4 Étale algebras, norm and trace

4.1 Separability

In this section we briefly review some standard facts about separable and inseparable field extensions that we will use repeatedly throughout the course. Those familiar with this material should feel free to skim it. In this section K denotes any field.

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, $\gcd(f, f')$ is a unit in $K[x]$ (i.e. of degree 0).[1] Otherwise f is *inseparable*.

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. This approach 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 nonzero linear polynomial is separable). This discrepancy does not change the definition of separable elements 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 necessarily separable). The extension L/K is *separable* if every $\alpha \in L$ is separable over K; otherwise it is *inseparable*.

Lemma 4.4. *An irreducible polynomial $f \in K[x]$ is inseparable if and only if $f' = 0$.*

Proof. Let $f \in K[x]$ be irreducible; then f is nonzero and not a unit, so $\deg f > 0$. If $f' = 0$ then $\gcd(f, f') = f \notin K^\times$ and f is inseparable. If f is inseparable then $g := \gcd(f, f')$ is a nontrivial divisor of f and f'. This implies $\deg g = \deg f$, since f is irreducible, but then $\deg f' < \deg f = \deg g$, so g cannot divide f' unless $f' = 0$. □

Corollary 4.5. *Let $f \in K[x]$ be irreducible and let $p \geq 0$ be the characteristic of K. We have $f(x) = g(x^{p^n})$ for some irreducible separable $g \in K[x]$ and integer $n \geq 0$ uniquely determined by f.*

Proof. If f is separable the theorem holds with $g = f$ and $n = 0$; for uniqueness, note that if $p = 0$ then $p^n \neq 0$ if and only if $n = 0$, and if $p > 0$ and $g(x^{p^n})$ is inseparable unless $n = 0$ because $g(x^{p^n})' = g'(x^{p^n})p^n x^{p^n - 1} = 0$ (by the previous lemma). Otherwise $f(x) := \sum f_r x^r$ is inseparable and $f'(x) = \sum r f_r x^{r-1} = 0$ (by the lemma), and this can occur only if $p > 0$ and $f_r = 0$ for all $r \geq 0$ not divisible by p. So $f = g(x^p)$ for some (necessarily irreducible) $g \in K[x]$. If g is separable we are done; otherwise we proceed by induction. As above, the uniqueness of g and n is guaranteed by the fact that $g(x^{p^n})' = 0$ for all $n > 0$. □

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

Lemma 4.7. *Let $L = K(\alpha)$ be an algebraic field 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.

[1] Here f' is the formal derivative of f in $K[x]$: if $f = \sum f_n x^n$ then $f' = n f_n x^{n-1}$.

Proof. Each element of $\mathrm{Hom}_K(L,\overline{K})$ 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 4.8. Let L/K be a finite extension of fields. The *separable degree* of L/K is

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

The *inseparable degree* of f is

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

We will see shortly that $[L:K]_s$ always divides $[L:K]$, so $[L:K]_i$ is an integer (in fact a power of $\mathrm{char}K$), but it follows immediately from our definition that

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

always holds.

Theorem 4.9. *Let L/K be an algebraic field extension. and let $\phi_K\colon K \to \Omega$ be a homomorphism to an algebraically closed field Ω. Then ϕ_K extends to a homomorphism $\phi_L\colon L \to \Omega$.*

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 $\phi_F\colon F \to \Omega$ extends ϕ_K by defining

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

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 be the field $\bigcup\{F : (F,\phi_F) \in \mathcal{C}\}$ and define $\phi_E\colon E \to \Omega$ 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 $\varphi_F\colon F \to \Omega$ be letting $\phi_F(\alpha)$ be 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 4.10. *Let $L/F/K$ be a tower of finite extensions of fields. Then*

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

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 4.9 allows us to define a bijection

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

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 $\hat{\phi}_1,\hat{\phi}_2 \in \mathrm{Aut}_K(\overline{K})$ are 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 4.11. *Let $L/F/K$ be a tower of finite extensions of fields. 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 $[L:K] = [L:K]_s[L:K]_i$. □

Theorem 4.12. *Let L/K be a finite extension of fields. The following are equivalent:*

(a) *L/K is separable;*

(b) *$[L:K]_s = [L:K]$;*

(c) *$L = K(\alpha)$ for some $\alpha \in L$ separable over K;*

(d) *$L \simeq K[x]/(f)$ for some monic irreducible separable polynomial $f \in K[x]$.*

Proof. The equivalence of (c) and (d) is immediate (let f be the minimal polynomial of α and let α be the image of x in $K[x]/(f)$), and the equivalence of (b) and (c) is given by Lemma 4.7. That (a) implies (c) is the PRIMITIVE ELEMENT THEOREM, see [1, §15.8] or [3, §V.7.4] for a proof. It remains only to show that (c) implies (a).

So let $L = K(\alpha)$ with α separable over K. For any $\beta \in L$ we can write $L = K(\beta)(\alpha)$, and we note that α is separable over $K(\beta)$, since its minimal polynomial over $K(\beta)$ divides it minimal polynomial over K, which is separable. Lemma 4.7 implies $[L:K]_s = [L:K]$ and $[L:K(\beta)]_s = [L:K(\beta)]$ (since $L = K(\alpha) = K(\beta)(\alpha)$), and 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 4.7). This applies to every $\beta \in L$, so L/K is separable and (a) holds. □

Corollary 4.13. *Let L/K be a finite extension of fields. Then $[L:K]_s \le [L:K]$ with equality if and only if L/K is separable.*

Proof. We have already 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 4.14. *Let $L/F/K$ is a tower of finite extensions of fields. Then L/K is separable if and only if both L/F and F/K separable.*

Proof. The forward implication is immediate and the reverse implication follows from Corollaries 4.11 and 4.13. □

Corollary 4.15. *Let $L/F/K$ be a tower of algebraic field extensions. Then L/K is separable if and only if both L/F and F/K are separable.*

Proof. As in the previous corollary the forward implication is immediate. To prove the reverse implication, we assume L/F and F/K are separable and show that every $\beta \in L$ is separable over K. If $\beta \in F$ we are done, and if not we at least know that β is separable over F. Let M/K be the subextension 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 4.16. *Let L/K be an algebraic field extension, and let*

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

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. □

Definition 4.17. Let L/K be an algebraic field extension. The field F in Corollary 4.16 is the *separable closure of K in L*. When L is an algebraic closure of K it is simply called a *separable closure* of K and denoted K^{sep}.

When K has characteristic zero the notions of separable closure and algebraic closure necessarily coincide. This holds more generally whenever K is a perfect field.

Definition 4.18. 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 4.19. *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 4.5 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 4.20. 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 of K.

Definition 4.21. An algebraic extension L/K is *purely inseparable* if $[L : K]_s = 1$.

Remark 4.22. The trivial extension K/K is both separable and purely inseparable (but this can happen only for trivial extensions).

Example 4.23. If $K = \mathbb{F}_p(t)$ and $L = K[x]/(x^p - t) = \mathbb{F}_p(t^{1/p})$, then L/K is a purely inseparable extension of degree p.

Proposition 4.24. *Let K be a field of characteristic $p > 0$. If L/K is purely inseparable of degree p then $L = K(a^{1/p}) \simeq K[x]/(x^p - a)$ for some $a \in K - K^p$.*

Proof. Every $\alpha \in L - K$ 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 (a difference of pth powers can be factored). We have $[L : K(\alpha)] = 1$, so $L = K(\alpha) \simeq K[x]/(x^p - a)$ as claimed. □

Theorem 4.25. *Let L/K be an algebraic extension and let F be the separable closure of K in L. Then L/F is purely inseparable.*

Proof. If L is separable then $L = F$ the theorem holds, so we assume otherwise, in which case the characteristic p of K must be nonzero. Fix an algebraic closure $\overline{K}$ of K that contains L. Let $\alpha \in L - F$ have minimal polynomial f over F. Use Corollary 4.5 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 lie in in the separable closure F of K in L. 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 4.26. *Every algebraic extension L/K can be uniquely decomposed into a tower of algebraic extensions $L/F/K$ with F/K separable and L/F purely inseparable.*

Proof. By Theorem 4.25, we can take F to be the separable closure K^s of K in L. This is the only possible choice because every separable extensions F/K lies in K^s and if $[K^s : F] \neq 1$ then $[L : F]_s \geq [K^s : F]_s = [K^s : F] > 1$ and then L/F is not not purely inseparable. □

Corollary 4.27. *The inseparable degree of any finite extension is a power of the characteristic.*

Proof. This follows from the proof of Theorem 4.25. □

4.2 Étale algebras

We now want to generalize the notion of a separable field extension to that of a separable algebra (over a field), also known as an *étale algebra*.

Definition 4.28. Let K be a field. 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. The dimension of an étale K-algebra is its dimension as a K-vector space. A homomorphism of étale K-algebras is simply a homomorphism of K-algebras.

Remark 4.29. One can define the notion of an étale A-algebra for any noetherian domain A; we will postpone this definition to a later lecture.

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. In general 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 finite étale K-algebra A is isomorphic to $K^n = K \times \cdots \times K$ for some positive integer n.

Étale algebras are a special case of *semisimple algebras*. Recall that a (not necessarily commutative) ring R is *simple* if it is nonzero and has no nonzero proper (two-sided) ideals, and *semisimple* if it is isomorphic to a nonempty finite product of simple rings $\prod R_i$. When R is a commutative ring, it is simple if and only if it is a field, and semisimple if and only if it is a finite product of fields. A *semisimple algebra* over a field is a finite product of simple algebras over the same field. If $A = \prod A_i$ is a finite product of simple algebras, then every nonzero ideal of A is a subproduct.

Proposition 4.31. *Let $A = \prod K_i$ be a K-algebra written that is a product of field extensions K_i/K. Every surjective homomorphism $\varphi\colon A \to B$ of K-algebras corresponds to the projection of A on to a subproduct of its factors.*

Proof. The ideal $\ker\varphi$ is a subproduct of $\prod K_i$, thus $A \simeq \ker\varphi \times \operatorname{im}\varphi$ and $B = \operatorname{im}\varphi$ is isomorphic to the complementary subproduct. □

Proposition 4.31 can be viewed as a generalization of the fact that every surjective homomorphism of fields is an isomorphism.

Corollary 4.32. *The decomposition of an étale algebra into field extensions is unique up to permutation and isomorphisms of factors.*

Proof. Let A be an étale K-algebra and suppose A is isomorphic (as a K-algebra) to two products of field extensions of K, say

$$\prod_{i=1}^{m} K_i \simeq A \simeq \prod_{j=1}^{n} L_j.$$

Composing with isomorphisms yields surjective K-algebra homomorphisms $\pi_i\colon \prod L_j \to K_i$ and $\pi_j\colon \prod K_i \to L_j$. Proposition 4.31 then implies that each K_i must be isomorphic to one of the L_j and each L_j must be isomorphic to one of the K_i (and $m = n$). □

Our main interest in étale algebras is that they naturally arise from (and are stable under) *base change*, a notion we now recall.

Definition 4.33. Let $\varphi\colon A \to B$ be a homomorphism of rings (so B is an A-module), and let M be any 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.

We have already seen one example of base change: if M is an A-module and $\mathfrak{p}$ is a prime ideal of A then $M_{\mathfrak{p}} = M \otimes_A A_{\mathfrak{p}}$ (as noted in Lecture 2, this another way to define the localization of a module).

Remark 4.34. 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* that converts a B-module M into an A-module by the rule $am = \varphi(a)m$ (if φ is inclusion this amounts to restricting the scalar multiplication by B to the subring A).

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 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 and M is a finite étale A-algebra.

Proposition 4.35. *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 L is a product of fields and we can apply the following argument to each of its factors.

By Theorem 4.12, $L \simeq K[x]/(f)$ 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 $K'[x]$. The f_i are separable and that no pair share a common factor (the ideals $(f_1), \ldots, (f_m)$ are pairwise coprime), since f is separable. 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 K'-algebra. We have $\dim_K L = \deg f = \dim_{K'} K'[x]/(f)$, so the dimension is preserved. □

Example 4.36. 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 $L \otimes_K \mathbb{C}$ will never be a field, it will be isomorphic to a $\mathbb{C}$-vector space of dimension $[L : K] > 1$.

Remark 4.37. In the proof of Proposition 4.35 we made essential use of the fact that the elements of an étale K-algebra are separable. Indeed, the proposition is false if we replace L with a commutative semisimple algebra that contains an inseparable element, as we now show. Without loss of generality, we can assume L is a purely inseparable extension of K (focus on one factor of L and base change to replace K by its maximal separable extension in L if necessary). Let α be an inseparable element of L. By Corollary 4.5, $f(x) = g(x^{p^n})$ for some irreducible separable $g \in K[x]$, where p is the characteristic of K, and g must have degree 1 since L/K is purely inseparable. Thus $f(x) = x^{p^n} - c$ for some $c \in K^\times$. Now consider the element

$$\gamma := \alpha \otimes 1 - 1 \otimes \alpha \in L \otimes_K L$$

We have $\gamma \neq 0$, since $\gamma \notin K$, but $\gamma^{p^n} = \alpha^{p^n} \otimes 1 - 1 \otimes \alpha^{p^n} = c \otimes 1 - 1 \otimes c = 0$ (since $c \in K$), so γ is a nonzero and nilpotent. This implies $L \otimes_K L$ is not a product of fields (separable or otherwise), hence not semisimple. This shows the category of commutative semisimple algebras is not stable under base change. In fact, one can define étale algebras as commutative semisimple algebras that remain semisimple after base change.

Corollary 4.38. *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 finite 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'.

Proof. This follows directly from the proof of Proposition 4.35. □

Proposition 4.39. *Suppose L is a finite étale K-algebra and Ω is a separably closed field extension of K. There is an isomorphism of finite étale Ω-algebras*

$$L \otimes_K \Omega \xrightarrow{\sim} \prod_{\sigma \in \mathrm{Hom}_K(L,\Omega)} \Omega$$

that sends $\beta \otimes 1$ to the vector $(\sigma(\beta))_\sigma$ for each $\beta \in L$.

Proof. We may reduce to the case that $L = K[x]/(f)$ is a separable field extension, and we may then factor $f(x) = (x-\alpha_1)\cdots(x-\alpha_n)$ over Ω, with the α_i are distinct. We have a bijection between $\mathrm{Hom}_K(K[x]/(f),\Omega)$ and the set $\{\alpha_i\}$: each $\sigma \in \mathrm{Hom}_K(K[x]/(f),\Omega)$ is determined by $\sigma(x) \in \{\alpha_i\}$, and for each α_i, the map $x \mapsto \alpha_i$ determines a K-algebra homomorphism $\sigma_i \in \mathrm{Hom}_K(K[x]/(f),\Omega)$. As in the proof of Proposition 4.35 we have Ω-algebra isomorphisms

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

which map

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

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 $\beta \otimes 1 \mapsto (\sigma_i(\beta))_i$ for every $\beta \in L$. □

Remark 4.40. The proof of Proposition 4.39 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 that is a factor of L split completely in $\Omega[x]$ (for example, when L is a field, one could take Ω to be its normal closure).

Example 4.41. 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 $\mathbb{Q}(i)$ is canonically embedded in its base change $\mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{C}$ to $\mathbb{C}$ via $\alpha \mapsto \alpha \otimes 1$. We have

$$-1 = i^2 = (i \otimes 1)^2 = i^2 \otimes 1^2 = -1 \otimes 1 = -(1 \otimes 1)$$

Thus as an isomorphism of $\mathbb{C}$-algebras, the basis $(1 \otimes 1, 1 \otimes i)$ for $\mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{C}$ is mapped to the basis $\big((1,1),(i,-i)\big)$ for $\mathbb{C} \times \mathbb{C}$. 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 4.39 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 we won't need this.

Definition 4.42. Let B/A be a (commutative) ring extension 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. We thus have group homomorphisms

$$\mathrm{N}_{B/A}\colon B^\times \to A^\times \qquad \text{and} \qquad T_{B/A}\colon B \to A.$$

Example 4.43. 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

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

Warning 4.44. 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, we not only need to pick a basis, we need to 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 (such as Magma).

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

Lemma 4.45. *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 $b \in B$*

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

Proof. Let $b \in B$, let $(b_1, \dots, b_n)$ 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 $(b_1 \otimes 1, \dots, b_n \otimes 1)$ 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

$$\varphi(\mathrm{N}_{B/A}(b)) = \varphi(\det M) = \det M' = \mathrm{N}_{B'/A'}(b \otimes 1)$$
$$\varphi(\mathrm{T}_{B/A}(b)) = \varphi(\mathrm{tr}\, M) = \mathrm{tr}\, M' = \mathrm{N}_{B'/A'}(b \otimes 1) \qquad \square$$

Theorem 4.46. *Let K be a field with separable closure Ω and let L be a finite étale K-algebra. 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 4.39.

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

The isomorphism $L \otimes_K \Omega \to \prod_\sigma \Omega = \Omega^n$ of Prop. 4.39 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 4.47. *Let L/K be a (not necessarily separable) extension of degree d, let $\overline{K}$ be an algebraic closure of K containing L, and let $\Sigma := \mathrm{Hom}_K(L, \overline{K})$. Let $\alpha \in L^\times$ have minimal polynomial $f \in K[x]$ with factorization $f(x) = \prod_i^d (x - \alpha_i)$ in $\overline{K}[x]$, and let $e = [L : K(\alpha)]$. Then*

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

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

Proof. See Problem Set 2. $\square$

Corollary 4.48. *Let $M/L/K$ be a tower of finite extensions. Then*

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

Proof. Fix a separable closure Ω of K that contains M. As in the proof of Lemma 4.10, 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 4.48 actually holds in much greater generality.

Theorem 4.49 (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 finite 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 [2, §III.9.4]. $\square$

References

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

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

[3] Nicolas Bourbaki, *Commutative Algebra: Chapters 1–7*, Springer, 1989.

[4] Anthony W. Knapp, *Advanced Algebra*, Digital Second Edition, 2016.

[5] Joseph J. Rotman, *Advanced Modern Algebra*, 2nd edition, Graduate Studies in Mathematics **114**, AMS, 2010.

18.785 Number Theory I
Fall 2016