On the Galois closure of commutative algebras

Gioia, A.

On the Galois closure of commutative algebras

Proefschrift

ter verkrijging van
de graad van Doctor aan de Universiteit Leiden
op gezag van Rector Magnificus prof. mr. C.J.J.M. Stolker,
volgens besluit van het College voor Promoties
te verdedigen op woensdag 4 september 2013
klokke 13:45 uur

door

Alberto Gioia

geboren te Codogno
in 1985

Samenstelling van de promotiecommissie:

Promotor: Prof. dr. H. W. Lenstra

Promotor: Prof. dr. B. Erez (Université Bordeaux I)

Copromotor: Dr. L. Taelman

Overige leden:

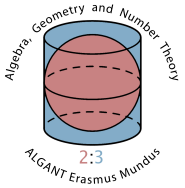
Prof. dr. Peter Stevenhagen

Prof. dr. M. Romagny (Université Rennes 1)

Dr. J. Draisma (Technische Universiteit Eindhoven)

Prof. dr. M. Bhargava (Princeton University en Universiteit Leiden)

This work was funded by Algant-Doc Erasmus Action and was carried out at Universiteit Leiden and l'Université Bordeaux 1.



THÈSE

présentée à

L'UNIVERSITÉ BORDEAUX I

ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE

par Alberto GIOIA

POUR OBTENIR LE GRADE DE

DOCTEUR

SPECIALITÉ : Mathématiques Pures

On the Galois closure of commutative algebras

Directeurs de recherche : Hendrik LENSTRA, Boas EREZ,
Lenny TAELMAN

Soutenue le : 4 Septembre 2013 à Leiden

Devant la commission d'examen formée de :

M ROMAGNY, Matthieu	Professeur	Université Rennes 1	Rapporteur
M DRAISMA, Jan	Docteur	Technische Universiteit Eindhoven	Rapporteur
M LENSTRA, Hendrik	Professeur	Universiteit Leiden	Directeur
M EREZ, Boas	Professeur	Université Bordeaux I	Directeur
M TAELMAN, Lenny	Docteur	Universiteit Leiden	Directeur
M STEVENHAGEN, Peter	Professeur	Universiteit Leiden	Examinateur
M BHARGAVA, Manjul	Professeur	Princeton University et Universiteit Leiden	Examinateur

Contents

Résumé (version longue)

Tous les anneaux et les algèbres considérés dans ce résumé sont commutatifs et unitaires. Soit R un anneau. Soit f un polynôme unitaire de degré n dans $R[Z]$. Soit A la R-algèbre $R[Z]/(f)$. Pour $i = 0, \ldots, n$, on définit des anneaux $F_i(A)$ et des polynômes f_i dans $F_i(A)[Z]$ par récurrence, de la façon suivante : soit $F_0(A) = R$, et soit $f_0 = f$. Si on a $F_i(A)$ et f_i on définit

$$F_{i+1}(A) = F_i(A)[x_{i+1}]/(f_i(x_{i+1})), \quad f_{i+1}(Z) = \frac{f_i(Z)}{Z - x_{i+1}} \in F_{i+1}(A)[Z].$$

On rémarque que pour $i = 0, \ldots, n$ le polynôme f_i est encore unitaire.

Si l'anneau R est un corps et si f est séparable et irréductible de groupe de Galois le groupe symétrique S_n, alors $F_n(A)$ est une clôture galoisienne de A/R. Donc il est possible de voir la construction de $F_n(A)$ comme une généralisation de la clôture galoisienne à une classe d'anneaux plus grande que celle des extensions séparables de corps (au moins pour les extensions avec groupe de Galois S_n).

Considérons une autre généralisation de la clôture galoisienne. Soit R un anneau connexe. Soit $\alpha\colon R \to K$ un point géométrique de R fixé. Soit $\pi = \pi(R, \alpha)$ le groupe fondamental étale de R en α. On a une anti-équivalence de catégories entre la catégorie des R-algèbres finies étales de rang n et la catégorie des ensembles finis avec n éléments, munis d'une action continue de π. Appelons de tels ensembles π-ensembles (voir définition 1.4.6 et théorème 1.4.9). Soit X un π-ensemble à n elements ; pour $i = 0, \ldots, n$ soit $\mathrm{Inj}(\{1, \ldots, i\}, X)$ l'ensemble des fonctions injectives de $\{1, \ldots, i\}$ dans X. Cet ensemble est muni d'une action naturelle de π, qui vient de l'action de π sur X. De cette façon à une R-algèbre A finie, étale de rang n, correspondant au π-ensemble X, on associe une R-algèbre finie, étale $G_i(A)$, de rang $n(n-1)\cdots(n-i+1)$, correspondant au π-ensemble $\mathrm{Inj}(\{1, \ldots, i\}, X)$.

Si la R-algèbre A est de la forme $R[Z]/(f)$ pour un polynôme unitaire f, alors pour tout $i = 0, \ldots, n$ on a que $G_i(A)$ est isomorphe à l'anneau $F_i(A)$ défini ci-dessus. Supposons que $R \to A$ est une extension séparable de corps, de degré n. Si le groupe de Galois est S_n, alors on a encore que $G_n(A)$ est

une clôture galoisienne de A. En général, $G_n(A)$ est un produit de copies de la clôture galoisienne.

La construction de $G_n(A)$ est plus naturelle que celle de la clôture galoisienne classique, parce qu'elle commute avec les changements de base. Pour tout $i = 0, \ldots, n$, la même chose est aussi vraie pour $F_i(A)$ et $G_i(A)$.

Plus géneralement, soit R un anneau et soit A une R-algèbre finie et localement libre de rang n. Dans [2], Manjul Bhargava et Matthew Satriano ont défini une clôture galoisienne de A/R. Donnons-en une définition équivalente.

Définition. Soit A une R-algèbre finie et localement libre de rang n. Une R-algèbre $A^{(n)}$ munie pour chaque $i = 1, \ldots, n$ d'un morphisme de R-algèbres $\alpha_i \colon A \to A^{(n)}$ est dit une *clôture galoisienne de A* si pour tout élément a de A le polynôme

$$\prod_{i=1}^{n} \big(Z - \alpha_i(a)\big) \in A^{(n)}[Z]$$

est égal à l'image du polyôme characteristique $P_a(Z)$ de a dans $A^{(n)}[Z]$ par le morphisme $R[Z] \to A^{(n)}[Z]$, et si de plus le couple $\big(A^{(n)}, (\alpha_i)_i\big)$ est universel pour cette propriété.

La construction de $A^{(n)}$ commute avec les changements de base (voir [2, Theorem 1]). Notons que l'idée pour la définition de $A^{(n)}$ est déjà dans la thèse de Bhargava. En effet, dans [1] il utilise une construction similaire pour la paramétrisation des anneaux de rang 3 et 4.

Dans le chapitre 1 de cette thèse nous costruisons pour tout anneau R et pour toute R-algèbre A localement libre de rang n, des algèbres $A^{(i)}$ pour chaque $i = 0, \ldots, n$. Ces algèbres généralisent les algèbres $F_i(A)$ et $G_i(A)$ (voir définition 1.3.1 et proposition 1.3.7). Comme $A^{(n)}$, ces "clôtures partielles" commutent avec les changements de base. Notre construction répond à une question posée dans [2, Question 4]. Nous établissons aussi une rélation entre notre construction et des constructions définies dans [9] par Daniel Ferrand (voir proposition 1.5.15).

Une fois la définition des $A^{(i)}$ donnée, nous étudions leurs propriétés. Le prémier résultat fondamental est théorème 1.4.4, qui–lorsque A est un produit fini de R-algèbres de rang fini, fournit une formule pour $A^{(i)}$ en fonction de plusieurs clôtures partielles des facteurs. Le théorème est une généralisation du théorème suivant (voir [2]).

Théorème ([2, Theorem 6])**.** *Pour $i = 1, \ldots, m$ soit A_i une R-algèbre localement libre de rang n_i. Soit A le produit des A_i, une R-algèbre localement libre de rang $n = \sum n_i$. Alors la clôture galoisienne de A satisfait :*

$$A^{(n)} \cong \left(\bigotimes_{i=1}^{m} A_i^{(n_i)} \right)^{\frac{n!}{n_1! \cdots n_m!}}.$$

Notre formule dans théorème 1.4.4 est très utile. Parmi ses applications figurent des resultats nouveaux pour les clôtures partielles aussi bien que pour la clôture galoisienne $A^{(n)}$. Par exemple nous montrons que $A^{(i)}$ n'est pas égale à l'anneau nul, en excluant quelques cas triviaux (voir proposition 1.4.17).

Avant de donner l'énoncé de notre résultat suivant, revenons à l'exemple du début. Soit donc K un corps et soit f un polynôme irréductible et séparable de degré n dans $K[Z]$. Soit L le corps $K[Z]/(f)$. Soit M la clôture galoisienne de L/K. On suppose que le groupe de Galois de M sur K est le groupe symétrique S_n. Dans ce cas, pour tout $i = 0, \ldots, n$, l'anneau $F_i(L)$ que nous avons défini ci-dessus est un corps et la sous-extension $K \to F_i(L)$ de M est isomorphe à $M^{S_{n-i}}$.

Une conséquence de la propriété universelle de $A^{(n)}$ est que le groupe S_n agit sur $A^{(n)}$ en permutant les morphismes naturels. Dans le chapitre 3 nous étudions cette action. En général, il n'est pas vrai que $A^{(i)}$ et $(A^{(n)})^{S_{n-i}}$ sont isomorphes, voir par exemple le cas où R est le corps $\mathbb{F}_2(X^2)$ et A est l'extension purement inséparable (ou radicielle) $\mathbb{F}_2(X)$ de R. Alors $A^{(2)}$ est égale à A, et l'action de S_2 est triviale. Donc $R \to (A^{(2)})^{S_2}$ n'est pas un isomorphisme. Pourtant, parce que l'extension est radicielle, le morphisme est un homéomorphisme universel. Rappelons qu'un morphisme d'anneaux $R \to A$ est un homéomorphisme universel, si pour tout $R \to R'$ le morphisme $\operatorname{Spec} A \otimes_R R' \to \operatorname{Spec} R'$ est un homéomorphisme (voir section 2.3).

Nous avons montré le résultat suivant.

Théorème (Théorème 3.2.9)**.** *Soit A une R-algèbre localement libre de rang n. Soit i dans $\{0, \ldots, n\}$. Alors, il existe un morphisme naturel $A^{(i)} \to \left(A^{(n)}\right)^{S_{n-i}}$, qui est un homéomorphisme universel.*

Pour démontrer ce théorème nous étudions, dans le chapitre 2 les schémas $X \to S$ munis d'une action par un groupe fini G telle que le quotient X/G soit universellement isomorphe au schéma de base S. Nous montrons alors le théorème suivant.

Théorème (Théorème 2.4.15)**.** *Soit $X \to S$ un schéma. Soit G un groupe fini qui agit sur $X \to S$. Alors les propositions suivantes sont équivalentes :*

1. *Le quotient X/G existe et le morphisme naturel $X/G \to S$ est un homéomorphisme universel.*
2. *Le morphisme $X \to S$ est entier et surjectif, et pour tout corps K sur S l'action de G sur chaque fibre non-vide de $X(K) \to S(K)$ est transitive.*

Dans le chapitre 4, nous étudions l'action du groupe alterné A_n sur $A^{(n)}$. Considérons à nouveau un exemple de la théorie de Galois. Soit K un corps de caracteristique différente de 2. Soit f un polynôme irréductible et séparable de degré n dans $K[Z]$. Soit M une clôture galoisienne de $K[Z]/(f)$. On suppose que le groupe de Galois de M/K est le groupe symétrique S_n. Les racines carrées du discriminant Δ_f de f sont dans M, et la sous-extension $K \to K[\sqrt{\Delta_f}\,]$ de M est M^{A_n}. Donc, $K \to K[\sqrt{\Delta_f}\,]$ dépend seulement de l'extension M/K et pas de f.

Soit R une $\mathbb{Z}[1/2]$-algèbre. Soit A une R-algèbre localement libre de rang n. Le déterminant $\bigwedge^n A$ est un R-module localement libre de rang 1. La forme discriminant $\bigwedge^n A \otimes \bigwedge^n A \to R$ définit une multiplication sur le R-module $R \oplus \bigwedge^n A$. On note la R-algèbre obtenue ainsi par $\Delta^{1/2}(A/R)$ et on l'appelle l'algèbre discriminant de A (voir définition 4.2.3). Si R est un corps et $A = R[Z]/(f)$ est un extension de R telle que le groupe de Galois d'une clôture galoisienne de A est S_n, alors $\Delta^{1/2}(A/R)$ est isomorphe à $R[\sqrt{\Delta_f}\,]$.

Nous montrons le théorème suivant.

Théorème (Théorème 4.3.8)**.** *Soit R une $\mathbb{Z}[1/2]$-algèbre. Soit A une R-algèbre localement libre de rang n. Alors, il existe un morphisme naturel de R-algèbres $\lambda\colon \Delta^{1/2}(A/R) \to A^{(n)}$ tel que l'homomorphisme $\Delta^{1/2}(A/R) \to (A^{(n)})^{A_n}$ induit par λ est un homéomorphisme universel.*

Nous ne sommes pas encore en mesure de dire si le morphisme λ est un isomorphisme en général.

A la fin de notre travail, nous donnons des indications sur un travail en préparation (en collaboration avec Owen Biesel). Le but de ce travail est de construire une algèbre discriminant pour les R-algèbres localement libres de rang n sur un anneau général R.

Introduction

All rings and algebras considered are commutative and have an identity element. Let R be a ring. Let f be a monic polynomial of degree n in $R[Z]$. Let A be the R-algebra $R[Z]/(f)$. Define rings $F_i(A)$ and polynomials f_i in $F_i(A)[Z]$ for $i = 0, \ldots, n$ recursively in the following way: let $F_0(A)$ be R, and let f_0 be f. Given $F_i(A)$ and f_i define

$$F_{i+1}(A) = F_i(A)[x_{i+1}]/(f_i(x_{i+1})), \quad f_{i+1}(Z) = \frac{f_i(Z)}{Z - x_{i+1}} \in F_{i+1}(A)[Z].$$

Note that for $i = 0, \ldots, n$ we have that f_i is monic.

Assume now the ring R above is a field and f is separable and irreducible. Assume moreover that the Galois group of f is the full symmetric group S_n. Then $F_n(A)$ is a Galois closure of A over R. So we could see the above construction of $F_n(A)$ as a generalization to a wider class of rings of the classical Galois closure (for S_n-extensions).

Here is another possible generalization of the Galois closure. Let R be a connected ring. Fix a geometric point $\alpha\colon R \to K$ of R. Let $\pi = \pi(R, \alpha)$ be the étale fundamental group of R in α. Then there is an anti-equivalence of categories between finite étale R-algebras of rank n and π-sets with n elements (see definition 1.4.6 and theorem 1.4.9). Given a π-set X with n elements, for all $i = 0, \ldots, n$ let $\mathrm{Inj}(\{1, \ldots, i\}, X)$ be the set of injective maps from $\{1, \ldots, i\}$ to X. The group π acts naturally on this set, via its action on X. In this way for a finite étale R-algebra A of rank n, corresponding to a π-set X, we define a finite étale R-algebra $G_i(A)$ of rank $n(n-1)\cdots(n-i+1)$, namely the finite étale R-algebra corresponding to $\mathrm{Inj}(\{1, \ldots, i\}, X)$.

If the finite étale R-algebra A is of the form $R[Z]/(f)$ for some monic polynomial f then for $i = 0, \ldots, n$ we have that $G_i(A)$ is isomorphic to the $F_i(A)$ given above. Assume $R \to A$ is a finite separable field extension of degree n. If it is an S_n-extension, then again $G_n(A)$ is a Galois closure of A. In general $G_n(A)$ is a product of copies of the Galois closure.

The construction of $G_n(A)$ is more natural than the classical Galois closure, because it commutes with base change. The same is true for $F_i(A)$ and $G_i(A)$ for $i = 0, \ldots, n$.

More generally, let R be a ring. Let A be a locally free R-algebra of rank n. A definition of Galois closure of A over R has been given by Manjul Bhargava and Matthew Satriano in [2]. Here is a definition that is equivalent to theirs.

Definition. Let A be a locally free R-algebra of rank n. An R-algebra $A^{(n)}$ given together with an R-algebra map $\alpha_i \colon A \to A^{(n)}$ for every $i = 1, \ldots, n$, is a *Galois closure of* A if for all $a \in A$ the polynomial

$$\prod_{i=1}^{n} \big(Z - \alpha_i(a)\big) \in A^{(n)}[Z]$$

is equal to the image of the characteristic polynomial $P_a(Z)$ of a in $A^{(n)}[Z]$ under the map $R[Z] \to A^{(n)}[Z]$, and if moreover the pair $\big(A^{(n)}, (\alpha_i)_i\big)$ is universal with this property.

The construction of $A^{(n)}$ commutes with base change (see [2, Theorem 1]).

Bhargava's idea for the definition of $A^{(n)}$ came from his thesis: in [1] he uses a similar construction for the parametrization of rings of rank 3 and 4.

In this thesis we construct for all rings R and locally free R-algebras A of rank n, algebras $A^{(i)}$ with $i = 0, \ldots, n$, generalizing the $F_i(A)$ and $G_i(A)$ (see definition 1.3.1 and proposition 1.3.7). Also these "intermediate closures" commute with base change. The existence of constructions with these properties was asked in [2, Question 4]. We also relate these constructions to certain constructions defined in [9] by Daniel Ferrand (see proposition 1.5.15).

We will then study some properties of the $A^{(i)}$. Our first main result is theorem 1.4.4, which expresses $A^{(i)}$, with A a finite product of locally free R-algebras of finite rank, in terms of various intermediate closures of the factors. It is a generalization of the following theorem from [2].

Theorem ([2, Theorem 6])**.** *For $i = 1, \ldots, m$ let A_i be a locally free R-algebra of rank n_i. Let A be the product of the A_i, a locally free R-algebra of rank $n = \sum n_i$. Then the Galois closure of A satisfies*

$$A^{(n)} \cong \left(\bigotimes_{i=1}^{m} A_i^{(n_i)} \right)^{\frac{n!}{n_1! \cdots n_m!}}.$$

Theorem 1.4.4 is a powerful tool. Among its applications we will see new results both on the intermediate closures and on $A^{(n)}$.

For the statement of the next result we first go back to our example. Let K be a field. Let f be a separable irreducible polynomial of degree n in $K[Z]$. Let L be the field $K[Z]/(f)$. Let M be a Galois closure of L over K. Assume the Galois group of M over K is the full symmetric group S_n. In this case

for all $i = 0, \ldots, n$ the ring $F_i(L)$ defined above is a field. The subextension $K \to F_i(L)$ of M is isomorphic to $M^{S_{n-i}}$.

From the universal property of $A^{(n)}$ follows that the group S_n acts on $A^{(n)}$ via R-algebra homomorphisms, by permuting the natural maps. It is not true that $A^{(i)}$ and $(A^{(n)})^{S_{n-i}}$ are isomorphic in general. However, something closely related is true.

Theorem (Theorem 3.2.9)**.** *Let A be a locally free R-algebra of rank n. Let i be an integer, with $0 \leq i \leq n$. Then there is a natural map $A^{(i)} \to \left(A^{(n)}\right)^{S_{n-i}}$, which is a universal homeomorphism.*

A ring homomorphism $R \to A$ is a universal homeomorphism if for all $R \to R'$ the map $\operatorname{Spec} A \otimes_R R' \to \operatorname{Spec} R'$ is a homeomorphism (see section 2.3).

The following example shows that we cannot get an isomorphism in general. Let R be the field $\mathbb{F}_2(X^2)$ and let A be the degree 2 purely inseparable extension $\mathbb{F}_2(X)$ of R. Then $A^{(2)}$ is equal to A and the action of S_2 is trivial. Hence $R \to (A^{(2)})^{S_2}$ is not an isomorphism. However, since the map is a purely inseparable field extension, it is a universal homeomorphism.

We also study the action of the alternating group A_n on $A^{(n)}$. Let us first consider a Galois theoretic example. Let K be a field of characteristic different from 2. Let f be a separable irreducible polynomial of degree n in $K[Z]$. Let M be a Galois closure of $K[Z]/(f)$. Suppose the Galois group of M over K is the full symmetric group S_n. The square roots of the discriminant Δ_f of f are in M, and the subextension $K \to K[\sqrt{\Delta_f}\,]$ of M is M^{A_n}. In particular $K \to K[\sqrt{\Delta_f}\,]$ only depends on the extension L/K, and not on f.

Let R be a $\mathbb{Z}[1/2]$-algebra. Let A be a locally free R-algebra of rank n. The determinant $\bigwedge^n A$ is a locally free R-module of rank 1. The discriminant form $\bigwedge^n A \otimes \bigwedge^n A \to R$ allows us to define a multiplication on the R-module $R \oplus \bigwedge^n A$. We denote the R-algebra obtained in this way by $\Delta^{1/2}(A/R)$ and call it the discriminant algebra of A (see definition 4.2.3). If R is a field and A is an S_n-extension of R of the form $R[Z]/(f)$ then $\Delta^{1/2}(A/R)$ is isomorphic to $R[\sqrt{\Delta_f}\,]$.

We will prove the following theorem.

Theorem (Theorem 4.3.8)**.** *Let R be a $\mathbb{Z}[1/2]$-algebra. Let A be a locally free R-algebra of rank n. Then there is a natural R-algebra map $\lambda\colon \Delta^{1/2}(A/R) \to A^{(n)}$ such that $\Delta^{1/2}(A/R) \to (A^{(n)})^{A_n}$ is a universal homeomorphism.*

I do not know if λ is an isomorphism in general.

Finally, we will give indications on future work (joint with Owen Biesel), which constructs a discriminant algebra of locally free R-algebras of rank n over a general commutative ring R.

An outline of the thesis: in chapter 1 we will introduce the intermediate closures and prove some of their basic properties, including the product formula mentioned above. We will also give some examples and explicit computations. In chapter 2 we will find necessary and sufficient conditions for $R \to A^G$ to be a universal homeomorphism given any R-algebra A, with an action of a finite group G. This will be used in chapter 3 and chapter 4 to prove the theorems mentioned above.

Conventions

In this thesis “ring” means “commutative ring with identity element”. If a non-commutative ring will appear it will be called “non-commutative ring”. Ring homomorphisms are required to respect the identity. Modules are unitary.

Algebras are rings, so the rules above apply.

Chapter 1

Galois closure for rings

1.1 Introduction

Let $K \to L$ be a finite separable field extension, and let f in $K[Z]$ be such that $L \cong K[Z]/(f)$. A Galois closure of L over K is a minimal Galois extension of K containing L. Equivalently, it is a field extension M of K, containing L, minimal with the property that f splits into linear factors in $M[Z]$.

Now assume that f has degree n, and the Galois group of f is S_n, the symmetric group on n letters. In this case we can construct a Galois closure as follows: let K_0 be K, and let f_0 be f. Given K_i and f_i we define K_{i+1} as $K_i[X_{i+1}]/(f_i(X_{i+1}))$. Denote by x_{i+1} the class of X_{i+1} in K_{i+1}. Let f_{i+1} be the quotient of f_i by $Z - x_{i+1}$ in $K_{i+1}[Z]$. The assumption that the Galois group of f is S_n guarantees that for $i = 0, \ldots, n$ the ring K_i is a field, and that K_n is the field we wanted to construct. In particular $x_1, \ldots, x_n$ are the roots of f in K_n.

Let R be a ring and let A be a locally free R-algebra of rank n (see definition 1.2.1). Manjul Bhargava and Matthew Satriano in [2] defined an R-algebra $G(A/R)$, which generalizes the Galois closure of an S_n-extension of K. In [2, Question 4] they asked whether it is possible to construct algebras $G^{(i)}(A/R)$ for $i = 1, \ldots, n$, with $G^{(n)}(A/R) = G(A/R)$, generalizing the intermediate K_i in the construction above.

In this chapter we construct such algebras, which we call m-closures, for all $0 \leq m \leq n$. These form the main object of study of this thesis. It is more natural and sometimes convenient to use a different description, which we will call S-closure, with S an arbitrary finite set. In the case of the intermediate K_i for fields, this means that we label the roots using the set S instead of $\{1, \ldots, i\}$. This will be made precise in section 1.3.

We will start by recalling some preliminary results on locally free modules and algebras in section 1.2. In particular, we recall the definition of characteristic polynomials of endomorphisms of a finite locally free module of constant rank, which is fundamental in the rest of the thesis. In section 1.3 we will give the definition, an explicit construction, and prove some basic properties of the S-closures.

We will then prove the "product formula" (theorem 1.4.4). This formula is a generalization of theorem 6 in [2], and expresses the S-closure of a product of R-algebras of finite rank in terms of T-closures of the factors, for various subsets T of S. This will be proved in section 1.4. In the same section we will also prove some consequences of this formula.

In section 1.5, we will relate the S-closures to certain constructions defined in [9] by Daniel Ferrand.

After that, in section 1.6 and section 1.7, we will study special cases, giving examples and explicit computations.

1.2 Preliminaries

In this section we will give results needed to define S-closures. First some facts about modules and algebras of rank n. We start with the definition.

Definition 1.2.1. For $n \geq 0$, a *locally free R-module of rank n* is a finitely generated R-module M such that for all primes $\mathfrak{p}$ of R the $R_\mathfrak{p}$-module $M_\mathfrak{p}$ is free of rank n. For brevity we will say M is an *R-module of rank n*. A *locally free R-algebra of rank n*, or an *R-algebra of rank n*, is an R-algebra that is of rank n as an R-module.

Proposition 1.2.2. *Let R be a ring and M be an R-module. The following are equivalent:*

1. *The module M is of rank n.*
2. *The module M is finitely presented and for all* maximal *ideals $\mathfrak{m}$ of R the $R_\mathfrak{m}$-module $M_\mathfrak{m}$ is free of rank n.*
3. *There exists a finite set $\{r_1, \ldots, r_N\} \subseteq R$ such that $r_1 + \cdots + r_N = 1$ and for all i the R_{r_i}-module M_{r_i} is free of rank n.*

Proof. See [18, Theorem 4.6]. □

Particularly important will be the definition of characteristic polynomials, which plays a fundamental role in the constructions we will consider. We first define the trace, following the notes on Galois theory for schemes by Hendrik Lenstra (see [18, Chapter 4]).

Lemma 1.2.3. *Let M be a finitely generated projective R-module and let $M^\vee$ be the R-module* $\mathrm{Hom}_R(M,R)$. *Then for any R-module N the map*

$$\begin{array}{rccc} \Phi\colon & N\otimes_R M^\vee & \to & \mathrm{Hom}_R(M,N) \\ & n\otimes f & \mapsto & \Big(x\mapsto f(x)n\Big) \end{array}$$

is an isomorphism.

Proof. Clearly this is true for $M = R$ and so also for M a free module of finite rank by taking direct sums. In general given a finitely generated projective module M there exists an R-module P such that $M\oplus P\cong R^n$ for some n. Then we know that $N\otimes_R (M\oplus P)^\vee \to \mathrm{Hom}_R(M\oplus P, N)$ is an isomorphism. Moreover, we have

$$\begin{aligned} N\otimes_R (M\oplus P)^\vee &\cong (N\otimes_R M^\vee)\oplus (N\otimes_R P^\vee), \text{ and} \\ \mathrm{Hom}_R(M\oplus P,N) &\cong \mathrm{Hom}_R(M,N)\oplus \mathrm{Hom}_R(P,N), \end{aligned}$$

The map $(N\otimes_R M^\vee)\oplus(N\otimes_R P^\vee)\to \mathrm{Hom}_R(M,N)\oplus\mathrm{Hom}_R(P,N)$ is the sum of $N\otimes_R M^\vee\to\mathrm{Hom}_R(M,N)$ and $N\otimes_R P^\vee\to\mathrm{Hom}_R(P,N)$. Since their sum is an isomorphism both maps are isomorphism. So the proof is complete. □

In particular one can take $N = M$ in lemma 1.2.3 and consider

$$\Phi^{-1}\colon \mathrm{End}(M)\to M\otimes_R M^\vee \tag{1}$$

We use this map to define the trace.

Definition 1.2.4. Let M be a projective finitely generated R-module. We define the *trace map*, denoted s_1, to be the composition of Φ^{-1} with the map $M\otimes_R M^\vee\to R$ sending $m\otimes f$ to $f(m)$. If A is a finite projective R-algebra, then we have a map $A\to\mathrm{End}(A)$ sending $a\in A$ to multiplication by a (here $\mathrm{End}(A)$ denotes the set of R-module endomorphisms of A). Composing this map with the trace map we get the trace map $A\to R$, which we denote again by s_1.

Note that the exterior power $\bigwedge^m M$ of an R-module of rank n is an R-module of rank $\binom{n}{m}$. This is because $\bigwedge^m$ commutes with base change (see [5, Chapitre III, §7, n. 5]) and if M is free of rank n then $\bigwedge^m M$ has rank $\binom{n}{m}$. By taking exterior powers we can define the determinant and the characteristic polynomial.

Definition 1.2.5. Let M be an R-module of rank n. For every $f\in\mathrm{End}(M)$ define the *determinant* of f, denoted $s_n(f)$ to be the trace of the endomorphism induced by f on $\bigwedge^n M$. For A an R-algebra of rank n we define the *norm* of $a\in A$, denoted $s_n(a)$, as the determinant of multiplication by a.

Remark 1.2.6. We will also use maps $s_i\colon \mathrm{End}(M) \to R$ for $i \geq 0$. These are defined as the trace of the i-th exterior power of $f \in \mathrm{End}(M)$. In particular s_1 is the trace as defined above and s_0 is just the constant map to 1.

Definition 1.2.7. Let M be an R-module of rank n. For every endomorphism f of M define the *characteristic polynomial* of f, denoted $P_f(X)$, as the determinant of the endomorphism $(\mathrm{Id} \otimes X - f \otimes \mathrm{Id})$ of $M \otimes_R R[X]$. For A an R-algebra of rank n, the characteristic polynomial of an element $a \in A$, denoted $P_a(X)$, is the characteristic polynomial of multiplication by a.

Remark 1.2.8. The coefficients of the characteristic polynomials are the s_i defined above, up to a sign. Explicitly we can write:

$$P_f(X) = \sum_{i=0}^{n} (-1)^i s_i(f) X^{n-i}.$$

See [17, Chapter XIX, Exercise 2].

Remark 1.2.9. Note that Cayley-Hamilton theorem holds, i.e. for all endomorphisms f of an R-module M of rank n, we have $P_f(f) = 0$. In fact, this holds for free modules (see [17, Chapter XIV, Theorem 3.1]) and if an element of $\mathrm{End}(M)$ is zero locally at every prime of R then it is zero. Moreover if A is an R-algebra, then $P_a(a)$ is zero since it is equal to P_a evaluated in the endomorphism given by multiplication by a, computed in 1.

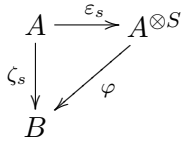
The following definition is standard, but it will be very important in the next chapters, so we give it here explicitly.

Definition 1.2.10. An R-algebra A is called integral over R if for all $a \in A$ there exists a monic polynomial $P \in R[X]$ such that $P(a) = 0$.

Remark 1.2.11. An R-algebra A of rank n is finite and hence also integral. For every $a \in A$ the characteristic polynomial of a is, by remark 1.2.9, an explicit monic polynomial that has a as a root.

The following construction is only a formal variant of the usual tensor power of an R-algebra (see also remark 1.2.13). This form will be useful later to simplify the notation, especially in section 1.4.

Definition 1.2.12. Let A be an R-algebra. For any finite set S the *tensor power of A indexed over S* is an R-algebra $A^{\otimes S}$ given with a map $\varepsilon_s\colon A \to A^{\otimes S}$ for every $s \in S$, such that for any R-algebra B with a map $\zeta_s\colon A \to B$ for every $s \in S$ we have a unique map $\varphi\colon A^{\otimes S} \to B$ making the following diagram commutative for every $s \in S$:



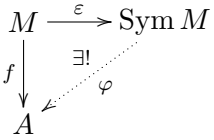
Remark 1.2.13. If $S = \{1, \dots, n\}$ then $A^{\otimes S}$ is $A^{\otimes n}$ with natural maps given by

$$\varepsilon_i \colon a \mapsto 1 \otimes \cdots \otimes a \otimes \cdots \otimes 1$$

(with a in the i-th position), because they have the same universal property. In general any bijection $S \to \{1, \dots, n\}$ induces a unique isomorphism $A^{\otimes S} \to A^{\otimes n}$ compatible with the natural maps.

Finally, we introduce generic elements, which we will use in the construction of the S-closure. To do that we define the *symmetric algebra*. A lot of information on this topic can be found in Bourbaki's algebra, see [5, Chapitre III, §6]. We will mostly need the following universal property (proposition 2 in Bourbaki).

Definition 1.2.14. Let M be an R-module. The *symmetric algebra* of M is an R-algebra $\operatorname{Sym} M$ given with an R-module map $\varepsilon \colon M \to \operatorname{Sym} M$ such that for all R-algebras A and R-module maps $f \colon M \to A$ there exists a unique R-algebra map $\varphi \colon \operatorname{Sym} M \to A$ making the following diagram commutative.



In other words the map

$$\operatorname{Hom}_{\text{R-alg}}(\operatorname{Sym} M, A) \to \operatorname{Hom}_R(M, A)$$

$$\varphi \mapsto \varphi \circ \varepsilon$$

is bijective.

Example 1.2.15. For every R-module M the symmetric algebra exists and can be explicitly constructed. For example if M is a free R-module with basis $e_1, \dots, e_n$ then the polynomial ring $R[e_1, \dots, e_n]$ with the map sending each e_i to e_i has the universal property of $\operatorname{Sym} M$.

In general the symmetric algebra of an R-module M is the quotient of the *tensor algebra* $\oplus_{n \geq 0} M^{\otimes n}$ of M (a non-commutative ring) by the two-sided ideal generated by the commutators. It is a graded algebra, with the degree 0 part isomorphic to R and the degree 1 part isomorphic to M. We will denote by $\operatorname{Sym}^n M$ the degree n part of $\operatorname{Sym} M$.

Definition 1.2.16. Let M be a finitely generated projective R-module. Tensoring the identity of M with the natural map $M^\vee \to \operatorname{Sym}(M^\vee)$ we get a morphism $M \otimes_R M^\vee \to M \otimes_R \operatorname{Sym}(M^\vee)$. Composing with the isomorphism Φ^{-1} defined in (1), we get an R-module map

$$\operatorname{End}(M) \to M \otimes_R \operatorname{Sym}(M^\vee).$$

We call the *generic element* of M, denoted γ_M or simply γ, the image of Id_M via the described map.

Remark 1.2.17. From the definition is clear that the generic element is an element of $M \otimes_R M^\vee$, so it can be written as $\sum m_i \otimes f_i$. Recall from 1.2.3 that $M \otimes_R M^\vee \to \mathrm{End}(M)$ sends $n \otimes g$ to the endomorphism $x \mapsto g(x)n$. The image of γ in $\mathrm{End}(M)$ is then $x \mapsto \sum f_i(x)m_i$. By definition of γ this map must be the identity, so for all $x \in M$ we have

$$x = \sum f_i(x)m_i.$$

In particular the m_i generate M over R. Moreover, the f_i generate $M^\vee$ as an R-module because given $f \in M^\vee$ we have:

$$f(x) = f\left(\sum f_i(x)m_i\right) = \sum f(m_i)f_i(x) = \left(\sum f(m_i)f_i\right)(x)$$

for all $x \in M$.

Example 1.2.18. Let M be a free R-module of rank n. We can then write the generic element of M explicitly: choose a basis $e_1, \ldots, e_n$ of M, and let $X_1, \ldots, X_n$ be the dual basis. Then $\mathrm{Sym}(M^\vee)$ is isomorphic to $R[X_1, \ldots, X_n]$ and the generic element of M is

$$\gamma = \sum_{i=1}^{n} e_i \otimes X_i$$

in $M \otimes_R \mathrm{Sym}(M^\vee)$.

Lemma 1.2.19. *Let M be a finitely generated projective R-module. Then the map*

$$M \to (M^\vee)^\vee$$
$$m \mapsto (f \mapsto f(m))$$

is an isomorphism.

Proof. The map is an isomorphism after localization at each prime of R. Hence it is an isomorphism. □

Remark 1.2.20. Note that the map in lemma 1.2.19 is still injective for M not finitely generated. In fact, we can reduce to free modules as above, and if x in a free module M is such that $f(x)$ is zero for all $f \in M^\vee$ then x is zero.

The following important property is the main reason why we will use the generic element.

Proposition 1.2.21. *Let M be a finitely generated projective R-module. Let R' be any R-algebra. Then the map*

$$\mathrm{Hom}_{R\text{-Alg}}(\mathrm{Sym}(M^\vee), R') \to M'$$

$$\varphi \mapsto (\mathrm{Id}_M \otimes \varphi)(\gamma)$$

is bijective.

Proof. Recall from lemma 1.2.3 that for all R-modules N we have that $N \otimes_R M^\vee \cong \mathrm{Hom}_R(M, N)$. By lemma 1.2.19 we have $M \cong (M^\vee)^\vee$. So we have

$$M' \cong \mathrm{Hom}_R(M^\vee, R') \cong \mathrm{Hom}_{R\text{-alg}}(\mathrm{Sym}(M^\vee), R'),$$

and hence $\mathrm{Sym}(M^\vee)$ represents the functor sending an R-algebra R' to the set M'. Taking $R' = \mathrm{Sym}(M^\vee)$ we have that φ_γ is the identity in $\mathrm{End}\,(\mathrm{Sym}(M^\vee))$, and by Yoneda's lemma we conclude the proof. □

Example 1.2.22. Let M be free of rank n. Write γ as $\sum_i e_i \otimes X_i$, with the notation introduced in example 1.2.18. The map φ_x is the unique R-algebra morphism $\mathrm{Sym}(M^\vee) \to R'$ sending e_i to $X_i(x)$ for all i. Hence, if A is a free R-algebra, the map $\mathrm{Id} \otimes \varphi_x$ is the evaluation map $A[X_1, \ldots, X_n] \to R'$ sending a polynomial f to $f(s_1, \ldots, s_n)$, where $(s_1, \ldots, s_n)$ is the element of R'^n representing x in the chosen basis.

Remark 1.2.23. Let A be an R-algebra. Let P_γ be the characteristic polynomial of γ in the $\mathrm{Sym}(A^\vee)$-algebra $A \otimes_R \mathrm{Sym}(A^\vee)$. Then for all $R \to R'$ and for all $a \in A' = A \otimes_R R'$ the map $A \otimes_R \mathrm{Sym}(A^\vee)[X] \to A'[X]$ induced by φ_a sends P_γ to the characteristic polynomial of a. This is true for free algebras as follows easily from example 1.2.22, so for an algebra of rank n it is true locally at every prime of R, hence the statement holds for algebras of rank n.

1.3 S-closures

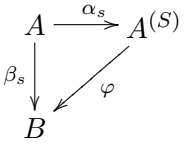
In this section we are going to define S-closures and prove their existence giving an explicit construction. We will use characteristic polynomials and generic elements, defined in section 1.2. We start with the definition.

Definition 1.3.1. Let A be an R-algebra of rank n, and let S be a finite set. An R-algebra $A^{(S)}$ given together with R-algebra maps $\alpha_s \colon A \to A^{(S)}$ for every $s \in S$, is an *S-closure of A* if for all $R \to R'$ and all $a \in A \otimes_R R'$ the polynomial

$$\Delta_a(X) = \prod_{s \in S} \big(X - (\alpha_s \otimes \mathrm{Id})(a)\big)$$

divides the characteristic polynomial P_a of a in $A^{(S)} \otimes_R R'[X]$, and the pair $\left(A^{(S)}, (\alpha_s)_{s\in S}\right)$ is universal with this property.

Being universal means that for all R-algebras B given with maps $\beta_s \colon A \to B$ for $s \in S$, if for all $R \to R'$ and $a \in A \otimes_R R'$ the polynomial $\prod_s (X - (\beta_s \otimes \mathrm{Id})(a))$ divides the characteristic polynomial of a in $B \otimes_R R'[X]$, then there is a unique morphism $\varphi \colon A^{(S)} \to B$ such that for every $s \in S$ the following diagram commutes:



Remark 1.3.2. From the universal property it follows (by standard argument) that if the S-closure of an R-algebra of rank n exists, then it is unique up to a unique isomorphism. The set $I = \{\alpha_s(a) \mid a \in A, s \in S\}$ has the same universal property as $A^{(S)}$, hence the S-closure is generated by I.

Remark 1.3.3. One can define the S-closure of a scheme X that is finite locally free of rank n over a scheme Y (see also the introduction of [2]). We will limit our study to the affine case.

In the rest of the section we give an explicit construction of the S-closure, showing it exists for any R-algebra of rank n and any finite set S, and we prove some easy consequences of the construction. We will need some results for the construction.

Lemma 1.3.4. *Let M be a locally free R-module. Then the map*

$$\begin{aligned} M &\to \prod_{\lambda \in M^\vee} R \\ m &\mapsto (\lambda(m))_\lambda \end{aligned}$$

is injective.

Proof. The map $M \cong (M^\vee)^\vee$ sending m to $\lambda \mapsto \lambda(m)$ is injective (see remark 1.2.20). The module $(M^\vee)^\vee$ can be identified with a submodule of $\prod_{\lambda\in M^\vee} R$ via the map sending $f \in (M^\vee)^\vee$ to $(f(\lambda))_\lambda$. So the proof is complete. □

Recall that given an R-module M we denote by $\mathrm{Sym}(M)$ the symmetric algebra of M (see definition 1.2.14). In the following lemma we denote by $\mathrm{Hom}_R(\mathrm{Sym}(M^\vee), R)$ the set of R-module morphisms from $\mathrm{Sym}(M^\vee)$ to R.

Lemma 1.3.5. *Let M be an R-module of rank n, and let C be an R-algebra. Let $t \in C \otimes_R \mathrm{Sym}(M^\vee)$. Then the following are equivalent:*

1. *The element t is zero.*
2. *For all λ in $\mathrm{Hom}_R(\mathrm{Sym}(M^\vee), R)$ we have $(\mathrm{Id}_C \otimes \lambda)(t)$ is zero in C.*
3. *For all $R \to R'$ and all R-algebra morphisms $\varphi\colon \mathrm{Sym}(M^\vee) \to R'$ we have $(\mathrm{Id}_C \otimes \varphi)(t)$ is zero in $C \otimes_R R'$.*

Proof. If t is zero then both *2* and *3* hold.

Suppose *3* holds. Then we can take $R' = \mathrm{Sym}(M^\vee)$ and φ the identity map, so t is zero and *1* and *3* are equivalent.

Suppose *2* holds. Since $\mathrm{Sym}(M^\vee)$ is locally free, the natural map

$$C \otimes_R \mathrm{Hom}_R\left(\mathrm{Sym}(M^\vee), R\right) \to \mathrm{Hom}_C\left(C \otimes_R \mathrm{Sym}(M^\vee), C\right)$$

is surjective. Let μ be in $\mathrm{Hom}_C(C \otimes_R \mathrm{Sym}(M^\vee), C)$ and let ν be in $C \otimes_R \mathrm{Hom}_R(\mathrm{Sym}(M^\vee), R)$, mapping to μ. Write ν as $\sum_i c_i \otimes \lambda_i$. Then we have

$$\mu(t) = \sum_i c_i(\mathrm{Id}_C \otimes \lambda_i(t))$$

and this is zero, since for all i we have $(\mathrm{Id}_C \otimes \lambda_i)(t) = 0$. Then lemma 1.3.4 with R equal C and M equal $C \otimes_R \mathrm{Sym}(M^\vee)$ implies that t is zero. Hence *1* and *2* are equivalent. □

We can now prove that the S-closure of a rank n algebra exists. We first introduce the notation we will use in the proof.

Notation 1.3.6. Let A be an R-algebra of rank n. We will write A_{Sym} for $A \otimes_R \mathrm{Sym}(A^\vee)$. Let S be a finite set. Note that

$$A_{\mathrm{Sym}}^{\otimes S} = (A \otimes_R \mathrm{Sym}(A^\vee))^{\otimes S} \cong A^{\otimes S} \otimes_R \mathrm{Sym}(A^\vee)$$

where the first tensor power is taken over $\mathrm{Sym}(A^\vee)$ and the last over R. We will use this canonical isomorphism without spelling it out. For $s \in S$ we denote by the same symbol both the natural map $\varepsilon_s\colon A \to A^{\otimes S}$ and its base change $\varepsilon_s\colon A_{\mathrm{Sym}} \to A_{\mathrm{Sym}}^{\otimes S}$.

Let $P_\gamma(X) \in A_{\mathrm{Sym}}[X]$ be the characteristic polynomial of the generic element. Define the polynomial

$$\Delta_\gamma = \prod_{s \in S} \left(X - \varepsilon_s(\gamma)\right)$$

in $A_{\mathrm{Sym}}^{\otimes S}[X]$. Note that since Δ_γ is monic, division with remainder of P_γ by Δ_γ can be done in $A_{\mathrm{Sym}}^{\otimes S}[X]$ and gives a unique quotient and remainder, with the remainder of degree less than $\#S$. We write

$$P_\gamma = \Delta_\gamma Q_\gamma + T_\gamma$$

and

$$T_\gamma = \sum_{0 \le i < \#S} t_i X^i$$

with t_i in $A^{\otimes S}_{\mathrm{Sym}}$.

In $A^{\otimes S}$ we define the following ideal:

$$J^{(S)} = \left\langle (\mathrm{Id}_{A^{\otimes S}} \otimes \lambda)(t_i) \mid i \ge 0, \lambda \in \mathrm{Hom}_R(\mathrm{Sym}(A^\vee), R) \right\rangle.$$

We will prove that $A^{\otimes S}/J^{(S)}$ is an S-closure for A.

Proposition 1.3.7 (Construction of $A^{(S)}$)**.** *Let A be an R-algebra of rank n and let S be a finite set. Let $C = A^{\otimes S}/J^{(S)}$, and define a map ζ_s for every $s \in S$ by composing the natural map $A \to A^{\otimes S}$ with the quotient map. Then (C, ζ_s) is an S-closure of A.*

Proof. We use the notation introduced in 1.3.6. We first show that for all $R \to R'$ and $a \in A \otimes_R R'$ the polynomial

$$\Delta_a = \prod_{s \in S} (X - (\varepsilon_s \otimes \mathrm{Id}_{R'})(a))$$

divides P_a in $C \otimes_R R'[X]$. Let T_a be the remainder of the division of P_a by Δ_a in $(A \otimes_R R')^{\otimes S}[X]$. Let $\varphi_a \colon \mathrm{Sym}(A^\vee) \to R'$ be the unique map such that $\mathrm{Id}_A \otimes \varphi_a$ sends γ to a, defined in proposition 1.2.21.

Note that $\mathrm{Id}_{A^{\otimes S}} \otimes \varphi_a$ sends $\varepsilon_s(\gamma)$ to $\varepsilon_s(a)$ for all $s \in S$. Hence $\mathrm{Id}_{A^{\otimes S}} \otimes \varphi_a(\Delta_\gamma)$ is Δ_a, and since also $\mathrm{Id}_A \otimes \varphi_a(P_\gamma)$ is P_a (see remark 1.2.23), and quotient and remainder are unique, also $\mathrm{Id}_{A^{\otimes S}} \otimes \varphi_a(T_\gamma)$ is T_a.

By definition of the ideal $J^{(S)}$ for all $i \ge 0$ the image of t_i in $C \otimes_R \mathrm{Sym}(A^\vee)$ via the quotient map satisfies condition *2* of lemma 1.3.5. Hence also condition *3* holds, so for all $R \to R'$ and for all $a \in A \otimes R'$ the map $\mathrm{Id}_C \otimes \varphi_a$ sends t_i to zero in $C \otimes_R R'$. So the coefficients of T_a are zero in $C \otimes_R R'$, and hence P_a is a multiple of Δ_a in $C \otimes_R R'[X]$, as we claimed.

We are left to show that C is universal with this property. Let B be an R-algebra with a map $\beta_s \colon A \to B$ for each $s \in S$, and such that for all $R \to R'$ and $a \in A \otimes_R R'$ we have that P_a is a multiple of $\prod(X - \beta_s(a))$ in $B \otimes_R R'[X]$. We need to show there exists a unique map $C \to B$ compatible with the given maps.

By the universal property of $A^{\otimes S}$ there is a unique map $\varphi \colon A^{\otimes S} \to B$ such that $\varphi \circ \varepsilon_s = \beta_s$ for all $s \in S$. Since P_γ is a multiple of $\prod(X - \beta_s(\gamma))$ in $B \otimes_R \mathrm{Sym}(A^\vee)[X]$, the images of the t_i in $B \otimes_R \mathrm{Sym}(A^\vee)$ via $\varphi \otimes \mathrm{Id}_{\mathrm{Sym}(A^\vee)}$ are zero, so they satisfy condition *1* of lemma 1.3.5, and hence also condition *2*. In particular, the map φ is zero on the ideal $J^{(S)}$, and hence it factors through C, giving the required map.

This map is necessarily unique, as C is generated by the images of the ζ_s. □

Remark 1.3.8. Let $(\lambda_i)_{i\in I}$ be a set of generators for $\mathrm{Hom}_R(\mathrm{Sym}(A^\vee), R)$. Then the ideal

$$\langle (\mathrm{Id}_{A^{\otimes S}} \otimes \lambda_i)(t_k) \mid k \geq 0, i \in I \rangle$$

in $A^{\otimes S}$ is equal to the ideal $J^{(S)}$ defined in 1.3.6. Moreover there exists $N \geq 0$ such that all the t_k are in $\mathrm{Sym}^{\leq N}(A^\vee)$ and the ideal $J^{(S)}$ can be generated by ranging over a set of generators for $\mathrm{Hom}_R(\mathrm{Sym}^{\leq N}(A^\vee), R)$. This gives a finite set of generators for $J^{(S)}$.

Example 1.3.9. Let A be free of rank n. Let $e_1, \ldots, e_n$ be a basis of A and let $X_1, \ldots, X_n$ be the dual basis. Here $A^{\otimes S} \otimes_R \mathrm{Sym}(A^\vee)$ is isomorphic to $A^{\otimes S}[X_1, \ldots, X_n]$ (see also example 1.2.15). Then the t_i defined in 1.3.6 are polynomials in the X_i with coefficients in $A^{\otimes S}$. For all monomials $X_1^{i_1} \cdots X_n^{i_n}$ we can define a linear map $R[X_1, \ldots, X_n] \to R$ that is one on $X_1^{i_1} \cdots X_n^{i_n}$ and zero on all other monomials. The images of t_i via these maps are its coefficients. The ideal $J^{(S)}$ can then be defined by the coefficients of the t_i. In section 1.7 we will use this set of generators for the ideal $J^{(S)}$ to compute examples.

We will prove in proposition 1.4.17 that, excluding trivial cases as in number *1* of proposition 1.3.12, the S-closure of an R-algebra is not the zero algebra.

We give a list of consequences of the definition and the construction. First some notation that we will use frequently in the rest of the thesis: if $S = \{1, \ldots, m\}$ we will denote $A^{(S)}$ by $A^{(m)}$.

Proposition 1.3.10. *Let A be an R-algebra of rank n. Then $A^{(n)}$ is isomorphic to the S_n-closure of Bhargava and Satriano.*

Proof. The algebra $G(A/R)$ with the natural maps $f_i \colon A \to G(A/R)$ for $i = 1, \ldots, n$, has the following universal property: for every $a \in A$ the elements $f_i(a)$ are roots of the characteristic polynomial in $G(A/R)[X]$ and given an R-algebra B together with maps $\beta_i \colon A \to B$ for $i = 1, \ldots, n$ such that for all $a \in A$ we have

$$P_a(X) = \prod_i (X - \beta_i(a))$$

there is a unique map $G(A/R) \to B$ compatible with the natural maps. Since the construction of $G(A/R)$ commutes with base change (theorem 1 in [2]) it also has the universal property of $A^{(n)}$. □

Remark 1.3.11. The Galois closure by Bhargava and Satriano is constructed as the quotient of $A^{\otimes n}$ (for A an R-algebra of rank n) by the ideal generated by the differences of the coefficients of P_a and of $\prod_i (X - \varepsilon_i(a))$ for all $a \in A$. A similar construction for the m-closure with arbitrary m would be to

take the quotient of $A^{\otimes m}$ by the ideal generated by the coefficients of the remainder in the division of P_a by

$$\Delta_a = \prod_{i=1}^{m}(X - \varepsilon_i(a))$$

for all $a \in A$. The fact that $G(A/R)$ commutes with base change is surprising and nontrivial, since we add in principle more relations if we require that P_a is a multiple of Δ_a for a in any base change of A. We give an example of this in 1.7.3, where we show that the constructions given here do not always commute with base change for $m < n$.

Proposition 1.3.12. *Let A be an R-algebra of rank n and let S be a finite set. Then:*

1. *If $\#S > n$ then $A^{(S)}$ is zero.*
2. *If $S = \varnothing$ then $A^{(S)}$ is R.*
3. *If $S = \{s\}$ then A together with the identity map $A \to A$ is an S-closure of A.*

Proof.

1. Let B be an R-algebra with maps $\beta_s\colon A \to B$ such that for all $R \to R'$ and $a \in A'$ the polynomial P_a is a multiple of $D_a = \prod(X - \beta_s(a))$ in $B'[X]$. Since both P_a and Δ_a are monic, the algebra B must be $\{0\}$ because by assumption the degree of D_a is strictly bigger than the degree of P_a. Then $\{0\}$ has the universal property for $A^{(S)}$.
2. Since 1 divides every polynomial, the universal property becomes: for every R-algebra B there exists a unique map $A^{(S)} \to B$. Since $A^{(S)} = R$ has this property, the proof is complete.
3. By Cayley-Hamilton (see remark 1.2.9) the polynomial $(X - a)$ divides $P_a(X)$ in $A[X]$ for every $R \to R'$ and any a in A'. The same is true for any R-algebra B with a map $f_s\colon A \to B$. Since $f_s = f_s \circ \mathrm{Id}_A$, we have that (A, α_s) has the universal property of $A^{(S)}$. The proof is complete. □

As discussed in section 1.1, given a separable field extension $L = K[X]/(f)$ of degree n we can construct a Galois closure of L/K by adjoining the n roots of f one by one. By definition a Galois closure of L must contain all the roots of f, but since the sum of the roots is equal to minus the coefficient of X^{n-1} in f, the field extension obtained by adding $n - 1$ roots is already a Galois closure. The next theorem shows that the same happens for S-closures.

Theorem 1.3.13. *Let A be an R-algebra of rank n. Then $A^{(n-1)} \cong A^{(n)}$.*

Proof. Define a map $\alpha_n \colon A \to A^{(n-1)}$ sending a to $s_1(a) - \sum_i \alpha_i(a)$ for $i = 1, \ldots, n-1$. We prove that $A^{(n-1)}$ with maps α_i for $i = 1, \ldots, n$ has the universal property for $A^{(n)}$. Clearly α_n is linear and for all R-algebras R' and $a \in A' = A \otimes_R R'$, the characteristic polynomial of a is equal to $\prod_i (X - \alpha_i(a))$. From this it follows that given any R-algebra B with n maps $\beta_i \colon A \to B$ satisfying the required property, the map $\psi \colon A^{(n-1)} \to B$ given by the universal property of $A^{(n-1)}$ satisfies $\beta_n = \psi \circ \alpha_n$.

It remains to show that α_n is multiplicative. We will use the following formula from [6]:

$$s_2(a+b) = s_2(a) + s_2(b) + s_1(a)s_1(b) - s_1(ab) \tag{1}$$

Since P_a is equal to $\prod_i (X - \alpha_i(a))$ we have that

$$s_1(a) = \textstyle\sum_i \alpha_i(a) \quad \text{and} \quad s_2(a) = \sum_{i<j} \alpha_i(a)\alpha_j(a)$$

Then we can compute

$$\begin{aligned} s_2(a+b) &= \sum_{i<j} \alpha_i(a+b)\alpha_j(a+b) = \\ &= \sum_{i<j} \alpha_i(a)\alpha_j(a) + \sum_{i<j} \alpha_i(b)\alpha_j(b) + \sum_{i \neq j} \alpha_i(a)\alpha_j(b) = \\ &= s_2(a) + s_2(b) + \sum_{i \neq j} \alpha_i(a)\alpha_j(b) \end{aligned}$$

and comparing with formula (1):

$$\sum_i \alpha_i(ab) = s_1(ab) = s_1(a)s_1(b) - \sum_{i \neq j} \alpha_i(a)\alpha_j(b) = \sum_i \alpha_i(a)\alpha_i(b).$$

Since α_i is multiplicative for $i = 1, \ldots, n-1$ follows that also α_n is multiplicative, as we wanted to show. □

Corollary 1.3.14. *Let A be an R-algebra of rank 2. Then A with the identity and the natural involution $a \mapsto s_1(a) - a$, is a 2-closure of A.*

Proof. Follows from theorem 1.3.13 and from number *3* of proposition 1.3.12. □

Remark 1.3.15. For any R-algebra A and any finite set S, by the universal property of $A^{(S)}$, there is a natural action of the symmetric group of S on $A^{(S)}$, exchanging the natural maps. This action will be discussed in detail in chapter 3.

1.4 The product formula

The theorem we are going to prove is a generalization to S-closures of the product formula that is proved in [2]; it is a formula to compute the S-closure of a product of algebras in terms of closures of the factors. We state the theorem here.

Theorem (Theorem 1.4.4)**.** *Let m be a positive integer. For $i = 1, \ldots, m$ let A_i be an R-algebra of rank n_i. Let A be $A_1 \times \cdots \times A_m$, an R-algebra of rank $n = \sum n_i$. Let S be a finite set and let $\mathscr{F}$ be the set of all maps $S \to \{1, \ldots, m\}$. Fix $F \in \mathscr{F}$ and let $S_i = F^{-1}(i)$. Write*

$$A^{(F)} = \bigotimes_{i=1}^{m} A_i^{(S_i)}$$

and let $\alpha_{s,i}$ for $s \in S_i$ be the natural map $A_i \to A_i^{(S_i)}$. Define an R-algebra

$$C = \prod_{F \in \mathscr{F}} A^{(F)}$$

and maps $\delta_s \colon A \to C$ for $s \in S$ by

$$(\delta_s(a_1, \ldots, a_m))_F = 1 \otimes \cdots \otimes \alpha_{s,i}(a_i) \otimes \cdots \otimes 1, \text{ with } i = F(s).$$

Then $(C, (\delta_s)_{s \in S})$ is the S-closure of A/R.

We will give the proof of the theorem after proving some lemmas.

Lemma 1.4.1. *Let R be a ring and let t be a positive integer. Then there exists polynomials $u(X), v(X) \in R[X]$ such that*

$$1 = u(X)X^t + v(X)(X-1)^t.$$

Proof. Let I be the ideal generated by X^t and $(X-1)^t$. We show that the quotient ring $S = R[X]/I$ is trivial, so that $1 \in I$. The image of X in S is nilpotent since $X^t = 0$, so $X - 1$ is a unit in S. But $X - 1$ is also nilpotent, hence S is trivial, as we wanted to show. □

Let P and Q be in $R[X]$. We will write $P \mid Q$ for "P divides Q".

Lemma 1.4.2. *Let A_i be R-algebras with A_i of rank n_i, for $i = 1, \ldots, m$. Let $S_1, \ldots, S_m$ be finite sets and let B be an R-algebra with maps $j_{s,i} \colon A_i \to B$ for $i = 1, \ldots, m$ and $s \in S_i$. Then the following are equivalent:*

1. *For all* $a = (a_1, \ldots, a_m) \in A$ *we have*

$$\prod_{i=1}^{m} \left(\prod_{s \in S_i} (X - j_{s,i}(a_i)) \right) \mid P_a(X)$$

in $B[X]$*, where* P_a *is the characteristic polynomial of* a*.*

2. *For all* $i \in \{1, \ldots, m\}$ *and for all* $a_i \in A_i$ *we have*

$$\prod_{s \in S_i} (X - j_{s,i}(a_i)) \mid P_{a_i}(X)$$

in $B[X]$*, where* P_{a_i} *is the characteristic polynomial of* a_i *in* A_i*.*

Proof. Note that P_a is equal to $\prod_i P_{a_i}(X)$, so clearly the second condition implies the first. Assume the first condition holds and fix $i \in \{1, \ldots, m\}$. Setting $a_j = 0$ for $j \neq i$ we have:

$$\prod_{s \in S_i} (X - j_{s,i}(a_i)) X^{N_1} \mid P_{a_i}(X) X^{N_2}$$

with $N_1 = \sum_{i \neq j} \#S_j$ and $N_2 = \sum_{i \neq j} n_j$. Setting $a_j = 1$ for $j \neq i$ we have

$$\prod_{s \in S_i} (X - j_{s,i}(a_i))(X-1)^{N_1} \mid P_{a_i}(X)(X-1)^{N_2}.$$

Put $t = N_2 - N_1$, and note that if $t < 0$ then

$$P_{a_i}(X) = X^{-t} \prod_{s \in S_i} (X - j_{s,i}(a_i))$$

and so the second condition holds. Assume $t \geq 0$, there exist $f(X)$ and $g(X)$ in $B'[X]$ such that:

$$P_{a_i}(X) X^t = \prod_{s \in S_i} (X - j_{s,i}(a_i)) f(X) \tag{1}$$

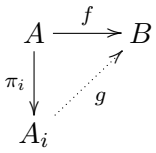
$$P_{a_i}(X)(X-1)^t = \prod_{s \in S_i} (X - j_{s,i}(a_i)) g(X) \tag{2}$$

By lemma 1.4.1 there exist $u(X)$ and $v(X)$ in $B'[X]$ such that $u(X)X^t + v(X)(X-1)^t = 1$. Multiplying (1) by $u(X)$ and (2) by $v(X)$ and adding the results we get

$$P_{a_i}(X) = (u(X)f(X) + v(X)g(X)) \prod_{s \in S_i} (X - j_{s,i}(a_i))$$

so the second condition holds and the proof is complete. □

Lemma 1.4.3. *Let $A = \prod_{i=1}^{m} A_i$ be a finite product of rings. If B is a connected ring then given a morphism $f\colon A \to B$ there exists a unique index i and a unique morphism $g\colon A_i \to B$ such that $f = g \circ \pi_i$, where $\pi_i\colon A \to A_i$ is the natural projection.*



Proof. Since B is connected the only idempotents are 0 and 1. Let 1_i be the element $(0, \ldots, 1, \ldots, 0)$ of A, where 1 is in the $i-th$ position. Since 1_i is idempotent $f(1_i)$ is idempotent in B. If $f(1_i) = 0$ for all i, then f would send 1 to 0, so there exist at least one i such that $f(1_i) = 1$. For $j \neq i$, we have

$$0 = f(0) = f(1_i 1_j) = f(1_i) f(1_j) = f(1_j)$$

so 1_j is zero if $j \neq i$ and hence i is unique. Then f factors through a unique A_i, as we wanted to show. □

We now prove the product formula.

Theorem 1.4.4. *Let m be a positive integer. For $i = 1, \ldots, m$ let A_i be an R-algebra of rank n_i. Let A be $A_1 \times \cdots \times A_m$, an R-algebra of rank $n = \sum n_i$. Let S be a finite set and let $\mathscr{F}$ be the set of all maps $S \to \{1, \ldots, m\}$. Fix $F \in \mathscr{F}$ and let $S_i = F^{-1}(i)$. Write*

$$A^{(F)} = \bigotimes_{i=1}^{m} A_i^{(S_i)}$$

and let $\alpha_{s,i}$ for $s \in S_i$ be the natural map $A_i \to A_i^{(S_i)}$. Define an R-algebra

$$C = \prod_{F \in \mathscr{F}} A^{(F)}$$

and maps $\delta_s\colon A \to C$ for $s \in S$ by

$$(\delta_s(a_1, \ldots, a_m))_F = 1 \otimes \cdots \otimes \alpha_{s,i}(a_i) \otimes \cdots \otimes 1, \text{ with } i = F(s).$$

Then $(C, (\delta_s)_{s \in S})$ is the S-closure of A/R.

Proof. We give first a summary of the proof: we show that for every $R \to R'$ and every $a \in A' = A \otimes_R R'$ the characteristic polynomial $P_a(X)$ is a multiple of

$$\Delta_a(X) = \prod_{s \in S} (X - \delta_s(a))$$

in $C \otimes_R R'[X]$; then we show that for every *connected* R-algebra B given with a map $\beta_s \colon A \to B$ for each $s \in S$, such that for every $R \to R'$ and every $a \in A'$ the characteristic polynomial $P_a(X)$ is a multiple of $\prod(X - \beta_s(a))$ in $B \otimes_R R'[X]$ there is a unique map $C \to B$ commuting with all the natural maps; from this we deduce the theorem for R a finitely generated $\mathbb{Z}$-algebra; then we prove the theorem in general.

That P_a is a multiple of Δ_a in $C \otimes_R R'[X]$ for every $R \to R'$ and for every $a \in A'$ follows from the easy implication in lemma 1.4.2 and the defining property of $A^{(S_i)}$.

Suppose B is a *connected* R-algebra with maps $\beta_s \colon A \to B$ for $s \in S$ and such that for all $R \to R'$ and for all $a \in A'$ we have

$$\prod_{s \in S} (X - \beta_s(a)) \mid P_a(X)$$

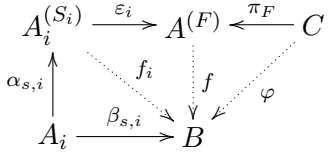
in $B \otimes_R R'[x]$. We show that there exists a unique map $\varphi \colon C \to B$ such that for all $s \in S$ we have $\beta_s = \varphi \circ \delta_s$. Since B is connected, by lemma 1.4.3 we can define a map $F \colon S \to \{1, \ldots, m\}$ by setting $F(s) = i$ if and only if β_s factors through A_i, i.e. there exists a map $\beta_{s,i}$ such that $\beta_s = \beta_{s,i} \circ \pi_i$, where π_i is the projection $A \to A_i$. For all $a \in A'$ we have that

$$\prod_{s \in S} (X - \beta_s(a)) = \prod_{i=1,\ldots,m} \left(\prod_{s \in F^{-1}(i)} (X - \beta_{s,i}(a_i)) \right)$$

holds in $B'[x]$. By lemma 1.4.2 for all $i \in \{1, \ldots, m\}$ and for all $a_i \in A_i'$ we have then

$$\prod_{s \in F^{-1}(i)} (X - \beta_{s,i}(a_i)) \mid P_{a_i}(X)$$

so the universal property of $A_i^{(S_i)}$ gives a unique map $f_i \colon A_i^{(S_i)} \to B$ such that for all $s \in S_i$ we have $\beta_{s,i} = f_i \circ \alpha_{s,i}$. Tensoring these maps, we get a unique map $f \colon A^{(F)} \to B$ such that for all i we have $f_i = f \circ \varepsilon_i$ where ε_i is the natural map $A_i^{(S_i)} \to A^{(F)}$. Composing with the projection $\pi_F \colon C \to A^{(F)}$ we obtain a map $\varphi \colon C \to B$. The following commutative diagram summarizes the situation for $s \in S_i$ fixed.



We have: $\pi_F \circ \delta_s = \varepsilon_i \circ \alpha_{s,i} \circ \pi_i$. So for every $s \in S$ we have that β_s is

$$\beta_{s,i} \circ \pi_i = f \circ \varepsilon_i \circ \alpha_{s,i} \circ \pi_i = f \circ \pi_F \circ \delta_s = \varphi \circ \delta_s$$

so φ satisfies the required condition. Uniqueness follows because the images of the δ_s generate C.

Suppose now R is finitely generated over $\mathbb{Z}$. From the construction of $A^{(S)}$ in proposition 1.3.7 we see that $A^{(S)}$ is finitely generated over R and hence also over $\mathbb{Z}$, so it is noetherian. Every noetherian ring is a finite product of connected rings by [14, Chapter 2, Exercise 2.13 (c)] and [14, Chapter 1, Proposition 1.5]. Write $A^{(S)}$ as $\prod_{j\in J} R_j$, with J a finite set and R_j connected. By applying the projection map $\pi_j\colon A^{(S)} \to R_j$ we get that

$$\prod_{s\in S}(X - \pi_j \circ \delta_s(a)) \mid P_a(X)$$

holds in every $R_j'[X]$, and since the R_j are connected the previous argument gives a map $\varphi_j\colon C \to B_j$ such that for all $s \in S$ we have $\pi_j \circ \alpha_s = \varphi_j \circ \delta_s$. By the universal property of the product we get a map $\varphi\colon C \to A^{(S)}$ such that for all $j \in J$ we have $\varphi_j = \pi_j \circ \varphi$. The following diagram shows the situation for j and s fixed.

$$\begin{array}{ccc} A & \xrightarrow{\delta_s} & A^{(S)} \\ {\scriptstyle\alpha_s}\downarrow & \overset{\varphi}{\nearrow} & \downarrow{\scriptstyle\pi_j} \\ C & \xrightarrow[\varphi_j]{} & R_j \end{array}$$

For all $s \in S$ and for all $j \in J$ we have $\pi_j \circ \delta_s = \pi_j \circ \varphi \circ \delta_s$, and hence the universal property of the product gives $\varphi \circ \delta_s = \delta_s$. So there exists a map $C \to A^{(S)}$ commuting with the natural maps and this is sufficient to conclude for R finitely generated over $\mathbb{Z}$.

Back to the general case: we no longer assume R to be finitely generated over $\mathbb{Z}$. The R-algebra A is finitely presented over R, so there exists a subring R_0 of R, finitely generated over $\mathbb{Z}$, and a finite R_0-algebra A_0 such that $A \cong R \otimes_{R_0} A_0$. Define the R_0-algebra C_0 in the obvious way and note that $C \cong R \otimes_{R_0} C_0$. We proved $A_0^{(S)}$ and C_0 are isomorphic and the constructions of $A^{(S)}$ and of C both commute with base change, so $A^{(S)}$ and C are isomorphic and the proof is complete. □

The product formula in [2] is now a corollary of theorem 1.4.4.

Corollary 1.4.5. *For $i = 1, \ldots, m$ let A_i be an R-algebra of rank n_i. Let A be the product of the A_i, an R-algebra of rank $n = \sum n_i$. Then the Galois closure of A satisfies*

$$A^{(n)} \cong \left(\bigotimes_{i=1}^{m} A_i^{(n_i)}\right)^{\frac{n!}{n_1!\cdots n_m!}}$$

Proof. By theorem 1.4.4 we write $A^{(n)}$ as a product indexed over maps $F\colon \{1,\dots,n\} \to \{1,\dots,m\}$. By proposition 1.3.12 a factor is not zero if and only if for all i we have $\#F^{-1}(i) = n_i$, so there are $\frac{n}{n_1!\cdots n_m!}$ non-zero factors and they are all isomorphic to $\bigotimes_i A_i^{(n_i)}$. The statement then follows from proposition 1.3.10. □

Using the product formula we can compute the S-closure of an étale R-algebra, generalizing theorem 4 in [2]. Recall from definition 1.2.4 that $s_1\colon A \to R$ denotes the trace map.

Definition 1.4.6. Let R be a ring and let A be an R-algebra of rank n. We say A is *finite étale* over R if the map $A \to A^\vee$ given by

$$a \mapsto (b \mapsto s_1(ab))$$

is an isomorphism.

Proposition 1.4.7. *Let R be a connected ring and let A be an R-algebra. Then A is finite étale if and only if there exists a finite projective R-algebra R', with $R \to R'$ injective, such that $A \otimes_R R'$ is isomorphic to $(R')^n$ as an R-algebra for some $n \geq 0$.*

Proof. See [18, Theorem 5.10]. □

Definition 1.4.8. Given a profinite group G the *category of finite G-sets* is the category whose objects are finite sets equipped with a continuous action of G, and morphisms are maps compatible with the action.

Theorem 1.4.9. *Let R be a connected ring and let K be a separably closed field. Let $\alpha\colon R \to K$ be a ring homomorphism. Then there exist*

1. *A profinite group $\pi = \pi(R, \alpha)$.*
2. *An equivalence of categories*

$$F\colon \{\text{finite étale } R\text{-algebras}\}^{\mathrm{op}} \to \{\text{finite } \pi\text{-sets}\}.$$

3. *An isomorphism of functors from $\mathrm{Hom}_{R\text{-Alg}}(-, K)$ to the composition of the forgetful functor $\{\text{finite } \pi\text{-sets}\} \to \{\text{sets}\}$ with F.*

Moreover, we have:

a. *The group π is uniquely determined up to isomorphism.*

b. *For all finite sets T we have $F(R^T) = T$ with trivial action of π.*

c. *Given finite étale R-algebras A and B the tensor product $A \otimes_R B$ is étale and $F(A \otimes_R B) = F(A) \times F(B)$ with the induced action.*

Proof. This is a combination of standard results on finite étale algebras. Results in [18, Section 5] contain everything that is needed. □

Definition 1.4.10. The group π above is called the *étale fundamental group of R in α.*

Proposition 1.4.11. *Let R be a connected ring and K a separably closed field. Let $\alpha\colon R \to K$ be a ring homomorphism and let π be the étale fundamental group of R in α. Let A be a finite étale R-algebra corresponding to a π-set T. Then for any finite set S the algebra $A^{(S)}$ is finite étale and corresponds to the set I of injective maps $S \to T$ with the action of π induced by the one on T.*

Proof. First suppose the action of π on T is trivial so that $A = R^T$. In this case by theorem 1.4.4 the S-closure of A is a product indexed over all maps $F\colon S \to T$ of the $F^{-1}(t)$-closure of R, for t in T. If F is not injective then there exists a $t \in T$ such that $F^{-1}(t)$ has at least two elements so the $F^{-1}(t)$-closure of R is zero by number *1* of proposition 1.3.12. If F is injective, then for all $t \in T$ the $F^{-1}(t)$-closure of R is R, by number *3* of proposition 1.3.12. Hence the S-closure of A is R^I.

In general, by proposition 1.4.7 there exists a finite projective R-algebra R' with $R \to R'$ injective such that $A \otimes_R R'$ is isomorphic to $(R')^n$ for some $n \geq 0$. We proved the S-closure of $(R')^n$ is isomorphic to $(R')^N$ for some N, then by proposition 1.4.7 the S-closure of A is finite étale. The π-set corresponding to $A^{(S)}$ is $\mathrm{Hom}_R(A^{(S)}, K)$, which is isomorphic to $\mathrm{Hom}_K((A \otimes_R K)^{(S)}, K)$ as π-sets. We are then reduced to proving that for A an étale algebra over K, corresponding to a set T, the S-closure of A corresponds to I. Since in this case $A = K^T$ this was proven already. □

Remark 1.4.12. Note that proposition 1.4.11 implies that if A is an étale R-algebra of rank n then $A^{(S)}$ is étale of rank $n(n-1)\cdots(n-\#S+1)$. This will be called the *expected rank* of $A^{(S)}$. For general algebras over fields it is possible that the rank of the S-closure is not the expected one. We will give examples in section 1.7.

An important consequence of the product formula is proposition 1.4.17, which says that the S-closure is not zero, excluding trivial cases. This was not previously known for the construction of Bhargava and Satriano. We need some facts about algebras over fields, which will be used also later on.

Lemma 1.4.13. *Let K be a field and let A be a finite K-algebra. Then A is isomorphic to a finite product of K-algebras $\prod_i A_i$ with A_i local with nilpotent maximal ideal.*

Proof. Follows from [8, Corollary 2.15, page 76]. It can also be proved directly as in [18, Theorem 2.6]. □

Corollary 1.4.14. *Let K be an algebraically closed field and let A be a finite K-algebra. Then A is local if and only if there exists a unique K-algebra map $A \to K$.*

Proof. Suppose A is local with maximal ideal $\mathfrak{m}$. Since A is finite over K the residue field is an algebraic extension of K. Since K is algebraically closed the residue field is K. In particular, there exists a K-algebra map $\pi\colon A \to K$. Since $A = K \oplus \mathfrak{m}$, and the kernel of any map $A \to K$ is $\mathfrak{m}$, all those maps are equal to π. So if A is local π is the unique map $A \to K$.

By lemma 1.4.13 any K-algebra A is a finite product of local algebras A_i. For each A_i we have a map $A \to A_i \to K$, and different factors give different maps. So if there is a unique map $A \to K$ there is one factor in the product, and hence A is local. □

Remark 1.4.15. Let K be algebraically closed and let A be a local K-algebra. Suppose A is integral over K, but not necessarily finite. Then the proof of corollary 1.4.14 applies without modifications with this assumption. In fact, also in this case the residue field of A is an algebraic extension of K and then it is K, and the rest follows.

Lemma 1.4.16. *Let K be an algebraically closed field and let A be a connected K-algebra of rank n. Then for all finite sets S with $0 \leq \#S \leq n$, the algebra $A^{(S)}$ is local.*

Proof. By lemma 1.4.13 and corollary 1.4.14, we have that A is local with nilpotent maximal ideal $\mathfrak{m}$ and residue field K. Let $f\colon A \to K$ be the quotient map. Any element $a \in A$ can be written as $r + m$ with $m \in \mathfrak{m}$ and $r \in K$. With this notation one has $f(a) = r$ and the characteristic polynomial of a is $(X - r)^n$. Since this is a multiple of $(X - f(a))^{\#S}$, the universal property of $A^{(S)}$ gives a unique K-algebra map $\varphi\colon A^{(S)} \to K$ such that for all $s \in S$ we have $\varphi \circ \delta_s = f$.

Any other K-algebra map $A^{(S)} \to K$ must also satisfy the same condition, and hence coincide with φ. So $A^{(S)}$ is local by corollary 1.4.14. □

Proposition 1.4.17. *Let R be a non-zero ring and A an R-algebra of rank $n > 0$. Let S be a set with $\#S \leq n$. Then $A^{(S)}$ is not zero.*

Proof. Suppose first that A is connected over an algebraically closed field. By lemma 1.4.16 in this case $A^{(S)}$ is local and hence not zero.

If A is any algebra of rank n over an algebraically closed field, then by lemma 1.4.13, we have that A is a finite product of connected K-algebras,

and by the above and the assumption on $\#S$, not all the $A^{(F)}$ in the formula in theorem 1.4.4 are zero, so $A^{(S)}$ is not zero.

Given $R \to K$ with K an algebraically closed field the non-zero algebra $(A \otimes_R K)^{(S)}$ is isomorphic to $A^{(S)} \otimes_R K$ since the S-closure commutes with base change. So $A^{(S)}$ is not zero, as we wanted to show. □

1.5 Polynomial laws

Given an R-algebra A of rank n and a sequence $n_1, \ldots, n_t$ with $\sum_i n_i = n$, Daniel Ferrand in [9] constructs an R-algebra $P^{(n_1,\ldots,n_t)}(A)$, using norms. In this section we will show that his definition is equivalent to the following: for all $R \to R'$ and all $a \in A \otimes_R R'$ the characteristic polynomial of a splits as a product of t polynomials of degrees $n_1, \ldots, n_t$ in $P^{(n_1,\ldots,n_t)}(A) \otimes_R R'[X]$, and $P^{(n_1,\ldots,n_t)}(A)$ is universal with this property. We will make this precise in proposition 1.5.11 and we will show in proposition 1.5.15 that $P^{(1,\ldots,1,n-m)}(A)$ (with m ones) is isomorphic to the m-closure of A.

The precise formulation of these results uses polynomial laws. This tool was first introduced by Norbert Roby in [24]; Daniel Ferrand in [9] gives a very clear presentation of the topic, though not as complete as the one by Roby. In this section we will just give the basic definitions and properties we need.

In [9, Lemme 4.1.1] Daniel Ferrand also proves a product formula that generalizes to $P^{(n_1,\ldots,n_t)}(A)$ the one we proved in theorem 1.4.4. We will not give a proof of this formula here.

If A is the algebra $R[x]/(f)$ for some monic polynomial f, a construction for $P^{(n_1,\ldots,n_t)}(A)$ is given by Dan Laksov in [16]. It is probably possible to generalize the construction by Laksov to define $P^{(n_1,\ldots,n_t)}(A)$ in a way similar to our definition of $A^{(m)}$, but we will not do it here.

Definition 1.5.1. Let R be a ring and let M be an R-module. We denote by $\underline{M}$ the functor R-Alg $\to$ Set sending an R-algebra S to the set $M \otimes_R S$ and a morphism $f\colon S \to S'$ to $\mathrm{Id}_M \otimes f$.

Definition 1.5.2. Let R be a ring and let M and N be two R-modules. A *polynomial law* is a natural transformation $f\colon \underline{M} \to \underline{N}$.

In detail: a polynomial law $\underline{M} \to \underline{N}$ is given by a (set-theoretical) map $f_S\colon M \otimes_R S \to N \otimes_R S$ for each R-algebra S such that for all $g\colon S \to S'$ the following diagram commutes:

$$\begin{array}{ccc} M \otimes_R S & \xrightarrow{f_S} & N \otimes_R S \\ {\scriptstyle \mathrm{Id}_M \otimes g}\downarrow & & \downarrow{\scriptstyle \mathrm{Id}_N \otimes g} \\ M \otimes_R S' & \xrightarrow[f_{S'}]{} & N \otimes_R S' \end{array}$$

Remark 1.5.3. Let R be a ring. A polynomial law $\underline{R^m} \to \underline{R^n}$ is a morphism $\mathbb{A}^m_R \to \mathbb{A}^n_R$.

Definition 1.5.4. Let R be a ring and M, N be R-modules. A polynomial law $f\colon \underline{M} \to \underline{N}$ is called *homogeneous* of degree n if for all R-algebras S, all elements $x \in M \otimes_R S$ and all elements $s \in S$ we have:

$$f_S(sx) = s^n f_S(x).$$

Example 1.5.5. Any polynomial law homogeneous of degree zero comes from a constant map $M \to N$. Any polynomial law homogeneous of degree one comes from a linear map $M \to N$. This is somehow surprising, since no additivity is required. A proof can be found in [24, Chapitre I, §11].

Remark 1.5.6. In this section a linear map $\alpha\colon M \to N$ will be seen as a polynomial law $\underline{M} \to \underline{N}$ homogeneous of degree 1. In particular given an R-algebra S the notation α_S will be used instead of $\alpha \otimes \mathrm{Id}_S$.

Definition 1.5.7. Let R be a ring and let A, B be R-algebras. A polynomial law $f\colon \underline{A} \to \underline{B}$ is called *multiplicative* if for all R-algebras S and for all elements $x, y \in A \otimes_R S$ we have:

$$f(xy) = f(x)f(y) \quad \text{and} \quad f(1) = 1$$

Example 1.5.8. Let M be a finitely generated projective R-module, then the i-th exterior power of the trace defined in remark 1.2.6 is a homogeneous polynomial law of degree i, for all i. If A is an R-algebra of rank n, then the norm map $A \to R$ is moreover multiplicative.

Proposition 1.5.9. *Let R be a ring, M a projective finitely generated R-module, and N be any R-module. Denote by S the ring* $\mathrm{Sym}(M^\vee)$. *Then for every element η in $N \otimes_R S$ there exists a unique polynomial law $f\colon \underline{M} \to \underline{N}$ such that $f_S(\gamma) = \eta$, with $\gamma \in M \otimes_R S$ the generic element of M.*

Proof. We prove uniqueness first. Let $f\colon \underline{M} \to \underline{N}$ be a polynomial law. Let R' be any R-algebra and let $x \in M' = M \otimes_R R'$. We show that knowing $f_S(\gamma)$ we can determine $f_{R'}(x)$. By proposition 1.2.21 there exists a unique R-algebra map $\varphi_x :: S \to R'$ such that $\mathrm{Id}_M \otimes \varphi_x(\gamma) = x$. By definition of polynomial law the following diagram commutes

$$\begin{array}{ccc} M \otimes S & \xrightarrow{\mathrm{Id}_M \otimes \varphi_x} & M' \\ {\scriptstyle f_S}\downarrow & & \downarrow{\scriptstyle f_{R'}} \\ N \otimes S & \xrightarrow{\mathrm{Id}_N \otimes \varphi_x} & N' \end{array}$$

Then we have $f_{R'}(x) = (\mathrm{Id}_M \otimes \varphi_x)(f_S(\gamma))$. So the claim is proved.

Now for existence, let η be in $N \otimes_R S$. For any R-algebra R' and any $x \in M'$ we define $f(x) = \mathrm{Id}_N \otimes \varphi_x(\eta)$. We need to check this is a polynomial law, i.e. that, given two R-algebras A and B, and a map $\psi\colon A \to B$ the following diagram commutes:

$$\begin{array}{ccc} M \otimes_R A & \xrightarrow{\mathrm{Id}_M \otimes \psi} & M \otimes B \\ {\scriptstyle f_A}\downarrow & & \downarrow{\scriptstyle f_B} \\ N \otimes A & \xrightarrow[\mathrm{Id}_N \otimes \psi]{} & N \otimes B \end{array}$$

Fix x in $M \otimes_R A$ and let y be $\mathrm{Id}_M \otimes \psi(x)$ in $M \otimes_R B$. The polynomial laws $\psi \circ \varphi_x$ and φ_y both have value y on γ, hence they are equal by the above. So we can write:

$$(\mathrm{Id}_N \otimes \psi)(f_A(x)) = (\mathrm{Id}_N \otimes \psi)(\mathrm{Id}_N \otimes \varphi_x(\eta)) = (\mathrm{Id}_N \otimes \varphi_y)(\eta) = f_B(y)$$

and since $f_B(y) = f_B(\mathrm{Id}_M \otimes \psi(x))$, the diagram commutes as we wanted to show. □

Remark 1.5.10. The set $\mathscr{P}(M, N)$ of polynomial laws $\underline{M} \to \underline{N}$ has a natural structure of graded R-module, the degree n part being homogeneous polynomial laws of degree n. If M is a projective finitely generated module, proposition 1.5.9 gives an isomorphism

$$\mathscr{P}(M, N) \cong N \otimes_R \mathrm{Sym}(M^\vee)$$

and this clearly respects the natural grading on both sides. Moreover if B is an R-algebra, then $\mathscr{P}(M, B)$ has a structure of graded R-algebra, and it is isomorphic to $B \otimes_R \mathrm{Sym}(M^\vee)$ as a graded R-algebras.

Recall that given R-algebras $R \to A$ and $R \to S$, with A finite locally free, and an element a in $A \otimes_R S$, we denote by $P_a \in S[X]$ the characteristic polynomial of a. If f is the endomorphism of $A \otimes_R S$ given by multiplication by a this is defined as the determinant of the endomorphism $(\mathrm{Id} \otimes X - f \otimes \mathrm{Id})$. Equivalently, we can write it as the image of $(X - a) \in A \otimes_R S[X]$ via the polynomial law s_n. We can now give the definition of $A^{(n_1,\dots,n_t)}$.

Proposition 1.5.11. *Let A be an R-algebra of rank n. Let C be an R-algebra and let $\delta_i\colon \underline{A} \to \underline{C}$ for $i = 1, \dots, t$ be polynomial laws. Suppose δ_i is homogeneous of degree n_i and that $\sum n_i$ is n. Then the following are equivalent:*

1. *The equality $s_n = \prod \delta_i$ holds (as polynomial laws) and $(C, (\delta_i)_i)$ is universal with this property.*
2. *For all $R \to S$ and for all $a \in A \otimes_R S$ we have*

$$P_a(X) = \prod_i \delta_{i,S[X]}(X - a)$$

in $C \otimes_R S[X]$ *and* $(C, (\delta_i)_i)$ *is universal with this property.*

3. *Let* η_i *be the element of* $C \otimes_R \mathrm{Sym}(A^\vee)$ *corresponding to* δ_i *and let* det *be the one corresponding to* s_n*. Then* det *is equal to the product of the* η_i *in* $C \otimes_R \mathrm{Sym}(A^\vee)$ *and* $(C, (\delta_i)_i)$ *is universal with this property.*

Proof. The first two statements are equivalent because $P_a(X)$ is equal to $s_{n,S[X]}(X-a)$, the constant term of $P_a(X)$ is $(-1)^n s_{n,S}(a)$ and the constant term of the product in *2* is

$$\prod_i (-1)^{n_i} \delta_{i,S}(a) = (-1)^n \prod \delta_{i,S}(a)$$

The third is equivalent with the first by proposition 1.5.9 and remark 1.5.10. □

Definition 1.5.12. Given $n_1, \ldots, n_t$, with $\sum n_i = n$, an algebra satisfying the equivalent conditions in proposition 1.5.11 will be denoted $A^{(n_1,\ldots,n_t)}$.

To connect the m-closures with the constructions above we will show in proposition 1.5.15 that the m-closure $A^{(m)}$ of an R-algebra of rank n is isomorphic to $A^{(1,\ldots,1,n-m)}$ (with m ones). The following two lemmas come from Ferrand [9] (see Règle 4.2.3).

Lemma 1.5.13. *Let* A *be an* R*-algebra of rank* n *and* B *be any* R*-algebra. Let* $f, g, h \colon \underline{A} \to \underline{B}$ *be polynomial laws. Suppose we have*

$$s_n = fg = fh$$

as polynomial laws. Then g *is equal to* h*.*

Proof. Let S be an R-algebra and let x be in $A \otimes_R S$. Then we have

$$s_{n,S[X]}(X+x) = f_{S[X]}(X+x) g_{S[X]}(X+x) = f_{S[X]}(X+x) h_{S[X]}(X+x)$$

The left hand side is monic because s_n is multiplicative. Hence its factor $f_{S[X]}(X+x)$ is a regular element of $B \otimes_R R'[X]$ (that is: it is not a right nor a left zero divisor), so the equality above implies $g_{S[X]}(X+x) = h_{S[X]}(X+x)$. Then the specialization $X \mapsto 0$ implies that $g_S(x) = h_S(x)$. Since x was arbitrary, the proof is complete. □

Lemma 1.5.14. *Let* A *be an* R*-algebra of rank* n *and* B *be any* R*-algebra. Let* $f, g \colon \underline{A} \to \underline{B}$ *be polynomial laws, with* f *multiplicative. Suppose we have*

$$s_n = fg$$

as polynomial laws. Then g *is multiplicative.*

Proof. As in the proof of lemma 1.5.13, for all $R \to S$ and x, y in $A \otimes_R S$ we have $f_{S[X]}(X + x)$ and $f_{S[X]}(X + y)$ are regular and their product is

$$f_{S[X]}(X^2 + (x + y)X + xy).$$

So we have

$$g_{S[X]}(X^2 + (x + y)X + xy) = g_{S[X]}(X + x)g_{S[X]}(X + y)$$

because the product of both with $f_{S[X]}(X^2 + (x + y)X + xy)$ is equal to $s_{n,S[X]}(X^2 + (x + y)X + xy)$. With the specialization $X \mapsto 0$ we get $g(xy) = g(x)g(y)$, as we wanted to show. □

We are now ready to compare the algebras $A^{(1,\dots,1,n-m)}$ and $A^{(m)}$.

Proposition 1.5.15. *Let A be an R-algebra of rank n. Then for all $m = 1, \dots, n$ we have $A^{(m)} \cong A^{(1,\dots,1,n-m)}$.*

Proof. Recall that $A^{(m)}$ is given with R-algebra maps $\alpha_i \colon A \to A^{(m)}$ for $i = 1, \dots, m$. We define a polynomial law $\alpha \colon A \to A^{(m)}$, multiplicative and homogeneous of degree $n - m$ and such that $\alpha \prod_i \alpha_i$ is equal to s_n. Let $\gamma \in A \otimes \mathrm{Sym}(A^\vee)$ be the generic element of A. By the universal property of $A^{(m)}$ we have that in $A^{(m)} \otimes \mathrm{Sym}(A^\vee)[X]$ the characteristic polynomial $P_\gamma(X)$ is equal to

$$Q_\gamma(X) \prod_{i=1}^{m} (X - \alpha_{i,\mathrm{Sym}(A^\vee)}(\gamma))$$

for some polynomial $Q_\gamma(X)$. The constant term of $Q_\gamma(X)$ is an element η of $A^{(m)} \otimes \mathrm{Sym}(A^\vee)$, and by proposition 1.5.9 this defines a unique polynomial law $\alpha \colon \underline{A} \to \underline{A^{(m)}}$. This is homogeneous of degree $n - m$ because η is homogeneous of degree $n - m$ since the constant term of P_γ is homogeneous of degree n and the constant term of $\prod(X - \alpha_{i,\mathrm{Sym}(A^\vee)}(\gamma))$ is homogeneous of degree m. Moreover α is multiplicative by lemma 1.5.14.

We are left to show that $A^{(m)}$ with the maps α_i and the polynomial law α has the universal property of $A^{(1,\dots,1,n-m)}$. For every $R \to S$ and every element $a \in A \otimes_R S$ the characteristic polynomial of a splits as

$$\alpha_{S[X]}(X - a) \prod_{i=1}^{m} (X - \alpha_{i,S}(a)) = \alpha_{S[X]}(X - a) \prod_{i=1}^{m} \alpha_{i,S[X]}(X - a).$$

Let B be an R-algebra given with linear maps $\beta_i \colon A \to B$ and a polynomial law $\beta \colon A \to B$ homogeneous of degree $n - m$. Suppose that for all $R \to S$ and all $a \in A \otimes_R A$ the polynomial $P_a(X)$ splits as

$$\beta_{S[X]}(X - a) \prod_i \beta_{i,S[X]}(X - a)$$

in $B[X]$. Since for all i we have $\beta_{i,S[X]}(X-a) = (X - \beta_{i,S}(a))$ by linearity, the universal property of $A^{(m)}$ gives a unique map $\varphi\colon A^{(m)} \to B$ such that for all i we have $\varphi \circ \alpha_i = \beta_i$. Since s_n is equal to both $(\varphi \circ \alpha)\prod_i \beta_i$ and $\beta \prod_i \beta_i$, by lemma 1.5.13 we have $\varphi \circ \alpha = \beta$, so the proof is complete. □

We have not shown existence of the algebras $A^{(n_1,\dots,n_t)}$. This is done by Daniel Ferrand in [9, §4.1], and we will not write it here.

1.6 Monogenic algebras

Let R be a ring and let f be a monic polynomial with coefficients in R. In this section we will describe explicitly the closures of the R-algebra $R[x]/(f)$ (a *monogenic* R-algebra). To do this an important tool is the following lemma.

Recall that for P and Q in $R[X]$ we write $P \mid Q$ for P divides Q.

Lemma (Lemma 1.6.5)**.** *Let R be a ring, and let g be a polynomial with coefficients in R. Let M be a free R-module of rank n and $\alpha \in \mathrm{End}(M)$. Let $a_i \in R$ for $i = 1, \dots m$. Suppose that*

$$\prod_{i=1}^{m}(X - a_i) \mid P_\alpha(X)$$

in $R[X]$, then also

$$\prod_{i=1}^{m}(X - g(a_i)) \mid P_{g(\alpha)}(X)$$

in $R[X]$.

We will need some preliminary results.

Definition 1.6.1. Let R be a ring. We denote by $R[Z]_n^{\mathrm{mon}}$ the set of monic polynomials of degree n in $R[Z]$.

Theorem 1.6.2. *Let $g \in R[X]$. For all $n \geq 0$ there exists a unique collection of maps $(\varphi_{n,A})_A$ indexed over all R-algebras A, with $\varphi_{n,A}\colon A[Z]_n^{\mathrm{mon}} \to A[Z]_n^{\mathrm{mon}}$, satisfying the following conditions:*

1. *For all $A \to B$ the diagram*

$$\begin{array}{ccc} A[Z]_n^{\mathrm{mon}} & \longrightarrow & B[Z]_n^{\mathrm{mon}} \\ \downarrow{\scriptstyle \varphi_{n,A}} & & \downarrow{\scriptstyle \varphi_{n,B}} \\ A[Z]_n^{\mathrm{mon}} & \longrightarrow & B[Z]_n^{\mathrm{mon}} \end{array}$$

   commutes.

2. For all $a_i \in A$ with $i = 1, \ldots, n$ we have

$$\varphi_{n,A}\left(\prod_{i=1}^{n}(Z - a_i)\right) = \prod_{i=1}^{n}(Z - g(a_i))\,.$$

Moreover, for all $n, m \geq 0$, for all $R \to A$, for all $f \in A[Z]_n^{\mathrm{mon}}$ and for all $g \in A[Z]_m^{\mathrm{mon}}$ we have

$$\varphi_n(f)\varphi_m(g) = \varphi_{n+m}(fg)$$

in $A[Z]_{n+m}^{\mathrm{mon}}$.

Proof. We prove uniqueness first. Suppose a map φ_n is given, having the properties above. Let T be the R-algebra $R[X_1, \ldots, X_n]$, and let Δ be the polynomial $\prod_i (Z - X_i)$ in $T[Z]_n^{\mathrm{mon}}$. By property *2* we have

$$\varphi_{n,T}(\Delta) = \prod_{i=1}^{n}(Z - g(X_i)).$$

Note that Δ can be written as

$$Z^n - s_1 Z^{n-1} + s_2 Z^{n-2} + \cdots + (-1)^n s_n$$

where s_i is the i-th elementary symmetric function in the X_i. Since $\prod_{i=1}^{n}(Z - g(X_i))$ is invariant under permutations of the X_i, by the fundamental theorem of symmetric functions (see [4, §6, Théorème 1]), there exist q_i in $S = R[s_1, \ldots, s_n]$ for $i = 1, \ldots, n$ such that

$$\varphi_{n,T}(\Delta) = Z^n + \sum_{i=1}^{n} q_i Z^{n-i}.$$

Now let A be any R-algebra and let

$$P = Z^n + \sum_{i=1}^{n}(-1)^i a_i Z^{n-1}$$

be a polynomial in $A[Z]_n^{\mathrm{mon}}$. Let π be the map $S \to A$ sending s_i to a_i. Note that $\pi(\Delta)$ is equal to P, so by property *1* we have that

$$\varphi_{n,A}(P) = \pi(\varphi_{n,T}(\Delta))$$

in $A[Z]_n^{\mathrm{mon}}$. Hence uniqueness follows.

In proving uniqueness we also have constructed a map having properties *1* and *2*, so existence is proved.

We now prove the last part. Let T be $R[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$, and define

$$\Delta_X = \prod_{i=1}^{n}(Z - X_i), \qquad \Delta_Y = \prod_{i=1}^{m}(Z - Y_i)$$

in $T[Z]_n^{\mathrm{mon}}$ and $T[Z]_m^{\mathrm{mon}}$ respectively. Note that we have

$$\Delta_X = Z^n + \sum_{i=1}^{n}(-1)^i s_i Z^{n-i}, \quad \Delta_Y = Z^m + \sum_{i=1}^{m}(-1)^i t_i Z^{m-i}$$

where s_i is the i-th elementary symmetric function in the X_i for $i = 1, \ldots, n$ and t_i is the i-th elementary symmetric function in the Y_i for $i = 1, \ldots, m$. Denote by S the subring $R[s_1, \ldots, s_n, t_1, \ldots, t_m]$ of T. Note that $\varphi_{n,T}(\Delta_X)$ and $\varphi_{n,T}(\Delta_Y)$ also have coefficients in S. By property *2* we have

$$\varphi_{T,n+m}(\Delta_X \Delta_Y) = \varphi_{T,n}(\Delta_X)\varphi_{T,m}(\Delta_Y)$$

in $T[Z]_{n+m}^{\mathrm{mon}}$, so the same holds in $S[Z]_{n+m}^{\mathrm{mon}}$.

For an R-algebra A and polynomials

$$f = Z^n + \sum_{i=1}^{n}(-1)^i a_i Z^{n-i}, \quad g = Z^m + \sum_{i=1}^{m}(-1)^i b_i Z^{m-i}$$

in $A[Z]_n^{\mathrm{mon}}$ and $A[Z]_m^{\mathrm{mon}}$ respectively, let π be the map $S \to A$ sending s_i to a_i for all $i = 1 \ldots, n$ and t_i to b_i for all $i = 1, \ldots, m$. Clearly π sends Δ_X to f and Δ_Y to g. Hence by property *1*, we have that $\varphi_{A,n}(f)\varphi_{A,m}(g) = \varphi_{A,n+m}(fg)$. The proof is complete. □

Example 1.6.3. We give an example to illustrate theorem 1.6.2. Let R be $\mathbb{Z}$ and g be X^2. For $n = 3$ consider

$$(Z - a)(Z - b)(Z - c)$$

in $A[Z]_3^{\mathrm{mon}}$ for some R-algebra A. The product

$$(Z - a^2)(Z - b^2)(Z - c^2)$$

is equal to

$$Z^3 - (a^2 + b^2 + c^2)Z^2 + (a^2b^2 + a^2c^2 + b^2c^2)Z - a^2b^2c^2Z^3$$

and for s_1, s_2, s_3 the elementary symmetric functions in a, b, c this is

$$Z^3 - (s_1^2 - 2s_2)Z^2 + (s_2^2 - 2s_1s_3)Z - s_3^2Z^3.$$

So the map $\varphi_{3,A}$ sends a polynomial

$$Z^3 - r_1Z^2 + r_2Z - r_3$$

in $A[Z]_3^{\mathrm{mon}}$ to

$$Z^3 - (r_1^2 - 2r_2)Z^2 + (r_2^2 - 2r_1r_3)Z - r_3^2Z^3.$$

Lemma 1.6.4. *Let R be a ring and g be a polynomial with coefficients in R. Let M be a free R-module of rank n and $\alpha \in \mathrm{End}(M)$. Then $\varphi_{R,n}\colon R[Z]_n^{\mathrm{mon}} \to R[Z]_n^{\mathrm{mon}}$ sends $P_\alpha(Z)$ to $P_{g(\alpha)}(Z)$.*

Proof. Suppose first that R is an algebraically closed field. We can write P_α as

$$\prod_{i=1,\dots,s} (Z - a_i)^{e_i}$$

for some $a_i \in R$ and $e_i > 0$ and since we can write the matrix representing α in Jordan normal form we have that $P_{g(\alpha)}(Z)$ is

$$\prod_{i=1,\dots,s} (Z - g(a_i))^{e_i}$$

Then the statement follows from theorem 1.6.2.

Next suppose R is the ring $\mathbb{Z}[(X_{r,s})_{r,s=1,\dots,n}]$ and α is the endomorphism given by the matrix $X = (X_{r,s})_{r,s}$. Consider the embedding $i\colon R \to K$, of R into the algebraic closure of its quotient field. Since $\varphi_{K,n}(i(P_X))$ is $i(P_{g(X)})$ and i is injective. By property *1* in theorem 1.6.2 we have that $\varphi_{R,n}(P_X)$ is equal to $P_{g(X)}$, as we wanted to show.

For a general ring choose a basis of M and write α as a matrix, say $\alpha = (a_{r,s})_{r,s=1,\dots,n}$. Let π be the map $\mathbb{Z}[(X_{r,s})_{r,s=1,\dots,n}] \to R$ sending $X_{r,s}$ to $a_{r,s}$. The map π sends P_X to P_α and $P_{g(X)}$ to $P_{g(\alpha)}$. By property *1* of $\varphi_{R,n}$ in theorem 1.6.2 we conclude that $\varphi_R(P_\alpha) = P_{g(\alpha)}$, as we wanted to show. □

Lemma 1.6.5. *Let R be a ring, and let g be a polynomial with coefficients in R. Let M be a free R-module of rank n and $\alpha \in \mathrm{End}(M)$. Let $a_i \in R$ for $i = 1, \dots m$. Suppose that*

$$\prod_{i=1}^{m} (Z - a_i) \mid P_\alpha(Z)$$

in $R[Z]$, then also

$$\prod_{i=1}^{m} (Z - g(a_i)) \mid P_{g(\alpha)}(Z)$$

in $R[Z]$.

Proof. By assumption there exists a polynomial Q in $R[Z]$ such that

$$P_\alpha(Z) = Q(Z) \prod_{i=1}^{m} (Z - a_i).$$

Since both P_α and $\prod_i (Z - a_i)$ are monic also Q must be monic. Then by theorem 1.6.2 we have that

$$\varphi_{R,n}\left(Q(Z)\prod_{i=1}^{m}(Z-a_i)\right) = \varphi_{R,n-m}\left(Q(Z)\right)\varphi_{R,m}\left(\prod_{i=1}^{m}(Z-a_i)\right).$$

By lemma 1.6.4 we have

$$\varphi_{R,n}\left(P_\alpha(Z)\right) = P_{g(\alpha)}(Z)$$

and by property *2* in theorem 1.6.2 we have

$$\varphi_{R,m}\left(\prod_{i=1}^{m}(Z-a_i)\right) = \prod_{i=1}^{m}(Z-g(a_i)).$$

So the claim is proved. □

We use lemma 1.6.5 to give an equivalent universal property for $A^{(m)}$ when A is monogenic.

Proposition 1.6.6. *Let R be a ring, and let A be $R[x]/f(x)$, with f a monic polynomial. Let C be an R-algebra and let $\zeta_i \colon A \to C$ for $i = 1, \ldots, m$ be R-algebra maps. Suppose $\prod_i (X - \zeta_i(x))$ divides $f(X)$ in $C[X]$, and the pair $(C, (\zeta_i)_{i=1,\ldots,m})$ is universal with this property. Then $(C, (\zeta_i)_{i=1,\ldots,m})$ is an m-closure of A.*

Proof. Note that $P_x(X)$ is equal to $f(X)$. The theorem now follows from lemma 1.6.5, since for every $R \to R'$ and any element $a \in A \otimes_R R'$ there exists a polynomial $g(X)$ in $R'[X]$ such that $g(x \otimes 1)$ is a. □

We can now give an explicit form for the m-closure of a monogenic algebra. The construction is the same we described in section 1.1 for fields; we recall it here: let R be a ring and let f be a monic polynomial in $R[X]$. Put $A_0 = R$ and $f_0 = f$. Given A_i and f_i for $i \geq 0$, define A_{i+1} to be $A_i[x_{i+1}]/f_i$, and f_{i+1} as the quotient

$$f_{i+1}(X) = \frac{f_i(X)}{(X - x_{i+1})}$$

in $A_{i+1}[X]$. We show that A_m is the m-closure of $R[x]/f$.

Theorem 1.6.7. *Let R be a ring, and let f be a monic polynomial in $R[X]$. Let m be between 0 and n and define maps $\alpha_i \colon R[X]/(f) \to A_m$ for $i = 1, \ldots, n$ sending x to x_i. Then A_m together with the α_i is the m-closure of $R[X]/(f)$.*

Proof. Note that the α_i are well defined since for all i we have $f(x_i) = 0$ in A_m. For the same reason $\prod_i (X - x_i)$ divides f in $A_m[X]$, so we only need to prove A_m is universal with this property.

Let B be an R-algebra given with maps $\beta_i \colon A \to B$ for $i = 1, \ldots, m$ and such that $\prod_i (X - \beta_i(x))$ divides f in $B[X]$. We need to prove there exists a unique map $\varphi \colon A_m \to B$ such that for every i we have $\beta_i = \varphi \circ \alpha_i$.

We prove existence by induction on m: if $m = 0$, then $A_0 = R$ and the unique map $R \to B$ is the required one. Suppose we have a map $\varphi \colon A_{m-1} \to B$ satisfying $\beta_i = \varphi \circ \alpha_i$ for $i = 1, \ldots, m-1$. Consider the induced map $A_{m-1}[X] \to B[X]$ and compose with the map $B[X] \to B$ sending X to $\beta_m(x)$. Since $\beta_m(x)$ is a root of f_{m-1} in $B[X]$, this map factors through A_m, giving the required map.

Any R-algebra map with this property sends x_i to $\beta_i(x)$ and hence coincides with φ because the x_i generate A_m, so the proof is complete. □

Corollary 1.6.8. *Let R be a ring and f be a monic polynomial in $R[X]$ of degree n. Let A be the R-algebra $R[X]/(f)$. Then for all $0 \leq m \leq n$ the algebra $A^{(m)}$ is free of rank $n(n-1)\cdots(n-m+1)$.*

Proof. This follows by induction since the description given above tells us that $A^{(i)}$ is free of rank $n - i + 1$ over $A^{(i-1)}$ for all $1 \leq i \leq n$. □

1.7 Examples and explicit computations

In this section we will see some explicit computations of S-closures, together with some techniques to simplify the computations.

Recall that for A an R-algebra and S any set we denote by $A^{\otimes S}$ the tensor power of A indexed over S, defined in definition 1.2.12, and for each $s \in S$ we denote by ε_s the natural map.

Lemma 1.7.1. *Let R be a ring and A be an R-algebra of rank n. Let r be in R and $a \in A$. For any finite set S define*

$$\Delta_a = \prod_{s \in S} (X - \varepsilon_s(a)).$$

Then $\Delta_a(X) \mid P_a(X)$ if and only if $\Delta_{a+r}(X) \mid P_{a+r}(X)$.

Proof. Note that $P_{a+r}(X) = P_a(X - r)$ and $\Delta_{a+r}(X) = \Delta_a(X - r)$. The statement is then clear. □

Remark 1.7.2. Let $P(X)$ be a polynomial with coefficients in a ring R and let $r_1, \ldots, r_m$ be in R with m at most equal to the degree of P. Define

$$\Delta(X) = \prod_{i=1}^{m}(X - r_i).$$

We find an expression for the remainder of the division of $P(X)$ by $\Delta(X)$. Write

$$P(X) = Q(X)\Delta(X) + T(X)$$

with degree of $T(X)$ smaller than m. Note that $Q(X)$ and $T(X)$ are uniquely determined by these properties.

Let $Q_0(X)$ be $P(X)$ and for all $i \geq 1$ define

$$Q_i(X) = \frac{Q_{i-1}(X)}{(X - r_i)}.$$

The remainder in the division of $P(X)$ by $(X - r_1)$ is $P(r_1)$, so we can write:

$$P(X) = Q_1(X)(X - r_1) + Q_0(r_1)$$

Dividing $Q_1(X)$ by $(X - r_2)$ we get:

$$Q_1(X) = Q_2(X)(X - r_2) + Q_1(r_2)$$

so that we have

$$P(X) = Q_2(X)(X - r_1)(X - r_2) + Q_1(r_2)(X - r_1)$$

and by uniqueness, the quotient and remainder of the division of $P(X)$ by $(X - r_1)(X - r_2)$ are $Q_2(X)$ and $Q_1(r_2)(X - r_1)$ respectively.

In the same way we can determine $Q(X)$ and $T(X)$ as follows:

$$P(X) = Q_m(X)\Delta(X) + \sum_{i=0}^{m-1}\left(Q_i(r_{i+1})\prod_{k=1}^{i}(X - r_k)\right).$$

This will be used to describe $A^{(S)}$ explicitly.

Explicit generators of $J^{(S)}$

Let R be a ring and A be an R-algebra of rank n. As we proved in proposition 1.3.7, the S-closure of A is the quotient of $A^{\otimes S}$ by an ideal that we denoted $J^{(S)}$. For convenience we recall the definition of $J^{(S)}$ when A is *free* of rank n (see 1.3.6 and example 1.3.9). Let $e_1, \ldots, e_n$ be a basis of A and let $X_1, \ldots, X_n$ be the dual basis. Let $\gamma \in A[X_1, \ldots, X_n]$ be the generic element

of A and let P_γ be its characteristic polynomial. Let ε_s be the natural map $A \to A^{\otimes S}$ and define

$$\Delta_\gamma(Z) = \prod_{s \in S} (Z - \varepsilon_s \otimes \mathrm{Id}(\gamma))$$

in $A^{\otimes S}[X_1, \ldots, X_n, Z]$. For a multi-index $I = (i_1, \ldots, i_n)$ write X^I for $X_1^{i_1} \cdots X_n^{i_n}$. Let T_γ be the remainder in the division of P_γ by Δ_γ in the ring $A^{\otimes S}[X_1, \ldots, X_n, Z]$. Write the coefficient of Z^i in T_γ as $\sum a_{I,i} X^I$ for I ranging over multi-indices as above. Then $J^{(S)}$ is the ideal of $A^{\otimes S}$ generated by the $a_{I,i}$.

We compute a set of generators of $J^{(S)}$ in case A is a connected algebra of rank n over a field K. Recall from lemma 1.4.13 that in this case A is local with nilpotent maximal ideal. For simplicity we will also take $S = \{1, \ldots, m\}$, and suppose $m \leq n$.

Choose a basis $e_1, e_2, \ldots, e_n$ of A such that $e_1 = 1$, and $e_2, \ldots, e_n$ are in $\mathfrak{m}$, and let $X_1, \ldots, X_n$ be the dual basis. The element $\gamma \in A[X_1, \ldots, X_n]$ can be written as $\sum e_i X_i$, as we have seen in example 1.2.18 and example 1.2.22. Denote by γ' the difference $\gamma - e_1 X_1$, and define in the obvious way the polynomials

$$P_{\gamma'}(Z), \quad \Delta_{\gamma'}(Z), \quad T_{\gamma'}(Z)$$

in $A[X_1, \ldots, X_n, Z]$. Write $\sum a'_{I,i} X^I$ for the coefficient of Z^i in $T_{\gamma'}(Z)$ and let $J^{(m)'}$ be the ideal of $A^{\otimes S}$ generated by the $a'_{I,i}$. By lemma 1.7.1 we have that $\Delta_{\gamma'}$ divides $P_{\gamma'}$ if and only if Δ_γ divides P_γ so we can repeat the argument in proposition 1.3.7 with $J^{(m)'}$ and we get that $A^{\otimes m}/J^{(m)'}$ is the m-closure of A.

Let γ'_i be the image of γ' via the i-th natural map from $A[X_1, \ldots, X_n]$ to the tensor power $A^{\otimes m}[X_1, \ldots, X_n]$. By remark 1.7.2 we can write

$$T_{\gamma'}(Z) = \sum_{i=0}^{m-1} \left(Q_i(\gamma'_{i+1}) \prod_{k=1}^{i} (Z - \gamma'_k) \right).$$

and the ideal generated by the coefficients of $T_{\gamma'}$ is equal to the ideal generated by the coefficients of $Q_i(\gamma'_{i+1})$.

Note that since $e_2, \ldots, e_n$ are nilpotent $P_{\gamma'}(Z)$ is equal to Z^n. For $i \geq 0$ and $k = 1, \ldots, n$ define $d_i(\gamma'_1, \ldots, \gamma'_k)$ to be the sum of all monomials of degree i in the variables $\gamma'_1, \ldots, \gamma'_k$. Then we have

$$Q_i(\gamma'_{i+1}) = d_{n-i}(\gamma'_1, \ldots, \gamma'_{i+1}) \in A^{\otimes m}[X_1, \ldots, X_n] \tag{1}$$

for all $i = 1, \ldots, m-1$. So $A^{(m)}$ is the quotient of $A^{\otimes m}$ by the ideal generated by the coefficients of these polynomials.

Example 1.7.3. For an R-algebra A of rank n in remark 1.3.11 we defined $G^{(m)}(A/R)$ to be the quotient of $A^{\otimes m}$ by the ideal I generated by the coefficients of the remainder in the division of P_a by $\prod_{i=1}^{m}(X-\varepsilon_i(a))$, with a ranging over A. In remark 1.3.11 we said that this construction, modeled on the one by Bhargava and Satriano, does not in general commute with base change for $m < n$. We are going to give an example here.

Let A be the $\mathbb{F}_2$-algebra $\mathbb{F}_2[X_1,\dots,X_4]/(X_1,\dots,X_4)^2$. We show that while $G^{(3)}(A/\mathbb{F}_2)$ has dimension 110, the dimension of $G^{(3)}(A\otimes_{\mathbb{F}_2}\mathbb{F}_4/\mathbb{F}_4)$ is at most 109, so this construction does not commute with base change.

Let $\mathfrak{m}$ be the maximal ideal of A. Since any element x in A can be written as $x = r + m$, with $r \in \mathbb{F}_2$ and m in $\mathfrak{m}$, by lemma 1.7.1 we can generate the ideal I with the coefficients of the remainder in the division of P_a by $\prod_{i=1}^{m}(X-\varepsilon_i(a))$, with a ranging over $\mathfrak{m}$, instead of A. Since the characteristic polynomial of $a \in \mathfrak{m}$ is X^5, the computations we did for $Q_i(\gamma'_{i+1})$ apply here as well. Then we have

$$I = \left\langle \sum_{i+j=4} a^i \otimes a^j \otimes 1,\ \sum_{i+j+k=3} a^i \otimes a^j \otimes a^k \mid a \in \mathfrak{m} \right\rangle.$$

But since multiplication of any two elements in $\mathfrak{m}$ is zero, most of the terms in the expressions above are zero and we get

$$I = \langle a \otimes a \otimes a \mid a \in \mathfrak{m} \rangle.$$

Moreover for all $x = r + m \in A^{\otimes 3}$ we have that $x(a\otimes a\otimes a)$ is equal to $r(a\otimes a\otimes a)$ for some $r \in R$, since a multiplied by any element in $\mathfrak{m}$ is zero, so the ideal I equals the $\mathbb{F}_2$-vector space generated by the $a\otimes a\otimes a$. Then I is a vector space generated by 15 non-zero vectors. So its dimension is at most 15, and the dimension of $G^{(3)}(A/\mathbb{F}_2)$ is at least $125-15=110$ (in fact it is 110).

Now consider the same construction over $\mathbb{F}_4$. Here $G^{(3)}(A\otimes_{\mathbb{F}_2}\mathbb{F}_4/\mathbb{F}_4)$ is equal to the quotient of $A^{\otimes 3}\otimes_{\mathbb{F}_2}\mathbb{F}_4$ by the ideal

$$J = \langle a \otimes a \otimes a \mid a \in \mathfrak{m} \otimes_{\mathbb{F}_2} \mathbb{F}_4 \rangle$$

but in this case the dimension of J is at least 16. In fact, consider the projection π from $(\mathfrak{m}\otimes_{\mathbb{F}_2}\mathbb{F}_4)^{\otimes 3}$ to the quotient $\mathrm{Sym}^3(\mathfrak{m}\otimes_{\mathbb{F}_2}\mathbb{F}_4)$, which is isomorphic to $(\mathbb{F}_4[T_1,T_2,T_3,T_4])_3$, the 20-dimensional vector space of homogeneous polynomials of degree 3 in 4 variables over $\mathbb{F}_4$. The subspace $\pi(W)$ is generated by third powers of polynomials of degree 1. Consider

$$\left(\sum_{i=1}^{4} r_i T_i\right)^3 = \left(\sum_{i=1}^{4} r_i^2 T_i^2\right)\left(\sum_{i=1}^{4} r_i T_i\right) = \sum_{i,j} r_i^2 r_j T_i^2 T_j$$

with r_i in $\mathbb{F}_4$. A computation shows that a basis for $\pi(W)$ is

$$\{T_1^3, T_2^3, T_3^3, T_4^3,$$
$$T_1^2T_2, T_1^2T_3, T_1^2T_4, T_2^2T_3, T_2^2T_4, T_3^2T_4,$$
$$T_1T_2^2, T_1T_3^2, T_1T_4^2, T_2T_3^2, T_2T_4^2, T_3T_4^2\}$$

so it has dimension 16. Hence there exists a surjective map from W to a space of dimension 16, and the dimension of W is at least 16. Then the algebra $G^{(3)}(A \otimes_{\mathbb{F}_2} \mathbb{F}_4/\mathbb{F}_4)$ has dimension at most $125 - 16 = 109$ (in fact the dimension is 105). So this construction does not commute with base change.

Algorithm for computing S-closures

As we pointed out in example 1.3.9 the construction using the generic element given in section 1.3 is completely explicit. To illustrate this, we give here an implementation of the construction using MAGMA [3]. The following code, has as input a finite commutative algebra A over a field K, given with generators and relations, and an integer m. As output it returns the m-closure of A. In the implementation, we use the MAGMA command `Algebra`, which computes a basis and the multiplication table of the input algebra A.

```
// Function: mClosure. Given an affine algebra A over a field K and an
// integer m returns the m-closure of A.

mClosure := function(A, m)

// Preliminaries
relations := Generators( DivisorIdeal( A ) ); // Relations in A
gen := Rank( A ); // Number of generators in A
K := CoefficientRing( A ); // Base ring of A
// The ring A as a K-vector space (B) and the bijection A -> B
B, f := Algebra( A );
fInv := Inverse( f );
d := Dimension( B ); // The dimension of B over K

// Vector with multiplication matrices for basis elements in B
Mat := [ Matrix( K, d, d, [ ElementToSequence( B.i * B.j ) : i in
[1..d] ] ) : j in [1..d] ];

// Construction of the m-th tensor power of A
// Polynomial ring for defining the tensor power
PolyRing := PolynomialRing( K, m * gen );
// Sequence with variables in PolyRing
x := [ [ PolyRing.(i+m*j-m) : i in [1..m] ] : j in [1..gen] ];
// Relations between elements in x
TensorPowerAlgebra := quo< PolyRing | [ Evaluate( rel, [ x[i][j] :
i in [1..gen] ]) : j in [1..m ], rel in relations ] >;
```

```
// Embeddings of A into the tensor power
alpha := [ hom< A -> TensorPowerAlgebra | [ TensorPowerAlgebra!(x[i][j])
: i in [1..gen] ] > : j in [1..m] ];

// The ring where the coefficients of Delta and the characteristic
// polynomial of the generic element live
GenericRing := PolynomialRing( TensorPowerAlgebra, d );
// The matrix of multiplication by the generic element
MultMat := Matrix( GenericRing, d, d, [ [ &+ [ GenericRing.n *
GenericRing!Mat[n][j][i] : n in [1..d] ] : i in [1..d] ] :
j in [1..d] ] );

// Construction of Delta and characteristic polynomial of gamma
// Polynomial ring with coefficients in GenericRing
Polynom<X> := PolynomialRing( GenericRing );
// a sequence gamma with gamma[i] the i-th embedding of gamma in GenericRing
gamma := [ &+ [ GenericRing!(alpha[i](fInv(Basis(B)[j]))) *
GenericRing.(j) : j in [1..d] ] : i in [1..m] ];
// The polynomial Delta
if m ne 0 then
Delta := &* [ X - gamma[i] : i in [1..m] ];
else Delta := Polynom!1;
end if;
// Characteristic polynomial of the generic element
CharPoly := CharacteristicPolynomial( MultMat );

// Computation of the coefficients of the remainder in the division of
// CharPoly by Delta (the relations to quotient out)
CoeffRemainder := Coefficients(Polynom!CharPoly mod Delta);
ClosureRelations := [];
for i in [1..#CoeffRemainder] do
ClosureRelations := ClosureRelations cat Coefficients(CoeffRemainder[i]);
end for;

// Final computation of A^{(m)}
Am := quo< TensorPowerAlgebra | ClosureRelations >;
return Am;
end function;
```

Dimensions of $A^{(m)}$ for A of dimension ≤ 6 over an algebraically closed field

We used the code provided above to compute the dimension of m-closures of all algebras of dimension $n \leq 6$ over an algebraically closed field K of characteristic 0. We use the classification in [23], by Bjorn Poonen. Note that for $n \geq 7$ there exist infinitely many non-isomorphic K-algebras (see references in [23]).

Note that we can reduce the computation to local algebras, since by lemma 1.4.13 every finite K-algebra is a product of local ones and by the product

formula (see theorem 1.4.4) we have:

$$\dim(A_1 \times A_2)^{(m)} = \sum_{k=0}^{m} \binom{m}{k} \dim A_1^{(k)} \dim A_2^{(m-k)}.$$

Explanation of the tables 1.7.4. Let A be a local K-algebra with maximal ideal $\mathfrak{m}$. In table 1.1 we consider all algebras with $n \leq 5$. We list the dimension of A, the sequence $d = (\dim(\mathfrak{m}^i/\mathfrak{m}^{i+1}))_{i\geq 1}$, the ideal defining A, and the dimension of $A^{(m)}$ for $m = 2, \ldots, n-1$. We did not write the dimension of the n-closure and of the 1-closure: by theorem 1.3.13 the $(n-1)$-closure is isomorphic to the n-closure, and by number *3* of proposition 1.3.12 the 1-closure is isomorphic to A. The algorithm was run in these cases as well, and confirms the results (or rather the results verify the algorithm). The table for dimension 6 is at the end of the chapter (table 1.2, page 41).

			$\dim A^{(m)}$		
n	d	Ideal	$m=2$	$m=3$	$m=4$
3	(1, 1)	(x^3)	6		
	(2)	$(x,y)^2$	6		
4	(1, 1, 1)	(x^4)	12	24	
	(2, 1)	(x^3, y^2, xy)	13	26	
		(x^2, y^2)	13	26	
	(3)	$(x,y,z)^2$	16	32	
5	(1, 1, 1, 1)	(x^5)	20	60	120
	(2, 1, 1)	(x^2, y^4, xy)	21	65	130
		$(x^2 + y^3, xy)$	21	65	130
	(2, 2)	(x^3, y^2, x^2y)	22	70	140
		(x^3, y^3, xy)	22	70	140
	(3, 1)	(x^2, y^2, z^2, xy, xz)	24	80	160
		$(x^2, y^2, z^3, xy, xz, yz)$	24	84	170
		$(x^2, y^2, xz, yz, xy + z^2)$	24	80	160
	(4)	$(x,y,z,w)^2$	25	105	220

Table 1.1: Dimension up to 5, see 1.7.4

Remark 1.7.5. Let A be a K-algebra of dimension n. In remark 1.4.12 we called $n(n-1)\cdots(n-m+1)$ the *expected rank* of the m-closure of A. From the tables it is apparent that it is in fact quite rare that the rank of the m-closure of a K-algebra A is equal to the expected one: for the algebras considered here this happens only for the 3-dimensional K-algebra $K[X,Y]/(X,Y)^2$, and for the cases already treated in the preceding sections, like for monogenic algebras (see theorem 1.6.7), and for $m = 0, 1$ or $m > n$ (see proposition 1.3.12). It would be interesting to know whether the dimension of $A^{(m)}$ can be smaller than the expected one, but no examples were found, nor a proof that this cannot happen. This was asked for the Galois closure in [2, Question 3].

Remark 1.7.6. The argument for the proof of Theorem 8 in [2] applies to m-closures as well. So for all m the dimension of the m-closure of a K-algebra of dimension n is at most the dimension of the m-closure of the algebra $K[X_1, \ldots, X_{n-1}]/(X_1, \ldots, X_{n-1})^2$.

Remark 1.7.7. Note that table 1.1 and 1.2 are specific to characteristic 0. In characteristic 2 the algebra of dimension 4 defined by the ideal (x^2, y^2) has 2-closure of dimension 16 and 3-closure of dimension 32, and not 13 and 26 as in the table. In particular (see also the discussion after theorem 6 in [2]), this implies there exist free $\mathbb{Z}$-algebras with a non locally free m-closure.

More computations about dimensions

The m-closure of an algebra can sometimes be equal to the whole $A^{\otimes m}$. Here is a sufficient condition.

Proposition 1.7.8. *Let A be a local algebra over a field K, with residue field K. Suppose there exists $t \geq 2$ such that for all a in the maximal ideal of A we have $a^t = 0$. Let n be the dimension of A and suppose $n - tm \geq 0$. Then $A^{(m)}$ is $A^{\otimes m}$.*

Proof. Let K' be any K-algebra and let a be in the maximal ideal of $A \otimes_K K'$. Let ε_i be the natural map $A \otimes_K K' \to A^{\otimes m} \otimes_K K'$. Since a^t is zero we have

$$X^t = (X - \varepsilon_i(a)) \sum_{k=0}^{t-1} \varepsilon_i(a)^k X^{t-k-1}$$

in $A^{\otimes m} \otimes_K K'[X]$ for $i = 1, \ldots, m$. The characteristic polynomial of a is X^n, since a is nilpotent. We can write

$$X^n = X^t \cdots X^t X^{n-tm} = \prod_{i=1}^{m} (X - \varepsilon_i(a)) X^{n-tm} \prod_{i=1}^{m} \left(\sum_{k=0}^{t-1} \varepsilon_i(a)^k X^{t-k-1} \right).$$

In particular $\prod_i (X - \varepsilon_i(a))$ divides the characteristic polynomial of a in $A^{\otimes m} \otimes_K K'[X]$. This proves our claim. □

The algebras of dimension n (over a field) defined in the following proposition have 2-closure of dimension $n^2 - 3$, which is bigger than the expected $n^2 - n$.

Proposition 1.7.9. *Let K be a field. For every $n \geq 3$ let A be the following n-dimensional K-algebra:*

$$A = K[x, y]/(x^{\frac{n}{2}+1}, y^{\frac{n}{2}}, xy), \text{ for } n \text{ even}$$
$$A = K[x, y]/(x^{\frac{n+1}{2}}, y^{\frac{n+1}{2}}, xy), \text{ for } n \text{ odd.}$$

Then $A^{(2)}$ has dimension $n^2 - 3$.

Proof. Let $\gamma \in A[Z_1, \ldots, Z_n]$ be the generic element of A and let γ' be $\gamma - Z_1$, the generic element of the maximal ideal of A. Denote by γ'_i for $i = 1, 2$ the image of γ' via the base change of the natural maps $\varepsilon_i \colon A \to A \otimes_R A$. Let I be the ideal in $A \otimes_R A$ such that $A \otimes_R A/I$ is $A^{(2)}$. By equation (1), page 34, the ideal I is generated by

$$\gamma_1'^{n-1} + \gamma_1'^{n-2}\gamma_2' + \cdots + \gamma_1'\gamma_2'^{n-2} + \gamma_2'^{n-1},$$

and by the relations in A this is equal to

$$\begin{gathered} \gamma_1'^{\frac{n}{2}}\gamma_2'^{\frac{n}{2}-1} + \gamma_1'^{\frac{n}{2}-1}\gamma_2'^{\frac{n}{2}}, \text{ for } n \text{ even} \\ \gamma_1'^{\frac{n-1}{2}}\gamma_2'^{\frac{n-1}{2}}, \text{ for } n \text{ odd.} \end{gathered}$$

Suppose now n is odd and let t be $\frac{n-1}{2}$. Write

$$\gamma' = \sum_{i=1}^{t} x^i Z_i + \sum_{i=1}^{t} y^i Z_{t+i}$$

Then γ'^t is $x^t Z_1^t + y^t Z_t^t$, and the ideal I is generated by

$$x^t \otimes x^t, \quad y^t \otimes y^t, \quad x^t \otimes y^t + y^t \otimes x^t.$$

It is now easy to see that the dimension of I is 3. For n even let $t = \frac{n}{2}$ and write

$$\gamma' = \sum_{i=1}^{t} x^i Z_i + \sum_{i=1}^{t-1} y^i Z_{t-1+i}.$$

Computing $\gamma'^t_1\gamma_2'^{t-1} + \gamma_1'^{t-1}\gamma_2'^t$ we see that I is generated by

$$x^t \otimes y + y \otimes x^t, \quad x^t \otimes x + x \otimes x^t$$

and one computes the dimension of I is again 3. □

It would be interesting to know the possible values for the dimensions of $A^{(m)}$.

d	Ideal	$\dim A^{(m)}$ m=2	m=3	m=4	m=5
(1, 1, 1, 1, 1)	(x^6)	30	120	360	720
(2, 1, 1, 1)	(x^2, y^5, xy)	31	129	393	785
	$(x^2 + y^4, xy)$	31	129	393	785
(2, 2, 1)	(xy, x^3, y^4)	33	141	436	870
	$(xy, x^3 + y^3)$	33	138	422	840
	(x^2, xy^2, y^4)	33	145	453	905
	(x^2, y^3)	33	142	439	875
	$(x^2 + y^3, xy^2, y^4)$	33	144	450	900
(2, 3)	$(x, y)^3$	36	165	539	1085
(3, 1, 1)	$(x^2, xy, y^2, xz, yz, z^4)$	34	160	520	1045
	$(x^2, xy, y^2 + z^3, xz, yz, z^4)$	34	154	488	975
	$(x^2, xy + z^3, y^2, xz, yz, z^4)$	34	154	488	975
(3, 2)	$(xy, yz, z^2, y^2 - xz, x^3)$	36	168	540	1080
	$(xy, z^2, xz - yz, x^2 + y^2 - xz)$	36	168	540	1080
	$(x^2, xy, xz, y^2, yz^2, z^3)$	36	176	587	1185
	$(x^2, xy, xz, yz, y^3, z^3)$	36	172	570	1150
	(xy, xz, y^2, z^2, x^3)	36	168	538	1075
	$(xy, xz, yz, x^2 + y^2 - z^2)$	36	164	516	1028
	$(x^2, xy, yz, xz + y^2 - z^2)$	36	164	518	1033
	(x^2, xy, y^2, z^2)	36	170	546	1090
(4, 1)	$(x^2, y^2, z^2, xy, xz, xw, yz, yw, zw, w^3)$	36	195	707	1457
	$(x^2, y^2, z^2, w^2, xy, xz, xw, yz, yw)$	36	193	667	1352
	$(x^2, y^2 + zw, z^2, w^2, xy, xz, xw, yz, yw)$	36	193	661	1334
	$(x^2, y^2, z^2, w^2, xy - zw, xz, xw, yz, yw)$	36	193	661	1334
(5)	$(x, y, z, w, v)^2$	36	216	876	1875

Table 1.2: Dimension 6, see 1.7.4

Chapter 2

Tate G-schemes

2.1 Introduction

Let $K \to L$ be a finite separable field extension and let $\widetilde{L}$ be a Galois closure of L over K. Let G be the Galois group of $\widetilde{L}$ over K. Then $\widetilde{L}^G$ is isomorphic to K. Similarly S_n acts on $A^{(n)}$ for A an R-algebra of rank n (see remark 1.3.15) and if A is finite étale then $(A^{(n)})^{S_n} \cong R$ as follows from the description in proposition 1.4.11 (see also example 3.2.12). However, such an isomorphism need not exist in general, even if we restrict to the particularly well-behaved class of monogenic rings.

For example take $R = \mathbb{F}_2$ and $A = \mathbb{F}_2[x]/(x^2)$. Then $A^{(2)}$ is isomorphic to A by corollary 1.3.14, and S_2 acts trivially since $\mathrm{Aut}(A)$ is trivial. The ring of invariants is then A, which is not isomorphic to R. Anders Thorup in [29] discusses this problem, for A monogenic of rank n, finding necessary and sufficient conditions for $a \in A^{(n)}$ to be invariant under S_n.

However, consider the following situation: let $K \to L$ be a normal extension of fields and let G be the group of K-automorphisms of L. Then L^G/K is purely inseparable. The most natural generalization to rings of a purely inseparable field extension is a universal homeomorphism (see section 2.3 for the definition). We will show in chapter 3 that the map $R \to (A^{(n)})^{S_n}$ is a universal homeomorphism (see theorem 3.2.9).

In this chapter, with this goal in mind, we will find necessary and sufficient conditions for $R \to A^G$ to be a universal homeomorphism given any R-algebra A, with an action of a finite group G. The notion of universal homeomorphism is scheme-theoretical, so we will develop the theory for schemes, instead of rings.

The analogue of the subring of invariants in the category of schemes is the *categorical quotient* that we discuss in section 2.2. The main result of the chapter is the following theorem.

Theorem (Theorem 2.4.15). *Let $X \to S$ be a scheme, with an action of a finite group G. Then the following are equivalent:*

1. *The categorical quotient X/G exists and the natural map $X/G \to S$ is a universal homeomorphism.*
2. *The map $X \to S$ is integral and surjective, and for all fields K over S the action of G on each non-empty fiber of $X(K) \to S(K)$ is transitive.*

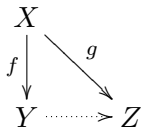
The main tool needed for the proof of this theorem is a result by Deligne (see [12, Corollaire IV.18.12.11]), which characterizes universal homeomorphisms of schemes. We will present here a simpler proof of this result (see theorem 2.3.8), which has been accepted in the Stacks Project (see [28, Lemma 01WM]).

2.2 Quotients of schemes

In this section we will give the definition of quotient of a scheme by the action of a finite group and discuss its existence and properties. Most of the content of this chapter can be found in SGA1, see [13, V.1]. This is just a collection of results needed to follow the rest of the chapter, given for convenience.

Definition 2.2.1. Let G be a group. A *G-scheme* is a scheme X with an action of G. If X is an S-scheme and G acts by morphisms of S-schemes we say X is a *G-scheme over S*.

Definition 2.2.2. Let X be a G-scheme. A morphism of schemes $f\colon X \to Y$ is called a *categorical quotient* of X (or simply a *quotient* of X) if it is G-invariant and for all G-invariant $g\colon X \to Z$ there exists a unique map $Y \to Z$ making the following diagram commutative:



If a quotient exists then it is unique up to a unique isomorphism.

We will denote the quotient by $\pi\colon X \to X/G$ and we will call X/G the *quotient scheme*.

Remark 2.2.3. Let X be a G-scheme over S. If X/G exists then it is naturally an S-scheme.

For us G will always be a *finite* group. Even in this case, the quotient of a G-scheme X need not exist. The first example was given by Serre in [26, Chapter III, page 51]. Here he points out that the variety described by Nagata in [22] has an action of $\mathbb{Z}/2\mathbb{Z}$, but no quotient scheme exists. Another example in a more modern language can be found in Geometric Invariant Theory (see [21, Chapter 4, page 83]), where a construction by Hironaka is described. The variety described there also has an action of $\mathbb{Z}/2\mathbb{Z}$, but no quotient exists.

The existence of a quotient can be guaranteed with the sufficient condition described in proposition 2.2.5. We give first a definition, which is standard, but fundamental.

Definition 2.2.4. A morphism of schemes $f\colon X \to Y$ is called *integral* if it is affine and for all $U = \operatorname{Spec} R$ affine open in Y with inverse image $f^{-1}(U) = \operatorname{Spec} A$, the induced ring map $R \to A$ is integral (see definition 1.2.10).

Proposition 2.2.5. *Let G be a finite group and let X be a G-scheme. Then the following are equivalent:*

1. *There exists a G-invariant affine morphism $f\colon X \to Y$ such that the induced map $\mathcal{O}_Y \to (f_*\mathcal{O}_X)^G$ is an isomorphism.*
2. *There exists a covering of X consisting of G-invariant affine open subsets.*
3. *Each orbit of G is contained in an affine open subset of X.*

If X satisfies the above conditions then $f\colon X \to Y$ is a quotient of X, the topology on Y is the quotient topology, the map f is integral and surjective and its (set-theoretical) fibers are the orbits of G.

Proof. See [13, Proposition V.1.3 and Proposition V.1.8]. □

Definition 2.2.6. Let G be a finite group and let X be a G-scheme. We say X is *admissible* if it satisfies the equivalent conditions in proposition 2.2.5.

For X affine we have the following.

Proposition 2.2.7. *Let G be a finite group and let let $X = \operatorname{Spec} A$ be an affine G-scheme. Then X is admissible and $\pi\colon X \to \operatorname{Spec} A^G$ is a quotient.*

Proof. Clear from proposition 2.2.5. □

Remark 2.2.8. Note that the requirement of being admissible is quite weak: for example let G be a finite group and X be a quasi-projective G-scheme over a scheme S. Then X is admissible because every finite set of points in X lying over the same point of S, is contained in an affine open subset of X (see [25, Proposition B.2]).

Remark 2.2.9. Being admissible is not a necessary condition for having a quotient: let K be a field, and let X be the affine line with double origin over K. Let $\mathbb{Z}/2\mathbb{Z}$ act on X by exchanging the two origins. Then the obvious map $X \to \mathbb{A}^1_K$ is a quotient, but X is not admissible. It is, however necessary if X is separated (see [25, Remark 4.5]).

Proposition 2.2.10. *Let G be a finite group and let X be an admissible G-scheme. Let U be an open subset of X/G. Then $\pi^{-1}(U)$ is an admissible G-scheme and the quotient is the restriction of π to $\pi^{-1}(U) \to U$.*

Proof. See [13, Corollary V.1.4]. □

Proposition 2.2.11. *Let G be a finite group and let X be an admissible G-scheme. Let H be a subgroup of G. Then X is also an admissible H-scheme. If moreover H is a normal subgroup then X/H is an admissible (G/H)-scheme and the natural map $X/G \to (X/H)/(G/H)$ is an isomorphism.*

Proof. A G-invariant affine open subset is also H-invariant so X/H is an admissible H-scheme. The rest is clear. □

Proposition 2.2.12. *Let G be a finite group and let X be a G-scheme. Suppose there exists an affine G-invariant morphism $X \to Y$. Then X is admissible.*

Proof. Since $X \to Y$ is affine and G-invariant we can cover X with G-invariant affine open subsets, so X is admissible. □

Proposition 2.2.13. *Let G be a finite group and let X be an admissible G-scheme over a scheme S. Then for all schemes $T \to S$ the base-change $X \times_S T$ is an admissible G-scheme over T.*

Proof. Since X is admissible, there exists a G-invariant affine morphism $X \to Y$ for some S-scheme Y by number *1* of proposition 2.2.5. Since the base change of an affine map is affine the map $X \times_S T \to Y \times_S T$ is affine and G-invariant. So $X \times_S T$ is admissible by proposition 2.2.12. □

Remark 2.2.14. Note that proposition 2.2.13 does not imply that the quotient of $X \times_S T$ is $(X/G) \times_S T$. This is false even for affine schemes. For example let S be $\operatorname{Spec} \mathbb{Z}$, let X be $\operatorname{Spec} \mathbb{Z}[\sqrt{2}]$ and let T be $\operatorname{Spec} \mathbb{F}_2$. Let G be the group with two elements and consider the action of G on X given by $\sqrt{2} \mapsto -\sqrt{2}$.

Clearly X/G is isomorphic to S, so $(X/G) \times_S T$ is isomorphic to T, but $X \times_S T$ is $\operatorname{Spec} \mathbb{F}_2[x]/(x^2)$ with the trivial action so that $(X \times_S T)/G$ is $\operatorname{Spec} \mathbb{F}_2[x]/(x^2)$, which is not isomorphic to T.

However, by the universal property of the quotient, there exists a natural map $(X \times_S T)/G \to (X/G) \times_S T$. A list of conditions under which this map is an isomorphism is given in Katz's and Mazur's "arithmetic moduli of elliptic curves" (see [15, Appendix $A7$]). We will see in proposition 2.4.13 that the natural map is a *homeomorphism* in general.

Lemma 2.2.15. *Let G be a finite group and let X be an admissible G-scheme. Let $f\colon X \to Y$ be an integral G-invariant map. Then $g\colon X/G \to Y$ is also integral.*

Proof. The situation is summarized in the following diagram:

$$\begin{array}{ccc} X & & \\ {\scriptstyle\pi}\downarrow & \searrow^{f} & \\ X/G & \xrightarrow[g]{} & Y \end{array}$$

Let U be an affine open subset of Y. Since f is integral $V = f^{-1}(U)$ is also open and affine, and since f is G-invariant, we have that V is stable under G. Surjectivity of π implies that $\pi(V)$ is equal to $g^{-1}(U)$. The restriction of π to $V \to g^{-1}(U)$ is a quotient by proposition 2.2.10. By proposition 2.2.7 the quotient of an affine scheme is affine so $g^{-1}(U)$ is affine, and then g is an affine map.

We can then reduce to the case X is $\operatorname{Spec} B$ and Y is $\operatorname{Spec} A$ and f comes from a ring map $A \to B$. Since $A \to B$ is integral every element of B is a root of a monic polynomial with coefficients in A, but then also the restriction to $A \to B^G$ is integral, and the proof is complete. □

2.3 Universal homeomorphisms

In this section we will discuss some properties of universal homeomorphisms of schemes. Here is the definition.

Definition 2.3.1. We say a morphism of schemes $f\colon X \to Y$ is a *universal homeomorphism* if for all maps $Z \to Y$, the projection $f_Z\colon X \times_Y Z \to Z$ is a homeomorphism. Similarly we define *universally closed* morphisms, *universally injective* morphisms and *universally surjective* morphisms.

The main result of the section is theorem 2.3.8, which we state here.

Theorem (Theorem 2.3.8). *A morphism of schemes f is a universal homeomorphism if and only if f is integral, surjective and universally injective.*

This theorem was first proved by Deligne in EGA IV (see [12, Theorem IV.18.12.11]).

We start with some standard results that we will use in the proof. References include EGA II (see [11, Section II.6]) and the Stacks Project (see [28, Section 01WG]).

Lemma 2.3.2. *Let $\varphi\colon R \to A$ be an integral injective map of rings. Then* $\operatorname{Spec}\varphi$ *is surjective.*

Proof. Let $\mathfrak{p} \in \operatorname{Spec} R$. We want to find a prime $\mathfrak{q} \in \operatorname{Spec} A$ such that $\mathfrak{q} \cap R = \mathfrak{p}$. This regards only primes containing $\mathfrak{p}$, so we can localize at $\mathfrak{p}$ and suppose R is a local ring with maximal ideal $\mathfrak{p}$.

We have to show there exists a prime of A containing $\mathfrak{p}A$; equivalently we show $\mathfrak{p}A \neq A$. Suppose $\mathfrak{p}A = A$, then we can write $1 = \sum_{i=1}^{n} m_i a_i$ for some $m_i \in \mathfrak{p}$ and $a_i \in A$. Since A is integral over R the R-algebra $B = R[a_1, \ldots, a_n]$ is finite. Since $1 = \sum m_i a_i$ we have $\mathfrak{p}B = B$ so by Nakayama's lemma $B = 0$. This is a contradiction since B contains R. So $\mathfrak{p}A \neq A$ and the proof is complete. □

Corollary 2.3.3. *Let $f\colon X \to Y$ be an integral morphism of schemes. Then f is closed.*

Proof. Since f is affine, we may assume f is the morphism $\operatorname{Spec} A \to \operatorname{Spec} R$ coming from a ring map $\varphi\colon R \to A$. Take a closed subscheme $\operatorname{Spec} A/I$ of X and let $J = \varphi^{-1}(I)$. The map $R/J \to A/I$ is integral and injective, hence the induced map on spectra is surjective by lemma 2.3.2. So f is closed. □

Lemma 2.3.4. *Let $f\colon X \to S$ be an integral morphism of schemes and $T \to S$ be a morphism of schemes. Then $X \times_S T \to T$ is integral.*

Proof. Since f is affine we can reduce to proving the base change of an integral ring map is integral.

Let $R \to A$ be an integral ring map and $R \to R'$ be any ring map. If $a \in A$ is a root of a monic polynomial $P \in R[x]$ then $a \otimes 1$ is a root of $P \otimes 1_{R'}$, so $a \otimes 1$ is integral over R'. Since sums and products of integral elements are integral, and for all $s \in R'$ the element $1 \otimes s$ is integral over R' , this shows $A \otimes_R R'$ is integral over R'. □

Lemma 2.3.5. *Let $f\colon X \to Y$ be a morphism of schemes. If f is a homeomorphism then f is affine.*

Proof. See [28, Lemma 04DE]. □

Lemma 2.3.6. *Let $f\colon X \to Y$ be a surjective morphism of schemes. Then f is universally surjective.*

Proof. See [10, Proposition I.3.6.1] or [28, Lemma 01S1]. □

After these basic results we are now ready to prove the characterization of universal homeomorphisms. The following proposition is the main ingredient. The proof given here has been accepted in the Stacks Project (see [28, Lemma 01WM]).

Proposition 2.3.7. *Let $f\colon X \to Y$ be a morphism of schemes. Then f is integral if and only if f is affine and universally closed.*

Proof. By definition an integral map is affine. By lemma 2.3.4 a base change of f is integral and hence closed by corollary 2.3.3, so f is universally closed.

Suppose f is affine and universally closed. We may assume f is the morphism $f\colon \operatorname{Spec} A \to \operatorname{Spec} R$ coming from a ring map $R \to A$. Let a be an element of A. We have to show that a is integral over R, i.e. that in the kernel I of the map $R[x] \to A$ sending x to a there is a monic polynomial. Consider the ring $B = A[x]/(ax-1)$ and let J be the kernel of the composition of natural maps $R[x] \to A[x] \to B$. If $f \in J$ there exists $q \in A[x]$ such that $f = q \cdot (ax-1)$ in $A[x]$ so if $f = \sum_i f_i x^i$ with $f_i \in R$, and $q = \sum_i q_i x^i$, with $q_i \in A$, then we have $f_i = aq_{i-1} - q_i$, for all $i \geq 0$. For $n \geq \deg q + 1$ the polynomial

$$\sum_{i\geq 0} f_i x^{n-i} = \sum_{i\geq 0} (aq_{i-1} - q_i)x^{n-i} = (a-x)\sum_{i\geq 0} q_i x^{n-i-1}$$

is clearly in I; if $f_0 = 1$ this polynomial is monic, so we are reduced to proving that J contains a polynomial with constant term 1. Equivalently, we can prove that $\operatorname{Spec} R[x]/(J + (x))$ is empty.

Since f is universally closed the base change $\operatorname{Spec} A[x] \to \operatorname{Spec} R[x]$ is closed, so the closed subset $\operatorname{Spec} B$ of $\operatorname{Spec} A[x]$ surjects on $\operatorname{Spec} R[x]/J$.

Consider the following diagram where every square is a pullback:

$$\begin{array}{ccccc}
\operatorname{Spec} B & \xrightarrow{\quad g \quad} & \operatorname{Spec} R[x]/J & \longrightarrow & \operatorname{Spec} R[x] \\
\uparrow & & \uparrow & & \uparrow{\scriptstyle 0} \\
\emptyset & \longrightarrow & \operatorname{Spec} R[x]/(J+(x)) & \longrightarrow & \operatorname{Spec} R
\end{array}$$

The bottom left corner is empty because it is the spectrum of $R \otimes_{R[x]} B$ where the map $R[x] \to B$ sends x to an invertible element and $R[x] \to R$ sends x to 0. Since g is surjective lemma 2.3.6 implies $\operatorname{Spec} R[x]/(J + (x))$ is empty, as we wanted to show. □

The following is the main result of this section. We recall the statement.

Theorem 2.3.8 (Deligne, Theorem IV.18.12.11 in [12]). *A morphism of schemes f is a universal homeomorphism if and only if f is integral, surjective and universally injective.*

Proof. If f is a universal homeomorphism, then f is surjective, universally injective and universally closed. Since f is a homeomorphism f is affine by lemma 2.3.5 so f is integral by proposition 2.3.7.

Suppose f is integral, surjective and universally injective. Since f is integral f is universally closed by proposition 2.3.7. Surjectivity is invariant under base change by lemma 2.3.6 so f is also universally bijective. Then f is a universal homeomorphism. □

Example 2.3.9. We give some examples and non-examples of universal homeomorphisms. For a ring map $f\colon R \to A$ we will say that f is a universal homeomorphism if the induced map $\operatorname{Spec} A \to \operatorname{Spec} R$ is a universal homeomorphism.

1. By theorem 2.3.8 is easy to see that a purely inseparable field extension $K \to L$ is a universal homeomorphism.

2. Again from theorem 2.3.8 follows that for $n \geq 1$ the map $R \to R[\varepsilon]/(\varepsilon^n)$ is a universal homeomorphism for any ring R.

3. Let L be $K(\alpha)$, with K a field and α a transcendental element. Then if we base change to $K[X]$ the closed point $(X - \alpha)$ of $\operatorname{Spec} K(\alpha)[X]$ is mapped to the generic point of $\mathbb{A}^1_K$, which is not closed. Hence $\operatorname{Spec} L \to \operatorname{Spec} K$ is not universally closed and so it is not a universal homeomorphism.

4. Let A be a finite separable algebra of dimension n over a field K. Then $\operatorname{Spec} A \to \operatorname{Spec} K$ is a universal homeomorphism if and only if $n = 1$. In fact, clearly this is not the case if $n = 0$ and if $n > 1$, then $\operatorname{Spec} A \times_K \bar{K}$ is the disjoint union of n copies of $\operatorname{Spec} \bar{K}$, so $\operatorname{Spec} A \to \operatorname{Spec} K$ is not universally injective.

5. A geometric example: the cusp. Let K be a field and let X be the curve in $\mathbb{A}^2_K$ defined by the equation $x^2 = y^3$. The natural map $\mathbb{A}^1_K \to X$, coming from the ring map $K[x, y]/(x^2 - y^3) \to K[t]$ sending x to t^3 and y to t^2, is a universal homeomorphism. Clearly the map is surjective and integral. Let $K \to F$ be any field extension. The F-rational points of X are all pairs (a, b) in F^2 such that $a^2 = b^3$ and the map $\mathbb{A}^1_K(F) \to X(F)$ sends $z \in F$ to the pair (z^3, z^2). This map is injective for all F because in any field if $z_1^2 = z_2^2$ and $z_1^3 = z_2^3$ then $z_1 = z_2$, so $\mathbb{A}^1_K \to X$ is universally injective (see lemma 2.4.6) and hence a universal homeomorphism.

2.4 Tate G-schemes

We introduce here the notion of Tate G-schemes, and prove some of their properties. The name comes from theorem 2.4.10, which was attributed to John Tate by Hendrik Lenstra (oral communication).

Definition 2.4.1. Let G be a finite group and let X be a G-scheme over S. We say X is a *Tate G-scheme* over S if $X \to S$ is a surjective integral morphism and for all fields K over S, the action of G on each non-empty fiber of $X(K) \to S(K)$ is transitive.

In this section we will prove theorem 2.4.15, the main result of the chapter. As we saw in section 2.1 this theorem is our motivation for introducing Tate G-schemes. We recall the statement here.

Theorem (Theorem 2.4.15)**.** *Let G be a finite group and $X \to S$ be a G-scheme over S. Then X is a Tate G-scheme over S if and only if X is admissible and $X/G \to S$ is a universal homeomorphism.*

We start the study of Tate G-schemes with some easy remarks. First note that all Tate G-schemes are admissible.

Proposition 2.4.2. *Let G be a finite group and let X be a Tate G-scheme over S. Then X is admissible.*

Proof. An integral map is affine, so this is true by proposition 2.2.12. □

Lemma 2.4.3. *Let $X \to S$ be integral and surjective and let K be an algebraically closed field. Then the map $X(K) \to S(K)$ is surjective.*

Proof. Any s in $S(K)$ factors through a residue field $\kappa(\mathfrak{p}_s)$ of S. Since $X \to S$ is surjective there is a point $\mathfrak{p}_x \in X$ mapping to $\mathfrak{p}_s$ and since $X \to S$ is integral the extension $\kappa(\mathfrak{p}_s) \to \kappa(\mathfrak{p}_x)$ is algebraic. Since K is algebraically closed the field extension $\kappa(\mathfrak{p}_s) \to K$, extends to a map $\kappa(\mathfrak{p}_x) \to K$. Then $\mathfrak{p}_x$ together with this field extension gives a K-point of X mapping to s. □

We can restrict ourselves to algebraically closed fields.

Lemma 2.4.4. *Let X be a G-scheme over S. If for all algebraically closed fields K the action of G on each non-empty fiber of $X(K) \to S(K)$ is transitive then the same is true for all fields.*

Proof. For all fields K given with a map $\operatorname{Spec} K \to S$ we have that $X(K)$ is a subset of $X(\bar{K})$ and $S(K)$ is a subset of $S(\bar{K})$, so the statement holds. □

Proposition 2.4.5. *Let G be a finite group and let X be a G-scheme over S. Then X is a* Tate G-scheme *over S if and only if $X \to S$ is surjective and integral and for all algebraically closed fields K over S, the action of G on each fiber of $X(K) \to S(K)$ is transitive.*

Proof. Combine lemma 2.4.4 with lemma 2.4.3. □

The following characterization of universally injective maps will be useful in the proof of the main result.

Lemma 2.4.6. *Let $f\colon X \to Y$ be a morphism of schemes. Then f is universally injective if and only if for all fields K the induced map $X(K) \to Y(K)$ is injective.*

Proof. See [10, Remarque 3.5.11], or [28, Lemma 01S4]. □

Corollary 2.4.7. *Let $f\colon X \to Y$ be a morphism of schemes. Then f is universally injective if and only if for all algebraically closed fields K the induced map $X(K) \to Y(K)$ is injective.*

Proof. Follows from lemma 2.4.6 and lemma 2.4.4 with G the trivial group. □

Example 2.4.8. Let $\{1\}$ be the trivial group and let $X \to S$ be a morphism of schemes. Then X is a Tate $\{1\}$-scheme over S if and only if $X \to S$ is a universal homeomorphism. In fact, by theorem 2.3.8 the morphism $X \to S$ is a universal homeomorphism if and only if it is integral, surjective and universally injective, and by definition $X \to S$ is a Tate $\{1\}$-scheme if and only if it is integral, surjective and for all fields K the induced map $X(K) \to S(K)$ is injective. By lemma 2.4.6 the last condition holds if and only if $X \to S$ is universally injective, so the claim is proved.

Finally, an observation on Tate G-schemes over algebraically closed fields.

Lemma 2.4.9. *Let X be a G-scheme over $S = \operatorname{Spec} K$, with K an algebraically closed field. Suppose $X \to S$ is integral and surjective. Then X is a Tate G-scheme over S if and only if the action of G is transitive on $X(K)$.*

Proof. First note that the action of G on $X(K)$ is transitive if and only if the action of G on each fiber of $X(K) \to S(K)$ is transitive. Then the conclusion follows since for every field extension $K \to L$ any map $\operatorname{Spec} L \to X$ factors through S, since X is integral and K algebraically closed. □

The following theorem is the main ingredient for the proof of our main result. It also gives us a non-trivial class of examples: every admissible G-scheme is a Tate G-scheme over the quotient. The proof we are going to present is more or less the one in [27, Lemma 15.1].

Theorem 2.4.10 ("Tate's lemma"). *Let G be a finite group and let X be an admissible G-scheme. Take $S = X/G$. Then X is a Tate G-scheme over S.*

Proof. By proposition 2.2.5 the map $\pi\colon X \to S$ is surjective and integral.

To check the third condition we can reduce to algebraically closed fields by proposition 2.4.5. Fix an algebraically closed field K and a K-point s of S. By lemma 2.4.3 there is at least one point in the fiber of s under $X(K) \to S(K)$. If there is only one then we have nothing to prove. Let x, y be in $X(K)$, both mapping to s in $S(K)$. It is sufficient to show there exists $\sigma \in G$ such that $\sigma \circ x = y$. That the set-theoretic points corresponding to x and y in X lie in the same orbit is clear. Let U be an affine open neighborhood of s. Since π is affine also $V = \pi^{-1}(U)$ is affine and both x and y factor over V. We are then reduced to the case $X = \operatorname{Spec} A$ for a ring A. It suffices to show that for all algebraically closed fields K and maps $f, g\colon A \to K$ that coincide on A^G there exists $\sigma \in G$ such that $f = g \circ \sigma$.

Let f, g, K be as above and let $\{a_1, \ldots, a_n\}$ be a finite subset of A. We show first that there exists a $\sigma \in G$ such that $f(a_i) = g(\sigma a_i)$ for all i. Consider the ring $A[X_1, \ldots, X_n, Z]$ with the induced action of G. Extend f and g to maps $f, g\colon A[X_1, \ldots, X_n, Z] \to K[X_1, \ldots, X_n, Z]$. Let $Q(X_1, \ldots, X_n) = \sum_i a_i X_i$. The polynomial $P(Z)$ defined as

$$\prod_{\tau \in G} (Z - \tau Q) = \prod_{\tau \in G} (Z - \sum_i \tau a_i X_i)$$

is in $A^G[X_1, \ldots, X_n, Z]$. So we have $f(P(Z)) = g(P(Z))$, and therefore

$$\prod_{\tau \in G} (Z - f(\tau Q)) = \prod_{\tau \in G} (Z - g(\tau Q))$$

Since $K[X_1, \ldots, X_n, Z]$ is a unique factorization domain and the factors are irreducible there is $\sigma \in G$ such that $f(Q) = g(\sigma Q)$ and hence $\sum_i f(a_i) X_i = \sum_i g(\sigma a_i) X_i$. This implies that for every i we have $f(a_i) = g(\sigma a_i)$, as we claimed.

We can then write $A = \cup_{\sigma \in G} A_\sigma$ where $A_\sigma = \{a \in A | f(\sigma a) = g(a)\}$. We show there is an A_σ that is equal to A. Suppose this is not the case so for all $\sigma \in G$ we can take $a_\sigma \in A \setminus A_\sigma$. The set $S = \{a_\sigma\}_{\sigma \in G}$ is finite hence, as we showed, there exists $\tau \in G$ such that for all $a \in S$ we have $f(a) = g(\tau a)$. In particular $f(a_\tau) = g(\tau a_\tau)$ so that $a_\tau \in A_\tau$, a contradiction. □

Being a Tate G-scheme is stable under base change.

Proposition 2.4.11. *Let G be a finite group and let X be a Tate G-scheme over S. Let T be an S-scheme. Then $X \times_S T$ with the induced action of G is a Tate G-scheme over T.*

Proof. Surjectivity and integrality are stable under base change by lemma 2.3.6 and lemma 2.3.4 respectively, so $X \times_S T \to T$ is integral and surjective.

For every field K the fibers of $(X \times_S T)(K) \to T(K)$ are fibers of $X(K) \to S(K)$, so the rest is clear. □

Lemma 2.4.12. *Let G be a finite group and let X be a Tate G-scheme over S. Then $X/G \to S$ is a homeomorphism.*

Proof. The map $X \to S$ is integral so $X/G \to S$ is integral by lemma 2.2.15, hence $X/G \to S$ is closed by proposition 2.3.7. Surjectivity is clear, so we are left to show $X/G \to S$ is injective.

Let x, y be in X and suppose they are mapped to the same element s in S. The residue fields $\kappa(x)$ and $\kappa(y)$ are both extensions of $\kappa(s)$ so they can be embedded in a field K. This gives us two K-points of X lying above the same K-point of S. So x and y are conjugate since X is a Tate G-scheme over S. Then $X/G \to S$ is injective and hence a homeomorphism. □

The following proposition is not new, even if the proof we give here probably is. The result follows from proposition 2.2.7 and a result in Katz's and Mazur's "arithmetic moduli of elliptic curves" attributed to Ofer Gabber (see [15, Proposition A7.2.1 and Corollary A7.2.2]). It can also be found in notes by Qing Liu (see [19]).

Proposition 2.4.13. *Let G be a finite group and let X be an admissible G-scheme over S. Let T be an S-scheme. Then the natural map $(X \times_S T)/G \to (X/G) \times_S T$ is a homeomorphism.*

Proof. By theorem 2.4.10 we know that $X \to X/G$ is a Tate G-scheme, so by proposition 2.4.11 and lemma 2.4.12 for all (X/G)-schemes U the map $(X \times_{X/G} U)/G \to U$ is a homeomorphism. Taking $U = (X/G) \times_S T$ we have

$$X \times_{X/G} U \cong (X \times_{X/G} (X/G)) \times_S T \cong X \times_S T$$

so $(X \times_S T)/G \to (X/G) \times_S T$ is a homeomorphism. □

Lemma 2.4.14. *Let G be a finite group and let X be an admissible G-scheme over S. Suppose $X/G \to S$ is universally injective. Then for all algebraically closed fields K the action of G on each non-empty fiber of $X(K) \to S(K)$ is transitive.*

Proof. Fix an algebraically closed field K and an $s \in S(K)$. By corollary 2.4.7 there is at most one element in the fiber of s in $(X/G)(K)$. Suppose there is one and denote it by x. By theorem 2.4.10 the action of G on the fiber of x in $X(K)$ is transitive, and hence also the action of G on the fiber of s in $X(K)$ is transitive, so the proof is complete. □

We are now ready to prove the main theorem. We recall the statement here.

Theorem 2.4.15. *Let G be a finite group and let $X \to S$ be a G-scheme over S. Then X is a Tate G-scheme over S if and only if X is admissible and $X/G \to S$ is a universal homeomorphism.*

Proof. Suppose $X \to S$ is Tate. We proved in proposition 2.4.2 that X is admissible. Fix a scheme $T \to S$. By proposition 2.4.11 the G-scheme $(X \times_S T) \to T$ is Tate and so by lemma 2.4.12 the map $(X \times_S T)/G \to T$ is a homeomorphism. Since by proposition 2.4.13 the map $(X \times_S T)/G \to (X/G) \times_S T$ is a homeomorphism also $(X/G) \times_S T \to T$ is a homeomorphism by composition. So $X/G \to S$ is a universal homeomorphism.

Suppose now X is admissible and $X/G \to S$ is a universal homeomorphism. By theorem 2.3.8 the map $f\colon X/G \to S$ is surjective, universally injective and integral. The map $X \to S$ is the composition of f and $X \to X/G$. Since f is integral and surjective and $X \to X/G$ is also integral and surjective by proposition 2.2.5, by composition $X \to S$ is integral and surjective. Since f is universally injective, by lemma 2.4.14 for all fields K the action of G on each non-empty fiber of $X(K) \to S(K)$ is transitive. If K is algebraically closed, by lemma 2.4.3 all fibers of $X(K) \to S(K)$ are non-empty, so the action of G is transitive on each fiber of $X(K) \to S(K)$. This is true for all algebraically closed fields K, so X is a Tate G-scheme over S by proposition 2.4.5. □

Example 2.4.16. Let A be the $\mathbb{Z}$-algebra $\mathbb{Z}[i]$. Let G be the group $\mathbb{Z}/2\mathbb{Z}$ acting on A by sending i to $-i$. It is easy to verify directly that $\operatorname{Spec} A \to \operatorname{Spec} \mathbb{Z}$ is a Tate G-scheme. The quotient is $\operatorname{Spec} A^G$ so it is in this case *isomorphic* to $\operatorname{Spec} \mathbb{Z}$. Note that the base change of A to $\mathbb{F}_2$ is also Tate with group $\mathbb{Z}/2\mathbb{Z}$ by proposition 2.4.11. In fact, the ring of invariants is $\mathbb{F}_2[\varepsilon]/(\varepsilon^2)$ which is universally homeomorphic to $\mathbb{F}_2$ (but not isomorphic).

2.5 Properties of Tate G-schemes

We now investigate further some properties of Tate G-schemes. Some of the results we will present are motivated by results in Galois theory for fields. We will give examples to illustrate these similarities.

Example 2.5.1. A finite Galois extension of fields $K \to L$ with Galois group G is a Tate G-scheme, since $L^G \cong K$. Let H be a subgroup of G, then $L^H \to L$ is a Galois extension with Galois group H. If moreover H is normal, then $K \to L^H$ is also Galois with Galois group G/H.

Something similar happens for Tate G-schemes, as we prove in the following propositions.

Proposition 2.5.2. *Let G be a finite group and let X be a Tate G-scheme over S. Let H be a subgroup of G. Then X/H exists and $X \to X/H$ is a Tate H-scheme.*

Proof. Recall that X is also an admissible H-scheme by proposition 2.2.11, so X/H exists. The statement is now "Tate's lemma" (theorem 2.4.10). □

Proposition 2.5.3. *Let G be a finite group and let X be a Tate G-scheme over S. Let H be a normal subgroup of G. Then $X/H \to S$ is a Tate G/H-scheme.*

Proof. By theorem 2.4.15 it is sufficient to prove that $(X/H)/(G/H) \to S$ is a universal homeomorphism. Since $(X/H)/(G/H)$ is isomorphic to X/G by proposition 2.2.11, and X/G is universally homeomorphic to S by theorem 2.4.15, the proof is complete. □

For the next proposition we need the following lemma.

Lemma 2.5.4. *Let G be a finite group and let $f\colon X \to Y$ be a morphism of G-schemes over a scheme S. Suppose X and Y are admissible and f is a universal homeomorphism. Then $g\colon X/G \to Y/G$ is a universal homeomorphism.*

Proof. The situation is summarized in the following diagram:

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ \downarrow & & \downarrow \\ X/G & \xrightarrow[g]{} & Y/G \end{array}$$

By theorem 2.3.8 we have to prove g is surjective, integral and universally injective. Since $Y \to Y/G$ and f are surjective also g is surjective. The map f is affine by lemma 2.3.5, and universally closed, so it is integral by proposition 2.3.7. Also $Y \to Y/G$ is integral by proposition 2.2.5, hence also $X \to Y/G$ is integral by composition. Then g is integral by lemma 2.2.15.

We are left to see that g is universally injective. Let K be an algebraically closed field. We need to prove the map $(X/G)(K) \to (Y/G)(K)$ is injective.

Let $\bar{x}, \bar{x}'$ be in $(X/G)(K)$ and suppose they are mapped to the same element $\bar{y}$ in $(Y/G)(K)$. By lemma 2.4.3 there exist x, x' in $X(K)$ lying above $\bar{x}$ and $\bar{x}'$ respectively and there exists $y \in Y(K)$ lying above $\bar{y}$. Moreover x and x' both map to y. Since f is a universal homeomorphism x and y are then equal, and so also $\bar{x}$ and $\bar{y}$ are. □

Example 2.5.5. Let K be a field and let L be a finite Galois extension of K with Galois group G. Let M be a purely inseparable extension of L. Suppose that G acts on M and that $L \to M$ is G-equivariant. Then M^G is a purely inseparable extension of K. This motivates proposition 2.5.6.

Proposition 2.5.6. *Let G be a finite group and let X and Y be G-schemes over S. Suppose that $f\colon X \to Y$ is a G-equivariant universal homeomorphism and that $Y \to S$ is a Tate G-scheme. Then $X \to S$ is a Tate G-scheme.*

Proof. The map $X/G \to Y/G$ is a universal homeomorphism by lemma 2.5.4 and $Y/G \to S$ is a universal homeomorphism because $Y \to S$ is Tate. Then also the composition $X/G \to S$ is a universal homeomorphism, since a composition of homeomorphisms is a homeomorphism, and hence $X \to S$ is Tate by theorem 2.4.15. □

Example 2.5.7. The following example motivates the next proposition. Let K be a field and let L_1 and L_2 be Galois extensions of K, considered inside a fixed algebraic closure of K. Let G_i be the Galois group of L_i/K for $i = 1, 2$. Suppose $L_1 \cap L_2 = K$. Then the compositum L_1L_2 is a Galois extension of K with group the product $G_1 \times G_2$ (see [17, Theorem 1.14, Chapter VI]).

Proposition 2.5.8. *Let G_1 and G_2 be finite groups and let $X_1 \to S$ and $X_2 \to S$ be Tate schemes, with groups G_1 and G_2 respectively. Then $X_1 \times_S X_2 \to S$ is a Tate G-scheme, with $G = G_1 \times G_2$.*

Proof. We show that $(X_1 \times_S X_2)/G \to S$ is a universal homeomorphism. We can write this map as the composition

$$(X_1 \times_S X_2)/G \xrightarrow{f} (X_1/G_1 \times_S X_2)/G_2 \xrightarrow{g} X_2/G_2 \xrightarrow{h} S.$$

We will prove that each of these maps is a universal homeomorphism. Since $X_1 \to S$ is a Tate G_1-scheme, by proposition 2.4.11 also $X_1 \times_S X_2 \to (X_1/G_1) \times_S X_2$ is a Tate G_1-scheme. Then $(X_1 \times_S X_2)/G_1 \to (X_1/G_1) \times_S X_2$ is a universal homeomorphism by theorem 2.4.15. Since the map is also G_2-equivariant f is a universal homeomorphism by lemma 2.5.4.

Since $X_1 \to S$ is a Tate G_1-scheme $X_1/G_1 \to S$ is a universal homeomorphism. Its base change to X_2, the map $(X_1/G_1 \times_S X_2) \to X_2$, is a G_2-equivariant universal homeomorphism so lemma 2.5.4 implies g is a universal homeomorphism.

Since $X_2 \to S$ is a Tate G_2-scheme also h is a universal homeomorphism, so the proof is complete. □

2.6 Tate G-schemes over algebraically closed fields

Let G be a finite group. We characterize Tate G-schemes over an algebraically closed field K.

Lemma 2.6.1. *Let K be an algebraically closed field and A be a connected K-algebra, intgral over K. Then every element of A is either a unit or nilpotent.*

Proof. Let a be in A. The ring $K[a]$ is connected because it is a subring of the connected ring A, and finite because a is integral over K. So $K[a]$ is local with nilpotent maximal ideal by lemma 1.4.13. Then a is either a unit or nilpotent. This holds for every $a \in A$, so the proof is complete. □

Lemma 2.6.2. *Let K be an algebraically closed field and A be a connected K-algebra, intgral over K. The following are equivalent.*

1. *The algebra A is connected.*
2. *The algebra A is local and the maximal ideal consists of nilpotent elements.*
3. *The algebra A is local.*
4. *The map $K \to A$ is a universal homeomorphism.*

Proof. By lemma 2.6.1 we have that *1* implies *2*.

Clearly *2* implies *3*.

Suppose *3* holds. By remark 1.4.15 there exists a unique K-algebra map $A \to K$, so $\operatorname{Spec} A$ has a unique K-point and $(\operatorname{Spec} A)(K) \to (\operatorname{Spec} K)(K)$ is injective. So $K \to A$ is a universal homeomorphism by theorem 2.3.8 and by corollary 2.4.7. Hence *4* holds.

Since $\operatorname{Spec} K$ is connected if $\operatorname{Spec} A$ is universally homeomorphic to $\operatorname{Spec} K$ in particular A is connected. So *4* implies *1*, and the proof is complete. □

Proposition 2.6.3. *Let X be a Tate G-scheme over an algebraically closed field K. Then X is affine, and $\mathcal{O}_X(X)$ is a finite product $A_0 \times \cdots \times A_0$ with A_0 a local integral K-algebra.*

Proof. The morphism $X \to \operatorname{Spec} K$ is integral and hence affine. Since $\operatorname{Spec} K$ is affine, also X is affine (see [11, Chapitre 2, §1, Corollaire 1.3.4]). Let A be the ring of global sections of X. By theorem 2.4.15 the quotient of $\operatorname{Spec} A$ by the action of G is homeomorphic to the one point space $\operatorname{Spec} K$. So G acts transitively on $\operatorname{Spec} A$ and $\operatorname{Spec} A$ is finite and discrete. Hence A is a finite product of local integral K-algebras, and all factors are isomorphic, since G permutes them transitively. □

Chapter 3

The action of $\operatorname{Sym} S$ on $A^{(S)}$

3.1 Introduction

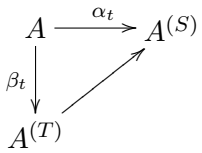
Let K be a field. Let $K \to L$ be a Galois extension of degree n. Let G be the Galois group of L over K. Then the natural map $K \to L^G$ is an isomorphism. Let $R \to A$ be an R-algebra. Let G be a finite group acting on A via R-algebra homomorphisms. In chapter 2 we gave necessary and sufficient criteria for $R \to A^G$ to be a universal homeomorphism (see theorem 2.4.15). In this case we say that $R \to A$ is Tate with group G. Being Tate with group G is in this sense a weaker version of being Galois with group G.

In this chapter we go back to our study of the Galois closure of commutative algebras, and show that the Galois closure $A^{(n)}$ of an R-algebra A of rank n, with the natural action of the symmetric group S_n is Tate over R. This can be seen as a (weak) Galois property of the Galois closure. In fact, we will prove more.

Let $K \to L$ be a separable extension of degree n. Let M be the Galois closure of L over K. Assume the Galois group of M over K is the symmetric group S_n. For $0 \leq m \leq n$ the subgroup S_m of S_n acts on M, and the corresponding field L^{S_m} is isomorphic to the intermediate field K_{n-m} defined in the introduction to chapter 1. Similarly, we will show that the Galois closure $A^{(n)}$ of an R-algebra of rank n, is Tate with group S_m over $A^{(m)}$. We now make this more precise.

Let A be an R-algebra of rank n. Let S be a finite set. Let T be a subset of S. Denote by $(\alpha_s)_{s\in S}$ the natural maps $A \to A^{(S)}$, and by $(\beta_t)_{t\in T}$ the natural maps $A \to A^{(T)}$. Note that $\prod_{t\in T}(X - \alpha_t(a))$ divides the characteristic polynomial of a in $A^{(S)}[X]$ for every $a \in A$ (and similarly for an a in a base change of A). Hence by the universal property of $A^{(T)}$ we have a unique map

$A^{(T)} \to A^{(S)}$ such that for every $t \in T$ the following diagram commutes



Recall from remark 1.3.15 that the symmetric group $\operatorname{Sym} S$ acts on $A^{(S)}$, permuting the maps α_s. Hence also the subgroup $G = \operatorname{Sym}(S \setminus T)$ of $\operatorname{Sym} S$ acts on $A^{(S)}$. Clearly G acts by $A^{(T)}$-algebra homomorphisms, so $\operatorname{Spec} A^{(S)}$ is a G-scheme over $\operatorname{Spec} A^{(T)}$. We will prove the following.

Theorem (Theorem 3.2.9)**.** *Let A be an R-algebra of rank n. Let S be a set with $\#S = n$, and let $T \subseteq S$. Let G be the group* $\operatorname{Sym}(S \setminus T)$*. Then* $\operatorname{Spec} A^{(S)}$ *with the natural action of G is a Tate G-scheme over* $\operatorname{Spec} A^{(T)}$*.*

By theorem 2.4.15 this is equivalent to saying that the map $A^{(T)} \to (A^{(S)})^G$ is a universal homeomorphism. In our proof of the above theorem the product formula for the S-closure (theorem 1.4.4) will be a crucial ingredient.

3.2 Proof of the main theorem

To prove that $A^{(T)} \to A^{(S)}$ is Tate with group $G = \operatorname{Sym}(S \setminus T)$ it suffices to prove that $A^{(S)}$ is integral over $A^{(T)}$, that the scheme morphism $\operatorname{Spec} A^{(S)} \to \operatorname{Spec} A^{(T)}$ is surjective, and that for all algebraically closed fields K the action of G on each fiber of

$$\operatorname{Hom}_{R\text{-Alg}}\left(A^{(S)}, K\right) \to \operatorname{Hom}_{R\text{-Alg}}\left(A^{(T)}, K\right)$$

is transitive. We will first prove integrality.

Proposition 3.2.1. *Let A be an R-algebra of rank n. Let S be a finite set. Then $A^{(S)}$ is integral over R.*

Proof. The elements $\alpha_s(a)$ for $s \in S$ and $a \in A$ form a set of R-algebra generators for $A^{(S)}$ (see remark 1.3.2). Since products and sums of integral elements are integral, it is sufficient to show $\alpha_s(a)$ is integral over R for all $s \in S$ and $a \in A$. By the defining property of $A^{(S)}$ these are roots of $P_a(X)$, which is in $R[X]$ and is monic, so $R \to A^{(S)}$ is integral. This concludes the proof. □

Corollary 3.2.2. *Let A be an R-algebra of rank n. Let S be a finite set, and let T be a subset of S. Then $A^{(S)}$ is integral over $A^{(T)}$.*

Proof. Follows immediately from proposition 3.2.1 since $A^{(T)} \to A^{(S)}$ is an R-algebra map. □

For the rest of the proof we will need to describe the map

$$\mathrm{Hom}_{K\text{-Alg}}\left(A^{(S)}, K\right) \to \mathrm{Hom}_{K\text{-Alg}}\left(A^{(T)}, K\right)$$

when A is a finite algebra over the algebraically closed field K. We do this in proposition 3.2.4. First we introduce some notation.

Definition 3.2.3. Let K be an algebraically closed field. Let A be a K-algebra of rank n. Fix a decomposition $A = A_1 \times \cdots \times A_m$ of A in connected K-algebras (see lemma 1.4.13). Let S be a finite set. We define a map

$$\Phi_S \colon \mathrm{Hom}_{K\text{-Alg}}\left(A^{(S)}, K\right) \to \mathrm{Maps}(S, \{1, \ldots, m\})$$

in the following way. Take $f \in \mathrm{Hom}_{K\text{-Alg}}(A^{(S)}, K)$. Let s be in S. Consider $f \circ \alpha_s \colon A \to K$. This map factors through A_i for some $i \in \{1, \ldots, m\}$ (see also lemma 1.4.3). Then the image of s via $\Phi_S(f)$ is i.

Let n_i be the rank of A_i. We denote by $\mathscr{F}_S \subseteq \mathrm{Maps}(S, \{1, \ldots, m\})$ the set of maps $F \colon S \to \{1, \ldots, m\}$ such that for all $i = 1, \ldots, m$ we have that $F^{-1}(i)$ has at most n_i elements.

Proposition 3.2.4. *Let K be an algebraically closed field. Let S be a finite set. We refer to definition 3.2.3 for the notation regarding A, and the map Φ_S. Then*

$$\Phi_S \colon \mathrm{Hom}_{K\text{-}Alg}\left(A^{(S)}, K\right) \to \mathscr{F}_S$$

is a bijection.

Moreover: let $T \subseteq S$ and let $f \colon \mathscr{F}_S \to \mathscr{F}_T$ be the map sending F to its restriction to T. Then the following diagram commutes:

$$\begin{array}{ccc} \mathrm{Hom}_{K\text{-}Alg}\left(A^{(S)}, K\right) & \xrightarrow{\Phi_S} & \mathscr{F}_S \\ \downarrow & & \downarrow f \\ \mathrm{Hom}_{K\text{-}Alg}\left(A^{(T)}, K\right) & \xrightarrow[\Phi_T]{} & \mathscr{F}_T \end{array}$$

Proof. By the product formula for the S-closure (theorem 1.4.4) we can write

$$A^{(S)} = \prod_{F \colon S \to \{1,\ldots,m\}} A^{(F)}$$

where the product is indexed over all maps $F \colon S \to \{1, \ldots, m\}$ and

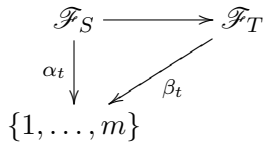
$$A^{(F)} = \bigotimes_{i=1}^{m} A_i^{(F^{-1}(i))}.$$

By number *1* of proposition 1.3.12, if $F^{-1}(i)$ has more than n_i elements for some i then $A^{(F^{-1}(i))}$ is zero, and hence $A^{(F)}$ is zero. If $F^{-1}(i)$ has at most n_i elements, then by lemma 1.4.16 we have that $A^{(F^{-1}(i))}$ is local. If $F \in \mathscr{F}_S$ then this happens for all $i = 1, \ldots, m$. So $A^{(F)}$ is a tensor product of finite local K-algebras with residue field K. Hence when $F \in \mathscr{F}_S$ we have that $A^{(F)}$ is local. So by corollary 1.4.14 for all $F \in \mathscr{F}_S$ we have a unique K-algebra map $A^{(F)} \to K$. Hence $\mathrm{Hom}_{K\text{-Alg}}(A^{(F)}, K)$ is empty if $F \notin \mathscr{F}_S$ and has one element if $F \in \mathscr{F}_S$. In particular

$$\Phi_S \colon \mathrm{Hom}_{K\text{-Alg}}\left(A^{(S)}, K\right) \to \mathscr{F}_S$$

is bijective.

By corollary 1.4.14 for each $i = 1, \ldots, m$ there is a unique K-algebra map $A_i \to K$. Hence $\mathrm{Hom}_{K\text{-Alg}}(A, K)$ is in bijection with $\{1, \ldots, m\}$. For all $t \in T$ the map α_t induces a map $\mathrm{Hom}_{K\text{-Alg}}(A^{(S)}, K) \to \mathrm{Hom}_{K\text{-Alg}}(A, K)$ by composition. The corresponding map $\mathscr{F}_S \to \{1, \ldots, m\}$ is the evaluation map, sending F to $F(t)$. In the same way for $t \in T$ the map $\mathscr{F}_T \to \{1, \ldots, m\}$ corresponding to β_t is the evaluation in t. The map $\mathscr{F}_S \to \mathscr{F}_T$ corresponding to the natural map $A^{(T)} \to A^{(S)}$ is the unique map such that for all $t \in T$ the following diagram commutes:



Since f makes the diagram above commute for all $t \in T$, the second claim is proved. □

Lemma 3.2.5. *Let A be an R-algebra of rank n. Let S be a set with $\#S \leq n$, and let T be a subset of S. Then the natural map* $\mathrm{Spec}\, A^{(S)} \to \mathrm{Spec}\, A^{(T)}$ *is surjective.*

Proof. It is sufficient to show that for every algebraically closed field K the map $\mathrm{Hom}_{R\text{-Alg}}(A^{(S)}, K) \to \mathrm{Hom}_{R\text{-Alg}}(A^{(T)}, K)$ is surjective. Since the constructions involved commute with base change, we can assume that R is equal to K, and prove that the map

$$\mathrm{Hom}_{K\text{-Alg}}\left(A^{(S)}, K\right) \to \mathrm{Hom}_{K\text{-Alg}}\left(A^{(T)}, K\right)$$

is surjective. By lemma 1.4.13 the K-algebra A can be written as $A_1 \times \cdots \times A_m$, with A_i local with residue field K and finite rank n_i. Take x in $\mathrm{Hom}_{K\text{-Alg}}(A^{(T)}, K)$. By proposition 3.2.4 the element x corresponds to a map $F' \colon T \to \{1, \ldots, m\}$ in $\mathscr{F}_T$. We can extend F' to a map $F \colon S \to \{1, \ldots, m\}$ in $\mathscr{F}_S$ because $\sum n_i$ is n and $\#S$ is at most n. The proof is then complete. □

Remark 3.2.6. Lemma 3.2.5 and corollary 3.2.2 together imply that the kernel of the natural map $A^{(T)} \to A^{(S)}$ consists of nilpotent elements. In all the examples we have computed the map is in fact injective. It would be interesting to know whether this is always the case.

Lemma 3.2.7. *Let S be a finite set. Let* $\operatorname{Sym} S$ *be the symmetric group on S. Let $n_1, \ldots, n_m$ be non-negative integers. Then the action of* $\operatorname{Sym} S$ *on the set of maps $F\colon S \to \{1, \ldots, m\}$ such that for all $i = 1, \ldots, m$ we have that $F^{-1}(i)$ has n_i elements is transitive.*

Proof. Clear. □

Lemma 3.2.8. *Let K be an algebraically closed field, and let A be a K-algebra of rank n. Let S be a set with $\#S = n$. Let T be a subset of S and let G be the group* $\operatorname{Sym}(S \setminus T)$. *Then G acts transitively on each fibers of*

$$\Phi_{S,T}\colon \operatorname{Hom}_{K\text{-}Alg}\left(A^{(S)}, K\right) \to \operatorname{Hom}_{K\text{-}Alg}\left(A^{(T)}, K\right)$$

Proof. By lemma 1.4.13 the K-algebra A can be written as $A_1 \times \cdots \times A_m$, with A_i local with residue field K and finite of rank n_i. In proposition 3.2.4 we described the set $\operatorname{Hom}_{K\text{-Alg}}(A^{(S)}, K)$ and the map $\Phi_{S,T}$. Since $\#S = n$ we have that $\operatorname{Hom}_{K\text{-Alg}}(A^{(S)}, K)$ is in bijection with the set $\mathscr{F}_S$ of maps $F\colon S \to \{1, \ldots, m\}$ such that for all $i = 1, \ldots, m$ we have that $F^{-1}(i)$ has n_i elements. The group G acts on $\mathscr{F}_S$ via its natural action on S. Let F' be a map $T \to \{1, \ldots, m\}$, and suppose ${F'}^{-1}(i)$ has at most n_i elements for all i. The fiber of $\Phi_{S,T}$ on F' is the set of maps $F\colon S \setminus T \to \{1, \ldots, m\}$ such that for all $i = 1, \ldots, m$ we have that $F^{-1}(i)$ has $n_i - \#{F'}^{-1}(i)$ elements. By lemma 3.2.7 we have that G acts transitively on this set. So the proof is complete. □

The main result now follows easily.

Theorem 3.2.9. *Let A be an R-algebra of rank n. Let S be a set with $\#S = n$, and let T be a subset of S. Let G be the group* $\operatorname{Sym}(S \setminus T)$. *Then $A^{(T)} \to A^{(S)}$ with the action of G is Tate.*

Proof. We proved that $A^{(T)} \to A^{(S)}$ is integral in corollary 3.2.2. We proved that $\operatorname{Spec} A^{(S)} \to \operatorname{Spec} A^{(T)}$ is surjective in lemma 3.2.5. To conclude we need to show that for all $R \to K$ with K an algebraically closed field the action of G on each fiber of

$$\operatorname{Hom}_{R\text{-Alg}}\left(A^{(S)}, K\right) \to \operatorname{Hom}_{R\text{-Alg}}\left(A^{(T)}, K\right)$$

is transitive. This follows from lemma 3.2.8, since the constructions involved commute with base change. □

Corollary 3.2.10. *Let A be an R-algebra of rank n. Let S be a set with $\#S = n$, and let T be a subset of S. Let G be the group* $\mathrm{Sym}(S \setminus T)$. *Then the natural map $A^{(T)} \to (A^{(S)})^G$ is a universal homeomorphism.*

Proof. Follows immediately from theorem 3.2.9 and theorem 2.4.15. □

Corollary 3.2.11. *Let A be an R-algebra of rank n. Then $R \to \left(A^{(n)}\right)^{S_n}$ is a universal homeomorphism.*

Proof. Apply corollary 3.2.10 with $S = \{1, \ldots, n\}$ and $T = \varnothing$. □

Example 3.2.12 (Étale case)**.** Let R be a connected ring. Let $\alpha\colon R \to K$ be a geometric point of R. Let π be the étale fundamental group of R in α. Let A be a finite étale R-algebra of rank n and let X be the corresponding π-set (see theorem 1.4.9). Then by proposition 1.4.11 for any finite set S with $\#S = n$ we have that $A^{(S)}$ corresponds to the set $\mathrm{Bij}(S, X)$ of bijections $S \to X$, with left action of π induced by the one on X. For all subsets T of S the group $G = \mathrm{Sym}(S \setminus T)$ acts on the right on this set, and the action commutes with the action of π. The quotient $Y = \mathrm{Bij}(S, X)/G$ is the π-set of injections from T to X. By proposition 1.4.11 the π-set Y corresponds to the R-algebra $A^{(T)}$. So in this case $A^{(T)} \to (A^{(S)})^G$ is an isomorphism.

Example 3.2.13 (Local case)**.** Let K be an algebraically closed field. Let A be a local K-algebra of rank n. Let S be a finite set with $\#S = n$. Let T be a subset of S. Let G be the group $\mathrm{Sym}(S \setminus T)$. By lemma 1.4.16 both $A^{(S)}$ and $A^{(T)}$ are local. Since $A^{(S)}$ is finite and local, we have that $\mathrm{Hom}_{K\text{-Alg}}(A^{(S)}, K)$ has one element by corollary 1.4.14.

By lemma 2.4.3 the map $(\operatorname{Spec} A^{(S)})(K) \to (\operatorname{Spec}(A^{(S)})^G)(K)$ is surjective. Hence also $\mathrm{Hom}_{K\text{-Alg}}((A^{(S)})^G, K)$ has one element. So the map

$$\mathrm{Hom}_{K\text{-Alg}}\left((A^{(S)})^G, K\right) \to \mathrm{Hom}_{K\text{-Alg}}\left(A^{(T)}, K\right)$$

is bijective, and then $\operatorname{Spec}(A^{(S)})^G \to \operatorname{Spec} A^{(T)}$ is universally bijective by lemma 2.4.9. Finally, the map $A^{(T)} \to (A^{(S)})^G$ is integral, hence it is a universal homeomorphism by theorem 2.3.8.

Chapter 4

Discriminant algebras

4.1 Introduction

Let K be a field of characteristic different from 2. Let f be a polynomial of degree n in $K[x]$, with leading coefficient equal to 1. Let $x_1, \ldots, x_n$ be the roots of f in an algebraic closure $\bar{K}$ of K. Then the *discriminant* of f is

$$\Delta_f = \prod_{i<j}(x_i - x_j)^2 \in K.$$

Obviously Δ_f is zero if and only if f has a double root. Hence Δ_f is invertible if and only if $L = K[X]/(f)$ is finite étale over K. Assume f is irreducible and Δ_f non zero. In this case let M be the splitting field of f (inside $\bar{K}$). Suppose the Galois group of M over K is the full symmetric group S_n. The square roots of Δ_f are in M since they are

$$\pm \prod_{i<j}(x_i - x_j),$$

and the x_i are elements of M. The subextension $K \to K[\sqrt{\Delta_f}\ ]$ of M is M^{A_n}. In particular $K \to K[\sqrt{\Delta_f}\ ]$ only depends on the extension L/K, and not on f.

Let R be a connected ring. Let $\alpha\colon R \to K$ be a geometric point of R. Let $\pi = \pi(R, \alpha)$ be the étale fundamental group of R in α. Let A be a finite étale R-algebra of rank n. Using π-sets (see theorem 1.4.9) one can define a finite étale R-algebra $\Delta^{\text{ét}}(A/R)$ of rank 2. In the case of a separable extension of fields this generalizes the A_n-invariants of M. This will be made precise in definition 4.2.12.

Alternatively, one could try to generalize the extension $K[\sqrt{\Delta_f}\ ]$ to more general rings. Let R be a ring. Let A be an R-algebra of rank n. Let

$\{a_1, \ldots, a_n\}$ be a basis of A. It is possible to define an element $\Delta(a_1, \ldots, a_n)$ of R, the discriminant of A with respect to the given basis. (Changing the basis changes the discriminant by the square of a unit in R.) One may then construct a natural R-algebra $\Delta^{1/2}(A/R)$ of rank 2 in which the discriminant has a square root. This construction will be particularly interesting when 2 is invertible in R. We will make this precise in definition 4.2.3.

Let R be a connected ring. Let A be an R-algebra of rank n. We have that $\Delta^{\text{ét}}(A/R)$ is isomorphic to $\Delta^{1/2}(A/R)$ when 2 is invertible in R and A is finite étale. We will give a proof of this known fact in proposition 4.2.13. This is not true if 2 is not invertible in R, see example 4.2.7.

Let R be a $\mathbb{Z}[1/2]$-algebra. Let A be an R-algebra of rank n. In this chapter we will explicitly construct a natural ring homomorphism $\lambda\colon \Delta^{1/2}(A/R) \to A^{(n)}$, and prove the following theorem.

Theorem (Theorem 4.3.8)**.** *Let R be a $\mathbb{Z}[1/2]$-algebra. Let A be an R-algebra of rank n. Then $\lambda\colon \Delta^{1/2}(A/R) \to A^{(n)}$ is Tate with group A_n.*

By theorem 2.4.15 this implies that $\Delta^{1/2}(A/R) \to (A^{(n)})^{A_n}$ is a universal homeomorphism. I do not know if this map is an isomorphism in general.

A natural question is whether it is possible to define for all rings R and R-algebras A of rank n an R-algebra $\Delta(A/R)$ of rank 2, generalizing both $\Delta^{\text{ét}}(A/R)$ and $\Delta^{1/2}(A/R)$. Here is a list of properties that $\Delta(A/R)$ should have:

- The construction of $\Delta(A/R)$ is functorial under isomorphisms and commutes with arbitrary base change.
- If A is finite étale and R is connected then $\Delta(A/R)$ is isomorphic to $\Delta^{\text{ét}}(A/R)$.
- If 2 is invertible in R then $\Delta(A/R)$ is isomorphic to $\Delta^{1/2}(A/R)$.
- We have that $\Delta(A/R)$ is finite étale if and only if A is finite étale.

Constructions satisfying these properties have been given by Pierre Deligne in [7] and by Ottmar Loos in [20]. In section 4.4 we will give indications on future work (joint with Owen Biesel), which gives a new and simpler construction of $\Delta(A/R)$. This uses ideas coming from the Galois closure for rings.

We will start by presenting preliminary results in section 4.2. These include the definitions of $\Delta^{\text{ét}}(A/R)$ and $\Delta^{1/2}(A/R)$, and the proof of some of the properties described above. We will then define the map $\lambda\colon \Delta^{1/2}(A/R) \to A^{(n)}$, and prove the above theorem in section 4.3. Finally we will give the new definition of $\Delta(A/R)$ in section 4.4.

4.2 Preliminaries

We give first the definition of discriminant for R-algebras of rank n.

Definition 4.2.1. Let A be an R-algebra of rank n. Recall from definition 1.2.4 the trace map $s_1 \colon A \to R$. The *discriminant form* of A is the bilinear form δ_A on $\bigwedge^n A$ defined as follows:

$$\delta_A(x_1 \wedge \cdots \wedge x_n, y_1 \wedge \cdots \wedge y_n) = \det\left(s_1(x_i y_j)\right)_{ij}$$

where $\det(a_{ij})_{ij}$ denotes the determinant of the matrix with a_{ij} in the i-th row and j-th column.

Remark 4.2.2. Let f be a polynomial in $R[x]$, with leading coefficient equal to 1. Consider the basis $1, x, \ldots, x^{n-1}$ of $A = R[x]/(f)$. The discriminant of f, defined in the introduction, is equal to $\delta_A(1 \wedge x \wedge \cdots \wedge x^{n-1}, 1 \wedge x \wedge \cdots \wedge x^{n-1})$.

We can now define the discriminant algebra $\Delta^{1/2}(A/R)$ of an R-algebra A of rank n, when 2 is invertible in R.

Definition 4.2.3. Let R be a $\mathbb{Z}[1/2]$-algebra. Let A be an R-algebra of rank n. The *discriminant algebra* of A is an R-algebra $\Delta^{1/2}(A/R)$ defined as follows. As an R-module $\Delta^{1/2}(A/R)$ is equal to $R \oplus \bigwedge^n A$. We define a multiplication using the bilinear form δ_A: let $x = x_1 \wedge \cdots \wedge x_n$ and $y = y_1 \wedge \cdots \wedge y_n$. Then for all r, r' in R we define

$$(r + x)(r' + y) = rr' + \delta_A(x, y) + ry + r'x$$

in $\Delta^{1/2}(A/R)$.

Remark 4.2.4. Definition 4.2.3 makes sense over any ring R, but we will show later that if 2 is not invertible in R this algebra does not have the properties we want (see example 4.2.7).

Remark 4.2.5. The above defines a functor from the category of R-algebras of rank n (with isomorphisms as morphisms) to R-algebras of rank 2. The construction of $\Delta^{1/2}(A/R)$ commutes with arbitrary base change.

Proposition 4.2.6. *Let R be a $\mathbb{Z}[1/2]$-algebra. Then $\Delta^{1/2}(R^n/R)$ is isomorphic to R^2 as an R-algebra.*

Proof. Let $e_1, \ldots, e_n$ be the standard basis of R^n. Take $e = e_1 \wedge \cdots \wedge e_n$ as a basis of $\bigwedge^n A$. By definition of $\Delta^{1/2}(R^n/R)$ we have

$$e^2 = \delta_{R^n}(e, e) = \det(s_1(e_i e_j))_{ij} = \det\left(\delta_{ij}\right)_{ij} = 1.$$

Since 2 is invertible in R the elements $(1 - e)/2$ and $(1 + e)/2$ are in $\Delta^{1/2}(R^n/R)$. These elements form a complete set of orthogonal idempotents in $\Delta^{1/2}(R^n/R)$. Hence $\Delta^{1/2}(R^n/R)$ is isomorphic to R^2 as an R-algebra, as we wanted to show. □

Example 4.2.7. Consider the $\mathbb{Z}$-algebra $\mathbb{Z}^n$. Then $\mathbb{Z} \oplus \bigwedge^n \mathbb{Z}^n$ with multiplication given by the discriminant form is isomorphic to $\mathbb{Z}[x]/(x^2-1)$. This is not isomorphic to $\mathbb{Z}^2$ as a $\mathbb{Z}$-algebra. This shows that proposition 4.2.6 does not hold if 2 is not invertible in R.

Lemma 4.2.8. *Let R be a ring. Let $n \geq 0$ be an integer and let M and N be R-modules of rank n. Let $f\colon M \to N$ be an R-module map. Then f is an isomorphism if and only if the induced map $\bigwedge^n M \to \bigwedge^n N$ is an isomorphism.*

Proof. See [5, Chapitre III, §8, no. 2, Théorème 1] for the free case. The result follows in general by localizing at primes of R. □

Lemma 4.2.9. *Let R be a ring. Let M and N be R-modules. Let L be an R-module of rank 1. Let $f\colon M \to N$ be an R-module map. Then f is an isomorphism if and only if $(f \otimes \mathrm{Id}_L)\colon M \otimes_R L \to N \otimes_R L$ is an isomorphism.*

Proof. This is clear if L is free. In general it follows by localizing at primes of R. □

Lemma 4.2.10. *Let R be a ring. Let M be an R-module of rank n. Then the map $\bigwedge^n(M^\vee) \otimes \bigwedge^n M \to R$ defined by*

$$(f_1 \wedge \cdots \wedge f_n) \otimes (x_1 \wedge \cdots \wedge x_n) \mapsto \det\left(f_i(x_j)\right)_{ij}$$

is an isomorphism.

Proof. By localizing at primes of R we can reduce to M a free R-module. Let $e_1, \ldots, e_n$ be a basis of M and let $X_1, \ldots, X_n$ be the dual basis. Since $(X_1 \wedge \cdots \wedge X_n) \otimes (e_1 \wedge \cdots \wedge e_n)$ is sent to 1, the proof is complete. □

Lemma 4.2.11. *Let A be an R-algebra of rank n. Then A is finite étale if and only if the map $\bigwedge^n A \otimes \bigwedge^n A \to R$ induced by the discriminant form δ_A is an isomorphism.*

Proof. By definition 1.4.6 we have that A is finite étale if and only if the map $f\colon A \to A^\vee$ given by

$$a \mapsto (b \mapsto s_1(ab))$$

is an isomorphism. By lemma 4.2.8 this is an isomorphism if and only if $\bigwedge^n f\colon \bigwedge^n A \to \bigwedge^n(A^\vee)$ is an isomorphism. By lemma 4.2.9 this is an isomorphism if and only if $\bigwedge^n A \otimes \bigwedge^n A \to \bigwedge^n(A^\vee) \otimes \bigwedge^n A$ is an isomorphism.

Composing with the isomorphism in lemma 4.2.10 we have that $\bigwedge^n f$ is an isomorphism if and only if the map

$$\bigwedge^n A \otimes \bigwedge^n A \to R$$
$$x_1 \wedge \cdots \wedge x_n \otimes y_1 \wedge \cdots \wedge y_n \mapsto \det\left(f(x_i)(y_j)\right)_{ij}$$

is an isomorphism. This is equal to the map induced by δ_A, so the proof is complete. □

Definition 4.2.12. Let R be a connected ring. Let $\alpha\colon R \to K$ be a geometric point of R. Let $\pi = \pi(R, \alpha)$ be the étale fundamental group of R in α. Let A be a finite étale R-algebra of rank n, corresponding to a π-set X. Consider the π-set $\mathrm{Bij}(\{1, \ldots, n\}, X)$ of bijections from $\{1, \ldots, n\}$ to X, with left action of π induced by the one on X. The symmetric group on n letters S_n acts on the right on the π-set $\mathrm{Bij}(\{1, \ldots, n\}, X)$, and so does the subgroup A_n of even permutations. We denote by $\mathrm{Or}\, X$ the quotient by the action of A_n, and call it the π-set of *orientations* of X. This is a set with two elements. We denote by $\Delta^{\text{ét}}(A/R)$ the corresponding finite étale R-algebra of rank 2.

Proposition 4.2.13. *Let R be a $\mathbb{Z}[1/2]$-algebra. Let A be an R-algebra of rank n. Then $\Delta^{1/2}(A/R)$ is finite étale if and only if A is finite étale.*

Suppose moreover that R is connected, and that A is finite étale. Let $\alpha\colon R \to K$ be a geometric point of R. Let $\pi = \pi(R, \alpha)$ be the étale fundamental group of R in α. Let X be the π-set corresponding to A. Then $\Delta^{1/2}(A/R)$ corresponds to $\mathrm{Or}\, X$.

Proof. By lemma 4.2.11 is sufficient to show that δ_A is an isomorphism if and only if $\delta_{\Delta^{1/2}(A/R)}$ is an isomorphism. Let M be $\bigwedge^2(\Delta^{1/2}(A/R))$. The map $\bigwedge^n A \to M$ that sends $x \in \bigwedge^n A$ to $1 \wedge x$ in M is an isomorphism. We show that the following diagram

$$\begin{array}{ccc} \bigwedge^n A \otimes \bigwedge^n A & \xrightarrow{\delta_A} & R \\ \sim\downarrow & & \sim\downarrow \cdot 4 \\ M \otimes M & \xrightarrow[\delta_{\Delta^{1/2}(A/R)}]{} & R \end{array}$$

commutes. Let $x \otimes y$ be in $\bigwedge^n A \otimes \bigwedge^n A$. By applying the map corresponding to δ_A and then multiplying by 4 we get $4\delta_A(x, y)$. On the other hand $x \otimes y$ is sent to $(1 \wedge x) \otimes (1 \wedge y)$ in $M \otimes M$, which is sent to the determinant of the matrix

$$\begin{pmatrix} s_1(1) & s_1(x) \\ s_1(y) & s_1(xy) \end{pmatrix}$$

by $\delta_{\Delta^{1/2}(A/R)}$ (here s_1 denotes the trace in $\Delta^{1/2}(A/R)$). Since $\Delta^{1/2}(A/R)$ has rank 2, we have that $s_1(1)$ is 2. Note that by definition of the multiplication in $\Delta^{1/2}(A/R)$ we have that xy is equal to $\delta_A(x,y)$, which is in R. So $s_1(xy)$ is $2\delta_A(x,y)$. Moreover $s_1(x)$ and $s_1(y)$ are zero. So the determinant is $4\delta_A(x,y)$, and the diagram commutes. Since 2 is invertible in R, multiplication by 4 is an isomorphism, so δ_A is an isomorphism if and only if $\delta_{\Delta^{1/2}(A/R)}$ is an isomorphism. Hence A is étale if and only if $\Delta^{1/2}(A/R)$ is étale.

To conclude the proof it suffices to show that if A is finite étale then the π-set corresponding to $\Delta^{1/2}(A/R)$ is $\operatorname{Or} X$. Since the construction of $\Delta^{1/2}(A/R)$ commutes with base change we can base change to K via α. Since $A \otimes_R K$ is isomorphic to K^X, the π-set corresponding to $\Delta^{1/2}(A/R)$ is equal to $\operatorname{Hom}_{K\text{-Alg}}(\Delta^{1/2}(K^X/K), K)$. We define a natural bijection between this set and $\operatorname{Or} X$.

Let x be in X. Let $e_x\colon X \to K$ be the map sending x to 1 and other elements to 0. Clearly $\{e_x\}_{x\in X}$ is a basis of K^X. Let g be a bijection from $\{1,\dots,n\}$ to X. The element $e_g = e_{g(1)} \wedge \cdots \wedge e_{g(n)}$ forms a basis of $\bigwedge^n K^X$. Hence, a K-algebra map $\Delta^{1/2}(K^X/R) \to K$ is completely determined by its value on e_g. This can only be 1 or -1 since the square of e_g in $\Delta^{1/2}(K^X/R)$ is 1, as we proved in proposition 4.2.6. (Note that the characteristic of K is different from 2, since $1/2$ is in R.) We define a map

$$\Phi\colon \operatorname{Bij}(\{1,\dots,n\}, X) \to \operatorname{Hom}_{K\text{-Alg}}(\Delta^{1/2}(K^X/K), K)$$

by sending a $g \in \operatorname{Bij}(\{1,\dots,n\}, X)$ to the map sending e_g to 1. For every σ in the symmetric group S_n we have that $e_{g\circ\sigma}$ is equal to e_g if and only if σ is an even permutation. If not then $e_{g\circ\sigma}$ is equal to $-e_g$. So for σ odd we have that $\Phi(e_{g\circ\sigma})$ sends e_g to -1. In particular Φ is surjective. Moreover Φ factors through $\operatorname{Or} X$, giving the bijection we were looking for. □

Remark 4.2.14. Proposition 4.2.13 shows that if 2 is invertible in R, and R is connected then the two functors $\Delta^{\text{ét}}(-/R)$ and $\Delta^{1/2}(-/R)$ are isomorphic.

4.3 Statement and proof of the main theorem

Let R be a $\mathbb{Z}[1/2]$-algebra. Let A be an R-algebra of rank n. We first define a map $\lambda\colon \Delta^{1/2}(A/R) \to A^{(n)}$.

Theorem 4.3.1. *Let A be an R-algebra of rank n. Let $A^{(n)}$ be the n-closure of A and let α_i for $i = 1,\dots,n$ be the natural maps. Then the R-module map $\lambda\colon \bigwedge^n A \to A^{(n)}$ defined by*

$$\lambda(x_1 \wedge \cdots \wedge x_n) = \det(\alpha_i(x_j))_{ij}$$

induces an R-algebra homomorphism $\Delta^{1/2}(A/R) \to A^{(n)}$.

Proof. Clearly λ is well defined. To prove the theorem it is sufficient to show that for $x = x_1 \wedge \cdots \wedge x_n$ and $y = y_1 \wedge \cdots \wedge y_n$ we have that $\lambda(x)\lambda(y)$ is equal to $\delta_A(x, y)$ in $A^{(n)}$. We have

$$\lambda(x)\lambda(y) = \det(\alpha_i(x_j))_{ij} \cdot \det(\alpha_i(y_j))_{ij}.$$

Since the determinant of a matrix is equal to the determinant of its transpose the above can be written as

$$\det(\alpha_j(x_i))_{ij} \cdot \det(\alpha_i(y_j))_{ij}.$$

Matrix multiplication gives then

$$\lambda(x)\lambda(y) = \det\left(\sum_{k=1}^{n} \alpha_k(x_i)\alpha_k(y_j)\right)_{ij},$$

and since the α_k are R-algebra homomorphisms we have

$$\det\left(\sum_{k=1}^{n} \alpha_k(x_i)\alpha_k(y_j)\right)_{ij} = \det\left(\sum_{k=1}^{n} \alpha_k(x_i y_j)\right)_{ij}.$$

Note that for all $a \in A$ we have that $-s_1(a)$ is the coefficient of X^{n-1} in $P_a(X)$, and $-\sum_k \alpha_k(a)$ is the coefficient of X^{n-1} in $\prod_k (X - \alpha_k(a))$. By definition of $A^{(n)}$ for all $a \in A$ the polynomials P_a and $\prod_k (X - \alpha_k(a))$ are equal in $A^{(n)}[X]$. So we have:

$$\det\left(\sum_{k=1}^{n} \alpha_k(x_i y_j)\right)_{ij} = \det(s_1(x_i y_i))_{ij} = \delta_A(x, y).$$

Hence in $A^{(n)}$ we have

$$\lambda(x)\lambda(y) = \delta_A(x, y),$$

as we wanted to show. □

We now will show that if 2 is invertible in R then λ is Tate with group A_n. It suffices to prove that λ is integral, that the corresponding scheme map $\operatorname{Spec} A^{(n)} \to \operatorname{Spec} \Delta^{1/2}(A/R)$ is surjective and that for all algebraically closed fields K the action of A_n on each fiber of

$$\operatorname{Hom}_{R\text{-Alg}}\left(A^{(n)}, K\right) \to \operatorname{Hom}_{R\text{-Alg}}\left(\Delta^{1/2}(A/R), K\right)$$

is transitive. We first show that λ is integral.

Proposition 4.3.2. *Let A be an R-algebra of rank n. Then we have that $\lambda\colon \Delta^{1/2}(A/R) \to A^{(n)}$ is integral.*

Proof. By proposition 3.2.1 we have that $A^{(n)}$ is integral over R. Since λ is an R-algebra map this concludes the proof. □

For the rest of the proof we will need to describe the map

$$\mathrm{Hom}_{K\text{-Alg}}\left(A^{(n)}, K\right) \to \mathrm{Hom}_{K\text{-Alg}}\left(\Delta^{1/2}(A/R), K\right)$$

when A is a finite étale algebra over the algebraically closed field K.

Proposition 4.3.3. *Let K be an algebraically closed field of characteristic different from 2. Consider the K-algebra $A = K^X$ for a finite set X of cardinality n. Then the diagram*

$$\begin{array}{ccc} \mathrm{Bij}(\{1,\dots,n\}, X) & \longrightarrow & \mathrm{Or}\, X \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{K-\mathrm{Alg}}\left(A^{(n)}, K\right) & \xrightarrow[\lambda]{} & \mathrm{Hom}_{K\text{-}Alg}\left(\Delta^{1/2}(A/K), K\right) \end{array}$$

commutes, where the bottom map is the map induced by λ, and the vertical ones are the bijections defined in proposition 1.4.11 and in proposition 4.2.13.

Proof. We denote by B the set $\mathrm{Bij}(\{1,\dots,n\}, X)$. Let x be in X. Let $e_x \colon X \to K$ be the map sending x to 1 and other elements to 0. Clearly $\{e_x\}_{x\in X}$ is a basis of K^X. Fix g in B. Denote by e_g the element $e_{g(1)} \wedge \cdots \wedge e_{g(n)}$ of $\bigwedge^n A$. Let $[g]$ be the image of g in $\mathrm{Or}\, X$. By proposition 4.2.13 the map $\mathrm{Or}\, X \to \mathrm{Hom}_{K\text{-Alg}}(\Delta^{1/2}(A/K), K)$ sends $[g]$ to the unique K-algebra map $\Delta^{1/2}(A/K) \to K$ sending e_g to 1.

By proposition 1.4.11 we have that $A^{(n)}$ is isomorphic to K^B. The map $B \to \mathrm{Hom}_{K-\mathrm{Alg}}(A^{(n)}, K)$ sends g to the projection to the component corresponding to g, which will be denoted π_g. Finally, the map $\mathrm{Hom}_{K-\mathrm{Alg}}(A^{(n)}, K) \to \mathrm{Hom}_{K\text{-Alg}}(\Delta^{1/2}(A/K), K)$ sends π_g to the composition $\pi_g \circ \lambda$. We prove that this K-algebra map sends e_g to 1.

For $i = 1, \dots, n$ let α_i be the natural map $A \to A^{(n)}$. We have

$$\pi_g\Big(\lambda(e_g)\Big) = \pi_g\Big(\det(\alpha_i(e_{g(j)}))_{ij}\Big) = \det\Big(\pi_g(\alpha_i(e_{g(j)}))\Big)_{ij}.$$

From the description of α_i given in theorem 1.4.4 we have that $\alpha_i(e_{g(j)})$ is equal to $\Big(e_{g(j)}(h(i))\Big)_{h\in B}$. So we have

$$\det\Big(\pi_g(\alpha_i(e_{g(j)}))\Big)_{ij} = \det\Big(e_{g(j)}(g(i))\Big)_{ij} = \det(\delta_{ij})_{ij}$$

which is 1. So $\pi_g \circ \lambda$ sends e_g to 1, as we wanted to show. □

Lemma 4.3.4. *Let K be an algebraically closed field of characteristic different from 2. Let A be an R-algebra of rank n. Suppose that A is not finite étale. Then $\Delta^{1/2}(A/R)$ is local.*

Proof. Up to isomorphism K^2 and $K[\varepsilon]/(\varepsilon^2)$ are the only K-algebras of rank 2. By proposition 4.2.13 we have that $\Delta^{1/2}(A/R)$ is not finite étale. Hence $\Delta^{1/2}(A/R)$ is isomorphic to $K[\varepsilon]/(\varepsilon^2)$, and so it is local. □

Proposition 4.3.5. *Let R be a $\mathbb{Z}[1/2]$-algebra. Let A be an R-algebra of rank n. Then the map* $\operatorname{Spec} A^{(n)} \to \operatorname{Spec} \Delta^{1/2}(A/R)$ *is surjective.*

Proof. It is sufficient to show that for every algebraically closed field K the map $\operatorname{Hom}_{R\text{-Alg}}(A^{(n)}, K) \to \operatorname{Hom}_{R\text{-Alg}}(\Delta^{1/2}(A/R), K)$ is surjective. Since the constructions involved commute with base change, we can then assume R is equal to K, and prove that the map

$$\operatorname{Hom}_{K\text{-Alg}}\left(A^{(n)}, K\right) \to \operatorname{Hom}_{K\text{-Alg}}\left(\Delta^{1/2}(A/R), K\right)$$

is surjective.

First suppose that A is not finite étale. Then by lemma 4.3.4 we have that $\Delta^{1/2}(A/R)$ is local. Hence $\operatorname{Hom}_{K\text{-Alg}}(\Delta^{1/2}(A/R), K)$ has one element by corollary 1.4.14. The map is then surjective.

If A is finite étale then A is isomorphic to K^X as a K-algebra, with X a finite set. By proposition 4.3.3 we have that the map $\operatorname{Hom}_{K\text{-Alg}}(A^{(n)}, K) \to \operatorname{Hom}_{K\text{-Alg}}(\Delta^{1/2}(A/R), K)$ corresponds to the quotient map

$$\operatorname{Bij}(\{1, \ldots, n\}, X) \to \operatorname{Or} X$$

via the bijections defined in proposition 1.4.11 and in proposition 4.2.13. In particular the map is surjective. □

Lemma 4.3.6. *Let $n_1, \ldots, n_m$ be non-negative integers. Suppose that there exists $i \in \{1, \ldots, m\}$ such that $n_i > 1$. Then the action of A_n on the set*

$$\mathscr{F} = \{F \colon \{1, \ldots, n\} \to \{1, \ldots, m\} \mid \text{for } i = 1, \ldots, m \colon \#F^{-1}(i) = n_i\}$$

is transitive.

Proof. Clear. □

Proposition 4.3.7. *Let K be an algebraically closed field of characteristic different from 2. Let A be a K-algebra of rank n. Then the action of A_n on each fiber of*

$$f \colon \operatorname{Hom}_{R\text{-}Alg}(A^{(n)}, K) \to \operatorname{Hom}_{R\text{-}Alg}(\Delta^{1/2}(A/R), K)$$

is transitive.

Proof. Write $A = A_1 \times \cdots A_m$ with A_i connected of rank n_i. Recall from proposition 3.2.4 that the set $\mathrm{Hom}_{K\text{-Alg}}(A^{(n)}, K)$ is in bijection with the set $\mathscr{F}$ of maps $F\colon \{1,\ldots,n\} \to \{1,\ldots,m\}$ such that $\#F^{-1}(i)$ is equal to n_i. We distinguish two cases.

First suppose that A is not finite étale. Then by lemma 4.3.4 we have that $\Delta^{1/2}(A/R)$ is local. So $\mathrm{Hom}_{R\text{-Alg}}(\Delta^{1/2}(A/R), K)$ has one element by corollary 1.4.14. The fiber is then equal to $\mathrm{Hom}_{K\text{-Alg}}(A^{(n)}, K)$. Since A is not finite étale there exists $i \in \{1,\ldots,m\}$ such that $n_i > 1$. Hence by lemma 4.3.6 the action of A_n on the fiber is transitive.

If A is finite étale then $\mathrm{Hom}_{K\text{-Alg}}(A^{(n)}, K) \to \mathrm{Hom}_{R\text{-Alg}}(\Delta^{1/2}(A/R), K)$ corresponds to the quotient map $S_n \to S_n/A_n$, as we proved in proposition 4.3.3. So the action of A_n on each fiber is transitive as we wanted to show. □

The main theorem now follows easily.

Theorem 4.3.8. *Let R be a $\mathbb{Z}[1/2]$-algebra. Let A be an R-algebra of rank n. Then $\lambda\colon \Delta^{1/2}(A/R) \to A^{(n)}$ is Tate with group A_n.*

Proof. We proved that $\Delta^{1/2}(A/R) \to A^{(n)}$ is integral in proposition 4.3.2. We proved that $\operatorname{Spec} A^{(n)} \to \operatorname{Spec} \Delta^{1/2}(A/R)$ is surjective in proposition 4.3.5. To conclude it suffices to show that for all $R \to K$ with K an algebraically closed field the action of G on each fiber of

$$\mathrm{Hom}_{R\text{-Alg}}\left(A^{(n)}, K\right) \to \mathrm{Hom}_{R\text{-Alg}}\left(\Delta^{1/2}(A/R), K\right)$$

is transitive. This follows from proposition 4.3.7, since the constructions involved commute with base change. □

Corollary 4.3.9. *Let R be a $\mathbb{Z}[1/2]$-algebra. Let A be an R-algebra of rank n. Then $\Delta^{1/2}(A/R) \to (A^{(n)})^{A_n}$ is a universal homeomorphism.*

Proof. Follows immediately from theorem 4.3.8 and theorem 2.4.15. □

4.4 More on discriminants

Let R be a ring. Let A be an R-algebra of rank n. We will define an R-algebra $\Delta(A/R)$ of rank 2, and list some of its properties without proof. This is forthcoming joint work with Owen Biesel. We will use results on polynomial laws from section 1.5.

Definition 4.4.1. Let R be a ring. Let A be an R-algebra of rank n. We denote by $\mathrm{Sym}_n A$ the ring of *symmetric tensors* $(A^{\otimes n})^{S_n}$.

Remark 4.4.2. Let R be a ring. Let A be an R-algebra of rank n. Recall the definition of $\operatorname{Sym} A$ and $\operatorname{Sym}^n A$ from 1.2.14 and example 1.2.15. We have that $(\operatorname{Sym}_n A)^\vee$ is naturally isomorphic to $\operatorname{Sym}^n(A^\vee)$.

Definition 4.4.3. Let R be a ring. Let A be an R-algebra of rank n. By proposition 1.5.9 the norm $s_n \colon \underline{A} \to \underline{R}$ gives a unique element of $\operatorname{Sym}^n(A^\vee)$. By remark 4.4.2 this gives an R-linear map $\varphi \colon \operatorname{Sym}_n A \to R$.

Proposition 4.4.4. *Let R be a ring. Let A be an R-algebra of rank n. Then the map $\varphi \colon \operatorname{Sym}_n A \to R$ is a ring homomorphism.*

Proof. The proof is in [9, Proposition 2.5.1]. It can also be found in the thesis of Owen Biesel. □

Definition 4.4.5. Let R be a ring. Let A be an R-algebra of rank n. Let S be $\operatorname{Sym}_n A$. The map φ makes R into an S-algebra. We define

$$\Delta(A/R) = (A^{\otimes n})^{A_n} \otimes_S R.$$

We give a list of facts about $\Delta(A/R)$ without proof. The proof will be contained in forthcoming work with Owen Biesel.

- The construction of $\Delta(A/R)$ is functorial under isomorphisms and commutes with arbitrary base change.
- If A is étale, then $\Delta(A/R)$ is isomorphic to $\Delta^{\text{ét}}(A/R)$ as an R-algebra.
- If 2 is invertible in R then $\Delta(A/R)$ is isomorphic to $\Delta^{1/2}(A/R)$ as an R-algebra.
- We have a short exact sequence of R-modules

  $$0 \to R \to \Delta(A/R) \to \bigwedge^n A \to 0$$

  where the map $R \to \Delta(A/R)$ is the natural map. In particular $\Delta(A/R)$ is locally free of rank 2.
- The natural isomorphism $\bigwedge^n A \to \bigwedge^{n+1}(A \times R)$, sending $x_1 \wedge \cdots \wedge x_n$ to $1 \wedge x_1 \wedge \cdots \wedge x_n$, induces a unique isomorphism $\Delta(A/R) \to \Delta(A \times R/R)$ such that

  $$\begin{array}{ccccccccc} 0 & \longrightarrow & R & \longrightarrow & \Delta(A/R) & \longrightarrow & \bigwedge^n A & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & R & \longrightarrow & \Delta(A \times R/R) & \longrightarrow & \bigwedge^{n+1}(A \times R) & \longrightarrow & 0 \end{array}$$

  commutes.

The correspondence sending an R-algebra A of rank n to $\Delta(A/R)$ gives a functor from the category of R-algebras of rank n with isomorphisms as morphisms to the category of R-algebras of rank 2 with isomorphisms. It is not known whether the functor $\Delta(-/R)$ is characterized by the above properties. If not, one could ask whether $\Delta(-/R)$ agrees with the construction by Pierre Deligne in [7], or with the one by Ottmar Loos in [20], or with both.

Bibliography

[1] Bhargava, M. Higher composition laws. III. The parametrization of quartic rings. *Ann. of Math. (2) 159*, 3 (2004), 1329–1360.

[2] Bhargava, M., and Satriano, M. On a notion of "Galois closure" for extensions of rings. `arxiv.org/abs/1006.2562`, 2010. Journal of the European Mathematical Society, to appear.

[3] Bosma, W., Cannon, J., and Playoust, C. The Magma algebra system. I. The user language. *J. Symbolic Comput. 24*, 3-4 (1997), 235–265. Computational algebra and number theory (London, 1993).

[4] Bourbaki, N. *Éléments de mathématique. XI. Première partie: Les structures fondamentales de l'analyse. Livre II: Algèbre. Chapitre IV: Polynomes et fractions rationnelles. Chapitre V: Corps commutatifs.* Actualités Sci. Ind., no. 1102. Hermann et Cie., Paris, 1950.

[5] Bourbaki, N. *Éléments de mathématique. Algèbre. Chapitres 1 à 3.* Hermann, Paris, 1970.

[6] de Smit, B. On the characteristic polynomial of the sum of two endomorphisms. Available at `http://www.math.leidenuniv.nl/~desmit/notes/charpols.pdf`, 2007.

[7] Deligne, P. Letter to M. Rost and M. Bhargava. `http://www.math.leidenuniv.nl/~jbrakenh/lowrank/deligne-rostbhargava.pdf`.

[8] Eisenbud, D. *Commutative algebra*, vol. 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[9] Ferrand, D. Un foncteur norme. *Bull. Soc. Math. France 126*, 1 (1998), 1–49.

[10] Grothendieck, A. Éléments de géométrie algébrique. I. Le langage des schémas. *Inst. Hautes Études Sci. Publ. Math.*, 4 (1960), 228.

[11] Grothendieck, A. Éléments de géométrie algébrique. II. Étude globale élémentaire de quelques classes de morphismes. *Inst. Hautes Études Sci. Publ. Math.*, 8 (1961), 222.

[12] Grothendieck, A. Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV. *Inst. Hautes Études Sci. Publ. Math.*, 32 (1967), 361.

[13] Grothendieck, A. *Revêtements étales et groupe fondamental (SGA 1)*. Documents Mathématiques (Paris), 3. Société Mathématique de France, Paris, 2003.

[14] Hartshorne, R. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[15] Katz, N. M., and Mazur, B. *Arithmetic moduli of elliptic curves*, vol. 108 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1985.

[16] Laksov, D. Splitting algebras, factorization algebras, and residues. `www.math.kth.se/~laksov/art/splittingmonthly.pdf`, 2009.

[17] Lang, S. *Algebra*, third ed., vol. 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[18] Lenstra, H. W. Galois theory for schemes. Available at `websites.math.leidenuniv.nl/algebra/GSchemes.pdf`, 2008.

[19] Liu, Q. Quotient maps and base change. `http://www.math.u-bordeaux1.fr/~qliu/Notes/quotient-homeo.ps`, 2002.

[20] Loos, O. Discriminant algebras of finite rank algebras and quadratic trace modules. *Math. Z. 257*, 3 (2007), 467–523.

[21] Mumford, D., Fogarty, J., and Kirwan, F. *Geometric invariant theory*, third ed., vol. 34 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (2)*. Springer-Verlag, Berlin, 1994.

[22] Nagata, M. On the imbedding problem of abstract varieties in projective varieties. *Mem. Coll. Sci. Univ. Kyoto. Ser. A. Math. 30* (1956), 71–82.

[23] Poonen, B. Isomorphism types of commutative algebras of finite rank over an algebraically closed field. In *Computational arithmetic geometry*, vol. 463 of *Contemp. Math.* Amer. Math. Soc., Providence, RI, 2008, pp. 111–120.

[24] Roby, N. Lois polynomes et lois formelles en théorie des modules. *Ann. Sci. École Norm. Sup. (3) 80* (1963), 213–348.

[25] Rydh, D. Existence and properties of geometric quotients. *J. Algebraic Geom. 22* (2013), 629–669.

[26] Serre, J.-P. *Algebraic groups and class fields*, vol. 117 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1988. Translated from the French.

[27] Stevenhagen, P. The arithmetic of number rings. In *Algorithmic number theory: lattices, number fields, curves and cryptography*, vol. 44 of *Math. Sci. Res. Inst. Publ.* Cambridge Univ. Press, Cambridge, 2008, pp. 209–266.

[28] The Stacks Project Authors. *Stacks Project*. Available at `http://math.columbia.edu/algebraic_geometry/stacks-git`.

[29] Thorup, A. On the invariants of the splitting algebra. Available at `http://arxiv.org/abs/1105.4478`, 2011.

Abstract

Let $K \to L$ be a separable field extension of degree n. Suppose the Galois group of a Galois closure M of L/K is the full symmetric group on n letters S_n. We have a tower of extensions $K \subseteq L = L_1 \subseteq \cdots \subseteq L_n = M$, where L_m for $m = 0, \ldots, n$ is the field of invariants of M under the action of $S_{n-m} \subseteq S_n$.

Let R be a commutative ring with identity. Let A be a commutative R-algebra, which is finite and locally free of rank n. Manjul Bhargava and Matthew Satriano constructed the R-algebra $A^{(n)}$. In the situation above, we have that $L^{(n)}$ is isomorphic to M. For this reason $A^{(n)}$ is called the Galois closure of A/R.

In this thesis we define R-algebras $A^{(m)}$, with $m = 0, \ldots, n$. We call $A^{(m)}$ the m-closure of A. In the situation above, we have that $L^{(m)}$ is isomorphic to L_m. We also prove several properties of these constructions. Here are some examples.

Let $t \geq 0$ be an integer. Let $A_1, \ldots, A_t$ be commutative R-algebras. For $i = 1, \ldots, t$ suppose A_i finite and locally free of rank n_i. Let A be the R-algebra $A_1 \times \cdots \times A_t$. Fix k in $\{0, \ldots, \mathrm{rank}(A)\}$. We prove a formula for $A^{(k)}$ in terms of various m-closures of the A_i.

The algebra $A^{(n)}$ comes with a natural action of S_n. In general $A^{(m)}$ is not isomorphic to the ring of invariants of $A^{(n)}$ under the action of S_{n-m}, as it is true for a separable field extension. However, we show that for $m = 0, \ldots, n$ there is a natural map $A^{(m)} \to (A^{(n)})^{S_{n-m}}$, which is a universal homeomorphism.

We also study the action of the alternating group A_n on $A^{(n)}$. For a field extension $K \to L$ as before, if the characteristic of K is not 2, then M^{A_n} is K adjoined with a square root of the discriminant. The discriminant algebra $\Delta(A/R)$ of A generalizes M^{A_n}. We prove that if 2 is invertible in R, then there is a natural map $\Delta(A/R) \to (A^{(n)})^{A_n}$, which is a universal homeomorphism.

Samenvatting

Zij L/K een separabele lichaamsuitbreiding van graad n. Stel dat de Galoisgroep van een Galoisafsluiting M van L/K de groep S_n is. Er is een toren van lichaamsuitbreidingen $K = L_0 \subseteq L = L_1 \subseteq \cdots \subseteq L_n = M$, waar L_m voor $m = 0, \ldots, n$ is de lichaam van invarianten onder de werking van $S_{n-m} \subseteq S_n$.

Zij R een commutatieve ring met 1. Zij A een commutatieve R-algebra, die eindig en lokaal vrij van rang n is. Manjul Bhargava en Matthew Satriano hebben de R-algebra $A^{(n)}$ gedefinieerd. In het bovenstaande geval is $L^{(n)}$ isomorf met M. Dit is de reden dat $A^{(n)}$ de Galoisafsluiting van A/R wordt genoemd.

Voor $m = 0, \ldots, n$ definiëren we een R-algebra $A^{(m)}$, de m-afsluiting van A. In de bovenstaande situatie is $L^{(m)}$ isomorf met L_m. We bewijzen verschillende eigenschappen van deze constructies. Hier zijn een aantal voorbeelden.

Zij $t \geq 0$ een geheel getal. Zij $A_1, \ldots, A_t$ commutatieve R-algebra's. Voor $i = 1, \ldots, t$ neem aan dat A_i eindig is en lokaal vrij van rang n_i. Zij A de R-algebra $A_1 \times \cdots \times A_t$. Neem k in $\{0, \ldots, \mathrm{rang}(A)\}$ vast. We bewijzen een formule voor $A^{(k)}$ in termen van verschillende m-afsluitingen van de A_i.

De algebra $A^{(n)}$ heeft een natuurlijke werking van S_n. In het algemeen is $A^{(m)}$ niet isomorf met de ring van invarianten $(A^{(n)})^{S_{n-m}}$, wat wel het geval is voor een separabele lichaamsuitbreiding. Echter, voor $m = 0, \ldots, n$ is er een natuurlijke afbeelding $A^{(m)} \to (A^{(n)})^{S_{n-m}}$, die een universeel homeomorfisme is.

We bestuderen ook de werking van de alternerende groep A_n op $A^{(n)}$. Voor een lichaamsuitbreiding L/K als voorheen, als de karakteristiek van K niet 2 is, is M^{A_n} gelijk aan K met een wortel van de discriminant toegevoegd. De discriminantalgebra $\Delta(A/R)$ van A generaliseert M^{A_n}. We bewijzen dat, als 2 inverteerbaar is in R, er een natuurlijke universeel homeomorfisme $\Delta(A/R) \to (A^{(n)})^{A_n}$ is.

Résumé

Soit $K \to L$ une extension de corps séparable de degré n. On suppose que le groupe de Galois d'une clôture galoisienne M de L/K est le groupe symétrique S_n. On a une tour d'extensions $K = L_0 \subseteq L = L_1 \subseteq \cdots \subseteq L_n = M$, où L_m pour $m = 0, \ldots, n$ est le corps des invariants de M sous l'action de $S_{n-m} \subseteq S_n$.

Soit R un anneau commutatif unitaire. Soit A une R-algèbre commutative, qui est finie et localement libre de rang n. Manjul Bhargava et Matthew Satriano ont défini une R-algèbre $A^{(n)}$. Dans le cas précedent $L^{(n)}$ est isomorphe à M. Pour cette raison, on appelle $A^{(n)}$ la clôture galoisienne de A/R.

Dans cette thèse on définit des R-algèbres $A^{(m)}$, où $m = 0, \ldots, n$. On appelle $A^{(m)}$ la m-clôture de A. Dans le cas précedent, le corps $L^{(m)}$ est isomorphe à L_m. On va démontrer plusieurs proprietés de ces constructions. On donne quelques exemples.

Soit $t \geq 0$ un nombre entier. Soient $A_1, \ldots, A_t$ des R-algèbres commutatives. Soit $i \in \{1, \ldots, t\}$, on suppose que A_i est finie et localement libre de rang n_i. Soit A la R-algèbre $A_1 \times \cdots \times A_t$. Soit $k \in \{0, \ldots, \mathrm{rang}(A)\}$. On donne une formule pour $A^{(k)}$ en fonction de plusieurs m-clôtures des A_i.

L'algèbre $A^{(n)}$ est munie d'une action naturelle de S_n. Généralement, $A^{(m)}$ n'est pas isomorphe à l'anneau des invariants de $A^{(n)}$ sous l'action de S_{n-m}, comme est le cas pour une extension de corps séparable. Pourtant, on montre qu'on a un morphisme naturel $A^{(m)} \to (A^{(n)})^{S_{n-m}}$, qui est un homéomorphisme universel.

On étudie aussi l'action du groupe alterné A_n sur $A^{(n)}$. Dans le cas d'une extension de corps $K \to L$ comme d'abord, si la caractéristique de K n'est pas 2, alors M^{A_n} est K avec une racine carrée du discriminant. L'algèbre discriminant $\Delta(A/R)$ de A est une généralisation de M^{A_n}. On montre que si 2 est inversible dans R, il existe un morphisme naturel $\Delta(A/R) \to (A^{(n)})^{A_n}$, qui est un homéomorphisme universel.

Acknowledgements

Thanks to Hendrik and Lenny for trying to teach me good taste in mathematics.

Thanks to Boas for always coming up with interesting ideas to work on.

Thanks to the promotiecommissie for the time spent reading my thesis and their useful comments.

Thanks to the ALGANT consortium for funding, but also for all the people who helped me throughout these years. Especially to Virginie and Christopher.

Thanks to Michiel, René, Samuel, and Samuele for the many mathematical discussions.

Thanks to the number theory, algebra, and geometry group in Leiden and the number theory group in Bordeaux for their help and their suggestions. Especially to Bas Edixhoven, Qing Liu, Bart de Smit, Peter Stevenhagen, Dajano Tossici.

Thanks to Owen, for the week of hard work in Leiden, which produced such nice results.

Thanks to my friends in Leiden for the wonderful time we had there. Especially to my paranymphs Samuele and Michiel, and to Carlo e Catherine, Daniele e Mirta, Alessio e Pamela, Michele, Andrea e Elena, Liu and Bo, Alfonso, Weidong... and all the others.

Thanks to my friends in Enschede. Because of you Enschede is my second favorite city in the Netherlands.

The greatest thanks to my family and friends in Italy, for being always close. Especially to mamma e papà, Elena e Marco e Martina, Emanuela, zio Marco e zia Angela e zia Gisa, Fabrizio e Stefania, Marco, Luigi Amedeo, Francesco e Emanuela, Luigi, Chiara e Jacopo, Michele, Tommaso, Cecilia e Roberto, Luigi e Bea, Daniele, Matteo.

Curriculum Vitae

Alberto Gioia was born on 26th May 1985 in Codogno, Italy. He grew up in Parma, where he got his diploma at the "Liceo classico G. D. Romagnosi" in 2004.

He then started his bachelor in mathematics at the university of Parma. In 2007 he finished his bachelor, and he started the ALGANT-master Erasmus program, spending the first year in Padova and the second in Leiden. He wrote his master thesis, with title "Normal forms in combinatorial algebra", under the supervision of Hendrik Lenstra in Leiden. He received his master degree at the ALGANT graduation ceremony in Leiden in 2009.

In 2010 he was awarded an ALGANT-Doc joint PhD program fellowship to continue his studies in mathematics at the universities of Leiden and Bordeaux, under the supervision of Hendrik Lenstra and Lenny Taelman in Leiden, and Boas Erez in Bordeaux.