4 Étale algebras

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, $\overline{K}$ is an algebraic closure that we will typically choose to contain any extensions L/K under consideration, and for any polynomial $f = \sum a_i x^i \in K[x]$ we use $f' := \sum i a_i x^{i-1}$ to denote the formal derivative of f (this definition also applies when K is an arbitrary ring).

Definition 4.1. A polynomial f in $K[x]$ is *separable* if $(f, f') = (1)$, that is, $\gcd(f, f')$ is a unit in $K[x]$. Otherwise f is *inseparable*.

If f is separable then it splits into distinct linear factors over $\overline{K}$, where it has $\deg f$ distinct roots; this is sometimes used as an alternative definition. Note that the property of separability is intrinsic to the polynomial f, it does not depend on the field we are working in; in particular, if L/K is any field extension the separability of a polynomial $f \in K[x] \subseteq L[x]$ does not depend on whether we view f as an element of $K[x]$ or $L[x]$.

Warning 4.2. Some older texts 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 older definition, but not under ours. 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 $n \geq 0$ that are 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*

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

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 4.8. Let L/K be a finite extension of fields. The *separable degree* of L/K is

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

The *inseparable degree* of L/K 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 the characteristic of K), but it follows immediately from our definition that

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

holds regardless.

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 $\phi_F \colon F \to \Omega$ 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 and $\overline{K}$ be an algebraic closure of K that contains L. Then*

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

Proof. The result is immediate when $F = K$ or $L = F$ (the RHS is 1 times the LHS), so we assume $K \subsetneq F \subsetneq L$ and decompose the extensions L/F and F/K into finite towers of non-trivial simple extensions

$$K = K_0 \subsetneq K_1 \subsetneq \cdots \subsetneq K_m = F = K_m \subsetneq K_{m+1} \subsetneq \cdots \subsetneq K_n = L,$$

where $K_i = K_{i-1}(\alpha_i)$ for $1 \le i \le n$. To prove the lemma it suffices to show that

$$\#\operatorname{Hom}_{K_0}(K_n, \overline{K}) = \prod_{i=1}^{n} \#\operatorname{Hom}_{K_{i-1}}(K_i, \overline{K})$$

for any tower of proper simple extensions $K_0 \subsetneq K_1 \subsetneq \cdots \subsetneq K_n$. We now consider the map

$$\begin{aligned}\Phi\colon \operatorname{Hom}_K(K_n, \overline{K}) &\to \overline{K}^n \\ \varphi &\mapsto (\varphi(\alpha_1), \cdots, \varphi(\alpha_n)).\end{aligned}$$

This map Φ is injective, since $\varphi\colon K_n = K_0(\alpha_1, \ldots, \alpha_n) \to \overline{K}$ is uniquely determined by the images $\varphi(\alpha_1), \ldots \varphi(\alpha_n)$, so it suffices to show that the image of Φ has cardinality $\prod_{i=1}^n h_i$, where $h_i := \#\operatorname{Hom}_{K_{i-1}}(K_i, \overline{K})$.

For any polynomial $f \in \overline{K}[x]$ let $r(f) := \{\beta \in \overline{K} : f(\beta) = 0\}$ be the set of its $\overline{K}$-roots. Each $\sigma \in \operatorname{Aut}_K(\overline{K})$ induces a bijection $r(f) \to r(\sigma(f))$ with $\#r(f) = \#r(\sigma(f))$.

Let f_i be the minimal polynomial of α_i over K_{i-1}. Lemma 4.7 implies $h_i = \#r(f_i)$, and for any $\varphi \in \operatorname{Hom}_K(K_n, \overline{K})$ we have $h_i = \#r(\varphi(f_i))$, since Theorem 4.9 allows us to extend φ to an element of $\operatorname{Hom}_K(\overline{K}, \overline{K}) = \operatorname{Aut}_K(\overline{K})$.

Let $\varphi_0\colon K \to \overline{K}$ be the inclusion map. For each $\varphi \in \operatorname{Hom}_K(K_n, \overline{K})$ we may define a compatible sequence of pairs (φ_i, β_i) with $\varphi_i \in \operatorname{Hom}_K(K_i, \overline{K})$ satisfying ${\varphi_i}_{|_{K_{i-1}}} = \varphi_{i-1}$ and $\beta_i \in r(\varphi_{i-1}(f_i))$ by putting $\varphi_i = \varphi_{|_{K_i}}$ and $\beta_i = \varphi(\alpha_i)$; note that $(\beta_1, \ldots, \beta_n)$ uniquely determine φ and the sequence of pairs (φ_i, β_i), so the set of such compatible sequences of pairs is in bijection with the image of Φ. We can construct such a compatible sequence by initially choosing $\beta_1 \in r(f_1)$ and letting $\varphi_1(\alpha_1) = \beta_1$ uniquely determine $\varphi_1 \in \operatorname{Hom}_K(K_1, \overline{K})$; there are exactly h_1 choices for the pair (φ_1, β_1). To extend this sequence we choose $\beta_2 \in r(\varphi_1(f_2))$ and let $\varphi_2(\alpha_2) = \beta_2$ and ${\varphi_2}_{|_{K_1}} = \varphi_1$ uniquely determine $\varphi_2 \in \operatorname{Hom}_K(K_2, \overline{K})$. There are exactly h_2 choices for the pair (φ_2, β_2). Continuing in this fashion, we find there are exactly $\prod_{i=1}^n h_i$ sequences of pairs (φ_i, β_i) corresponding to some $\varphi \in \operatorname{Hom}_K(K_n, \overline{K})$. The image of the map Φ thus has cardinality $\prod_{i=1}^n h_i$ as desired. □

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 [2, §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 its 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 $[L : K]_s \leq [L : K]$ with equality if and only if L/K is separable.*

Proof. We have already established this for simple extensions, and otherwise we may 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 $L/F/K$ be 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 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. Perfect fields of positive characteristic are characterized by the following property.

Theorem 4.19. *A field K of characteristic $p > 0$ is perfect if and only if $K = K^p$, that is, every element of K is a pth power, equivalently, the map $x \mapsto x^p$ is an automorphism.*

Proof. If $K \neq K^p$ then for any $\alpha \in K - K^p$ the polynomial $x^p - \alpha$ is irreducible and the extension $K[x]/(x^p - \alpha)$ is inseparable, implying that K is not perfect. Now suppose $K = K^p$ and let $f \in K[x]$ be irreducible. By Corollary 4.5, we have $f(x) = g(x^{p^n})$ for some separable $g \in K[x]$ and $n \geq 0$. If $n > 0$ then

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

where $\tilde{g}$ is the polynomial obtained from g by replacing each coefficient with its pth root (thus $\tilde{g}(x)^p = g(x^p)$, since we are in characteristic p). But this contradicts the irreducibility of f. So $n = 0$ and $f = g$ is separable. The fact that every irreducible polynomial in $K[x]$ is separable implies that every algebraic extension of K is separable, so K is perfect. □

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

Proof. If a field K has cardinality p^n then $\#K^\times = p^n - 1$, thus $\alpha = \alpha^{p^n} = (\alpha^{p^{n-1}})^p$ for all $\alpha \in K$ and every element of K is a pth power. □

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 of K.

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 (but not inseparable!); conversely, an extension that is separable and purely inseparable is trivial.

Example 4.24. 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 4.25. *Let K be a field of characteristic $p > 0$. If L/K is purely inseparable of degree p then $L = K(a^{1/p}) \simeq K[x]/(x^p - a)$ 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 4.26. *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/K is separable then $L = F$ and 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, and thus lie in the separable closure F of K in L, but $g \in F[x]$ is irreducible and cannot have any roots in F unless it has degree 1. Thus $f(x) = x^{p^n} - a$ for some $a \in F$ (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 uniquely decomposed into a tower of algebraic extensions $L/F/K$ with F/K separable and L/F purely inseparable.*

Proof. By Theorem 4.26, we can take F to be the separable closure of K in L, and this is the only possible choice, since we must have $[L : F]_s = 1$. □

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

Proof. This follows from the proof of Theorem 4.26. □

4.2 Étale algebras

We now want to generalize the notion of a separable field extension. By Theorem 4.12, every finite separable extension L/K can be explicitly represented as $L = K[x]/(f)$ for some separable irreducible $f \in K[x]$. If f is not irreducible then we no longer have a field, but we do have a ring $K[x]/(f)$ that is also a K-vector space, in which the ring multiplication is compatible with scalar multiplication. In other words, L is a (unital) commutative K-algebra whose elements are all separable over K. The notion of separability extends to elements of a K-algebra (even non-commutative ones): an element is separable over K if and only it is the root of some separable polynomial in $K[x]$ (in which case its minimal polynomial must be separable). Recall that the minimal polynomial of an element α of a K-algebra A is the monic generator of the kernel of the K-algebra homomorphism $K[x] \to A$ defined by $x \mapsto \alpha$; note that if A is not a field, minimal polynomials need not be irreducible.

It follows from the Chinese remainder theorem that if f is separable then the K-algebra $K[x]/(f)$ is isomorphic to a direct product of finite separable extensions of K. Indeed, if $f = f_1 \cdots f_n$ is the factorization of f into irreducibles in $K[x]$ then

$$\frac{K[x]}{(f)} = \frac{K[x]}{(f_1 \cdots f_n)} \simeq \frac{K[x]}{(f_1)} \times \cdots \times \frac{K[x]}{(f_n)},$$

where the isomorphism is both a ring isomorphism and a K-algebra isomorphism. The separability of f implies that the f_i are separable and the ideals (f_i) are pairwise coprime (this justifies our application of the Chinese remainder theorem). We thus obtain a K-algebra that is isomorphic to a finite product of separable field extensions $K[x]/(f_i)$ of K. Algebras of this form are called *étale algebras* (or *separable algebras*).

Definition 4.29. Let K be a field. An *étale K-algebra* is a K-algebra L that is isomorphic to a finite product of finite separable field 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 a homomorphism of K-algebras (which means a ring homomorphism that commutes with scalar multiplication).

Remark 4.30. One can define the notion of an étale A-algebra for any noetherian domain A (we will consider this in a later lecture).

Example 4.31. If K is a separably closed field then every étale K-algebra A is isomorphic to $K^n = K \times \cdots \times K$ for some positive integer n (and therefore an étale K-algebra).

Étale algebras are *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 R is *semisimple* if it is isomorphic to a nonempty finite product of simple rings $\prod R_i$.[1] A commutative ring is simple if and only if it is a field, and semisimple if and only if it is isomorphic to a finite product of fields; this applies in particular to commutative semisimple K-algebras. Every étale K-algebra is thus semisimple (but the converse does not hold).

The ideals of a semisimple commutative ring $R = \prod_{i=1}^n R_i$ are easy to describe; each corresponds to a subproduct. To see this, note that the projection maps $R \to R_i$ are surjective homomorphisms onto a simple ring, thus for any R-ideal I, its image in R_i is either the zero ideal or the whole ring (note that the image of an ideal under a surjective ring homomorphism is an ideal). In particular, for each index i, either every $(r_1, \ldots, r_n) \in I$ has $r_i = 0$ or some $(r_1, \ldots, r_n) \in I$ has $r_i = 1$; it follows that I is isomorphic to the product of the R_i for which I projects onto R_i.

Proposition 4.32. *Let $A = \prod K_i$ be a K-algebra 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 4.32 can be viewed as a generalization of the fact that every surjective homomorphism of fields is an isomorphism.

Corollary 4.33. *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 4.32 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 4.34. 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.

[1]There are many equivalent (and a few inequivalent) definitions, but this is the simplest.

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 $M_\mathfrak{p} = M \otimes_A A_\mathfrak{p}$ (this is another way to define the localization of a module).

Remark 4.35. 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 an étale A-algebra.

Proposition 4.36. *Suppose L is an étale K-algebra and K'/K is any field extension. Then $L \otimes_K K'$ is an 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 separable $f \in K[x]$, and if $f = f_1 f_2 \cdots f_m$ is the factorization of f in $K'[x]$, we have isomorphisms of K'-algebras

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

in which each factor $K'[x]/(f_i)$ is a finite separable extension of K' (as discussed above, this follows from the CRT because f is separable). Thus $L \otimes_K K'$ is an étale K'-algebra, and $\dim_K L = \deg f = \dim_{K'} K'[x]/(f)$, so the dimension is preserved. □

Example 4.37. Any finite dimensional real vector space V is an 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 an 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 4.38. In the proof of Proposition 4.36 we made essential use of the fact that the elements of an étale K-algebra are separable. Indeed, the proposition does not hold if L is a finite semisimple commutative K-algebra that contains an inseparable element.

Corollary 4.39. *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'.

Proof. This follows directly from the proof of Proposition 4.36. □

The following proposition gives several equivalent characterizations of étale algebras, including a converse to Corollary 4.39 (provided the field K is not too small). Recall that an element α of a ring is *nilpotent* if $\alpha^n = 0$ for some n, and a ring is *reduced* if it contains no nonzero nilpotents.

Theorem 4.40. *Let L be a commutative K-algebra of finite dimension and assume that the dimension of L is less than the cardinality of K. The following are equivalent:*

- (a) *L is an étale K-algebra.*
- (b) *Every element of L is separable over K.*
- (c) *$L \otimes_K K'$ is reduced for every extension K'/K.*
- (d) *$L \otimes_K K'$ is semisimple for every extension K'/K.*
- (e) *$L = K[x]/(f)$ for some separable $f \in K[x]$.*

The implications $(a) \Leftrightarrow (b) \Leftrightarrow (c) \Leftrightarrow (d) \Leftarrow (e)$ hold regardless of the dimension of L.

Proof. To show $(a) \Rightarrow (b)$, let $L = \prod_{i=1}^n K_i$ with each K_i/K separable, and consider $\alpha = (\alpha_1, \ldots, \alpha_n) \in L = \prod_{i=1}^n K_i$. Each $\alpha_i \in K_i$ is separable over K with separable minimal polynomial $f_i \in K[x]$, and α is a root of $f := \operatorname{lcm}\{f_1, \ldots, f_n\}$, which is separable (the LCM of a finite set of separable polynomials is separable), thus α is separable.

To show $(b) \Rightarrow (c)$, note that if $\alpha \in L$ is nonzero and separable over K it cannot be nilpotent (the minimal polynomial of a nonzero nilpotent is x^n for some $n > 1$ and is therefore not separable), and separability is preserved under base change.

The equivalence $(c) \Leftrightarrow (d)$ follows from Lemma 4.41 below.

To show $(d) \Rightarrow (a)$, we first note we can assume L is semisimple (take $K' = K$), and it suffices to treat the case where L is a field. By base-changing to the separable closure of K in L, we can further reduce to the case that L/K is a purely inseparable field extension. If $L = K$ we are done. Otherwise we may pick an inseparable $\alpha \in L$, and, as in the proof of Theorem 4.26, the minimal polynomial of α has the form $f(x) = x^{p^n} - a$ for some $a \in K$ and $n \geq 1$. Now consider

$$\gamma \coloneqq \alpha \otimes 1 - 1 \otimes \alpha \in L \otimes_K L$$

We have $\gamma \neq 0$, since $\gamma \notin K$, but $\gamma^{p^n} = \alpha^{p^n} \otimes 1 - 1 \otimes \alpha^{p^n} = a \otimes 1 - 1 \otimes a = 0$, so γ is a nonzero nilpotent and $L \otimes_K L$ is not reduced, contradicting $(c) \Leftrightarrow (d)$.

We have $(e) \Rightarrow (a)$ from Corollary 4.39. For the converse, suppose $L = \prod_{i=1}^n L_i$ with each L_i/K a finite separable extension of K. Pick a monic irreducible separable polynomial $f_1(x)$ so that $L_1 \simeq K[x]/(f_1(x))$, and then do the same for $i = 2, \ldots, n$ ensuring that each polynomial f_j we pick is not equal to f_i for any $i < j$. This can be achieved by replacing $f_j(x)$ with $f_j(x + a)$ for some $a \in K^\times$ if necessary. Here we use the fact that there are at least n distinct choices for a, under our assumption that the dimension of L is less than the cardinality of K (note that if $f(x)$ is irreducible then the polynomials $f(x+a)$ are irreducible and pairwise coprime as a ranges over K). The polynomials $f_1, \ldots f_n$ are then coprime and separable, so their product f is separable and $L = K[x]/(f)$, as desired. ☐

The following lemma is a standard exercise in commutative algebra that we include for the sake of completeness.

Lemma 4.41. *Let K be a field. A commutative K-algebra of finite dimension is semisimple if and only if it is reduced.*

Proof. If A is semisimple it is clearly reduced (otherwise we could project a nonzero nilpotent of A to a nonzero nilpotent in a field); we only need to prove the converse. Every ideal of a commutative K-algebra A is also a K-vector space; this implies that when $\dim_K A$ is finite A satisfies both the ascending and descending chain conditions and is therefore noetherian and artinian. This implies that A has finitely many maximal ideals $M_1, \ldots M_n$ and that the intersection of these ideals (the radical of A) is equal to the set of nilpotent elements of A (the nilradical of A); see Exercises 19.12 and 19.13 in [1], for example.

Taking the product of the projection maps $A \twoheadrightarrow A/M_i$ yields a surjective ring homomorphism $\varphi\colon A \twoheadrightarrow \bigoplus_{i=1}^n A/M_i$ from A to a product of fields. If A is reduced then $\ker\varphi = \cap M_i = \{0\}$ and φ is an isomorphism, implying that A is semisimple. □

Proposition 4.42. *Suppose L is an étale K-algebra and Ω is a separably closed field extension of K. There is an isomorphism of étale Ω-algebras*

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

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 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 4.36 we have Ω-algebra isomorphisms

$$\frac{K[x]}{(f)} \otimes_K \Omega \stackrel{\sim}{\to} \frac{\Omega[x]}{(f)} \stackrel{\sim}{\to} \prod_{i=1}^n \frac{\Omega[x]}{(x-\alpha_i)} \stackrel{\sim}{\to} \prod_{i=1}^n \Omega.$$

which map

$$x \otimes 1 \mapsto x \mapsto (\alpha_1, \ldots, \alpha_n) \mapsto (\sigma_1(x), \ldots, \sigma_n(x)).$$

The element $x \otimes 1$ generates $L \otimes_K \Omega$ as an Ω-algebra, and it follows that $\beta \otimes 1 \mapsto (\sigma(\beta))_\sigma$ for every $\beta \in L$. □

Remark 4.43. The proof of Proposition 4.42 does not require Ω to be separably closed. If $L \simeq K[x]/(f)$ as in Theorem 4.40 (with f not necessarily irreducible), we can take Ω to be any extension of K that contains the splitting field of f.

Example 4.44. 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 $(1 \otimes 1, i \otimes 1)$ 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 4.42 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, $\mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{C} \not\simeq \mathbb{R}^2$.

References

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

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

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

[4] Nicolas Bourbaki, *Algebra II: Chapters 4–7*, Springer, 1989.

[5] Uriya First, Zinovy Reichstein, Santiago Salazar, *On the number of generators of a separable algebra over a finite field*, arXiv:1709.06982, 2017.

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

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