finite extension of fields. The trace pairing $\langle\cdot,\cdot\rangle_{L/K}$ is a nondegenerate symmetric bilinear pairing.*

Proof. Bilinearity follows from the K-linearity of the trace map $\mathrm{T}_{L/K}$, and symmetry is immediate. Since L/K is separable, $\mathrm{T}_{L/K}$ is not the zero map (as proved on Problem Set 2) and we may pick $z \in L$ for which $\mathrm{T}_{L/K}(z) \neq 0$. Then for every $x \in L^\times$ we have $\langle x, z/x\rangle_{L/K} = \mathrm{T}_{L/K}(z) \neq 0$, which means that the left kernel of $\langle\cdot,\cdot\rangle_{L/K}$ is trivial, hence it is nondegenerate. □

We now assume that L/K is separable. For the next several lectures we will be working in the following setting: A is a Dedekind domain with fraction field K, the extension L/K is finite separable, and B is the integral closure of A in L (which we will shortly prove is also a Dedekind domain). As a convenient shorthand, we will write "assume $AKLB$" to indicate that we are using this setup.

Definition 4.59. Assume $AKLB$ and let $M \subseteq L$ be an A-module. The *dual A-module* is

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

Proposition 4.60. *Assume $AKLB$. Then B is a finitely generated A-module.*

Proof. By Proposition 4.55, B spans L as a K-vector space, so it contains a basis $(e_1, \ldots, e_n)$ for L as a K-vector space. Let $M \subseteq B$ be the A-span of $(e_1, \ldots, e_n)$. Then M is an A-submodule of L that lies in the A-submodule B of L. We have $B \subseteq B^*$, by Proposition 4.56 and the definition of B^*, and $M \subseteq B$ implies $B^* \subseteq M^*$. We thus have inclusions

$$M \subseteq B \subseteq B^* \subseteq M^*.$$

The A-module M is generated by $(e_1, \ldots, e_n)$, and its dual M^* is generated by the unique K-basis $(e_1', \ldots, e_n')$ for L satisfying $\langle e_i', e_j\rangle_{L/K} = \delta_{ij}$, by Proposition 4.54. Note that

$$\mathrm{T}_{L/K}(e_i' e_j) = \langle e_i', e_j\rangle_{L/K} = \delta_{ij} \in \{0, 1\} \subseteq A,$$

so the e_i' all lie in M^*. Since A is noetherian, and M^* is finitely generated, every A-submodule of M^* is finitely generated, including B (and B^*). □

Remark 4.61. The theorem above is not true when L/K is not required to be separable, not even when A is a PID; see [2, Ex. 11, p. 205]. We used the separability hypothesis when we invoked Proposition 4.54, which only applies to nondegenerate pairings.

Lemma 4.62. *Let $A \subseteq B$ be an arbitrary extension of domains with B integral over A, and let $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1$ be primes of B. Then $\mathfrak{q}_0 \cap A \subsetneq \mathfrak{q}_1 \cap A$ and $\dim A \geq \dim B$.*

Proof. We first replace B with $B/\mathfrak{q}_0$ and replace A, $\mathfrak{q}_0$, and $\mathfrak{q}_1$ with their images in $B/\mathfrak{q}_0$ (the new B is integral over the new A, since the image of a monic polynomial in $A[x]$ is a monic polynomial in $(A/(\mathfrak{q}_0 \cap A))[x]$). Then $\mathfrak{q}_0 = 0$ and $\mathfrak{q}_1$ is a nonzero prime ideal. Let $x \in \mathfrak{q}_1$ be nonzero. Its minimal polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ has coefficients in A and nonzero constant coefficient a_0 (otherwise divide by x). We have $a_0 = -a_1x - \cdots - x^n \in \mathfrak{q}_1$, thus $0 \neq a_0 \in \mathfrak{q}_1 \cap A$. So $\mathfrak{q}_1 \cap A$ is not the zero ideal and therefore properly contains $\mathfrak{q}_0 \cap A = \{0\}$. We can now apply this result to any chain of distinct prime ideals in B to get a chain of distinct prime ideals in A, thus $\dim A \geq \dim B$. □

Theorem 4.63. *Assume AKLB. Then B is a Dedekind domain.*

Proof. We note that:

- B is noetherian because it is finitely generated over A, which is noetherian;
- B is integrally closed in L, which is its fraction field;
- B has dimension at most 1, since $\dim B \leq \dim A \leq 1$.

Thus B is a Dedekind domain. □

Remark 4.64. Theorem 4.63 holds without the assumption that L/K is separable. This follows from the Krull-Akizuki Theorem, see [5, Thm. 11.7] or [4, §VII.2.5], which is used to prove that B is noetherian (even though it need not be finitely generated as an A-module).

Corollary 4.65. *The ring of integers of a number field is a Dedekind domain.*

References

[1] M. Artin, *Algebra*, 2nd edition, Pearson, 2010.

[2] Z.I. Borevich and I.R. Shafarevich, *Number theory*, Academic Press, 1966.

[3] N. Bourbaki, *Algebra I: Chapters 1–3*, Springer, 1989.

[4] N. Bourbaki, *Commutative Algebra: Chapters 1–7*, Springer, 1989.

[5] H. Matsumura, *Commutative ring theory*, Cambridge University Press, 1986.