MAT 535 Ring and Field Extensions

1 Introduction

These are notes on ring and field extensions supplementing the material from our textbook. Some of the notes are cut-and-pasted from previous courses I taught. Much of the notes are exercises working through the basic results about these notions.

2 Ring extensions

Many of the basic notions for field extensions apply equally well to ring extensions, i.e., to morphisms of commutative rings. The most basic ring extensions are products of copies of a ring, the template for étale ring extensions (which in case of field extensions are finite separable field extensions), and polynomial algebras, which together with étale ring extensions form the template for smooth ring extensions (for field extensions, these roughly correspond to separably generated field extensions). We begin with polynomial algebras.

Definition 2.1. For every commutative ring R, for every R-module M, the **tensor R-algebra** $T_R^\bullet(M)$ on M is the $\mathbb{Z}_{\geq 0}$-graded associative, unital R-algebra whose degree-d graded summand $T_R^d(M)$ equals $M^{\otimes_R d} = M \otimes_R \cdots \otimes_R M$ for every d in $\mathbb{Z}_{\geq 0}$, and such that, for all d and e in $\mathbb{Z}_{\geq 0}$, the R-bilinear product from $M^{\otimes_R d} \times M^{\otimes_R e}$ to $M^{\otimes_R (d+e)}$ sends each ordered pair of "pure tensors" (a, b), for $a = \vec{v}_1 \otimes \cdots \otimes \vec{v}_d$ and for $b = \vec{w}_1 \otimes \cdots \otimes \vec{w}_e$, to the concatenation $a \cdot b := \vec{v}_1 \otimes \cdots \otimes \vec{v}_d \otimes \vec{w}_1 \otimes \cdots \otimes \vec{w}_e$. The **symmetric R-algebra** $\mathsf{Sym}_R^\bullet(M)$ on M is the quotient R-algebra of $T_R^\bullet(M)$ by the **commutator ideal**, i.e., by the two-sided ideal generated by all elements $a \cdot b - b \cdot a$. In particular, for every set Σ, the **tensor R-algebra** on the set Σ, respectively the **polynomial R-algebra** on the set Σ, is the tensor R-algebra, resp. the symmetric R-algebra, on the free R-module associated to Σ.

Lemma 2.2. *For every commutative ring R and for every R-module M, the $\mathbb{Z}_{\geq 0}$-graded R-module $T_R^\bullet(M)$ together with the R-bilinear product above is a $\mathbb{Z}_{\geq 0}$-graded R-algebra. Also the two-sided commutator ideal is a homogeneous ideal. Thus $\mathsf{Sym}_R^\bullet(M)$ is also a quotient $\mathbb{Z}_{\geq 0}$-graded R-algebra.*

Proposition 2.3 (Universal property of the tensor algebra)**.** *For every commutative ring R, for every R-module M, for every associative, unital R-algebra A (such that $R \cdot 1$ is in the center of A), for every morphism u_1 of R-modules from M to A, there exists a unique R-algebra homomorphism u from $T_R^\bullet(M)$ to A whose restriction to $T_R^1(M) = M$ is u_1.*

Proof. This is proved in the note on adjoint functors. □

Corollary 2.4 (Tensor powers are functors)**.** *For every commutative ring R, for every morphism v of R-modules from an R-module M to an R-module N, there exists a unique morphism $T_R^\bullet(v)$ of associative, unital $\mathbb{Z}_{\geq 0}$-graded R-algebras from $T_R^\bullet(M)$ to $T_R^\bullet(N)$ whose restriction to $T_R^1(M) = M$ is the composition of v with the inclusion of the direct summand $N = T_R^1(N)$ into $T_R^\bullet(N)$. For every nonnegative integer d, the rule associating $T_R^d(M)$ to every R-module M and associating $T_R^d(v)$ to every R-module morphism v is a (non-additive) functor from $R-$**Mod** to itself.*

Corollary 2.5 (Natural action of the symmetric group)**.** *For every commutative ring R, for every nonnegative integer d, for every element σ of the symmetric group $\mathfrak{S}_d$, for every R-module M, there is a unique morphism of R-modules $T_{R,M}^\sigma$ from $T_R^d(M)$ to $T_R^d(M)$ such that for every ordered d-tuple $(m_1, \ldots, m_d)$ of elements of M, we have $T_{R,M}^\sigma(m_{\sigma(1)} \otimes \cdots \otimes m_{\sigma(d)})$ equals $m_1 \otimes \cdots \otimes m_d$. This is a natural transformation from T_R^d to itself. Also, T_R^{Id} is the identity natural transformation, and $T_R^\tau \circ T_R^\sigma$ equals $T_R^{\tau\circ\sigma}$ for all elements σ and τ of $\mathfrak{S}_d$.*

Lemma 2.6 (Compatibility with short exact sequences)**.** *For every commutative ring R, for every nonnegative integer d, for every short exact sequence of R-modules,*

$$0 \to M' \to M \to M'' \to 0,$$

there is an associated filtration by R-submodules $T_R^d(M) = F^0 \supseteq \cdots \supseteq F^d$ and a surjective R-module homomorphism to $F^\ell/F^{\ell+1}$ from the direct sum over all subsets $I \subseteq \{1, \ldots, d\}$ of cardinality ℓ of the tensor product $N_1 \otimes_R \cdots \otimes_R N_d$ where N_i equals M' if i is in I and M'' otherwise. If M'' is projective, this surjection is an isomorphism. This filtration is compatible with morphisms of short exact sequences of R-modules.

Exercise 2.7. When R equals $\mathbb{C}[t]/\langle t^2\rangle$, when M equals R, when M' equals $\langle t\rangle/\langle t^2\rangle$, and when M'' equals $\mathbb{C}[t]/\langle t\rangle$, for $d = 2$, prove that the natural map from the nonzero R-module $M' \otimes_R M'$ to F^2 is not an isomorphism (rather it is the zero map).

Lemma 2.8 (Ranks of tensor powers)**.** *For every free R-module M, for every nonnegative integer d, also $T_R^d(M)$ is a free R-module. If M has finite rank n, also $T_R^d(M)$ has finite rank n^d.*

Proposition 2.9 (Universal property of the symmetric algebra)**.** *For every commutative ring R, for every R-module M, for every commutative R-algebra S, for every morphism u_1 of R-modules from M to A, there exists a unique R-algebra homomorphism u from $\mathsf{Sym}_R^\bullet(M)$ to S whose restriction to $\mathsf{Sym}_R^1(M) = M$ is u_1.*

Proof. This is also proved in the note on adjoint functors. □

Corollary 2.10 (Symmetric powers are functors)**.** *For every commutative ring R, for every morphism v of R-modules from an R-module M to an R-module N, there exists a unique morphism $\mathsf{Sym}^\bullet_R(v)$ of associative, unital $\mathbb{Z}_{\geq 0}$-graded R-algebras from $\mathsf{Sym}^\bullet_R(M)$ to $\mathsf{Sym}^\bullet_R(N)$ whose restriction to $\mathsf{Sym}^1_R(M) = M$ is the composition of v with the inclusion of the direct summand $N = \mathsf{Sym}^1_R(N)$ into $\mathsf{Sym}^\bullet_R(N)$. For every nonnegative integer d, the rule associating $\mathsf{Sym}^d_R(M)$ to every R-module M and associating $\mathsf{Sym}^d_R(v)$ to every R-module morphism v is a (non-additive) functor from $R-\mathbf{Mod}$ to itself. The natural quotient maps define a natural transformation from the functor T^d_R to the functor Sym^d_R.*

Corollary 2.11 (Symmetric powers are quotients for the symmetric group action)**.** *For every commutative ring R, for every integer d, for every element σ of the symmetric group $\mathfrak{S}_d$, for every R-module M, for the surjective R-module homomorphism $q^d_{R,M}$ from $T^d_R(M)$ to $\mathsf{Sym}^d_R(M)$, the composition $q^d_{R,M} \circ T^\sigma_{R,M}$ equals $q^d_{R,M}$. For every R-module homomorphism q' from $T^d_R(M)$ to an R-module N such that $q' \circ T^\sigma_{R,M}$ for every elements σ of $\mathfrak{S}_d$, there exists a unique R-module homomorphism $\widetilde{q'}$ from $\mathsf{Sym}^d_R(M)$ to N such that q' equals $\widetilde{q'} \circ q^d_{R,M}$. The morphisms $q^d_{R,M}$ form a natural transformation q^d_R from T^d_R to Sym^d_R.*

Lemma 2.12 (Compatibility with short exact sequences)**.** *For every commutative ring R, for every nonnegative integer d, for every short exact sequence of R-modules,*

$$0 \to M' \to M \to M'' \to 0,$$

there is an associated filtration by R-submodules $\mathsf{Sym}^d_R(M) = F^0 \supseteq \cdots \supseteq F^d$ and a surjective R-module homomorphism to $F^\ell/F^{\ell+1}$ from the tensor product $Sym^{d-\ell}_R(M'') \otimes_R Sym^\ell_R(M')$. If M'' is projective, this surjection is an isomorphism. This filtration is compatible with morphisms of short exact sequences of R-modules.

Exercise 2.13. When R equals $\mathbb{C}[t]/\langle t^2\rangle$, when M equals R, when M' equals $\langle t\rangle/\langle t^2\rangle$, and when M'' equals $\mathbb{C}[t]/\langle t\rangle$, for $d = 2$, prove that the natural map from the nonzero R-module $\mathsf{Sym}^r_R(M') = M' \otimes_R M'$ to F^2 is not an isomorphism (rather it is the zero map).

Corollary 2.14 (Ranks of symmetric powers)**.** *For every commutative ring R, for every free R-module M, for every nonnegative integer d, also $\mathsf{Sym}^d_R(M)$ is a free R-module. If M has finite rank n, also $\mathsf{Sym}^d_R(M)$ has finite rank $\binom{n+d-1}{d}$.*

Corollary 2.15 (Polynomial algebra on a set of variables)**.** *For every commutative ring R, for every commutative R-algebra S, for every function f from a set Σ to S, there exists a unique R-algebra homomorphism $\widetilde{f_R}$ from $\mathsf{Sym}^\bullet_R(Free_R(\Sigma))$ to S whose restriction to $\mathsf{Sym}^1_R(Free_R(\Sigma)) = Free_R(\Sigma)$ is the unique morphism of R-modules to S induced by f.*

Proof. This follows from the proposition by using the universal property of $\mathrm{Free}_R(\Sigma)$ to reformulate u_1 as a function f from Σ to S. □

Definition 2.16. For every morphism of commutative rings, $u : R \to S$, for every function f from a set Σ to S, the set $f(\Sigma)$ **generates** S as an R-algebra if (and only if) the induced R-algebra homomorphism $\mathsf{Sym}^1_R(\mathrm{Free}_R(\Sigma)) \to S$ is surjective. In particular, S is **finitely generated** as an R-algebra if (and only if) there exists a function from a finite set Σ that generates S as an R-algebra. Similarly, S is **finitely presented** as an R-algebra if (and only if) there exists a function from a finite set Σ that generates S as an R-algebra and such that the kernel of the surjection from $\mathsf{Sym}^\bullet_R(\mathrm{Free}_R(\Sigma))$ to S is also a finitely generated ideal. As a special case, u is a **primitive extension** if S is generated by a single element, i.e., S is isomorphic to a quotient R-algebra of the polynomial R-algebra.

Lemma 2.17 (Composition stability for finite generatedness / presentedness)**.** *For every morphism of commutative rings, $u : R \to S$, for every function $f : \Sigma \to S$ that generates S as an R-algebra, for every morphism of commutative rings $v : S \to T$, and for every function $g : \Theta \to T$ that generates T as an S-algebra, also the function $h := g \sqcup (v \circ f)$ from $\Theta \sqcup \Sigma$ to T generates as an R-algebra. The kernel of $\widetilde{h}_R$ is generated by the images of the kernels of $\widetilde{f}_R$ and $\widetilde{g}_S$. Thus, if both the kernels of $\widetilde{f}_R$ and $\widetilde{g}_S$ are finitely generated, then also the kernel of $\widetilde{h}_R$ is finitely generated.*

Proof. Denote the kernel of $\widetilde{f}_R$ by I, and denote the kernel of $\widetilde{g}_S$ by J. Then S is isomorphic to $R[\Sigma]/I$ as an R-algebra, and T is isomorphic to $S[\Theta]/J$ as an S-algebra. Thus, as an R-algebra, T is isomorphic to $((R[\Sigma]/I)[\Theta])/J$, which equals $((R[\Sigma]/I) \otimes_R R[\Theta])/J$, which in turn equals $(R[\Sigma] \otimes_R R[\Theta])/(J \oplus (I \otimes_R R[\Theta]))$, i.e., $R[\Sigma \sqcup \Theta]/(J \oplus (I \otimes_R R[\Theta]))$. □

Definition 2.18. For every associative, unital ring A, for every right A-module M, this is **flat**, respectively **faithfully flat**, if (and only if) the functor $M \otimes_A (-)$ from $A - \mathbf{Mod}$ to $\mathbb{Z} - \mathbf{Mod}$ is exact, resp. faithful and exact (and there is an analogous definition for left A-modules). For every morphism of commutative rings, $u : R \to S$, the morphism is **flat**, respectively **faithfully flat** if (and only if) the morphism u makes S into an R-module that is flat, resp. faithfully flat. A flat morphism of commutative rings, $u : R \to S$, is **finite faithfully flat** if (and only if) the R-module S is a finitely generated, faithfully flat R-module.

Lemma 2.19 (Flatness, projectivity, and freeness over local rings)**.** *For every commutative ring R, every free R-module is projective, and every projective R-module is flat. For every commutative ring R that is local with unique maximal ideal $\mathfrak{m}$, for every finitely presented R-module P, the R-module P is free if and only if it is projective if and only if it is flat if and only if $\mathsf{Tor}^R_1(R/\mathfrak{m}, P)$ is a zero module.*

Proof. Every free R-module is projective since it is a direct summand of itself (with complement a zero submodule). As a direct summand of a free module, every projective R-module is flat.

Now assume that R is a local ring. If P is flat, then $\mathsf{Tor}_1^R(R/\mathfrak{m}, P)$ is a zero module. For every finitely generated R-module P, lifting the elements of a finite $R/\mathfrak{m}$-vector space basis of $P/\mathfrak{m}P$ to elements in P defines a surjection, $T : R^{\oplus n} \twoheadrightarrow P$, such that the induced homomorphism $(R/\mathfrak{m})^{\oplus n} \to P/\mathfrak{m}P$ is an isomorphism. If also $\mathrm{Tor}_1^R(R/\mathfrak{m}, P)$ is a zero module, then we have a short exact sequence of $R/\mathfrak{m}$-vector spaces,

$$0 \to (R/\mathfrak{m}) \otimes_R \mathsf{Ker}(T) \to (R/\mathfrak{m})^{\oplus n} \xrightarrow{\overline{T}} P \to 0$$

Since $\overline{T}$ is an isomorphism, also $(R/\mathfrak{m}) \otimes_R \mathrm{Ker}(T)$ is a zero module. If P is finitely presented, then $\mathrm{Ker}(T)$ is finitely generated. Then by Nakayama's Lemma, the R-module $\mathrm{Ker}(T)$ is a zero module, i.e., T is an isomorphism. Thus P is a free R-module. □

Proposition 2.20 (Flat and finitely presented is projective)**.** *For every commutative ring R, for every finitely presented R-module P, the module is projective if and only if it is flat if and only if $\mathsf{Tor}_1^R(\mathit{Frac}(R/\mathfrak{p}), P)$ is a zero module for every prime ideal $\mathfrak{p}$ in R.*

Proof. Let P be a finitely presented R-module such that $\mathsf{Tor}_1^R(\mathrm{Frac}(R/\mathfrak{p}), P)$ is a zero module for every prime ideal $\mathfrak{p}$. For every maximal ideal $\mathfrak{m}$, by the argument above, there exists an R-module homomorphism $q : R^{\oplus n} \to P$ such that the induced homomorphism $R_{\mathfrak{p}}^{\oplus n} \to M_{\mathfrak{p}}$ is an isomorphism. Then the cokernel of q and the kernel of q are finitely generated R-modules that are annihilated by $\mathfrak{m}$. By Nakayama's Lemma, there exists an element $r \in R \setminus \mathfrak{m}$ such that the kernel and cokernel of R are annihilated by r.

In particular, for every R-module N, the R-module $\mathsf{Ext}_R^1(P, N)$ is annihilated by r. Since this holds for every maximal ideal, the ideal generated by the elements r as above equals all of R (by the Axiom of Choice). Thus, there exist finitely many elements $(r_1, \ldots, r_m)$ of R that annihilate $\mathsf{Ext}_R^1(P, N)$ such that $1 = r_1 + \cdots + r_m$. Thus 1 annihilates $\mathrm{Ext}_R^1(P, N)$, i.e., this is a zero module. Since this holds for every R-module N, the R-module P is projective. □

Lemma 2.21 (Flat modules with nonzero residual modules are faithfully flat)**.** *For every commutative ring R, for every flat R-module P, the R-module is faithfully flat if and only if $P \otimes_R R/\mathfrak{m}$ is nonzero for every maximal ideal $\mathfrak{m}$ of R.*

Proof. Since P is already flat, the module is faithfully flat if and only if $P \otimes_R M$ is nonzero for every nonzero R-module M. Every R-module is an increasing union of its finitely generated R-submodules. Thus, it suffices to prove $P \otimes_R M$ is nonzero for nonzero finitely generated R-modules M. Every such R-module has a filtration where the associated graded pieces are each of the form R/I for some proper ideal I of R (that depends on the module and the term in the filtration). Thus, $P \otimes_R M$ has a filtration where each associated graded piece is $P \otimes_R (R/I)$. By the Axiom of Choice, for every proper ideal I in R, there exists a maximal ideal $\mathfrak{m}$ of R containing I. Thus, there is a surjection from R/I to $R/\mathfrak{m}$. So there is a surjection from $P \otimes_R (R/I)$ to $P \otimes_R (R/\mathfrak{m})$. Thus $P \otimes_R (R/I)$ is nonzero if $P \otimes_R (R/\mathfrak{m})$ is nonzero. □

Definition 2.22. For every morphism of commutative rings, $u : R \to S$, for every element s of S, the element s is **integral** for u, or integral over R (when u is understood), if (and only if) the R-subalgebra of S generated by s is a finitely generated R-module. A morphism u of commutative rings is **integral** if (and only if) every element of S is integral over R. A morphism u of commutative rings is **finite** if (and only if) S is finitely generated as an R-module. A finite morphism u of commutative rings is **Artinian** if (and only if) S is an Artinian R-module, i.e., S has a (finite) composition series whose associated graded modules are simple R-modules.

Lemma 2.23 (Criteria for integrality)**.** *For every morphism of commutative rings, $u : R \to S$, for every element s of S, the element s is integral for u if and only if there exists an R-subalgebra S' of S containing s that is finitely generated as an R-module if and only if s satisfies a monic polynomial with coefficients in R.*

Proof. If s is integral for u, then the R-subalgebra $S' := u(R)[s]$ of S is finitely generated as an R-module. More generally, if there exists an R-subalgebra S' of S containing s that is finitely generated as an R-algebra, then the R-module endomorphism of left multiplication by s on S' comes from an $n \times n$ matrix A with entries in R, for some choice of n generators of S' as an R-module. The characteristic polynomial $p(t)$ of A is a monic polynomial with coefficients in R. By the Cayley-Hamilton Theorem, the element $p(s)$ of S' equals 0. Thus s satisfies a monic polynomial with coefficients in R. More generally, for every monic polynomial $p(t)$ of degree n with coefficients in R such that $p(s)$ equals 0, the monic polynomial gives an R-linear relation $s^n = -(c_1 s^{n-1} + \cdots + c_{n-1}s + c_n 1)$, showing that the R-submodule of S generated by $1, s, \ldots, s^{n-1}$ already contains s^n. By induction, it contains $s^{n+\ell}$ for every nonnegative integer ℓ. Thus the R-subalgebra $u(R)[s]$ is generated by $1, s, \ldots, s^{n-1}$ as an R-module, i.e., s is integral for u. □

Proposition 2.24 (Finitely generated, integral extensions are finite)**.** *An integral ring extension is finite if and only if it is finitely generated.*

Proof. Every finite ring extension is clearly finitely generated: the finite set of R-module generators are also a finite set of R-algebra generators. Conversely, for an integral morphism of commutative rings, $u : R \to S$, assume that S is finitely generated as an R-algebra. We will prove that S is a finite R-module by induction on the least number of generators as an R-algebra. If the number is 0, then S is already a quotient ring of R, which is also a cyclic R-module, hence finitely generated.

By way of induction, assume that the least number of generators n is positive and the result has been proved for fewer generators. Then there exists an R-subalgebra T of S that is finitely generated as an R-algebra by $n-1$ elements, and S is generated over T by a single element s. Since S is integral over R, every R-subalgebra of S is integral over R, i.e., T is integral over R. Thus, by the induction hypothesis, T is finitely generated as an R-module. Since s is integral over R, it is also integral over T. By the previous lemma, S is finitely generated as a T-module. Since both the ring

extensions $R \to T$ and $T \to S$ are finite ring extensions, also the composite ring extension $R \to S$ is a finite ring extension. Thus, by induction on n, every integral ring extension that is finitely generated as an algebra is also finitely generated as a module. □

We are most interested in commutative rings that are fields, and in ring homomorphisms that are field extensions. Fields (and integral domains, and local rings, etc.) are special in that the only idempotents are 1 and 0.

3 Idempotents and ring decompositions

After polynomial algebras, the other example of "elementary" ring extensions are products of copies of a ring. In order to describe decompositions of a ring as a product of factors, it is convenient to discuss idempotents.

Definition 3.1. For every commutative ring R, an element e of R is an **idempotent** if (and only if) $e \cdot e$ equals e. In particular, the multiplicative identity 1 is the **unit idempotent** and the additive identity 0 is the **zero idempotent**. All other idempotents are nonzero, noninvertible idempotents.

Lemma 3.2 (Complement, meet, and join)**.** *For every commutative ring R, for all idempotent elements e and e' of R, also $1-e$ and ee' are idempotent elements. Thus $e+e'-ee' = 1-(1-e)(1-e')$ is an idempotent element. If particular, if ee' equals 0, also $e+e'$ is an idempotent element.*

Lemma 3.3. *For every morphism of commutative rings, $u : R \to S$, for every idempotent element e of R, also $u(e)$ is an idempotent element of S. Also u maps the unit idempotent to the unit idempotent and the zero idempotent to the zero idempotent.*

Definition 3.4. For every commutative ring R, the **idempotent set**, denoted $\mathsf{Idem}(R)$, is the subset of R of all idempotent elements. For all elements e and e' in $\mathsf{Idem}(R)$, the **meet** of e and e' is $e \wedge e' = ee'$, i.e., meet is multiplication. Also the **join** of e and e' is $e \vee e' = e + e' - ee'$. For every morphism of commutative rings, $u : R \to S$, the restriction of u to $\mathsf{Idem}(R)$ as a function to $\mathsf{Idem}(S)$ is denoted $\mathsf{Idem}(u)$.

Lemma 3.5 (Idempotents form a Boolean algebra)**.** *For every commutative ring R, the set $\mathsf{Idem}(R)$ is a Boolean algebra whose join identity equals 0 and whose meet identity equals 1: meet and join are both commutative and associative, meet and join distribute, and, for all idempotents e and e', each of $e \wedge e$, $e \vee e$, $e \wedge (e \vee e')$ and $e \vee (e \wedge e')$ equal e.*

Lemma 3.6. *For every morphism of commutative rings, $u : R \to S$, the function $\mathsf{Idem}(u)$ is a morphism of Boolean algebras.*

Proposition 3.7 (Idempotents form a functor)**.** *The rules above define a functor* Idem *from* **CRing** *to the full subcategory* **BoolAlg** *whose objects are Boolean algebras, and* Idem *is right adjoint to the inclusion of* **BoolAlg** *in* **CRing***.*

Definition 3.8. For every commutative ring R, for every ordered pair (e', e'') of idempotents in R, the pair is **orthogonal** if (and only if) $e'e''$ equals 0. For every commutative ring R, for every ordered pair (e, e') of idempotents in R, the idempotent e' **decomposes** e if (and only if) ee' equals e'. In this case, also $e'' := e - e'$ is an idempotent that decomposes e, the pair (e', e'') is orthogonal, and e equals $e' + e''$. An idempotent e' of R is **primitive** if (and only if), for every idempotent e of R, either ee' equals e' or ee' equals 0, i.e., either e' decomposes e or e' is orthogonal to e. A subset Σ of $\mathsf{Idem}(R)$ is **orthogonal** if (and only if) every ordered pair of distinct elements of Σ is orthogonal. A nonempty othogonal subset Σ of $\mathsf{Idem}(R)$ is **complete** if (and only if) the natural ring homomorphism $R \to \prod_{e \in \Sigma} R \cdot e$ is an isomorphism. A complete, orthogonal subset is **redundant** if (and only if) it contains 0 as an element, otherwise it is **irredundant**. An irredundant, complete, orthogonal subset is a **decomposition** of R. A decomposition of R is a **primitive decomposition** if (and only if) every idempotent in the decomposition is primitive. A decomposition of R is **trivial** if (and only if) it equals $\{1\}$, otherwise it is **nontrivial**. A **finite decomposition** of R is a decomposition that is a finite set.

Proposition 3.9 (Primitive idempotents)**.** *For every commutative ring* R*, for every idempotent* e *in* R*, the idempotent* $1 - e$ *is orthogonal to* e*. For every idempotent* e' *in* R*, the idempotent* e *is orthogonal to* e' *if and only if* $e'(1 - e)$ *equals* e'*, i.e., if and only if* e' *decomposes* $1 - e$*. A nonzero idempotent* e' *is primitive if and only if, for every idempotent* e*, either* e' *decomposes* e *or* e' *decomposes* $1 - e$*. For every finite, primitive decomposition* Σ *of* R*, every idempotent in* R *is of the form* $\sum_{e \in I} e$ *for a unique subset* I *of* Σ*, and the primitive idempotents correspond to singleton subsets of* Σ*. There exists a finite, primitive decomposition* Σ *if and only if the Boolean algebra* $\mathsf{Idem}(R)$ *is a finite set, in which case this Boolean algebra is isomorphic to the Boolean algebra* $\mathcal{P}(\Sigma)$*, the power set of* Σ*, with intersection as meet and union as join.*

Proof. An element e is idempotent if and only if $e(1 - e)$ equals 0. Since $1 - (1 - e)$ equals e, this holds if and only if $1 - e$ is idempotent, and then e and $1 - e$ are orthogonal idempotents. For every element e', the product $e'e$ equals 0 if and only if $e'(1 - e)$ equals e'. In that case, also $e''(1 - e)$ equals e'' and $e''e'$ equals 0 for $e'' := (1 - e) - e'$. Thus, $e'' \cdot e''$ equals $e''(1 - e) - e''e'$ equals e'', i.e., e'' is an idempotent, e'' is orthogonal to e', and $1 - e$ equals $e' + e''$, so that e' decomposes $1 - e$.

For every finite, primitive decomposition, say $\Sigma = \{e_1, \ldots, e_n\}$, we have that $e_i e_j$ equals e_i if i equals j, and 0 otherwise. Also $e_1 + \cdots + e_n$ equals 1. Thus, for every idempotent e, also e equals $e \cdot 1$ equals $ee_1 + \cdots + ee_n$. Since each e_i is primitive, ee_i equals either e_i or 0. Thus, e equals the sum of e_i over those e_i in the finite set $I = \Sigma_e$ of all e_i with ee_i equal to e_i. By convention, the empty set corresponds to the idempotent 0. Altogether, the correspondence associating $I = \Sigma_e$ to e and

associating $e \sum_{e \in I} e$ to I gives inverse bijections between the Boolean algebra of idempotents in R and the Boolean algebra $\mathcal{P}(\Sigma)$ of subsets of Σ. □

Corollary 3.10 (Noetherian rings have finite primitive decompositions)**.** *For every commutative ring R, for every irredundant decomposition Σ of R, for each subset I of Σ, the subset $R \cdot I = \sum_{e \in I} R \cdot e$ is an ideal in R whose annihilator is $R \cdot (\Sigma \smallsetminus I)$. In particular, if R is Noetherian, there exists a finite, primitive decomposition such that every factor ring is Noetherian. Conversely, every product of finitely many Noetherian rings is a Noetherian ring.*

Definition 3.11. For every commutative ring R, for every finite, irredundant decomposition Σ of R, a **refinement** of Σ is a finite, irredundant decomposition $\widetilde{\Sigma}$ of R such that every element of Σ equals $\sum_{e \in I} e$ for a unique subset I of $\widetilde{\Sigma}$.

Lemma 3.12 (Refinement and partitions)**.** *For every commutative ring R, refinement defines a lattice operation on the set of finite, irredundant decompositions. If R has a finite, primitive decomposition Σ, every finite, irredundant decomposition of R corresponds to a partition of Σ, and refinement corresponds to refinement of partitions.*

Definition 3.13. For every morphism of commutative rings, $u : R \to S$, a u-**decomposition** is an ordered pair (Ξ, Σ) of a finite, irredundant decomposition Ξ of R and a refinement Σ of the finite, irredundant decomposition $u(\Xi) \smallsetminus \{0\}$ of S. For every element e of Ξ, the e-**fiber** of Σ, is the subset Σ_e of all elements e' in Σ such that $u(e)e'$ equals e'. A u-**refinement** of (Ξ, Σ) is an ordered pair $(\widetilde{\Xi}, \widetilde{\Sigma})$ such that $\widetilde{\Xi}$ is a refinment of Ξ, and $\widetilde{\Sigma}$ is a refinement both of Σ and of $u(\widetilde{\Xi}) \smallsetminus \{0\}$.

Finite decompositions arise when considering "locally constant" functions in algebra, e.g., the rank of a finitely generated, projective module.

Proposition 3.14 (Rank decomposition)**.** *For every nonzero commutative ring R, for every finitely generated, projective R-module M, there exists a nonempty, finite set $\mathsf{rank}_R(M)$ of nonnegative integers and a finite, irredundant decomposition $\Sigma = \{e_{M,d} | d \in \mathsf{rank}_R(M)\}$ of R such that, for every element d of $\mathsf{rank}_R(M)$, the factor ring $R \cdot e_{M,d}$ is a nonzero ring and $(R \cdot e_{M,d}) \otimes_R M$ is a finitely generated, projective $R \cdot e_{M,d}$-module of constant rank d.*

Proof. Since M is finitely generated, it is a quotient R-module of $R^{\oplus e}$ for some nonnegative integer e. Since M is projective, this quotient splits. Thus M is the image of an R-module endomorphism U of $R^{\oplus e}$ (even an idempotent endomorphism) whose cokernel is projective. (Conversely, for every R-module endomorphism of $R^{\oplus e}$, for finite integer e, if the cokernel is projective, then the image is a finitely generated, projective module.)

For every element d of $\mathsf{rank}_R(M)$, for every choice I of d rows and of d columns of U, i.e., of a $d \times d$ submatrix U_I of U, let $R_{d,I}$ be the R-algebra obtained by taking the quotient of R by the

ideal generated by the determinants of all $(d+1)\times(d+1)$ submatrices of U and then inverting the determinant of U_I. Let R_d be the image of R in $\prod_I R_{d,I}$, where the product is over all sets I of d rows and d columns of the $e\times e$ matrix. By construction, $R_d\otimes_R M$ is a finitely generated, projective R_d-module of constant rank d.

It only remains to prove that the natural R-algebra homomorphism from R to $\prod_{d\in\mathsf{rank}_R(M)} R_d$ is an isomorphism (this then gives the idempotents by inverting the isomorphism). Since both the domain and target are finitely generated R-modules, by Nakayama's Lemma, we can check this after localization at each maximal ideal $\mathfrak{m}$ of R. Every finitely generated, projective module over a local ring is free of (constant) finite rank d. Thus, $R_\mathfrak{p}\otimes_R R_c$ equals a zero module unless $c=d$, and the natural homomorphism $R_\mathfrak{p}\to R_\mathfrak{p}\otimes_R R_d$ is an isomorphism. □

Definition 3.15. For every commutative ring R, for every finite, finitely presented and flat morphism of commutative rings, $u:R\to S$, the R-algebra S is R-**indecomposable** if (and only if) every idempotent in S is the u-image of an idempotent in R. A u-decomposition (Ξ,Σ) is u-**primitive** if (and only if) for every idempotent e in Ξ and for every idempotent e' in Σ such that $u(e)e'$ equals e', the $R\cdot e$-algebra $S\cdot e'$ is $R\cdot e$-indecomposable.

Exercise 3.16. For R equal to the product ring $\mathbb{Z}\times\mathbb{Z}$ with primitive idempotents $\mathbf{e}_1=(1,0)$ and $\mathbf{e}_2=(0,1)$, for S equals the product ring $R\times R$ with the diagonal morphism $u:R\to S$ sending each element $r=(r_1,r_2)$ to (r,r) and with idempotents $\mathbf{e}'_1=(1,0)$ and $\mathbf{e}'_2=(0,1)$ prove that both $(\Xi,\Sigma)=(\{1\},\{\mathbf{e}'_1,\mathbf{e}'_2\})$ and $(\widetilde{\Xi},\widetilde{\Sigma})=(\{1\},\{\mathbf{e}''_1,\mathbf{e}''_2\})$ are primitive decompositions, where $\mathbf{e}''_1=\mathbf{e}_1\mathbf{e}'_1+\mathbf{e}_2\mathbf{e}'_2$ and $\mathbf{e}''_2=\mathbf{e}_1\mathbf{e}'_2+\mathbf{e}_2\mathbf{e}'_1$. Thus, there is more than one u-primitive decomposition. However, prove that

$$(\{\mathbf{e}_1,\mathbf{e}_2\},\{\mathbf{e}_1\mathbf{e}'_1,\mathbf{e}_1\mathbf{e}'_2,\mathbf{e}_2\mathbf{e}'_1,\mathbf{e}_2\mathbf{e}'_2\})$$

is a common u-refinement of both of these u-primitive decompositions.

4 Algebras of set functions.

The main example of an R-algebra with a specified decomposition is the set of R-valued functions on a set, i.e., an R-algebra of set functions. The basic idea of Galois theory is that every finite separable field extension, and every finite étale morphism of commutative rings more generally, is *locally* (for the faithfully flat topology, or even for the étale topology) just an R-algebra of set functions. In particular, the Galois connection between intermediate field extensions and subgroups of the Galois group follows from consideration of R-algebras of set functions. The main results of this section are Corollary 4.13 and Proposition 4.14 that characterize the R-flat quotient R-algebra of the algebra of set functions, and the R-subalgebras whose quotient module is R-flat. In each

case, these are precisely what one would guess, at least after passing to the nonzero factor rings of a finite decomposition of R.

Definition 4.1. For every commutative ring R, for every set Σ, the R-**algebra of functions** on Σ, denoted R^Σ, is the set of all set functions $a : \Sigma \to R$. This is an R-algebra under pointwise addition, pointwise scaling, and pointwise multiplication; i.e., for a, b in R^Σ and for λ in R, for every σ in Σ we define

$$(a+b)(\sigma) := a(\sigma) + b(\sigma), \quad (\lambda \cdot b)(\sigma) := \lambda \cdot b(\sigma), \quad (a \cdot b)(\sigma) := a(\sigma) \cdot b(\sigma).$$

Lemma 4.2 (Algebras of set functions)**.** *For every commutative ring R, for every set Σ, the R-module R^Σ with valuewise multiplication is a commutative R-algebra whose additive identity is the constant function with value 0 and whose multiplicative identity is the constant function with value 1.*

Definition 4.3. For every commutative ring R, for every function $u : \Sigma \to T$, the **associated morphism** of R-algebras of functions is,

$$R^u : R^T \to R^\Sigma, \quad R^u(a) := a \circ u.$$

Lemma 4.4 (Functoriality)**.** *For every commutative ring R, for every function $u : \Sigma \to T$, the R-module homomorphism R^u is a morphism of R-algebras. For every pair of set functions,*

$$u : \Sigma \to T, \quad v : T \to \Theta,$$

the composition $F^u \circ F^v$ equals $F^{v \circ u}$. Also, for every set Σ, also F^{Id_Σ} is the identity morphism of F^Σ. Altogether, $R^\bullet$ is a functor from the opposite category $(\mathbf{Set})^{opp}$ of the category of sets to $R - \mathbf{Alg}$.

Definition 4.5. For every commutative ring R, for every set Σ, and for every R-algebra B, a **binary** R**-operation** on $\Sigma \times B$ a function,

$$\beta : \Sigma \times B \to R,$$

such that for every σ in Σ, the (curry) map,

$$\beta_\sigma : B \to R, \quad b \mapsto \beta(\sigma, b),$$

is an R-algebra morphism. The set of all binary R-operations on $\Sigma \times B$ is denoted $\mathcal{F}_\Sigma^R(B)$. For every R-algebra morphism $f : A \to B$, the **associated morphism** of sets of binary R-operations is

$$\mathcal{F}_\Sigma^R(f) : \mathcal{F}_\Sigma^R(B) \to \mathcal{F}_\Sigma^R(A), \quad \beta \mapsto \beta \circ (\mathrm{Id}_\Sigma \times f).$$

Lemma 4.6 (Functoriality in the algebra)**.** *For every commutative ring R, for every R-algebra morphism, $f : A \to B$, for every set Σ, for every binary R-operation β on $\Sigma \times B$, also $\mathcal{F}_\Sigma^R(f)$ maps β to a binary R-operation on $\Sigma \times A$. Thus $\mathcal{F}_\Sigma^R(f)$ is well-defined. Also $\mathcal{F}_\Sigma^R(Id_B)$ is the identity on $\mathcal{F}_\Sigma^R(B)$, and $\mathcal{F}_\Sigma^R$ is compatible with composition. Altogether, $\mathcal{F}_\Sigma^R$ is a functor from the opposite category $(R - \mathbf{Alg})^{opp}$ of the category of R-algebras to* **Set***, the category of sets.*

Definition 4.7. For every commutative ring R and for every set Σ, the **evaluation binary R-operation** is

$$\alpha_\Sigma^R : \Sigma \times R^\Sigma \to R, \quad (\sigma, a) \mapsto a(\sigma).$$

Lemma 4.8. *For every commutative ring R and for every set Σ, the evaluation binary R-operation α_Σ^R is a binary R-operation.*

Definition 4.9. For every commutative ring R, for every set Σ, for every R-algebra B, and for every binary R-operation β on $\Sigma \times B$, the **associated R-algebra morphism** is

$$\widetilde{\beta} : B \to R^\Sigma, \quad b \mapsto (\sigma \mapsto \beta_\sigma(b)).$$

Lemma 4.10 (Universal property of the algebra of set functions)**.** *For every commutative ring R, for every set Σ, for every R-algebra B, and for every binary R-operation β on $\Sigma \times B$, the function $\widetilde{\beta}$ is a morphism of R-algebras. In fact, it is the unique morphism of R-algebras such that $\mathcal{F}_\Sigma^R(\widetilde{\beta})$ maps α_Σ^R to β. Thus, the element α_Σ^R in $\mathcal{F}_\Sigma^R(R^\Sigma)$ represents the functor $\mathcal{F}_\Sigma^R$. Altogether, $R^\bullet$ is left adjoint to the Yoneda functor h_R from $(R - \mathbf{Alg})^{opp}$ to* **Set***.*

Proposition 4.11 (Injections and surjections)**.** *For every nonzero commutative ring R and for every set map, $u : \Sigma \to T$, both of the following hold.*

(i) The R-algebra homomorphism R^u is injective if and only if u is surjective.

(ii) Also R^u is surjective if and only if u is injective.

Proof. **(i)** First assume that u is injective, i.e., the associated surjective set map

$$u_{\text{surj}} : \Sigma \to u(\Sigma)$$

is a bijection. Denote by u_{surj}^{-1} the inverse bijection. For every set map $a : \Sigma \to R$, define $u_!(a) : T \to R$ to be the unique set map which equals $a \circ u_{\text{surj}}^{-1}$ on $u(\Sigma)$ and which equals 0 on the complement $T - u(\Sigma)$. Then $R^u(u_!(a))$ equals a, so that R^u is surjective. Note that the rule $a \mapsto u_!(a)$ is a right inverse to R^u which is an R-module homomorphism. But $u_!(1)$ equals 1 if and only if u is surjective. So in general $u_!$ is not a ring homomorphism (since it does not send 1 to 1).

Next assume that u is not injective. Then there exist distinct elements σ and σ' in Σ such that $u(\sigma)$ equals $u(\sigma')$. For every b in R^T, $R^u(b)$ equals $b \circ u$, and so has equal values on σ and σ'. Define $\mathbf{e}_\sigma : \Sigma \to R$ to be the set map which equals 1 on σ, and which equals 0 on $\Sigma - \{\sigma\}$. Since $\mathbf{e}_\sigma$ has different values on σ and σ' (since 1 does not equal 0 in R), $\mathbf{e}_\sigma$ is not in the image of R^u. Thus R^u is not surjective.

(ii) First assume that u is surjective. Let b and b' be elements in R^T such that $R^u(b)$ equals $R^u(b')$, i.e., $b \circ u$ equals $b \circ u'$. For every τ in T, there exists σ in Σ with $\tau = u(\sigma)$. Thus $b(\tau)$ equals $(b \circ u)(\sigma)$, which equals $(b' \circ u)(\sigma)$ by hypothesis, and this equals $b'(\tau)$. So b equals b'. Therefore R^u is injective.

Next assume that u is not surjective, i.e., there exists τ in T which is not in $u(\Sigma)$. Then $R^u(\mathbf{e}_\tau)$ equals 0, which equals $R^u(0)$. But $\mathbf{e}_\tau$ is not equal to 0. Thus R^u is not injective. □

Because of the proposition, injective set maps with target Σ determine R-algebra quotients of R^Σ. Because quotient objects are a bit less canonical than subobjects, we will instead talk about the kernel of the quotient homomorphims, which is an ideal in R^Σ. Similarly, surjective set maps with source Σ determine R-subalgebras of R^Σ.

Proposition 4.12 (Ideals and quotients of algebras of set functions)**.** *For every nonzero commutative ring R and for every finite set Σ, every ideal in R^Σ whose quotient is a projective R-module is of the form $Ker(R^u)$ for an injective function $u : T \to \Sigma$, at least after passing to the nonzero factor rings of a finite decomposition of R. For every injective function $u' : T' \to \Sigma$ such that that $Ker(R^{u'})$ equals $Ker(R^u)$, there exists a unique function $v : T' \to T$ such that u' equals $u \circ v$ (and necessarily v is a bijection).*

Proof. Let I be an ideal in R^Σ, over every factor ring of R, let T_I to be the subset of Σ consisting of all elements τ such that $\alpha_{\Sigma,\tau}(I)$ equals $\{0\}$. This defines a locally constant function on the factor rings to the finite power set of Σ. Thus, there exists a finite decomposition of R such that this is a constant function on each factor ring. After replacing R by each factor ring, assume that this is a constant function.

Let $u_I : T_I \to \Sigma$ be the inclusion map. The claim is that I equals $\mathrm{Ker}(R^{u_I})$. By construction, I is contained in $\mathrm{Ker}(R^{u_I})$. Thus, the image R^{T_I} is a quotient R-algebra of R^Σ/I. Both of these are projective R-modules of finite, constant rank. Thus this splits as an R-module homomorphism, and the kernel is also a projective R-module of finite, constant rank (the difference of the previous ranks). The quotient R-algebra homomorphism is an isomorphism if and only if this difference rank equals 0, i.e., if and only if the two previous ranks are equal. This can be checked after replacing R by any residue field $R/\mathfrak{m}$ for any maximal ideal $\mathfrak{m}$ (since R is a nonzero ring, it has a maximal ideal). Thus, without loss of generality, now assume that R equals F is a field.

For every element σ in Σ, denote by $\mathbf{e}_\sigma$ the set function which equals 1 on σ and which equals 0 on $\Sigma - \{\sigma\}$. Then $\mathrm{Ker}(F^{u_I})$ is the free F-vector space with basis $\{\mathbf{e}_\sigma | \sigma \in \Sigma - T_I\}$. For every element σ in $\Sigma - T_I$, $\alpha_{\Sigma,\sigma}(I)$ is an F-submodule of F which is not equal to $\{0\}$, i.e., it is a nonzero ideal in R. Since F is a field, this ideal equals all of F, i.e., there exists an element a in I such that $a(\sigma)$ equals 1. Since I is an ideal, $\mathbf{e}_\sigma \cdot a$ is in I. But $\mathbf{e}_\sigma \cdot a$ equals $\mathbf{e}_\sigma$, so $\mathbf{e}_\sigma$ is in I. Thus I contains $\mathrm{span}(\mathbf{e}_\sigma | \sigma \in \Sigma - T_I)$, i.e., I contains $\mathrm{Ker}(F^{u_I})$, proving that I equals $\mathrm{Ker}(F^{u_I})$.

Now let $u : T \to \Sigma$ be the inclusion of a subset of Σ. And let $u' : T' \to \Sigma$ be an injective set map such that $\mathrm{Ker}(R^{u'})$ equals $\mathrm{Ker}(R^u)$. For every σ in $\Sigma - T$, since $\mathbf{e}_\sigma$ is in $\mathrm{Ker}(R^u)$, also $R^{u'}(\mathbf{e}_\sigma)$ equals 0. Thus σ is not in the image of u'. So $\mathrm{Image}(u')$ is contained in T. Define $v : T' \to T$ to be the unique map such that u' equals $u \circ v$.

The final claim is that v is a bijection. Since u' is an injection, also v is an injection. And for every τ in T, since $\mathbf{e}_\tau$ is not in $\mathrm{Ker}(R^u)$, also $\mathbf{e}_\tau$ is not in $\mathrm{Ker}(R^{u'})$. Thus τ is in the image of u. Therefore also v is surjective, i.e., v is a bijection. □

Corollary 4.13 (Surjective morphisms between algebras of set functions)**.** *For every nonzero commutative ring R, and for all finite sets Σ and T, every surjective R-algebra homomorphism $R^\Sigma \to R^T$ is of the form R^u for a unique set map $u : \Sigma' \to \Sigma$, at least after passing to the nonzero factor rings of a finite decomposition of R. In this case, u is an injection. If R^u is an isomorphism, then u is a bijection.*

Proof. The corollary is trivial if T is empty. Thus assume that T is nonempty. Let $\phi : R^\Sigma \to R^T$ be a surjective R-algebra homomorphism. For every element τ of T, let $e_\tau : \{\tau\} \to T$ be the inclusion. The composition $R^{e_\tau} \circ \phi$ is a surjection from R^Σ to $R^{\{\tau\}}$ whose kernel is an ideal with projective quotient R-algebra. By Proposition 4.12, after passing to factor rings, this is the kernel of the R-algebra homomorphism of a subset of R^Σ. Since this kernel is maximal ideals with R-projective quotient of positive rank, the subset is a minimal nonempty subset, i.e., a singleton set $\{\sigma\}$ for a unique element σ of Σ.

For every τ as above, define $u(\tau)$ to be this unique element σ. Then $u : T \to \Sigma$ is the unique set map such that $R^{e_\tau} \circ R^u$ equals $R^{e_\tau} \circ \phi$ for every element τ of T. But the product map

$$(R^{e_\tau})_{\tau \in T} : R^T \to \prod_{\tau \in T} R^{\{\tau\}}$$

is an isomorphism. Since the composition of this isomorphism with R^u equals the composition with ϕ, R^u equals ϕ. Thus u is the unique set map such that R^u equals ϕ.

Also, if $u(\tau)$ equals $u(\tau')$, then $R^{e_\tau} \circ R^u$ equals $R^{e_{\tau'}} \circ R^u$. Thus $R^{e_\tau} \circ \phi$ equals $R^{e_{\tau'}} \circ \phi$. Since ϕ is surjective, this means that R^{e_τ} equals $R^{e_{\tau'}}$. In particular they have equal kernels. But again by Proposition 4.12, this implies that τ equals τ'. Therefore u is injective.

Finally, if R^u is invertible, then the same argument proves that the inverse map is of the form R^v for a unique set map $v : \Sigma \to T$, which is an injective set map. But then $R^{u\circ v}$ and $R^{v\circ u}$ are the respective identity maps on R^Σ and R^T. Since R^{Id_Σ} and R^{Id_T} are also the identity maps, the uniqueness of the set maps above implies that $u \circ v$ equals Id_Σ and $v \circ u$ equals Id_T. Thus u is a bijection. □

For the proof of the next proposition, it is useful to make two definitions. First of all, for every a in R^Σ, the *support* of a is the set of all elements σ in Σ such that the induced R-module morphisms

$$(-)\cdot a\cdot \mathbf{e}_\sigma : R \to R^\Sigma\cdot \mathfrak{e}_\sigma \cong R,$$

is surjective, hence an isomorphism.

Next, for every subset T of Σ, define $\mathbf{e}_T$ to be the set function $\Sigma \to R$ which equals 1 on T and which equals 0 on $\Sigma - T$. Sometimes this is called the *characteristic function* or the *indicator function* of T. Observe that $\mathrm{Supp}(\mathbf{e}_T)$ equals T.

Proposition 4.14 (Subalgebras of algebras of set functions and partitions)**.** *Let R be a nonzero commutative ring, and let Σ be a finite set. Every R-subalgebra in R^Σ whose quotient is a projective R-module is of the form Image(R^q) for a surjective set map $q : \Sigma \to \Theta$, at least after passing to the nonzero factor rings in a finite decompostion of R. If $q' : \Sigma \to \Theta'$ is a surjective set map with Image$(R^{q'})$ equal to Image(R^q), then there exists a unique set map $w : \Theta \to \Theta'$ such that q' equals $w \circ q$ (and necessarily w is a bijection).*

Proof. Let B be an R-subalgebra of R^Σ (in particular B contains 1) such that R^Σ/B is a projective R-module. Let σ be any element of Σ. For every factor ring, consider the collection of all nonempty subsets of Σ of the form $\mathrm{Supp}(b)$ for all elements b of B with nonempty support. This collection is a subset of the power set of Σ, and there are only finitely many such subsets. Moreover, this is locally constant on factor rings of finite decompositions of R. Thus, after replacing R by each nonzero factor ring of some finite decomposition of R, assume that this collection is unchanged under passing to (nonzero) factor rings of finite decompositions of R. Similarly, assume that the projective R-module R^Σ/B has constant rank n.

There is at least one subset of Σ in the collection, namely $\Sigma = \mathrm{Supp}(1)$. For any two distinct minimal subsets, T and T', which are the supports of elements b and b' of B, then the support of bb' equals the intersection of the supports of b and b', i.e., $T \cap T'$. Since T and T' are minimal, $T \cap T'$ is empty, i.e., any two distinct minimal subsets are disjoint.

Now assume that R is a field F. Let T be a minimal set among all such subsets. For every b in B whose support is contained in T and with $b(\sigma)$ invertible for at least one σ in T, the element $b_\sigma := b\cdot b - b(\sigma)\cdot b$ is in B and has strictly smaller support than T. Since T is minimal, the support

is an empty set. Since F is a field, this element is zero, i.e., $b \cdot b$ equals $b(\sigma) \cdot b$. Since $b(\sigma)$ is a nonzero element of F, also $(1/b(\sigma))b$ is an element of the F-algebra B, and this is idempotent. Thus, this idempotent element with support T equals $\mathbf{e}_T$, i.e., b equals $b(\sigma)\mathbf{e}_T$. So the F-subalgebra B contains the element $\mathbf{e}_T$ and $B \cdot \mathbf{e}_T$ equals $F \cdot \mathbf{e}_T$. Also $1 - \mathbf{e}_T = \mathbf{e}_{\Sigma \smallsetminus T}$ is an element of B, and we may repeat this argument for the F-subalgebra $B \cdot \mathbf{e}_{\Sigma \smallsetminus T}$ of the F-algebra $F^{\Sigma \smallsetminus T}$. Thus, by induction on the cardinality of Σ, there exists a partition of Σ, say $q : \Sigma \twoheadrightarrow \Theta$, such that the collection consists of all q-preimages of nonempty subsets of Θ and B equals the image of F^q.

Now consider the general case, where R is a nonzero ring that is not necessarily a field. Since R is nonzero, there exists a maximal ideal $\mathfrak{m}$ in R. Denote the residue field $R/\mathfrak{m}$ by F. Then also $F \otimes_R B$ is a subalgebra of $F \otimes_R R^\Sigma = F^\Sigma$ whose quotient is an F-vector space of dimension n, the rank of R^Σ/B. By the above, the collection of support sets for $F \otimes_R B$, which also equals the collection of support sets for B by the local constancy hypothesis, equals the inverse image of all nonempty subsets of Θ for a partition, $q : \Sigma \twoheadrightarrow \Theta$. Let $s : \Theta \to \Sigma$ be a splitting of q, i.e., $s \circ q$ equals Id_Θ.

Consider the composition of the inclusion $B \hookrightarrow R^\Sigma$ with the R-algebra morphism $R^s : R^\Sigma \to R^\Theta$. After base change from R to the residue field F, this is surjective. By Nakayama's Lemma, the cokernel R-module is annihilated by some element not in $\mathfrak{m}$. Since this holds for every maximal ideal of $\mathfrak{m}$, the annihilator of the cokernel finitely generated R-module is contained in no maximal ideal, i.e., it equals all of R (hence contains the element 1). So the cokernel is a zero module, i.e., the composition is surjective. By comparing ranks after base change to F, both the domain and target of this surjective R-module homomorphism are projective R-modules of the same constant rank, so this R-module homomorphism is even an isomorphism. An R-algebra homomorphism that is an isomorphism of R-modules is an isomorphism of R-algebras. Thus the composition is an R-algebra isomorphism.

Since $B \to R^\Theta$ is an isomorphism, the inverse images of the idempotents are idempotents in B, hence idempotents in R^Σ. But we know all the idempotents in R^Σ, each is of the form $\mathbf{e}_T \cdot e$ for some idempotent e in R and some subset T of Σ. Thus, after further decomposition of R into factor rings if necessary, B contains the idempotent $\mathbf{e}_T$ for the q-fiber set T over each element of Θ. In other words, the image of R^q is an R-subalgebra of B. But both B and the image of R^q are R-subalgebras of R^Σ that project isomorphically to R^Θ under R^s. Thus B equals the image of R^q. □

Corollary 4.15 (Morphisms between algebras of set functions)**.** *For every nonzero commutative ring, R, and for all finite sets, Σ and Σ', every R-algebra homomorphism $\phi : R^{\Sigma'} \to R^\Sigma$ is of the form R^u for a unique set map $u : \Sigma \to \Sigma'$, at least after passing to the nonzero factor rings of a finite decomposition of R. Also ϕ is surjective, resp. injective, if and only if u is injective, resp. surjective.*

Proof. Let $\phi : R^{\Sigma'} \to R^{\Sigma}$ be an R-algebra homomorphism. By Proposition 4.14, there exists a surjective set map $q : \Sigma \to \Theta$ such that Image(ϕ) equals Image(R^q), at least after passing to the nonzero factor rings of a finite decomposition of R. Thus ϕ factors through a surjective R-algebra homorphism $\psi : R^{\Sigma'} \to R^{\Theta}$, i.e., $R^q \circ \psi$ equals ϕ, and ψ is unique. By Corollary 4.13, there exists a unique set map $v : \Theta \to \Sigma'$ such that R^v equals ψ, and v is injective. Thus $u = v \circ q$ is the unique set map such that R^u equals ϕ. And by Proposition 4.11, ϕ is surjective, resp. injective, if and only if u is injective, resp. surjective. □

Before continuing we note that both Proposition 4.12 and Proposition 4.14 fail if Σ is an infinite set. First, consider the ideal I in R^{Σ} consisting of all set functions $\Sigma \to R$ which are zero on the complement of a finite subset of Σ (depending on the set function). Let $q : T \to \Sigma$ be a set map such that Ker(R^q) contains I. For every σ in Σ, $\mathbf{e}_\sigma$ is in I, thus $R^q(\mathbf{e}_\sigma)$ equals 0. This means that σ is not in the image of q, i.e., Image(q) is the empty set. This forces T to be the empty set. But then Ker(R^q) is all of R^{Σ}. Since Σ is infinite, 1 is not in I. Thus 1 is in Ker(R^q), but not in I. Therefore I is not of the form Ker(R^q). In fact, the correct notion in the case of infinite sets Σ is the notion of an *ultrapower*, special case of *ultraproducts* built using *ultrafilters*. This is a crucial ingredient in the work of James Ax and Simon Kochen on Emil Artin's conjecture extending his notion of quasi-algebraically closed fields to p-adic fields. (All finite fields are quasi-algebraically closed, and Artin conjectured an extension to p-adic fields. This conjecture was "asymptotically" proved by Ax-Kochen, but disproved in specific cases by Guy Terjanian, with later counterexamples by David Leep.)

Next, consider the R-subspace $B = R \cdot 1 + I$ of R^{Σ}. It is straightforward to check that this is an R-subalgebra of R^{Σ}. The supports of elements of B are precisely the finite subsets of Σ together with the cofinite subsets of Σ, i.e., sets whose complements are finite. The minimal sets among these sets are the singleton sets. So if B were of the form Image(R^q) for a set map $q : \Sigma \to \Theta$, then the fibers of q would be singleton sets, i.e., q would be injective. But then by Proposition 4.11, R^q is surjective so that Image(R^q) equals R^{Σ}. Every infinite set Σ contains an infinite subset T whose complement $\Sigma - T$ is also infinite. So $\mathbf{e}_T$ is an element in R^{Σ} which is not in B. Therefore B is not of the form Image(R^q).

5 Group actions on sets.

We need two results about groups acting on sets. Let $(G, \cdot)$ be a group acting transitively on a set Σ, say via $\mu : G \times \Sigma \to \Sigma$. Let Θ be a partition of Σ which is *G-invariant*, i.e., for every T in Θ and for every g in G, $g \cdot T$ is also in Θ. Then there is an induced action of G on Θ. Moreover, for every T and T' in Θ, since G acts transitively on Σ there exists an element g in G mapping an element

of T to an element of T', i.e., $g \cdot T$ intersects T'. Since Θ is partition, this implies that $g \cdot T$ equals T'. Thus G acts transitively on Θ.

Fix one element T in Θ, and denote by H the stabilizer subgroup, i.e., the set of all h in G such that $h \cdot T$ equals T. The claim is that T equals $H \cdot \tau$ for one, and hence every, element τ in T. Let τ be an element in T. Since $H \cdot T$ is contained in T (in fact equals T), $H \cdot \tau$ is contained in T. And for every element τ' in T, since G acts transitively on Σ, there exists g in G with $g \cdot \tau$ equal to τ'. But then $g \cdot T$ intersects T. Since Θ is a partition, $g \cdot T$ equals T. Thus g is contained in H. So τ' is contained in $H \cdot \tau$. Therefore T equals $H \cdot \tau$ for each element τ in T.

Since G acts transitively on Θ, every partition set is of the form $g \cdot T$. Therefore the partition sets of Θ are precisely the sets of the form $gH \cdot \tau$, as gH varies over the left cosets of H in G, i.e., the elements of G/H. In summary, we have proved the following.

Proposition 5.1 (Equivariant partitions of a G-set)**.** *For every group G, for every nonempty set Σ with a transitive left action of G, for every partition Θ of Σ which is G-invariant, and for every element τ in Σ, denoting by H the stabilizer subgroup of the partition set containing τ, the partition Θ is precisely the collection of subsets $\{gH \cdot \tau | gH \in G/H\}$.*

There is one final observation. Let H be a subgroup of G. Let $G \times (G/H) \to G/H$ be the standard left action of G on G/H. Let $t : G/H \to G/H$ be a set map which is G-equivariant, i.e., $t(g \cdot kH) = g \cdot t(kH)$ for every coset kH in G/H. Define k_0H to be $t(H)$. Then for every coset kH in G/H, we have

$$t(kH) = t(k \cdot H) = k \cdot t(H) = (kk_0)H.$$

So t is uniquely determined by the coset k_0H. However, it is not necessarily well-defined. In order to be well-defined, we must have that $t(hH)$ equals $t(H)$ for every h in H, i.e., hk_0H must equal k_0H for every h in H. In other words Hk_0H must equal k_0H. But this is precisely the condition that k_0 is an element of the normalizer $N_G(H)$. In summary, we have the following.

Proposition 5.2 (Equivariant self-maps of a transitive G-set)**.** *For every group G and for every subgroup H of G, every left G-equivariant map $t : G/H \to G/H$ is of the form $t(kH) = kk_0H$ for a unique coset k_0H in $N_G(H)/H$, and every such map is well-defined and G-equivariant.*

6 Field extensions

The main application of the results about algebras of set functions is to the classification of finite, separable field extensions and their automorphism groups.

Definition 6.1. An associative, unital ring $(D, +, \cdot)$ is a **division algebra** if (and only if) the set of nonzero elements of the ring is a group under multiplication (in particular, this set is nonempty, or, equivalently, the multiplicative identity 1 is nonzero). The set $D^\times$ of nonzero elements of a division algebra D with its group operation $\cdot$ is the **multiplicative group** of D. Every division algebra that is commutative is a **field**.

Lemma 6.2. *For every nonzero commutative ring R, for every ideal I of R, the quotient R/I is a field if and only if I is a maximal ideal.*

Lemma 6.3. *For every nonzero commutative ring R, the set Σ of all nonzerodivisors in R is a saturated, multiplicatively closed subset of R whose associated fraction R-algebra, $\Sigma^{-1}R$, is a field if and only if R is an integral domain. In this case, the field is denoted $\mathrm{Frac}(R)$, the **fraction field** of R.*

Lemma 6.4. *For every nonzero commutative ring R, for every ideal $\mathfrak{p} \subsetneq R$, the quotient commutative ring $R/\mathfrak{p}$ is an integral domain if and only if $\mathfrak{p}$ is a prime ideal. In this case, the R-algebra $\mathrm{Frac}(R/\mathfrak{p})$ is denoted $\kappa(\mathfrak{p})$, the **residue field** of the prime ideal $\mathfrak{p}$ in R.*

Lemma 6.5 (Characteristic of a field)**.** *For every field F, either the kernel of the unique ring homomorphism from $\mathbb{Z}$ to F equals $p\mathbb{Z}$ for some prime integer $p(>1)$, or the homomorphism from $\mathbb{Z}$ to F factors uniquely through the fraction field $\mathbb{Q} = \mathrm{Frac}(\mathbb{Z})$, but not both. In particular, it is the second case for each finite field F, and then the cardinality of F equals $q = p^e$ for some unique positive integer e.*

Proof. Since F is a field, the image of $\mathbb{Z}$ in F is an integral domain. Thus, the kernel is a prime ideal. The nonzero prime ideals in $\mathbb{Z}$ are precisely the ideals $p\mathbb{Z}$ for $p(>1)$ a prime integer, and then $\mathbb{Z}/p\mathbb{Z}$ is a subring of F, so $p \cdot F$ equal $\{0\}$. Otherwise, the kernel is the zero ideal, i.e., the homomorphism from $\mathbb{Z}$ to F is injective. In particular, the image of $\mathbb{Z} \smallsetminus \{0\}$ is contained in $F \smallsetminus \{0\}$, i.e., the image is invertible in F. Thus, the unique ring homomorphism from $\mathbb{Z}$ to F factors uniquely through $\mathbb{Q}$. In particular, for every nonzero element x of F, for every nonzero integer m and for every integer n, there exists a unique element y of F such that $n \cdot x$ equals $m \cdot y$, namely $y = (n/m) \cdot x$.

Since $\mathbb{Q}$ is infinite, for every finite field F the ring homomorphism from $\mathbb{Z}$ to F factors through the residue field $\mathbb{Z}/p\mathbb{Z}$ for some unique prime integer $p(>1)$. Thus, F is a vector space over $\mathbb{Z}/p\mathbb{Z}$. Since F is a finite set with at least two elements (namely 0 and 1), the dimension e of this vector space is finite, equal to a positive integer. Thus, the cardinality of F equals $q = p^e$. □

Definition 6.6. For every field F, if the unique ring homomorphism from $\mathbb{Z}$ to F is injective, then F has **characteristic zero**, also written $\mathrm{char}(F) = 0$, in which case the image of the unique ring homomorphism $\mathbb{Q} \hookrightarrow F$ is the **prime subfield** of F. Otherwise F has **characteristic** p for the unique prime integer $p(>1)$ such that the kernel equals $p\mathbb{Z}$, also written $\mathrm{char}(F) = p$, and the **prime subfield** of F is the image of the unique ring homomorphism $\mathbb{Z}/p\mathbb{Z} \hookrightarrow F$.

Proposition 6.7 (Frobenius homomorphisms)**.** *For every prime integer $p(>1)$, for every commutative ring R such that the image of $\mathbb{Z}$ in R equals $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, the self-map $Frob_R$ from R to R that sends every element x to x^p is a $\mathbb{F}_p$-algebra endomorphism of R. In particular, for every field F of characteristic p, the self-map $Frob_F$ is an endomorphism of $\mathbb{F}_p$-extensions.*

Proof. Of course Frob_R is multiplicative. By the Binomial Theorem, for all elements x and y of R, also

$$(x+y)^p = x^p + \sum_{n=1}^{p-1} \binom{p}{n} x^{p-n}y^n + y^p.$$

Since p is a prime and $n < p$, also $\binom{p}{n}$ equals pm for some positive integer m. Thus $\binom{p}{n}$ equals 0 in R. So Frob_R is also additive, i.e., it is a ring endomorphism. Of course every element in $\mathbb{F}_p$ is mapped back to itself by the self-map sending each x to x^p. Thus, this is even a $\mathbb{F}_p$-algebra endomorphism. □

Corollary 6.8 (Iterates of Frobenius)**.** *For every finite field F with $q = p^e$ elements, for every F-algebra R, the e-fold self-composition Frob_R^e is an F-algebra endomorphism of R. If R is an integral domain, then the image of F in R equals the fixed set of Frob_R^e.*

Proof. Since the multiplicative group $F^\times = F \smallsetminus \{0\}$ is an Abelian group with $q-1$ elements, every element x of $F \smallsetminus \{0\}$ has multiplicative order dividing $q-1$, i.e., $x^{q-1}-1$ equals 0. Thus, every nonzero element x of F is a root of both $t^{q-1}-1$ and $t^q - t = t(t^{q-1}-1)$. Since also 0 is a root of $t^q - t$, the polynomial $t^q - t$ in $F[t]$ factors completely into pairwise distinct, monic, irreducible linear polynomials,

$$t^q - t = \prod_{x \in F} (t - x).$$

In particular, $x^q = \mathrm{Frob}_R^e(x)$ equals x for every x in F. Thus, the endomorphism Frob_R^e of the ring R acts as the identity on the image of F. So Frob_R^e is an F-algebra endomorphism of R.

If R is an integral domain, so that R is a subring of its fraction field $\mathrm{Frac}(R)$, then the factorization above of $t^q - t$ is also the (unique) factorization in $\mathrm{Frac}(R)[t]$. Thus, the only roots of $t^q - t$ in R are the elements in the image of F, i.e., the image of F equals the fixed set of Frob_R^e. □

Definition 6.9. A **field extension** is a morphism of commutative rings, $u : F \to E$, such that both $(F, +, \cdot)$ and $(E, +, \cdot)$ are fields. A field extension is **finite** if and only if it is finite as a morphism of commutative rings, and then the dimension of E as an F-vector space is the **degree** of the finite field extension, denoted $[E : F]$. A finite field extension is a **finite primitive** extension if (and only if) it is a primitive ring extension, i.e., E is isomorphic as an F-algebra to a quotient of $F[t]$. A field extension is **finitely generated** if and only if E is the fraction field of a finitely generated F-subalgebra of E. For every field extension, $u : F \to E$, the **algebraic closure** of F in E is the

integral closure of F in E. In particular, a field extension is **algebraic** if (and only if) it is an integral ring homomorphism.

Lemma 6.10 (Functoriality of fraction fields)**.** *For the category* **IntDomain** *whose objects are commutative rings that are integral domains and whose morphisms are injective ring homomorphisms between integral domains, and for the full subcategory* **Field***, the fraction field functor is left adjoint to the inclusion of* **Field** *in* **IntDomain***.*

Lemma 6.11 (Integral domains whose fraction field is a finite module)**.** *For every injective ring homomorphism $u : R \to E$ from an integral domain R to a field E, if u is an integral ring extension (i.e., every element of E satisfies a monic polynomial with coefficients in R) then u is an isomorphism from R to a subfield of E.*

Proof. For every nonzero element y of R, there exists an element x of E such that $xu(y)$ equals 1 in E. Since u is integral, then x satisfies a monic polynomial with coefficients in R, i.e.,

$$x^n = -(u(c_1)x^{n-1} + \cdots + (-1)^{\ell-1}u(c_\ell)x^{n-\ell} + \cdots + (-1)^{n-1}u(c_{n-1})), \quad c_1, \ldots, c_{n-1} \in R.$$

Multiply both sides of the equation by $u(y^{n-1})$ to obtain,

$$x = -u(c_1 + \cdots + (-1)^{\ell-1}c_\ell y^{\ell-1} + \cdots + (-1)^{n-1}c_{n-1}y^{n-1}).$$

Thus x is an element of $u(R)$. Since this holds for every nonzero element y of R, the commutative ring $u(R)$ is a field. □

Corollary 6.12 (Finitely generated, algebraic extensions are finite)**.** *An algebraic field extension is finite if and only if it is finitely generated.*

Proof. This follows from Proposition 2.24. □

Proposition 6.13 (Subextensions of finite field extensions)**.** *For every finite field extension, $u : F \to E$, for every F-subextension L of E, also $F \to L$ is a finite field extension, and $[E : F]$ equals $[E : L] \cdot [L : F]$.*

Proof. The F-subextension L is an F-vector subspace of the F-vector space E, and E has finite dimension $[E : F]$. Thus, also L has finite dimension $[L : F] \leq [E : F]$. Since E has finite dimension as an F-vector space, it also has finite dimension as an L-vector space, $[E : L] \leq [E : F]$. Finally, for every F-vector space basis $x_1, \ldots, x_\ell$ for L, and for every L-vector space basis $y_1, \ldots, y_m$ for E, the set $\{x_i y_j | 1 \leq i \leq \ell, 1 \leq j \leq m\}$ is an F-vector space basis for E. Hence $[E : F]$ equals $[E : L] \cdot [L : F]$. □

7 Finite fields

This interlude on finite fields both establishes the basic facts about finite extensions of finite fields. This verifies the Fundamental Theorem of Galois Theory explicitly in an important case. Also it proves both the Primitive Element Theorem and the Normal Basis Theorem for finite fields (thus reducing the general case to the cases of each of those theorems to the case of infinite fields).

Lemma 7.1. *For every field F, the group $F^\times = F \smallsetminus \{0\}$ under multiplication is an Abelian group, and every finite subgroup is cyclic. In particular, if F is a finite field with cardinality $q = p^e$ for a prime integer $p(>1)$ and a positive integer e, then $F^\times$ is a cyclic group of order $p^e - 1$.*

Proof. Since F is a commutative ring, the group $F^\times$ is Abelian. For every integer $\ell > 1$, the elements of $F^\times$ of order dividing ℓ are the roots of the monic polynomial $t^\ell - 1$. Each such root gives a unique linear irreducible monic factor of $t^\ell - 1$. By unique factorization of polynomials (a consequence of the division dlgorithm for polynomials), the number of such factors is at most the degree ℓ. For every finite Abelian group $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$, the number of elements of order dividing ℓ equals ℓ^2, which is strictly larger than ℓ. Thus, $F^\times$ contains no subgroup isomorphic to $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$. By the Structure Theorem for Finitely Generated Abelian Groups, it follows that every finite subgroup of $F^\times$ is cyclic. In particular, if F is a finite field of cardinality $q = p^e$, then $F^\times = F \smallsetminus \{0\}$ is a cyclic group of order $p^e - 1$. □

Proposition 7.2 (Existence and uniqueness of a finite field extension of specified positive degree of a finite field)**.** *For every prime integer $p(>1)$, for every positive integer e, for every finite field F of cardinality $q = p^e$, for every positive integer d, there exists a finite field extension, $u : F \to E$, of degree d, and this is unique up to (non-unique) isomorphism of F-extensions. Moreover, the function $Frob_E^e$ from E to E that sends every element x to x^q is an F-linear field automorphism of E of order d. The fixed field of $(Frob_E^e)^c$ is the unique F-subextension of E of degree c for each positive integer divisor c of d. Every automorphism of E as an F-extension equals $(Frob_E^e)^r$ for an integer r whose class in $\mathbb{Z}/d\mathbb{Z}$ is unique. Also, for every element x of E, the size c of the orbit $\mathcal{O} = \{x, Frob_E^e(x), \dots, (Frob_E^e)^{c-1}(x)\}$ under $Frob_E^e$ is a positive integer divisor of d, and the minimal polynomial $m_x(t)$ of x over F factors in E as $\prod_{y \in \mathcal{O}}(t - y)$.*

Proof. First, let $F \to E$ be a finite field extension of degree d. Since $F^\times = F \smallsetminus \{0\}$ is a cyclic group of order $q - 1$, every nonzero element of F is a root of the polynomial $t^{q-1} - 1$, thus also a root of $t(t^{q-1} - 1) = t^q - t$. So the polynomial $t^q - t$ in $F[t]$, and hence also in $E[t]$, factors uniquely as

$$t^q - t = \prod_{x \in F}(t - x).$$

Thus, the only roots of $t^q - t$ in E are the elements x of F, i.e., for x an element of E, the element x^q equals x if and only if x is an element of F. Since x^q equals Frob_E^e, the fixed subfield of Frob_E^e

in E is precisely F. So the subgroup of $\mathsf{Aut}_F(E)$ generated by Frob_E^e is a cyclic group of order d, and the fixed subfield of this group is F.

For every element x of E, the orbit $\mathcal{O}$ of x under the action of this cyclic group of order d is a set of size c dividing d, i.e., the orbit equals,

$$\mathcal{O} = \{x, \mathrm{Frob}_E^e(x), \dots, (\mathrm{Frob}_E^e)^{c-1}(x)\},$$

where c is the smallest positive integer with $(\mathrm{Frob}^e)^c(x)$ equal to x, i.e., with x a root of $t^{q^c} - t$. Consider the minimal polynomial $m_x(t)$ of x over F. Since Frob_E^e maps every coefficient of $m_x(t)$ back to itself, also $\mathrm{Frob}_E^e(m_x(y))$ equals $m_x(\mathrm{Frob}_E^e(y))$ for every y in E. In particular, since $m_x(t)$ is zero on the element x, it is zero on the entire orbit of x under Frob_E^e. Thus, each of the c distinct elements in the orbit are roots of $m(t)$, i.e., $m(t)$ is divisible in $E[t]$ by the monic polynomial $\prod_{r=0}^{c-1}(t-(\mathrm{Frob}^e)^r(x))$. Since the coefficients of this polynomial are elementary symmetric polynomials in the elements of an orbit, each coefficient is fixed by Frob_E^e. Thus, each coefficient is an element of F. So the polynomial is already in $F[t]$. Since it is a monic polynomial in $F[t]$ of positive degree that divides the irreducibe monic polynomial $m(t)$, we have equality,

$$m_x(t) = \prod_{y \in \mathcal{O}} (t - y).$$

Since $E^\times = E \smallsetminus \{0\}$ is a cyclic group of order $q^d - 1$, we also have that $t^{q^d} - t$ factors in $E[t]$ as

$$t^{q^d} - t = \prod_{x \in E} (t - x).$$

Let $x \in E^\times$ be a generator of the cyclic group, i.e., x^{q^d-1} equals 1, but x^m is different from 1 for every proper (positive) divisor m of $q^d - 1$. For every F-algebra

Consider the minimal polynomial $m_x(t)$ of x in $F[t]$, which factors in $E[t]$ as,

$$m_x(t) := \prod_{y \in \mathcal{O}} (t - y).$$

Since the multiplicative order of x equals $q^d - 1$, the elements $x, \mathrm{Frob}_E^e(x) = x^q, \dots, (\mathrm{Frob}_E^e)^{d-1}(x) = x^{q^{d-1}}$ are pairwise distinct, i.e., the orbit has the maximal size d,

$$\mathcal{O} = \{x, \mathrm{Frob}_E^e(x), \dots, (\mathrm{Frob}_E^e)^r(x), \dots, (\mathrm{Frob}_E^e)^{d-1}(x)\}.$$

Let σ be an F-algebra automorphism of E. Since $m_x(t)$ is a polynomial with coefficients in F, for every y in E, also $m_x(\sigma(y))$ equals $m_x(y)$. In particular, σ permutes the roots of $m_x(t)$. Thus, there exists a unique integer $r = 0, \dots, d-1$ such that $\sigma(x)$ equals $(\mathrm{Frob}_E^e)^r(x)$. Then the F-algebra

automorphism $\sigma^{-1} \circ (\mathrm{Frob}_E^e)^r$ maps x back to itself. Since it is a field automorphism, it also maps each power x^m back to itself. But x is a generator of the cyclic group $E^\times$. Thus it maps every element of $E^\times$ back to itself. Since it also sends 0 to 0 (as an additive map), this is the identity function on E. Therefore σ equals $(\mathrm{Frob}_E^e)^r$.

Since $m_x(t)$ is a degree-d, monic, irreducible polynomial in $F[t]$, the F-algebra homomorphism from $F[t]/\langle m_x(t)\rangle$ to the F-subextension $F[x]$ sending t to x is an isomorphism. As explained above, $F[x]$ equals all of E. So x determines an isomorphism of $F[t]/\langle m_x(t)\rangle$ with E. Since x also is a root of the polynomial $t^{q^d} - t$, we have a factorization in $F[t]$,

$$t^{q^d} - t = m_x(t) \cdot g(t),$$

for a monic polynomial $g(t)$ in $F[t]$.

Now let E'/F be any field extension of degree d. By the same argument as above, the polynomial $t^{q^d} - t$ completely factors over E'. Thus, there exists an element x' in E' such that $m_x(x')$ equals 0. This defines an F-algebra homomorphism $F[t]/\langle m_x(t)\rangle \to E'$ sending t to x'. Combined with the unique F-algebra isomorphism from $F[t]/\langle m_x(t)\rangle$ to E sending t to x, this determines a unique F-algebra homomorphism u from E to E' sending x to x'. Since these F-extensions both have degree d, this F-algebra homomorphism is an isomorphism. $F[t]/\langle m_x(t) \cong F[x] = E$ as F-extensions. Please note, since there are d distinct roots of $m_x(t)$ in E', the F-algebra isomorphism u is certainly not unique. Rather it has a free action by the cyclic group $\mathsf{Aut}_F(E)$ of order d generated by Frob_E^e.

By the same argument as above, for every F-subextension L of E that has degree c over F, for some positive divisor c of d, also $L^\times$ is a cyclic group of order $q^c - 1$, hence the polynomial $t^{q^c} - t$ splits as $\prod_{x \in L}(t - x)$ in $L[t]$. Thus the roots of $t^{q^c} - t$ in E are precisely the elements of L. Therefore L is the fixed field of $(\mathrm{Frob}_E^e)^c$. Hence the fixed field of $(\mathrm{Frob}_E^e)^c$ is the unique F-subextension of E that has degree c. Also, for the generator x of $E^\times$, since x^m has order $q^c - 1$ for the integer $m = (q^d - 1)/(q^c - 1) = 1 + q^c + q^{2c} + \cdots + q^{d-c}$, also L equals the subfield $F[x^m]$ of E, i.e., we have an explicit generator of L as an F-subextension of E once we find a generator of the multiplicative group $E^\times$ (this is a computationally difficult problem).

Finally, we prove existence of a degree-d field extension of F. This is proved by induction on the positive integer d. If d equals 1, there is nothing to prove: take E to equal F. Thus, by way of induction, assume that d is greater than 1 and the result is proved for all smaller values of d.

Let $\ell (> 1)$ be a prime divisor of d. Consider the polynomial $t^{q^\ell} - t$ in $F[t]$. We have a factorization,

$$t^{q^\ell} - t = g(t) \cdot \prod_{x \in F}(t - x),$$

for some monic polynomial $g(t)$ of degree $q^\ell - q$. Since $t^{q^\ell} - t$ is relatively prime to its formal derivative, which equals -1, this polynomial is square-free (and separable). Thus, none of the factors $t - x$ for $x \in F$ is a root of $g(t)$, i.e., $g(t)$ has no linear factors.

Let $m(t)$ be a monic, irreducible factor of $g(t)$ in $F[t]$ of minimal degree. The degree c of this polynomial is greater than 1 and no greater than $q^\ell - q$. Let L be the F-extension $F[t]/\langle m(t)\rangle$ of degree c. Then the multiplicative group $L^\times$ is a cyclic group of order $q^c - 1$. For the root $\bar{t}$ of $m(t)$ in L, of course $\bar{t}$ is nonzero (or else $m(t)$ factors already over F), hence $\bar{t}$ is an element of $L^\times$. Thus $(\mathrm{Frob}_L^e)^c(\bar{t})$ equals $\bar{t}$. Thus for every integer s, also $((\mathrm{Frob}_L^e)^c)^s(\bar{t})$ equals $\bar{t}$. Since $m(t)$ is a factor of $t^{q^\ell} - t$, also $(\mathrm{Frob}_L^e)^\ell(\bar{t})$ equals $\bar{t}$. Thus for every integer r, also $((\mathrm{Frob}_L^e)^\ell)^r(\bar{t})$ equals $\bar{t}$. If ℓ does not divide c, then there exist integers r and s such that 1 equals $r\ell + sc$, since ℓ is prime. But then we have,

$$\mathrm{Frob}_L^e(\bar{t}) = ((\mathrm{Frob}_L^e)^\ell)^r(((\mathrm{Frob}_L^e)^c)^s(\bar{t})) = ((\mathrm{Frob}_L^e)^\ell)^r(\bar{t}) = \bar{t},$$

i.e., $\bar{t}$ is in the fixed subfield of Frob_L^e. As proved above, the fixed subfield equals F, which contradicts that $m(t)$ is a monic, irreducible polynomial of degree $c > 1$ in $F[t]$. Therefore ℓ does divide c. So $q^\ell - 1$ divides $q^c - 1 = (q^\ell - 1)(1 + q^\ell + q^{2\ell} + \cdots + q^{c-\ell})$. Therefore there exists an element y in $L^\times$ of multiplicative order $q^\ell - 1$. As above, the subfield $F[y]$ of L is an F-subextension of degree ℓ.

If d equals ℓ, then we are done, the field $E = F[y]$ is an F-extension of degree $d = \ell$. Otherwise, the integer d/ℓ is an integer > 1 that is strictly less than d. By the induction hypothesis, there exists a field extension $F[y] \hookrightarrow E$ that has degree d/ℓ. Therefore the composition $F \hookrightarrow F[y] \hookrightarrow E$ is a field extension of degree d. By induction on d, for every positive integer d there exists a field extension $F \hookrightarrow E$ that has degree e. □

We reformulate these results in the following long-winded way because this is the formulation of the Fundamental Theorem of Galois Theory for finite extensions of finite fields.

Corollary 7.3 (Galois theory for finite fields)**.** *For every finite field F, for every finite field extension $u : F \to E$ such that the minimal polynomial $m_x(t)$ in $F[t]$ of each element x of E splits completely in $E[t]$ as a product of distinct linear factors (every finite field extension of F satisfies this condition), the automorphism group $\mathsf{Aut}_F(E)$ (which is a cyclic group of order d generated by $Frob_F^e$) has cardinality equal to the degree $[E : F]$ (and every positive integer d is such a degree), for every subgroup H of $\mathsf{Aut}_F(E)$ (i.e., for every cyclic subgroup of order c a positive integer divisor of d), the fixed field $\mathsf{Fix}^H(E)$ of H is an F-subextension of E, the automorphism group $\mathsf{Aut}_{\mathsf{Fix}^H(E)}(E)$ equals H, the degree $[E : \mathsf{Fix}^H(E)]$ equals $\#H$, and the degree $[\mathsf{Fix}^H(E) : F]$ equals $[\mathsf{Aut}_F(E) : H]$. Similarly, for every F-subextension L of E, the automorphism group $\mathsf{Aut}_L(E)$ is a subgroup of $\mathsf{Aut}_F(E)$, the fixed field $\mathsf{Fix}^{\mathsf{Aut}_L(E)}$ equals E, the order $\#\mathsf{Aut}_L(E)$ equals the degree $[E : L]$, and the degree $[L : F]$ equals $[\mathsf{Aut}_F(E) : \mathsf{Aut}_L(E)]$. Altogether, this defines an order reversing bijection between the subgroups of $\mathsf{Aut}_F(E)$ (i.e., positive integer divisors c of d) and the F-subextensions of E. Finally, this bijection identifies normal subgroups (in fact, every subgroup of $\mathsf{Aut}_F(E)$ is a normal subgroup) with F-subextensions L such that the minimal polynomial $m_x(t)$ of every element x in F splits completely in $L[t]$ as a product of distinct linear factors (in fact, every F-subextension of E has this property).*

Definition 7.4. For every prime integer $p(>1)$, for every positive integer e, for any of the degree-e, monic, irreducible factors $m(t)$ of the polynomial $t^q - t$ in $\mathbb{F}_p[t]$ (for $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$), the field $\mathbb{F}_p[t]/f_i(t)\mathbb{F}_p[t]$ is a **Galois field** of cardinality $q = p^e$, usually denoted $\mathbb{F}_q$, and sometimes denoted $GF(q)$.

Remark 7.5. Of course every field of cardinality p is uniquely isomorphic to its prime subfield $\mathbb{F}_p$. For positive integers $e > 1$, finite fields of cardinality q are isomorphic, yet the isomorphism is not unique. However, we may use the Axiom of Choice (or some more algorithmic approach) to choose one degree-e, monic, irreducible factor $f_i(t)$ of $t^q - t$ in $\mathbb{F}_p[t]$ for each positive integer e. It is a standard convention in algebra to assume that such a degree-e extension is specified for each positive integer e, and to denoted that specified extension by $\mathbb{F}_q = \mathbb{F}_{p^e}$.

8 Algebraic closures

Algebraic closures of field extensions give one matroid structure on each field E. Then the general Steinitz – MacLane Exchange Theorem for matroids gives the basic results about transcendence bases for finitely generated field extensions.

Definition 8.1. An ordered pair $(E, \overline{\bullet})$ of a set E and an inclusion-preserving function $\overline{\bullet}$ from the power set $\mathcal{P}(E)$ to itself is a **matroid** if (and only if), both $\Sigma \subseteq \overline{\Sigma} = \overline{\overline{\Sigma}}$ for every subset Σ of E, and for every subset Σ of E and for all elements x and y of $E \smallsetminus \overline{\Sigma}$, if x is an element of $\overline{\Sigma \sqcup \{y\}}$ then also y is an element of $\overline{\Sigma \sqcup \{x\}}$. A subset $\mathcal{B}$ of E is **independent** if (and only if), for every proper subset $\mathcal{A} \subsetneq \mathcal{B}$, also $\overline{\mathcal{A}}$ is a proper subset of $\overline{\mathcal{B}}$. A subset $\mathcal{B}$ of E is **generating** if (and only if) $\overline{\mathcal{B}}$ equals E. Finally, a **basis** is a subset of E that is both independent and generating.

Lemma 8.2 (Algebraic closure defines a matroid)**.** *For every field extension, $u : F \to E$, for every subset Σ of E, the algebraic closure $\overline{\Sigma}$ in E of the F-subextension $F(\Sigma)$ gives a matroid structure on $\mathcal{P}(E)$.*

Proof. Let x and y be elements of $E \smallsetminus F(\Sigma)$ such that x is in the algebraic closure of $F(\Sigma \sqcup \{y\})$ in E. Then x satisfies a minimal, irreducible, monic polynomial $m_x(y;t) = t^n + c_1(y)t^{n-1} + \cdots + c_n(y)$ whose coefficients $c_\ell(y)$ are elements of $\overline{\Sigma}(y)$, i.e., fractions of polynomials in y with coefficients in the algebraic closure $\overline{\Sigma}$ in E of $F(\Sigma)$. There are finitely many coefficients, hence there is a common denominator in $\overline{\Sigma}[y]$, say $b_0(y)$. Then, denoting $b_0(y)c_\ell(y)$ by $b_\ell(y)$ in $\overline{\Sigma}[y]$ for $\ell = 1, \ldots, n$, we have an identity

$$b_0(y)x^n + b_1(y)x^{n-1} + \cdots + b_n(y) = 0.$$

If $b_\ell(y)$ is a constant polynomial in y for $\ell = 0, \ldots, n$, then x satisfies a monic polynomial over $\overline{\Sigma}$, hence x is in $\overline{\Sigma}$, contrary to hypothesis. Thus, at least one of the coefficients $b_\ell(y)$ has strictly

positive degree in y. Denoting by d the maximal degree, the identity above is equivalent to an identity,

$$a_0(x)y^d + a_1(x)y^{d-1} + \cdots + a_d(x) = 0,$$

for elements $a_m(x)$ in $\overline{\Sigma}[x]$. Thus y is also an element of $\overline{\Sigma \sqcup \{x\}}$. □

Definition 8.3. For a field extension, $u : F \to E$, a subset $\mathcal{B}$ of E is **transcendental** if (and only if) the induced F-algebra homomorphism to E from the F-polynomial ring $F[\mathcal{B}]$ on the set B is injective, i.e., if and only if $\mathcal{B}$ is an independent set for the matroid structure of algebraic closure. For a field extension $u : F \to E$, a transcendental subset $\mathcal{B}$ of E is a **transcendence basis** if (and only if) E is an algebraic extension of the induced morphism of F-extensions $u_{\mathcal{B}} : \mathrm{Frac}(F[\mathcal{B}]) \to E$, i.e., if (and only if) $\mathcal{B}$ is a basis for the matroid structure. A field extension $u : F \to E$ is **purely transcendental** if (and only if) there exists a transcendence basis $\mathcal{B}$ such that $u_{\mathcal{B}}$ is an isomorphism.

Theorem 8.4 (Steinitz – MacLane Exchange)**.** *For every matroid $(E, \overline{\bullet})$, for every finite basis $\mathcal{B}$, for every independent set $\mathcal{C}$, and for all subsets $\mathcal{B}_0 \subseteq \mathcal{B}$ and $\mathcal{C}_0 \subseteq \mathcal{C}$ such that $\mathcal{B}_0 \cup \mathcal{C}_0$ is also a basis, for every element x of $\mathcal{C} \smallsetminus \mathcal{C}_0$ there exists an element y of $\mathcal{B}_0$ such that also $(\mathcal{B}_0 \smallsetminus \{y\}) \cup (\mathcal{C}_0 \cup \{x\})$ is a basis. Thus, there exists a subset $\mathcal{A}$ of $\mathcal{B}$ such that $\mathcal{A} \cup \mathcal{C}$ is a basis, so that the cardinality of $\mathcal{C}$ is less than or equal to the cardinality of $\mathcal{B}$. So if there exists a finite basis $\mathcal{B}$ for a matroid, then every basis has the same (finite) cardinality as $\mathcal{B}$.*

Proof. Since $\mathcal{C}$ is independent, $\overline{\mathcal{C} \smallsetminus \{x\}}$ is a proper subset of $\overline{\mathcal{C}}$, so that x is not an element of $\overline{\mathcal{C} \smallsetminus \{x\}}$. Since also $\overline{\mathcal{C}_0}$ is a subset of $\overline{\mathcal{C} \smallsetminus \{x\}}$, also x is not an element of $\overline{\mathcal{C}_0}$. Yet x is an element of $\overline{\mathcal{B}_0 \cup \mathcal{C}_0}$. Since $\mathcal{B}_0$ is finite, among the subset $\mathcal{A}$ of $\mathcal{B}_0$ such that x is in $\overline{\mathcal{A} \cup \mathcal{C}_0}$ (e.g., $\mathcal{A}$ equals all of $\mathcal{B}_0$) there exists at least one minimal element $\mathcal{A}$ (for set inclusion), and each minimal element is nonempty.

For every element y of the nonempty set $\mathcal{A}$, since $\mathcal{A}$ is minimal, x is not an element of $\overline{\Sigma}$ for $\Sigma = (\mathcal{A} \smallsetminus \{y\}) \cup \mathcal{C}_0)$, yet x is an element of $\overline{\Sigma \cup \{y\}}$. By the exchange axiom, also y is an element of $\overline{\Sigma \cup \{x\}}$. Thus $\mathcal{B}_0$ is a subset of $\overline{\Theta}$ for $\Theta = (\mathcal{B}_0 \smallsetminus \{y\}) \cup (\mathcal{C}_0 \cup \{x\})$, i.e., Θ is a generating set. We leave it to the reader to check that also Θ is independent. □

Remark 8.5. Assuming the Axiom of Choice, a variant of this argument also shows that the cardinalities of bases are equal even when the cardinalities are infinite.

Proposition 8.6 (Transcendence degree is well-defined)**.** *For every field extension $u : F \to E$, for every transcendental subset, and for every generating set of E as a field extension of F, the transcendental subset can be extended to a transcendence basis using elements of the generating set. Any two transcendence bases for u have equal cardinality.*

Proof. Apply the Steinitz-MacLane Exchange Theorem to the matroid of algebraic closures in E of F-subextensions spanned by Σ. □

Definition 8.7. For every field extension $u : F \to E$, the **transcendence degree** of u, or of E over F (if u is understood) equals the cardinality of any transcendence basis for E over F.

Corollary 8.8 (Existence of a transcendence basis)**.** *Every finitely generated field extension $u : F \to E$ has a finite transcendence basis. Every subextension of a finitely generated field extension also has a finite transcendence basis.*

Proof. By the previous proposition, there exists a finite transcendence basis for E as an F-extension that is a subset of any specified finite generating set for E as an F-extension. For every F-subextension L of E, every transcendental subset of L has cardinality bounded above by the finite transcendence degree of E over F by the Steinitz – MacLane Exchange Theorem. Thus, for a transcendental subset of maximal cardinality, it is a transcendence basis for the subextension (whose finite cardinality is bounded above by the finite transcendence degree of E over F). □

Finally, we present the classic proof by Emil Artin that algebraic closures of a field exist. This is a forerunner of the techniques of James Ax and Simon Kochen using ultraproducts of fields.

Theorem 8.9 (Existence of Algebraic Closures)**.** *For every field F, there exists a field extension $u : F \to E$ such that every monic, irreducible polynomial in $F[t]$ has a root in E. The algebraic closure $\overline{F}$ of F in E is an algebraically closed field that is algebraic over F.*

Proof. First of all, if there exists a field extension $u : F \to E$ such that every monic, irreducible polynomial over F has a root in E, then the algebraic closure $\overline{F}$ of F in E is already algebraically closed. Indeed, every monic irreducible polynomial $f(t)$ in $\overline{F}[t]$ has finitely many coefficients, each of which is an element in $\overline{F}$, hence lies in a finite F-subextension of E. Thus, there exists a finite subextension L/E that contains all the coefficients. Since $f(t)$ is irreducible in the bigger ring $\overline{F}[t]$, it is also irreducible in $L[t]$. Thus $L[t]/\langle f(t)\rangle$ is a finite field extension of F. The F-linear operator of multiplication by $\overline{t}$ on this finite dimensional F-vector space has a minimal polynomial $m(t)$ that is a product of monic, irreducible polynomials $g(t)$ in $F[t]$. Of course $f(t)$ is one of the irreducible factors in $L[t]$, hence $f(t)$ divides the image in $L[t]$ of one of the irreducible factors $g(t)$ of the minimal polynomial $m(t)$. Since $g(t)$ has a root x in E, the finite F-subextension $L[x]$ of E contains a root x of $f(t)$. So $f(t)$ has a root in $\overline{F}$. Since $f(t)$ was irreducible, and has a linear root, it follows that $f(t)$ equals $t - x$, i.e., $f(t)$ is linear. Since this holds for every monic, irreducible polynomial $f(t)$ in $\overline{F}[t]$, the field $\overline{F}$ is algebraically closed.

Now let Σ be the subset of $F[t]$ whose elements are all monic, irreducible polynomials. For every $g(t)$ in Σ, the quotient F-algebra $F[t]/\langle g(t)\rangle$ is nonzero. Let R be the polynomial F-algebra $F[\Sigma]$ with one variable x_g for each element g in Σ. Let I be the ideal in R generated by all elements $g(x_g)$ for all elements $g = g(t)$ in Σ.

If I equals the entire ring R, then there is a finite R-linear combination of elements of the form $g(x_g)$ that sums to 1, and each of the coefficients in this R-linear combination also involves only finitely many of the variables. Altogether, there exists a finite set of pairwise distinct elements $g_1, \dots, g_n$ such that already the intersection of I with the finitely generated polynomial F-algebra $F[x_{g_1}, \dots, x_{g_n}]$ contains 1. However, the finite tensor product $(F[t]/\langle g_1(t)\rangle) \otimes_F \cdots \otimes_F (F[t]/\langle g_n(t)\rangle)$ is nonzero, in fact it is an F-algebra of dimension precisely $\deg(g_1)\cdots\deg(g_n)$. There is an F-algebra homomorphism from $F[x_{g_1}, \dots, x_{g_n}]$ to this tensor product that factors through the ideal I, namely the map that sends x_{g_1} to $t \otimes 1 \otimes \cdots \otimes 1 \otimes 1$, etc., until x_{g_n} which maps to $1 \otimes 1 \otimes \cdots \otimes 1 \otimes t$. Thus, the intersection of I with $F[x_{g_1}, \dots, x_{g_n}]$ does not contain 1.

Since I is a proper ideal in R, by the Axiom of Choice, there exists a maximal ideal $\mathfrak{m}$ in R that contains I. The quotient ring $R/\mathfrak{m}$ is a field extension E of F. By construction, for every irreducible, monic polynomial $g(t)$ in $F[t]$, there exists a root in E, namely the image of x_g. □

9 Properties of ring extensions

For certain properties of ring extensions, the lemmas satisfied by those properties come up so often that Grothendieck referred to these lemmas by the term *sorites* (from the same notion in philosophy referring to the "heap paradox"). There is a sense in which each individual lemma is trivial, at least given the preceding lemmas. However, the aggregate structure of all of the lemmas is nontrivial, much like the grains of sand in a heap. Moreover, the structure of all the lemmas together becomes a useful organizing principle for studying any new property of ring extensions: study the new property by determining which of the "sorites" lemmas the new property satisfies. Eventually, some of these lemmas evolved into the notion of a Grothendieck (pre)topology, leading to the related notion of *topos* of Michael Artin and Grothendieck. Here is yet another important property of associative, unital R-algebras where all of this applies.

Definition 9.1. For every commutative ring R, a morphism of associative, unital rings, $u : R \to S$, with image in the center of S is **separable** if (and only if) the following surjective morphism of S – S-bimodules admits a right inverse that is a morphism of S – S-bimodules,

$$\beta_{S/R} : S \otimes_R S \to S, \quad s' \otimes s'' \mapsto s' \cdot s''.$$

An element ϵ of $S \otimes_R S$ is a

Definition 9.2. separable idempotent if (and only if) both $\beta_{S/R}(\epsilon)$ equals 1 and $(s \otimes 1) \cdot \epsilon$ equals $\epsilon \cdot (1 \otimes s)$ for every element s of S.

Proposition 9.3 (Separability and idempotents)**.** *A morphism of associative, unital rings, $u : R \to S$, is separable if and only if there exists a separable idempotent. In that case, there is a bijection between the set of right inverse $S-S$-bimodule morphisms of $\beta_{S/R}$ and the set of separable idempotents by the function that sends each right inverse $S-S$-bimodule morphism σ to the element $\epsilon = \sigma(1)$ and that sends each separable idempotent ϵ to the right inverse $S-S$-bimodule morphism $\sigma(s) = (s \otimes 1) \cdot \epsilon = \epsilon \cdot (1 \otimes s)$.*

Proof. The two operations in the statement are inverse bijections by chasing through the definitions. □

Corollary 9.4 (Quotients of separable algebras)**.** *For every morphism of associative, untial rings, $u : R \to S$, if S is separable over R, then for every two-sided ideal I in S, also S/I is separable over R.*

Proof. The image in $(S/I) \otimes_R (S/I) = S \otimes_R S/(I \otimes_R S + S \otimes_R I)$ of a separable idempotent is a separable idempotent. □

For morphisms of commutative rings, this simplifies a bit.

Corollary 9.5 (Separable extensions of commutative rings)**.** *A morphism of commutative rings, $u : R \to S$, is separable if and only if there exists an element ϵ with $\beta_{S/R}(\epsilon)$ equal to 1 and that is annihilated by the entire kernel ideal $\langle \{s \otimes 1 - 1 \otimes s | s \in S\} \rangle$ of $\beta_{S/R}$. In particular, since ϵ is annihilated by $1 - \epsilon$, these elements are precisely the separable idempotents.*

Proof. Since the rings are commutative, $\epsilon \cdot (1 \otimes s)$ equals $(1 \otimes s) \cdot \epsilon$. Thus, an element ϵ satisfying $\beta_{S/R}(\epsilon)$ equals 1 is a separable idempotent if and only if $(s \otimes 1 - 1 \otimes s) \cdot \epsilon$ equals 0 for every element s of S, i.e., if and only if ϵ is annihilated by the kernel of $\beta_{S/R}$. □

Among the lemmas that make up the *sorites*, several of them actually make up Grothendieck's notion of a (pre)topology on a category.

Definition 9.6. For every category $\mathbf{C}$ that has finite fiber products, a **Grothendieck pretopology** on $\mathbf{C}$ is an $\mathsf{obj}(\mathbf{C})$-class $\mathcal{T}$ such that the members $\mathfrak{U}$ of the fiber class $\mathcal{T}_X$ over each object X are sets of $\mathbf{C}$-morphisms to X, $\mathfrak{U} = \{f : U \to T\}_{f \in \mathfrak{U}}$, called **$\mathcal{T}$-covering families** of X, that satisfy all of the following conditions.

(i) For every $\mathbf{C}$-isomorphism, $f : U \to X$, the singleton set $\{f\}$ is a member of $\mathcal{T}_X$.

(ii) For every $\mathcal{T}$-covering family $\mathfrak{U}$ of X, for every $\mathbf{C}$-morphism $g : \widetilde{X} \to X$, also the pullback family $g^*\mathfrak{U} = \{U \times_{f,X,g} \widetilde{X} \to \widetilde{X}\}_{f \in \mathfrak{U}}$ is a $\mathcal{T}$-covering family of $\widetilde{X}$.

(iii) For every $\mathcal{T}$-covering family $\mathfrak{U} = \{f : U \to X\}_{f\in\mathfrak{U}}$ of X, for every set $\mathfrak{V} = \{\mathfrak{V}_f\}_{f\in\mathfrak{U}}$ of $\mathcal{T}$-covering families $\mathfrak{V}_f = \{g : V \to U\}_{g\in\mathfrak{V}_f}$ of each domain U of a morphism f in $\mathfrak{U}$, the set $\{f \circ g : V \to X\}_{f\in\mathfrak{U},g\in\mathfrak{V}_f}$ is a $\mathcal{T}$-covering family of X.

For categories that also have arbitrary "disjoint unions" (i.e., coproducts of each set of objects relative to an initial object), it is often convenient to reformulate each covering family $\mathfrak{U}$ into a single morphism $(\sqcup_{f\in\mathfrak{U}}U) \xrightarrow{\sqcup f} X$. This gives the following notion.

Definition 9.7. For every category $\mathbf{C}$ with finite fiber products, for every property $\mathcal{P}$ of $\mathbf{C}$-morphisms, the property $\mathcal{P}$ is **pretopological** if (and only if) it satisfies all of the following.

(i) Every $\mathbf{C}$-isomorphism satisfies $\mathcal{P}$.

(ii) For every $\mathbf{C}$-morphism $f : U \to X$ that satisfies $\mathcal{P}$, for every $\mathbf{C}$-morphism $g : \widetilde{X} \to X$, also the pullback morphism $U \times_{f,X,g} \widetilde{X} \to \widetilde{X}$ satisfies $\mathcal{P}$.

(iii) For every $\mathbf{C}$-morphism $f : U \to X$ that satisfies $\mathcal{P}$, for every $\mathbf{C}$-morphism $g : V \to U$ that satisfies $\mathcal{P}$, also $f \circ g : V \to X$ satisfies $\mathcal{P}$.

(iv) For every $\mathbf{C}$-morphism $f : U \to X$ that satisfies $\mathcal{P}$, for every $\mathbf{C}$-morphism $g : V \to X$ that satisfies $\mathcal{P}$, also $U \sqcup V \xrightarrow{f\sqcup g} X$ satisfies $\mathcal{P}$.

Lemma 9.8. *For every category $\mathbf{C}$ with finite fiber products and arbitrary disjoint unions, for every property $\mathcal{P}$ of $\mathcal{C}$-morphisms that is pretopological, there is an associated Grothendieck pretopology $\mathcal{T}$ such that for every object X, the $\mathcal{T}$-covering families of X are those sets of $\mathcal{C}$-morphisms to X, $\mathfrak{U} = \{f : U \to X\}_{f\in\mathfrak{U}}$, such that $(\sqcup_{f\in\mathfrak{U}}U) \to X$ satisfies $\mathcal{P}$. Conversely, for every Grothendieck pretopology $\mathcal{T}$, for the property $\mathcal{P}$ of $\mathbf{C}$-morphisms $f : U \to X$ that $\{f : U \to X\}$ is a singleton $\mathcal{T}$-covering family, the property $\mathcal{P}$ is pretopological.*

This applies to commutative rings by choosing $\mathbf{C}$ to be the opposite category $\mathbf{CRing}^{\mathrm{opp}}$. Thus, finite fiber products correspond to tensor products of rings, and disjoint union corresponds to (direct) products of factor rings.

Definition 9.9. For every property $\mathcal{P}$ of morphisms of commutative rings, $u : R \to S$, the property $\mathcal{P}$ is **checkable after faithfully flat base change** if (and only if), for every faithfully flat morphism of commutative rings, $v : R \to T$, the morphism u satisfies $\mathcal{P}$ whenever the base change morphism $\mathrm{Id}_T \otimes u : T \to T \otimes_{v,R,u} S$ satisfies $\mathcal{P}$.

Theorem 9.10 (Ring properties that give a Grothendieck pretopology)**.** *For the opposite category $\mathbf{CRing}^{opp}$ of the category of commutative rings, each of the following properties $\mathcal{P}$ is pretopological: finite, fintely generated, finitely presented, flat, faithfully flat, or separable.*

Proof. **(i)** Every isomorphism of commutative rings is finite, finitely generated (using zero variables), finitely presented (using zero variables and zero defining relations), flat, faithfully flat, and separable, since the multiplication map $R \otimes_R R \to R$ is an isomorphism.

(ii) For every R-algebra S that is finite, i.e., a quotient of $R^{\oplus n}$ as an R-module, respectively finitely generated, i.e., $S = R[x_1, \dots, x_n]/I$, finitely presented, i.e., $S = R[x_1, \dots, x_n]/\langle f_1, \dots, f_c \rangle$, flat, faithfully flat, separable, for every R-algebra $\widetilde{R}$, also the $\widetilde{R}$-algebra $\widetilde{R} \otimes_R S$ is the corresponding quotient of $\widetilde{R}^{\oplus n}$, resp. the quotient $\widetilde{R}[x_1, \dots, x_n]/I \cdot \widetilde{R}[x_1, \dots, x_n]$, the quotient $\widetilde{R}[x_1, \dots, x_n]/\langle f_1, \dots, f_c \rangle$, flat over $\widetilde{R}$, faithfully flat over $\widetilde{R}$, separable over $\widetilde{R}$. For the last one, if e is a separable idempotent in $S \otimes_R S$, then the image of e in $\widetilde{R} \otimes (S \otimes_R S) \cong (\widetilde{R} \otimes_R S) \otimes_{\widetilde{R}} (\widetilde{R} \otimes_R S)$ is a separable idempotent.

(iii) For every morphism of commutative rings, $u : R \to S$, for every morphism of commutative rings, $w : S \to T$, if both u and w are finite, i.e., S is a quotient of $R^{\oplus n}$ and T is a quotient of $S^{\oplus m}$ respectively finitely generated, i.e., S is $R[x_1, \dots, x_n]/I$ and T is $S[y_1, \dots, y_m]/J$, finitely presented, i.e., S is $R[x_1, \dots, x_n]/\langle f_1, \dots, f_c \rangle$ and T is $S[y_1, \dots, y_m]/\langle g_1, \dots, g_d \rangle$, flat, faithfully flat, separable, then also $v := w \circ u$ is finite, i.e., T is a quotient of $(R^{+n})^{\oplus m} \cong R^{\oplus(mn)}$, finitely generated, i.e., T is $R[x_1, \dots, x_n, y_1, \dots, y_m]/(I \cdot R[x_1, \dots, x_n, y_1, \dots, y_m] + J \cdot R[x_1, \dots, x_n, y_1, \dots, y_m])$, finitely presented, i.e., T is $R[x_1, \dots, x_n, y_1, \dots, y_m]/\langle f_1, \dots, f_c, g_1, \dots, g_d \rangle$, flat (since both $S \otimes_R (-)$ and $T \otimes_S (-)$ are exact functors, so is the composite functor $T \otimes_R (-)$), faithfully flat (same as above but with "exact" replaced by "faithful and exact"), separable. In this last case, if there exists a separable idempotent $e_{T/S}$ in $T \otimes_S T$ that splits the ring as $T \times T'$, and if there exists a separable idempotent $e_{S/R}$ in $S \otimes_R S$ that splits the ring as $S \times S'$, then in the ring $T \otimes_R T \cong T \otimes_S (S \otimes_R S) \otimes_S T$, the image of $e_{S/R}$ splits the ring as $(T \otimes_S S \otimes_S T) \times (T \otimes_S S' \otimes_S T)$, i.e., as $(T \otimes_S T) \times (T \otimes_S S' \otimes_S T)$. Then the product of the image of $e_{S/R}$ and the idempotent $e_{T/S}$ splits the first factor as $T \otimes_S T \cong T \times T'$, i.e., $T \otimes_R T \cong T \times (T' \times (T \otimes_S S' \otimes_S T))$. So T is a separable R-algebra.

(iv) For every morphism of commutative rings, $u_1 : R \to S_1$ and $u_2 : R \to S_2$, that are both finite, i.e., S_1 is a quotient of $R^{\oplus n_1}$ and S_2 is a quotient of $R^{\oplus n_2}$, respectively finitely generated, i.e., each S_i is a quotient R-algebra $R[t_{i,1}, \dots, t_{i,n_i}]/I_i$, finitely presented, i.e., each S_i is $R[t_{i,1}, \dots, t_{i,n_i}]/\langle f_{i,1}, \dots, f_{i,c_i} \rangle$, flat, i.e., each $S_i \otimes_R (-)$ is exact, faithfully flat, i.e., each $S_i \otimes_R (-)$ is faithful and exact, separable, then so is $S_1 \times S_2$. For finiteness, $S_1 \times S_2$ is a quotient of $R^{\oplus(n_1+n_2)}$. For finite generatedness and finite presentation, $S_1 \times S_1$ is a quotient of $R[t_{1,1}, \dots, t_{1,n_1}, t_{2,1}, \dots, t_{2,n_2}]$ by the ideal $I_1 \cdot R[t_{i,j}] + I_2 \cdot R[t_{i,j}] + \langle t_{1,j} t_{2,k} \rangle_{1 \le j \le n_1, 1 \le k \le n_2}$. For flatness and faithful flatness, use that $(S_1 \times S_2) \otimes_R (-)$ is the direct sum of $S_1 \otimes_R (-)$ and $S_2 \otimes_R (-)$, hence is exact, respectively faithful and exact, if each direct summand is. Finally, given a separable idempotent e_1 in $S_1 \otimes_R S_1$ and a separable idempotent e_2 in $S_2 \otimes_R S_2$, then the sum of the images of e_1 and e_2 for the decomposition $(S_1 \times S_2) \otimes_R (S_1 \times S_2) \cong (S_1 \otimes_R S_1) \times (S_1 \otimes_R S_2) \times (S_1 \otimes_R S_2) \times (S_s \otimes_R S_2)$ split off a factor of $S_1 \times \{0\} \times \{0\} \times S_2 \cong S_1 \times S_2$. □

Proposition 9.11 (Module properties checkable after faithfully flat base change)**.** *For every commutative ring R, for every R-module M, each of the following properties is checkable after faithfully flat base change: M is finitely generated, M is finitely presented, M is flat, M is faithfully flat, M is finitely generated and projective.*

Proof. Let $v : R \to \widetilde{R}$ be a faithfully flat morphism of commutative rings. First suppose that $\widetilde{R} \otimes_R M$ is finitely generated as a $\widetilde{R}$-module. The $\widetilde{R}$-module $\widetilde{R} \otimes_R M$ is generated by the image of $\{1\} \otimes M$. Thus, there exists a finite subset Σ of M whose image in $\widetilde{R} \otimes_R M$ generates as a $\widetilde{R}$-module. This finite subset defines an R-module homomorphism, $q : R^\Sigma \to M$. Since $\mathrm{Id} \otimes q : \widetilde{R}^\Sigma \to \widetilde{R} \otimes_R M$ is surjective, and since $\widetilde{R}$ is faithfully flat as an R-module, also q is surjective. Thus, M is a finitely generated R-module.

Similarly, if $\widetilde{R} \otimes_R M$ is finitely presented, then $\widetilde{R} \otimes_R \mathrm{Ker}(q)$ is finitely generated as a $\widetilde{R}$-module by the image of $\{1\} \otimes_R \mathrm{Ker}(q)$. Thus, there exists a finite subset Θ of $\mathrm{Ker}(q)$ such that the morphism $R^\Theta \to \mathrm{Ker}(q)$ becomes surjective after base change by $\widetilde{R} \otimes_R (-)$. Since $\widetilde{R}$ is a faithfully flat R-module, this morphism is already surjective, i.e., M is already a finitely presented R-module.

Since the functor $(-) \otimes_{\widetilde{R}} (\widetilde{R} \otimes_R M)$ is naturally isomorphic to the functor $(-) \otimes_R M$, the functor $(-) \otimes_{\widetilde{R}} (\widetilde{R} \otimes_R M)$ is exact, respectively faithful and exact, if and only if the functor $(-) \otimes_R M$ is exact, resp. faithful and exact. Thus, the $\widetilde{R}$-module $\widetilde{R} \otimes_R M$ is flat, respectively faithfully flat, if and only if the R-module M is flat, resp. faithfully flat.

Finally, the $\widetilde{R}$-module $\widetilde{R} \otimes_R M$ is finitely presented and flat if and only if the R-module M is finitely presented and flat. Since a module over a ring is finitely presented and flat if and only if it is finitely finitely generated and projective, the $\widetilde{R}$-module $\widetilde{R} \otimes_R M$ is finitely generated and projective if and only if the R-module M is finitely generated and projective. □

Proposition 9.12 (Algebra properties checkable after faithfully flat base change)**.** *For every morphism of commutative rings, $u : R \to S$, each of the following properties is checkable after faithfully flat base change: u is finite, u is finitely generated, u is finitely presented, u is flat, u is faithfully flat, and u is finite, finitely presented and separable.*

Proof. Let $u : R \to S$ be a morphism of commutative rings, and let $v : R \to \widetilde{R}$ be a faithfully flat morphism of commutative rings. If $\widetilde{R} \otimes_R S$ is finitely generated as a $\widetilde{R}$-algebra, then since $\{1\} \otimes S$ generates the $\widetilde{R}$-algebra $\widetilde{R} \otimes_R S$, there exists a finite subset of S such that the induced R-algebra homomorphism $q : R[t_1, \ldots, t_n] \to S$ gives a surjective $\widetilde{R}$-algebra homomorphism,

$$\mathrm{Id}_{\widetilde{R}} \otimes q : \widetilde{R}[t_1, \ldots, t_n] \twoheadrightarrow \widetilde{R} \otimes_R S.$$

Since $\widetilde{R}$ is a faithfully flat R-module, also q is surjective, i.e., S is a finitely generated R-module.

In a similar way, if $\widetilde{R} \otimes_R S$ is finitely presented as a $\widetilde{R}$-algebra, then for the surjective R-algebra homomorphism, $q : R[t_1, \ldots, t_n] \twoheadrightarrow S$, we can find a finite collection $f_1, \ldots, f_c$ in the kernel of q whose

images in $\widetilde{R}[t_1,\dots,t_n]$ generate the kernel of $\mathrm{Id}_{\widetilde{R}}\otimes q$. Thus, the induced map from $R[t_1,\dots,t_n]^{\oplus c}\to \mathrm{Ker}(q)$ becomes surjective after tensoring by $\widetilde{R}\otimes_R(-)$. Since $\widetilde{R}$ is a faithfully flat R-module, already the induced map is surjective, i.e., S is finitely presented.

By the previous result, the R-module S is finitely generated, respectively finitely presented, flat, faithfully flat, if and only if the $\widetilde{R}$-module $\widetilde{R}\otimes_R S$ is finitely generated, resp. finitely presented, flat, faithfully flat.

Finally suppose that $\widetilde{R}\otimes_R S$ is finite, finitely presented and separable. Then this module is finitely presented over $\widetilde{R}$, hence also S is a finitely presented R-module. Moreover, over the commutative ring $(\widetilde{R}\otimes_R S)\otimes_{\widetilde{R}}(\widetilde{R}\otimes_R S)$, the module $\widetilde{R}\otimes_R S$ is finitely generated and projective. Of course this ring is naturally isomorphic to $\widetilde{R}\otimes_R(S\otimes_R S)$, and this module is the base change by the faithfully flat ring homomorphism $S\otimes_R S\to \widetilde{R}\otimes_R(S\otimes_R S)$ of the $S\otimes_R S$-module S. Thus, also S is finitely generated and projective as a module over $S\otimes_R S$. So S is finite, finitely presented and separable over R. □

Corollary 9.13 (Categories of algebras)**.** *For each of the properties $\mathcal{P}$ in the theorem, every identity morphism satisfies $\mathcal{P}$, and the composition of any two morphisms that satisfy $\mathcal{P}$ satisfies $\mathcal{P}$. Thus, there is a subcategory of* $\mathbf{CRing}^{opp}$ *(or, equivalently, a subcategory of* **CRing***) with the same objects as* **CRing** *whose morphism are those morphisms of commutative rings that satisfy $\mathcal{P}$.*

Definition 9.14. A morphism of commutative rings, $u: R\to S$, is **étale** if (and only if) it is finitely presented, flat and separable. It is **faithfully étale** if (and only if) it is finitely presented, faithfully flat and separable. It is **finite faithfully étale** if (and only if) it is finite, faithfully flat and separable.

Corollary 9.15. *The property of being finite faithfully 'etale is pretopological and checkable after faithfully flat base change.*

Remark 9.16. Of course there are many other properties than those above that are pretopological and / or checkable after faithfully flat base change. These are the ones that are relevant for this note. Three of the most important Grothendieck pretopologies on the (opposite category of) **CRing** are the **fppf pretopology** of morphisms that are faithfully flat and finitely presented, the **étale pretopology** of morphisms that are faithfull flat and étale, and the **smooth pretopology** of morphisms that are faithfully flat and smooth. A morphism of commutative rings, $u: R\to S$, is **smooth** (for the usual definition) if and only if there exists a faithfully flat étale morphism $w: S\to T$ such that the R-algebra T is étale over $R[t_1,\dots,t_n]$ for some integer n.

10 Splitting extensions

All finite field extensions are finite, finitely presented, faithfully flat ring homomorphisms. A field extension is finite faithfully étale if and only if it is a finite, separable field extension. All finite flat morphisms that are separable have a decomposition as a product after a finite faithfully étale ring extension that is indecomposable and minimal with this property, i.e., after a *splitting extension*. The first step is a decomposition of the domain ring.

Definition 10.1. For every morphism of commutative rings, $u : R \to S$, the morphism is a **totally split morphism** if (and only if) there exists a u-decomposition (Ξ, Σ) such that for every R-idempotent e in Ξ and for every S-idempotent e' in Σ with $u(e)e'$ equal to e', the ring homomorphism $R \cdot e \to S \cdot e'$ is an isomorphism.

In other words, a morphism of commutative rings, $u : R \to S$, is totally split if and only if there exists a finite decomposition of R such that after base change to each nonzero factor ring, the R-algebra S is isomorphic to a product of finitely many copies of R (the number of copies depends on the factor ring).

Definition 10.2. For every morphism of commutative rings, $u : R \to S$, a morphism of commutative rings, $v : R \to T$, **splits** u if (and only if) $T \to T \otimes_R S$ is a totally split morphism. A **splitting extension** of u is an indecomposable, faithfully flat morphism of commutative rings, $v : R \to T$, that splits u such that, for every morphism of commutative rings, $\widetilde{v} : R \to \widetilde{T}$, that splits u, there exists a (typically non-unique) morphism of commutative rings, $f : T \to \widetilde{T}$, such that $f \circ v$ equals $\widetilde{v}$.

Exercise 10.3. For the finite morphism of commutative rings, $u : R \to S$, with $S = R \times R$, prove that $v = u$ satisfies all of the conditions for a splitting extension except indecomposability. Of course $\mathrm{Id}_R : R \to R$ satisfies all of the conditions including indecomposability. So if we want uniqueness (up to non-unique isomorphism), we need to impose an additional hypothesis for v such as indecomposability.

The goal is to characterize morphisms of commutative rings, $u : R \to S$, that are split by a faithfully flat morphism of commutative rings, $v : R \to T$, and to prove that each of these has a splitting extension v that is even finite faithfully étale, indecomposable, and splits itself. It is convenient to do this through a series of lemmas.

Lemma 10.4 (Necessity of étaleness)**.** *For every morphism of commutative rings, $u : R \to S$, for every faithfully flat morphism of commutative rings, $v : R \to T$, if v splits u, then u is finite and étale.*

Proof. For every finite set Σ, the T-algebra $\prod_{e\in\Sigma} T$ is finite faithfully étale. Since this can be checked after faithfully flat base change, if $T \otimes_R S$ is isomorphic to $\prod_{e\in\Sigma} T$, then also S is a finitely faithfully étale R-algebra. □

Lemma 10.5 (The decomposition is canonical)**.** *For every morphism of commutative rings, $u : R \to S$, for every morphism of commutative rings, $v : R \to T$, and for every decomposition (Ξ, Σ) of $T \otimes_R S$ as a T-algebra, for every idempotent e in Ξ, the set $\mathsf{Hom}_{R-\mathbf{Alg}}(S, T\cdot e)$ is naturally bijective to the subset Σ_e of idempotents e' of Σ such that ee' equals e'. In particular, if $(T\cdot e)\otimes_R S$ is nonzero, then there exists a morphism w_e of commutative rings from S to $T\cdot e$ such that $w_e \circ u$ equals v_e, where v_e is the composition of v with the projection from T to $T\cdot e$.*

Proof. After passing to factor rings, assume that $T\otimes_R S$ is isomorphic as a T-algebra to the algebra of set functions T^Σ for a finite set Σ. By Corollary 4.13, every T-algebra homomorphism from T^Σ to T is the T-algebra homomorphism of evaluation at a unique element of Σ. This establishes the canonical bijection. □

Lemma 10.6 (Compatibility with subalgebras and quotient algebras of S)**.** *For every morphism of commutative rings, $u : R \to S$, for every morphism of commutative rings, $v : R \to T$, if v splits u, then also v splits every R-subalgebra $\widetilde{S}$ of S such that $S/\widetilde{S}$ is a projective R-module, and v splits every quotient R-algebra of S that is a projective R-module. In particular, for every finite decomposition of S, the morphism v splits every factor ring. Conversely, for every finite decomposition of S, $S \xrightarrow{\cong} \prod_{e\in\Sigma} S\cdot e$, if v splits the R-algebra $S\cdot e$ for every e in Σ, then v splits u.*

Proof. As in the previous proof, this follows from Corollary 4.13 and Proposition 4.14. □

Lemma 10.7 (Induction Step)**.** *For every morphism of commutative rings, $u : R \to S$, for every decomposition $S = S_1 \times S_1'$ such that $u_1 : R \to S_1$ is faithfully flat and indecomposable, for every splitting extension $w : S_1 \to T$ of the S_1-algebra $S_1 \otimes_R S$, also the composition $v = w \circ u_1$ is a splitting extension for u. If w splits itself, then also v splits itself.*

Proof. Since $T \otimes_R S$ is naturally isomorphic to $T \otimes_{S_1} (S_1 \otimes_R S)$, if w splits the S_1-algebra $S_1 \otimes_R S$, then v splits u. Every composition of indecomposable, faithfully flat morphisms is indecomposable and faithfully flat, by Theorem 9.10. Thus v is indecomposable and faithfully flat.

For every morphism that splits u, say $\widetilde{v} : R \to \widetilde{T}$, also $\widetilde{v}$ splits the factor ring S_1. Thus there exists an R-algebra morphism, $\widetilde{w} : S_1 1 \to \widetilde{T}$. Since $\widetilde{T} \otimes_R S$ is naturally isomorphic to $\widetilde{T} \otimes_{S_1} (S_1 \otimes_R S)$, also $\widetilde{w}$ splits the S_1-algebra $S_1 \otimes_R S$. Since w is a splitting extension for this algebra, there exists a morphism of commutative rings, $f : T \to \widetilde{T}$, such that $f \circ w$ equals $\widetilde{w}$. Thus, also $\widetilde{v}$ equals $\widetilde{w} \circ u_1$ equals $(f \circ w) \circ u_1$ equals $f \circ (w \circ u_1)$ equals $f \circ v$. So v is a splitting extension of u.

If w splits itself, then the left T-algebra $T \otimes_{S_1} T$ is isomorphic to a product of copies of T, say $\prod_{i=1}^m T$. Since the morphism from S to T factors through the quotient S_1, also this is naturally

isomorphic to $T \otimes_S T$. Also the left T-algebra $T \otimes_{S_1} (S_1 \otimes_R S)$ is isomorphic to a product of copies of T, say $\prod_{j=1}^n T$. Then the left T-algebra $((T \otimes_{S_1} (S_1 \otimes_R S))) \otimes_S T$ is isomorphic as a left T-algebra to a product of n copies of $T \otimes_S T$, which is isomorphic as a left T-algebra to a product of mn copies of T. By associativity of tensor product, the left T-algebra $((T \otimes_{S_1} (S_1 \otimes_R S))) \otimes_S T$ is naturally isomorphic to $T \otimes_R T$. Thus the left T-algebra $T \otimes_R T$ is isomorphic to a product of mn copies of T. So v splits itself. □

Lemma 10.8 (Splittings are functorial in v)**.** *For every morphism of commutative rings, $u : R \to S$, for every morphism of commutative rings, $v : R \to T$, for every ring homomorphism, $w : T \to U$, if v splits u, then also $w \circ v$ splits u.*

Proof. IF $T \otimes_R S$ is isomorphic as a T-algebra to a product $\prod_{e \in \Sigma} T$, then also $U \otimes_R S \cong U \otimes_T (T \otimes_R S)$ is isomorphic as a U-algebra to $U \otimes_T \prod_{e \in \Sigma} T \cong \prod_{e \in \Sigma} (U \otimes_T T) \cong \prod_{e \in \Sigma} U$. □

Lemma 10.9 (Compatibility with subextensions)**.** *For every morphism of commutative rings, $u : R \to S$, for every morphism of commutative rings, $\widetilde{u} : R \to \widetilde{S}$, and for every morphism of commutative rings, $w : \widetilde{S} \to T$, the composition $v = w \circ \widetilde{u}$ splits u if and only if w splits the $\widetilde{S}$-algebra $\widetilde{S} \otimes_R S$. If both $\widetilde{u}$ and v are faithfully flat, respectively faithfully flat and indecomposable, then so is v.*

Proof. Since the T-algebra $T \otimes_{\widetilde{S}} (\widetilde{S} \otimes_R S)$ is naturally isomorphic to $T \otimes_R S$, one of these is isomorphic as a T-algebra to a finite product of copies of T if and only if the other one is isomorphic as a T-algebra to a finite product of copies of T. Faithful flatness is compatible with composition by Theorem 9.10. □

Corollary 10.10 (The morphism u factors v)**.** *For every faithfully flat morphism of commutative rings, $u : R \to S$, for every morphism of commutative rings, $v : R \to T$, the morphism v splits u if and only if there exists a morphism of commutative rings, $w : S \to T$, such that $w \circ u$ equals v and such that w splits the S-algebra $S \otimes_R S$, at least after passing to the nonzero factor rings in a finite decomposition of R.*

Proof. Suppose first that v splits u. By Lemma 10.5, after passing to the nonzero factor rings in a finite decomposition of R, there exists a canonical bijection of $\mathrm{Hom}_{R\text{-}\mathbf{Alg}}(S, T)$ with the set of idempotents in a decomposition of $T \otimes_R S$ as a product of copies of T. Of course if T is the zero ring, there is nothing to prove: take w to be the unique morphism of rings to the zero ring. Thus, assume that T is nonzero. Since S is faithfully flat over R, also $T \otimes_R S$ is faithfully flat over T. Thus, the index set for the product is nonempty, i.e., there exists an R-algebra morpism w from S to T. By Lemma 10.9, v splits u if and only if w splits the S-algebra $S \otimes_R S$. □

Corollary 10.11 (Splitting the complement)**.** *For every finite faithfully étale morphism of commutative rings, $u : R \to S$, for every morphism of commutative rings, $v : R \to T$, the morphism v*

splits u if and only if there exists a morphism of commutative rings, $w : S \to T$, such that $w \circ u$ equals v and such that w splits the S-algebra $S' = (S \otimes_R S) \cdot (1 - e)$ complementary to the factor $S = (S \otimes_R S) \cdot e$ (at least after passing to the nonzero factor rings in a finite decomposition of R).

Proof. By the previous result, v splits u if and only if there exists a morphism of commutative rings, $w : S \to T$, such that w splits $S \otimes_R S$ as an S-algebra. Since u is separable, the S-algebra $S \otimes_R S$ splits as $S \times S'$. Since the factor S is already split over S, the morphism w splits the S-algebra $S \otimes_R S$ if and only if w splits the S-algebra S'. □

Lemma 10.12 (Splitting subrings and quotient rings)**.** *For every morphism of commutative rings, $u : R \to S$, for every morphism of commutative rings, $v : R \to T$, that splits u, also v splits every R-subalgebra of S whose quotient R-module is projective. Also, v splits all quotient R-algebras of S that are projective as R-modules.*

Proof. For every R-subalgebra $\widetilde{R}$ of T such that $T/\widetilde{R}$ is a projective R-module, and for every $\widetilde{R}$-subalgebra $\widetilde{S}$ of T such that $T/\widetilde{S}$ is a projective R-module, since $T \otimes_R T$ is a product of copies of T as a T-algebra, also the T-subalgebras $T \otimes_R \widetilde{R}$ and $T \otimes_R \widetilde{S}$ are products of copies of T, by Corollary 4.13 and Proposition 4.14. Moreover these come from a partition of a set of primitive idempotents of $T \otimes_R T$ (as a T-algebra) together with a refinement of that partition.

In particular, since this can be checked after faithfully flat base change (by Proposition 9.12), $\widetilde{R}$ is finite faithfully étale over R. Since $R \to T$ is faithfully flat, also the base change $\widetilde{R} \to T \otimes_R \widetilde{R}$ is faithfully flat. Of course this factors as the composition $\widetilde{R} \to T$ followed by the T-algebra morphism $T \to T \otimes_R \widetilde{R}$. Since, as a T-algebra, $T \otimes_R \widetilde{R}$ is a direct product of finitely many copies of T, also as a T-module it is a direct sum of finitely many copies of T. As a direct summand of the projective $\widetilde{R}$-module, $T \otimes_R \widetilde{R}$, also T is a projective $\widetilde{R}$-module, i.e., $\widetilde{R} \to T$ is finite and faithfully flat. Since $R \to T$ is separable, also the base change $\widetilde{R} \to T \otimes_R \widetilde{R}$ is separable (by Theorem 9.10), so also the quotient $\widetilde{R}$-algebra T is separable. Altogether, $\widetilde{R} \to T$ is finite faithfully étale. For the same reason, also $\widetilde{R} \to \widetilde{S}$ and $\widetilde{S} \to T$ are finite faithfully étale.

Since $T \otimes_R \widetilde{S}$ is a T-subalgebra of the totally split T-algebra $T \otimes_R T \cong T^\Sigma$, and since the quotient of this T-subalgebra is projective, this T-subalgebra arises from a partition Π of Σ, at least after passing to the nonzero factor rings of a finite decomposition, by Proposition 4.14. As a quotient T-algebra that is also a projective T-module, also the quotient $T \otimes_{\widetilde{R}} \widetilde{S}$ of $T \otimes_R \widetilde{S}$ is a totally split T-algebra, by Corollary 4.13. Thus, the finite faithfully étale, indecomposable $\widetilde{R}$-algebra T also splits $\widetilde{R} \to \widetilde{S}$. □

Theorem 10.13 (Existence of splitting extensions)**.** *Let R be a nonzero commutative ring whose set $Idem(R)$ of idempotents is finite. For every morphism of commutative rings, $u : R \to S$, the morphism is finite étale if and only if there exists a faithfully flat morphism of rings, $v : R \to T$, that*

splits u. In this case, there exists a splitting extension $v : R \to T$ of u. Moreover, v is itself finite faithfully étale, and v splits itself. More generally, for every R-subalgebra $\widetilde{R}$ of T such that $T/\widetilde{R}$ is a projective R-module, for every $\widetilde{R}$-subalgebra $\widetilde{S}$ of T such that $T/\widetilde{S}$ is a projective R-module, also $\widetilde{R}$ is finite faithfully étale over R, $\widetilde{S}$ is finite faithfully étale over $\widetilde{R}$, T is finite faithfully étale over $\widetilde{S}$, and the $\widetilde{R}$-algebra T splits the $\widetilde{R}$-algebra $\widetilde{S}$. Finally, there exists a u-primitive decomposition of S, each factor is finite étale over R, and each factor is split by v.

Proof. By Lemma 10.4, if there exists a splitting extension v for u, then u is finite étale.

Next assume that u is finite étale. Up to passing to the nonzero factor rings in a finite decomposition of R, assume that S has constant rank n, for some nonnegative integer n. If n equals 0 or 1, then already $\mathrm{Id}_R : R \to R$ is a splitting extension for u. By way of induction, assume that n is greater than 1, and assume the theorem holds for smaller values of n.

First we prove that there exists a finite faithfully étale morphism that splits u. Then we construct a u-primitive decomposition of S. Finally we construct a splitting extension of u. Since n is strictly positive, the morphism u is faithfully flat. Since u is separable, the S-algebra $S \otimes_R S$ has a decomposition into $S \times S'$. Since the (left) S-module $S \otimes_R S$ is projective of constant rank $n > 1$, also the factor S' is a projective S-module of constant rank $n - 1$. Since S' is a quotient of the separable S-algebra $S \otimes_R S$, also S' is separable by Corollary 9.4. Thus, S' is a finite faithfully étale S-algebra. By the induction hypothesis, there exists a splitting extension $w' : S \to T'$ for the finite faithfully étale S-algebra S', i.e., $T' \otimes_S S'$ is isomorphic to a product of $n-1$ copies of T'. By Lemma 10.9 and Corollary 10.11, also the composition $v' = w' \circ u$ from R to T' is a faithfully flat morphism (typically not indecomposable) that splits u. By Lemma 10.7, the R-algebra T' splits itself. By Lemma 10.4 or by Theorem 9.10, also T' is separable over R. So T' is finite faithfully étale over R.

The issue is that T' is not necessarily indecomposable over R, since S is not necessarily indecomposable over R. But now we can use the splitting over T' to bound the idempotents in S, thus producing a u-decomposition of S that gives indecomposable factors. Let Σ be the set of n idempotents in $S \otimes_R T'$ that give the decomposition of $S \otimes_R T'$ as a T'-algebra. Denote by $\mathcal{P}(\Sigma)$ the subset of $\mathsf{Idem}(S \otimes_R T')$ of all sums of subsets of Σ (including 0 for the empty sum). For every idempotent e of R, consider the intersection of $\mathcal{P}(\Sigma) \cdot e$ with the image of $S \cdot e$. This is a finite subset whose inverse image in $\mathcal{P}(\Sigma)$ is a finite subset. There are only finitely many finite subsets of $\mathcal{P}(\Sigma)$. Since also there are only finitely many idempotents in R, there exists a finite decomposition of R such that this function is constant over every nonzero factor ring (e.g., the finite decomposition of all primitive idempotents in R has this property). Up to passing to such a nonzero factor ring, assume that this function is constant. Then the subset of $\mathcal{P}(\Sigma)$ is (the set of all subsets of) a partition of Σ. The partition subsets define idempotents in S that give a u-primitive u-decomposition of S.

Thus, also assume that there exists a decomposition of S into factor rings, each of which is finite faithfully étale and indecomposable over R.

Denote the u-primitive factorization of S by $S = S_1 \times \cdots \times S_r$. Up to passing to the nonzero factor rings in a finite decomposition of R, assume that each S_i is a finitely generated, projective R-module of constant positive rank n_i with $n_1 + \cdots + n_r = n$. Thus, each S_i is finite and faithfully flat over R. By Corollary 9.4, each S_i is also separable over R, i.e., each S_i is finite faithfully étale over R. As earlier, after base change to S_1, the complementary factor S_1' of the factor S_1 in the S_1-algebra $S_1 \otimes_R S$ is a finitely generated, projective S_1-module of rank $n-1$ strictly less than 1. By the induction hypothesis, there exists a splitting extension $w : S \to T$ for the finite faithfully étale S_1-algebra S_1'. Now by Lemma 10.7, the composition $v = w \circ u_1$ is a splitting extension for u that is finite faithfully étale over R and also splits itself. Thus, by induction on the rank, for every finite étale morphism u, there exists a splitting extension v for u that is finite faithfully étale and splits itself. The last part of the theorem follows from Lemma 10.12 □

Remark 10.14. The hypothesis that R has only finitely many idempotents is necessary for this proof, although there is a result for rings with infinitely many idempotents: O. E. Villamayor and D. Zelinsky, "Galois theory with infinitely many idempotents", *Nagoya Math. J.*, vol. 35 (1969), pp. 83 – 98. Here is an example inspired by that paper. Let R be the subring of $\prod_{n\in\mathbb{Z}_{\geq 0}} \mathbb{C}$ of all countable sequences $x = (x_n)_{n\in\mathbb{Z}_{\geq 0}}$ of complex numbers such that, for an integer n_0 (that depends on x), for all integers $n \geq n_0$, the values x_n are independent of n and equal an element of $\mathbb{R}$. Let S be $R[t]/(t^2+1)R[t]$. This is certainly not indecomposable. For every integer n there exists a surjective ring homomorphism $R \to R_n = \mathbb{C}$ that sends x to x_n. The base change $R_n \otimes_R S$ equals $\mathbb{C}[t]/(t^2+1)\mathbb{C}[t]$, which decomposes as $\mathbb{C}\cdot(1-i\bar{t})/2 \times \mathbb{C}\cdot(1+i\bar{t})/2$. Yet there is no S/R-decomposition that is R-indecomposable. Indeed, there is also the surjection $R \to R_\infty = \mathbb{R}$ that maps the sequence $(x_n)_{n\in\mathbb{Z}_{\geq 0}}$ to $\lim_{n\to\infty} x_n$, and the base change $R_\infty \otimes_R S$ equals $\mathbb{C}$, which is indecomposable over $\mathbb{R}$. So there does not exist any faithfully flat extension of R that splits S and that is indecomposable over R.

Remark 10.15. However, the hypothesis that $\mathrm{Idem}(R)$ is finite is satisfied in most applications, e.g., whenever R is a Noetherian ring. Moreover, even if R is not Noetherian, for every finite, finitely presented, flat, étale R-algebra S, by the *limit theorems* in EGA, there exists a finitely generated $\mathbb{Z}$-subalgebra R_0 of R, and a finite, finitely presented, flat, étale R_0-algebra S_0 such that S is isomorphic as an R-algebra to $R \otimes_{R_0} S_0$. Since R_0 is Noetherian, the hypothesis does hold for R_0.

11 Galois extensions

Definition 11.1. A commutative ring R is **Artinian** if (and only if) every decreasing chain of ideals in R stabilizes.

Proposition 11.2. *Every commutative ring R that is Artinian is also Noetherian. Moreover, a commutative ring R is Artinian if and only if it admits a finite decomposition such that every factor ring is a local Artinian ring. A local ring $(R, \mathfrak{m})$ is Artinian if and only if both $\mathfrak{m}^e$ equals $\{0\}$ for all sufficient positive integers e and $\mathfrak{m}/\mathfrak{m}^2$ has finite dimension as a vector space over the residue field $R/\mathfrak{m}$.*

Every local Artinian ring is a local Noetherian ring $(R, \mathfrak{m})$ that equals its own *completion*: the inverse limit of $R/\mathfrak{m}^{e+1}$ over all nonnegative integers. The structure of complete local Noetherian rings described by the Cohen structure theorem. However, for local Artinian rings that contain a field, the answer is much simpler.

Corollary 11.3. *For every field F, for every finite F-algebra S, there is a finite decomposition of F into a product of finite F-algebras, each of which is a local Artinian ring. These are precisely the finite F-algebras that are indecomposable. Each is of the form $E[t_1, \ldots, t_n]/I$ for a finite field extension $F \to E$, for a (finite) nonnegative integer n, and for an ideal $I = \langle g_1(t_1, \ldots, t_n), \ldots, g_r(t_1, \ldots, t_n)\rangle$ contained in $\langle t_1, \ldots, t_n\rangle$ such that $\langle t_1, \ldots, t_n\rangle^e$ is contained in I for all sufficiently positive integers e (if n equals 0, this is just E).*

Now let E be a field and consider the E-algebra $E[t]/\langle t^2\rangle$. This certainly is a finite faithfully flat E-algebra.

Lemma 11.4. *For every nonzero commutative ring R, the R-algebra $R[t]/\langle t^2\rangle$ is not separable. Thus, for every finite faithfully flat R-algebra S that admits a surjective R-algebra morphism to $R[t]/\langle t^2\rangle$, also the R-algebra S is not separable.*

Proof. Consider the tensor product R-algebra $(R[t]/\langle t^2\rangle) \otimes_R (R[t]/\langle t^2\rangle)$ with its product morphism to $R[t]/\langle t^2\rangle$. Denoting $\bar{t} \otimes 1$ by x and $1 \otimes \bar{t}$ by y, this R-algebra is also $R[x, y]/\langle x^2, y^2\rangle$ with the R-algebra morphism to $R[t]/\langle t^2\rangle$ that sends each of x and y to t. Thus, every element in the fiber over 1 is of the form $1 + ax + by + cxy$ for unique elements a, b, c of R. The product of this element with the element $x - y$ in the kernel is $x - y + (b - a)xy$, which is not zero since the coefficients of x and y do not equal 0. Since there is no separable idempotent, i.e., the R-algebra $R[t]/\langle t^2\rangle$ is not separable. □

Proposition 11.5. *For every field F, the finite F-algebras that are separable are precisely the finite products of finite separable field extensions $F \to E$.*

Proof. As proved in the theorem, if $F \to S$ is finite separable, and $\widetilde{R}$ is an F-subalgebra of S such that $S/\widetilde{R}$ is a projective F-module, then also $F \to \widetilde{R}$ and $\widetilde{R} \to S$ are finite separable. Of course every F-module (i.e., F-vector space) is projective. Hence, for every F-subalgebra $\widetilde{R}$ of S, also $\widetilde{R} \to S$ is finite separable.

By the structure theorem, every finite F-algebra is a product of finite F-algebras that are local and Artinian of the form $S = E[t_1, \ldots, t_n]/I$, where $F \to E$ is a finite field extension, where n is a nonnegative integer, and where I is an ideal contained in $\langle t_1, \ldots, t_n \rangle$ that contains $\langle t_1, \ldots, t_n \rangle^e$ for some positive integer e.

Since E is a quotient F-algebra of S, if S is a finite separable F-algebra, then $F \to E$ is finite and separable. By the first paragraph, if S is a finite separable F-algebra, also S is a finite separable F-algebra. Altogether, S is a finite separable F-algebra if and only if both $F \to E$ is finite separable and $E \to S$ is finite separable.

Of course $E \to S$ is an isomorphism if and only if I equals $\langle t_1, \ldots, t_n \rangle$. By way of contradiction, assume that it is not. Let d be the largest positive integer such that $\langle t_1, \ldots, t_n \rangle^e$ is not contained in I, and let t be an element of $\langle t_1, \ldots, t_n \rangle^e$ that is not contained in I. Then the induced E-algebra homomorphism from $E[t]$ to S factors through an injective E-algebra homomorphism from $E[t]/\langle t^2 \rangle$ to S. The quotient is an E-vector space, hence it is projective. Thus, also $E[t]/\langle t^2 \rangle$ is a separable E-algebra. But that contradicts the lemma. Therefore, by contradiction, if S is separable over F, also I equals $\langle t_1, \ldots, t_n \rangle$, i.e., the E-algebra homomorphism $E \to S$ is an isomorphism. Altogether, a finite F-algebra is separable over F if and only if it is a product of finitely many finite separable field extensions of F. □

Definition 11.6. For every field F, for every (nonzero and noninvertible) irreducible monic polynomial $m(t)$ in the polynomial F-algebra $F[t]$, the element $m(t)$ is a **separably irreducible** monic polynomial if (and only if) the finite field extension $E = F[t]/m(t)F[t]$ of F is separable. More generally, a squarefree monic polynomial $m(t)$ is **separable** if (and only if) the finite flat F-algebra $E = F[t]/m(t)F[t]$ is separable.

Lemma 11.7. *For every field F, for every (nonzero and noninvertible) irreducible monic polynomial $m(t)$ in $F[t]$, the element $m(t)$ is separably irreducible if the formal derivative $m'(t)$ is nonzero. In particular, both $m'(t)$ is nonzero and $m(t)$ is separably irreducible unless the characteristic of F is $p > 0$, there exists a positive integer r, and there exists a (nonzero and noninvertible) irreducible monic polynomial $g(t)$ such that $m(t)$ equals $g(t^{p^r})$. Moreover, there exists a unique such r and $g(t)$ for which $g'(t)$ is nonzero (hence $g(t)$ is separably irreducible).*

Proof. Since $m(t)$ is irreducible, and since $m'(t)$ has strictly smaller degree than $f(t)$, the element $m'(t)$ is zero if and only if $m'(t)$ is a multiple of $m(t)$, i.e., $m'(t)$ is nonzero if and only if $m'(t)$ is relatively prime to $m(t)$. By the Euclidean Algorithm (or the corollary that $F[t]$ is a principal

ideal domain), $m'(t)$ is relatively prime to $m(t)$ if and only if there exist elements $r(t), s(t) \in F[t]$ such that

$$1 = s(t)m(t) + r(t)m'(t).$$

Inside $F[t,u]$, note that $m(t) - m(u)$ equals $(t-u)(m'(t) + (t-u)h(t,u))$ for some unique $h(t,u) \in F[t,u]$. Also, the kernel of $\beta_{E/F}$ in the F-algebra $E \otimes_F E = F[t,u]/\langle m(t), m(u)$ is a principal ideal generated by (the image of) $t-u$. Thus, the element $\epsilon(t,u) := \text{Image}(r(t)m'(t) + (t-u)r(t)h(t,u))$ in $E \otimes_F E$ maps under $\beta_{F/E}$ to the image of $r(t)m'(t)$, which is congruent to 1 module $m(t)$. Moreover,

$$(t-u)\cdot\epsilon(t,u) = \text{Image}\left(r(t)\cdot((t-u)(m'(t) + (t-u)h(t,u)))\right),$$

which is congruent to the image of $r(t)(m(t) - m(u))$. Since both $m(t)$ and $m(u)$ map to 0 in $E \otimes_F E$, it follows that $\epsilon(t,u)$ is annihilated by the kernel of $\beta_{F/E}$. In particular, since $1 - \epsilon(t,u)$ is in the kernel of $\beta_{F/E}$, notice that $\epsilon(t,u)\cdot(1-\epsilon(t,u))$ equals 0, i.e., $\epsilon(t,u)$ is an idempotent element.

Of course for every (nonzero and noninvertible) monic polynomial $m(t)$, say $m(t) = t^n + c_1t^{n-1} + \cdots + c_{n-1}t + c_n$, also the formal derivative equals $nt^{n-1} + (n-1)c_1t^{n-1} + \cdots + 1\cdot c_{n-1}$. Notice that this is nonzero if F has characteristic 0, since then nt^{n-1} is nonzero. If F has characteristic $p > 0$, this is nonzero unless n equals pm for some positive integer m, and c_ℓ equals 0 except if $\ell = pk$ for some positive integer k. Then $g(t) := t^m + \sum_{k=0}^{m-1} c_{pm}t^{m-k}$ is the unique polynomial in $F[t]$ such that $g(t^p)$ equals $m(t)$. Since $m(t)$ is irreducible, also $g(t)$ is irreducible. Iterating and using induction, there exists a unique positive integer r and a unique separably irreducible monic polynomial $g(t)$ such that $m(t)$ equals $g(t^{p^r})$. □

Next assume that $m(t)$ is a monic, irreducible polynomial in $F[t]$, so that $E = F[t]/m(t)F[t]$ is a finite field extension of F. If the characteristic of F equals $p > 0$, then there exists a unique nonnegative integer r (possibly r equals zero) and a unique monic polynomial $m_{(r)}(t)$ in $F[t]$ such that $m'_{(r)}(t)$ is nonzero and $m(t) = m_{(r)}(t^{p^r})$. Since $m(t)$ is irreducible, also $m_{(r)}(t)$ is irreducible, hence $m_{(r)}(t)$ is a separable irreducible polynomial.

Proposition 11.8 (Separable polynomials)**.** *For every field F, for every monic, irreducible polynomial $m(t)$ in $F[t]$, the corresponding F-extension $E = F[t]/\langle m(t)\rangle$ is a separable field extension of F if and only if the F-algebra $E \otimes_F E$ has only the zero nilpotent element if and only if the integer r above equals zero if and only if the formal derivative $m'(t)$ is nonzero if and only if the formal derivative $m'(t)$ is relatively prime to $m(t)$.*

Proof. By straightforward computation, $m'(t)$ equals zero if and only if $m(t)$ equals $m_{(r)}(t^{p^r})$ for positive integer r. Since $m_{(r)}(t)$ is a separable irreducible polynomial in $F[t]$, for every root x of $m(t)$ in E (i.e., for $x = \bar{t}$), also the element $y = x^{p^r}$ is a root of $m_{(r)}(t)$ in E. Let L be the F-subextension $F[y]$. Then L is separable over F. However, the minimal polynomial over L of the

element $z = x^{p^{r-1}}$ is $t^p - y$, and this is inseparable. In particular, for $K = L[z] \cong L[t]/\langle t^p - y$, we have $K \otimes_L K$ is isomorphic as a K-algebra to $K[t]/\langle t^p - y\rangle = K[t]/\langle (t-z)^p\rangle$. This contains the nonzero nilpotent element $\bar{t} - z$. So K/L is not separable. Since this is a subextension of E/F, also E/F is not separable. Altogether, if $m'(t)$ equals zero, then E/F is not separable.

As proved earlier, if $m'(t)$ is nonzero, then $m'(t)$ is relatively prime to $m(t)$, and then E/F is separable. Therefore E/F is separable if and only if the monic, irreducible polynomial $m(t)$ is separable, i.e., $m'(t)$ is relatively prime to $m(t)$. □

Corollary 11.9. *For every field F, for every monic, squarefree polynomial $m(t)$ in $F[t]$, the corresponding (finite, finitely presented, faithfully flat) F-algebra $E = F[t]/\langle m(t)\rangle$ is separable over F if and only if the F-algebra $E \otimes_F E$ has only the zero nilpotent element if and only if the formal derivative $m'(t)$ is relatively prime to $m(t)$. If $m(t)$ is not squarefree, then $F[t]/\langle m(t)\rangle$ has nonzero nilpotent elements, hence it is not separable over F.*

Proof. Of course if $m(t) = h(t)g(t)^2$ for a monic, irreducible polynomial $g(t)$ in $F[t]$, then the image of $h(t)g(t)$ in $F[t]/\langle m(t)\rangle$ is nonzero, but the square is zero. So $F[t]/\langle m(t)\rangle$ has nilpotent elements, hence it is not separable over F. Thus, $F[t]/\langle m(t)\rangle$ can only be separable if the factorization of $m(t)$ into monic, irreducible factors is $m(t) = g_1(t)\cdots g_m(t)$ for pairwise distinct, monic, irreducible polynomial $g_i(t)$ in $F[t]$. In this case, the corollary follows from the previous result and the Chinese Remainder Theorem. □

Definition 11.10. A finite separable field extension, $v : F \to E$, is **Galois** if (and only if) v is a splitting field of itself.

Corollary 11.11 (Existence of splitting fields)**.** *For every finite separable field extension, $u : F \to L$, there exists a splitting field, $v : F \to E$. For every F-subextension $\widetilde{F}$ of E, and for every $\widetilde{F}$-subextension $\widetilde{L}$ of E, also $E/\widetilde{F}$ splits $\widetilde{L}/\widetilde{F}$. In particular, choosing $\widetilde{F}$ to equal F and choosing $\widetilde{L}$ to equal E, v is a splitting field for itself, i.e., E/F is a Galois extension.*

Proof. This is just the reformulation of Theorem 10.13 in the case of field extensions. □

Corollary 11.12. *For every finite separable field extension, $u : F \to L$, for every field extension, $v : F \to E$, that splits u, the natural E-algebra homomorphism $E \otimes_F L \to E^{\mathsf{Hom}_{F-\mathbf{Alg}}(L,E)}$ is an isomorphism. In particular, the set $\mathsf{Hom}_{F-\mathbf{Alg}}(L, E)$ is a finite set of cardinality equal to $[L : F]$.*

Proof. By adjointness of tensor and Hom, the natural map from $\mathsf{Hom}_{F-\mathbf{Alg}}(L, E)$ to $\mathsf{Hom}_{E-\mathbf{Alg}}(E \otimes_F L, E)$ is a bijection. Since $E \otimes_F L$ is isomorphic as an E-algebra to E^Σ for a finite set Σ, every E-algebra homomorphism from E^Σ to E is projection from E^Σ to $E^\Sigma \cdot \delta_\sigma = E$ for an element σ of Σ and the corresponding idempotent δ_σ. This defines a natural bijection of Σ with $\mathsf{Hom}_{F-\mathbf{Alg}}(L, E)$. In particular, the size of $\mathsf{Hom}_{F-\mathbf{Alg}}(L, E)$ equals the dimension of $E \otimes_F L$ as an E-vector space, and this equals the dimension of L as an F-vector space. □

Corollary 11.13 (Sizes of Galois groups of finite Galois extensions)**.** *For every finite Galois field extension, $v : F \to E$, there is a natural E-algebra isomorphism $E \otimes_F E \to E^{\mathsf{Aut}_F(E)}$. In particular, $\mathsf{Aut}_F(E)$ is a finite group whose cardinality equals $[E : F]$.*

Proof. Every F-algebra homomorphism from E to E is injective, thus also surjective by the Rank-Nullity Theorem. Therefore $\mathsf{Hom}_{F-\mathbf{Alg}}(E, E)$ equals the group $\mathsf{Aut}_F(E)$ of all F-algebra automorphisms of E. Now the result holds by the previous corollary. □

Corollary 11.14 (Fixed fields of Galois groups)**.** *For every finite, Galois extension of fields, $v : F \to E$, the degree $[E : F]$ equals the cardinality of $\mathsf{Aut}_F(E)$, and the fixed subfield of $\mathsf{Aut}_F(E)$ equals F. Thus, for every F-subextension L of E, also the fixed subfield of $\mathsf{Aut}_L(E)$ equals L.*

Proof. We already proved that $\mathsf{Aut}_F(E)$ is a finite group whose cardinality equals $[E : F]$. For the fixed subfield L of the finite group $\mathsf{Aut}_F(E)$, also E/L is finite and Galois. Thus, $\mathsf{Aut}_F(E)$ equals $\mathsf{Aut}_L(E)$ is a finite group with cardinality $[E : L]$. Since $[E : F]$ equals $[E : L]$, also $[L : F]$ equals 1, i.e., the F-algebra homomorphism $F \hookrightarrow L$ is an isomorphism. Therefore the fixed field of $\mathsf{Aut}_F(E)$ equals F.

Since E is also finite, Galois over every F-subextension L of E, also the fixed field of $\mathsf{Aut}_L(E)$ equals L. □

Corollary 11.15 (Transitivity of Galois actions)**.** *For every finite Galois extension, $v : F \to E$, for every F subextension, $F \xrightarrow{u} L \xrightarrow{w} E$, the action of $\mathsf{Aut}_F(E)$ on the set $\mathsf{Hom}_{F-\mathbf{Alg}}(L, E)$ by postcomposition is transitive with orbit of size $[L : F]$, and the stabilizer of w equals $\mathsf{Aut}_{u(L)}(E)$.*

Proof. Since u is a subextension of v, also v splits u. Thus, the E-algebra $E \otimes_F L$ is isomorphic to $\prod_{w \in \Sigma} E$. The set Σ is naturally bijective with $\mathsf{Hom}_{E-\mathbf{Alg}}(E \otimes_F L, E)$, by Corollary 4.13. By adjointness of tensor and Hom, this set is naturally bijective with $\mathsf{Hom}_{F-\mathbf{Alg}}(L, E)$. Since the dimension of the E-vector space $E \otimes_F L$ equals the cardinality of Σ, and since this also equals the dimension of the F-vector space L, the set $\mathsf{Hom}_{F-\mathbf{Alg}}(L, E)$ has cardinality $[E : L]$.

By definition, the stabilizer of the action on the element w equals $\mathsf{Aut}_{u(L)}(E)$. By the previous result, this stabilizer subgroup of $\mathsf{Aut}_F(E)$ has cardinality $[E : u(L)]$. Therefore the orbit of w under the action has size equal to the index of this subgroup, $\#\mathsf{Aut}_F(E)/\#\mathsf{Aut}_{u(L)}(E)$. This equals $[E : F]/[E : u(L)]$, i.e., $[u(L) : F]$, which is the size of the entire set $\mathsf{Hom}_{F-\mathbf{Alg}}(L, E)$. Therefore the action of $\mathsf{Aut}_F(E)$ on $\mathsf{Hom}_{F-\mathbf{Alg}}(L, E)$ is transitive. □

Corollary 11.16 (Galois extensions split their minimal polynomials)**.** *For every finite Galois extension, $v : F \to E$, for every element x of E, the minimum polynomial $m_x^F(t)$ in $F[t]$ of x factors in $E[t]$ as $\prod_{y \in \Sigma}(t - y)$, i.e., it has d pairwise distinct roots in E, where d is the degree of $m_x^F(t)$. The group $\mathsf{Aut}_F(E)$ acts transitively on the set of roots.*

Proof. By definition, the F-subextension $L = F[x]$ is isomorphic to $F[t]/\langle m_x^F(t)\rangle$. Thus, the F-algebra homomorphisms are the same as roots of $m_x^F(t)$ in E, by the universal property of the F-algebra $F[t]/\langle m_x^F(t)$. By the previous result, this set has size $[L:F] = d$, and the group $\mathsf{Aut}_F(E)$ acts transitively on this set. □

Proposition 11.17 (Extension of field automorphisms for finite Galois extensions)**.** *For every finite Galois field extension, $v : F \to E$, for every F-subextension, $F \xrightarrow{u} L \xrightarrow{w} E$, the extension u is Galois if and only if L splits the minimum polynomial of each of its elements if and only if every element of $Aut_F(E)$ maps L to itself if and only if $\mathsf{Aut}_F(L)$ has size $[L:F]$. In this case, every F-automorphism of E maps L to itself, so that there is a well-defined restriction group homomorphism, $(\cdot)|_L : \mathsf{Aut}_F(E) \to \mathsf{Aut}_F(L)$. This group homomorphism is surjective, and the kernel is $\mathsf{Aut}_L(E)$. Thus the subgroup $\mathsf{Aut}_L(E)$ of $\mathsf{Aut}_F(E)$ is normal.*

Proof. By the previous result, if L/F is Galois, then L splits the minimum polynomial $m_x^F(t)$ of x for every element x of L. Since $\mathrm{Aut}_F(E)$ transitive permutes the roots of $m_x^F(t)$, if L contains all the roots of $m_x^F(t)$ for every element x of L, then every element of $\mathrm{Aut}_F(E)$ maps every element x of L to an element of L, i.e., $\mathrm{Aut}_F(E)$ maps L back to itself. Finally, if $\mathrm{Aut}_F(E)$ maps L back to itself, then there is a restriction homomorphism from $\mathrm{Aut}_F(E)$ to $\mathrm{Aut}_F(L)$. The kernel of this homomorphism is $\mathrm{Aut}_L(E)$, which has index $[L:F]$ in $\mathrm{Aut}_F(E)$. Thus, the image of the restriction homomorphism has order $[L:F]$. So $\mathsf{Aut}_F(L)$ has order at least $[L:F]$. The image of the natural L-algebra homomorphism ϕ from $L \otimes_F L$ to $\prod_{\sigma\in\mathsf{Aut}_F(L)} L$ is an algebra of set functions L^Σ for a partition of $\mathsf{Aut}_F(L)$ by Corollary 4.13. For elements σ and τ of $\mathsf{Aut}_F(L)$ in the same partition set, the compositions from $L \otimes_F L$ to $\prod_{\mathsf{Aut}_F(L)} L$ followed by the projection of σ, resp. τ to L are equal. These compositions are σ, resp. τ, by the definition of ϕ. So if σ is different from τ, they are not in the same partition set. Thus ϕ is surjective. So the size of $\mathsf{Aut}_F(L)$, i.e., the L-dimension of the image of ϕ, is less than or equal to the L-dimension of $L \otimes_F L$, i.e., less than or equal to $[L:F]$. Since the image of the restriction homomorphism has size equal to $[L:F]$, it follows that $\#\mathrm{Aut}_F(L)$ equals $[L:F]$ and ϕ is an isomorphism. Thus, u splits itself, i.e., u is a finite Galois extension. □

Definition 11.18. An algebraic field extension, $v : F \to E$, is **Galois** if and only if E equals the union of its finite F-subextensions that are Galois, i.e., every element x of E is contained in a subextension L of E that is finite Galois over F. The **set of finite Galois subextensions** of E/F is the subset $\mathsf{Gal}(E/F)$ of the power set $\mathcal{P}(E)$ whose elements are F-subextensions L of E that are finite, Galois over F. This set is partially ordered by set inclusion. For all F-subextensions $F \subseteq L \subseteq K \subseteq E$ of E with both L and K finite, Galois extensions of F, the **restriction homomorphism** is the surjective group homomorphism res_L^K from $\mathsf{Aut}_F(K)$ to $\mathsf{Aut}_F(L)$ that restricts each F-algebra automorphism of K to the associated F-algebra automorphism of L.

Corollary 11.19. *For every algebraic field extension, $v : F \to E$, that is Galois, the system $((\mathsf{Aut}_F(L))_{L\in\mathsf{Gal}(E/F)}, (\mathsf{res}^K_L)_{(L,K)\in\mathsf{Gal}(E/F)^2, L\subseteq K})$ is a compatible family of groups and group homomorphisms. For every F-subextension $F \xrightarrow{u} L \xrightarrow{w} E$, also w is Galois. If F is an element of $\mathsf{Gal}(E/F)$, then every element of $\mathsf{Aut}_F(E)$ maps L to itself, and the restriction homomorphism res^E_L from $\mathsf{Aut}_F(E)$ to $\mathsf{Aut}_F(L)$ is surjective with kernel equal to $\mathsf{Aut}_L(E)$. For every pair $F \subseteq L \subseteq K \subseteq E$ of F-subextensions of E such that both L and K are finite, Galois over F, also $\mathsf{res}^K_L \circ \mathsf{rest}^E_K$ equals res^E_L. Thus, the system of group homomorphisms $(\mathsf{res}^E_L)_{L\in\mathsf{Gal}(E/F)}$ factors uniquely through a group homomorphism from $\mathsf{Aut}_F(E)$ to the inverse limit over elements L of $\mathsf{Gal}(E/F)$ of $\mathsf{Aut}_F(L)$. This group homomorphism is an isomorphism from $Aut_F(E)$ to the inverse limit.*

Proof. For F-subextensions, $F \subseteq L \subseteq K \subseteq J \subseteq E$ with each of L, K and J a finite, Galois extension of F, restriction res^J_L of an F-algebra automorphism from J to L equals the composition of restrictions, $\mathrm{res}^K_L \circ \mathrm{rest}^J_K$. Thus, this is a compatible family.

For every element x of E, there exists an F-subextension K of E that is finite Galois over F and that contains x as an element. Thus, for every F-subextension $F \subseteq L \subseteq E$ such that L is finite over F, also the image in E of the natural homomorphism $L \otimes_F K \to E$ is finite Galois over L and contains x as an element. Thus E is also Galois over L.

Since E is the union of all of it F-subextensions L that are finite, Galois over F, every F-algebra automorphism σ of E is uniquely determined by all of its restrictions $\sigma|_L$. Thus, the homomorphism from E to the inverse limit is injective. On the other hand, let $(\sigma_L)_{L\in\mathsf{Gal}(E/F)}$ be a compatible family of F-algebra automorphisms σ_L of L for each F-subextension L of E that is finite, Galois over F. For every pair K and L of F-subextensions of E that are finite, Galois over F, the image J of the natural F-algebra homomorphism $K \otimes_F L \to E$ is also an F-subextension that is finite, Galois over F. Thus, both σ_L and σ_K equal $\mathrm{res}^J_L(\sigma_J)$ and $\mathrm{res}^J_K(\sigma_J)$. In particular, the restrictions of both σ_K and σ_L to $L \cap K$ equal the restriction of σ_J to $L \cap K$. Since, for every pair (K, L) in $\mathsf{Gal}(E/F)^2$ the restrictions of both σ_K and σ_L to $K \cap L$ agree, there is a unique function σ_E from E to itself such that, for every element L of $\mathsf{Gal}(E/F)$, the function σ_E maps L to itself and $\mathsf{res}^E_L(\sigma_E)$ equals σ_L.

For every pair (x, y) of elements of E, there exists a pair (K, L) of elements of $\mathsf{Gal}(E/F)$ such that x is an element of K and y is an element of L. But then $x + y$ and $x \cdot y$ are elements of J. Since σ_J is an F-algebra automorphism of J, both $\sigma_J(x + y)$ equals $\sigma_J(x) + \sigma_J(y)$ and $\sigma_J(x \cdot y)$ equals $\sigma_J(x) \cdot \sigma_J(y)$. Thus, also $\sigma(x+y) = \sigma(x)+\sigma(y)$ and $\sigma(x\cdot y)$ equals $\sigma(x)\cdot\sigma(y)$. So σ is an F-algebra automorphism of E. Altogether, it follows that the group homomorphism from $\mathsf{Aut}_F(E)$ to the inverse limit over all element L of $\mathsf{Gal}(E/F)$ of $\mathsf{Aut}_F(L)$ is an isomorphism.

For every element L in $\mathsf{Gal}(E/F)$, for every element K in $\mathsf{Gal}(E/F)$ such that L is an F-subextension of K, also res^L_K is surjective. Thus, by the Axiom of Choice, for every element σ_L in $\mathsf{Aut}_F(L)$, there exists a system $(\sigma_K)_{K\in\mathsf{Aut}_F(K)}$ in the inverse limit extending σ_L. Therefore the restriction homomorphism res^E_L is surjective with kernel equal to $\mathsf{Aut}_L(E)$. □

12 Automorphism groups and fixed subrings

Historically, *invariant theory* was one of the main motivations for the development of Noetherian rings. Both invariant theory and Galois theory have to do with the fixed subring of a collection of automorphisms.

Definition 12.1. For every morphism of commutative rings, $u : R \to S$, for every subset Σ of the group $\mathsf{Aut}_{R\text{-}\mathbf{Mod}}(S) \subset \mathsf{Hom}_{R\text{-}\mathbf{Mod}}(S)$ of all R-algebra automorphisms of S, the **fixed R-subalgebra** of Σ is the R-subalgebra $\mathsf{Fix}^{\Sigma}(S)$ of S consisting of all elements s in S such that $\sigma(s) = s$ for all elements σ in Σ. Similarly, for every subset Θ of S, the **stabilizer subgroup** of θ equals the subgroup $\mathsf{Aut}_{\Theta}(S)$ of $\mathsf{Aut}_{R\text{-}\mathbf{Alg}}(S)$ fo all elements σ in $\mathsf{Aut}_{R\text{-}\mathbf{Alg}}(S)$ such that $\sigma(s) = s$ for all elements s in Θ. In particular, for every R-subalgebra T of S, this equals the subgroup $\mathsf{Aut}_{T\text{-}\mathbf{Alg}}(S)$ of $\mathsf{Aut}_{R\text{-}\mathbf{Alg}}(S)$.

Proposition 12.2 (The fixed ring is an order reversing lattice map)**.** *For every morphism of commutative rings, $u : R \to S$, all of the following hold.*

(i) For every subset Σ of $\mathsf{Aut}_{R\text{-}\mathbf{Alg}}(S)$, the R-subalgbra $\mathsf{Fix}^{\Sigma}(S)$ equals $\mathsf{Fix}^{\langle\Sigma\rangle}(S)$, for the subgroup $\langle\Sigma\rangle$ of $\mathsf{Aut}_{R\text{-}\mathbf{Alg}}(S)$ generated by Σ.

(ii) The R-subalgebra $\mathsf{Fix}^{\{Id_S\}}(S)$ equals S.

(iii) For all subsets $\Sigma \subseteq \widetilde{\Sigma} \subseteq \mathsf{Aut}_{R\text{-}\mathbf{Alg}}(S)$, also $\mathsf{Fix}^{\widetilde{\Sigma}}(S)$ is an R-subalgebra of $\mathsf{Fix}^{\Sigma}(S)$.

(iv) For every subset I of $\mathcal{P}(\mathsf{Aut}_{R\text{-}\mathbf{Alg}}(S))$, for the union subset $\cup I$ of $\mathsf{Aut}_{R\text{-}\mathbf{Alg}}(S)$, the R-subalgebra $\mathsf{Fix}^{\cup I}(S)$ equals $\cap_{\Sigma\in I}\mathsf{Fix}^{\Sigma}(S)$.

(v) For every subset Σ of $\mathsf{Aut}_{R\text{-}\mathbf{Mod}}(S)$, for the R-subalgebra $T = \mathsf{Fix}^{\Sigma}(S)$, the subset $\mathsf{Aut}_{T\text{-}\mathbf{Alg}}(S)$ contains Σ.

(vi) For every subset Σ of $\mathsf{Aut}_{R\text{-}\mathbf{Mod}}(S)$, for every element σ of $\mathsf{Aut}_{R\text{-}\mathbf{Mod}}(S)$, the R-subalgebra $\sigma(\mathsf{Fix}^{\Sigma}(S))$ equals $\mathsf{Fix}^{\sigma\cdot\Sigma\cdot\sigma^{-1}}(S)$.

Proof. **(i)** Since Σ is a subset of the subgroup $\langle\Sigma\rangle$, the R-subalgebra $\mathsf{Fix}^{\langle\Sigma\rangle}(S)$ is an R-subalgebra of $\mathsf{Fix}^{\Sigma}(S)$. On the other hand, since every element σ of Σ fixes the R-subalgebra $T := \mathsf{Fix}^{\Sigma}(S)$, the subgroup $\mathsf{Aut}_{T\text{-}\mathbf{Alg}}(S)$ of $\mathsf{Aut}_{R\text{-}\mathbf{Alg}}(S)$ contains Σ. Thus, it contains the subgroup $\langle\Sigma\rangle$ generated by Σ. Since $\langle\Sigma\rangle$ is a subgroup of $\mathsf{Aut}_{T\text{-}\mathbf{Alg}}(S)$, also T is an R-subalgebra of $\mathsf{Fix}^{\langle\Sigma\rangle}(S)$, i.e., $\mathsf{Fix}^{\Sigma}(S)$ equals $\mathsf{Fix}^{\langle\Sigma\rangle}(S)$.

(ii) The identity automorphism of S fixes all of S.

(iii) For every element s of $\mathsf{Fix}^{\widetilde{\Sigma}}(S)$, since s is fixed by all of $\widetilde{\Sigma}$, in particular it is fixed by the subset Σ. Thus, $\mathsf{Fix}^{\widetilde{\Sigma}}(S)$ is an R-subalgebra of $\mathsf{Fix}^{\Sigma}(S)$.

(iv) An element s of S is fixed by every element in every subset Σ of $\mathsf{Aut}_{R\text{-}\mathbf{Alg}}(S)$ that is an element of I if and only if s is in the fixed set $\mathsf{Fix}^{\Sigma}(S)$ for every element Σ of I. Thus $\mathsf{Fix}^{\cup I}(S)$ equals $\cap_{\Sigma\in I}\mathsf{Fix}^{\Sigma}(S)$.

(v) Since $T = \mathsf{Fix}^{\Sigma}(S)$ is fixed by Σ, also Σ is in the subgroup $\mathsf{Aut}_{T\text{-}\mathbf{Alg}}(S)$ of automorphisms of S that fix T.

(vi) For every element s of S, for every element σ' of $\mathsf{Aut}_{R\text{-}\mathbf{Alg}}(S)$, for the element $s' = \sigma^{-1}(s)$, we have $\sigma'(s')$ equals s' if and only if $\sigma\cdot\sigma'\cdot\sigma^{-1}(s)$ equals s. Thus, s is an element of $\sigma(\mathsf{Fix}^{\Sigma}(S))$ if and only if s is an element of $\mathsf{Fix}^{\sigma\cdot\Sigma\cdot\sigma^{-1}}(S)$. □

Proposition 12.3 (The automorphism group is an order reversing lattice map)**.** *For every morphism of commutative rings, $u : R \to S$, all of the following hold.*

(i) For every subset Θ of S, the subgroup $\mathsf{Aut}_{\Theta}(S)$ equals $\mathsf{Aut}_{T\text{-}\mathbf{Alg}}(S)$ for the R-subalgebra $T = R[\Theta]$ of S generated by Θ.

(ii) The subgroup $\mathsf{Aut}_{R\text{-}\mathbf{Alg}}(S)$ equals all of $\mathsf{Aut}_{R\text{-}\mathbf{Alg}}(S)$, and $\mathsf{Aut}_{S\text{-}\mathbf{Alg}}(S)$ equals $\{Id_S\}$.

(iii) For all R-subalgebras $T \subseteq \widetilde{T} \subseteq S$, also $\mathsf{Aut}_{\widetilde{T}\text{-}\mathbf{Alg}}(S)$ is a subgroup of $\mathsf{Aut}_{T\text{-}\mathbf{Alg}}(S)$.

(iv) For every subset J of $\mathcal{P}(S)$, for the union subset $\cup J$ of S, the subgroup $\mathsf{Aut}_{\cup J}(S)$ equals $\cap_{\Theta\in J}\mathsf{Aut}_{\Theta}(S)$.

(v) For every R-subalgebra T of S, for the subgroup $\Sigma = \mathsf{Aut}_{T\text{-}\mathbf{Alg}}(S)$, the R-subalgebra $\mathsf{Fix}^{\Sigma}(S)$ contains T.

(vi) For every R-subalgebra T of S, for every element σ of $\mathsf{Aut}_{T\text{-}\mathbf{Alg}}(S)$, the subgroup $\mathsf{Aut}_{\sigma(T)\text{-}\mathbf{Alg}}(S)$ equals $\sigma\cdot\mathsf{Aut}_{T\text{-}\mathbf{Alg}}(S)\cdot\sigma^{-1}$.

Proof. **(i)** For every element σ of $\mathsf{Aut}_R(S)$ that fixes $R[\Theta]$, it also fixes the subset Θ. Therefore, $\mathsf{Aut}_{T\text{-}\mathbf{Alg}}(S)$ is a subgroup of $\mathsf{Aut}_{\Theta}(S)$. On the other hand, if σ fixes Θ, then since σ is an R-algebra homomorphism, the fixed locus of σ is an R-subalgebra of S that contains Θ. Hence the fixed locus contains $R[\Theta]$. So, also $\mathsf{Aut}_{T\text{-}\mathbf{Alg}}(S)$ equals $\mathsf{Aut}_{\Theta}(S)$.

(ii) Of course $\mathsf{Aut}_{R\text{-}\mathbf{Alg}}(S)$ equals itself by reflexivity. The only automorphism of S that fixes all of S is the identity automorphism.

(iii) For every element σ of $\mathsf{Aut}_{\widetilde{T}\text{-}\mathbf{Alg}}(S)$, since σ fixes $\widetilde{T}$, also σ fixes the R-subalgebra T of $\widetilde{T}$. Thus, $\mathsf{Aut}_{\widetilde{T}\text{-}\mathbf{Alg}}(S)$ is a subgroup of $\mathsf{Aut}_{T\text{-}\mathbf{Alg}}(S)$.

(iv) An element σ of $\mathsf{Aut}(S)$ fixes the union in S of all elements Θ in J if and only if, for every element Θ in J, the element σ fixes Θ, i.e., if and only if σ is an element of $\mathsf{Aut}_\Theta(S)$ for every element Θ in J. Thus, $\mathsf{Aut}_{\cup J}(S)$ equals $\cap_{\Theta \epsilon J}\mathsf{Aut}_\Theta(S)$.

(v) For every element σ of Σ, by definition, σ fixes T. Thus, the fixed set of σ contains T. Since this holds for every element of Σ, the fixed set $\mathsf{Fix}^\Sigma(S)$ contains T.

(vi) For every element s of S, for every element σ' of $\mathsf{Aut}_{R-\mathbf{Alg}}(S)$, for the element $s' = \sigma^{-1}(s)$, we have $\sigma'(s')$ equals s' if and only if $\sigma \cdot \sigma' \cdot \sigma^{-1}(s)$ equals s. Thus, s is an element of $\sigma(\mathsf{Fix}^\Sigma(S))$ if and only if s is an element of $\mathsf{Fix}^{\sigma\cdot\Sigma\cdot\sigma^{-1}}(S)$. □

Definition 12.4. For every morphism of commutative rings, $u : R \to S$, the **R-subalgebra (thin) category**, $R - \mathbf{Subalg}(S)$, is the category whose objects are R-subalgebras T of S, and where there is a morphism from $\widetilde{T}$ to T if and only if T is an R-subalgebra of $\widetilde{T}$, in which case the inclusion is the unique morphism. Similarly, for every group Γ, the **subgroup (thin) category** of Γ, $\mathbf{Subgroup}(\Gamma)$, is the category whose objects are subgroups of Γ, and where there is a morphism from $\widetilde{H}$ to H if and only if $\widetilde{H}$ is a subgroup of H (as subgroups of Γ), in which case the inclusion is the unique morphism.

Corollary 12.5. *For every morphism of commutative rings, $u : R \to S$, the ordered pair $(\mathsf{Fix}^\bullet(S), \mathsf{Aut}_\bullet(S))$ of the functor $\mathsf{Fix}^\bullet(S)$ from $\mathbf{Subgroup}(\mathsf{Aut}_{R-\mathbf{Alg}}(S))$ to $R - \mathbf{Subalg}(S)$ and the functor $\mathsf{Aut}_\bullet(S)$ from $R - \mathbf{Subalg}(S)$ to $\mathbf{Subgroup}(\mathsf{Aut}_{R-\mathbf{Alg}}(S))$ is a **Galois connection**, i.e., it is an adjoint pair of functors between these thin categories. Thus, both compositions are endofunctors of the respective categories that are idempotent (i.e., all higher self-compositions of each endofunctor equals that same endofunctor).*

We already have the first half of the Fundamental Theorem of Galois Theory.

Corollary 12.6. *For every finite, Galois field extension, $v : F \to E$, for every F-subextension L of E, the fixed subfield in E of the subgroup $\mathsf{Aut}_L(E)$ of $\mathsf{Aut}_F(E)$ equals L.*

Proof. Denote the fixed subfield by K. By definition of $\mathsf{Aut}_L(E)$, the F-subextension L is a subfield of K. Thus, $[E : K]$ is less than or equal to $[E : L]$. By construction, $\mathsf{Aut}_K(E)$ contains $\mathsf{Aut}_L(E)$ as a subgroup. Thus, the cardinality of $\mathsf{Aut}_K(E)$ is at least as large as $\mathsf{Aut}_L(E)$. Since the cardinality of $\mathsf{Aut}_L(E)$ equals $[E : L]$ and since $\mathsf{Aut}_K(E)$ equals $[E : K]$, we conclude that also $[E : L]$ is less than or equal to $[E : K]$. Therefore $[E : K]$ equals $[E : L]$, so that also $[L : K]$ equals 1, i.e., L equals K. □

The following theorem of Emil Artin gives the second half of the Fundamental Theorem of Galois Theory.

Theorem 12.7 (Artin's Linear Independence of Multiplicative Homomorphisms)**.** *For every field E, for every group G, for every nonempty, finite sequence $(\rho_1, \dots, \rho_n)$ of pairwise distinct group homomorphisms from G to the multiplicative group $E^\times$, these are E-linearly independent elements of the E-vector space E^G of E-valued functions on G.*

Proof. This is proved by induction on n. The base case is $n = 1$. In this case, for the group identity element 1_G of G, also $rho_1(1_G)$ equals the multiplicative identity 1 in E. Thus, for every element c_1 of E such that $c_1 \cdot \rho_1$ is the zero function, then $c_1 = c_1 \cdot 1 = c_1 \cdot \rho_1(1_G)$ equals 0, i.e., there is only the trivial E-linear relation.

By way of induction, assume that $n > 1$, and assume that the theorem holds for all smaller values of n. Let $(c_1, \dots, c_n)$ be an ordered n-tuple of elements of E such that the E-linear combination function $f := c_1 \cdot \rho_1 + \cdots + c_n \cdot \rho_n$ is the zero function. Since ρ_n does not equal ρ_1, there exists an element h of G such that $\rho_n(h)$ is different from $\rho_1(h)$. Since f is the zero function, also the following function f^h is also the zero function,

$$f^h : G \to E, \quad f^h(g) := f(hg) = (c_1\rho_1(h)) \cdot \rho_1(g) + \cdots + (c_n\rho_n(h))\rho_n(g).$$

Of course also $\rho_n(h) \cdot f$ is the zero function. Thus the difference is the zero function,

$$f^h - \rho_n(h) \cdot f : G \to E, \quad (f^h - \rho_n(h) \cdot f)(g) = f(hg) - \rho_n(h)f(g) =$$

$$c_1(\rho_1(h) - \rho_n(h)) \cdot \rho_1(g) + \cdots + c_{n-1}(\rho_{n-1}(h) - \rho_n(h)) \cdot \rho_{n-1}(g).$$

By the induction hypothesis, for $k = 1, \dots, n-1$, we have $c_k(\rho_k(h) - \rho_n(h))$ equals 0. In particular, c_1 equals 0. Thus, $(c_2, \dots, c_n)$ is an ordered $(n-1)$-tuple of elements of E such that $c_2 \cdot \rho_2 + \cdots + c_n \cdot \rho_n$ equals the zero function. By the induction hypothesis, c_k equals 0 for every $k = 2, \dots, n$. Altogether, c_k equals 0 for every $k = 1, 2, \dots, n$. This proves the result by induction on n. □

Corollary 12.8. *For every field E, for every nonempty, finite sequence $\Sigma = (\sigma_1, \dots, sigma_n)$ of pairwise distinct automorphisms of the field E, for the fixed subfield $F = \mathsf{Fix}^\Sigma(E)$, the dimension of E as an F-vector space is $\geq n$ (possibly infinite).*

Proof. Consider the F-linear endomorphisms $\sigma_1, \dots, \sigma_n$ of E. Of course each sends 0 to 0. Thus, an E-linear combination of $\sigma_1, \dots, \sigma_n$ equals the zero function if and only if its restriction to the multiplicative group $E^\times = E \smallsetminus \{0\}$ is the zero function. By Artin's theorem, the only such linear combination comes from $(c_1, \dots, c_n) = (0, \dots, 0)$.

Since each σ_k is an F-linear endomorphism of E, by adjointness, each is equivalent to an E-linear transformation from $E \otimes_F E$ to E, where the E-vector space structure on $E \otimes_F E$ is $e \cdot (e_1 \otimes e_2) = (ee_1) \otimes e_2$. By the Rank-Nullity Theorem, every m-tuple of E-linear functionals on the E-vector space $E \otimes_F E$ has a nontrivial linear relation if m is strictly greater than $\dim_E(E \otimes_F E) = \dim_F(E)$. Therefore $\dim_F(E)$ is at least as positive as n. □

Theorem 12.9 (Numerical Fundamental Theorem of Galois Theory)**.** *For every field E, for every finite subgroup G of the (possibly infinite) group $\mathsf{Aut}(E)$ of field automorphisms of E, for the fixed subfield $F = \mathsf{Fix}^G(E)$, the dimension of E as an F-vector space is finite and equals the cardinality of G.*

Proof. By the earlier corollary, the dimension of E as an F-vector space is at least as large as G, possibly infinite. Every G-orbit $\mathcal{O} = \{x_1, \ldots, x_c\}$ in E has finite cardinality c dividing the finite cardinality d of G. The coefficients of the minimal polynomial $m_{\mathcal{O}}(t) = \prod_{x \in \mathcal{O}}(t - x)$ are G-invariant elements of E, i.e., $m_{\mathcal{O}}(t)$ is a degree-c, monic, irreducible polynomial in $F[t]$. Thus, every element x of E is algebraic over F of degree c dividing d, and the extension E splits the minimal polynomial. So E contains a splitting field over F of each of its elements. Therefore E is a filtering union of its finite F-subextensions L/F that are finite, Galois extensions of F, i.e., E is algebraic and Galois over F.

For every nested pair $L \subseteq K$ of finite F-subextensions that are finite, Galois over F, by Proposition 11.17, the restriction homomorphism $\mathsf{Aut}_F(K) \to \mathsf{Aut}_F(L)$ is surjective. Thus, using the Axiom of Choice, also $\mathsf{Aut}_F(E) \to \mathsf{Aut}_F(L)$ is surjective. But for every finite F-subextension L/F that is normal, the size of the automorphism group $\mathsf{Aut}_F(L)$ is finite and equals $[L : F]$. Thus, $d = \#G$ is an absolute bound on the degrees of finite F-subextensions of E. Since E is the filtering union of these finite F-subextensions, also E is a finite extension over F that is finite, Galois over F of degree bounded by d. Since E/F is a finite field extension that is Galois, $[E : F]$ equals the finite cardinality of $\mathsf{Aut}_F(E)$. □

Corollary 12.10 (The second half of the Fundamental Theorem of Galois Theory)**.** *For every finite, Galois extension of fields, $v : F \to E$, for every subgroup H of $\mathsf{Aut}_F(E)$, the degree of E over $L = \mathsf{Fix}^H(E)$ equals the cardinality of H, and $\mathsf{Aut}_L(E)$ equals H.*

Proof. By Artin's Theorem, the degree $[E : L]$ equals the cardinality of H. Denote $\mathsf{Aut}_L(E)$ by K. By the definition of L, the subgroup H is a subgroup of K. So the cardinality of K is at least as positive as the cardinality of H. Again by Artin's Theorem, the degree of $[E : \mathsf{Fix}^K(E)]$ equals the cardinality of K, which is at least as positive as $[E : L]$. But L is a subfield of $\mathsf{Fix}^K(E)$. Thus, L equals $\mathsf{Fix}^K(E)$, and the cardinality of K equals the cardinality of H. Therefore K equals H, i.e., $\mathsf{Aut}_L(E)$ equals H. □

Theorem 12.11 (The Fundamental Theorem of Galois Theory)**.** *For every finite, Galois extension of fields, $v : F \to E$, the Galois connection $(\mathsf{Fix}^\bullet(S), \mathsf{Aut}_\bullet(S))$ is an equivalence, i.e., these order reversing functions between the partially ordered set of subgroups of $\mathsf{Aut}_F(E)$ and the partially ordered set of F-subextensions of E are inverse bijections. Moreover, $[E : \mathsf{Fix}^H(E)]$ equals the cardinality of H for every subgroup H of $\mathsf{Aut}_F(E)$, and the cardinality of $\mathsf{Aut}_L(E)$ equals $[E : L]$ for every F-subextension L of E. Finally, for every F-subextension L of E, the group $\mathsf{Aut}_F(L)$*

is canonically isomorphic to the quotient group $N_{\mathsf{Aut}_F(E)}(\mathsf{Aut}_L(E))/\mathsf{Aut}_L(E)$. *Thus,* L *is itself a Galois extension of* F *if and only if* $\mathsf{Aut}_L(E)$ *is a normal subgroup of* $\mathsf{Aut}_F(E)$*, in which case this normal subgroup equals the kernel of the restriction homomorphism* res_L^E *from* $\mathsf{Aut}_F(E)$ *to* $\mathsf{Aut}_F(L)$.

Proof. That these are order reversing functions follows from Proposition 12.2 and Proposition 12.3. That these functions are inverse bijections follows from Corollary 11.14 and Corollary 12.10. Finally, for every F-subextension L of E, the group $\mathsf{Aut}_F(L)$ has a natural right action on $\mathsf{Hom}_{F-\mathbf{Alg}}(L, E)$ via precomposition. Since the left action of $\mathsf{Aut}_F(E)$ on this set is transitive, for every F-algebra automorphism τ of L, there exists an F-algebra automorphism σ of E such that σ restricts to τ on L. Thus, the group of F-algebra automorphisms of L equals the quotient by $\mathsf{Aut}_L(E)$ inside the subgroup of all elements of $\mathsf{Aut}_F(E)$ that map L back to itself. By Proposition 12.3(vi), an element σ of $\mathsf{Aut}_F(E)$ has $\sigma(L) = L$ if and only if σ normalizes the subgroup $\mathsf{Aut}_L(E)$. □

13 A second proof

In this section we give a different proof of parts of the Fundamental Theorem of Galois Theory that more explicitly use the E-algebra isomorphism of $E \otimes_F E$ with $E^{\mathsf{Aut}_F(E)}$. This is a special case of the more general technique of *descent*.

Let E be a field, and let $G \leq \mathsf{Aut}(E)$ be a finite subgroup of the group of field automorphisms of E. Denote by F the fixed set $\mathsf{Fix}^G(E)$, i.e., F equals

$$\mathsf{Fix}^G(E) := \{a \in E | \forall \sigma \in G, \sigma(a) = a\}.$$

By the Numerical Fundamental Theorem of Gaois Theory, $v : F \to E$ is a finite field extension that is normal, the group G equals $\mathsf{Aut}_F(E)$, and $[E : F]$ equals the cardinality of G.

Now consider the set map

$$\beta : E \times E \to E^G, \quad \beta(c, b) : \sigma \mapsto c\sigma(b).$$

It is straightforward to verify that β is an F-bilinear map and thus determines an F-linear map

$$T : E \otimes_F E \to E^G.$$

In fact, if we consider $E \otimes_F E$ as a left E-vector space via the scaling rule $\lambda \cdot (c \otimes b) := (\lambda c) \otimes b$, then T is even E-linear. If we choose a basis $(b_i)_{i \in I}$ for E as an F-vector space, then $(1 \otimes b_i)_{i \in I}$ is an E-basis for $E \otimes_F E$ (with respect to this left E-vector space structure). And if we use the standard basis $\mathbf{e}_\sigma$ for E^G, then the matrix of the linear transformation T is $[\sigma(b_i)]_{(i,\sigma) \in I \times G}$, i.e.,

$$T(1 \otimes b_i) = \sum_{\sigma \in G} \sigma(b_i)\mathbf{e}_\sigma.$$

Since we know the E-subalgebras of E^G, this means that we know the E-subalgebras of $E \otimes_F E$.

Corollary 13.1. *For the left E-vector space structure on $E \otimes_F E$, every E-subalgebra of $E \otimes_F E$ is of the form $T^{-1}(\mathrm{Image}(E^q))$ for a unique partition $q : G \to \Theta$.*

There is a left action of G on the ring $E \otimes_F E$ by F-algebra isomorphisms $\widehat{\sigma}$ defined as follows,

$$\widehat{\sigma}\cdot : E \otimes_F E \to E \otimes_F E, \quad \widehat{\sigma}(c \otimes b) := \sigma(c) \otimes b.$$

Notice that $\widehat{\sigma}\cdot$ is *not* E-linear for the left E-vector space structure on $E \otimes_F E$, (although it is E-linear for the *right* E-vector space structure). There is also a left action of G on E^G by F-algebra isomorphisms $\widetilde{\sigma}\cdot$ defined as follows,

$$\widetilde{\sigma}\cdot : E^G \to E^G, \quad \widetilde{\sigma} \cdot t : \tau \mapsto \sigma(t(\sigma^{-1}\tau)).$$

Proposition 13.2. *The F-algebra isomorphism T is left G-equivariant, i.e., $T((\widehat{\sigma}\cdot f)$ equals $\widetilde{\sigma}\cdot T(f)$ for every σ in G and every f in $E \otimes_F E$. Every left E-subalgebra of $E \otimes_F E$ which is mapped to itself by every $\widehat{\sigma}\cdot$ is of the form $T^{-1}(\mathrm{Image}(E^q))$ for the quotient $q : G \to G/H$ associated to a unique subgroup H of G.*

Proof. It is straightforward to verify that $T(\widehat{\sigma}(c \otimes b))$, i.e., $T(\sigma(c) \otimes b)$, is the set map sending each element τ to $\sigma(c)\tau(b)$. But this is the same as $\sigma(t(\tau^{-1}\sigma))$ where t is the set map $\rho \mapsto c \otimes \rho(b)$, i.e., t equals $T(c \otimes b)$. Thus $T(\widehat{\sigma}(c \otimes b))$ equals $\widetilde{\sigma}T(c \otimes b)$.

By Corollary 12.10, every left E-subalgebra of $E \otimes_F E$ comes from a unique partition $q : G \to \Theta$ of G. And $\mathrm{Image}(E^q)$ is spanned by the elements $\mathbf{e}_T$ for elements T of the partition. If this algebra is mapped to itself by $\widetilde{\sigma}$, then in particular $\widetilde{\sigma}(\mathbf{e}_T)$ is contained in the algebra. But this element is simply $\mathbf{e}_{\sigma \cdot T}$. So for every partition set T in Θ, $\sigma \cdot T$ is a union of partition sets in Θ. By considering the minimal partition sets, it follows that the partition is G-invariant. And then by Proposition 5.1, there exists a unique subgroup $H \leq G$ such that the partition Θ is simply G/H, the set of H-cosets in G. Conversely, it is straightforward to verify that for every subgroup H of G, the algebra corresponding to the partition G/H is G-invariant. Therefore the G-invariant F-subalgebras of F^G are precisely the subalgebras arising from the partitions G/H of subgroups H of G. □

There are also *right* actions of G on $E \otimes_F E$ and on E^G by F-algebra isomorphisms defined as follows,

$$\cdot\widehat{\sigma} : E \otimes_F E \to E \otimes_F E, \quad (c \otimes b) \cdot \widehat{\sigma} := c \otimes \sigma(b).$$

Notice that $\cdot\widehat{\sigma}$ is left E-linear, but it is not right E-linear. There is also a right action of G on E^G by E-algebra isomorphisms $\cdot\widetilde{\sigma}$ defined as follows,

$$\cdot\widetilde{\sigma} : E^G \to E^G, \quad t \cdot \widetilde{\sigma} : \tau \mapsto t(\tau\sigma).$$

Proposition 13.3. *The E-algebra isomorphism T is right G-equivariant, i.e., $T(f\cdot\widehat{\sigma})$ equals $T(f)\cdot\widetilde{\sigma}$ for every σ in G and every f in $E\otimes_f E$. For every left E-subalgebra B of $E\otimes_F E$ which is mapped to itself by every $\widehat{\sigma}\cdot$, there exists a unique subgroup H of G such that B equals $E\otimes_F \mathsf{Fix}^H(E)$.*

Proof. Just as in the proof of Proposition 13.2, it is straightforward to check that T is right G-equivariant (in fact this is even easier than checking that T is left G-equivariant). In Proposition 13.3 we already characterized the subalgebras B as above as $T^{-1}(\mathrm{Image}(E^q))$ coming from the quotient $q : G \to G/H$ for a unique subgroup H. The last step is to observe that E^q is the E-algebra of all set functions $t : G \to E$ which are constant on every fiber of q. But since these fibers are left cosets $\tau H = \{\tau\sigma | \sigma \in H\}$, this is precisely the same as saying that $(t\cdot\widetilde{\sigma})(\tau)$ equals $t(\tau)$ for every $\widetilde{\sigma}$ in H. And this is the same as saying that $t\cdot\widetilde{\sigma}$ equals t for every σ in H. Using that T is an E-algebra isomorphism which is G-equivariant, it follows that B is the set of elements,

$$B = \{f \in E\otimes_F E | \forall \sigma \in H, f\cdot\widehat{\sigma} = f\}.$$

Choose a basis $(c_i)_{i\in I}$ for E over F. Then every f in $E\otimes_F E$ is of the form

$$f = \sum_{i\in I} c_i \otimes b_i$$

for a unique I-tuple $(c_i)_{i\in I}$ of elements in E. And

$$f\cdot\widehat{\sigma} = \sum_{i\in I} c_i \otimes \sigma(b_i).$$

Thus $f\cdot\widehat{\sigma}$ equals f if and only if every $\sigma(b_i)$ equals b_i. Thus $f\cdot\widehat{\sigma}$ equals f for every σ in H if and only if every b_i is in the fixed field $\mathsf{Fix}^H(E)$. Therefore B is precisely $E\otimes_F \mathsf{Fix}^H(E)$ for a unique subgroup H of G, and for every subgroup H of B, $E\otimes_F \mathsf{Fix}^H(E)$ is a left G-invariant, left E-subalgebra of $E\otimes_F E$. □

Theorem 13.4 (Fundamental Theorem of Galois Theory (redux))**.** *For every finite, Galois extension of fields, $v : F \to E$, the Galois connection $(\mathsf{Fix}^\bullet(S), \mathsf{Aut}_\bullet(S))$ is an equivalence, i.e., these order reversing functions between the partially ordered set of subgroups of $\mathsf{Aut}_F(E)$ and the partially ordered set of F-subextensions of E are inverse bijections. Moreover, $[E : \mathsf{Fix}^H(E)]$ equals the cardinality of H for every subgroup H of $\mathsf{Aut}_F(E)$, and the cardinality of $\mathsf{Aut}_L(E)$ equals $[E : L]$ for every F-subextension L of E. Finally, for every F-subextension L of E, the group $\mathsf{Aut}_F(L)$ is canonically isomorphic to the quotient group $N_{\mathsf{Aut}_F(E)}(\mathsf{Aut}_L(E))/\mathsf{Aut}_L(E)$. Thus, L is itself a Galois extension of F if and only if $\mathsf{Aut}_L(E)$ is a normal subgroup of $\mathsf{Aut}_F(E)$, in which case this normal subgroup equals the kernel of the restriction homomorphism res^E_L from $\mathsf{Aut}_F(E)$ to $\mathsf{Aut}_F(L)$.*

Proof. Let H be a subgroup of G, and let L be $\mathsf{Fix}^H(E)$. Let H' be $\mathsf{Aut}_L(E)$. By definition, H is contained in H'. Also by definition, L is contained in $L' := \mathsf{Fix}^{H'}(E)$. So $\#H'$ is $\geq \#H$ and $[F : L']$ is $\leq [F : L]$. And by Theorem 12.9, we have

$$\#H = [E : L], \#H' = [E : L'].$$

Thus $\#H$ equals $\#H'$, i.e., H' equals H. So $\mathsf{Fix}^\bullet(E)$ is injective, and $\mathsf{Aut}_\bullet(E)$ is a left inverse of this injective map.

For every subextension L of E/F, consider the E-subalgebra $B_L := E \otimes_F L$ of $E \otimes_F E$. The field L is the set of elements b in E such that $1 \otimes b$ is in B_L, so the number of subextensions L is no greater than the number of E-subalgebras B_L. But B_L is a left G-invariant, left F-subalgebra of $E \otimes_F E$. By Proposition 13.2, the number of such E-subalgebras equals the number of subgroups H of G. And since $\mathsf{Aut}_\bullet(E)$ is injective, the number of extensions of the form $L = \mathsf{Fix}^H(E)$ also equals the number of subgroups of G. Therefore every subextension L of E/F is of the form $\mathsf{Fix}^H(E)$ for some unique subgroup H of G. So $\mathsf{Fix}^\bullet(E)$ is surjective. Thus $\mathsf{Fix}^\bullet(E)$ is a bijection. And since $\mathsf{Aut}_\bullet(E)$ is a left inverse, it is the inverse bijection.

It is straightforward to check that both bijections are order reversing. Since they are inverses, it follows that both are strictly order reversing, i.e., one element is greater than a second element if and only if the image of the first is less than the image of the second. Thus they strictly reverse upper bounds and lower bounds, i.e., meets and joins.

Let L be $\mathsf{Fix}^H(E)$. Since $[E : F]$ equals $[E : L][L : F]$, and since $[E : F] = \#G$ and $[E : L] = \#H$, it follows that $[L : F]$ equals $[G : H]$. Iterating gives $[\mathsf{Fix}^K(E) : \mathsf{Fix}^H(F)]$ equals $[H : K]$.

Finally, let L be $\mathsf{Fix}^H(E)$. For every σ in $N_G(H)$ and for every τ in H, $\tau' := \sigma\tau\sigma^{-1}$ is also in H, and every τ' in H arises in this way. Thus for every b in L,

$$\tau'\sigma(b) = \sigma\tau(b) = \sigma(b),$$

so that $\sigma(b)$ is fixed by every τ' in H, i.e., $\sigma(b)$ is again in L. Therefore the action of $N_G(H)$ on E maps L back into itself. So there is a homomorphism from $N_G(H)$ to $\mathsf{Aut}_F(L)$. By the definition of L, the kernel of this homomorphism is H. Thus there is an injective homomorphism $N_G(H)/H \to \mathsf{Aut}_F(L)$. The claim is that every F-automorphism $\theta : L \to L$ is in the image of this homomorphism, i.e., this homomorphism is an isomorphism.

Every F-automorphism $\theta : L \to L$ determines an E-algebra automorphism,

$$\mathrm{Id}_E \otimes \theta : E \otimes_F L \to E \otimes_F L, \quad c \otimes b \mapsto c \otimes \theta(b).$$

And this E-algebra automorphism commutes with the left G-action by $\widehat{\sigma}\cdot$. Of course we can recover θ from $\mathrm{Id}_E \otimes \theta$ by applying this to elements of the form $1 \otimes b$. So the number of F-algebra automorphisms of L is no greater than the number of E-algebra automorphisms of $E \otimes_F L$

which commute with the left G-action. Using T, every such automorphism is equivalent to an E-algebra automorphism of the E-subalgebra $E^{G/H}$ of F^G which commutes with the left G-action by $\widetilde{\sigma}\cdot$. By Corollary 4.15, every automorphism of $E^{G/H}$ is of the form F^t for a unique bijection $t : G/H \to G/H$. Finally, since θ commutes with the left G-action on $E \otimes_F L$, t commutes with the left G-action on G/H. Thus, by Proposition 5.2, there exists a unique coset k_0H in $N_G(H)/H$ such that $t(kH) = kk_0H$ for every kH in G/H. Therefore the number of such automorphisms is bounded by $[N_G(H) : H]$. But we already produced an injective homomorphism from $N_G(H)/H$ into the group of such automorphisms. Therefore this injective homomorphism is an isomorphism, i.e., $\mathsf{Aut}(L/E)$ equals $N_G(H)/H$.

In particular, since $[L : F]$ equals $[G : H]$, the size of $\mathsf{Aut}_F(L)$ equal $[L : F]$ if and only if $N_G(H)$ equals all of G, i.e., if and only if H is normal in G. Therefore, using Theorem 12.9 once more, F equals $\mathsf{Fix}^{\mathsf{Aut}_F(L)}(L)$ if and only if H is normal in G, i.e., L/F is Galois if and only if H is a normal subgroup of G. And in this case $\mathsf{Aut}(L/F)$ equals $N_G(H)/H$. □

14 Some results from commutative algebra

To prove some of the standard results about finitely generated field extensions that are not algebraic, we need to use some results of commutative ring theory of independent importance. We review some of these from the first semester. For the other results, we give references to the textbook *Commutative algebra* by David Eisenbud.

For every infinite field F, since every nonzero polynomial of degree e has at most e roots in F, the evaluation F-algebra homomorphism from $F[t]$ to F^F is injective. The analogue for higher d also holds.

Lemma 14.1. *For every infinite field F, for every positive integer d, the evaluation homomorphism from $F[t_1, \ldots, t_d]$ to F^{F^d} is injective.*

Proof. This is proved by induction on d, with the argument above proving the result for $d = 1$. By way of induction, assume d is greater than 1 and the result holds for smaller values of d. Let e be the largest nonnegative integer such that $m(t_1, \ldots, t_d)$ has a nonzero coefficient for some monomial that has t_i^e as a factor for at least one $i = 1, \ldots, d$. If e equals 0, then the polynomial is a nonzero constant, which has nonzero evaluation for every element in F^d. Thus, assume that e is positive.

Up to reordering the variables, assume that there is a nonzero coefficient of at least one monomial that equals $t_1^{e_1} \cdots t_{d-1}^{e_{d-1}} t_d^e$ for nonnegative integers $e_1, \ldots, e_{d-1}$. Then there exists a unique polynomial $g_e(t_1, \ldots, t_{d-1})$ such that $m(t_1, \ldots, t_{d-1}, t_d)$ equals $g_e(t_1, \ldots, t_{d-1})t_d^e$ plus terms whose t_d-degree is strictly less than e. By the induction hypothesis, there exists an element $(a_1, \ldots, a_{d-1})$ in F^d such

that $g_e(a_1, \dots, a_{d-1})$ is nonzero, say $c_e \neq 0$. Then $m(a_1, \dots, a_{d-1}, t_d)$ equals $c_e t^e$ plus terms of strictly lower degree. This is a nonzero polynomial of degree e. Thus, there are at most e roots in F. Since F is infinite, there exists an element a_d in F that is not a root, i.e., $m(a_1, \dots, a_{d-1}, a_d)$ is nonzero. This proves the result for d. By induction, the result holds for every positive integer d. □

Theorem 14.2 (Primitive Element Theorem)**.** *For every finite field extension, $v : F \to E$, that is normal, for every F-subextension, $F \xrightarrow{u} L \xrightarrow{w} E$, there exists an element x in L such that $F[x]$ equals L.*

Proof. If F is a finite field, then we even know that for every subfield L, for every generator x of the finite cyclic group $L^\times$, then L equals $\{0\} \cup \{x^m | m = 0, \dots, \#L - 1\}$. So L equals $F[x]$. Thus, without loss of generality, assume that F is infinite.

By the Fundamental Theorem of Galois Theory, there are only finitely many F-subextensions of E, and these are in bijection with the finitely many subgroups of $\mathsf{Aut}_F(E)$. In particular, there are only finitely many F-subextensions K of L that are properly contained in L. For each, let $\chi_K : L \to F$ be a nonzero linear polynomial whose kernel contains K (possibly equal to K). The product of χ_K over the finitely many proper F-subextensions K of L is a homogeneous, nonzero polynomial p in $n = [L : F]$ variables with coefficients in F. By the previous lemma, since F is infinite, there exists an element x of L such that $p(x)$ is nonzero. In particular, each of the factors $\chi_K(x)$ is nonzero, so that x is not contained in K for any proper F-subextension K of L. Thus, $F[x]$ is contained in none of the proper F-subextensions K of L, i.e., $F[x]$ equals all of L. □

For every finite field extension, $v : F \to E$, that is normal, for every field extension, $u : F \to L$, that v splits, we have an isomorphism of (left) E-algebras,

$$T^{v,u} : E \otimes_F L \to E^{\mathsf{Hom}_{F-\mathbf{Alg}}(L,E)}, \quad y \otimes x \mapsto (\sigma \mapsto y\sigma(x)),$$

where σ varies over the finitely many F-algebra homomorphisms from L to E (each of which is an injective field extension). In particular, since v splits itself, we have the E-algebra isomorphism,

$$T^{v,v} : E \otimes_F E \to E^{\mathsf{Hom}_F(E,E)}.$$

The set $\mathsf{Hom}_F(E, E)$ is $\mathsf{Aut}_F(E)$, which is a group under composition of F-algebra automorphisms. So there is a quite different structure of associative, unital E-algebra on $E^{\mathsf{Aut}_F(E)}$, namely the convolution product of the group algebra,

$$(\chi : \sigma \mapsto \chi(\sigma) * (\xi : \tau \mapsto \xi(\tau)) := (\rho \mapsto \sum_{(\sigma,\tau),\sigma\circ\tau=\rho} \chi(\sigma)\xi(\tau)).$$

For the standard basis elements δ_σ for the E-vector space $E^{\mathsf{Aut}_F(E)}$ with $\delta_\sigma(\sigma) = 1$ and otherwise $\delta_\sigma(\tau) = 0$, these elements are idempotent for the usual commutative F-algebra structure. However, for the convolution product, for all elements σ and τ of $\mathsf{Aut}_F(E)$, we have

$$\delta_\sigma * \delta_\tau = \delta_{\sigma\circ\tau}.$$

Of course this associative, unital E-algebra is typically not commutative, so the E-linear isomorphisms $T^{v,v}$ is certainly not a ring isomorphism (thus not even a ring homomorphism) from the commutative E-algebra $E \otimes_F E$. However, there is a natural right module structure on $E \otimes_F E$ by the group algebra $E^{\mathsf{Aut}_F(E)}$ for which this is an isomorphism of right modules,

$$(x \otimes y) * \delta_\sigma := x \otimes \sigma^{-1}(y).$$

Altogether, we conclude that this right $E^{\mathsf{Aut}_F(E)}$-module structure on $E \otimes_F E$ is just a copy of the right regular representation of $E^{\mathsf{Aut}_F(E)}$ on itself.

This $E^{\mathsf{Aut}_F(E)}$-module structure on $E \otimes_F E$ is the base change by $E \otimes_F (-)$ of a right $F^{\mathsf{Aut}_F(E)}$-module structure on E,

$$y * \delta_\sigma := \sigma^{-1}(y).$$

Since the E/F-base change of this module structure is isomorphic to the right regular representation, it is natural to ask whether E also isomorphic to the right regular representation of $F^{\mathsf{Aut}_F(E)}$ on itself. This is precisely the statement of the Normal Basis Theorem.

Theorem 14.3 (Normal Basis Theorem)**.** *For every finite field extension, $v : F \to E$, that is normal, the natural structure of right module on E for $F^{\mathsf{Aut}_F(E)}$ by $y * \delta_\sigma := \sigma^{-1}(y)$ is isomorphic to the right regular representation of $F^{\mathsf{Aut}_F(E)}$ on itself, i.e., there exists an element y in E such that the F-linear transformation $F^{\mathsf{Aut}_F(E)} \to E$ sending each δ_σ to $\sigma^{-1}(y)$ is an isomorphism.*

Proof. In case there is an *a priori* description of the right $F^{\mathsf{Aut}_F(E)}$-modules, we can try to prove this by base change. For instance, since the base change of the right $F^{\mathsf{Aut}_F(E)}$-module E with respect to the faithfully flat morphism $F^{\mathsf{Aut}_F(E)} \to E^{\mathsf{Aut}_F(E)}$ is a free right $E^{\mathsf{Aut}_F(E)}$-module (of rank one), in particular it is flat as a right module. Hence also E is flat as a right $F^{\mathsf{Aut}_F(E)}$-module.

Also, for all $F^{\mathsf{Aut}_F(E)}$-modules M, the dimensions of the F-vector space Tor groups and Ext groups of M and E over $F^{\mathsf{Aut}_F(E)}$ equal the dimensions of the corresponding E-vector space Tor groups and Ext groups for the base change modules of M and E from $F^{\mathsf{Aut}_F(E)}$ to $E^{\mathsf{Aut}_F(E)}$. Often this is enough to prove that the right $F^{\mathsf{Aut}_F(E)}$-module structure on E equals the right regular representation of $F^{\mathsf{Aut}_F(E)}$ on itself. Later, after studying representations of finite groups, we will see this works whenever F is a characteristic 0 field, or even just if the characteristic does not divide $[E : F]$. Using the explicit description of irreducible representations of the symmetric and

alternating groups via Young symmetrizers, Specht modules, etc., it works in all characteristics if $\mathsf{Aut}_F(E)$ is a symmetric group or alternating group (this is the "generic" situation in an appropriate sense). Also, this method works if $\mathsf{Aut}_F(E)$ is an Abelian group.

If $\mathsf{Aut}_F(E)$ is an Abelian group, then $F^{\mathsf{Aut}_F(E)}$ is a commutative F-algebra that has finite dimension as an F-vector space. As proved earlier, every such algebra has a finite decomposition as a product of finite commutative F-algebras that are local Artinian rings. To prove that a module is isomorphic to the right regular representation for the product ring, it is equivalent to prove that for each factor ring, the base change of the module over the factor ring is isomorphic to the right regular representation of the factor ring. Since E is a flat $F^{\mathsf{Aut}_F(E)}$-module, the base change for each factor ring is flat as a module over that factor ring. Since the dimension as an F-vector space is finite, each of these flat modules is also finitely presented. Every finitely presented, flat module over a local Artinian commutative ring is free of finite rank, by Nakayama's Lemma. Of course the rank times the F-vector space dimension of the local Artinian ring equals the F-vector space dimension of the base change module. Since the E-vector space dimensions of the E/F-base changes of the local Artinian ring and the module equal the F-vector space dimensions of the original modules, the rank is invariant under E/F-base change. Since $E \otimes_F E$ is a free $E^{\mathsf{Aut}_F(E)}$-module of rank 1, also each base change of E by the factor rings of $F^{\mathsf{Aut}_F(E)}$ are free modules of rank 1. Thus, E is a free $F^{\mathsf{Aut}_F(E)}$-module of rank 1.

If F is a finite field of cardinality $q = p^e$, then for every field extension E/F of finite degree $[F : E]$ is a normal extension with Abelian (even cyclic) Galois group. Thus the argument above proves that the right $F^{\mathsf{Aut}_F(E)}$-module E is isomorphic to the right regular representation of $F^{\mathsf{Aut}_F(E)}$ on itself. Hence assume that F is infinite. The goal is to prove that for some element x in the d-dimensional affine space E over F, the determinant of the F-linear transformation from the d-dimensional F-vector space $F^{\mathsf{Aut}_F(E)}$ to the d-dimensional F-vector space E sending each element $(\chi : \sigma \to \chi(\sigma))$ to $\sum_{\sigma \in \mathsf{Aut}_F(E)} \chi(\sigma) \cdot \sigma(x)$ is an isomorphism. Up to choosing F-vector space bases for $F^{\mathsf{Aut}_F(E)}$ and E, this linear transformation is a $d \times d$ matrix whose entries are F-linear functionals applied to the element x in the F-vector space E. Thus, the determinant is a homogeneous polynomial of degree d with coefficients in F on the d-dimensional affine space E over F. By hypothesis, after we base change from F to E, there does exist an element in $E \otimes_F E$ making the matrix invertible. Thus, the base change of the polynomial is not identically zero, i.e., the coefficient of at least one monomial is nonzero. Since the homomorphism from F to E is injective, this coefficient of the F-coefficient polynomial on E is also nonzero. Since the field F is infinite, by Lemma 14.1, there exists an element x in E on which the polynomial is nonzero. Therefore there exists x in E such that the F-linear transformation is invertible. □

Remark 14.4. For finite fields there is a much sharper version proved by Hendrik Lenstra and René Schoof.

Theorem 14.5 (Hilbert Basis Theorem)**.** *For every commutative ring R that is Noetherian, for every finitely generated ring extension, $u : R \to S$, also S is Noetherian.*

Proof. By induction, it suffices to prove that $R[t]$ is Noetherian. Let I be an ideal in $R[t]$. If I is the zero ideal, then it is finitely generated by 0. Hence assume that I is nonzero. Let J be the ideal of R generated by all leading coefficients of elements of I. Since R is Noetherian, the generating set of I consisting of leading coefficients has a finite subset that generates, i.e., there exist elements $f_1, \ldots, f_n$ whose leading coefficients generate J.

Let d be the maximum of the finitely many nonnegative integers $d_i = \deg_t(f_i)$. The R-submodule $R[t]_{\leq d-1}$ of all polynomials with degree $\leq d$ is a finitely generated R-module generated by $1, t, \ldots, t^{d-1}$. Since R is Noetherian, the R-submodule $I \cap R[t]_{\leq d-1}$ is also finitely generated as an R-module, say by $g_1, \ldots, g_m$.

The claim, to be proved by induction on the degree e of h, is that for every element h of I, this element is in the subideal I' that is the $R[t]$-module generated by $f_1, \ldots, f_n$ and $g_1, \ldots, g_m$. If e is $\leq d-1$, then h is in $I \cap R[t]_{\leq d-1}$, hence it is in the R-module generated by $g_1, \ldots, g_m$. Thus, by way of induction, assume that $e \geq d$ and the result is proved for all elements of I that have strictly lower degree.

The leading coefficient of h is an element of J. Since J is generated by the leading coefficients of $f_1, \ldots, f_n$, then there exist elements $r_1, \ldots, r_n$ of R such that the leading coefficient of h equals the leading coefficient of the following element of I'

$$r_1 t^{e-d_1} f_1 + \cdots + r_n t^{e-d_n} f_n.$$

Thus the difference is an element of I that has strictly smaller degree. By the induction hypothesis, this difference is in I'. Thus also h is in I'. □

Corollary 14.6. *For every commutative ring R that is Noetherian, every finitely generated R-algebra is also finitely presented.*

Proof. Every finitely generated R-algebra S is a quotient of a polynomial R-algebra $R[t_1, \ldots, t_m]$ by an ideal I. By the Hilbert Basis Theorem, the ring $R[t_1, \ldots, t_m]$ is Noetherian. Thus I is finitely generated. □

The next result is most often paired with the *Rabinowitsch trick* to prove the Strong Hilbert Nullstellensatz (a characterization of radical ideals in finitely generated algebras over a field). Since our application here does not need the Strong Hilbert Nullstellensatz, we stick with the Weak Hilbert Nullstellensatz.

Theorem 14.7 (Weak Hilbert Nullstellensatz)**.** *For every field extension $u : F \to E$, the field E is finitely generated as an F-algebra if and only if u is finite.*

Proof. If u is finite, then every finite set of generators of E as an F-module gives a finite set of generators of E as an F-algebra. Next, assume that E is finitely generated as an F-field extension (not necessarily as an F-algebra). Among every finite generating set as a field extension, there exists a finite transcendence basis. If the transcendence basis is empty, then E is algebraic over F, and thus finite over F (since the field extension is finitely generated). Thus, without loss of generality, assume that E has a nonempty, finite transcendence basis, say $\{t_1, \dots, t_n\}$.

By hypothesis, E is finite as an extension of $F(t_1, \dots, t_n)$, i.e., it is a vector space over this field that has finite dimension d. For every basis for this vector space, each element of E has a representation as a $d \times d$ matrix with entries in this field. In particular, for every finite generating set of E as an algebra over $F(t_1, \dots, t_n)$, each of the elements of the generating set gives a $d \times d$ matrix that has d^2 entries. Each entry is a fraction of elements in $F[t_1, \dots, t_n]$. Thus, there is a common denominator $g(t_1, \dots, t_n)$ for the entries of all of these finitely many matrices. So the F-subalgebra generated by these elements is contained in the finitely generated F-subalgebra $F[t_1, \dots, t_n][1/g]$. However, the nonzero element $1 + t_1 g(t_1, \dots, t_n)$ is not invertible in this F-algebra. So the F-subalgebra generated by these finitely many elements does not contain all of $F(t_1, \dots, t_n)$, hence it does not equal E. Therefore E is not finitely generated as an F-algebra. □

The next result is the Normalization Theorem of Emmy Noether. The formulation here is the one from the book *Commutative algebra* by David Eisenbud.

Theorem 14.8 (Noether Normalization Theorem, p.287 of *Commutative algebra*)**.** *For every field F and for every finitely generated F-subalgebra R of its fraction ring E, for every chain of ideals $\mathfrak{A}_1 \subsetneq \cdots \subsetneq \mathfrak{A}_n$ such that the (Krull) dimensions d_ℓ of the quotient rings $R/\mathfrak{A}_\ell$ form a strictly decreasing sequence, $d_1 > \cdots > d_n \geq 0$, there exists a (finite) subset $\{t_1, \dots, t_d\}$ of R such that R is integral (hence finite) over $F[t_1, \dots, t_d]$ (so that also this is a transcendence basis for E over F) and such that the ideal $\mathfrak{A}_\ell \cap F[t_1, \dots, t_d]$ in $F[t_1, \dots, t_d]$ equals the ideal $\langle t_{1+d_\ell}, \dots, t_d \rangle$ for every $\ell = 1, \dots, n$. If R is $\mathbb{Z}_{\geq 0}$-graded and each ideal $\mathfrak{A}_\ell$ is homogeneous, then the elements t_i can be chosen to be homogeneous. If the field E is infinite, and if $s_1, \dots, s_m$ is a generating set for R as an E-algebra, then the elements $t_1, \dots, t_{d_n}$ can each be chosen to be a k-linear combination of the elements $s_1, \dots, s_m$.*

One of the main corollaries of the Noether Normalization Theorem is the following finiteness theorem whose proof uses finite Galois theory. Returning to the subject of invariant subrings, the corollary below is one of the key ingredients in the proof of finite generatedness of the invariant

ring for an algebraic action of a geometrically reductive group scheme on a finitely generated algebra over an excellent Noetherian ring (due, altogether, to Gordan, Haboush, Hilbert, Mumford, Nagata and Seshadri). Our application of this theorem is to a result about finitely generated field extensions that are not finite so the logic is not circular. Our development of finite Galois theory never uses the Noether Normalization Theorem, and we will complete the proof of the corollary after proving the Fundamental Theorem of Galois Theory.

Corollary 14.9 (Emmy Noether, p. 297 of *Commutative algebra*)**.** *For every finitely generated field extension, $u : F \to E$, for every finitely generated F-subalgebra R of E such that E is a finite extension of $\mathrm{Frac}(R)$, the integral closure of R in E is a finite extension of R, hence a finitely generated F-algebra.*

Proposition 14.10. *For every finitely generated field extension $u : F \to E$, for every finitely generated F-subalgebra R of E, the integral closure of R in E is a finite extension of R, hence a finitely generated F-algebra.*

Proof. This is the same as the previous corollary when E is a finite extension of the fraction field L of R. Thus, assume that E is a finitely generated extension of L that is not a finite extension, i.e., the transcendence degree is at least one.

Since E is a finitely generated field extension of L, there exists a finitely generated R-algebra S such that E is the fraction field of S. Since also R is a finitely generated F-algebra, also S is a finitely generated F-algebra. By the previous corollary, the integral closure of S in E is finite over S, hence finitely generated over R. Replace S by this integral closure, so that now S is integrally closed in E.

Also the finitely generated L-algebra $L \otimes_R S$, i.e., the localization of S at the multiplicatively closed set $R \smallsetminus \{0\}$, is integrally closed in E. Thus, $L \otimes_R S$ contains the algebraic closure $\overline{L}$ of L in E. Since E has positive transcendence degree over R, the algebra $L \otimes_R S$ is not a field.

Since the integral domain $L \otimes_R S$ is not a field, every maximal ideal $\mathfrak{m}$ of $L \otimes_R S$ properly contains the zero ideal. Therefore, the residue field $(L \otimes_R S)/\mathfrak{m}$ is a field extension of $\overline{L}$ that is finitely generated as an L-algebra. Thus the residue field is a finite field extension of L by the Weak Hilbert Nullstellensatz. As a subextension of this finite field extension, also the algebraic closure $\overline{L}$ of L in E is a finite field extension of L. Now, by the previous corollary, the integral closure of R in this finite field extension $\overline{L}$ of its fraction field L is a finite extension of R. □

Corollary 14.11. *Every subextension of a finitely generated field extension is also a finitely generated field extension.*

Proof. Let $u : F \to E$ be a finitely generated field extension. For every subextension L, there exists a finite transcendence basis $t_1, \ldots, t_n$ for L over F (by the Steinitz – MacLane Exchange

Theorem). This transcendence basis gives an isomorphism of the polynomial ring $F[t_1, \dots, t_n]$ with an F-subalgebra R of L. By the previous proposition, the algebraic closure $\overline{\mathrm{Frac}(R)}$ in E of the fraction field $\mathrm{Frac}(R)$ is finite over $\mathrm{Frac}(R)$. Since $t_1, \dots, t_n$ is a transcendence basis for L over F, the extension L is algebraic over $\mathrm{Frac}(R)$, hence it is contained in $\overline{\mathrm{Frac}(R)}$. As a subextension of a finite field extension, L is also a finite extension of $\mathrm{Frac}(R)$. Thus L is a finitely generated extension of F. □

One of the key consequences is the following.

Corollary 14.12. *For every field F, for every finitely generated F-algebra S that is a unique factorization domain, for every subgroup G of the group $\mathsf{Aut}_{F-\mathbf{Alg}}(S)$, not necessarily finite, there exists a nonzero G-invariant element s of S and a finitely generated F-subalgebra R of $\mathsf{Fix}^G(S[1/s])$ whose fraction field inside $\mathsf{Frac}(S)$ equals $\mathsf{Fix}^G(\mathsf{Frac}(S))$. Moreover, we can assume that R is integrally closed in $S[1/s]$.*

Proof. By the previous result, $\mathsf{Frac}(S)^G$ is a finitely generated extension field of F. Thus, there exist finitely many nonzero elements that generate the field. Since S is a unique factorization domain, each of these elements is of the form t_i/s_i for unique nonzero elements t_i and s_i in S that have no common factor. Thus, for every element σ in G, since t_i/s_i equals $\sigma(t_i)/\sigma(s_i)$, also s_i equals $\sigma(s_i)$. Let s be the product of the finitely many denominators s_i. Let R be the F-subalgebra of $S[1/s]$ generated by the finitely many elements t_i/s_i. By construction R is contained in $\mathsf{Fix}^G(S[1/s])$ and $\mathsf{Frac}(R)$ equals $\mathsf{Fix}^G(\mathsf{Frac}(S))$. Since the integral closure of R in $S[1/s]$ is finite over R, we may replace R by the integral closure of R in $S[1/s]$. □

Hilbert asked whether it might be true that the F-algebra $\mathsf{Fix}^G(S)$ is finitely generated, at least when G is a linear algebraic subgroup of $\mathsf{Aut}_F(S)$. Miyanishi Nagata gave the first counterexamples. However, through the combined results of Paul Gordan, William Haboush, David Hilbert, David Mumford and Miyanishi Nagata, this is true when G is a linear algebraic group that is *reductive*. One of the first results along these lines is due to Emmy Noether, and was an early application of the notion of Noetherian rings.

Proposition 14.13. *For every finitely generated ring extension, $u : R \to S$, for every R-subalgebra T of S such that S is finite over T, there exists a finitely generated ring R-subalgebra T' of T such that S is finite over T'. If also R is Noetherian, then T is finitely generated over R.*

Proof. Each of the finitely many generators satisfies a monic polynomial with coefficients in T, and there are only finitely many such coefficients. Thus, the R-algebra T' generated by all of these coefficients is a finitely generated R-algebra, and S is already finite over T'. If R is Noetherian, then T' is also Noetherian by the Hilbert Basis Theorem. Then T is a T'-submodule of the finitely

generated T'-module S. Thus T is also a finitely generated T'-module, i.e., T is finite over T'. In particular T is finitely generated over T'. Since both $R \to T'$ and $T' \to T$ are finitely generated, also $R \to T$ is finitely generated. □

Corollary 14.14 (Emmy Noether)**.** *For every Noetherian ring R, for every finitely generated ring extension, $u : R \to S$, for every finite subgroup G of $\mathsf{Aut}_{R-\mathbf{Alg}}(S)$, also the fixed R-subalgebra $\mathsf{Fix}^G(S)$ is a finitely generated R-algebra.*

Proof. Every element s of S satisfies the monic polynomial $\prod_{g\in\Gamma}(t - g \cdot s)$ whose coefficients are elementary symmetric polynomials in the finite set $\Gamma \cdot s$, hence Γ-invariant. Thus S is integral over S^Γ. Now apply the previous result. □

15 Unramified extensions

Definition 15.1. A nonzero, commutative ring R is a **local ring** if R has a unique maximal ideal $\mathfrak{m}$. A local ring R is **Henselian**, or a **Hensel ring**, if (and only if) every finite R-algebra S has a finite decomposition, $S \cong \prod_{\sigma\in\Sigma} S_\sigma$, where each S_σ is a local ring (if S is the zero ring, this is the empty decomposition).

Lemma 15.2. *For every Henselian local ring R, every local ring S that is a finite R-algebra is also a Henselian local ring.*

Lemma 15.3. *For every Henselian local ring R, for every monic polynomial $m(t)$ in $R[t]$, and for every root x_0 in $k := R/\mathfrak{m}$ of the image $m_0(t)$ in $k[t]$ such that $m_0'(x_0)$ is nonzero, i.e., x_0 is a simple root of $m_0(t)$, there exists a root x of $m(t)$ in R whose image in k equals x_0, and x is unique. More generally, for all monic polynomials $f_0(t)$ and $g_0(t)$ in $k[t]$ that are relatively prime and such that $m_0(t)$ equals $f_0(t)g_0(t)$, there exist unique monic polynomials $f(t)$ and $g(t)$ in $R[t]$ mapping to $f_0(t)$ and $g_0(t)$ such that $f(t)g(t)$ equals $m(t)$.*

Theorem 15.4. *For every local ring R, the local ring is Henselian if and only if, for every monic polynomial $m(t)$ in $R[t]$ and for every simple root x_0 in k of the image $m_0(t)$ in $k[t]$, there exists a root x of $m(t)$ that maps to x_0.*

Lemma 15.5 (Hensel's Lemma)**.** *For every local ring R, for every monic polynomial $m(t)$ in $R[t]$, for every root x_e of $m(t)$ in $R/\mathfrak{m}^{1+e}$ whose image x_0 in $R/\mathfrak{m} = k$ has $m_0'(x_0)$ nonzero, there exists a unique root x_{e+1} of $m(t)$ in $R/\mathfrak{m}^{2+e}$ w whose image in $R/\mathfrak{m}^{1+e}$ equals x_e.*

Definition 15.6. For every local ring R, the **$\mathfrak{m}$-adic completion** of R is the inverse limit ring $\widehat{R} := \varprojlim_e R/\mathfrak{m}^{1+e}$. For every local ring R, the ring R is **$\mathfrak{m}$-adically complete** if (and only if) the natural ring homomorphism from R to $\widehat{R}$ is an isomorphism.

Corollary 15.7 (Hensel's Lemma, II)**.** *Every complete local ring is Henselian.*

Theorem 15.8 (Krull Intersection Theorem)**.** *For every Noetherian local ring R, for every finitely generated R-module M, the common intersection in M of $\mathfrak{m}^{1+e}M$ over all positive integers e is the zero submodule. In particular, the ring homomorphism from R to $\widetilde{R}$ is injective.*

Exercise 15.9. Let R' be $\mathbb{C}[z^{1/m} : m \in \mathbb{Z}_{\geq 1}]/\langle z^{1/m} - (z^{1/(mn)})^n : (r,s) \in \mathbb{Z}_{\geq 1}\rangle$. There is a $\mathbb{C}$-algebra homomorphism from R' to $\mathbb{C}$ that maps $z^{1/m}$ to 0 for every m in $\mathbb{Z}_{\geq 1}$. Let R be the localization of R' at the corresponding maximal ideal. Prove that the maximal ideal $\mathfrak{m}$ of R equals its own square ideal, $\mathfrak{m}^2$, hence equals $\mathfrak{m}^{1+e}$ for every positive integer e. Thus, one cannot drop the hypothesis that R is Noetherian in the statement of the Krull Intersection Theorem (although the theorem does hold for a wider class than Noetherian local rings).

Exercise 15.10. Let R be the localization of the $\mathbb{C}$-algebra $\mathbb{C}[s,t]/\langle t^2 - s^2(1+s)\rangle$ at the kernel of the $\mathbb{C}$-algebra homomorphism to $\mathbb{C}$ sending both s and t to 0. Prove that R is a Noetherian local ring that is an integral domain, yet the completion $\widetilde{R}$ is not an integral domain. However, if R is a regular local domain, then so is $\widetilde{R}$, so that both R and $\widetilde{R}$ are integral domains.

Definition 15.11. For every Noetherian local ring R, an element x in $\widetilde{R}$ is **Henselizable** over R if (and only if) x is contained in an R-subalgebra S of $\widetilde{R}$ that is finitely presented, flat and separable over R. The set of all such elements in $\widetilde{R}$ is the **Henselization** of R, denoted R^h.

Proposition 15.12. *For every Noetherian local ring R, the Henselization R^h inside $\widetilde{R}$ is a Noetherian local ring with maximal ideal equal to $\mathfrak{m}R^h = \widetilde{m} \cap R^h$ and residue field equal to $R/\mathfrak{m} = \widetilde{R}/\widetilde{m}$. The local ring homomorphism $R \hookrightarrow R^h$ is flat and separable (typically not finitely presented). The Noetherian local ring R^h is Henselian. Every local homomorphism from R to a Henselian local ring factors uniquely through $R \hookrightarrow R^h$. If R is an integral domain, then the F-algebra $F \otimes_R \widetilde{R}$ is a finite product of field extensions $(F \otimes_R \widetilde{R})_\eta$ of F, and the F-subalgebra $F \otimes_R R^h$ is the corresponding finite product of the separable closures of F in each $(F \otimes_R \widetilde{R})_\eta$. If R is a regular local ring, then so are $\widetilde{R}$ and R^h.*

We record here the main theorem comparing the Henselization to the completion. The original version is due to Michael Artin. The version below uses the amazing theorem of Dorin Popescu, as applied by Brian Conrad and Johan de Jong, to weaken the original hypotheses.

Theorem 15.13 (Artin Approximation Theorem)**.** *For every Noetherian local ring R that is excellent, for every finite collection $f_1, \ldots, f_c$ of elements in $R[t_1, \ldots, t_n]$, for every ordered n-tuple $(\widetilde{x}_1, \ldots, \widetilde{x}_n)$ of elements in $\widetilde{R}$ such that $(f_1(\widetilde{x}_1, \ldots, \widetilde{x}_n), \ldots, f_c(\widetilde{x}_1, \ldots, \widetilde{x}_n))$ equals $(0, \ldots, 0)$, for every nonnegative integer e, there exists an ordered n-tuple of elements $(x_1, \ldots, x_n)$ in R^h such that $(f_1(x_1, \ldots, x_n), \ldots, f_c(x_1, \ldots, x_n))$ equals $(0, \ldots, 0)$ and $\widetilde{x}_i - x_i$ is contained in $\mathfrak{m}^{1+e}$ for every $i = 1, \ldots, n$.*

Remark 15.14. In particular, for every Noetherian local ring R that is excellent, it follows that R^h is simply the set of all elements of $\widetilde{R}$ that satisfy a (not necessarily monic) polynomial in $R[t]$. Please note, when R is also an integral domain, this means that the image of $F \otimes_R R^h$ in each F-extension $(F \otimes_R \widetilde{R})_\eta$ is the full algebraic closure of $F \otimes_R R^h$, i.e., the separable closure of F in $(F \otimes_R \widetilde{R})_\eta$ is already algebraically closed in $(F \otimes_R \widetilde{R})_\eta$. This is one of the main criteria for distinguishing excellent Noetherian rings from more general Noetherian rings.

Proposition 15.15. *For every Henselian local ring R, for every finite, separable field extension κ of the residue field k, there exists a local homomorphism $u : R \to S$ that is finite faithfully étale and a surjective isomorphism of R-algebras, $\phi : S/\mathfrak{m}S \xrightarrow{\cong} \kappa$, and the pair $(u : R \to S, \phi)$ is unique up to unique isomorphism. In particular, if κ is a finite, Galois extension of k, then the homomorphisms $\mathsf{Aut}_R(S) \to \mathsf{Aut}_k(\kappa)$ and $\mathsf{Aut}_R(S) \to \mathsf{Aut}_F(S \otimes_R F)$ are both isomorphisms. There exists an algebraic, Galois field extension F^{nr} of F that is a filtering union of all such finite, Galois extensions $S \otimes_R F$ and whose Galois group is naturally isomorphic to the Galois group of k^{sep}/k, the separable closure of k.*

Corollary 15.16. *For every prime integer $p(>1)$ and for every positive integer e, for the unique Henselian discrete valuation ring R with maximal ideal pR that is integral over $\mathbb{Z}_{p\mathbb{Z}}$ and with residue field $R/pR \cong \mathbb{F}_q$, the absolute Galois group of F surjects onto the absolute Galois group $\widetilde{Z}$ of $\mathbb{F}_q$. This group is a topologically cyclic group, isomorphic to the profinite completion $\widetilde{\mathbb{Z}}$ of $\mathbb{Z}$, with the image of $Frob^e$ one topological generator. The corresponding algebraic, Galois field extension F^{nr} of F is the filtering union of fraction fields of finite faithfully étale R-algebras that are integral domains. All of this persists upon replacing R by the completion $\widetilde{R}$.*

Remark 15.17. In his doctoral thesis, Serge Lang proved that $\mathbb{Q}_p^{\mathrm{nr}}$ is a *quasi-algebraically closed field* in the sense of Emil Artin.

16 Tamely ramified extensions

Lemma 16.1. *For every Henselian discrete valuation ring R, for every generator π of the unique maximal ideal $\mathfrak{m}$, for every positive integer d that is not divisible by $\mathrm{char}(k)$, the characteristic of the residue field, the R-algebra $R[\pi^{1/d}] := R[t]/\langle t^d - \pi \rangle$ is an R-algebra that is a free R-module of rank d and that is a local ring with unique maximal ideal $\pi^{1/d} \cdot R[\pi^{1/d}]$ and with residue field k. The field extension $F \otimes_R R[\pi^{1/d}]$ of F is separable of degree d. If there exists a primitive d^{th}-root of unity in k, then this is a finite, Galois field extension whose Galois group is naturally isomorphic to the group μ_d of d^{th}-roots of unity in R.*

Definition 16.2. For every integer c that is either 0 or a prime integer $p(>1)$, the subset $\mathbb{Z}_{\geq 1}^{(c)}$ of $\mathbb{Z}_{\geq 1}$ consists of all integers d that are not divisible by c, i.e., $\mathbb{Z}_{\geq 1}^{(0)}$ equals all of $\mathbb{Z}_{\geq 1}$, and $\mathbb{Z}_{\geq 1}^{(p)}$ equals

the subset of $\mathbb{Z}_{\geq 1}$ of all integers d that are prime to p. For every Henselian discrete valuation ring R with unique maximal ideal $\mathfrak{m} = \pi \cdot R$ and with residue field k, for all elements d and e of $\mathbb{Z}_{\geq 1}^{(\mathrm{char}(k))}$, the **associated R-algebra morphism** from $R[\pi^{1/d}]$ to $R[\pi^{1/(de)}]$ is the unique R-algebra morphism ϕ_{de}^{d} that sends $\pi^{1/d}$ to $(\pi^{1/(de)})^e$. The colimit over all d in $\mathbb{Z}_{\geq 1}^{(\mathrm{char}(k))}$ of $R[\pi^{1/d}]$ is the **maximal tamely ramified extension** of R, denoted R^{tame}.

Proposition 16.3. *For every Henselian discrete valuation ring R with unique maximal ideal $\mathfrak{m} = \pi \cdot R$ and with residue field k that contains a primitive d^{th}-root of unity for every positive integer d that is not divisibly by $\mathrm{char}(k)$, the maximal tamely ramified extension R^{tame} is a flat, integral R-algebra that is a local ring. The field extension $F \otimes_R R^{tame}$ of F is an algebraic, Galois extension with Galois group naturally isomorphic to $\widetilde{\mu}^{(char(k))}$, the inverse limit over all d in $\mathbb{Z}_{\geq 1}^{(char(k))}$ of μ_d.*

Corollary 16.4. *Let k be the algebraic, Galois extension $\cup_{d \in \mathbb{Z}_{\geq 1}} \mathbb{Q}(\mu_d)$ of $\mathbb{Q}$ with Galois group $\widetilde{\mathbb{Z}}^\times$ acting on each subextension $\mathbb{Q}(\mu_d)$ through the quotient $(\mathbb{Z}/d\mathbb{Z})^\times$ sending each generator ζ of μ_d to $[e] \cdot \zeta := \zeta^e$. Let R be the Henselization of the local k-algebra $k[\pi]_{\langle \pi \rangle}$. Then the fraction field $F \otimes_R R^{tame}$ is an algebraic, Galois extension of F with Galois group $\widetilde{\mu}$. In particular, this is an algebraic, Galois extension of the Henselization of $\mathbb{Q}[\pi]_{\langle \pi \rangle}$. The Galois group fits into a short exact sequence,*

$$\{1\} \to \widetilde{\mu} \to \mathsf{Aut} \to \widetilde{\mathbb{Z}}^\times \to 0,$$

where the outer automorphism group action of each $(\mathbb{Z}/d\mathbb{Z})^\times$ on μ_d is as described above.

Corollary 16.5. *For each prime integer $p(>1)$ and positive integer e, let k be the algebraic closure $\cup_{d \in \mathbb{Z}_{\geq 1}^{(p)}} \mathbb{F}_q[\mu_d]$ of $\mathbb{F}_q$ with Galois group $\widetilde{Z} \cdot Frob^e$ acting on $\mathbb{F}_q[\mu_d]$ through the quotient $(\mathbb{Z}/r\mathbb{Z}) \cdot Frob^e$, where r is the multiplicative order of q modulo d. Let R be either the Henselization of $k[\pi]_{\langle \pi \rangle}$ or the unique algebraic, flat, separable extension of $\mathbb{Z}_{p\mathbb{Z}}$ that is Henselian with residue field k. Then the fraction field $F \otimes_R R^{tame}$ is an algebraic, Galois extension of F with Galois group $\widetilde{\mu}^{(p)}$. In particular, this is an algebraic, Galois extension of the Henselization of $\mathbb{F}_q[\pi]_{\langle \pi \rangle}$, resp. of the unique, degree-e, flat, separable extension of the Henselization of $\mathbb{Z}_{p\mathbb{Z}}$ that is an integral domain. The Galois group fits into a short exact sequence,*

$$\{1\} \to \widetilde{\mu}^{(p)} \to \mathsf{Aut} \to \widetilde{\mathbb{Z}} \cdot Frob^e \to 0,$$

where the outer automorphism group action of each $(\mathbb{Z}/r\mathbb{Z}) \cdot Frob^e$ on μ_d is as above, i.e., $[m]Frob^e$ sends each element ζ of μ_d to ζ^{q^m}.

The most important theorem about the maximal tamely ramified extension is the following very important theorem, absurdly named *Abhyankar's Lemma*.

Theorem 16.6 (Abhyankar's Lemma)**.** *For every Henselian discrete valuation ring R with unique maximal ideal $\mathfrak{m} = \pi \cdot R$ and with residue field $k = R/\pi \cdot R$ that is separably closed, every separable field extension of F whose degree is not divisible by $\mathrm{char}(k)$ is a subextension of the fraction field extension of $R \hookrightarrow R[\pi^{1/d}]$ for some positive integer d that is not divisible by $\mathrm{char}(k)$.*

In particular, this generalizes the following characterization of the algebraic closure of the characteristic zero Laurent series field.

Theorem 16.7 (Newton-Puiseux Theorem)**.** *For every Henselian discrete valuation ring R with unique maximal ideal $\mathfrak{m} = \pi \cdot R$ and with residue field $k = R/\pi \cdot R$ that is an algebraically closed field of characteristic zero, the algebraic closure of the fraction field F of R equals the fraction field $F \otimes_R R^{tame}$ of the maximal tamely ramified extension $\cup_{d \in \mathbb{Z}_{\geq 1}} R[\pi^{1/d}]$.*

Proof. Let $m(t)$ be a degree-d, monic, irreducible polynomial in $F[t]$. The goal is to prove that the image of $m(t)$ in $(F \otimes_R R[\pi^{1/m}])$ factors as a product of linear factors for some positive integer m.

Since $\mathrm{char}(k)$ equals 0, or more generally if d is invertible in F, we can perform a linear change of variables $t \mapsto t - (c_1/d)$, called a *Tschirnhausen transformation*, such that the coefficient of t^{d-1} becomes zero. Up to clearing denominators, the monic polynomial now equals $c_0^{-1}(c_0 t^d + c_2 t^{d-2} + \cdots + c_{d-1}t + c_d)$ for elements c_ℓ in R such that $c_0 = \pi^e$ for some integer $e \geq 0$, and such that the minimum of the π-adic valuation $\mathsf{val}_\pi(c_\ell)$ equals 0, for those ℓ with c_ℓ nonzero.

If every c_ℓ equals 0, then this polynomial already factors into a product of linear terms in $F[t]$, e.g., it equals a nonzero constant time t^d. Thus, assume that c_ℓ is nonzero for some $\ell = 2, \ldots, d$. In particular, assume that $d \geq 2$.

There exists some nonnegative integer r such that $e+r$ is divisible by d, i.e., $e+r$ equals df for some nonnegative integer f, and such that also $r \geq ((d-\ell)e - d\mathsf{val}_\pi(c_\ell))/\ell$ for every integer $\ell = 2, \ldots, d$ with c_ℓ nonzero. Setting $s = \pi^f t$, then we can rewrite this monic polynomial in t as $c_0^{-1}\pi^r$ times the monic, irreducible polynomial $\widetilde{m}(s) = s^d + b_2 s^{d-2} + \cdots + b_{d-1}s + b_0$ in $R[t]$, where now $\mathsf{val}_\pi(b_\ell)$ is nonnegative for all $\ell = 2, \ldots, d$ such that b_ℓ is nonzero.

Let v be the minimum of $\mathsf{val}_\pi(b_\ell)/\ell$ over all $\ell = 2, \ldots, d$ such that b_ℓ is nonzero. Let m be the least positive integer such that v equals $\mathsf{val}_\pi(b_m)/m$. Since m is not divisible by the characteristic of k, we can extend from the Henselian discrete valuation ring R to the Henselian discrete valuation ring $R[\pi^{1/m}]$. After the substitution $s = \pi^v u = (\pi^{1/m})^{\mathsf{val}_\pi(b_m)}u$, we can once again change coordinates so that the monic polynomial equals a nonzero constant times a monic polynomial $\widehat{m}(u) = u^d + a_2 u^{d-2} + \cdots + a_{d-1}u + a_d$ in $R[\pi^{1/m}][u]$ where now the $\pi^{1/m}$-adic valuation of a_ℓ is nonnegative for every $\ell = 2, \ldots, d$ such that a_ℓ is nonzero, and also the $\pi^{1/m}$-adic valuation of a_m equals 0. Thus, the image of this polynomial in $k[u]$ has the form $u^d + \overline{a}_2 u^{d-2} + \cdots + \overline{a}_{d-1}u + \overline{a}_d$, and $\overline{a}_m$ is nonzero.

In particular, this polynomial is not of the form $(u-\lambda)^d$, i.e., a single linear polynomial repeated d times. Therefore the reduction is of the form $\overline{f}(u)\overline{g}(u)$ for monic polynomials $\overline{f}(u)$ and $\overline{g}(u)$ in $k[u]$ of positive degree that are relatively prime.

Since $R[\pi^{1/\ell}]$ is a Henselian discrete valuation ring, there exist unique monic polynomials $f(u)$ and $g(u)$ in $R[\pi^{1/m}][u]$ with $f(u)g(u) = u^d + a_2^{d-2} + \cdots + a_{d-1}u + a_d$ and with images $\overline{f}(u)$ and $\overline{g}(u)$ in $k[u]$. Since the image of $m(t)$ in $R[\pi^{1/\ell}][t]$ factors as a product of relatively prime, monic polynomials of positive degree strictly less than d, we can now repeat with these factors. Therefore, by induction on the degree d, for every positive degree polynomial in $R[t]$, there exists an integer n not divisible by $\mathrm{char}(k)$ such that the image of the polynomial in $R[\pi^{1/n}][t]$ factors into a product of linear polynomials. □

Corollary 16.8. *For every algebraically closed field k of characteristic 0, one algebraic closure of the field $k(\!(t)\!)$ of Laurent polynomials with coefficients in k is the field $\cup_{d\in\mathbb{Z}_{\geq 1}} k(\!(t^{1/d})\!)$ of Puiseux series with coefficients in k. This is an algebraic, Galois extension of $k(\!(t)\!)$ whose Galois group equals $\widehat{\mu}$, the inverse limit over all positive integers d of the group μ_d of d^{th}-roots of unity in k.*

17 Wildly ramified extensions

Here we say very little. For local p-adic fields K, e.g., finite extensions K of the fraction fields $\mathbb{Q}_p$ of the complete discrete valuation rings $\mathbb{Z}_p$ of p-adic integers, there is an explicit description of the *inertia group*, i.e., the Galois group of an algebraic closure of $(\mathbb{Q}_p^{\mathrm{nr}})^{\mathrm{tame}}$ as an infinite iterated extension of copies of $\mathbb{Z}/p\mathbb{Z}$. In particular, every finite Galois extension L/K with Abelian Galois group is determined up to isomorphism by the image in $K^\times$ of the norm map on $L^\times$. Once we pass to $(K^{\mathrm{nr}})^{\mathrm{tame}}$, these subgroups land in the infinite p-group $\cup_{d\in\mathbb{Z}_{\geq 1}^{(p)}}(1+p^{1/d}R[p^{1/d}])$. So the Abelianization of the Galois group is an infinite p-group, and local class field theory gives a natural filtration on this group whose associated graded pieces are explicitly known. Similarly, for the tamely ramified extension $\cup_{d\in\mathbb{Z}_{\geq 1}^{(p)}}\overline{\mathbb{F}}_p(\!(t^{1/d})\!)$ of the Laurent series field $\overline{\mathbb{F}}_p(\!(t)\!)$, every finite group that is generated by its p-Sylow subgroups is a quotient of the absolute Galois group. In fact, by the proof of Abhyankar's Conjecture by Michel Raynaud and David Harbater, every such group is already the Galois group of a finite faithfully étale extension of the polynomial ring $\overline{\mathbb{F}}_p[t]$.