ALBANIAN JOURNAL OF MATHEMATICS
Volume 13, Number 1, Pages 000–000
ISSN: 1930-1235;

PRIMITIVE RECURSIVE DECIDABILITY FOR LARGE RINGS OF ALGEBRAIC INTEGERS

AHARON RAZON

Elta Systems Ltd,
100 Yitzchak Hanasi Blvd,.
Ashdod, 7710202, Israel.

Abstract. Lou v. d. Dries proves in [Dri88] that the elementary theory $\mathrm{Th}(\tilde{\mathbb{Z}})$ of the ring $\tilde{\mathbb{Z}}$ of all algebraic integers is decidable. For a prime number p, let $\widetilde{\mathbb{F}_p(t)}$ be the algebraic closure of $\mathbb{F}_p(t)$ and denote the integral closure of $\mathbb{F}_p[t]$ in $\widetilde{\mathbb{F}_p(t)}$ by $\widetilde{\mathbb{F}_p[t]}$. Lou v. d. Dries and Angus Macintyre prove in [DrM90] that $\mathrm{Th}(\widetilde{\mathbb{F}_p[t]})$ is decidable. One of the main results of this work states that both $\mathrm{Th}(\tilde{\mathbb{Z}})$ and $\mathrm{Th}(\widetilde{\mathbb{F}_p[t]})$ are primitive recursive.

Moreover, let $\tilde{\mathbb{Q}}$ be the field of all algebraic numbers and let $\mathrm{Gal}(\mathbb{Q}) = \mathrm{Gal}(\tilde{\mathbb{Q}}/\mathbb{Q})$ be the absolute Galois group of $\mathbb{Q}$. For each positive integer e we equip the group $\mathrm{Gal}(\mathbb{Q})^e$ with its unique normalized Haar measure. For each $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e) \in \mathrm{Gal}(\mathbb{Q})^e$ let $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ be the fixed field of $\sigma_1, \ldots, \sigma_e$ in $\tilde{\mathbb{Q}}$ and let $\tilde{\mathbb{Z}}(\boldsymbol{\sigma})$ be the ring of integers of $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$. Given a sentence θ in the language of rings, we let α be the Haar measure of the set of all $\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{Q})^e$ for which θ holds in $\tilde{\mathbb{Z}}(\boldsymbol{\sigma})$. We prove that α is a rational number which can be effectively computed in a primitive recursive way. We prove a similar result also in the function field case.

MSC 2010: Primary: 12E30;
Keywords: Primitive recursive decidability, PAC field over a subring, Galois stratification

Introduction

Let $\mathcal{O}$ be a Dedekind domain with a trivial Jacobson radical and with a global field of quotients K. Denote the absolute Galois group of K by $\mathrm{Gal}(K)$. For each non-negative integer e and each e-tuple $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e) \in \mathrm{Gal}(K)^e$ let $\tilde{K}(\boldsymbol{\sigma})$ be the fixed field of $\sigma_1, \ldots, \sigma_e$ in $\tilde{K}$ and let $\widetilde{\mathcal{O}}(\boldsymbol{\sigma})$ be the integral closure of $\mathcal{O}$ in $\tilde{K}(\boldsymbol{\sigma})$. In particular, for $e = 0$, $\widetilde{\mathcal{O}}$ is the integral closure of $\mathcal{O}$ in $\tilde{K}$. Denote the language of rings extended with constant symbol for each element of $\mathcal{O}$ by $\mathcal{L}(\mathrm{ring}, \mathcal{O})$. In each ring that contains a homomorphic image of $\mathcal{O}$ we interpret these constant

E-mail address: razona@elta.co.il.
This work originates from the PhD thesis of the author from Tel Aviv University and carried out under the supervision of Prof. Moshe Jarden.

symbols as the residues of the appropriate elements of $\mathcal{O}$. Consider a sentence θ in $\mathcal{L}(\text{ring}, \mathcal{O})$ and let α be the Haar measure of all $\boldsymbol{\sigma} \in \text{Gal}(K)^e$ such that θ holds in $\tilde{\mathcal{O}}(\boldsymbol{\sigma})$. If $e = 0$, and θ is true in $\tilde{\mathcal{O}}$, then $\alpha = 1$, otherwise $\alpha = 0$. The purpose of this work is to prove that for each e, α is a rational number which can be effectively computed (i.e., in a primitive recursive way) if $\mathcal{O}$ is an effective computability domain (Definition 1.4). The latter condition holds in particular for $\mathcal{O} = \mathcal{O}_0$, where $\mathcal{O}_0 = \mathbb{Z}$ or $\mathcal{O}_0 = \mathbb{F}_p[t]$ and also for $\mathcal{O} = S_0^{-1}\mathcal{O}_0$, where S_0 is a presented multiplicative subset of $\mathcal{O}_0$ and either $S_0 = \mathcal{O}_0 \setminus \{0\}$ (in which case $\mathcal{O} = K$) or S_0 is relatively prime to infinitely many irreducible elements of $\mathcal{O}_0$.

In [Dri88], v.d. Dries extends $\mathcal{L}(\text{ring}, \mathcal{O})$ with "radical relations" to a language $\mathcal{L}_{\text{rad}}(\mathcal{O})$ (§2.1) and establishes a recursive elimination of quantifiers procedure for $\tilde{\mathbb{Z}}$ in this language. In particular, he proves that $\tilde{\mathbb{Z}}$ is decidable. This is the case where $e = 0$ and $\mathcal{O} = \mathbb{Z}$. The case where $e \geq 1$ and $\mathcal{O} = K$ is [FrJ08, p. 726, Thm. 30.7.2]. We combine the methods of proof of both cases to get the general result.

After a section of preparations, the work is divided into two sections. The first three subsections in Section 2 are an elaboration of the first two sections of [Dri88]. The key to the elimination procedure of v.d. Dries is Rumely's density theorem [Rum86]. In order to apply the later tool, one has to decompose algebraic sets defined over an integral domain R which contain K into absolutely irreducible varieties, and to do it uniformly with respect to all homomorphisms of R into $\tilde{K}$. v.d. Dries applies here a compactness argument from model theory. We replace the compactness argument by an application of the Bertini-Noether theorem. Then we establish a primitive recursive procedure for an elimination of existential quantifiers (in the language $\mathcal{L}_{\text{rad}}(\mathcal{O})$) on Zariski open subsets of K-varieties. The elimination works over each ring of integers O_M of a perfect algebraic extension M of K which is PAC over O_M [JaR94]. In particular it works over almost all rings $\tilde{\mathcal{O}}(\boldsymbol{\sigma})$.

The Galois Stratification of [FrJ08, §30] assumes in addition that M is e-free, i.e., that $\text{Gal}(M) \cong \hat{F}_e$. In particular, M is a Frobenius field. Subsection 3.1 extends this notion to a Frobenius field over O_M, which means that M is PAC over O_M and $\text{Gal}(M)$ has the embedding property. In addition we generalize [FrJ08, p. 564, Prop. 24.1.4] by using Rumely's local-global principle for absolutely irreducible varieties over M [JaR98, Thm. 1.5]. Subsections 2–5 in Section 3 extend the Galois Stratification to Radical Galois Stratification. The latter allows us to eliminate quantifiers from formulas of the language $\mathcal{L}_{\text{rad}}(\mathcal{O})$. The elimination procedure requires more general formulas which we call radical Galois formulas. They include data for a stratification of the affine space $\mathbb{A}^n$ into K-normal basic sets A: each coordinate ring $K[A]$ is equipped with a Galois ring cover C such that for each subextension L of $K(C)/K(A)$, $(C \cap L)/K[A]$ is a ring cover. Moreover, to each L with $\text{rank}(\text{Gal}(K(C)/L)) \leq e$ we associate a "ring of integers" $\mathcal{O}[C \cap L]$ and a quantifier free sentence θ_L in $\mathcal{L}_{\text{rad}}(\mathcal{O}[C \cap L])$. In each consequent elimination of a quantifier we code the data of the eliminated quantifier in a new set of ring covers and sentences, till there are no more quantifiers. Finally, Subsection 3.6 concludes the proof on the primitive recursive decidability for large rings of algebraic integers.

Among others we have to factor an ideal in the ring of integers of a global field into prime ideals. We describe a procedure for this factorization in Appendix A.

Another auxiliary tool that the procedure applies is a local elimination procedure. More precisely, it uses elimination of quantifiers for the theory of valuation domains which are not fields but with algebraically closed quotient field in the language of

rings augmented by a binary relation symbol which stands for divisibility. Appendix B is an elaboration of Weispfening's primitive recursive procedure [Wei84] for this theory.

In a forthcoming paper we use Corollary 3.29 of this work to prove the following result: Let $\mathbb{Q}_{\text{symm}}$ (resp. $\mathbb{F}_p(t)_{\text{symm,ins}}$) be the compositum of all symmetric extensions of $\mathbb{Q}$ (resp. the purely inseparable extension of the compositum of all symmetric extensions of $\mathbb{F}_p(t)$). Then, the theory of the ring of integers of $\mathbb{Q}_{\text{symm}}$ and the theory of the ring of integers of $\mathbb{F}_p(t)_{\text{symm,ins}}$ are primitive recursively decidable.

Acknowledgements: I wish to thank Professor Moshe Jarden for his stimulating guidance and for the values he has taught me, both by setting high and challenging demands and by exposing me to his image of a mathematician. I also thank Joachim Schmid for useful remarks and Dan Haran for helpful discussions.

1. Preparations

1.1. **Notations and the Explicit Case.** The Jacobson radical of a commutative ring with a unit is the intersection of all maximal ideals of the ring. In particular, the Jacobson radical of a field is zero.

We shall use the following notations throughout this work.

Notation 1.1.

a) $\mathcal{O}$ is a Dedekind domain with Jacobson radical $\mathbf{0}$ and with global quotient field K.

b) P_K is the set of all non-zero prime ideals of $\mathcal{O}$.
Since $\mathcal{O}$ is a Dedekind domain, each $\mathfrak{p} \in P_K$ is maximal, and since K is global, the residue field $\bar{K}_{\mathfrak{p}} = \mathcal{O}/\mathfrak{p}$ is finite. To each $\mathfrak{p} \in P_K$ corresponds a valuation $v_{\mathfrak{p}}$ of K.

c) For each algebraic extension L of K, let $\mathcal{O}_L$ be the integral closure of $\mathcal{O}$ in L and let P_L be the set of all maximal ideals of $\mathcal{O}_L$ (which is in fact the set of all non-zero prime ideals of $\mathcal{O}_L$). In particular $\mathcal{O}_K = \mathcal{O}$. Note that the Jacobson radical of $\mathcal{O}_L$ is zero. To each $\mathfrak{p} \in P_L$ corresponds a valuation $v_{\mathfrak{p}}$ of L which extends $v_{\mathfrak{p}\cap K}$; for a positive integer n and $\mathbf{a} = (a_1, \ldots, a_n) \in L^n$ we denote $v_{\mathfrak{p}}(\mathbf{a}) = \min\limits_{1\le i\le n} v_{\mathfrak{p}}(a_i)$. If L is a normal extension of K and $\sigma \in \mathrm{Aut}(L/K)$, then σ acts naturally on P_L by $v_{\mathfrak{p}^\sigma}(a^\sigma) = v_{\mathfrak{p}}(a)$ for each $\mathfrak{p} \in P_L$ and $a \in L$. We denote the localization of $\mathcal{O}_L$ at $\mathfrak{p}$ by $\mathcal{O}_{L,\mathfrak{p}}$. That is $\mathcal{O}_{L,\mathfrak{p}} = \{x \in L |\ v_{\mathfrak{p}}(x) \ge 0\}$. Then $\mathcal{O}_{L,\mathfrak{p}}$ is a valuation ring. If $[L : K] < \infty$, then $\mathcal{O}_L$ is a Dedekind domain. In the general case, $\mathcal{O}_L = \bigcap\limits_{\mathfrak{p}\in P_L} \mathcal{O}_{L,\mathfrak{p}}$.

d) $\tilde{K}$ is the algebraic closure of K.
$\widetilde{\mathcal{O}} = \mathcal{O}_{\tilde{K}}$, $\tilde{P} = P_{\tilde{K}}$, and $\widetilde{\mathcal{O}}_{\mathfrak{P}} = \mathcal{O}_{\tilde{K},\mathfrak{P}}$ for $\mathfrak{P} \in \tilde{P}$.

e) In order that the results of this work will be accomplished also for the case $\mathcal{O} = K$ we define in this case, for each algebraic extension L of K, $\mathcal{O}_L = L$, $P_L = \{\mathbf{0}\}$ and, for $\mathfrak{p} \in P_L$, $v_{\mathfrak{p}}(x) = 0$ for each $x \in L^\times$ and $\mathcal{O}_{L,\mathfrak{p}} = L$. In particular $\widetilde{\mathcal{O}} = \tilde{K}$ and $\widetilde{\mathcal{O}}_{\mathfrak{P}} = \tilde{K}$ for $\mathfrak{P} \in \tilde{P}$.

Definition 1.2. We are talking on the **explicit case** if $\mathcal{O}$ is presented in K [FrJ08, p. 404, the paragraph after Def. 19.1.1]. Since K is global, it has elimination theory [FrJ08, p. 410, Def. 19.2.8].

In the explicit case we have in particular that $\tilde{K}$ is a presented field with elimination theory [FrJ08, p. 413, Lemma 19.4.1]. Also, $\widetilde{\mathcal{O}}$ is presented in $\tilde{K}$ since for each $x \in \tilde{K}$ we can compute $f(X) = \mathrm{irr}(x, K)$ and check if all its coefficients belong to $\mathcal{O}$; if so then $x \in \widetilde{\mathcal{O}}$, otherwise $x \notin \widetilde{\mathcal{O}}$.

1.2. **Effective Computability Domain.**

Definition 1.3. A commutative domain R is called **Euclidean ring** if there exists a function

$$\delta : R \setminus \{0\} \to \mathbb{N}$$

which satisfies that for each $a, b \in R \setminus \{0\}$, $\delta(ab) = \delta(a)\delta(b)$ and there exist $c, r \in R$ such that $a = bc + r$ and $\delta(r) < \delta(b)$ or $r = 0$. We also define $\delta(0) = 0$.

If in addition R satisfies that for each $n \in \mathbb{N}$, the set $\{a \in R |\ \delta(a) \leq n\}$ is finite, then R is called **Euclidean ring of finite type**.

For example, $\mathbb{Z}$ with $\delta(a) = |a|$ and $\mathbb{F}_p[t]$ with $\delta(g(t)) = c^{\deg(g)}$, where $2 \leq c \in \mathbb{N}$ is any constant, are Euclidean rings of finite type.

An Euclidean ring is in particular a principal ideal domain and hence is a unique factorization domain.

An Euclidean ring of finite type R is called **presented** if the following four properties are satisfied:

(1) R is a presented ring [FrJ08, p. 404, Definition 19.1.1].
(2) For each $n \in \mathbb{N}$, the finite set $\{a \in R \,|\, \delta(a) \leq n\}$ is given explicitly.
Note that $\{a \in R \,|\, \delta(a) = 1\}$ is the set of invertible elements of R. Indeed, let $a \in R$. It follows from the equality $\delta(1) = \delta(1 \cdot 1) = \delta(1) \cdot \delta(1)$ that $\delta(1) = 1$; hence, if $ab = 1$, then $\delta(a)\delta(b) = \delta(ab) = 1$ and therefore $\delta(a) = 1$. On the other hand, there exist $c, r \in R$ such that $1 = ac + r$ and $\delta(r) < \delta(a)$. Hence, if $\delta(a) = 1$, then $r = 0$ and $ac = 1$.
(3) The set of the irreducible elements of R is a primitive recursive subset of R which is given explicitly. Also, each element of R can be written effectively as a product of irreducible elements of R (up to an invertible element of R).
(4) The function δ is presented and we can effectively perform division with a remainder as above.

In particular we can effectively find, using Euclid's algorithm, a greatest common divisor of two elements in R.

Definition 1.4. We say that the ring $\mathcal{O}$ is an **effective computability domain** (i.e., we can effectively perform in it calculations), if $\mathcal{O}$ is presented in K and $\mathcal{O} = S_0^{-1}\mathcal{O}_0$, where $\mathcal{O}_0$ is an Euclidean domain of finite type and S_0 is a presented multiplicative subset of $\mathcal{O}_0$ (S_0 is presented by a set of generators which contains irreducible elements of $\mathcal{O}_0$ given explicitly). Note that for $S_0 = \mathcal{O}_0 \setminus \{0\}$ we get $\mathcal{O} = K$. Also, the Jacobson radical of $\mathcal{O}$ is zero if and only if $\mathcal{O} = K$ or S_0 is disjoint from an infinite subset of the irreducible elements of $\mathcal{O}_0$.

1.3. **Pseudo Algebraic Closed Fields over Rings of Integers.** Recall that a field M is **pseudo algebraically closed** (**PAC**) if every absolutely irreducible variety V defined over M has an M-rational point. If R is a subring of M, then M may have a stronger property [JaR94]:

Definition 1.5. Let R be a subset of a field M. We say that M is **PAC** over R if for every absolutely irreducible variety V of dimension $r \geq 0$ and for each

dominating separable rational map $\varphi\colon V \to \mathbb{A}^r$ over M there exists $\mathbf{a} \in V(M)$ such that $\varphi(\mathbf{a}) \in R^r$.

Note that if S is a subring of M which contains R, then M is also PAC over S.

As in the case of PAC fields, it suffices to check the condition of Definition 1.5 only for plane curves [JaR94, Lemma 1.3]:
Let R be a subring of a field M. A necessary and sufficient condition for M to be PAC over R is:
For each absolutely irreducible polynomial $f \in M[T,X]$ such that $\frac{\partial f}{\partial X} \neq 0$ and for each $0 \neq g \in M[T]$ there exists $(a,b) \in R \times M$ such that $f(a,b) = 0$ and $g(a) \neq 0$.

We denote the separable closure of K by K_{sep} and the absolute Galois group, $\mathrm{Gal}(K_{\mathrm{sep}}/K)$, of K by $\mathrm{Gal}(K)$. Recall that if $\sigma_1, \ldots, \sigma_e \in \mathrm{Gal}(K)$, then $K_{\mathrm{sep}}(\boldsymbol{\sigma})$ is the fixed field in K_{sep} of $\sigma_1, \ldots, \sigma_e$. We denote its maximal purely inseparable extension by $\tilde{K}(\boldsymbol{\sigma})$. The following result follows from [JaR94, Prop. 3.1]:

Proposition 1.6. *Let e be a positive integer. Then, for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, the fields $K_{\mathrm{sep}}(\boldsymbol{\sigma})$ and $\tilde{K}(\boldsymbol{\sigma})$ are PAC over $\mathcal{O}$.*

We denote the integral closure, $\mathcal{O}_{\tilde{K}(\boldsymbol{\sigma})}$, of $\mathcal{O}$ in $\tilde{K}(\boldsymbol{\sigma})$ by $\widetilde{\mathcal{O}}(\boldsymbol{\sigma})$. Then, it follows from Proposition 1.6, in particular, that

Proposition 1.7. *Let e be a positive integer. Then, for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, the field $\tilde{K}(\boldsymbol{\sigma})$ is PAC over $\widetilde{\mathcal{O}}(\boldsymbol{\sigma})$.*

This property of the field $\tilde{K}(\boldsymbol{\sigma})$ that it is PAC over $\widetilde{\mathcal{O}}(\boldsymbol{\sigma})$ is responsible for the next three results which we shall use in this work. The first result is a consequence from the weak approximation theorem for absolutely irreducible varieties over $\tilde{K}(\boldsymbol{\sigma})$, the second result is a consequence from Rumely's local global principle for absolutely irreducible varieties over $\tilde{K}(\boldsymbol{\sigma})$, and the third result is that $\widetilde{\mathcal{O}}(\boldsymbol{\sigma})$ is a Bezout domain. We shall prove these properties in general for a perfect algebraic extension M of K which is PAC over $\mathcal{O}_M$. In particular this includes $M = \tilde{K}$ since $\tilde{K}$ is perfect and PAC over $\widetilde{\mathcal{O}}$.

Lemma 1.8. *Assume that $\mathcal{O} \neq K$ and let M be a perfect algebraic extension of K which is PAC over $\mathcal{O}_M$. Let $c_1, \ldots, c_q$ be nonunits in $\mathcal{O}_M$. Then there are distinct $\mathfrak{n}_1, \ldots, \mathfrak{n}_q \in P_M$ such that $c_i \in \mathfrak{n}_i$ for all i.*

Proof. Let L be a finite subextension of M/K which contains $c_1, \ldots, c_q$. Since $c_1, \ldots, c_q$ are nonunits in $\mathcal{O}_L$, there exist $\mathfrak{m}_1, \ldots, \mathfrak{m}_q \in P_L$ such that $c_i \in \mathfrak{m}_i$, $i = 1, \ldots, q$.

Let $\mathcal{S} = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_q\}$. For each $\mathfrak{m} \in \mathcal{S}$, let $L_{t\mathfrak{m}}$ be the maximal Galois extension of L in which $\mathfrak{m}$ totally splits. If $L_{\mathfrak{m}}$ is a Henselian closure of L with respect to $v_{\mathfrak{m}}$, then $L_{t\mathfrak{m}} = \bigcap_{\sigma \in \mathrm{Gal}(L)} L_{\mathfrak{m}}^{\sigma}$. Then $L_{\mathrm{tot},\mathcal{S}} := \bigcap_{\mathfrak{m} \in \mathcal{S}} L_{t\mathfrak{m}}$ is the maximal Galois extension of L in which each $\mathfrak{m} \in \mathcal{S}$ totally splits. By [JaR95, Lemma 1.4], $M_1 = M \cap L_{\mathrm{tot},\mathcal{S}}$ is **weakly P$\mathcal{S}$C over** $\mathcal{O}_{M_1}$: for each absolutely irreducible polynomial $h \in M_1[T,Y]$ which is monic in Y such that the roots of $h(0,Y)$ are distinct and in $L_{\mathrm{tot},\mathcal{S}}$, and for each $g \in M_1[T]$ such that $g(0) \neq 0$ there exists $(a,b) \in \mathcal{O}_{M_1} \times M_1$ such that $h(a,b) = 0$ and $g(a) \neq 0$.

Since $\mathcal{O}_L$ has a trivial Jacobson radical, it follows that P_L is infinite. In particular $P_L \setminus \mathcal{S} \neq \emptyset$. If $\mathfrak{m} \in P_L \setminus \mathcal{S}$ and v is an extension of $v_{\mathfrak{m}}$ to a valuation of M_1, then the Henselian closure of M_1 at v is L_{sep} [JaR95, Prop. 1.9(a)]. If L_1 is a finite

subextension of M_1/L, then L_1 is a global field and the Henselization of L_1 at $v|_{L_1}$ is not separably closed. Hence $M \cap L_{\mathrm{tot},\mathcal{S}}/L$ is an infinite extension. Therefore each $\mathfrak{m} \in \mathcal{S}$ factors in $\mathcal{O}_M$.

Conclude that there exist distinct $\mathfrak{n}_1, \dots, \mathfrak{n}_q \in P_M$ such that $\mathfrak{m}_i \subset \mathfrak{n}_i$ (hence $c_i \in \mathfrak{n}_i$), $i = 1, \dots, q$. □

Theorem 1.9. *Let M be a perfect algebraic extension of K which is PAC over $\mathcal{O}_M$. Let V be an absolutely irreducible closed variety in $\mathbb{A}^m$ which is defined over M, let $f \in \mathcal{O}_M[X_1, \dots, X_m]$ and define $V_f := \{\mathbf{x} \in V \,|\, f(\mathbf{x}) \neq 0\}$. Suppose that $V_f(\widetilde{\mathcal{O}}_{\mathfrak{P}}) \neq \emptyset$ for every $\mathfrak{P} \in \tilde{P}$. Let $k_1, \dots, k_q$ be polynomials in $\mathcal{O}_M[\mathbf{X}]$ with $q = 0$ if $\mathcal{O} = K$. Assume that for each j between 1 and q there exists $\mathfrak{P}_j \in \tilde{P}$ and $\mathbf{a}_{\mathfrak{P}_j} \in V_f(\widetilde{\mathcal{O}}_{\mathfrak{P}_j})$ such that $k_j(\mathbf{a}_{\mathfrak{P}_j})$ is a nonunit in $\widetilde{\mathcal{O}}_{\mathfrak{P}_j}$. Then there exists $\mathbf{a} \in V_f(\mathcal{O}_M)$ such that $k_j(\mathbf{a})$ is a nonunit in $\mathcal{O}_M$ for all j.*

Proof. If $q = 0$, the theorem follows from Rumely's local-global principle for absolutely irreducible affine varieties over M [JaR98, Thm. 1.5]. So assume that $q \geq 1$ (hence $\mathcal{O} \neq K$).

For each $\mathfrak{p} \in P_M$ we choose a Henselian closure $M_{\mathfrak{p}}$ of M at $v_{\mathfrak{p}}$ and extend $v_{\mathfrak{p}}$ to a valuation of $M_{\mathfrak{p}}$. We denote the ring of integers $\{x \in M_{\mathfrak{p}} \,|\, v_{\mathfrak{p}}(x) \geq 0\}$ of $M_{\mathfrak{p}}$ by $\mathcal{O}_{M_{\mathfrak{p}},\mathfrak{p}}$. Since M is PAC, it follows that $M_{\mathfrak{p}} = \tilde{K}$ [FrJ08, p. 205, Cor. 11.5.5]. Hence, for each $\mathfrak{p} \in P_M$, there exists $\mathfrak{P} \in \tilde{P}$ such that $v_{\mathfrak{p}} = v_{\mathfrak{P}}$ (and therefore $\mathcal{O}_{M_{\mathfrak{p}},\mathfrak{p}} = \widetilde{\mathcal{O}}_{\mathfrak{P}}$). Thus $V_f(\mathcal{O}_{M_{\mathfrak{p}},\mathfrak{p}}) \neq \emptyset$ for every $\mathfrak{p} \in P_M$. Also, for each j between 1 and q, we can replace $\mathfrak{P}_j$ and $\mathbf{a}_{\mathfrak{P}_j}$ by $\mathfrak{P}_j^\sigma$ and $\mathbf{a}_{\mathfrak{P}_j}^\sigma$, respectively, for some $\sigma \in \mathrm{Gal}(M)$, to assume that $v_{\mathfrak{P}_j} = v_{\mathfrak{p}_j}$, where $\mathfrak{p}_j = \mathfrak{P}_j \cap M$.

Let $j \in \{1, \dots, q\}$. Denote $\gamma_j = v_{\mathfrak{p}_j}(f(\mathbf{a}_{\mathfrak{P}_j}))$. Then $0 \leq \gamma_j < \infty$. Let $W_j = \{\big(\mathbf{x}, f(\mathbf{x}), k_j(\mathbf{x})\big) \,|\, \mathbf{x} \in V\}$. Then W_j is an absolutely irreducible closed variety in $\mathbb{A}^{m+2}$ which is defined over M such that $W_j(\mathcal{O}_{M_{\mathfrak{p}},\mathfrak{p}}) \neq \emptyset$ for every $\mathfrak{p} \in P_M$. It follows from the weak approximation theorem for affine absolutely irreducible varieties over M [JaR98, Thm. 1.8(a)] that there exists $\big(\mathbf{a}_j, f(\mathbf{a}_j), k_j(\mathbf{a}_j)\big) \in W_j(\mathcal{O}_M)$ such that

$$v_{\mathfrak{p}_j}\big(\big(\mathbf{a}_j, f(\mathbf{a}_j), k_j(\mathbf{a}_j)\big) - \big(\mathbf{a}_{\mathfrak{P}_j}, f(\mathbf{a}_{\mathfrak{P}_j}), k_j(\mathbf{a}_{\mathfrak{P}_j})\big)\big) > \gamma_j.$$

In particular, $v_{\mathfrak{p}_j}\big(f(\mathbf{a}_j)\big) = \gamma_j < \infty$ (hence $f(\mathbf{a}_j) \neq 0$). Therefore $\mathbf{a}_j \in V_f(\mathcal{O}_M)$. Moreover, since $k_j(\mathbf{a}_{\mathfrak{P}_j})$ is a nonunit in $\widetilde{\mathcal{O}}_{\mathfrak{P}_j}$, $v_{\mathfrak{p}_j}(k_j(\mathbf{a}_{\mathfrak{P}_j})) > 0$. Hence $v_{\mathfrak{p}_j}(k_j(\mathbf{a}_j)) > 0$ and, therefore, $k_j(\mathbf{a}_j)$ is a nonunit in $\mathcal{O}_M$.

By Lemma 1.8, there exist distinct $\mathfrak{n}_1, \dots, \mathfrak{n}_q \in P_M$ such that $k_j(\mathbf{a}_j) \in \mathfrak{n}_j$ for all j. Let

$$W = \{(\mathbf{x}, f(\mathbf{x}), k_1(\mathbf{x}), \dots, k_q(\mathbf{x})) \,|\, \mathbf{x} \in V\}.$$

Then W is an absolutely irreducible closed variety in $\mathbb{A}^{m+1+q}$ which is defined over M. Let $\gamma = v_{\mathfrak{n}_1}(f(\mathbf{a}_1))$. Then $0 \leq \gamma < \infty$. By the weak approximation theorem for affine absolutely irreducible varieties over M [JaR98, Thm. 1.8(a)], again, there exists $(\mathbf{a}, f(\mathbf{a}), k_1(\mathbf{a}), \dots, k_q(\mathbf{a})) \in W(\mathcal{O}_M)$ such that

$$v_{\mathfrak{n}_j}\big((\mathbf{a}, f(\mathbf{a}), k_1(\mathbf{a}), \dots, k_q(\mathbf{a})) - (\mathbf{a}_j, f(\mathbf{a}_j), k_1(\mathbf{a}_j), \dots, k_q(\mathbf{a}_j))\big) > \gamma,$$

$j = 1, \dots, q$. In particular $f(\mathbf{a}) \neq 0$; hence $\mathbf{a} \in V_f(\mathcal{O}_M)$. Also, for each j between 1 and q, $v_{\mathfrak{n}_j}(k_j(\mathbf{a})) > 0$ (since $v_{\mathfrak{n}_j}(k_j(\mathbf{a}_j)) > 0$); hence $k_j(\mathbf{a})$ is a nonunit in $\mathcal{O}_M$. □

Theorem 1.10. *Let M be a perfect algebraic extension of K which is PAC over $\mathcal{O}_M$, let $V \subseteq \mathbb{A}^n$ be an absolutely irreducible variety defined over M, and let $\mathbf{a} = (a_1, \dots, a_n) \in V(\tilde{K})$. Then there exists $\mathbf{b} = (b_1, \dots, b_n) \in V(M)$ such that, for*

each i between 1 and n, we get that, if $a_i \in M^\times$, then $\frac{b_i}{a_i}$ is an invertible element of $\mathcal{O}_M$, and if $a_i = 0$, then $b_i \in \mathcal{O}_M$.

Proof. We denote the set of all natural numbers between 1 and n such that $a_i \neq 0$ (resp., $a_i \in M^\times$) by I (resp., I_0). Let $0 \neq a \in \mathcal{O}$ be such that $aa_i \in \widetilde{\mathcal{O}}$ for each $i \in I \smallsetminus I_0$ and let $\mathbf{x} = (x_1, \ldots, x_n)$ be a generic point of V. Denote $I_1 = \{i+n \,|\, i \in I_0\}$ and let

$$y_i = \begin{cases} \frac{x_i}{a_i} & i \in I_0 \\ \frac{a_i}{x_i} & i \in I_1 \\ ax_i & i \in I \smallsetminus I_0 \\ x_i & i \in \{1,\ldots,n\} \smallsetminus I \end{cases} \quad \text{and} \quad c_i = \begin{cases} 1 & i \in I_0 \\ 1 & i \in I_1 \\ aa_i & i \in I \smallsetminus I_0 \\ 0 & i \in \{1,\ldots,n\} \smallsetminus I \end{cases}.$$

Let $W \subseteq \mathbb{A}^{n+|I_0|}$ be the M-variety generated by the point $\mathbf{y} = (y_1, \ldots, y_{n+|I_0|})$. Since $M(\mathbf{y}) = M(\mathbf{x})$, W is an absolutely irreducible variety over M, and since $\mathbf{c} \in W(\widetilde{\mathcal{O}})$, $W(\widetilde{\mathcal{O}}) \neq \emptyset$. Then, since $\mathcal{O}_M$ satisfies Rumely's local global principle, it follows that $W(\mathcal{O}_M) \neq \emptyset$ [JaR98, Cor. 1.7 (for $N = \tilde{K}$)]. Suppose that $\mathbf{d} \in W(\mathcal{O}_M)$. In particular, $d_i \cdot d_{i+n} = 1$ for each $i \in I_0$. Let

$$b_i = \begin{cases} a_i d_i & i \in I_0 \\ \frac{d_i}{a} & i \in I \smallsetminus I_0 \\ d_i & i \in \{1,\ldots,n\} \smallsetminus I \end{cases}.$$

Then $\mathbf{b} = (b_1, \ldots, b_n) \in V(M)$ and it satisfies that $\frac{b_i}{a_i} = d_i$ is an invertible element of $\mathcal{O}_M$ for each $i \in I_0$, and $b_i = d_i \in \mathcal{O}_M$ for each $i \in \{1,\ldots,n\} \smallsetminus I$. □

An integral domain R is called a **Bezout domain** if each finitely generated ideal of R is principal.

Lemma 1.11. *Let M be an algebraic extension of K which is PAC over $\mathcal{O}_M$. Let $0 \neq a \in \mathcal{O}_M$ and let $\alpha \in \widetilde{\mathcal{O}}$ and $n \in \mathbb{N}$ be such that $\alpha^n = a$. Then there exists $\beta \in \mathcal{O}_M$ such that $\frac{\beta}{\alpha}$ is an invertible element of $\widetilde{\mathcal{O}}$.*

Proof. Let $0 \neq b \in \mathcal{O}_M$ and consider $\beta \in \widetilde{\mathcal{O}}$ which satisfies $\beta^n + ab\beta - a = 0$. Then $(\frac{\beta}{\alpha})^n + b\alpha \cdot \frac{\beta}{\alpha} - 1 = 0$ and $1 + b\alpha \cdot (\frac{\alpha}{\beta})^{n-1} - (\frac{\alpha}{\beta})^n = 0$. Therefore $\frac{\alpha}{\beta}, \frac{\beta}{\alpha} \in \widetilde{\mathcal{O}}$ and hence $\frac{\beta}{\alpha}$ is invertible in $\widetilde{\mathcal{O}}$.

Consider now the absolutely irreducible polynomial $f(T, X) = X^n + aTX - a \in M[T, X]$ which satisfies $\frac{\partial f}{\partial X} \neq 0$. Since M is PAC over $\mathcal{O}_M$, it follows that there exists $(b, \beta) \in \mathcal{O}_M \times M$ such that $\beta^n + ab\beta - a = f(b, \beta) = 0$ and, by the above discussion, it follows that $\frac{\beta}{\alpha}$ is an invertible element of $\widetilde{\mathcal{O}}$. □

Theorem 1.12. *Let M be an algebraic extension of K which is PAC over $\mathcal{O}_M$, let K_1 be a finite subextension of M/K and let $\mathfrak{a}$ be an ideal of $\mathcal{O}_{K_1}$. Then there exist a finite subextension L of M/K_1 and $c \in \mathcal{O}_L$ such that $\mathfrak{a}\mathcal{O}_L = c\mathcal{O}_L$. Hence $\mathcal{O}_M$ is a Bezout domain.*

Proof. Since K_1 is a global field, $\mathcal{O}_{K_1}$ has a finite class number $h > 0$. Hence there exists $a \in \mathcal{O}_{K_1}$ such that $\mathfrak{a}^h = a\mathcal{O}_{K_1}$. Let $\alpha \in \widetilde{\mathcal{O}}$ be such that $\alpha^h = a$. Then, it follows from Lemma 1.11 that there exists $c \in \mathcal{O}_M$ such that $\varepsilon = \frac{c}{\alpha}$ is invertible in $\widetilde{\mathcal{O}}$. Therefore $\varepsilon^h = \frac{c^h}{a}$ is an invertible element of $\mathcal{O}_M$. Let $L = K_1(c)$. Then

$$(\mathfrak{a}\mathcal{O}_L)^h = \mathfrak{a}^h\mathcal{O}_L = a\mathcal{O}_L = (\tfrac{c}{\varepsilon})^h\mathcal{O}_L = (c\mathcal{O}_L)^h.$$

Thus, since $\mathcal{O}_L$ is a Dedekind domain, $\mathfrak{a}\mathcal{O}_L = c\mathcal{O}_L$. □

1.4. **Rings Covers and Decomposition Groups.** Recall the definitions of a discriminant and a ring cover [FrJ08, Section 6.1]:
Let R be an integrally closed integral domain with a quotient field E.

Definition 1.13. Let f be a monic polynomial in $R[X]$ and suppose that $\prod_{i=1}^{n}(X-x_i)$ is the decomposition of f into linear factors. The **discriminant** of f is, up to a sign,

$$\mathrm{Disc}(f) = \prod_{i\neq j}(x_i - x_j) = \prod_{j=1}^{n} f'(x_j)\,.$$

Then, $\mathrm{Disc}(f) \in R$ and $\mathrm{Disc}(f) \neq 0$ if and only if the x_i's are distinct.

Suppose that f is irreducible. In this case

$$\mathrm{Disc}(f) = N_{E(x_1)/E}(f'(x_1))\,.$$

We call $N_{E(x_1)/E}(f'(x_1))$ the **discriminant of** x_1 **over** E.

Remark 1.14. Let E' be a subextension of $E(x_1)/E$ and let R' be the integral closure of R in E'. Since each root of the polynomial $\mathrm{irr}(x_1, E')$ is also a root of the polynomial $\mathrm{irr}(x_1, E)$, it follows that the discriminant, d', of x_1 over E' divides the discriminant, d, of x_1 over E in R'. In particular, if d is an invertible element of R, then d' is an invertible element of R'.

Definition 1.15. [FrJ08, p. 109, Def. 6.1.3]. Consider two integrally closed integral domains $R \subseteq S$ with their respective quotient fields $E \subseteq F$ such that F/E is finite and separable. Suppose that $S = R[z]$, where z is integral over R and the discriminant of z over E is a unit of R (that is, an invertible element in R). In this set up we say that S/R is a **ring cover** and that F/E is the corresponding **field cover**. In this case [FrJ08, p. 109, Lemma 6.1.2] implies that S is the integral closure of R in F. We call the element z a **primitive element for the cover**. If in addition F/E is Galois, then S/R is called a **Galois ring cover**.

Remark 1.16. In the explicit case, if $R = K[x_1, \ldots, x_n]$ is a finitely generated extension of K, but not necessarily integrally closed, then we can find, effectively if R is presented over K, $x_{n+1} \in E = K(x_1, \ldots, x_n)$ such that $R' = K[x_1, \ldots, x_{n+1}]$ is integrally closed [FrJ08, Section 19.7]. Suppose that z is a primitive element for the extension F/E and that $f \in R[Z]$ is an irreducible polynomial over E such that $f(z) = 0$. Multiply x_{n+1} by the inverse of the product of the leading coefficient and the discriminant of f. Then $S' = R'[z]$ is a ring cover of R' with a primitive element z. If R' and z are presented over K, then the discriminant $\mathrm{Disc}(f) = N_{F/E}(f'(z))$ can be effectively computed [FrJ08, Section 19.2].

Recall the definition of a normal basic set [FrJ08, Section 19.6]:

Definition 1.17. Let L be a field.

a) An L-constructible subset A of $\mathbb{A}^n$ is called L-**basic** if $A = V \smallsetminus V(g)$, where $V = V(f_1, \ldots, f_m)$ with $f_1, \ldots, f_m, g \in L[X_1, \ldots, X_n]$ is an L-variety on which g does not vanish. If $\mathbf{x}$ is a generic point of V, then we call $L[A] = L[\mathbf{x}, g(\mathbf{x})^{-1}]$ the **coordinate ring** of A and $L(A) = L(\mathbf{x})$ the **function field** of A. The **dimension** of A is the transcendence degree of $L(A)/L$. Furthermore, the basic set A is **normal** if $L[A]$ is integrally

closed, and A is **presented** if the polynomials $f_1, \ldots, f_m, g$ and the ring $L[A]$ are presented.

b) Let P be a property of constructible sets (e.g., basic, normal, nonsingular, etc.). A P-**stratification** of a constructible set A is a finite collection $\{A_i |\ i \in I\}$ of disjoint constructible sets having property P such that $A = \bigcup_{i \in I}^{\cdot} A_i$. We refer to A_i as a P-set, $i \in I$.

c) Let A be an L-normal basic set and let C be an integral domain extending $L[A]$ such that $C/L[A]$ is a (Galois) ring cover. We call C/A a **(Galois) ring/set cover** over L.

As a result from Remark 1.16 we get

Remark 1.18. In the explicit case, suppose that A is a presented K-normal set and that F is a presented finite separable extension of $K(A)$. Then [FrJ08, p. 426, Lemma 19.7.2] effectively produces an integral domain C with these properties: the quotient field, $K(C)$, of C is F; and there is a presented K-basic set A', open in A, with C/A' a ring/set cover over K. Also, we can effectively find a primitive element z for the ring cover $C/K[A']$.

The next lemma [FrJ08, p. 424, Lemma 19.6.6] is the key lemma in the stratification procedure of Chapter II.

Lemma 1.19. *(The stratification lemma). Let* P *be a property of constructible sets. Suppose that for each presented L-basic set A we can effectively compute an L-basic* P*-set B, open in A. Then we can effectively produce a* P*-stratification of each presented constructible set.*

Now, Recall the definition of a decomposition group of a homomorphism and the definition of an Artin symbol [FrJ08, Section 30.1]:

Definition 1.20. Let C/A be a Galois ring/set cover over a field L with

$$L[A] = L[x_1, \ldots, x_n, g(\mathbf{x})^{-1}]$$

and let z be a primitive element for the ring cover $C/L[A]$. We denote the Galois group $\mathrm{Gal}(L(C)/L(A))$ by $\mathrm{Gal}(C/A)$ and consider a field M which contains L. If $(a_1, \ldots, a_n) \in A(M)$, then the L-specialization $\mathbf{x} \mapsto \mathbf{a}$ uniquely extends to a homomorphism φ_0 of $L[A]$ into M. We extend φ_0 further to a homomorphism φ from C into a Galois extension $N = M(\varphi(z))$ of M. Then

a) $$D(\varphi) = \{\sigma \in \mathrm{Gal}(C/A) |\ (\forall u \in C)[\varphi(u) = 0 \Rightarrow \varphi(\sigma u) = 0]\}$$ is the **decomposition group** of φ,

b) $$D_M(\varphi) = \{\sigma \in \mathrm{Gal}(C/A) |\ (\forall u \in C)[\varphi(u) \in M \Rightarrow \varphi(\sigma u) = \varphi(u)]\}$$ is a subgroup of $D(\varphi)$. If we want to emphasize that $D_M(\varphi)$ is a subgroup of $\mathrm{Gal}(C/A)$ we shall also write $D_M(\varphi)_{,L(A)}$ instead of $D_M(\varphi)$.

c) As φ ranges over all possible extensions of φ_0 to C, the group $D_M(\varphi)$ ranges over a conjugacy class of subgroups of $\mathrm{Gal}(C/A)$. We refer to this class as the **Artin symbol** of $\mathbf{a}$ in $\mathrm{Gal}(C/A)$ and we denote it by $\mathrm{Ar}(C/A, M, \mathbf{a})$. Whenever there can be no confusion, we omit reference to the cover from the Artin symbol and write it as $\mathrm{Ar}(A, M, \mathbf{a})$. If $H \in \mathrm{Ar}(A, M, \mathbf{a})$, then
$$\mathrm{Ar}(A, M, \mathbf{a}) = \{H^\sigma |\ \sigma \in \mathrm{Gal}(C/A)\}\,.$$

Remark 1.21. We continue to hold the notations in Definition 1.20 and let $\bar{E}$ and $\bar{F}$ be the quotient fields of $\varphi(L[A])$ and $\varphi(C)$, respectively. Then

a) Each $\sigma \in D(\varphi)$ induces an element $\overline{\sigma}$ of $\mathrm{Gal}(\bar{F}/\bar{E})$ by the formula $\overline{\sigma}(\varphi(u)) = \varphi(\sigma u)$ for each $u \in C$. From [FrJ08, p. 109, Lemma 6.1.4], the map $\varphi' \colon D(\varphi) \to \mathrm{Gal}(\bar{F}/\bar{E})$ that maps σ to $\overline{\sigma}$ is an isomorphism. Furthermore, φ' maps the subgroup $D_M(\varphi)$ of $D(\varphi)$ onto $\mathrm{Gal}(\bar{F}/\bar{F}\cap M)$. Thus, the composition of the isomorphism $\mathrm{res}_{\bar{F}} : \mathrm{Gal}(N/M) \to \mathrm{Gal}(\bar{F}/\bar{F}\cap M)$ with $(\varphi')^{-1}$ gives an isomorphism $\varphi^* : \mathrm{Gal}(N/M) \to D_M(\varphi)$, where $\varphi(\varphi^*(\sigma)(u)) = \sigma(\varphi(u))$ for each $\sigma \in \mathrm{Gal}(N/M)$ and each $u \in C$.

b) If $M = L$, then $D_M(\varphi) = D(\varphi)$.

c) If D/A is another Galois ring/set cover such that $C \subseteq D$ and φ is an L-homomorphism of D into $\tilde{M}$, then $\mathrm{res}_{L(C)} D_M(\varphi) = D_M(\mathrm{res}_{L(C)}\varphi)$ and hence, for $\mathbf{a} \in A(M)$, we get that
$$\mathrm{Ar}(C/A, M, \mathbf{a}) = \mathrm{res}_{L(C)}\mathrm{Ar}(D/A, M, \mathbf{a})$$
[FrJ08, page 709].

d) Replacement of A by an open subset A' does not affect the Artin symbol. Indeed, let $h \in L[X_1, \ldots, X_n]$ be a polynomial that does not vanish on A and let $A' = A \smallsetminus V(h)$, and $C' = C[h(\mathbf{x})^{-1}]$, where $\mathbf{x}$ is a generic point of A. Then C'/A' is also a Galois ring/set cover. If $\mathbf{a} \in A'(M)$, then $\mathrm{Ar}(A', M, \mathbf{a}) = \mathrm{Ar}(A, M, \mathbf{a})$.

e) More generally, if A' is an L-normal basic set contained in A with a generic point $\mathbf{x}'$, then the specialization $\mathbf{x} \mapsto \mathbf{x}'$ uniquely extends to an L-homomorphism, τ_0, of $L[A]$ into $L[A']$ [FrJ08, p. 424, Remark 19.6.4]. We further extend τ_0 to a homomorphism τ from C onto a Galois extension $L(C')$ of $L(A')$, where $C' = \tau(C)$. Then C'/A' is a Galois ring/set cover and τ induces an isomorphism $\tau^* : \mathrm{Gal}(C'/A') \to D(\tau)$ such that $\tau(\tau^*(\sigma)(u)) = \sigma(\tau(u))$ for each $\sigma \in \mathrm{Gal}(C'/A')$ and each $u \in C$ (this follows from a) and b) for $L(A')$ instead of L and M). If $\mathbf{a} \in A'(M)$, then $\tau^*(\mathrm{Ar}(A', M, \mathbf{a})) \subseteq \mathrm{Ar}(A, M, \mathbf{a})$ [FrJ08, page 710].

2. Elimination by Parts of Quantifiers from Existential Formulas

2.1. **Radical Relations.**

Notation 2.1. Let R be a commutative ring with a unit.

a) For $a_1, \ldots, a_n \in R$ we denote the ideal of R which is generated by $a_1, \ldots, a_n$ by $(a_1, \ldots, a_n)R$; i.e., $(a_1, \ldots, a_n)R = a_1R + \cdots + a_nR$. We omit the reference to R if it is clear from the context.

b) Let $\mathfrak{a}, \mathfrak{b}$ be two ideals of R. We denote the ideal
$$\{z \in R |\ z\mathfrak{b} \subseteq \mathfrak{a}\}$$
by $\mathfrak{a} : \mathfrak{b}$. Note that $\mathfrak{b} \subseteq \mathfrak{a} \Leftrightarrow \mathfrak{a} : \mathfrak{b} = R$.

c) We denote the collection of all maximal ideals by $\mathrm{Max}(R)$ and the collection of all nonzero prime ideals of R by $\mathrm{Spec}(R)$. For $\mathfrak{p} \in \mathrm{Spec}(R)$ we denote the localization of R at $\mathfrak{p}$ by $R_{\mathfrak{p}}$.

d) For an ideal $\mathfrak{a}$ of R we denote the **Jacobson radical** of $\mathfrak{a}$ by $\mathrm{Rad}_R\mathfrak{a} = \bigcap_{\substack{\mathfrak{m}\in\mathrm{Max}(R)\\ \mathfrak{m}\supseteq\mathfrak{a}}} \mathfrak{m}$ if $\mathfrak{a} \neq R$ and by $\mathrm{Rad}_R\mathfrak{a} = R$ if $\mathfrak{a} = R$ (we omit the reference to R if it is clear from the context). If $\mathrm{Max}(R) = \mathrm{Spec}(R)$ and $\mathfrak{a} \neq 0$ this is also the **nilradical**
$$\sqrt{\mathfrak{a}} = \{x \in R \,|\, \text{there exists } n \in \mathbb{N} \text{ such that } x^n \in \mathfrak{a}\}$$
of $\mathfrak{a}$ [Mat86, page 3]. If R is a field, then $\mathrm{Rad}_R\mathbf{0} = \mathbf{0} = \sqrt{\mathbf{0}}$.

e) Suppose that R is a Bezout domain. For $x, y \in R$ we denote a generator of the ideal $(x, y)R$ (which is determined up to a unit of R) by $\gcd(x, y)$. We denote

$$(x : y) = \begin{cases} \frac{x}{\gcd(x,y)} & y \neq 0 \\ \\ 1 & y = 0 \end{cases}.$$

Then $(x : y)$ is a generator of the ideal $xR : yR = \{z \in R \mid zy \in xR\}$. Indeed, it is clear that $(x : y) \in xR : yR$ and if $y = 0$ then $xR : \{0\} = \{z \in R | \ 0 \in xR\} = R$. Therefore, suppose that $y \neq 0$ and let $z \in R$ be such that $yz \in xR$. That is, there exists $a \in R$ such that $yz = ax$. Then $\frac{ax}{y} = z \in R$. Let $d = \gcd(x, y)$. Then $d \neq 0$ and there exist $x', y' \in R$ such that $x = x'd$, $y = y'd$, and $\gcd(x', y') = 1$. Hence, since $\frac{ax'}{y'} = \frac{ax}{y} = z \in R$, it follows that $y'|a$ in R. Therefore $\frac{a}{y'} \in R$ and $z = \frac{a}{y'}x' = \frac{a}{y'}\frac{x}{\gcd(x,y)} = \frac{a}{y'}(x : y)$. That is $z \in (x : y)R$. Thus $xR : yR = (x : y)R$.

Remark 2.2. Let R be a commutative ring with a unit.

a) For each $x, y \in R$ and each $\mathfrak{p} \in \mathrm{Spec}(R)$,
$$R_{\mathfrak{p}} \models x|y \Leftrightarrow (xR : yR) \not\subseteq \mathfrak{p}\,.$$
Indeed, $(xR : yR) \not\subseteq \mathfrak{p}$ if and only if there exists $z \in R \setminus \mathfrak{p}$ such that $zy \in xR$ iff $y \in xR_{\mathfrak{p}}$ iff $x|y$ in $R_{\mathfrak{p}}$.

b) Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of R. Then
$$\mathfrak{a} \subseteq \mathrm{Rad}_R\mathfrak{b} \Leftrightarrow \left(\forall \mathfrak{m} \in \mathrm{Max}(R)\right)\left[\mathfrak{b} \subseteq \mathfrak{m} \Rightarrow \mathfrak{a} \subseteq \mathfrak{m}\right].$$

c) Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of R. Then
$$\mathfrak{a} \subseteq \mathrm{Rad}_R\mathfrak{b} \Leftrightarrow (\forall z \in R)\left[1 \in \mathfrak{a} + zR \Rightarrow 1 \in \mathfrak{b} + zR\right].$$
Indeed, if $\mathfrak{b} = R$, then the claim is clear. Also, if R is a field and $\mathfrak{b} = 0$, then $\mathrm{Rad}_R\mathfrak{b} = 0$ and the claim is clear. Therefore, assume that R is not a field and $\mathfrak{b} \neq R$. If $\mathfrak{a} \subseteq \mathrm{Rad}_R\mathfrak{b}$, then $\mathfrak{a}$ is contained in each $\mathfrak{m} \in \mathrm{Max}(R)$ which contains $\mathfrak{b}$. Let $z \in R$ satisfies $\mathfrak{a} + zR = R$ and assume, on the contrary, that $\mathfrak{b} + zR \neq R$. Then there exists $\mathfrak{m} \in \mathrm{Max}(R)$ which contains $\mathfrak{b} + zR$ (and in particular contains $\mathfrak{b}$). Since $\mathfrak{a} \subseteq \mathfrak{m}$, $\mathfrak{m} + zR = R$. But this is a contradiction to $zR \subseteq \mathfrak{m}$. Conversely, let $\mathfrak{a}$ be an ideal of R such that for each $z \in R$, $\mathfrak{b} + zR = R$ or $\mathfrak{a} + zR \neq R$. Let $\mathfrak{m} \in \mathrm{Max}(R)$ which contains $\mathfrak{b}$. We need to show that $\mathfrak{a} \subseteq \mathfrak{m}$. Indeed, each $z \in \mathfrak{m}$ satisfies $\mathfrak{b} + zR \subseteq \mathfrak{m} \neq R$ and hence it follows from the assumption that also $\mathfrak{a} + zR \neq R$. Therefore $\mathfrak{a} + \mathfrak{m} \neq R$ and thus $\mathfrak{a} \subseteq \mathfrak{m}$.

d) Let $x, y_1, \ldots, y_l \in R$. Then
$$x \in \mathrm{Rad}(y_1, \ldots, y_l) \Leftrightarrow (\forall z \in R)[1 \in (z, x) \Rightarrow 1 \in (z, y_1, \ldots, y_l)]\,.$$

Remark 2.3. If L is an algebraic extension of K, then $\mathrm{Max}(\mathcal{O}_L) = \mathrm{Spec}(\mathcal{O}_L) = P_L$ and hence, for each ideal $\mathfrak{a}$ of $\mathcal{O}_L$,
$$\mathrm{Rad}_{\mathcal{O}_L}\mathfrak{a} = \bigcap_{\substack{\mathfrak{p} \in P_L \\ \mathfrak{p} \supseteq \mathfrak{a}}} \mathfrak{p} = \{x \in \mathcal{O}_L \,|\, \text{there exists } n \in \mathbb{N} \text{ such that } x^n \in \mathfrak{a}\}\,.$$
Note that if $\mathfrak{a} = \mathbf{0}$ then, since the Jacobson radical of $\mathcal{O}_L$ is zero, it follows that $\mathrm{Rad}_{\mathcal{O}_L}\mathfrak{a} = \mathbf{0} = \sqrt{\mathfrak{a}}$.

For $\mathfrak{p} \in P_L$, $\mathrm{Max}(\mathcal{O}_{L,\mathfrak{p}}) = \{\mathfrak{p}\mathcal{O}_{L,\mathfrak{p}}\} = \mathrm{Spec}(\mathcal{O}_{L,\mathfrak{p}})$.

Definition 2.4. Let R be a commutative ring with a unit. For any two positive integers k, l we introduce a $(2k + 2l)$-place relation $\mathrm{Rad}_{k,l}$ on R as follows: Let $\mathbf{a} = (a_1, \ldots, a_k), \mathbf{b} = (b_1, \ldots, b_k) \in R^k$, $\mathbf{c} = (c_1, \ldots, c_l), \mathbf{d} = (d_1, \ldots, d_l) \in R^l$; then

$$R \models \mathrm{Rad}_{k,l}(\mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d}) \Leftrightarrow \prod_{i=1}^{k}(a_iR : b_iR) \subseteq \mathrm{Rad}_R\Big(\sum_{j=1}^{l}(c_jR : d_jR)\Big)\,.$$

Remark 2.5. Let R be a commutative ring with a unit.

a) By Remark 2.2 c), the relations $\mathrm{Rad}_{k,l}$ are definable in the ring R in the language of rings.

b) Let $a \in R$. Then $\quad a = 0 \Leftrightarrow \mathrm{Rad}_{1,1}(1,1,0,a)\,.$
Indeed, let $\mathbf{0}$ be the zero ideal in R. Then
$$a = 0 \Leftrightarrow aR \subseteq \mathbf{0} \Leftrightarrow (\mathbf{0} : aR) = R \Leftrightarrow \mathrm{Rad}_R(\mathbf{0} : aR) = R$$
$$\Leftrightarrow 1R : 1R \subseteq \mathrm{Rad}_R(0R : aR) \Leftrightarrow \mathrm{Rad}_{1,1}(1,1,0,a)\,.$$

c) If R is a field, then, for each $a, b \in R$, $aR : bR = R$ or $aR : bR = \mathbf{0}$ and we have
$$aR : bR = \mathbf{0} \Leftrightarrow a = 0 \wedge b \neq 0 \text{ and } aR : bR = R \Leftrightarrow a \neq 0 \vee b = 0\,.$$
Also, for each two ideals $\mathfrak{a}$ and $\mathfrak{b}$ of R,
$$\mathfrak{ab} = R \Leftrightarrow \mathfrak{a} = R \wedge \mathfrak{b} = R \quad (\mathfrak{ab} = \mathbf{0} \Leftrightarrow \mathfrak{a} = \mathbf{0} \vee \mathfrak{b} = \mathbf{0})\,,$$
$$\mathfrak{a} + \mathfrak{b} = R \Leftrightarrow \mathfrak{a} = R \vee \mathfrak{b} = R \quad (\mathfrak{a} + \mathfrak{b} = \mathbf{0} \Leftrightarrow \mathfrak{a} = \mathbf{0} \wedge \mathfrak{b} = \mathbf{0})\,, \text{ and}$$
$$\mathfrak{a} \subseteq \mathrm{Rad}_R\mathfrak{b} \Leftrightarrow \mathfrak{a} = \mathbf{0} \vee \mathfrak{b} = R$$
(since $\mathrm{Rad}_R\mathfrak{b} = \mathfrak{b}$). Hence, in this case, we can replace the relations $\mathrm{Rad}_{k,l}$ by a disjunction of conjunctions of equalities and inequalities.

Remark 2.6. Let R be a Bezout domain. Then

a) For $\mathbf{a}, \mathbf{b} \in R^k$ and $\mathbf{c}, \mathbf{d} \in R^l$ we have
$$R \models \mathrm{Rad}_{k,l}(\mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d}) \Leftrightarrow \prod_{i=1}^{k}(a_i : b_i) \in \mathrm{Rad}_R\Big(\sum_{j=1}^{l}(c_j : d_j)R\Big)\,.$$

b) For $a, b_1, \ldots, b_l \in R$,
$$a \in (b_1, \ldots, b_l)R \Leftrightarrow 1 \in ((b_1 : a), \ldots, (b_l : a))R$$
$$\Leftrightarrow R \models \mathrm{Rad}_{1,l}(1, 1, b_1, \ldots, b_l, a, \ldots, a)\,.$$
That is, we can get a quantifier-free definition of ideal membership using the relation $\mathrm{Rad}_{1,l}$.

c) Diophantine problems on $\widetilde{\mathcal{O}}$ can be reduced to (decidable) ideal membership questions and hence, by b), to questions of the form $\widetilde{\mathcal{O}} \models \mathrm{Rad}_{k,l}(\mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d})$ (Note that $\widetilde{\mathcal{O}}$ is a Bezout domain). Here are two examples:

(1) Skolem [Sko34]: A polynomial $\quad a_0X^n + a_1X^{n-1} + \cdots + a_n \in \widetilde{\mathcal{O}}[X] \quad$ represents a unit of $\widetilde{\mathcal{O}}$ (i.e., there exists $x \in \widetilde{\mathcal{O}}$ such that $a_0x^n + a_1x^{n-1} + \cdots + a_n$ is a unit of $\widetilde{\mathcal{O}}$) if and only if $1 \in (a_0, \ldots, a_n)\widetilde{\mathcal{O}}$.

(2) Birch [Bir85]: If the polynomial $\sum a_{ij}X^iY^j \in \widetilde{\mathcal{O}}[X, Y]$ is homogeneous and $b \in \widetilde{\mathcal{O}}$, then: there exist $x, y \in \widetilde{\mathcal{O}}$ such that $\sum a_{ij}x^iy^j = b$ if and only if b belongs to the ideal generated by the a_{ij}'s.

Remark 2.7. Let M be an algebraic extension of K.

a) Let L be a finite subextension of M/K and let $\mathfrak{a}, \mathfrak{b}$ be two ideals of $\mathcal{O}_L$. Then

(1) For each $\mathfrak{p} \in P_L$ and each $\mathfrak{P} \in P_M$ which lies above $\mathfrak{p}$, $\mathfrak{P} \supseteq \mathfrak{a}\mathcal{O}_M \Leftrightarrow \mathfrak{p} \supseteq \mathfrak{a}$.

Every torsion-free module $\mathcal{M}$ over a Dedekind domain A (i.e., $0 \neq a \in A$, $0 \neq m \in \mathcal{M} \Rightarrow am \neq 0$) is flat [Mat86, Ex. 11.8, p. 86]. In particular, $\mathcal{O}_M$ is a flat $\mathcal{O}_L$-module and it follows from [Mat86, Thm. 7.4] that

(2) $$(\mathfrak{a}\cap\mathfrak{b})\mathcal{O}_M=\mathfrak{a}\mathcal{O}_M\cap\mathfrak{b}\mathcal{O}_M \quad \text{and}$$
(3) $$(\mathfrak{a}:\mathfrak{b})\mathcal{O}_M=\mathfrak{a}\mathcal{O}_M:\mathfrak{b}\mathcal{O}_M\ .$$

Over $\mathfrak{a}$ there are only finitely many prime ideals. Hence, by (2) and (1),

(4) $$(\mathrm{Rad}_{\mathcal{O}_L}\mathfrak{a})\mathcal{O}_M=(\bigcap_{\substack{\mathfrak{p}\in P_L\\ \mathfrak{p}\supseteq\mathfrak{a}}}\mathfrak{p})\mathcal{O}_M=\bigcap_{\substack{\mathfrak{p}\in P_L\\ \mathfrak{p}\supseteq\mathfrak{a}}}(\mathfrak{p}\mathcal{O}_M)$$
$$\subseteq\bigcap_{\substack{\mathfrak{p}\in P_L\\ \mathfrak{p}\supseteq\mathfrak{a}}}\ \bigcap_{\substack{\mathfrak{P}\in P_M\\ \mathfrak{P}\supseteq\mathfrak{p}\mathcal{O}_M}}\mathfrak{P}=\bigcap_{\substack{\mathfrak{P}\in P_M\\ \mathfrak{P}\supseteq\mathfrak{a}\mathcal{O}_M}}\mathfrak{P}=\mathrm{Rad}_{\mathcal{O}_M}(\mathfrak{a}\mathcal{O}_M)\,.$$

Also, by (1),

(5) $$(\mathrm{Rad}_{\mathcal{O}_M}(\mathfrak{a}\mathcal{O}_M))\cap\mathcal{O}_L=\bigcap_{\substack{\mathfrak{P}\in P_M\\ \mathfrak{P}\supseteq\mathfrak{a}\mathcal{O}_M}}(\mathfrak{P}\cap\mathcal{O}_L)=\bigcap_{\substack{\mathfrak{p}\in P_L\\ \mathfrak{p}\supseteq\mathfrak{a}}}\mathfrak{p}=\mathrm{Rad}_{\mathcal{O}_L}\mathfrak{a}\,.$$

Then, it follows from (4) and (5) that

(6) $$\mathfrak{b}\mathcal{O}_M\subseteq\mathrm{Rad}_{\mathcal{O}_M}(\mathfrak{a}\mathcal{O}_M)\Leftrightarrow\mathfrak{b}\subseteq\mathrm{Rad}_{\mathcal{O}_L}\mathfrak{a}\,.$$

Suppose that $\mathfrak{a}=\prod_{\mathfrak{p}\in P_L}\mathfrak{p}^{e(\mathfrak{p})}$ and $\mathfrak{b}=\prod_{\mathfrak{p}\in P_L}\mathfrak{p}^{f(\mathfrak{p})}$, where $e(\mathfrak{p})$ and $f(\mathfrak{p})$ are non-negative integers and almost all of them are zero. Then

(7) For each $\mathfrak{p}\in P_L$, $\quad e(\mathfrak{p})>f(\mathfrak{p})\Leftrightarrow\mathfrak{a}\supseteq\mathfrak{p}\mathfrak{b}\Leftrightarrow\mathfrak{a}:\mathfrak{b}\subseteq\mathfrak{p}$.

Thus
$$\mathfrak{a}:\mathfrak{b}=\prod_{\substack{\mathfrak{p}\in P_L\\ e(\mathfrak{p})>f(\mathfrak{p})}}\mathfrak{p}^{e(\mathfrak{p})-f(\mathfrak{p})}\,.$$

b) Let $\mathbf{a},\mathbf{b}\in\mathcal{O}_M^k$ and $\mathbf{c},\mathbf{d}\in\mathcal{O}_M^l$ and suppose that all the coordinates of $\mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d}$ are in $\mathcal{O}_L$, for a finite extension L of K. It follows from (3) that for each $x,y\in\mathcal{O}_L$, $(x\mathcal{O}_L:y\mathcal{O}_L)\mathcal{O}_M=x\mathcal{O}_M:y\mathcal{O}_M$. Hence, it follows from (6) that

(8) $$\mathcal{O}_M\models\mathrm{Rad}_{k,l}(\mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d})$$
$$\Leftrightarrow\prod_{i=1}^{k}(a_i\mathcal{O}_L:b_i\mathcal{O}_L)\subseteq\mathrm{Rad}_{\mathcal{O}_L}\Big(\sum_{j=1}^{l}(c_j\mathcal{O}_L:d_j\mathcal{O}_L)\Big)$$
$$\Leftrightarrow\mathcal{O}_L\models\mathrm{Rad}_{k,l}(\mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d})\ .$$

Since the coordinates of $\mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d}$ belong to $\widetilde{\mathcal{O}}$, it follows that (8) is satisfied also for $\widetilde{\mathcal{O}}$ instead of $\mathcal{O}_M$. Thus
$$\widetilde{\mathcal{O}}\models\mathrm{Rad}_{k,l}(\mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d})\Leftrightarrow\mathcal{O}_M\models\mathrm{Rad}_{k,l}(\mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d})\ .$$

c) Let $\mathbf{a},\mathbf{b}\in\mathcal{O}_M^k$ and $\mathbf{c},\mathbf{d}\in\mathcal{O}_M^l$. Then

$\mathcal{O}_M\models\mathrm{Rad}_{k,l}(\mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d})\Leftrightarrow$
$$(\forall\mathfrak{P}\in P_M)\Big[\Big(\bigwedge_{j=1}^{l}v_{\mathfrak{P}}(c_j)>v_{\mathfrak{P}}(d_j)\Big)\Rightarrow\Big(\bigvee_{i=1}^{k}v_{\mathfrak{P}}(a_i)>v_{\mathfrak{P}}(b_i)\Big)\Big]\,.$$

Indeed, it follows from (8) that
$$\mathcal{O}_M\models\mathrm{Rad}_{k,l}(\mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d})\Leftrightarrow$$
$$\prod_{i=1}^{k}(a_i\mathcal{O}_L:b_i\mathcal{O}_L)\subseteq\mathrm{Rad}_{\mathcal{O}_L}\Big(\sum_{j=1}^{l}(c_j\mathcal{O}_L:d_j\mathcal{O}_L)\Big)$$

where L is a finite subextension of M/K such that $\mathbf{a},\mathbf{b}\in\mathcal{O}_L^k$ and $\mathbf{c},\mathbf{d}\in\mathcal{O}_L^l$. Denote $\mathfrak{a}_i=(a_i\mathcal{O}_L:b_i\mathcal{O}_L)$, $i=1,\dots,k$, $\mathfrak{b}_j=(c_j\mathcal{O}_L:d_j\mathcal{O}_L)$, $j=1,\dots,l$, $\mathfrak{a}=\prod_{i=1}^k\mathfrak{a}_i$ and $\mathfrak{b}=\sum_{j=1}^l\mathfrak{b}_j$. Then, it follows from (7) that

$$\begin{aligned}
&\mathcal{O}_M\models \mathrm{Rad}_{k,l}(\mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d})\Leftrightarrow \mathfrak{a}\subseteq \mathrm{Rad}_{\mathcal{O}_L}\mathfrak{b}\\
&\Leftrightarrow(\forall\mathfrak{p}\in P_L)\Big[\mathfrak{b}\subseteq\mathfrak{p}\Rightarrow\mathfrak{a}\subseteq\mathfrak{p}\Big]\Leftrightarrow(\forall\mathfrak{p}\in P_L)\Big[\bigwedge_{j=1}^l\mathfrak{b}_j\subseteq\mathfrak{p}\Rightarrow\bigvee_{i=1}^k\mathfrak{a}_i\subseteq\mathfrak{p}\Big]\\
&\Leftrightarrow(\forall\mathfrak{p}\in P_L)\Big[\Big(\bigwedge_{j=1}^l v_\mathfrak{p}(c_j)>v_\mathfrak{p}(d_j)\Big)\Rightarrow\Big(\bigvee_{i=1}^k v_\mathfrak{p}(a_i)>v_\mathfrak{p}(b_i)\Big)\Big]\\
&\Leftrightarrow(\forall\mathfrak{P}\in P_M)\Big[\Big(\bigwedge_{j=1}^l v_\mathfrak{P}(c_j)>v_\mathfrak{P}(d_j)\Big)\Rightarrow\Big(\bigvee_{i=1}^k v_\mathfrak{P}(a_i)>v_\mathfrak{P}(b_i)\Big)\Big],
\end{aligned}$$

as required.

Proposition 2.8. *When $\mathcal{O}$ is an effective computability domain, then the relation $\mathrm{Rad}_{k,l}$ on $\widetilde{\mathcal{O}}$ is primitive recursive.*

Proof. Let $\mathbf{a},\mathbf{b}\in\widetilde{\mathcal{O}}^k$ and $\mathbf{c},\mathbf{d}\in\widetilde{\mathcal{O}}^l$. Then it follows from (8) that

$$\widetilde{\mathcal{O}}\models \mathrm{Rad}_{k,l}(\mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d})\Leftrightarrow\mathcal{O}_L\models\mathrm{Rad}_{k,l}(\mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d})\,, \tag{9}$$

where L is a finite extension of K such that $\mathbf{a},\mathbf{b}\in\mathcal{O}_L^k$ and $\mathbf{c},\mathbf{d}\in\mathcal{O}_L^l$. If $p=\mathrm{char}K>0$ we (effectively) find a power q of p such that L^q is a separable extension of K. Then, it follows from Remark 2.7 c) that

$$\begin{aligned}
&\mathcal{O}_L\models \mathrm{Rad}_{k,l}(\mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d})\\
&\Leftrightarrow(\forall\mathfrak{p}\in P_L)\Big[\Big(\bigwedge_{j=1}^l v_\mathfrak{p}(c_j)>v_\mathfrak{p}(d_j)\Big)\Rightarrow\Big(\bigvee_{i=1}^k v_\mathfrak{p}(a_i)>v_\mathfrak{p}(b_i)\Big)\Big]\\
&\Leftrightarrow(\forall\mathfrak{p}\in P_{L^q})\Big[\Big(\bigwedge_{j=1}^l v_\mathfrak{p}(c_j^q)>v_\mathfrak{p}(d_j^q)\Big)\Rightarrow\Big(\bigvee_{i=1}^k v_\mathfrak{p}(a_i^q)>v_\mathfrak{p}(b_i^q)\Big)\Big]\\
&\Leftrightarrow\mathcal{O}_{L^q}\models\mathrm{Rad}_{k,l}(\mathbf{a}^q,\mathbf{b}^q,\mathbf{c}^q,\mathbf{d}^q)\ .
\end{aligned}$$

Hence we can assume in (9), without loss, that L is a finite separable extension of K.

Now, by Remark 2.7 c), we can check whether the ideal inclusion in (8) holds by prime ideal factorization in $\mathcal{O}_L$: any $\mathfrak{p}\in P_L$ that divides *each* $c_j\mathcal{O}_L$ to higher multiplicity than it divides the corresponding $d_j\mathcal{O}_L$, $j=1,\dots,l$, must divide *some* $a_i\mathcal{O}_L$ (i between 1 and k) to higher multiplicity than it does the corresponding $b_i\mathcal{O}_L$. That is, in order to show that the relation $\mathrm{Rad}_{k,l}$ on $\widetilde{\mathcal{O}}$ is primitive recursive, we need to know how to (effectively) factor, for every finite separable extension L of K and each $x\in\mathcal{O}_L$, the ideal $x\mathcal{O}_L$ into a product of prime ideals. The factorization procedure is written in Appendix A for the case that $\mathcal{O}=\mathcal{O}_0$ is a presented Euclidean domain of finite type. In the general case $\mathcal{O}=S_0^{-1}\mathcal{O}_0$, where S_0 is a presented multiplicative subset of $\mathcal{O}_0$. We find $s\in S_0$ such that $s\cdot N_{L/K}(x)\in\mathcal{O}_0$. Then $sx\in\mathcal{O}_{0,L}$. We factor the ideal $sx\mathcal{O}_{0,L}$ into a product of prime ideals of $\mathcal{O}_{0,L}$:

$$sx\mathcal{O}_{0,L}=\prod_{\mathfrak{p}\in I}\mathfrak{p}\,.$$

For each $\mathfrak{p} \in I$ we find an irreducible element p of $\mathcal{O}_0$ such that $p\mathcal{O}_0 = \mathfrak{p} \cap \mathcal{O}_0$. If $p \in S_0$ then $S_0^{-1}\mathfrak{p} = \mathcal{O}_L = S_0^{-1}\mathcal{O}_{0,L}$ and if $p \notin S_0$ then $S_0^{-1}\mathfrak{p}$ is a proper prime ideal of $S_0^{-1}\mathcal{O}_{0,L} = \mathcal{O}_L$. We denote $I' = \{\mathfrak{p} \in I \,|\, \mathfrak{p} \cap \mathcal{O}_0 = p\mathcal{O}_0 \text{ for some } p \notin S_0\}$. Then

$$x\mathcal{O}_L = xS_0^{-1}\mathcal{O}_{0,L} = S_0^{-1}\big(sx\mathcal{O}_{0,L}\big) = S_0^{-1}\Big(\prod_{\mathfrak{p}\in I}\mathfrak{p}\Big) = \prod_{\mathfrak{p}\in I'}\big(S_0^{-1}\mathfrak{p}\big)\,.$$

Thus, $x\mathcal{O}_L = \prod_{\mathfrak{p}\in I'}\big(S_0^{-1}\mathfrak{p}\big)$ is the factorization of the ideal $x\mathcal{O}_L$ into a product of prime ideals of $\mathcal{O}_L$. □

2.2. **The Languages $\mathcal{L}_{\mathrm{div}}$ and $\mathcal{L}_{\mathrm{rad}}$.**

Definition 2.9. Let $\mathcal{L} = \{0, 1, +, -, \cdot\}$ be the language of rings.

a) $\mathcal{L}_{\mathrm{div}} = \{0, 1, +, -, \cdot, |\ \}$ is the language of rings augmented by the symbol $|$ of a binary relation which is interpreted in any ring as divisibility: $x|y \leftrightarrow \exists z[xz = y]$.
$\mathcal{L}_{\mathrm{rad}} = \{0, 1, +, -, \cdot, (\mathrm{Rad}_{k,l})_{k,l\geq 1}\}$ is the language of rings augmented by the extra predicates $\mathrm{Rad}_{k,l}$.

b) Let R be a commutative ring with a unit. We denote the languages $\mathcal{L}$, $\mathcal{L}_{\mathrm{div}}$, and $\mathcal{L}_{\mathrm{rad}}$ augmented by a constant symbol for each element of R by $\mathcal{L}(R)$, $\mathcal{L}_{\mathrm{div}}(R)$, and $\mathcal{L}_{\mathrm{rad}}(R)$, respectively. In any ring which contains an homomorphic image $\bar{R}$ of R, these symbols are interpreted as elements of $\bar{R}$ which satisfy the additive and multiplicative tables of corresponding elements in R.

Note that each formula in the language $\mathcal{L}(\mathbb{Z})$ (resp., $\mathcal{L}_{\mathrm{div}}(\mathbb{Z})$, $\mathcal{L}_{\mathrm{rad}}(\mathbb{Z})$) can be translated into a formula in the language $\mathcal{L}$ (resp., $\mathcal{L}_{\mathrm{div}}$, $\mathcal{L}_{\mathrm{rad}}$).

Remark 2.10.

a) An atomic formula in the language $\mathcal{L}_{\mathrm{div}}(R)$ is a formula of the form $a|b$, where a and b are terms in the language $\mathcal{L}(R)$. Note that equalities can be replaced by divisibilities using $a = 0 \leftrightarrow 0|a$.

b) An atomic formula in the language $\mathcal{L}_{\mathrm{rad}}(R)$ is of the form $\mathrm{Rad}_{k,l}(\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d})$ where a_i, b_i, $i = 1, \ldots, k$, and c_j, d_j, $j = 1, \ldots, l$, are terms in the language $\mathcal{L}(R)$. Note that, by Remark 2.5 b), we can replace equalities using the equivalence $a = 0 \leftrightarrow \mathrm{Rad}_{1,1}(1, 1, 0, a)$.

c) If E is a field, then by Remark 2.5 c), for each quantifier-free formula $\varphi(X_1, \ldots, X_n)$ in the language $\mathcal{L}_{\mathrm{rad}}(E)$ corresponds a quantifier-free formula $\psi(X_1, \ldots, X_n)$ in the language $\mathcal{L}(E)$ such that for each field F which contains E and each $\mathbf{a} \in F^n$ we have

$$F \models \varphi(\mathbf{a}) \Leftrightarrow F \models \psi(\mathbf{a})\,.$$

By Remark 2.7 b) we get

Proposition 2.11. *Let $\psi(Y_1, \ldots, Y_n)$ be quantifier-free $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$-formula. Then, for every algebraic extension M of K and each $\mathbf{a} \in \mathcal{O}_M^n$ we have*

$$\widetilde{\mathcal{O}} \models \psi(\mathbf{a}) \Leftrightarrow \mathcal{O}_M \models \psi(\mathbf{a})\,.$$

We shall use the following definition and the lemma after it in the beginning of Section 3.

Definition 2.12.

a) Let R be a commutative ring with a unit and let θ be a quantifier-free sentence in the language $\mathcal{L}_{\mathrm{rad}}(R)$. We define the **definition set** D_θ **of** θ **in** R by an induction on the structure of θ:

If θ is the atomic formula $\mathrm{Rad}_{k,l}(\mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d})$ where $\mathbf{a},\mathbf{b}\in R^k$ and $\mathbf{c},\mathbf{d}\in R^l$, we denote $I=\{1,\dots,k\}$, $J=\{1,\dots,l\}$ and define

$$I_{\mathbf{a}}=\{i\in I\,|\,a_i\neq 0\},\quad I_{\mathbf{b}}=\{i\in I\,|\,b_i\neq 0\},\quad \text{and}$$
$$J_{\mathbf{c}}=\{j\in J\,|\,c_j\neq 0\},\quad J_{\mathbf{d}}=\{j\in J\,|\,d_j\neq 0\}\,.$$

Then D_θ is defined to be the set

$$\{a_i,b_{i'},c_j,d_{j'}\,|\,i\in I_{\mathbf{a}},\,i'\in I_{\mathbf{b}},\,j\in J_{\mathbf{c}},\,j'\in J_{\mathbf{d}}\}\,.$$

If θ is the formula $\theta=\theta_1\vee\theta_2$ and D_{θ_1}, D_{θ_2} have already been defined, then $D_\theta=D_{\theta_1}\cup D_{\theta_2}$. And if θ is the formula $\neg\chi$ and D_χ has already been defined, then $D_\theta=D_\chi$.

b) Let R be an integrally closed integral domain with quotient field E, let F be a finite separable extension of E and let z be a primitive element for the extension F/E which is integral over R. Let θ be a quantifier-free formula in the language $\mathcal{L}_{\mathrm{rad}}(R[z])$; that is, to θ corresponds a quantifier-free formula $\varphi(Z)$ in the language $\mathcal{L}_{\mathrm{rad}}(R)$ such that $\theta=\varphi(z)$. Then D_θ is a finite subset of $R[z]\setminus\{0\}$. Let

$$c_\theta=N_{F/E}(\prod_{d\in D_\theta}d)\,.$$

Then c_θ is a nonzero element of R. If $D_\theta=\emptyset$ we denote $c_\theta=1$. We call c_θ the **content of** θ **in** R.

Suppose that R is presented in E and E has elimination theory. Then, if θ is a presented sentence, that is, $\mathrm{irr}(z,E)$ and $\varphi(Z)$ are given, then we can effectively find D_θ and c_θ.

Lemma 2.13. *Let R be an integrally closed integral domain with a quotient field E. Let F be a finite separable extension of E with a primitive element z which is integral over R. Let θ be a quantifier-free sentence in the language $\mathcal{L}_{\mathrm{rad}}(R[z])$. Let D_θ be the definition set of θ in $R[z]$ and let c_θ be the content of θ in R. Let M be an algebraic extension of K and suppose that there exists a homomorphism $\tau:R[z]\to M$ which satisfies $\tau(c_\theta)\neq 0$, $\tau(\theta)\in\mathcal{L}_{\mathrm{rad}}(\mathcal{O}_M)$, and $\mathcal{O}_M\models\tau(\theta)$.*

Let $\tau':R[z]\to M$ be a homomorphism which satisfies that $\frac{\tau'(d)}{\tau(d)}$ is an invertible element of $\mathcal{O}_M$ for each $d\in D_\theta$. Then $\tau'(\theta)\in\mathcal{L}_{\mathrm{rad}}(\mathcal{O}_M)$ and $\mathcal{O}_M\models\tau'(\theta)$.

Proof. Let $\varphi(Z)$ be a quantifier-free formula in the language $\mathcal{L}_{\mathrm{rad}}(R)$ which satisfies $\theta=\varphi(z)$. It suffices to prove the lemma under the assumption that $\varphi(Z)$ is an atomic formula. Therefore, suppose that $\varphi(Z)$ is the formula

$$\mathrm{Rad}_{k,l}\big(\mathbf{a}(Z),\mathbf{b}(Z),\mathbf{c}(Z),\mathbf{d}(Z)\big)\,,$$

where $\mathbf{a}(Z),\mathbf{b}(Z)\in R[Z]^k$ and $\mathbf{c}(Z),\mathbf{d}(Z)\in R[Z]^l$. Then $\tau(\theta)$ is the sentence

$$\mathrm{Rad}_{k,l}\big(\tau(\mathbf{a}(z)),\tau(\mathbf{b}(z)),\tau(\mathbf{c}(z)),\tau(\mathbf{d}(z))\big)\,.$$

Let i be a positive integer between 1 and k. If $a_i(z)=0$, then $\tau(a_i(z))=0=\tau'(a_i(z))$. If $a_i(z)\neq 0$, then $a_i(z)\in D_\theta$ (in particular, $\tau(a_i(z))\neq 0$) and hence $\frac{\tau'(a_i(z))}{\tau(a_i(z))}$ is an invertible element of $\mathcal{O}_M$. In any case, $\tau(a_i(z))\mathcal{O}_M=\tau'(a_i(z))\mathcal{O}_M$. Similarly, $\tau(b_i(z))\mathcal{O}_M=\tau'(b_i(z))\mathcal{O}_M$ for each i between 1 and k and $\tau(c_j(z))\mathcal{O}_M=$

$\tau'(c_j(z))\mathcal{O}_M$, $\tau(d_j(z))\mathcal{O}_M = \tau'(d_j(z))\mathcal{O}_M$ for each j between 1 and l. Thus $\tau'(\theta) \in \mathcal{L}_{\mathrm{rad}}(\mathcal{O}_M)$ and

$$\begin{aligned}
\mathcal{O}_M \models \tau(\theta) &\Leftrightarrow \mathcal{O}_M \models \mathrm{Rad}_{k,l}\big(\tau(\mathbf{a}(z)), \tau(\mathbf{b}(z)), \tau(\mathbf{c}(z)), \tau(\mathbf{d}(z))\big) \\
&\Leftrightarrow \prod_{i=1}^{k} \big(\tau(a_i(z))\mathcal{O}_M : \tau(b_i(z))\mathcal{O}_M\big) \\
&\qquad \subseteq \mathrm{Rad}_{\mathcal{O}_M}\Big(\sum_{j=1}^{l} \big(\tau(c_j(z))\mathcal{O}_M : \tau(d_j(z))\mathcal{O}_M\big)\Big) \\
&\Leftrightarrow \prod_{i=1}^{k} \big(\tau'(a_i(z))\mathcal{O}_M : \tau'(b_i(z))\mathcal{O}_M\big) \\
&\qquad \subseteq \mathrm{Rad}_{\mathcal{O}_M}\Big(\sum_{j=1}^{l} \big(\tau'(c_j(z))\mathcal{O}_M : \tau'(d_j(z))\mathcal{O}_M\big)\Big) \\
&\Leftrightarrow \mathcal{O}_M \models \mathrm{Rad}_{k,l}\big(\tau'(\mathbf{a}(z)), \tau'(\mathbf{b}(z)), \tau'(\mathbf{c}(z)), \tau'(\mathbf{d}(z))\big) \Leftrightarrow \mathcal{O}_M \models \tau'(\theta)\,.
\end{aligned}$$

□

Remark 2.14.

a) If $\mathcal{O} = K$, then $\mathcal{O}_M = M$. Assume that there exists a homomorphism $\tau\colon R[z] \to M$ which satisfies $\tau(c_\theta) \neq 0$, $\tau(\theta) \in \mathcal{L}_{\mathrm{rad}}(M)$, and $M \models \tau(\theta)$. Then, for any homomorphism $\tau' : R[z] \to M$ which satisfies $\tau'(c_\theta) \neq 0$ we have that $\frac{\tau'(d)}{\tau(d)}$ is an invertible element of $\mathcal{O}_M$ for each $d \in D_\theta$. Therefore, for each such homomorphism τ', $M \models \tau'(\theta)$.

b) If $R = K[x_1, \ldots, x_n]$, then to θ corresponds a quantifier-free formula $\psi(\mathbf{X}, Z)$ in $\mathcal{L}_{\mathrm{rad}}(K)$ such that $\theta = \psi(\mathbf{x}, z)$. Suppose there is a K-homomorphism, $\tau\colon K[\mathbf{x}, z] \to \tilde{K}$, which satisfies $\tau(c_\theta) \neq 0$ and $\tilde{K} \models \tau(\theta)$. Then, for every algebraic extension M of K and each K-homomorphism, $\tau'\colon K[\mathbf{x}, z] \to M$, which satisfies $\tau'(c_\theta) \neq 0$ we have $M \models \tau'(\theta)$.
Indeed, it follows from a) that $\tilde{K} \models \tau'(\theta)$. That is,

$$\tilde{K} \models \psi(\tau'(\mathbf{x}), \tau'(z))\,.$$

Hence, it follows from Proposition 2.11 that $M \models \psi(\tau'(\mathbf{x}), \tau'(z))$. Thus, $M \models \tau'(\theta)$.

The next theorem is proved in Appendix B.

Theorem 2.15. *For each formula $\varphi(\mathbf{Y})$, $\mathbf{Y} = (Y_1, \ldots, Y_n)$, in the language $\mathcal{L}_{\mathrm{div}}(\mathcal{O})$ there exists a quantifier-free formula $\overline{\varphi}(\mathbf{Y})$ in the same language, such that $\varphi(\mathbf{Y}) \leftrightarrow \overline{\varphi}(\mathbf{Y})$ holds in all nontrivial valuation rings (i.e., which are not fields), which contain a homomorphic image of $\mathcal{O}$, with algebraically closed quotient field.*

Moreover, if $\mathcal{O}$ is a presented ring and $\varphi(\mathbf{Y})$ is presented, then we can effectively (primitive recursively) construct $\overline{\varphi}(\mathbf{Y})$.

This theorem is corollary 3.4 in [Wei84] (for $\mathcal{O} = \mathbb{Z}$) which is an improvement of [Rob56, p. 54]. (See also [MMD83, p. 83]; here, however, the procedure is only recursive.)

Lemma 2.16. *For each formula $\varphi(\mathbf{Y})$, $\mathbf{Y} = (Y_1, \ldots, Y_n)$, in the language $\mathcal{L}_{\mathrm{div}}(\mathcal{O})$ we can construct, effectively, if $\mathcal{O}$ is a presented ring and $\varphi(\mathbf{Y})$ is presented, a*

quantifier-free $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$-formula $\varphi'(\mathbf{Y})$ such that for every algebraic extension M of K and for each $\mathbf{a} \in \mathcal{O}_M^n$ we have

$$(\forall \mathfrak{P} \in \tilde{P})\, \widetilde{\mathcal{O}}_{\mathfrak{P}} \models \varphi(\mathbf{a}) \Leftrightarrow \mathcal{O}_M \models \varphi'(\mathbf{a})\,.$$

Moreover, if $\mathcal{O} = K$, then $\varphi'(\mathbf{Y})$ is a quantifier-free $\mathcal{L}(K)$-formula, and if $\mathcal{O} \neq K$, then $\varphi'(\mathbf{Y})$ is a conjunction $\varphi_1(\mathbf{Y}) \wedge \cdots \wedge \varphi_r(\mathbf{Y})$ of atomic $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$-formulas.

Proof. If $\mathcal{O} = K$, then $\widetilde{\mathcal{O}}_{\mathfrak{P}} = \tilde{K}$ for $\mathfrak{P} \in \tilde{P}$. Then, since the theory of algebraically closed fields which contain K has an effective procedure of quantifiers elimination in the language $\mathcal{L}(K)$, the claim is clear. Therefore, suppose that $\mathcal{O} \neq K$. Then, for each $\mathfrak{P} \in \tilde{P}$, $\widetilde{\mathcal{O}}_{\mathfrak{P}}$ is not a field. Hence, using Theorem 2.15, we can assume that $\varphi(\mathbf{Y})$ is a quantifier-free formula in the language $\mathcal{L}_{\mathrm{div}}(\mathcal{O})$. We write $\varphi(\mathbf{Y})$ in conjunctive normal form:

$$\bigwedge_{i\in I} \Big(\bigvee_{j\in J_i} \varphi_{ij}(\mathbf{Y}) \vee \bigvee_{j\in J_i'} \neg\varphi_{ij}(\mathbf{Y})\Big)$$

in which $\varphi_{ij}(\mathbf{Y})$ is an atomic formula in the language $\mathcal{L}_{\mathrm{div}}(\mathcal{O})$. It suffices to prove the desired result for each of the conjuncts. Hence, we may assume, without loss, that $\varphi(\mathbf{Y})$ is the formula

$$\bigvee_{j=1}^{l} \psi_j(\mathbf{Y}) \vee \bigvee_{i=1}^{k} \neg\chi_i(\mathbf{Y})\,,$$

where $\chi_i(\mathbf{Y})$ is the formula $\alpha_i(\mathbf{Y})|\beta_i(\mathbf{Y})$ and $\psi_j(\mathbf{Y})$ is the formula $\gamma_j(\mathbf{Y})|\delta_j(\mathbf{Y})$, with $\alpha_i, \beta_i, \gamma_j, \delta_j \in \mathcal{O}[\mathbf{Y}]$. That is, we assume that $\varphi(\mathbf{Y})$ is the formula

$$\alpha_1(\mathbf{Y}) \nmid \beta_1(\mathbf{Y}) \vee \cdots \vee \alpha_k(\mathbf{Y}) \nmid \beta_k(\mathbf{Y}) \vee \gamma_1(\mathbf{Y})|\delta_1(\mathbf{Y}) \vee \cdots \vee \gamma_l(\mathbf{Y})|\delta_l(\mathbf{Y})\,.$$

Hence, it suffices to prove that for every algebraic extension M of K and each $\mathbf{a} \in \mathcal{O}_M^n$ we have

$$(\forall \mathfrak{P} \in \tilde{P})\, \widetilde{\mathcal{O}}_{\mathfrak{P}} \models \varphi(\mathbf{a}) \Leftrightarrow \mathcal{O}_M \models \mathrm{Rad}_{k,l}(\boldsymbol{\alpha}(\mathbf{a}), \boldsymbol{\beta}(\mathbf{a}), \boldsymbol{\gamma}(\mathbf{a}), \boldsymbol{\delta}(\mathbf{a}))\,,$$

where $\boldsymbol{\alpha}(\mathbf{a}) = (\alpha_1(\mathbf{a}), \ldots, \alpha_k(\mathbf{a}))$, etc. Indeed, using Remarks 2.2 a) and b) and 2.7 b), we get

$$\begin{aligned}
&(\forall \mathfrak{P} \in \tilde{P})\, \widetilde{\mathcal{O}}_{\mathfrak{P}} \models \varphi(\mathbf{a}) \\
&\Leftrightarrow (\forall \mathfrak{P} \in \tilde{P})\Big(\bigvee_{i=1}^{k} [(\alpha_i(\mathbf{a})\widetilde{\mathcal{O}} : \beta_i(\mathbf{a})\widetilde{\mathcal{O}}) \subseteq \mathfrak{P}] \vee \bigvee_{j=1}^{l} [(\gamma_j(\mathbf{a})\widetilde{\mathcal{O}} : \delta_j(\mathbf{a})\widetilde{\mathcal{O}}) \not\subseteq \mathfrak{P}]\Big) \\
&\Leftrightarrow (\forall \mathfrak{P} \in \tilde{P})\Big[\Big(\bigwedge_{j=1}^{l} (\gamma_j(\mathbf{a})\widetilde{\mathcal{O}} : \delta_j(\mathbf{a})\widetilde{\mathcal{O}}) \subseteq \mathfrak{P}\Big) \Rightarrow \Big(\bigvee_{i=1}^{k} (\alpha_i(\mathbf{a})\widetilde{\mathcal{O}} : \beta_i(\mathbf{a})\widetilde{\mathcal{O}}) \subseteq \mathfrak{P}\Big)\Big] \\
&\Leftrightarrow (\forall \mathfrak{P} \in \tilde{P})\Big[\Big(\sum_{j=1}^{l} (\gamma_j(\mathbf{a})\widetilde{\mathcal{O}} : \delta_j(\mathbf{a})\widetilde{\mathcal{O}})\Big) \subseteq \mathfrak{P} \Rightarrow \Big(\prod_{i=1}^{k} (\alpha_i(\mathbf{a})\widetilde{\mathcal{O}} : \beta_i(\mathbf{a})\widetilde{\mathcal{O}})\Big) \subseteq \mathfrak{P}\Big] \\
&\Leftrightarrow \prod_{i=1}^{k} (\alpha_i(\mathbf{a})\widetilde{\mathcal{O}} : \beta_i(\mathbf{a})\widetilde{\mathcal{O}}) \subseteq \mathrm{Rad}_{\widetilde{\mathcal{O}}}\Big(\sum_{j=1}^{l} (\gamma_j(\mathbf{a})\widetilde{\mathcal{O}} : \delta_j(\mathbf{a})\widetilde{\mathcal{O}})\Big) \\
&\Leftrightarrow \widetilde{\mathcal{O}} \models \mathrm{Rad}_{k,l}(\boldsymbol{\alpha}(\mathbf{a}), \boldsymbol{\beta}(\mathbf{a}), \boldsymbol{\gamma}(\mathbf{a}), \boldsymbol{\delta}(\mathbf{a})) \\
&\Leftrightarrow \mathcal{O}_M \models \mathrm{Rad}_{k,l}(\boldsymbol{\alpha}(\mathbf{a}), \boldsymbol{\beta}(\mathbf{a}), \boldsymbol{\gamma}(\mathbf{a}), \boldsymbol{\delta}(\mathbf{a}))\,.
\end{aligned}$$

□

2.3. **Special Existential Formulas.**

Definition 2.17. We introduce, for convenience, two auxilary predicates $\underline{\mathrm{R}}$ (binary) and $\underline{\mathrm{NU}}$ (unary) to be interpreted in any commutative ring with a unit R as follows: For each $a, b \in R$,

$$R \models a\underline{\mathrm{R}}b \Leftrightarrow a \in \mathrm{Rad}_R(bR) \wedge b \neq 0, \text{ and}$$

$$R \models \underline{\mathrm{NU}}(a) \Leftrightarrow a \text{ is not an invertible element of } R\,.$$

Note that, by Remark 2.2 d), the predicate $\underline{\mathrm{R}}$ can be defined in the language $\mathcal{L}$. The predicate $\underline{\mathrm{NU}}$ is also definable in the language $\mathcal{L}$: $\underline{\mathrm{NU}}(x) \leftrightarrow \forall y[xy \neq 1]$.

Remark 2.18. We interpret the predicates $\underline{\mathrm{R}}$ and $\underline{\mathrm{NU}}$ for a localization $\widetilde{\mathcal{O}}_{\mathfrak{P}}$ of $\widetilde{\mathcal{O}}$ at $\mathfrak{P} \in \tilde{P}$: it follows from Remark 2.3 that for each $a, b \in \widetilde{\mathcal{O}}_{\mathfrak{P}}$,

$$(\widetilde{\mathcal{O}}_{\mathfrak{P}} \models a\underline{\mathrm{R}}b) \Leftrightarrow (\exists n \in \mathbb{N})[a^n \in b\widetilde{\mathcal{O}}_{\mathfrak{P}}] \wedge b \neq 0, \quad \text{and}$$

$$(\widetilde{\mathcal{O}}_{\mathfrak{P}} \models \underline{\mathrm{NU}}(a)) \Leftrightarrow a \in \mathfrak{P}\widetilde{\mathcal{O}}_{\mathfrak{P}} \Leftrightarrow v_{\mathfrak{P}}(a) > 0\,.$$

Definition 2.19. A **special existential formula** $\varphi(\mathbf{Y})$, $\mathbf{Y} = (Y_1, \ldots, Y_n)$, is a formula of the form

$$\exists \mathbf{X}[\mathbf{f}(\mathbf{X}, \mathbf{Y}) = 0 \wedge g(\mathbf{X}, \mathbf{Y}) \neq 0 \wedge \mathbf{R}(\mathbf{X}, \mathbf{Y}) \wedge \mathbf{NU}(\mathbf{X}, \mathbf{Y})]\,,$$

with $\mathbf{X} = (X_1, \ldots, X_m)$, $\mathbf{f}(\mathbf{X}, \mathbf{Y}) = (f_1(\mathbf{X}, \mathbf{Y}), \ldots, f_k(\mathbf{X}, \mathbf{Y}))$, $\mathbf{R}(\mathbf{X}, \mathbf{Y})$ a conjunction $\bigwedge_{1 \leq i \leq p} h_{i1}(\mathbf{X}, \mathbf{Y})\,\underline{\mathrm{R}}\,h_{i2}(\mathbf{X}, \mathbf{Y})$ and $\mathbf{NU}(\mathbf{X}, \mathbf{Y})$ a conjunction $\bigwedge_{1 \leq j \leq q} \underline{\mathrm{NU}}(k_j(\mathbf{X}, \mathbf{Y}))$, where $f_1, \ldots, f_k$, g, h_{i1}, h_{i2} $(1 \leq i \leq p)$, k_j $(1 \leq j \leq q)$ are polynomials in $\mathcal{O}[\mathbf{X}, \mathbf{Y}]$. If $\mathcal{O} = K$, we require that $p = q = 0$.

For each $\mathbf{a} \in \tilde{K}^n$ let $V_{\mathbf{f},\mathbf{a}}$ be the algebraic set

$$\{\mathbf{x} \in \mathbb{A}^m |\ f_1(\mathbf{x}, \mathbf{a}) = 0, \ldots, f_k(\mathbf{x}, \mathbf{a}) = 0\}\,.$$

Proposition 2.20. *Let $\varphi(\mathbf{Y})$ be the special existential formula of Definition 2.19. Then, there exists a quantifier-free formula $\overline{\varphi}(\mathbf{Y})$ in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$ such that for every perfect algebraic extension M of K which is PAC over $\mathcal{O}_M$ and for each $\mathbf{a} \in \mathcal{O}_M^n$ which satisfies that $V_{\mathbf{f},\mathbf{a}}$ is absolutely irreducible we have: $\mathcal{O}_M \models \varphi(\mathbf{a}) \leftrightarrow \overline{\varphi}(\mathbf{a})$.*

Moreover, in the explicit case, if $\varphi(\mathbf{Y})$ is presented, then we can effectively construct $\overline{\varphi}(\mathbf{Y})$.

Proof. Let M be a perfect algebraic extension of K which is PAC over $\mathcal{O}_M$ and let $\mathbf{a} \in \mathcal{O}_M^n$ which satisfies that $V_{\mathbf{f},\mathbf{a}}$ is absolutely irreducible.

Claim: $\mathcal{O}_M \models \varphi(\mathbf{a})$ if and only if (1) and (2) below are satisfied:

(1) $\quad (\forall \mathfrak{P} \in \tilde{P})\,\widetilde{\mathcal{O}}_{\mathfrak{P}} \models \exists \mathbf{X}[\mathbf{f}(\mathbf{X}, \mathbf{a}) = 0 \wedge g(\mathbf{X}, \mathbf{a}) \neq 0 \wedge \mathbf{R}(\mathbf{X}, \mathbf{a})]\,,$

(2) for each j between 1 and q there is $\mathfrak{P}_j \in \tilde{P}$ such that
$\widetilde{\mathcal{O}}_{\mathfrak{P}_j} \models \exists \mathbf{X}[\mathbf{f}(\mathbf{X}, \mathbf{a}) = 0 \wedge g(\mathbf{X}, \mathbf{a}) \neq 0 \wedge \mathbf{R}(\mathbf{X}, \mathbf{a}) \wedge \underline{\mathrm{NU}}(k_j(\mathbf{X}, \mathbf{a}))]\,.$

Indeed, it is clear that if $\mathcal{O}_M \models \varphi(\mathbf{a})$, then (1) and (2) hold. Conversely, suppose that (1) and (2) hold. We take maximal ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_q \in \tilde{P}$ as in (2) and points $\mathbf{x}_j \in (\widetilde{\mathcal{O}}_{\mathfrak{P}_j})^m$ such that

$$(3)\qquad \widetilde{\mathcal{O}}_{\mathfrak{P}_j} \models \mathbf{f}(\mathbf{x}_j,\mathbf{a})=0\wedge g(\mathbf{x}_j,\mathbf{a})\neq 0\wedge \bigwedge_{1\le i\le p} h_{i1}(\mathbf{x}_j,\mathbf{a})\,\underline{\mathrm{R}}\,h_{i2}(\mathbf{x}_j,\mathbf{a})\wedge \underline{\mathrm{NU}}(k_j(\mathbf{x}_j,\mathbf{a}))\,.$$

If follows from Remark 2.18 that there is $n\in\mathbb{N}$ and there are $z_{ij}\in\widetilde{\mathcal{O}}_{\mathfrak{P}_j}$ for $1\le i\le p$, $1\le j\le q$, such that

$$(4)\qquad h_{i1}(\mathbf{x}_j,\mathbf{a})^n = z_{ij}\cdot h_{i2}(\mathbf{x}_j,\mathbf{a})\,.$$

We pick a finite extension L of K containing the coordinates of $\mathbf{a}$ and of the $\mathbf{x}_j$'s and z_{ij}'s. Then there is a finite set $\mathcal{S}\subseteq P_L$ such that if $\mathfrak{p}\in P_L\smallsetminus\mathcal{S}$, then the coordinates of the $\mathbf{x}_j$'s and z_{ij}'s are $\mathfrak{p}$-integral, i.e. in $\mathcal{O}_{L,\mathfrak{p}}$. Note that by multiplying (4) by $h_{i1}(\mathbf{x}_j,\mathbf{a})^{n'}$, we can enlarge n in (4) at will, changing the z_{ij}'s ($z_{ij}\to z_{ij}\cdot h_{i1}(\mathbf{x}_j,\mathbf{a})^{n'}$), but without changing the x_j's, L, or $\mathcal{S}$.

Let $\widetilde{\mathcal{S}}$ be the set of all prime ideals in $\tilde{P}$ which lie above the prime ideals in $\mathcal{S}$ and let $\mathcal{S}_0$ be a set of representatives of $\widetilde{\mathcal{S}}$ over L; that is, $\mathcal{S}_0$ contains, for each $\mathfrak{p}\in\mathcal{S}$, exactly one prime ideal $\mathfrak{P}\in\widetilde{\mathcal{S}}$ which lies over $\mathfrak{p}$. Then, for each $\mathfrak{P}'\in\widetilde{\mathcal{S}}$ there exist $\mathfrak{P}\in\mathcal{S}_0$ and $\sigma\in\mathrm{Aut}(\tilde{K}/L)$ such that $\mathfrak{P}'=\mathfrak{P}^\sigma$.

By (1) there are, for each $\mathfrak{P}\in\mathcal{S}_0$, points $\mathbf{x}_\mathfrak{P}\in\widetilde{\mathcal{O}}_\mathfrak{P}^m$ and $z_{i\mathfrak{P}}\in\widetilde{\mathcal{O}}_\mathfrak{P}$, $1\le i\le p$, such that, taking n in (4) large enough, we have:

$$(5)\quad \widetilde{\mathcal{O}}_\mathfrak{P}\models \mathbf{f}(\mathbf{x}_\mathfrak{P},\mathbf{a})=0\ \wedge\ g(\mathbf{x}_\mathfrak{P},\mathbf{a})\neq 0 \wedge \bigwedge_{1\le i\le p}\,(h_{i1}(\mathbf{x}_\mathfrak{P},\mathbf{a})^n = z_{i\mathfrak{P}}\cdot h_{i2}(\mathbf{x}_\mathfrak{P},\mathbf{a})\wedge h_{i2}(\mathbf{x}_\mathfrak{P},\mathbf{a})\neq 0)\,.$$

Hence, for each $\mathfrak{P}\in\widetilde{\mathcal{S}}$ there exist points $\mathbf{x}_\mathfrak{P}\in\widetilde{\mathcal{O}}_\mathfrak{P}^m$ and $z_{i\mathfrak{P}}\in\widetilde{\mathcal{O}}_\mathfrak{P}$, $1\le i\le p$, such that (5) holds.

We consider now the following system of equalities and inequalities in the variables $(X_1,\dots,X_m,Z_1,\dots,Z_p)$:

$$(6)\quad \mathbf{f}(\mathbf{X},\mathbf{a})=0\ \wedge\ g(\mathbf{X},\mathbf{a})\neq 0\wedge \bigwedge_{1\le i\le p}\,(h_{i1}(\mathbf{X},\mathbf{a})^n = Z_i\cdot h_{i2}(\mathbf{X},\mathbf{a})\wedge h_{i2}(\mathbf{X},\mathbf{a})\neq 0)\,.$$

Since the extra $\mathbf{Z}$-variables appear linearly and $h_{i2}(\mathbf{X},\mathbf{a})\neq 0$ for each i between 1 and p, the equations in (6) define an absolutely irreducible variety in $\mathbb{A}^{m+p}$ over M which is birational equivalent to $V_{\mathbf{f},\mathbf{a}}$, and (6) defines a nonempty Zariski-open subset of this variety. Moreover, by (3), (4) and (5), we have a solution to the system (6) in $\widetilde{\mathcal{O}}_\mathfrak{P}^{m+p}$ for each $\mathfrak{P}\in\tilde{P}$, and if $\mathfrak{P}=\mathfrak{P}_j$, $1\le j\le q$, then this solution $(\mathbf{x}_j,\mathbf{z}_j)$ can further be taken such that $k_j(\mathbf{x}_j,\mathbf{a})$ is not an invertible element of $\widetilde{\mathcal{O}}_\mathfrak{P}$.

It then follows from Theorem 1.9 that (6) has a solution $(\mathbf{x},\mathbf{z})\in\mathcal{O}_M^{m+p}$ such that $k_j(\mathbf{x},\mathbf{a})$ is not an invertible element of $\mathcal{O}_M$ for $j=1,\dots,q$. Also, for i between 1 and p, $h_{i1}(\mathbf{x},\mathbf{a})^n = z_i h_{i2}(\mathbf{x},\mathbf{a})$. Hence, it follows from Remark 2.3 that $h_{i1}(\mathbf{x},\mathbf{a})\in\mathrm{Rad}_{\mathcal{O}_M}(h_{i2}(\mathbf{x},\mathbf{a})\mathcal{O}_M)$. Thus, $\mathcal{O}_M\models\varphi(\mathbf{a})$, and we have established our claim.

Now, by Lemma 2.16, we can put condition (1) (after rewriting it in the language $\mathcal{L}(\mathcal{O})$) in quantifier-free form; that is, we can construct a quantifier-free formula $\widetilde{\varphi}(\mathbf{Y})$ in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$ such that for all $\mathbf{a}\in\mathcal{O}_M^n$ we have

$$(7)\qquad (\forall\mathfrak{P}\in\tilde{P})\,\widetilde{\mathcal{O}}_\mathfrak{P}\models\exists\mathbf{X}[\mathbf{f}(\mathbf{X},\mathbf{a})=0\wedge g(\mathbf{X},\mathbf{a})\neq 0\wedge\mathbf{R}(\mathbf{X},\mathbf{a})] \Leftrightarrow \mathcal{O}_M\models\widetilde{\varphi}(\mathbf{a})\,.$$

Similarly, we can construct a quantifier-free formula $\psi_j(\mathbf{Y})$, $j = 1, \dots, q$, in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$ such that for all $\mathbf{a} \in \mathcal{O}_M^n$ we have

$$(\forall \mathfrak{P} \in \tilde{P})\, \widetilde{\mathcal{O}}_{\mathfrak{P}} \models \neg\exists \mathbf{X}[\mathbf{f}(\mathbf{X}, \mathbf{a}) = 0 \wedge g(\mathbf{X}, \mathbf{a}) \neq 0 \wedge \mathbf{R}(\mathbf{X}, \mathbf{a}) \wedge \underline{\mathrm{NU}}(k_j(\mathbf{X}, \mathbf{a}))] \\ \Leftrightarrow \mathcal{O}_M \models \psi_j(\mathbf{a})\,,$$

and hence

(8)

$$(\exists \mathfrak{P} \in \tilde{P})\, \widetilde{\mathcal{O}}_{\mathfrak{P}} \models \exists \mathbf{X}[\mathbf{f}(\mathbf{X}, \mathbf{a}) = 0 \wedge g(\mathbf{X}, \mathbf{a}) \neq 0 \wedge \mathbf{R}(\mathbf{X}, \mathbf{a}) \wedge \underline{\mathrm{NU}}(k_j(\mathbf{X}, \mathbf{a}))] \\ \Leftrightarrow \mathcal{O}_M \models \neg\psi_j(\mathbf{a})\,.$$

Combining (7) and (8) with our established claim we see that for each $\mathbf{a} \in \mathcal{O}_M^n$ with absolutely irreducible $V_{\mathbf{f},\mathbf{a}}$ we have

$$\mathcal{O}_M \models \varphi(\mathbf{a}) \leftrightarrow \widetilde{\varphi}(\mathbf{a}) \wedge (\neg\psi_1(\mathbf{a}) \wedge \cdots \wedge \neg\psi_q(\mathbf{a}))\,.$$

□

Lemma 2.21. *Let $\varphi(\mathbf{Y})$, with $\mathbf{Y} = (Y_1, \dots, Y_n)$, be an existential formula in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$. Then there are special existential formulas $\varphi_1(\mathbf{Y}), \dots, \varphi_t(\mathbf{Y})$ such that for every algebraic extension M of K which satisfies that $\mathcal{O}_M$ is a Bezout domain we have*

$$\mathcal{O}_M \models \varphi(\mathbf{Y}) \leftrightarrow \varphi_1(\mathbf{Y}) \vee \cdots \vee \varphi_t(\mathbf{Y})\,.$$

Moreover, if $\varphi(\mathbf{Y})$ is presented, then we can effectively construct $\varphi_1(\mathbf{Y}), \dots, \varphi_t(\mathbf{Y})$.

Proof. We write $\varphi(\mathbf{Y})$ as $\exists \mathbf{X}\, \theta(\mathbf{X}, \mathbf{Y})$ with $\mathbf{X} = (X_1, \dots, X_m)$ and θ a quantifier-free formula in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$. If $\mathcal{O} = K$, then, by Remark 2.10 c), there exists a quantifier-free $\mathcal{L}(K)$-formula $\theta'(\mathbf{X}, \mathbf{Y})$ such that $M \models \theta \leftrightarrow \theta'$. Therefore $\varphi'(\mathbf{Y}) := \exists \mathbf{X} \theta'(\mathbf{X}, \mathbf{Y})$ is a special existential formula such that $M \models \varphi \leftrightarrow \varphi'$. So assume that $\mathcal{O} \neq K$. We put θ in disjunctive normal form. We first note that, by Notation 2.1 e),

(9) $$z = (x : y) \Leftrightarrow \exists a, b, c, d\, [a = bx + cy \wedge x = za \wedge y = da]\,.$$

It is clear that we can get rid of atoms $\mathrm{Rad}_{k,l}(\cdots)$ occurring (positively) in θ in favor of conditions $(\cdot\, \underline{\mathrm{R}}\, \cdot)$, extra equations, inequations, and extra existentially quantified variables. Here the idea is to use (9), Remark 2.6 a), and the following equivalence which holds in all Bezout domains with Jacobson radical zero:

$$x \in \mathrm{Rad}(y_1, \dots, y_l) \Leftrightarrow \exists a, b_1, \dots, b_l, c_1, \dots, c_l \\ [a = b_1 y_1 + \cdots + b_l y_l \wedge \bigwedge_{1 \leq i \leq l} ac_i = y_i \wedge ((a = 0 \wedge x = 0) \vee x \underline{\mathrm{R}} a)]\,.$$

Similarly, negations $\neg\mathrm{Rad}_{k,l}(\cdots)$ can be eliminated in favor of conditions $\underline{\mathrm{NU}}(\cdot\cdot)$: here the idea is to use (9), Remark 2.6 a), and the following equivalence (which follows from Remark 2.2 d)):

$$x \notin \mathrm{Rad}(y_1, \dots, y_l) \Leftrightarrow \exists z[1 \in (x, z) \wedge 1 \notin (y_1, \dots, y_l, z)] \\ \Leftrightarrow \exists z \exists a, b, c, d_1, \dots, d_l, e, f_1, \dots, f_l, g \\ [1 = ax + bz \wedge \underline{\mathrm{NU}}(c) \wedge c = d_1 y_1 + \cdots + d_l y_l + ez \wedge \bigwedge_{1 \leq i \leq l} cf_i = y_i \wedge cg = z]$$

(it is written in the last line that the greatest common divisor, c, of $y_1, \dots, y_l$ and z is not invertible).

After these operations we reduce, without loss, to the case that θ is a disjunction of conjunctions of formulas

$$f(\mathbf{X},\mathbf{Y})=0,\ g(\mathbf{X},\mathbf{Y})\neq 0,\ h_1(\mathbf{X},\mathbf{Y})\,\underline{\mathrm{R}}\,h_2(\mathbf{X},\mathbf{Y}),\text{ and }\underline{\mathrm{NU}}(k(\mathbf{X},\mathbf{Y})),$$

with f, g, h_1, h_2, k in $\mathcal{O}[\mathbf{X},\mathbf{Y}]$.

Now we distribute $\exists\mathbf{X}$ over the disjuncts and end up with a disjunction as desired. □

2.4. **Quantifier Elimination from Existential Formulas on Zariski-Open Sets.** This subsection is the link to the stratification procedure of Section 3. The connection is done through Proposition 2.26 in which we eliminate quantifiers from existential formulas in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$ on Zariski-open sets of K-varieties, modulo every ring of integers $\mathcal{O}_M$ of a perfect algebraic extension M of K which is PAC over $\mathcal{O}_M$. Lemma 2.21 allows us to reduce to elimination of quantifiers from special existential formulas. In order to be able to use Proposition 2.20, we show in Lemma 2.24 how to decompose an algebraic set, defined over a given integral domain R containing K, into absolutely irreducible varieties, uniformly for each homomorphism of R into $\tilde{K}$. To this end we first need an improved version of Bertini-Noether theorem.

Lemma 2.22. *Let R be an integral domain with quotient field F and let $f_1,\dots,f_k\in R[X_1,\dots,X_m]$. Suppose that the algebraic set $A=V(f_1,\dots,f_k)$ decomposes into a union of absolutely irreducible varieties defined over F by polynomials with coefficients in R. Let $A=V_1\cup\cdots\cup V_s$ be the decomposition of A into its absolutely irreducible components and suppose that $V_i=V(f_{i1},\dots,f_{i,\rho(i)})$, $i=1,\dots,s$, where $f_{ij}\in R[X_1,\dots,X_m]$.*

Then there exists a nonzero element $c\in R$ such that if $a\mapsto\bar{a}$ is a homomorphism of R into a field $\bar{F}$ with $\bar{c}\neq 0$, then $\bar{V}_i=V(\bar{f}_{i1},\dots,\bar{f}_{i,\rho(i)})$ is absolutely irreducible, $\dim(\bar{V}_i)=\dim(V_i)$, $i=1,\dots,s$, and $\bar{A}=V(\bar{f}_1,\dots,\bar{f}_r)=\bar{V}_1\cup\cdots\cup\bar{V}_s$ is the decomposition of $\bar{A}$ into its absolutely irreducible components.

Moreover, in the explicit case, i.e. when R is presented in F and F has elimination theory, we can effectively construct c.

Proof. Let $\widetilde{\Pi}(R)$ be the theory of algebraically closed fields containing a homomorphic image of R in the language $\mathcal{L}(R)$. It follows from Bertini-Noether theorem [FrJ08, p. 179, Prop. 10.4.2] that for each i between 1 and s there is $0\neq c_i\in R$, which can be effectively constructed in the explicit case [FrJ08, p. 179, the remark after Prop. 10.4.2], such that if $a\mapsto\bar{a}$ is a homomorphism of R into a field $\bar{F}$ with $\bar{c}_i\neq 0$, then $\bar{V}_i$ is absolutely irreducible and $\dim(\bar{V}_i)=\dim(V_i)$. Also, since $A=V_1\cup\cdots\cup V_s$ (resp., $V_i\not\subseteq V_j$ for each $i\neq j$) if and only if $A(E)=V_1(E)\cup\cdots\cup V_s(E)$ (resp., $V_i(E)\not\subseteq V_j(E)$ for each $i\neq j$) for every algebraically closed field E containing a homomorphic image of R, it follows that the statement "$A=V_1\cup\cdots\cup V_s$ and $V_i\not\subseteq V_j$ for each $i\neq j$" is equivalent modulo $\widetilde{\Pi}(R)$ to a sentence of $\mathcal{L}(R)$. Hence, by [FrJ08, p. 165, Thm. 9.2.1], there is $0\neq c_0\in R$, which can be effectively computed in the explicit case [FrJ08, p. 168, Thm. 9.3.1], such that if $a\mapsto\bar{a}$ is a homomorphism of R into a field $\bar{F}$ with $\bar{c}_0\neq 0$, then $\bar{A}=\bar{V}_1\cup\cdots\cup\bar{V}_s$ and $\bar{V}_i\not\subseteq\bar{V}_j$ for each $i\neq j$. Hence $c=c_0c_1\cdots c_s$ is the desired element. □

Definition 2.23. Let R be an integrally closed integral domain with quotient field E, let $\tilde{R}$ be the integral closure of R in $\tilde{E}$, and let E_{ins} be the maximal purely

inseparable extension of E inside $\tilde{E}$. Let A be an E-closed Zariski subset of $\mathbb{A}^m$ defined by polynomials with coefficients in $\tilde{R} \cap E_{\text{ins}}$.

a) A **system** $(P, q, A_L^* \ (E \subseteq L \subseteq P), x)$ for the pair (A, R) consists of:
   i. a finite Galois extension P of E,
   ii. a power q of $\text{char}(E)$ ($q = 1$ if $\text{char}(E) = 0$) such that A is defined by polynomials with coefficients in $R^{\frac{1}{q}}$,
   iii. for each subextension L of P/E, an L-closed subset, A_L^*, of A which is defined by polynomials with coefficients in $\tilde{R} \cap L^{\frac{1}{q}}$ and decompose into absolutely irreducible varieties defined over $L^{\frac{1}{q}}$ by polynomials with coefficients in $\tilde{R} \cap L^{\frac{1}{q}}$:
   $$A_L^* = V_{L,1} \cup \cdots \cup V_{L,s_L}\,, \quad \text{and}$$
   iv. $0 \neq x \in R$.

b) We say that the system $(P, q, A_L^* \ (E \subseteq L \subseteq P), x)$ is a **solution** for the pair (A, R) if for each $z \in \tilde{E}$ which satisfies that $Q = E(z)$ is a Galois extension of E containing P and for each $0 \neq x_z \in R$ satisfying that $R[x_z^{-1}, z]/R[x_z^{-1}]$ is a ring cover we have for $R' = R[(x_z x)^{-1}]$ and $S = R'[z]$:
   if M is a perfect field and φ_0 is a homomorphism of R' into M, then for each homomorphism φ of S into a Galois extension $N = M(\varphi(z))$ of M which extends φ_0 we have (here we define $\varphi(u^{\frac{1}{q}}) = \varphi(u)^{\frac{1}{q}}$ for each $u \in S$)
   (1) for each subextension L of P/E,
   $$\varphi(A_L^*) = \varphi(V_{L,1}) \cup \cdots \cup \varphi(V_{L,s_L})$$
   is a decomposition of $\varphi(A_L^*)$ into a union of absolutely irreducible varieties, and
   (2) $$\varphi_0(A)(M) = \varphi(A^*_{Q_0 \cap P})(M)\,,$$
   where Q_0 is the fixed field of $D_M(\varphi)_{,E}$ in Q.

Lemma 2.24. *(Uniform Decomposition-Intersection Procedure). Let R be an integrally closed integral domain with quotient field E and let $\tilde{R}$ be the integral closure of R in $\tilde{E}$. Let A be an E-closed Zariski subset of $\mathbb{A}^m$ defined by polynomials with coefficients in $\tilde{R} \cap E_{\text{ins}}$. Then there exists a system $(P, q, A_L^* \ (E \subseteq L \subseteq P), x)$ which is a solution to the pair (A, R) such that for any two subextensions L_1 and L_2 of P/E which are conjugate by an element of $\text{Gal}(P/E)$ there exists $\sigma \in \text{Gal}(P/E)$ which satisfies $L_2 = \sigma L_1$ and $A_{L_2}^* = \sigma(A_{L_1}^*)$.*

Moreover, in the explicit case (when R is presented in E and E has elimination theory), if A is presented, then we can effectively find P, q, and x and for each subextension L of P/E we can effectively construct A_L^* and decompose it into its absolutely irreducible components over $L^{\frac{1}{q}}$.

Proof. We shall prove by induction on the dimension of the algebraic set A that there exists a system $(P, q, A_L^* \ (E \subseteq L \subseteq P), x)$ which is a solution to the pair (A, R). Then we shall show that we can find such a system such that for any two subextensions L_1 and L_2 of P/E which are conjugate by an element of $\text{Gal}(P/E)$ there exists $\sigma \in \text{Gal}(P/E)$ which satisfies $L_2 = \sigma L_1$ and $A_{L_2}^* = \sigma(A_{L_1}^*)$.

PART A: *Begining of the induction.* We decompose A into its absolutely irreducible components, $A = \bigcup_{i \in I} V_i$, and then construct a finite Galois extension P_0 of E and a power q_0 of $\text{char}(E)$ ($q_0 = 1$ if $\text{char}(E) = 0$) such that A is defined over

$E^{\frac{1}{q_0}}$ and each V_i is defined over $P_0^{\frac{1}{q_0}}$. We multiply the polynomials which define the V_i's by a suitable nonzero element of R in order to assume that their coefficients belong to $\tilde{R} \cap P_0^{\frac{1}{q_0}}$.

Let $E_1, \ldots, E_n$ be the list of all subextensions of P_0/E. For each k between 1 and n, we identify $\mathrm{Gal}(P_0/E_k)$ with $\mathrm{Gal}(P_0^{\frac{1}{q_0}}/E_k^{\frac{1}{q_0}})$. Then $\mathrm{Gal}(P_0/E_k)$ permutes the V_i's. Consider a decomposition

$$\{V_i |\ i \in I\} = \bigcup_{j \in J_k} \{V_i |\ i \in I_{kj}\}$$

into $\mathrm{Gal}(P_0/E_k)$-orbits. For each $j \in J_k$, $U_{kj} = \bigcap_{i \in I_{kj}} V_i$ is invariant under $\mathrm{Gal}(P_0/E_k)$ and is therefore an E_k-closed subset of A. If I_{kj} consists of only one element i, then $U_{kj} = V_i$ is an absolutely irreducible variety which is defined over $E_k^{\frac{1}{q_0}}$. Otherwise, $\dim(V_i) = \dim(V_{i'})$ and $V_i \neq V_{i'}$ for distinct $i, i' \in I_{kj}$. Hence, $\dim(U_{kj}) < \dim(V_i) \leq \dim(A)$ [FrJ08, p. 174, Lemma 10.1.2], where $i \in I_{kj}$. Let

$$A_k = \bigcup_{\substack{j \in J_k \\ |I_{kj}|=1}} U_{kj} \qquad \text{and} \qquad B_k = \bigcup_{\substack{j \in J_k \\ |I_{kj}|>1}} U_{kj}\,.$$

Then A_k is a union of absolutely irreducible varieties which are defined over $E_k^{\frac{1}{q_0}}$ and $\dim(B_k) < \dim(A)$.

We find, by Lemma 2.22, $0 \neq c_0 \in \tilde{R} \cap P_0^{\frac{1}{q_0}}$ such that if $a \mapsto \bar{a}$ is a homomorphism of $\tilde{R} \cap P_0^{\frac{1}{q_0}}$ into a field M with $\bar{c}_0 \neq 0$, then $\overline{V_i}$ is absolutely irreducible, $\dim(\overline{V_i}) = \dim(V_i)$, for each $i \in I$, and $\bigcup_{i \in I} \overline{V_i}$ is the decomposition of $\bar{A}$ into its absolutely irreducible components. Also, we can choose c_0 such that for each k between 1 and n, $\overline{U_{kj}} = \bigcap_{i \in I_{kj}} \overline{V_i}$, for each $j \in J_k$, $\overline{A_k} = \bigcup_{\substack{j \in J_k \\ |I_{kj}|=1}} \overline{U_{kj}}$ and $\overline{B_k} = \bigcup_{\substack{j \in J_k \\ |I_{kj}|>1}} \overline{U_{kj}}$. Let $x_0 = N_{P_0/E}(c_0^{q_0})$. Then $x_0 \in R$.

Now, let $z \in \tilde{E}$ be such that $Q = E(z)$ is a Galois extension of E which contains P_0. Then, if L is a subextension of Q/E such that $L \cap P_0 = E_k$, then $\mathrm{Gal}(Q/L)$ permutes the V_i's in the same way as $\mathrm{Gal}(P_0/E_k)$. That is, the decomposition $\bigcup_{j \in J_k} \{V_i \mid i \in I_{kj}\}$ is also a decomposition of $\{V_i |\ i \in I\}$ into $\mathrm{Gal}(Q/L)$-orbits. Let x_z be a nonzero element in R which satisfies that $R[x_z^{-1}, z]/R[x_z^{-1}]$ is a ring cover and denote $R' = R[(x_z x_0)^{-1}]$ and $S = R'[z]$.

CLAIM: *Let M be a perfect field, let φ_0 be a homomorphism of R' into M, and let φ be a homomorphism of S into a Galois extension $N = M(\varphi(z))$ of M which extends φ_0. Then, for each subextension E_k of P_0/E,*

$$\varphi(A_k) = \bigcup_{\substack{j \in J_k \\ |I_{kj}|=1}} \varphi(U_{kj})$$

is the decomposition of $\varphi(A_k)$ into its absolutely irreducible components, and if the fixed field Q_0 of $D_M(\varphi)_{,E}$ in Q satisfies that $Q_0 \cap P_0 = E_k$, then $\varphi_0(A)(M) = \varphi(A_k)(M) \cup \varphi(B_k)(M)$.

Indeed, since $\varphi_0(x_0^{-1})$ is defined, it follows that $\varphi(c_0) \neq 0$ and therefore $\varphi(V_i)$ is absolutely irreducible and $\dim(\varphi(V_i)) = \dim(V_i)$, for each $i \in I$, and $\bigcup_{i\in I} \varphi(V_i)$ is the decomposition of $\varphi_0(A)$ into its absolutely irreducible components. Let $\overline{Q}$ be the quotient field of $\varphi(S)$. Consider the isomorphism

$$\varphi' : \mathrm{Gal}(Q/Q_0) = D_M(\varphi)_{,E} \to \mathrm{Gal}(\overline{Q}/\overline{Q} \cap M)$$

given by $\sigma \mapsto \overline{\sigma}$, where $\overline{\sigma}$ is defined by the formula $\overline{\sigma}(\varphi(u)) = \varphi(\sigma u)$ for each $u \in S$ (Remark 1.21 a)). Also, we identify $\mathrm{Gal}(\overline{Q}/\overline{Q}\cap M)$ with $\mathrm{Gal}(\overline{Q}^{\frac{1}{q_0}}/\overline{Q}^{\frac{1}{q_0}}\cap M)$. Then $\mathrm{Gal}(\overline{Q}/\overline{Q}\cap M)$ permutes the $\varphi(V_i)$'s and, since $\bigcup_{j\in J_k} \{V_i|\ i \in I_{kj}\}$ is a decomposition of $\{V_i|\ i \in I\}$ into $\mathrm{Gal}(Q/Q_0)$-orbits (because $E_k = Q_0 \cap P_0$), it follows that $\bigcup_{j\in J_k} \{\varphi(V_i)|\ i \in I_{kj}\}$ is a decomposition of $\{\varphi(V_i)|\ i \in I\}$ into $\mathrm{Gal}(\overline{Q}/\overline{Q}\cap M)$-orbits, because $\sigma V_i = V_j$ if and only if $\overline{\sigma}(\varphi(V_i)) = \varphi(V_j)$. Also, $\varphi(U_{kj}) = \bigcap_{i\in I_{kj}} \varphi(V_i)$, for each $j \in J_k$, $\varphi(A_k) = \bigcup_{\substack{j\in J_k \\ |I_{kj}|=1}} \varphi(U_{kj})$, and $\varphi(B_k) = \bigcup_{\substack{j\in J_k \\ |I_{kj}|>1}} \varphi(U_{kj})$. It suffices to show that $\varphi_0(A)(M) \subseteq \varphi(A_k)(M) \cup \varphi(B_k)(M)$. Let $\mathbf{y} \in \varphi(A)(M)$. Then, there exist $j \in J_k$ and $i \in I_{kj}$ such that $\mathbf{y} \in \varphi(V_i)(M)$. If $|I_{kj}| = 1$, then $\mathbf{y} \in \varphi(A_k)(M)$. Otherwise, we consider $i' \in I_{kj}$. By the above, there exists $\overline{\sigma} \in \mathrm{Gal}(\overline{Q}/\overline{Q} \cap M)$ such that $\varphi(V_{i'}) = \overline{\sigma}(\varphi(V_i))$. Since $\overline{Q}/\overline{Q}\cap M$ is a Galois extension, $\overline{\sigma}$ extends to an element of $\mathrm{Gal}(\overline{Q}M/M)$. Hence, $\mathbf{y} \in \varphi(V_{i'})(M)$ (because M is perfect). It follows that $\mathbf{y} \in \varphi(U_{kj})(M)$ and therefore $\mathbf{y} \in \varphi(B_k)(M)$, as was to be shown.

If B_k is an empty set for each k between 1 and n, then it follows from the claim that the system $(P_0, q_0, A_k\ (1 \leq k \leq n), x_0)$ is a solution for the pair (A, R).

PART B: *The induction's assumption.* If B_k is nonempty, we use induction on the dimension to obtain

- i k. a finite Galois extension P_k of E_k,
- ii k. a power q_k of $\mathrm{char}(E)$ such that B_k is defined by polynomials with coefficients in $\tilde{R} \cap E_k^{\frac{1}{q_k}}$,
- iii k. for each subextension F of P_k/E_k, an F-closed subset, $A_F^{(k)}$, of B_k which is defined by polynomials with coefficients in $\tilde{R} \cap F^{\frac{1}{q_k}}$ and decompose into a union of absolutely irreducible varieties defined over $F^{\frac{1}{q_k}}$ by polynomials with coefficients in $\tilde{R} \cap F^{\frac{1}{q_k}}$:

$$A_F^{(k)} = \bigcup_{i\in I_F^{(k)}} W_{F,i}^{(k)}, \quad \text{and}$$

- iv k. a nonzero element x_k in $R_k = \tilde{R} \cap E_k$,

such that the system $(P_k, q_k, A_F^{(k)}\ (E_k \subseteq F \subseteq P_k), x_k)$ is a solution for the pair (B_k, R_k):
For each $z \in \tilde{E}$ which satisfies that $E_k(z)$ is a Galois extension of E_k containing P_k and for each $0 \neq x_z \in R_k$ which satisfies that $R_k[x_z^{-1}, z]/R_k[x_z^{-1}]$ is a ring cover, we have, for $R_k' = R_k[(x_z x_k)^{-1}]$ and $S = R_k'[z]$, that

if M is a perfect field and φ_k is a homomorphism of R'_k into M, then for each homomorphism φ of S into a Galois extension $N = M(\varphi(z))$ of M which extends φ_k we have

$(1k)$ for each subextension F of P_k/E_k,

$$\varphi(A_F^{(k)}) = \bigcup_{i\in I_F^{(k)}} \varphi(W_{F,i}^{(k)})$$

is a decomposition of $\varphi(A_F^{(k)})$ into a union of absolutely irreducible varieties, and

$(2k)$ $$\varphi_k(B_k)(M) = \varphi(A^{(k)}_{Q_k\cap P_k})(M)\,,$$

where Q_k is the fixed field of $D_M(\varphi)_{,E_k}$ in $E_k(z)$.

PART C: *Conclusion of the induction.* If B_k is an empty set, we denote $P_k = P_0$, $q_k = q_0$, $x_k = 1$, and for each subextension F of P_k/E_k let $A_F^{(k)}$ be the empty set.

Let P be a finite Galois extension of E which contains $P_1\cdots P_n$, let $q = \max\limits_{0\le k\le n} q_k$, and let $x = N_{P/E}(x_0x_1\cdots x_n)$. Then A is defined by polynomials with coefficients in $R^{\frac{1}{q}}$ and $0\ne x\in R$. For a subextension L of P/E we denote

$$A_L^* = A_k \cup A_F^{(k)}\,,$$

where k is a positive integer between 1 and n such that $E_k = L\cap P_0$ and $F = L\cap P_k$. Then A_L^* is an L-closed subset of A which is defined by polynomials with coefficients in $\tilde{R}\cap L^{\frac{1}{q}}$ and decompose into a union of absolutely irreducible varieties defined over $L^{\frac{1}{q}}$ by polynomials with coefficients in $\tilde{R}\cap L^{\frac{1}{q}}$:

$$A_L^* = \bigcup_{\substack{j\in J_k\\ |I_{kj}|=1}} U_{kj} \cup \bigcup_{i\in I_F^{(k)}} W_{F,i}^{(k)} = V_{L,1}\cup\cdots\cup V_{L,s_L}\,.$$

Now, let $z\in\tilde{E}$ satisfies that $E(z)$ is a Galois extension of E containing P and let $0\ne x_z\in R$ be such that $R[x_z^{-1},z]/R[x_z^{-1}]$ is a ring cover. We denote $R' = R[(x_zx)^{-1}]$ and $S = R'[z]$. Let M be a perfect field, let φ_0 be a homomorphism of R' into M, and let φ be a homomorphism of S into a Galois extension $N = M(\varphi(z))$ of M which extends φ_0.

We denote $x_z^{(0)} = x_z\cdot\frac{x}{x_0}$. Then $0\ne x_z^{(0)}\in R$ (because $\frac{x}{x_0}$ is an element of E which is integral over R) satisfies that $R[(x_z^{(0)})^{-1},z]/R[(x_z^{(0)})^{-1}]$ is a ring cover and $R' = R[(x_z^{(0)}x_0)^{-1}]$. Let L be a subextension of P/E and let k be a positive integer between 1 and n such that $E_k = L\cap P_0$. It follows from the claim in Part A that $\varphi(A_k) = \bigcup\limits_{\substack{j\in J_k\\ |I_{kj}|=1}} \varphi(U_{kj})$ is the decomposition of $\varphi(A_k)$ into its absolutely irreducible components, and if the fixed field Q_0 of $D_M(\varphi)_{,E}$ in $E(z)$ satisfies $E_k = Q_0\cap P_0$, then $\varphi_0(A)(M) = \varphi(A_k)(M)\cup\varphi(B_k)(M)$.

Let $R_k = \tilde{R}\cap E_k$ and $R'_k = R_k[(x_zx)^{-1}]$. We denote $x_z^{(k)} = x_z\cdot\frac{x}{x_k}$. Then $0\ne x_z^{(k)}\in R_k$ (because $\frac{x}{x_k}$ is an element of E_k which is integral over R) satisfies that $R_k[(x_z^{(k)})^{-1},z]/R_k[(x_z^{(k)})^{-1}]$ is a ring cover. Also, $R'_k = R_k[(x_z^{(k)}x_k)^{-1}]$ and $S = R'_k[z]$ (because S is integral over R' and in particular contains R_k). We denote $F = L\cap P_k$. It follows by $(1k)$ that $\varphi(A_F^{(k)}) = \bigcup\limits_{i\in I_F^{(k)}} \varphi(W_{F,i}^{(k)})$ is a decomposition of

$\varphi(A_F^{(k)})$ into a union of absolutely irreducible varieties and hence

$$\begin{aligned}\varphi(A_L^*) = \varphi(A_k) \cup \varphi(A_F^{(k)}) = \bigcup_{\substack{j\in J_k \\ |I_{kj}|=1}} \varphi(U_{kj}) \cup \bigcup_{i\in I_F^{(k)}} \varphi(W_{F,i}^{(k)}) \\ = \varphi(V_{L,1}) \cup \cdots \cup \varphi(V_{L,s_L})\end{aligned}$$

is a decomposition of $\varphi(A_L^*)$ into a union of absolutely irreducible varieties.

Now, suppose that the fixed field Q_0 of $D_M(\varphi)_{,E}$ in $E(z)$ satisfies $E_k = Q_0 \cap P_0$ and $F = Q_0 \cap P_k$. Consider the isomorphism $\varphi^* : \mathrm{Gal}(N/M) \to D_M(\varphi)_{,E}$ which satisfies $\varphi(\varphi^*(\sigma)(u)) = \sigma(\varphi(u))$ for each $\sigma \in \mathrm{Gal}(N/M)$ and each $u \in S$ (Remark 1.21 a)). Then, for $u \in R'_k \subseteq Q_0$, we have $\varphi^*(\sigma)(u) = u$ (because $\varphi^*(\sigma) \in D_M(\varphi)_{,E}$) and hence $\varphi(u) = \sigma(\varphi(u))$, for each $\sigma \in \mathrm{Gal}(N/M)$. Thus $\varphi(R'_k) \subseteq M$. Let Q_k be the fixed field of $D_M(\varphi)_{,E_k}$ in $E(z) = E_k(z)$. Since $D_M(\varphi)_{,E_k}$ is a subgroup of $D_M(\varphi)_{,E}$ and φ^* is an isomorphism of $\mathrm{Gal}(N/M)$ on $D_M(\varphi)_{,E}$ and also on $D_M(\varphi)_{,E_k}$, it follows that $D_M(\varphi)_{,E_k} = D_M(\varphi)_{,E}$. Hence $Q_k = Q_0$. Therefore $Q_k \cap P_k = Q_0 \cap P_k = F$. It follows by (2$k$) that

$$\varphi(B_k)(M) = \varphi(A^{(k)}_{Q_k\cap P_k})(M) = \varphi(A_F^{(k)})(M)\,.$$

In addition, $Q_0 \cap P$ satisfies $(Q_0 \cap P) \cap P_0 = E_k$ and $(Q_0 \cap P) \cap P_k = F$. Hence

$$\begin{aligned}\varphi_0(A)(M) &= \varphi(A_k)(M) \cup \varphi(B_k)(M) \\ &= \varphi(A_k)(M) \cup \varphi(A_F^{(k)})(M) = \varphi(A^*_{Q_0\cap P})(M)\,,\end{aligned}$$

as required.

PART D: *Construction of the system such that $\sigma A_L^* = A^*_{\sigma L}$ for each subextension L of P/E and each $\sigma \in \mathrm{Gal}(P/E)$.* We identify $\mathrm{Gal}(P/E)$ with $\mathrm{Gal}(P^{\frac{1}{q}}/E^{\frac{1}{q}})$. Let L be a subextension of P/E and let $\sigma \in \mathrm{Gal}(P/E)$. Then $A^{(\sigma)}_{\sigma L} := \sigma A_L^*$ is a σL-closed subset of A which is defined by polynomials with coefficients in $\tilde{R} \cap \sigma L^{\frac{1}{q}}$ and decompose into a union of absolutely irreducible varieties defined over $\sigma L^{\frac{1}{q}}$ by polynomials with coefficients in $\tilde{R} \cap \sigma L^{\frac{1}{q}}$:

$$A^{(\sigma)}_{\sigma L} = \bigcup_{i=1}^{s_L} V^{(\sigma)}_{\sigma L,i}\,,$$

where $V^{(\sigma)}_{\sigma L,i} := \sigma V_{L,i}$, $1 \le i \le s_L$.

Let z' be an element in $\tilde{E}$ which satisfies that $Q = E(z')$ is a Galois extension of E containing P and let $x_{z'}$ be a nonzero element in R which satisfies that $R[x_{z'}^{-1}, z']/R[x_{z'}^{-1}]$ is a ring cover. We denote $R' = R[(x_{z'}x)^{-1}]$ and $S' = R'[z']$. Let M be a perfect field, let φ_0 be a homomorphism of R' into M, and let φ' be a homomorphism of S' into a Galois extension $N = M(\varphi'(z'))$ of M which extends φ_0.

We extend σ to an element of $\mathrm{Gal}(Q/E)$. We denote $z = \sigma^{-1}z'$, $x_z = x_{z'}$, $S = \sigma^{-1}S' = R'[z]$, and let φ be a homomorphism of S into $N = M(\varphi(z))$ which is defined by $\varphi(u) = \varphi'(\sigma u)$ for each $u \in S$. Then φ extends φ_0 and $R[x_z^{-1}, z]/R[x_z^{-1}]$ is a ring cover.

In these notations, it follows from (1) that

$$\varphi'(A^{(\sigma)}_{\sigma L}) = \varphi'(\sigma A^*_L) = \varphi(A^*_L) = \bigcup_{i=1}^{s_L} \varphi(V_{L,i}) = \bigcup_{i=1}^{s_L} \varphi'(\sigma V_{L,i}) = \bigcup_{i=1}^{s_L} \varphi'(V^{(\sigma)}_{\sigma L,i})$$

is the decomposition of $\varphi'(A^{(\sigma)}_{\sigma L})$ into a union of absolutely irreducible varieties.

Also, by (2),

$$\varphi_0(A)(M) = \varphi(A^*_{Q_0\cap P})(M) = \varphi'(\sigma A^*_{Q_0\cap P})(M) = \varphi'(A^{(\sigma)}_{\sigma(Q_0\cap P)})(M) = \varphi'(A^{(\sigma)}_{Q'_0\cap P})(M)\,,$$

where Q_0 is the fixed field of $D_M(\varphi)_{,E}$ in Q and $Q'_0 = \sigma Q_0$ is the fixed field of $D_M(\varphi')_{,E} = \sigma D_M(\varphi)_{,E}\sigma^{-1}$ in Q.

Now, for each conjugacy class $\mathcal{C}$ of $\mathrm{Gal}(P/E)$, we choose a subextension L of P/E such that $\mathrm{Gal}(P/L) \in \mathcal{C}$. Let $G = \mathrm{Gal}(P/L)$ and $H = \{\sigma \in G \,|\, \sigma L = L\}$. Then $H < G$. Suppose that $[G : H] = r$ and let $\sigma_1 = 1, \sigma_2, \ldots, \sigma_r$ be a system of left coset representatives of G modulo H. We replace, for each i between 2 and r, $A^*_{\sigma_i L}$ by $A^{(\sigma_i)}_{\sigma_i L} = \sigma_i A^*_L$. In this way we get that the new obtained system $(P, q, A^*_L\,(E \subseteq L \subseteq P), x)$ is a solution for the pair (A, R) such that for any two subextensions L_1 and L_2 of P/E which are conjugate by an element of $\mathrm{Gal}(P/E)$ there exists $\sigma \in \mathrm{Gal}(P/E)$ which satisfies $L_2 = \sigma L_1$ and $A^*_{L_2} = \sigma A^*_{L_1}$.

Finally, if E has elimination theory, then Chapter 19 of [FrJ08] shows how to make all the above constructions effective. □

Definition 2.25. Let q be a power of $\mathrm{char}(K)$ ($q = 1$ if $\mathrm{char}(K) = 0$) and let $\psi(Y_1, \ldots, Y_n)$ be a quantifier-free formula in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}^{\frac{1}{q}})$. We define the formula $\psi^q(\mathbf{Y})$ in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$ by an induction on the structure of $\psi(\mathbf{Y})$:

a) if $\psi(\mathbf{Y})$ is the formula $\mathrm{Rad}_{k,l}(\mathbf{a}(\mathbf{Y}), \mathbf{b}(\mathbf{Y}), \mathbf{c}(\mathbf{Y}), \mathbf{d}(\mathbf{Y}))$, where $\mathbf{a}, \mathbf{b} \in \mathcal{O}^{\frac{1}{q}}[\mathbf{Y}]^k$ and $\mathbf{c}, \mathbf{d} \in \mathcal{O}^{\frac{1}{q}}[\mathbf{Y}]^l$, then $\psi^q(\mathbf{Y})$ is the formula

$$\mathrm{Rad}_{k,l}(\mathbf{a}^q(\mathbf{Y}), \mathbf{b}^q(\mathbf{Y}), \mathbf{c}^q(\mathbf{Y}), \mathbf{d}^q(\mathbf{Y}))\,;$$

b) if $\psi(\mathbf{Y})$ is the disjunction $\psi_1(\mathbf{Y}) \vee \psi_2(\mathbf{Y})$ and $\psi^q_1(\mathbf{Y})$, $\psi^q_2(\mathbf{Y})$ were already defined, then $\psi^q(\mathbf{Y})$ is the disjunction $\psi^q_1(\mathbf{Y}) \vee \psi^q_2(\mathbf{Y})$;

c) if $\psi(\mathbf{Y})$ is the negation $\neg\varphi(\mathbf{Y})$ and $\varphi^q(\mathbf{Y})$ was already defined, then $\psi^q(\mathbf{Y})$ is the negation $\neg\varphi^q(\mathbf{Y})$.

For every perfect algebraic extension M of K and each $\mathbf{a} \in \mathcal{O}^n_M$ we have

$$\mathcal{O}_M \models \psi(\mathbf{a}^{\frac{1}{q}}) \Leftrightarrow \mathcal{O}_M \models \psi^q(\mathbf{a})\,.$$

Proposition 2.26. *Let $\psi(\mathbf{Y})$, $\mathbf{Y} = (Y_1, \ldots, Y_n)$, be an existential formula in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$ and let $V \subseteq \mathbb{A}^n$ be a K-variety with a generic point $\mathbf{y}$.*

Then, there exist a finite Galois extension P of $K(\mathbf{y})$ and a polynomial $h_\psi \in \mathcal{O}[\mathbf{Y}]$ which does not vanish on V such that the pair (ψ, V) is **solvable** *by the pair (P, h_ψ):*
Let Q be a finite Galois extension of $K(\mathbf{y})$ which contains P and let D_0/B_0 be a Galois ring/set cover such that $B_0 = V \setminus V(h_0)$, where $h_0 \in \mathcal{O}[\mathbf{Y}]$ is a polynomial which does not vanish on V and $K(D_0) = Q$. Let $\mathcal{C}$ be a conjugacy class of $\mathrm{Gal}(Q/K(\mathbf{y}))$ and let L be the fixed field in Q of one of the groups in $\mathcal{C}$. Let z_L be a primitive element for the extension $L/K(\mathbf{y})$ which is integral over $\mathcal{O}[\mathbf{y}]$,

let $p_{\mathcal{C}} \in \mathcal{O}[\mathbf{Y}, Z]$ be a polynomial which satisfies that $p_{\mathcal{C}}(\mathbf{y}, Z)$ is a multiple of $\mathrm{irr}(z_L, K(\mathbf{y}))$ by an invertible element of $K[B_0] = K[\mathbf{y}, h_0(\mathbf{y})^{-1}]$, and suppose that the discriminant of z_L over $K(\mathbf{y})$ is invertible in $K[B_0]$. Then there exists a quantifier-free formula $\overline{\psi}_{\mathcal{C}}(\mathbf{Y}, Z)$ in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$, such that if $h \in \mathcal{O}[\mathbf{Y}]$ is a common multiple of h_0 and h_ψ then, for $B = V \setminus V(h)$ and $D = D_0[h(\mathbf{y})^{-1}]$, the pair $(p_{\mathcal{C}}, \overline{\psi}_{\mathcal{C}})$ is a **solution** *for the triple $(\psi, D/B, \mathcal{C})$:*
For every perfect algebraic extension M of K which is PAC over $\mathcal{O}_M$ and for each $\mathbf{b} \in B(\mathcal{O}_M)$ which satisfies $\mathrm{Ar}(D/B, M, \mathbf{b}) = \mathcal{C}$ we have

$$\begin{aligned}\mathcal{O}_M \models \psi(\mathbf{b}) &\Leftrightarrow \mathcal{O}_M \models \exists Z[p_{\mathcal{C}}(\mathbf{b}, Z) = 0 \wedge \overline{\psi}_{\mathcal{C}}(\mathbf{b}, Z)] \\ &\Leftrightarrow \mathcal{O}_M \models \forall Z[p_{\mathcal{C}}(\mathbf{b}, Z) = 0 \to \overline{\psi}_{\mathcal{C}}(\mathbf{b}, Z)]\,.\end{aligned}$$

Moreover, in the explicit case, if ψ and V are presented, then we can effectively construct P and h_ψ and if also $\mathcal{C}$ is presented (by $p_{\mathcal{C}}$), then we can effectively construct $h_{\mathcal{C}}$ and $\overline{\psi}_{\mathcal{C}}$.

Proof. CASE I: *$\psi(\mathbf{Y})$ is a special existential formula.*

$$\psi(\mathbf{Y}) : \exists \mathbf{X}[\mathbf{f}(\mathbf{X}, \mathbf{Y}) = 0 \wedge T(\mathbf{X}, \mathbf{Y})]$$

where $\mathbf{X} = (X_1, \ldots, X_m)$, $\mathbf{f}(\mathbf{X}, \mathbf{Y}) = (f_1(\mathbf{X}, \mathbf{Y}), \ldots, f_k(\mathbf{X}, \mathbf{Y}))$ with $f_1, \ldots, f_k \in \mathcal{O}[\mathbf{X}, \mathbf{Y}]$, and $T(\mathbf{X}, \mathbf{Y})$ is

$$g(\mathbf{X}, \mathbf{Y}) \neq 0 \wedge \bigwedge_{i \in I} (h_{i1}(\mathbf{X}, \mathbf{Y}) \ \underline{\mathrm{R}} \ h_{i2}(\mathbf{X}, \mathbf{Y})) \wedge \bigwedge_{j \in J} \underline{\mathrm{NU}}(k_j(\mathbf{X}, \mathbf{Y}))$$

with h_{i1}, h_{i2}, g $(i \in I)$, k_j $(j \in J)$ polynomials in $\mathcal{O}[\mathbf{X}, \mathbf{Y}]$. Let

$$A = \{\mathbf{x} \in \mathbb{A}^m |\ \mathbf{f}(\mathbf{x}, \mathbf{y}) = 0\}\,.$$

Then A is a $K(\mathbf{y})$-closed Zariski subset of $\mathbb{A}^m$ which is defined by polynomials with coefficients in $\mathcal{O}[\mathbf{y}]$.

STEP A: *Finding P and h_ψ.* We denote $R_0 = K[\mathbf{y}]$ and $E = K(\mathbf{y})$. We find, by Remark 1.16, $0 \neq x_0 \in R_0$ such that $R = R_0[x_0^{-1}]$ is integrally closed and we denote the integral closure of R in $\tilde{E}$ by $\tilde{R}$. Then Lemma 2.24 gives, effectively in the explicit case,

i. a finite Galois extension P of E,
ii. a power q of $\mathrm{char}(E)$,
iii. for each subextension L of P/E, an L-closed subset, A_L^*, of A which is defined by polynomials with coefficients in $\tilde{R} \cap L^{\frac{1}{q}}$ and decompose into a union of absolutely irreducible varieties defined over $L^{\frac{1}{q}}$ by polynomials with coefficients in $\tilde{R} \cap L^{\frac{1}{q}}$ such that
   (3) for any two subextensions L_1 and L_2 of P/E which are conjugate by an element of $\mathrm{Gal}(P/E)$ there exists $\sigma \in \mathrm{Gal}(P/E)$ which satisfies $L_2 = \sigma L_1$ and $A_{L_2}^* = \sigma A_{L_1}^*$, and
iv. $0 \neq x \in R$,

such that the system $(P, q, A_L^*\ (E \subseteq L \subseteq P), x)$ is a solution for the pair (A, R).

We find a non-negative integer r such that $x_0^r x \in R_0 = K[\mathbf{y}]$ and then we find $0 \neq a_0 \in \mathcal{O}$ such that $x' = a_0 x_0^{r+1} x \in \mathcal{O}[\mathbf{y}]$. Then $x' \neq 0$ and it satisfies that $R_0[(x')^{-1}] = R_0[x_0^{-1}][x^{-1}] = R[x^{-1}]$. We find a polynomial $0 \neq h_\psi \in \mathcal{O}[\mathbf{Y}]$ such that $h_\psi(\mathbf{y}) = x'$. In particular, h_ψ does not vanish on V and $R[x^{-1}] = K[\mathbf{y}, h_\psi(\mathbf{y})^{-1}]$.

Now, let Q be a finite Galois extension of $K(\mathbf{y})$ which contains P and let D_0/B_0 be a Galois ring/set cover such that $B_0 = V \setminus V(h_0)$, where $h_0 \in \mathcal{O}[\mathbf{Y}]$ is a polynomial which does not vanish on V and $K(D_0) = Q$. Let $\mathcal{C}$ be a conjugacy domain of $\mathrm{Gal}(Q/K(\mathbf{y}))$ and let L be the fixed field in Q of one of the groups in $\mathcal{C}$. Let z_L be a primitive element for the extension $L/K(\mathbf{y})$ which is integral over $\mathcal{O}[\mathbf{y}]$, let $p_{\mathcal{C}} \in \mathcal{O}[\mathbf{Y}, Z]$ be a polynomial which satisfies that $p_{\mathcal{C}}(\mathbf{y}, Z)$ is a multiple of $\mathrm{irr}(z_L, K(\mathbf{y}))$ by an invertible element of $K[B_0]$, and suppose that the discriminant of z_L over $K(\mathbf{y})$ is invertible in $K[B_0]$.

STEP B: *Finding* $\overline{\psi}_{\mathcal{C}}$. The algebraic set $A^*_{L\cap P}$ decompose into a union of absolutely irreducible varieties which are defined over $(L \cap P)^{\frac{1}{q}}$ (and hence over $L^{\frac{1}{q}}$):

$$A^*_{L\cap P} = V_1 \cup \cdots \cup V_s\,.$$

Suppose that

$$V_i = \{\mathbf{x} \in \mathbb{A}^m | \, \mathbf{f}_i(\mathbf{x}, \mathbf{y}^{\frac{1}{q}}, z_L^{\frac{1}{q}}) = 0\}\,, \quad i = 1, \ldots, s\,,$$

where $\mathbf{f}_i(\mathbf{X}, \mathbf{Y}', Z') = (f_{i1}(\mathbf{X}, \mathbf{Y}', Z'), \ldots, f_{i,\rho(i)}(\mathbf{X}, \mathbf{Y}', Z'))$ with

$$f_{ij} \in \mathcal{O}^{\frac{1}{q}}[\mathbf{X}, \mathbf{Y}', Z'], \quad j = 1, \ldots, \rho(i),\ i = 1, \ldots, s\,.$$

For each i between 1 and s, let $\psi_i'(\mathbf{Y}', Z')$ be the following special existential formula in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}^{\frac{1}{q}})$:

$$\exists \mathbf{X}[\mathbf{f}_i(\mathbf{X}, \mathbf{Y}', Z') = 0 \wedge T(\mathbf{X}, \mathbf{Y}'^q)]\,.$$

It follows from Proposition 2.20, with $\mathbf{Y}$ replaced by $(\mathbf{Y}', Z')$, that there exists, for each i between 1 and s, a quantifier-free formula $\overline{\psi_i'}(\mathbf{Y}', Z')$ in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}^{\frac{1}{q}})$, which can be effectively constructed in the explicit case, such that for every perfect algebraic extension M of K which is PAC over $\mathcal{O}_M$ and for each $(\mathbf{b}, c) \in \mathcal{O}_M^{n+1}$ which satisfies that

$$V_{i,(\mathbf{b},c)} = \{\mathbf{x} \in \mathbb{A}^m | \ \mathbf{f}_i(\mathbf{x}, \mathbf{b}^{\frac{1}{q}}, c^{\frac{1}{q}}) = 0\}$$

is an absolutely irreducible variety, we have

$$\mathcal{O}_M \models \exists \mathbf{X}[\mathbf{f}_i(\mathbf{X}, \mathbf{b}^{\frac{1}{q}}, c^{\frac{1}{q}}) = 0 \wedge T(\mathbf{X}, \mathbf{b})] \leftrightarrow \overline{\psi_i'}(\mathbf{b}^{\frac{1}{q}}, c^{\frac{1}{q}})\,.$$

For each i between 1 and s, let $\overline{\psi}_i(\mathbf{Y}, Z)$ be the quantifier-free formula $\overline{\psi_i'}^q(\mathbf{Y}, Z)$ in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$. We denote

$$\overline{\psi}_{\mathcal{C}}(\mathbf{Y}, Z) := \overline{\psi}_1(\mathbf{Y}, Z) \vee \cdots \vee \overline{\psi}_s(\mathbf{Y}, Z)\,.$$

Note that $\overline{\psi}_{\mathcal{C}}$ depends indeed only on $\mathcal{C}$, by $p_{\mathcal{C}}$, and not on L, because if L' is another fixed field of one of the groups in $\mathcal{C}$, then there exists $\tau \in \mathrm{Gal}(Q/E)$ such that $L' = \tau L$. In particular, $L \cap P$ and $L' \cap P$ are conjugate by $\mathrm{res}_P(\tau) \in \mathrm{Gal}(P/E)$. Hence, it follows from (3) that there exists $\sigma \in \mathrm{Gal}(P/E)$ such that $L' \cap P = \sigma(L \cap P)$ and $A^*_{L'\cap P} = \sigma A^*_{L\cap P}$. Extend σ to an element of $\mathrm{Gal}(Q/E)$. Then

$$A^*_{L'\cap P} = \sigma V_1 \cup \cdots \cup \sigma V_s = \bigcup_{i=1}^{s} \{\mathbf{x} \in \mathbb{A}^m | \ \mathbf{f}_i(\mathbf{x}, \mathbf{y}^{\frac{1}{q}}, \sigma z_L^{\frac{1}{q}}) = 0\}\,.$$

Hence, the formula $\psi_i'(\mathbf{Y}', Z') : \exists \mathbf{X}[\mathbf{f}_i(\mathbf{X}, \mathbf{Y}', Z') = 0 \wedge T(\mathbf{X}, \mathbf{Y}'^q)]$ depends only on the choice of the polynomial $p_{\mathcal{C}}(\mathbf{y}, Z)$, $i = 1, \ldots, s$, and therefore $\overline{\psi}_{\mathcal{C}}$ does not depend on L.

Let $h \in \mathcal{O}[\mathbf{Y}]$ be a common multiple of h_0 and h_ψ and let $B = V \setminus V(h)$ and $D = D_0[h(\mathbf{y})^{-1}]$.

STEP C: *The pair* $(p_{\mathcal{C}}, \overline{\psi}_{\mathcal{C}})$ *is a solution for the triple* $(\psi, D/B, \mathcal{C})$. Let M be a perfect algebraic extension of K which is PAC over $\mathcal{O}_M$ and let $\mathbf{b}$ be an element in $B(\mathcal{O}_M)$ which satisfies $\mathrm{Ar}(D/B, M, \mathbf{b}) = \mathcal{C}$. We denote $R' = K[B] = K[\mathbf{y}, h(\mathbf{y})^{-1}]$ and let φ_0 be the K-homomorphism of R' into M which is defined by the specialization $\mathbf{y} \mapsto \mathbf{b}$. Then $\varphi_0(A) = \{\mathbf{x} \in \mathbb{A}^m |\ \mathbf{f}(\mathbf{x}, \mathbf{b}) = 0\}$. Let φ be a K-homomorphism of D into a Galois extension $N = M(\varphi(D))$ of M which extends φ_0 such that L is the fixed field, E_φ, of $D_M(\varphi)_{,E}$ in Q. Consider the isomorphism $\varphi^* : \mathrm{Gal}(N/M) \to D_M(\varphi)_{,E}$ which satisfies $\varphi(\varphi^*(\sigma)(u)) = \sigma(\varphi(u))$, for each $\sigma \in \mathrm{Gal}(N/M)$ and each $u \in D$ (Remark 1.21 a)). Then, for each $u \in D \cap L$, we have $\varphi^*(\sigma)(u) = u$ (because $\varphi^*(\sigma) \in D_M(\varphi)_{,E}$) and hence $\varphi(u) = \sigma(\varphi(u))$ for each $\sigma \in \mathrm{Gal}(N/M)$. Thus, $\varphi(D \cap L) \subseteq M$. In particular, $c = \varphi(z_L) \in M$. Also, c is integral over $\mathcal{O}[\mathbf{b}]$ (because z_L is integral over $\mathcal{O}[\mathbf{y}]$) and hence $c \in \mathcal{O}_M$. It follows from Lemma 2.24, for $S = D$, that

$$\varphi(A^*_{L\cap P}) = \varphi(V_1) \cup \cdots \cup \varphi(V_s)$$

is a decomposition of $\varphi(A^*_{L\cap P})$ into a union of absolutely irreducible varieties, and

$$\varphi_0(A)(M) = \varphi(A^*_{L\cap P})(M) = \varphi(V_1)(M) \cup \cdots \cup \varphi(V_s)(M)\,.$$

Thus, $V_{i,(\mathbf{b},c)} = \varphi(V_i)$ is an absolutely irreducible variety, for each i between 1 and s, and

$$\{\mathbf{x} \in \mathcal{O}_M^m |\ \mathbf{f}(\mathbf{x}, \mathbf{b}) = 0\} = \bigcup_{i=1}^{s} \{\mathbf{x} \in \mathcal{O}_M^m |\ \mathbf{f}_i(\mathbf{x}, \mathbf{b}^{\frac{1}{q}}, c^{\frac{1}{q}}) = 0\}\,.$$

Hence

$$\begin{aligned}
\mathcal{O}_M \models \psi(\mathbf{b}) &\Leftrightarrow \mathcal{O}_M \models \exists \mathbf{X}[\mathbf{f}(\mathbf{X}, \mathbf{b}) = 0 \wedge T(\mathbf{X}, \mathbf{b})] \\
&\Leftrightarrow \mathcal{O}_M \models \exists \mathbf{X}[\bigvee_{i=1}^{s} \mathbf{f}_i(\mathbf{X}, \mathbf{b}^{\frac{1}{q}}, c^{\frac{1}{q}}) = 0 \wedge T(\mathbf{X}, \mathbf{b})] \\
&\Leftrightarrow \mathcal{O}_M \models \bigvee_{i=1}^{s} \exists \mathbf{X}[\mathbf{f}_i(\mathbf{X}, \mathbf{b}^{\frac{1}{q}}, c^{\frac{1}{q}}) = 0 \wedge T(\mathbf{X}, \mathbf{b})] \\
&\Leftrightarrow \mathcal{O}_M \models \bigvee_{i=1}^{s} \overline{\psi_i'}(\mathbf{b}^{\frac{1}{q}}, c^{\frac{1}{q}}) \Leftrightarrow \mathcal{O}_M \models \bigvee_{i=1}^{s} \overline{\psi}_i(\mathbf{b}, c) \\
&\Leftrightarrow \mathcal{O}_M \models \overline{\psi}_{\mathcal{C}}(\mathbf{b}, c)\,.
\end{aligned}$$

That is,

$$\mathcal{O}_M \models \psi(\mathbf{b}) \Leftrightarrow \mathcal{O}_M \models \exists Z[p_{\mathcal{C}}(\mathbf{b}, Z) = 0 \wedge \overline{\psi}_{\mathcal{C}}(\mathbf{b}, Z)]\,.$$

It is left to show that $\mathcal{O}_M \models \psi(\mathbf{b}) \Leftrightarrow \mathcal{O}_M \models \forall Z[p_{\mathcal{C}}(\mathbf{b}, Z) = 0 \to \overline{\psi}_{\mathcal{C}}(\mathbf{b}, Z)]$. To this end, let $d = \deg_Z p_{\mathcal{C}}$ and let $c_1, \ldots, c_d \in \widetilde{\mathcal{O}}$ be the roots of the polynomial $p_{\mathcal{C}}(\mathbf{b}, Z)$. Since the discriminant of z_L over $K(\mathbf{y})$ is invertible in $K[B]$, it follows that

$$\prod_{i\neq j}(c_i - c_j) = \mathrm{Disc}(\varphi_0(\mathrm{irr}(z_L, K(\mathbf{y})))) = \varphi_0(\mathrm{Disc}(\mathrm{irr}(z_L, K(\mathbf{y})))) \neq 0$$

and hence $c_i \neq c_j$ for $i \neq j$. Now, let i be a positive integer between 1 and d such that $c_i \in \mathcal{O}_M$ and extend the specialization $(\mathbf{y}, z_L) \mapsto (\mathbf{b}, c_i)$ to a K-homomorphism, φ_i, of D. Then, for each $\sigma \in D_M(\varphi_i)_{,E}$ we have $\varphi_i(\sigma z_L) = \varphi_i(z_L)$ (because $\varphi_i(z_L) = c_i \in M$) and hence $\sigma z_L = z_L$ (because z_L and σz_L are different roots of the polynomial $p_{\mathcal{C}}(\mathbf{y}, Z)$ if and only if $\varphi_i(z_L)$ and $\varphi_i(\sigma z_L)$ are different

roots of the polynomial $p_{\mathcal{C}}(\mathbf{b}, Z)$). Therefore $z_L \in E_{\varphi_i}$ (and hence $L \subseteq E_{\varphi_i}$), where E_{φ_i} is the fixed field of $D_M(\varphi_i)_{,E}$ in Q. But, there exists $\tau \in \mathrm{Gal}(Q/E)$ such that $\tau L = E_{\varphi_i}$; hence $L = E_{\varphi_i}$. Therefore, returning on the argument of the previous pharagraph for φ_i instead of φ, we get

$$\mathcal{O}_M \models \psi(\mathbf{b}) \Leftrightarrow \mathcal{O}_M \models \overline{\psi}_{\mathcal{C}}(\mathbf{b}, c_i)\,.$$

Thus

$$\mathcal{O}_M \models \psi(\mathbf{b}) \Leftrightarrow \mathcal{O}_M \models \forall Z[p_{\mathcal{C}}(\mathbf{b}, Z) = 0 \to \overline{\psi}_{\mathcal{C}}(\mathbf{b}, Z)]\,.$$

CASE II: *The general case.* By Theorem 1.12 and Lemma 2.21 we can find, effectively if $\psi(\mathbf{Y})$ is presented, special existential formulas

$$\psi_1(\mathbf{Y}), \ldots, \psi_t(\mathbf{Y})$$

such that for every perfect algebraic extension M of K which is PAC over $\mathcal{O}_M$ we have

$$\mathcal{O}_M \models \psi(\mathbf{Y}) \leftrightarrow \psi_1(\mathbf{Y}) \vee \cdots \vee \psi_t(\mathbf{Y})\,. \tag{4}$$

By case I, we find, for each i between 1 and t, a finite Galois extension P_i of $K(\mathbf{y})$ and a polynomial $h_{\psi_i} \in \mathcal{O}[\mathbf{Y}]$ which does not vanish on V such that the pair (ψ_i, V) is solvable by the pair (P_i, h_{ψ_i}). We denote $P = P_1 \cdots P_t$ and $h_\psi = h_{\psi_1} \cdots h_{\psi_t}$.

Let Q be a finite Galois extension of $K(\mathbf{y})$ which contains P and let D_0/B_0 be a Galois ring/set cover such that $B_0 = V \setminus V(h_0)$, where $h_0 \in \mathcal{O}[\mathbf{Y}]$ is a polynomial which does not vanish on V and $K(D_0) = Q$. Let $\mathcal{C}$ be a conjugacy class of $\mathrm{Gal}(Q/K(\mathbf{y}))$ and let L be the fixed field in Q of one of the fields in $\mathcal{C}$. Let z_L be a primitive element for the extension $L/K(\mathbf{y})$ which is integral over $\mathcal{O}[\mathbf{y}]$, let $p_{\mathcal{C}} \in \mathcal{O}[\mathbf{Y}, Z]$ be a polynomial which satisfies that $p_{\mathcal{C}}(\mathbf{y}, Z)$ is a multiple of $\mathrm{irr}(z_L, K(\mathbf{y}))$ by an invertible element of $K[B_0]$, and suppose that the discriminant of z_L over $K(\mathbf{y})$ is invertible in $K[B_0]$. Let $h \in \mathcal{O}[\mathbf{Y}]$ be a common multiple of h_0 and h_ψ and denote $B = V \setminus V(h)$ and $D = D_0[h(\mathbf{y})^{-1}]$.

Let i be a positive integer between 1 and t. Since the pair (ψ_i, V) is solvable by the pair (P_i, h_{ψ_i}), it follows that there exists a quantifier-free formula $\overline{\psi_i}_{\mathcal{C}}(\mathbf{Y}, Z)$, in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$, such that the pair $(p_{\mathcal{C}}, \overline{\psi_i}_{\mathcal{C}})$ is a solution for the triple $(\psi_i, D/B, \mathcal{C})$. That is, for every perfect algebraic extension M of K which is PAC over $\mathcal{O}_M$ and for each $\mathbf{b} \in B(\mathcal{O}_M)$ which satisfies $\mathrm{Ar}(D/B, M, \mathbf{b}) = \mathcal{C}$ we have

$$\begin{aligned} \mathcal{O}_M \models \psi_i(\mathbf{b}) &\Leftrightarrow \mathcal{O}_M \models \exists Z[p_{\mathcal{C}}(\mathbf{b}, Z) = 0 \wedge \overline{\psi_i}_{\mathcal{C}}(\mathbf{b}, Z)] \\ &\Leftrightarrow \mathcal{O}_M \models \forall Z[p_{\mathcal{C}}(\mathbf{b}, Z) = 0 \to \overline{\psi_i}_{\mathcal{C}}(\mathbf{b}, Z)]\,. \end{aligned} \tag{5}$$

We denote

$$\overline{\psi}_{\mathcal{C}}(\mathbf{Y}, Z) : \overline{\psi_1}_{\mathcal{C}}(\mathbf{Y}, Z) \vee \cdots \vee \overline{\psi_t}_{\mathcal{C}}(\mathbf{Y}, Z)\,.$$

Then, for every perfect algebraic extension M of K which is PAC over $\mathcal{O}_M$ and for each $\mathbf{b} \in B(\mathcal{O}_M)$ which satisfies $\mathrm{Ar}(D/B, M, \mathbf{b}) = \mathcal{C}$ we have, using (4) and (5), that

$$\begin{aligned} \mathcal{O}_M \models \psi(\mathbf{b}) &\Leftrightarrow \mathcal{O}_M \models \psi_1(\mathbf{b}) \vee \cdots \vee \psi_t(\mathbf{b}) \\ &\Leftrightarrow \mathcal{O}_M \models \bigvee_{i=1}^{t} \exists Z[p_{\mathcal{C}}(\mathbf{b}, Z) = 0 \wedge \overline{\psi_i}_{\mathcal{C}}(\mathbf{b}, Z)] \\ &\Leftrightarrow \mathcal{O}_M \models \exists Z[p_{\mathcal{C}}(\mathbf{b}, Z) = 0 \wedge (\bigvee_{i=1}^{t} \overline{\psi_i}_{\mathcal{C}}(\mathbf{b}, Z))] \\ &\Leftrightarrow \mathcal{O}_M \models \exists Z[p_{\mathcal{C}}(\mathbf{b}, Z) = 0 \wedge \overline{\psi}_{\mathcal{C}}(\mathbf{b}, Z))]\,. \end{aligned}$$

Similarly, $\mathcal{O}_M \models \psi(\mathbf{b}) \Leftrightarrow \mathcal{O}_M \models \forall Z[p_{\mathcal{C}}(\mathbf{b}, Z) = 0 \to \overline{\psi}_{\mathcal{C}}(\mathbf{b}, Z)]$. □

3. Radical Galois Stratification

Introduction. In this section we shall prove the theorem that was formulated in the introduction (Theorem 3.33): Let e be a non-negative integer. For each $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e) \in \mathrm{Gal}(K)^e$ let $\tilde{K}(\boldsymbol{\sigma})$ be the fixed field in $\tilde{K}$ of $\sigma_1, \ldots, \sigma_e$ and let $\widetilde{\mathcal{O}}(\boldsymbol{\sigma})$ be the integral closure of $\mathcal{O}$ in $\tilde{K}(\boldsymbol{\sigma})$. Let θ be a sentence in the language $\mathcal{L}(\mathrm{ring}, \mathcal{O})$ and let α be the Haar measure of all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ such that θ is true in $\widetilde{\mathcal{O}}(\boldsymbol{\sigma})$. Then, α is a rational number which can be effectively computed in a primitive recursive way when $\mathcal{O}$ is an effective computability domain.

For the convenience of the reader, we shall describe in this introduction to Section 3, in general lines, the primitive recursive procedure of quantifiers elimination in the stratification procedure.

We rewrite θ in a disjunctive normal form:

$$(Q_1 X_1) \cdots (Q_n X_n)\big[\bigvee_{i=1}^{k} \bigwedge_{j=1}^{l} f_{ij}(\mathbf{X}) = 0 \wedge g_{ij}(\mathbf{X}) \neq 0\big],$$

where $\mathbf{X} = (X_1, \ldots, X_n)$, Q_i is the existential quantifier $\exists$ or the universal quantifier $\forall$, and $f_{ij}, g_{ij} \in \mathcal{O}[\mathbf{X}]$. The formula in the brackets defines a K-constructible set $A \subseteq \mathbb{A}^n$. Now, we stratify the affine space $\mathbb{A}^n$ into a finite union of disjoint K-normal basic sets

$$\mathbb{A}^n = \bigcup_{i \in I_n}^{\cdot} A_i$$

such that for each $i \in I_n$, $A_i \subseteq A$ or $A_i \subseteq \mathbb{A}^n \smallsetminus A$, where each A_i is of the form $V_i \smallsetminus V(g_i)$ with $g_i \in K[\mathbf{X}]$, V_i is a K-variety on which g_i does not vanish, and the ring $K[A_i] = K[\mathbf{x}_i, g(\mathbf{x}_i)^{-1}]$ is integrally closed, where $\mathbf{x}_i$ is a generic point of V_i. For each $i \in I_n$ we choose a quantifier-free sentence θ_i in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$ such that θ_i is true if $A_i \subseteq A$ and θ_i is false if $A_i \subseteq \mathbb{A}^n \smallsetminus A$. We denote by $\mathcal{A}_n(\mathcal{O})$ the system $\langle \mathbb{A}^n, A_i, \theta_i \,|\, i \in I_n \rangle$ and by $\mathrm{Sen}(\mathcal{A}_n(\mathcal{O}))$ the system of sentences $(\theta_i \,|\, i \in I_n)$. For an algebraic extension M of K and for $\mathbf{a} \in \mathbb{A}^n(\mathcal{O}_M)$ we write $(\mathcal{A}_n, M, \mathbf{a}) \models \mathrm{Sen}(\mathcal{A}_n(\mathcal{O}))$ if $\mathcal{O}_M \models \theta_i$ for the unique $i \in I_n$ such that $\mathbf{a} \in A_i$. In these notations we have that for every algebraic extension M of K,

$$\mathcal{O}_M \models \theta \Leftrightarrow (Q_1 X_1) \cdots (Q_n X_n)[(\mathcal{A}_n, M, (X_1, \ldots, X_n)) \models \mathrm{Sen}(\mathcal{A}_n(\mathcal{O}))].$$

This is the situation at the starting point of the elimination procedure. At the general stage of this procedure we are dealing with objects that have also "height".

Suppose that we have eliminated the quantifiers $Q_n, \ldots, Q_{m+1}$, in order, where m is a positive integer between 1 and n. In this stage $\mathbb{A}^m$ is stratified into a union of disjoint K-normal basic sets, $\mathbb{A}^m = \bigcup_{i \in I_m}^{\cdot} A_i$, and for each $i \in I_m$ we build the following complex structure over A_i: C_i is an integral domain which extends $K[A_i]$ such that $C_i/K[A_i]$ is a Galois ring cover with Galois group $\mathrm{Gal}(K(C_i)/K(A_i)) = \mathrm{Gal}(C_i/A_i)$. Here $K(A_i) = K(\mathbf{x}_i)$, where $\mathbf{x}_i = (x_{i1}, \ldots, x_{im})$ is a generic point of A_i. In addition, for each subextension L of $K(C_i)/K(A_i)$, $(C_i \cap L)/K[A_i]$ is a ring cover.

Let $\mathcal{H}$ be the family of all finite groups H such that $\mathrm{rank}(H) \leq e$ and let $\mathrm{Conj}(C_i/A_i, \mathcal{H})$ be the set of all conjugacy classes of subgroups of $\mathrm{Gal}(C_i/A_i)$ which belong to $\mathcal{H}$. Note that when $e = 0$, $\mathcal{H} = \{\mathbf{1}\}$; hence $\mathrm{Conj}(C_i/A_i, \mathcal{H})$ contains

only one conjugacy class, which is $\{\mathrm{Gal}(C_i/C_i)\}$. For each $\mathcal{C} \in \mathrm{Conj}(C_i/A_i, \mathcal{H})$ we denote the set of all fixed fields in $K(C_i)$ of groups in $\mathcal{C}$ by $\mathrm{Fix}(\mathcal{C})$. For each $L \in \mathrm{Fix}(\mathcal{C})$ we choose a primitive element z_L for the extension $L/K(A_i)$ such that: for every $L_1, L_2 \in \mathrm{Fix}(\mathcal{C})$ there exists $\sigma \in \mathrm{Gal}(C_i/A_i)$ which satisfies $L_2 = \sigma L_1$ and $z_{L_2} = \sigma z_{L_1}$, z_L is integral over $\mathcal{O}[\mathbf{x}_i]$, and the discriminant of z_L over $K(A_i)$ is invertible in $K[A_i]$ (recall that $(C_i \cap L)/K[A_i]$ is a ring cover). Let $p_{i,\mathcal{C}} \in \mathcal{O}[\mathbf{X}, Z]$ be such that $p_{i,\mathcal{C}}(\mathbf{x}_i, Z)$ is a multiple of $\mathrm{irr}(z_L, K(A_i))$ by an invertible element of $K[A_i]$, for $L \in \mathrm{Fix}(\mathcal{C})$. For each $L \in \mathrm{Fix}(\mathcal{C})$ we attach a quantifier-free sentence $\theta_{i,L}$ in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}[\mathbf{x}_i, z_L])$, such that $\theta_{i,\sigma L} = \sigma\theta_{i,L}$ for each $\sigma \in \mathrm{Gal}(C_i/A_i)$ which satisfies $z_{\sigma L} = \sigma z_L$. That is, there is a quantifier-free formula $\varphi_{i,\mathcal{C}}(X_1, \ldots, X_m, Z)$ in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$ such that $\theta_{i,L} = \varphi_{i,\mathcal{C}}(\mathbf{x}_i, z_L)$ for each $L \in \mathrm{Fix}(\mathcal{C})$. Let $\boldsymbol{\theta}_{i,\mathcal{H}}$ be the system of sentences $(\theta_{i,L} \,|\, L \in \mathrm{Fix}(\mathcal{C}), \mathcal{C} \in \mathrm{Conj}(C_i/A_i, \mathcal{H}))$. We say that $\boldsymbol{\theta}_{i,\mathcal{H}}$ is a **quantifier-free sentence in the language** $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}[C_i/A_i, \mathcal{H}])$.

Let M be one of the fields $\tilde{K}(\boldsymbol{\sigma})$, chosen at random. Then $\mathcal{O}_M = \widetilde{\mathcal{O}}(\boldsymbol{\sigma})$ is the integral closure of $\mathcal{O}$ in M. For almost all (with respect to the Haar measure) $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, $\tilde{K}(\boldsymbol{\sigma})$ is a perfect field and is PAC over $\widetilde{\mathcal{O}}(\boldsymbol{\sigma})$ (Proposition 1.7) which satisfies $\mathrm{Gal}(\tilde{K}(\boldsymbol{\sigma})) \cong \hat{F}_e$ [FrJ08, p. 379, Thm. 18.5.6]. We denote the set of all fields M such that M is a perfect algebraic extension of K which is PAC over $\mathcal{O}_M$ and $\mathrm{Gal}(M) \cong \hat{F}_e$ by $\mathcal{F}_e(\mathcal{O})$. Note that $\mathrm{Gal}(M) \cong \hat{F}_e$ iff $\mathrm{Im}(\mathrm{Gal}(M)) = \mathcal{H}$ [FrJ08, p. 360, Lemma 17.7.1]. If $M \in \mathcal{F}_e(\mathcal{O})$, then $\mathrm{Gal}(M)$ has in particular the embedding property [FrJ08, p. 568, Lemma 24.3.3] and M is a Frobenius field over $\mathcal{O}_M$ (Subsection 3.1).

Let $M \in \mathcal{F}_e(\mathcal{O})$, $\mathbf{a} \in A_i(\mathcal{O}_M)$. Denote the Artin symbol, $\mathrm{Ar}(C_i/A_i, M, \mathbf{a})$, of $\mathbf{a}$ in $\mathrm{Gal}(C_i/A_i)$ (Definition 1.20 c)) by $\mathcal{C}$. We write $(C_i/A_i, M, \mathbf{a}) \models \boldsymbol{\theta}_{i,\mathcal{H}}$ iff

$$\mathcal{O}_M \models \exists Z[p_{i,\mathcal{C}}(\mathbf{a}, Z) = 0 \wedge \varphi_{i,\mathcal{C}}(\mathbf{a}, Z)]\,.$$

We say that the pair $(C_i/A_i, \boldsymbol{\theta}_{i,\mathcal{H}})$ is **compatible** iff

a) for each $\mathcal{C} \in \mathrm{Conj}(C_i/A_i, \mathcal{H})$, the content of $\theta_{i,L}$ in $K[A_i]$ (Definition 2.12 b)), for $L \in \mathrm{Fix}(\mathcal{C})$, is an invertible element of $K[A_i]$; and

b) for every $M \in \mathcal{F}_e(\mathcal{O})$ and $\mathbf{a} \in A_i(\mathcal{O}_M)$ we have, for $\mathcal{C} = \mathrm{Ar}(A_i, M, \mathbf{a})$, that

$$\begin{aligned} &\mathcal{O}_M \models \exists Z[p_{i,\mathcal{C}}(\mathbf{a}, Z) = 0 \wedge \varphi_{i,\mathcal{C}}(\mathbf{a}, Z)] \\ \Leftrightarrow\ &\mathcal{O}_M \models \forall Z[p_{i,\mathcal{C}}(\mathbf{a}, Z) = 0 \to \varphi_{i,\mathcal{C}}(\mathbf{a}, Z)]\,. \end{aligned}$$

We assume that all the sentences $\boldsymbol{\theta}_{i,\mathcal{H}}$ are compatible with the cover C_i/A_i. (For each $\mathcal{C} \in \mathrm{Conj}(C_i/A_i, \mathcal{H})$ and each $L \in \mathrm{Fix}(\mathcal{C})$, the discriminant of z_L over $K(A_i)$ is invertible in $K[A_i]$; this assumption will allow us, using Proposition 2.26, to build in each stage of the elimination procedure such a quantifier-free sentence $\boldsymbol{\theta}_{i,\mathcal{H}}$.)

In the starting point of the elimination procedure, when $m = n$, we take, for each $i \in I_n$, $C_i = K[A_i]$ and hence $\mathrm{Gal}(C_i/A_i) = \mathbf{1}$. In particular, $\mathrm{Gal}(C_i/A_i)$ has only one conjugacy class $\mathcal{C} = \{\mathbf{1}\}$ which belongs, of course, to $\mathrm{Conj}(C_i/A_i, \mathcal{H})$. We attach to it a quantifier-free formula θ_i in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$ such that θ_i is true or false according to if $A_i \subseteq A$ or $A_i \subseteq \mathbb{A}^n \setminus A$.

We call the system

$$\mathcal{A}_m(\mathcal{O}, \mathcal{H}) = \langle \mathbb{A}^m, C_i/A_i, \boldsymbol{\theta}_{i,\mathcal{H}} \,|\, i \in I_m \rangle$$

a **radical Galois stratification** (with respect to $\mathcal{H}$) of $\mathbb{A}^m$ over $\mathcal{O}$ and the system $\mathcal{A}_m = \langle \mathbb{A}^m, C_i/A_i \,|\, i \in I_m \rangle$ the **normal stratification under** $\mathcal{A}_m(\mathcal{O}, \mathcal{H})$. Let

$$\mathrm{Sen}(\mathcal{A}_m(\mathcal{O}, \mathcal{H})) = (\boldsymbol{\theta}_{i,\mathcal{H}} \,|\, i \in I_m)$$

be the system of sentences of $\mathcal{A}_m(\mathcal{O},\mathcal{H})$. For $M\in\mathcal{F}_e(\mathcal{O})$ and $\mathbf{a}\in\mathbb{A}^m(\mathcal{O}_M)$, we write $(\mathcal{A}_m,M,\mathbf{a})\models \mathrm{Sen}(\mathcal{A}_m(\mathcal{O},\mathcal{H}))$ if $(C_i/A_i,M,\mathbf{a})\models \boldsymbol{\theta}_{i,\mathcal{H}}$ for the unique $i\in I_m$ such that $\mathbf{a}\in A_i$.

If $\mathcal{O}=K$, we denote, for each $i\in I_m$, by $\mathrm{Con}(A_i,\mathcal{H})$ the conjugacy domain of $\mathrm{Gal}(C_i/A_i)$ which contains all the subgroups G that belong to $\mathcal{H}$ and satisfy, for $\mathcal{C}=\{G^\sigma\,|\,\sigma\in\mathrm{Gal}(C_i/A_i)\}$, that there exists $(\tilde{\mathbf{a}},\tilde{z})\in A_i(\tilde{K})\times\tilde{K}$ such that $p_{i,\mathcal{C}}(\tilde{\mathbf{a}},\tilde{z})=0$ and $\tilde{K}\models\varphi_{i,\mathcal{C}}(\tilde{\mathbf{a}},\tilde{z})$. Let $M\in\mathcal{F}_e(K)$ and $\mathbf{a}\in A_i(M)$. Then

$$\mathrm{Ar}(A_i,M,\mathbf{a})\subseteq\mathrm{Con}(A_i,\mathcal{H})\Leftrightarrow(C_i/A_i,M,\mathbf{a})\models\boldsymbol{\theta}_{i,\mathcal{H}}\,.$$

Indeed, let $\mathcal{C}=\mathrm{Ar}(A_i,M,\mathbf{a})$ and $L\in\mathrm{Fix}(\mathcal{C})$. Then there exists a K-homomorphism, $\tau'\colon K[\mathbf{x}_i,z_L]\to M$, such that $\tau'(\mathbf{x}_i)=\mathbf{a}$. Also, the content of $\theta_{i,L}$ in $K[A_i]$ is an invertible element of $K[A_i]$. Note that $\mathcal{C}\subseteq\mathrm{Con}(A_i,\mathcal{H})$ iff there exists a K-homomorphism, $\tau\colon K[\mathbf{x}_i,z_L]\to\tilde{K}$, which satisfies that $\tilde{K}\models\tau(\theta_{i,L})$. Hence, by Remark 2.14 b),

$$\begin{aligned}\mathcal{C}\subseteq\mathrm{Con}(A_i,\mathcal{H})\Leftrightarrow M\models\tau'(\theta_{i,L})&\Leftrightarrow M\models\exists Z[p_{i,\mathcal{C}}(\mathbf{a},Z)=0\wedge\varphi_{i,\mathcal{C}}(\mathbf{a},Z)]\\&\Leftrightarrow(C_i/A_i,M,\mathbf{a})\models\boldsymbol{\theta}_{i,\mathcal{H}}\,.\end{aligned}$$

In this way we can replace the radical Galois stratification $\mathcal{A}_m(\mathcal{O},\mathcal{H})$ of $\mathbb{A}^m$ by the usual Galois stratification [FrJ08, Chapter 30]

$$\mathcal{A}_m(\mathcal{H})=\langle\mathbb{A}^m,C_i/A_i,\mathrm{Con}(A_i,\mathcal{H})\,|\,i\in I_m\rangle$$

of $\mathbb{A}^m$.

Now, let $\pi:\mathbb{A}^m\to\mathbb{A}^{m-1}$ be the projection defined by

$$\pi(x_1,\ldots,x_m)=(x_1,\ldots,x_{m-1})\,.$$

If Q_m is the existential quantifier $\exists$, we build a radical Galois stratification $\mathcal{A}_{m-1}(\mathcal{O},\mathcal{H})$ of $\mathbb{A}^{m-1}$ over $\mathcal{O}$, such that for every $M\in\mathcal{F}_e(\mathcal{O})$ and each $\mathbf{b}\in\mathbb{A}^{m-1}(\mathcal{O}_M)$, $(\mathcal{A}_{m-1},M,\mathbf{b})\models\mathrm{Sen}(\mathcal{A}_{m-1}(\mathcal{O},\mathcal{H}))$ iff there exists $\mathbf{a}\in\mathbb{A}^m(\mathcal{O}_M)$ such that $\pi(\mathbf{a})=\mathbf{b}$ and $(\mathcal{A}_m,M,\mathbf{a})\models\mathrm{Sen}(\mathcal{A}_m(\mathcal{O},\mathcal{H}))$. In this way, we code the information on the existential quantifier in the formula

$$\exists X_m[(\mathcal{A}_m,M,(X_1,\ldots,X_{m-1},X_m))\models\mathrm{Sen}(\mathcal{A}_m(\mathcal{O},\mathcal{H}))]$$

inside a new radical Galois stratification $\mathcal{A}_{m-1}(\mathcal{O},\mathcal{H})$.

If Q_m is the universal quantifier $\forall$, we build the complement to $\mathcal{A}_m(\mathcal{O},\mathcal{H})$:

$$\mathcal{A}_m^c(\mathcal{O},\mathcal{H})=\langle\mathbb{A}^m,C_i/A_i,\neg\boldsymbol{\theta}_{i,\mathcal{H}}\,|\,i\in I_m\rangle\,.$$

Note that since the pair $(C_i/A_i,\boldsymbol{\theta}_{i,\mathcal{H}})$ is compatible, for each $i\in I_m$, it follows that for every $M\in\mathcal{F}_e(\mathcal{O})$ and each $\mathbf{a}\in\mathbb{A}^m(\mathcal{O}_M)$,

$$(\mathcal{A}_m,M,\mathbf{a})\not\models\mathrm{Sen}(\mathcal{A}_m(\mathcal{O},\mathcal{H}))\Leftrightarrow(\mathcal{A}_m^c,M,\mathbf{a})\models\mathrm{Sen}(\mathcal{A}_m^c(\mathcal{O},\mathcal{H}))\,.$$

Now, we find a radical Galois stratification $\mathcal{A}_{m-1}^c(\mathcal{O},\mathcal{H})$ of $\mathbb{A}^{m-1}$ over $\mathcal{O}$ such that for every $M\in\mathcal{F}_e(\mathcal{O})$ and each $\mathbf{b}\in\mathbb{A}^{m-1}(\mathcal{O}_M)$, $(\mathcal{A}_{m-1}^c,M,\mathbf{b})\models\mathrm{Sen}(\mathcal{A}_{m-1}^c(\mathcal{O},\mathcal{H}))$ iff there exists $\mathbf{a}\in\mathbb{A}^m(\mathcal{O}_M)$ such that $\pi(\mathbf{a})=\mathbf{b}$ and $(\mathcal{A}_m^c,M,\mathbf{a})\models\mathrm{Sen}(\mathcal{A}_m^c(\mathcal{O},\mathcal{H}))$. The complementary radical Galois stratification to $\mathcal{A}_{m-1}^c(\mathcal{O},\mathcal{H})$ satisfies, for every $M\in\mathcal{F}_e(\mathcal{O})$ and each $\mathbf{b}\in\mathbb{A}^{m-1}(\mathcal{O}_M)$, that $(\mathcal{A}_{m-1},M,\mathbf{b})\models\mathrm{Sen}(\mathcal{A}_{m-1}(\mathcal{O},\mathcal{H}))$ iff $(\mathcal{A}_m,M,\mathbf{a})\models\mathrm{Sen}(\mathcal{A}_m(\mathcal{O},\mathcal{H}))$ for all $\mathbf{a}\in\mathbb{A}^m(\mathcal{O}_M)$ such that $\pi(\mathbf{a})=\mathbf{b}$.

In any case, for every $M\in\mathcal{F}_e(\mathcal{O})$ and each $(a_1,\ldots,a_{m-1})\in\mathbb{A}^{m-1}(\mathcal{O}_M)$, we have

$$(\mathcal{A}_{m-1},M,(a_1,\ldots,a_{m-1}))\models\mathrm{Sen}(\mathcal{A}_{m-1}(\mathcal{O},\mathcal{H}))$$

if and only if $Q_m a_m \in \mathcal{O}_M$ such that $(\mathcal{A}_m, M, \mathbf{a}) \models \mathrm{Sen}(\mathcal{A}_m(\mathcal{O}, \mathcal{H}))$, where $\mathbf{a} = (a_1, \ldots, a_m)$.

In this way we eliminate the quantifiers $Q_n, \ldots, Q_1$ from θ, in order. In the final stage we get a radical Galois stratification (with respect to $\mathcal{H}$) $\mathcal{A}_0(\mathcal{O}, \mathcal{H})$ of $\mathbb{A}^0$ over $\mathcal{O}$ such that, for every $M \in \mathcal{F}_e(\mathcal{O})$,

$$\begin{aligned}\mathcal{O}_M \models \theta &\Leftrightarrow (Q_1 X_1) \cdots (Q_n X_n)[(\mathcal{A}_n, M, (X_1, \ldots, X_n)) \models \mathrm{Sen}(\mathcal{A}_n(\mathcal{O}))] \\ &\Leftrightarrow (\mathcal{A}_0, M, O) \models \mathrm{Sen}(\mathcal{A}_0(\mathcal{O}, \mathcal{H}))\,,\end{aligned}$$

where O is the only point in $\mathbb{A}^0$. The normal stratification $\mathcal{A}_0$ under $\mathcal{A}_0(\mathcal{O}, \mathcal{H})$ is trivial: $\mathcal{A}_0 = \langle \mathbb{A}^0, C_0/A_0 \rangle$, where $A_0 = \mathbb{A}^0 = \{O\}$. In this case $K(A_0) = K$, $C_0 = L$ is a finite Galois extension of K, and, for every algebraic extension M of K,

$$\mathrm{Ar}(A_0, M, O) = \{\mathrm{Gal}(L/L \cap M)^\sigma \,|\, \sigma \in \mathrm{Gal}(L/K)\}\,.$$

In addition, $\mathrm{Sen}(\mathcal{A}_0(\mathcal{O}, \mathcal{H}))$ contains only one system of sentences $\boldsymbol{\chi}_{\mathcal{H}} = (\chi_{K'} \,|\, K' \in \mathrm{Field}(L/K, \mathcal{H}))$, where $\mathrm{Field}(L/K, \mathcal{H})$ is the set of all subextensions K' of L/K such that $\mathrm{Gal}(L/K') \in \mathcal{H}$, and $\chi_{K'}$ is a quantifier-free sentence in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}_{K'})$ such that if K_1' and K_2' are two subextensions of L/K which are conjugate by an element of $\mathrm{Gal}(L/K)$, then there exists $\sigma \in \mathrm{Gal}(L/K)$ which satisfies $K_2' = \sigma K_1'$ and $\chi_{K_2'} = \sigma \chi_{K_1'}$. Hence, for every $M \in \mathcal{F}_e(\mathcal{O})$, the condition $(\mathcal{A}_0, M, O) \models \mathrm{Sen}(\mathcal{A}_0(\mathcal{O}, \mathcal{H}))$ reduces to $\mathrm{Gal}(L/L \cap M) \in \mathcal{H}$ and $\mathcal{O}_M \models \chi_{L \cap M}$. It follows from Proposition 2.11 that $\mathcal{O}_M \models \chi_{L \cap M}$ iff $\widetilde{\mathcal{O}} \models \chi_{L \cap M}$. We denote

$$\mathrm{Con}_\theta(\mathcal{H}) = \{\mathrm{Gal}(L/K') \in \mathcal{H} \,|\, K' \text{ is a subextension of } L/K \text{ s.t. } \widetilde{\mathcal{O}} \models \chi_{K'}\}\,.$$

Then, $\mathrm{Con}_\theta(\mathcal{H})$ is a conjugacy domain of subgroups of $\mathrm{Gal}(L/K)$ which belong to $\mathcal{H}$. Moreover, when $\mathcal{O}$ is an effective computability domain, if e is given and θ is presented, then we can effectively find it (because, by Proposition 2.8, the relation $\mathrm{Rad}_{k,l}$ on $\widetilde{\mathcal{O}}$ is primitive recursive). We arrive, then, to the conclusion that, for every $M \in \mathcal{F}_e(\mathcal{O})$,

$$\mathcal{O}_M \models \theta \Leftrightarrow \mathrm{Gal}(L/L \cap M) \in \mathrm{Con}_\theta(\mathcal{H})\,.$$

Let k be the number of $\boldsymbol{\sigma}_0 \in \mathrm{Gal}(L/K)^e$ such that $\langle \boldsymbol{\sigma}_0 \rangle \in \mathrm{Con}_\theta(\mathcal{H})$. Then, it follows from above that $\alpha = \dfrac{k}{[L:K]^e}$ is the desired rational number; that is, α is the Haar measure of all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ such that θ is true in $\widetilde{\mathcal{O}}(\boldsymbol{\sigma})$.

3.1. **Frobenius Fields over Rings of Integers.** Recall that a field M is a **Frobenius field** if M is PAC and $\mathrm{Gal}(M)$ has the embedding property [FrJ08, p. 564, Def. 24.1.3].

Definition 3.1. Let R be a subring of a field M. We say that M is a **Frobenius field over** R if M is PAC over R and $\mathrm{Gal}(M)$ has the embedding property.

A Frobenius field satisfies the decomposition group's property [FrJ08, p. 564, Prop. 24.1.4]. We shall prove here a similar proposition for a Frobenius field over a subring for the special case which we are interested in this work:

Proposition 3.2. *Let M be a perfect algebraic extension of K and suppose that M is Frobenius over $\mathcal{O}_M$. Let y be a transcendental element over M and denote $E = M(y)$. Let F be a finite Galois extension of E and let S/R be a ring cover over M with a field cover F/E, where $R = M[y, g(y)^{-1}]$ with a nonzero polynomial g in $M[Y]$. Let N be the algebraic closure of M in F and let H be a subgroup*

of $\mathrm{Gal}(F/E)$ *such that* $H \in \mathrm{Im}(\mathrm{Gal}(M))$ *and* $\mathrm{res}_N(H) = \mathrm{Gal}(N/M)$. *Let* E' *be the fixed field of* H *in* F *and let* z *be a primitive element for the extension* E'/E *which is integral over* $\mathcal{O}_M[y]$. *Let* θ *be a quantifier-free sentence in the language* $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}_M[y,z])$ *and suppose that there exists an* M*-homomorphism* $\tau\colon S \to \tilde{K}$ *which satisfies that* $\tau(y), \tau(z) \in \mathcal{O}_M$, $\tau(c_\theta) \neq 0$, *and* $\mathcal{O}_M \models \tau(\theta)$, *where* c_θ *is the content of* θ *in* R.

Then, there exists an M*-homomorphism* $\psi\colon S \to \tilde{K}$ *which satisfies that* $\psi(y), \psi(z) \in \mathcal{O}_M$, $\mathcal{O}_M \models \psi(\theta)$, *and* $D_M(\psi) = H$, *where*

$$D_M(\psi) = \{\sigma \in \mathrm{Gal}(F/E) |\ (\forall u \in S)[\psi(u) \in M \Rightarrow \psi(\sigma u) = \psi(u)]\}\,.$$

Proof. The fixed field $E' = F(H)$ of H in F satisfies that $N \cap E' = M$. Hence $\mathrm{res}\colon \mathrm{Gal}(F/E') \to \mathrm{Gal}(N/M)$ is surjective. We apply the embedding property of $\mathrm{Gal}(M)$ on the diagram

$$\begin{array}{ccc} & & \mathrm{Gal}(M) \\ & & \downarrow \mathrm{res} \\ \mathrm{Gal}(F/E') & \xrightarrow{\mathrm{res}} & \mathrm{Gal}(N/M)\,. \end{array}$$

This gives a Galois extension N' of M which contains N and an isomorphism $j\colon \mathrm{Gal}(N'/M) \to \mathrm{Gal}(F/E')$ with $\mathrm{res}_N(j(\sigma)) = \mathrm{res}_N(\sigma)$ for each $\sigma \in \mathrm{Gal}(N'/M)$. In particular, $N'E' \cap F = NE'$. Let $F' = N'F$. Then

$$\mathrm{Gal}(F'/E') = \{(\sigma_1, \sigma_2) \in \mathrm{Gal}(N'/M) \times \mathrm{Gal}(F/E') |\ \mathrm{res}_N(\sigma_1) = \mathrm{res}_N(\sigma_2)\}\,.$$

Let $\Delta = \{(\sigma, j(\sigma)) |\ \sigma \in \mathrm{Gal}(N'/M)\}$ and let D be the fixed field of Δ in F'. Then, it follows from the field crossing argument (which appears, for example, in Part A of the proof of [FrJ08, p. 431, Lemma 20.2.2] and, of course, in the proof of [FrJ08, p. 564, Prop. 24.1.4]) that $DN' = DF = F'$, $F \cap D = E'$, and $N' \cap D = M$. In particular, D is a regular extension of M of transcendence degree 1.

The integral closure U of R in D is finitely generated over R [Lan64, p. 120]:

$$U = R[x_1, \ldots, x_n] = M[y, g(y)^{-1}, x_1, \ldots, x_n]\,.$$

Let D_θ be the definition set of θ in $\mathcal{O}_M[y,z]$. Since z belongs to E' and is integral over $\mathcal{O}_M[y]$, it follows that $z \in U$ and hence $D_\theta \subset U$. Suppose, without loss, that $D_\theta \subseteq \{x_1, \ldots, x_n\}$ and let W be an M-variety which is generated by the point $(y, g(y)^{-1}, \mathbf{x})$. Since M is perfect and PAC over $\mathcal{O}_M$, it follows from Theorem 1.10 (applied to W instead of to V) that there exists an M-epimorphism $\psi_U\colon U \to M$ such that $\psi_U(y), \psi_U(z) \in \mathcal{O}_M$ and $\frac{\psi_U(d)}{\tau(d)}$ is an invertible element of $\mathcal{O}_M$ for each $d \in D_\theta$ (because $\tau(c_\theta) \neq 0$ and hence $\tau(d) \neq 0$). Hence, since $\mathcal{O}_M \models \tau(\theta)$, it follows from Lemma 2.13 that $\mathcal{O}_M \models \psi_U(\theta)$. Let z' be a primitive element for the extension N'/M. Then, since D is linearly disjoint from N' over M, it follows from [FrJ08, p. 110, Remark 6.1.7] that the integral closure V of U in F' is $N'U = U[z'] = N' \otimes_M U$. In particular, $S \subseteq V$. Hence ψ_U extends to an N'-epimorphism $\psi'\colon V \to N'$. Since $[F' : D] = [N' : M]$, it follows that the decomposition group

$$D(\psi') = \{\sigma \in \mathrm{Gal}(F'/E') |\ (\forall v \in V)[\psi'(v) = 0 \Rightarrow \psi'(\sigma v) = 0]\}$$

is Δ [FrJ08, p. 109, Lemma 6.1.4] (Note that $D(\psi') = D(\mathrm{Ker}(\psi'))$ in the notations of [FrJ08, §6.1]). Let ψ be the restriction of ψ' to S and let

$$D(\psi) = \{\sigma \in \mathrm{Gal}(F/E) |\ (\forall u \in S)[\psi(u) = 0 \Rightarrow \psi(\sigma u) = 0]\}\,.$$

Then, $\mathrm{Gal}(F/E') = \mathrm{res}_F D(\psi') \leq D(\psi) \leq \mathrm{Gal}(F/E')$ and hence $D(\psi) = H$. Finally, by Remark 1.21 b), $D_M(\psi) = D(\psi) = H$. □

3.2. **Cover-Sentence Pairs.**

Notation 3.3. Let A be a K-normal basic subset of $\mathbb{A}^n$ with

$$K[A] = K[x_1, \ldots, x_n, g(\mathbf{x})^{-1}],$$

where g is a polynomial in $\mathcal{O}[X_1, \ldots, X_n]$, and let C/A be a Galois ring/set cover over K. Also, let $\mathcal{H}$ be a family of finite groups.

a) $\bar{A}$ is the Zariski closure of A in $\mathbb{A}^n$. That is, $\bar{A}$ is the K-variety generated by $\mathbf{x} = (x_1, \ldots, x_n)$.

b) $\mathcal{O}[\bar{A}] = \mathcal{O}[\mathbf{x}]$ is called the **ring of integers of** $\bar{A}$.

c) $\mathrm{Conj}(C/A)$ is the set of all conjugacy classes of subgroups of $\mathrm{Gal}(C/A)$. $\mathrm{Conj}(C/A, \mathcal{H})$ is the set of all the conjugacy classes of subgroups of $\mathrm{Gal}(C/A)$ which belong to $\mathcal{H}$.

d) For each $\mathcal{C} \in \mathrm{Conj}(C/A)$, $\mathrm{Fix}(\mathcal{C})$ is the set of all the fixed fields in $K(C)$ of subgroups in $\mathcal{C}$.

e) $\mathrm{Field}(C/A)$ is the set of all subextensions of $K(C)/K(A)$.
$\mathrm{Field}(C/A, \mathcal{H}) = \{L \in \mathrm{Field}(C/A) \mid \mathrm{Gal}(K(C)/L) \in \mathcal{H}\}$.

f) For each $L \in \mathrm{Field}(C/A)$ we choose a primitive element z_L for the extension $L/K(A)$ which is integral over $K[A]$ such that for each $\mathcal{C} \in \mathrm{Conj}(C/A)$ and every $L_1, L_2 \in \mathrm{Fix}(\mathcal{C})$ there exists $\sigma \in \mathrm{Gal}(C/A)$ which satisfies $L_2 = \sigma L_1$ and $z_{L_2} = \sigma z_{L_1}$. (First choose, for each $\mathcal{C} \in \mathrm{Conj}(C/A)$, $L \in \mathrm{Fix}(\mathcal{C})$ and fix such z_L. Denote $G = \mathrm{Gal}(K(C)/L)$ and $H = \{\sigma \in G \mid \sigma L = L\}$. Then $H < G$. Suppose that $[G : H] = r$ and let $\sigma_1 = 1, \sigma_2, \ldots, \sigma_r$ be a system of left coset representatives of G modulo H. Now define $z_{\sigma_i L} = \sigma_i z_L$, $i = 2, \ldots, r$.) We multiply g by a suitable element of $\mathcal{O}[\mathbf{X}]$ in order to assume that the discriminant of z_L over $K(A)$ is invertible in $K[A]$. Then, $(C \cap L)/A$ is a ring/set cover over K with a field cover $L/K(A)$ and with a primitive element z_L. Now, we multiply z_L by an invertible element of $K[A]$ in order to assume that z_L is integral over $\mathcal{O}[\mathbf{x}]$. (Note that the discriminant of z_L over $K(A)$ remains invertible in $K[A]$.)
We say that C/A is a **complete Galois ring/set cover over** K. That is,
for each $L \in \mathrm{Field}(C/A)$, $(C \cap L)/A$ is a ring/set cover over K.
We call z_L an $\mathcal{O}[\bar{A}]$-**integral primitive element for the ring/set cover** $(C \cap L)/A$.
We call the system of primitive elements $\mathbf{z} = (z_L \mid L \in \mathrm{Field}(C/A))$ an $\mathcal{O}[\bar{A}]$-**integral primitive element for** C/A.
$\mathcal{O}[C \cap L] = \mathcal{O}[\mathbf{x}, z_L]$ is called the **ring of integers of** $C \cap L$.
We call the system of rings of integers $\mathcal{O}[C/A] = (\mathcal{O}[C \cap L] \mid L \in \mathrm{Field}(C/A))$ the **ring of integers of** C/A, and we denote $\mathcal{O}[C/A, \mathcal{H}] = (\mathcal{O}[C \cap L] \mid L \in \mathrm{Field}(C/A, \mathcal{H}))$.

g) For each $L \in \mathrm{Field}(C/A, \mathcal{H})$, let θ_L be a quantifier-free sentence in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}[C \cap L])$ such that $\theta_{\sigma L} = \sigma\theta_L$ for each $\sigma \in \mathrm{Gal}(C/A)$ which satisfies $z_{\sigma L} = \sigma z_L$. That is, for each $\mathcal{C} \in \mathrm{Conj}(C/A, \mathcal{H})$ there exists a quantifier-free formula $\varphi_{\mathcal{C}}(X_1, \ldots, X_n, Z)$ in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$ such that $\theta_L = \varphi_{\mathcal{C}}(\mathbf{x}, z_L)$ for each $L \in \mathrm{Fix}(\mathcal{C})$.
We call the system of sentences $\boldsymbol{\theta}_{\mathcal{H}} = (\theta_L \mid L \in \mathrm{Field}(C/A, \mathcal{H}))$ a **quantifier-free sentence in the language** $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}[C/A, \mathcal{H}])$.

h) Let $\boldsymbol{\theta}_{\mathcal{H}}$, $\boldsymbol{\chi}_{\mathcal{H}}$ be quantifier-free sentences in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}[C/A, \mathcal{H}])$.

$\neg\boldsymbol{\theta}_{\mathcal{H}} = (\neg\theta_L \,|\, L \in \mathrm{Field}(C/A,\mathcal{H}))$ is the **negation** of $\boldsymbol{\theta}_{\mathcal{H}}$,
$\boldsymbol{\theta}_{\mathcal{H}} \vee \boldsymbol{\chi}_{\mathcal{H}} = (\theta_L \vee \chi_L \,|\, L \in \mathrm{Field}(C/A,\mathcal{H}))$ is the **disjunction** of $\boldsymbol{\theta}_{\mathcal{H}}$ with $\boldsymbol{\chi}_{\mathcal{H}}$, and
$\boldsymbol{\theta}_{\mathcal{H}} \wedge \boldsymbol{\chi}_{\mathcal{H}} = (\theta_L \wedge \chi_L \,|\, L \in \mathrm{Field}(C/A,\mathcal{H}))$ is the **conjunction** of $\boldsymbol{\theta}_{\mathcal{H}}$ with $\boldsymbol{\chi}_{\mathcal{H}}$.

i) For each $\mathcal{C} \in \mathrm{Conj}(C/A,\mathcal{H})$, let $c_{\theta_{\mathcal{C}}} := c_{\theta_L}$ be the content of θ_L in $K[A]$ (Definition 2.12 b)), for $L \in \mathrm{Fix}(\mathcal{C})$.
We call $c_{\boldsymbol{\theta}_{\mathcal{H}}} = \prod_{\mathcal{C}\in\mathrm{Conj}(C/A,\mathcal{H})} c_{\theta_{\mathcal{C}}}$ the **content of $\boldsymbol{\theta}_{\mathcal{H}}$ in** $K[A]$.
Let $h_{\boldsymbol{\theta}_{\mathcal{H}}} \in \mathcal{O}[\mathbf{X}]$ be such that $h_{\boldsymbol{\theta}_{\mathcal{H}}}(\mathbf{x})$ is a multiply of $c_{\boldsymbol{\theta}_{\mathcal{H}}}$ by an invertible element of $K[A]$. Then, $h_{\boldsymbol{\theta}_{\mathcal{H}}}$ is a polynomial in $\mathcal{O}[\mathbf{X}]$ which satisfies that $h_{\boldsymbol{\theta}_{\mathcal{H}}}(\mathbf{x}) \neq 0$ and for every K-homomorphism, $\tau_0 \colon K[A] \to \tilde{K}$, and for each $L \in \mathrm{Field}(C/A,\mathcal{H})$ we have

$$h_{\boldsymbol{\theta}_{\mathcal{H}}}(\tau_0(\mathbf{x})) \neq 0 \Rightarrow \tau_0(c_{\theta_L}) \neq 0\,.$$

Such a polynomial is called a **content polynomial of $\boldsymbol{\theta}_{\mathcal{H}}$**.

j) For a profinite group G we denote the set of all finite quotients of G by $\mathrm{Im}(G)$.
We denote the set of all fields M such that M is a perfect algebraic extension of K which is Frobenius over $\mathcal{O}_M$ and $\mathrm{Im}(\mathrm{Gal}(M)) = \mathcal{H}$ by $\mathcal{F}_{\mathcal{H}}(\mathcal{O})$.

3.4. *Compatible Cover-Sentence.*

Definition 3.5. Let C/A be the complete Galois ring/set cover over K of Notation 3.3 and let $\mathcal{H}$ be a family of finite groups. Let $\mathbf{z}$ be an $\mathcal{O}[\bar{A}]$-integral primitive element for the cover C/A, let $\mathcal{O}[C/A]$ be the corresponding ring of integers of C/A, and let $\boldsymbol{\theta}_{\mathcal{H}}$ be a quantifier-free sentence in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}[C/A,\mathcal{H}])$. For each $\mathcal{C} \in \mathrm{Conj}(C/A,\mathcal{H})$, let $p_{\mathcal{C}}$ be a polynomial in $\mathcal{O}[\mathbf{X},Z]$ which satisfies that $p_{\mathcal{C}}(\mathbf{x},Z)$ is a multiple of $\mathrm{irr}(z_L,K(\mathbf{x}))$ by an invertible element of $K[A]$ and let $\varphi_{\mathcal{C}}(\mathbf{X},Z)$ be a quantifier-free formula in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$ which satisfies $\varphi_{\mathcal{C}}(\mathbf{x},z_L) = \theta_L$, for each $L \in \mathrm{Fix}(\mathcal{C})$.

a) Let $M \in \mathcal{F}_{\mathcal{H}}(\mathcal{O})$ and $\mathbf{a} \in A(\mathcal{O}_M)$ and denote $\mathcal{C} = \mathrm{Ar}(A,M,\mathbf{a})$. Since $\mathcal{H} = \mathrm{Im}(\mathrm{Gal}(M))$, we have $\mathcal{C} \in \mathrm{Conj}(C/A,\mathcal{H})$. It follows from Remark 1.21 a) that for every K-homomorphism, $\tau \colon C \to \tilde{K}$, such that $\tau(\mathbf{x}) = \mathbf{a}$ we have $\tau(z_L) \in M$, where L is the fixed field of $D_M(\tau)$ in $K(C)$. Also, $\tau(z_L)$ is integral over $\mathcal{O}[\mathbf{a}]$ (because z_L is integral over $\mathcal{O}[\mathbf{x}]$); hence $\tau(z_L) \in \mathcal{O}_M$ and $\tau(\theta_L) = \varphi_{\mathcal{C}}(\mathbf{a},\tau(z_L))$ is a quantifier-free formula in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}_M)$. In particular, it follows from the assumption $\mathcal{C} = \mathrm{Ar}(A,M,\mathbf{a})$ that

$$\mathcal{O}_M \models \exists Z[p_{\mathcal{C}}(\mathbf{a},Z) = 0]\,.$$

We write $(C/A,M,\mathbf{a}) \models \boldsymbol{\theta}_{\mathcal{H}}$ iff there exists a K-homomorphism, $\tau \colon C \to \tilde{K}$, which extends the specialization $\mathbf{x} \mapsto \mathbf{a}$ such that $\mathcal{O}_M \models \tau(\theta_L)$, where L is the fixed field of $D_M(\tau)$ in $K(C)$.
Alternatively, $(C/A,M,\mathbf{a}) \models \boldsymbol{\theta}_{\mathcal{H}}$ iff $\mathcal{O}_M \models \exists Z[p_{\mathcal{C}}(\mathbf{a},Z) = 0 \wedge \varphi_{\mathcal{C}}(\mathbf{a},Z)]$.

b) We say that the cover-sentence pair $(C/A,\boldsymbol{\theta}_{\mathcal{H}})$ is **compatible** iff the following two conditions are satisfied:
1. the content, $c_{\boldsymbol{\theta}_{\mathcal{H}}}$, of $\boldsymbol{\theta}_{\mathcal{H}}$ in $K[A]$ is invertible in $K[A]$, and
2. for every $M \in \mathcal{F}_{\mathcal{H}}(\mathcal{O})$ and each $\mathbf{a} \in A(\mathcal{O}_M)$ we have that if there exists a K-homomorphism, $\tau \colon C \to \tilde{K}$, such that $\tau(\mathbf{x}) = \mathbf{a}$ and $\mathcal{O}_M \models \tau(\theta_L)$, where L is the fixed field of $D_M(\tau)$ in $K(C)$, then for every

K-homomorphism, $\tau'\colon C \to \tilde{K}$, such that $\tau'(\mathbf{x}) = \mathbf{a}$ we have $\mathcal{O}_M \models \tau'(\theta_{L'})$, where L' is the fixed field of $D_M(\tau')$ in $K(C)$.

Alternatively, $(C/A, \boldsymbol{\theta}_{\mathcal{H}})$ is compatible iff $c_{\boldsymbol{\theta}_{\mathcal{H}}}$ is invertible in $K[A]$ and for every $M \in \mathcal{F}_{\mathcal{H}}(\mathcal{O})$ and each $\mathbf{a} \in A(\mathcal{O}_M)$ we have, for $\mathcal{C} = \mathrm{Ar}(A, M, \mathbf{a})$, that

$$\mathcal{O}_M \models \exists Z[p_{\mathcal{C}}(\mathbf{a}, Z) = 0 \wedge \varphi_{\mathcal{C}}(\mathbf{a}, Z)]$$
$$\Rightarrow \mathcal{O}_M \models \forall Z[p_{\mathcal{C}}(\mathbf{a}, Z) = 0 \to \varphi_{\mathcal{C}}(\mathbf{a}, Z)]\,.$$

(Alternatively, $\mathcal{O}_M \models \eta_{\mathcal{C}}(\mathbf{a})$, where $\eta_{\mathcal{C}}(\mathbf{X})$ is the formula

$$\exists Z[p_{\mathcal{C}}(\mathbf{X}, Z) = 0 \wedge \varphi_{\mathcal{C}}(\mathbf{X}, Z)] \to \forall Z[p_{\mathcal{C}}(\mathbf{X}, Z) = 0 \to \varphi_{\mathcal{C}}(\mathbf{X}, Z)]\,.)$$

Remark 3.6. If $(C/A, \boldsymbol{\theta}_{\mathcal{H}})$ is a compatible cover-sentence pair, then for every $M \in \mathcal{F}_{\mathcal{H}}(\mathcal{O})$ and each $\mathbf{a} \in A(\mathcal{O}_M)$ we have

$$(C/A, M, \mathbf{a}) \not\models \boldsymbol{\theta}_{\mathcal{H}} \Leftrightarrow (C/A, M, \mathbf{a}) \models \neg\boldsymbol{\theta}_{\mathcal{H}}\,.$$

Indeed, Let $\mathcal{C} = \mathrm{Ar}(A, M, \mathbf{a})$. Then, in the notations of Definition 3.5,

$$\begin{aligned}(C/A, M, \mathbf{a}) \not\models \boldsymbol{\theta}_{\mathcal{H}} &\Leftrightarrow \mathcal{O}_M \not\models \exists Z[\,p_{\mathcal{C}}(\mathbf{a}, Z) = 0 \wedge \varphi_{\mathcal{C}}(\mathbf{a}, Z)] \\ &\Leftrightarrow \mathcal{O}_M \not\models \forall Z[\,p_{\mathcal{C}}(\mathbf{a}, Z) = 0 \to \varphi_{\mathcal{C}}(\mathbf{a}, Z)] \\ &\Leftrightarrow \mathcal{O}_M \models \exists Z[\,p_{\mathcal{C}}(\mathbf{a}, Z) = 0 \wedge \neg\varphi_{\mathcal{C}}(\mathbf{a}, Z)] \\ &\Leftrightarrow (C/A, M, \mathbf{a}) \models \neg\boldsymbol{\theta}_{\mathcal{H}}\,.\end{aligned}$$

Remark 3.7. We interpret the notations in Notation 3.3 and Definition 3.5 in the case $n = 0$. That is, when $A = \mathbb{A}^0$ consists of one point, O, the origin. In this case $K(A) = K$, $C = L$ is a finite Galois extension of K, and for every algebraic extension M of K,

$$\mathrm{Ar}(A, M, O) = \{\mathrm{Gal}(L/L \cap M)^{\sigma} \,|\, \sigma \in \mathrm{Gal}(L/K)\}\,.$$

Hence, $\mathcal{O}[\bar{A}] = \mathcal{O}$ and, for each $K' \in \mathrm{Field}(L/K, \mathcal{H})$, $z_{K'}$ is a primitive element for the extension K'/K which is integral over $\mathcal{O}$ (therefore $z_{K'} \in \mathcal{O}_{K'}$) such that for each $\mathcal{C} \in \mathrm{Conj}(L/K, \mathcal{H})$ and every $K'_1, K'_2 \in \mathrm{Fix}(\mathcal{C})$ there exists $\sigma \in \mathrm{Gal}(L/K)$ which satisfies $K'_2 = \sigma K'_1$ and $z_{K'_2} = \sigma z_{K'_1}$, $\mathcal{O}[C \cap K'] = \mathcal{O}_{K'}$, and $\theta_{K'}$ is a quantifier-free sentence in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}_{K'})$ such that $\theta_{\sigma K'} = \sigma\theta_{K'}$ for each $\sigma \in \mathrm{Gal}(L/K)$ which satisfies $z_{\sigma K'} = \sigma z_{K'}$. For each $\mathcal{C} \in \mathrm{Conj}(L/K, \mathcal{H})$, $p_{\mathcal{C}}$ is a monic polynomial in $\mathcal{O}[Z]$ which satisfies $p_{\mathcal{C}}(Z) = \mathrm{irr}(z_{K'}, K)$ and $\varphi_{\mathcal{C}}(Z)$ is a quantifier-free formula in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$ which satisfies $\varphi_{\mathcal{C}}(z_{K'}) = \theta_{K'}$, for each $K' \in \mathrm{Fix}(\mathcal{C})$.

Let $M \in \mathcal{F}_{\mathcal{H}}(\mathcal{O})$ and let $\mathcal{C} = \{\mathrm{Gal}(L/L \cap M)^{\sigma} \,|\, \sigma \in \mathrm{Gal}(L/K)\}$. Then

$$(C/A, M, O) \models \boldsymbol{\theta}_{\mathcal{H}} \Leftrightarrow \mathcal{O}_M \models \exists Z[\,p_{\mathcal{C}}(Z) = 0 \wedge \varphi_{\mathcal{C}}(Z)]\,.$$

Let $z_1, \ldots, z_m$ be all the roots of $p_{\mathcal{C}}(Z)$ in $\mathcal{O}_M$. Then, if the pair $(C/A, \boldsymbol{\theta}_{\mathcal{H}})$ is compatible, then

$$\mathcal{O}_M \models \bigvee_{i=1}^{m} \varphi_{\mathcal{C}}(z_i) \Leftrightarrow \mathcal{O}_M \models \bigwedge_{i=1}^{m} \varphi_{\mathcal{C}}(z_i)\,.$$

3.8. *Induced Cover-Sentence.*

Definition 3.9. We continue to hold the notations of Notation 3.3 and Definition 3.5.

Let A' be a K-normal basic set contained in A with a generic point $\mathbf{x}'$. Then, the specialization $\mathbf{x} \mapsto \mathbf{x}'$ extends uniquely to a K-homomorphism, τ_0, of $K[A]$ into

$K[A']$. We extend τ_0 further to a homomorphism τ from C into a Galois extension $K(C')$ of $K(A')$, where $C' = \tau(C)$. Then, C'/A' is a Galois ring/set cover and τ induces an isomorphism $\tau^*\colon \mathrm{Gal}(C'/A') \to D(\tau)$ such that $\tau(\tau^*(\sigma)(u)) = \sigma(\tau(u))$ for each $\sigma \in \mathrm{Gal}(C'/A')$ and each $u \in C$ (Remark 1.21 e)). Let E_τ be the fixed field of $D(\tau)$ in $K(C)$.

For each subextension L' of $K(C')/K(A')$, there is a unique subextension L of $K(C)/E_\tau$ such that $\tau^*(\mathrm{Gal}(K(C')/L')) = \mathrm{Gal}(K(C)/L)$ (hence $\tau(C \cap L) = C' \cap L'$ and $[L' : K(A')] = [L : E_\tau]$). We denote $z'_{L'} = \tau(z_L)$ and, if $L' \in \mathrm{Field}(C'/A', \mathcal{H})$, we denote $\theta'_{L'} = \tau(\theta_L)$ ($L' \in \mathrm{Field}(C'/A', \mathcal{H})$ implies $L \in \mathrm{Field}(C/A, \mathcal{H})$). Then, $z'_{L'}$ is integral over $\mathcal{O}[\bar{A}'] = \mathcal{O}[\mathbf{x}']$ (because z_L is integral over $\mathcal{O}[\mathbf{x}]$),

$$C' \cap L' = \tau(C \cap L) = \tau(K[\mathbf{x}, z_L]) = K[\mathbf{x}', z'_{L'}] = K[A'][z'_{L'}]\,,$$

$p_{\mathcal{C}}(\mathbf{x}', z'_{L'}) = 0$ and, if $L' \in \mathrm{Field}(C'/A', \mathcal{H})$, then $\theta'_{L'} = \varphi_{\mathcal{C}}(\mathbf{x}', z'_{L'})$, where $\mathcal{C}$ is the conjugacy class of $\mathrm{Gal}(C/A)$ which satisfies $L \in \mathrm{Fix}(\mathcal{C})$.

Since the discriminant, d_L, of z_L over $K(A)$ is invertible in $K[A]$, it follows that the discriminant, d'_L, of z_L over E_τ is invertible in $C \cap E_\tau$ (Remark 1.14). Hence, the discriminant, $d'_{L'} = \tau(d'_L)$, of $z'_{L'}$ over $K(A')$ is invertible in $K[A']$. Therefore, $z'_{L'}$ is an $\mathcal{O}[\bar{A}']$-integral primitive element for the ring/set cover $(C' \cap L')/A'$.

Let $\mathcal{O}[C' \cap L'] = \mathcal{O}[\mathbf{x}', z'_{L'}]$ be the ring of integers of $C' \cap L'$. Then, if $L' \in \mathrm{Field}(C'/A', \mathcal{H})$, then $\theta'_{L'}$ is a quantifier-free sentence in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}[C' \cap L'])$.

Let $\mathcal{C}'$ be the conjugacy class of $\mathrm{Gal}(C'/A')$ which satisfies that $L' \in \mathrm{Fix}(\mathcal{C}')$ (hence $\tau^*(\mathcal{C}') \subseteq \mathcal{C}$). We say that $\mathcal{C}'$ is **induced by τ from $\mathcal{C}$**. Note that if $L'_1, L'_2 \in \mathrm{Fix}(\mathcal{C}')$, then the corresponding $L_1, L_2 \in \mathrm{Fix}(\mathcal{C})$ are conjugate by an element of $D(\tau)$. Thus, there exists $\sigma \in \mathrm{Gal}(C'/A')$ which satisfies $L_2 = \tau^*(\sigma)L_1$ and $z_{L_2} = \tau^*(\sigma)z_{L_1}$. Therefore $L'_2 = \sigma L'_1$ and

$$z'_{L'_2} = z'_{\sigma L'_1} = \tau(z_{\tau^*(\sigma)L_1}) = \tau(z_{L_2}) = \tau(\tau^*(\sigma)(z_{L_1})) = \sigma(\tau(z_{L_1})) = \sigma z'_{L'_1}\,,$$

since $\tau(\tau^*(\sigma)(C \cap L_1)) = \sigma(\tau(C \cap L_1)) = \sigma(C' \cap L'_1)$. Hence, if $\mathcal{C}' \in \mathrm{Conj}(C'/A', \mathcal{H})$, then also $\theta'_{L'_2} = \sigma\theta'_{L'_1}$.

Let $p'_{\mathcal{C}'}$ be a polynomial in $\mathcal{O}[\mathbf{X}, Z]$ which satisfies that $p'_{\mathcal{C}'}(\mathbf{x}', Z)$ is a multiple of $\mathrm{irr}(z'_{L'}, K(\mathbf{x}'))$ by an invertible element of $K[A']$. Then, since $p_{\mathcal{C}}(\mathbf{x}', z'_{L'}) = 0$, it follows that $p'_{\mathcal{C}'}(\mathbf{x}', Z) \,|\, p_{\mathcal{C}}(\mathbf{x}', Z)$ in $K[A'][Z]$ (because $\mathrm{irr}(z_L, K(\mathbf{x})) \in K[A][Z]$ and $\mathrm{irr}(z'_{L'}, K(\mathbf{x}')) \in K[A'][Z]$). If $\mathcal{C}' \subseteq \mathcal{H}$, we let $\varphi'_{\mathcal{C}'}(\mathbf{X}, Z)$ be the formula $\varphi_{\mathcal{C}}(\mathbf{X}, Z)$ (note that if $\mathcal{C}' \subseteq \mathcal{H}$, then $\mathcal{C} \subseteq \mathcal{H}$).

We get, in particular, that C'/A' is a complete Galois ring/set cover over K with an $\mathcal{O}[\bar{A}']$-integral primitive element $\mathbf{z}' = (z'_{L'} \,|\, L' \in \mathrm{Field}(C'/A'))$, $\mathcal{O}[C'/A'] = (\mathcal{O}[C' \cap L'] \,|\, L' \in \mathrm{Field}(C'/A'))$ is the corresponding ring of integers, and $\boldsymbol{\theta}'_{\mathcal{H}} = (\theta'_{L'} \,|\, L' \in \mathrm{Field}(C'/A', \mathcal{H}))$ is a quantifier-free sentence in $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}[C'/A', \mathcal{H}])$, where $\mathcal{O}[C'/A', \mathcal{H}] = (\mathcal{O}[C' \cap L'] \,|\, L' \in \mathrm{Field}(C'/A', \mathcal{H}))$.

For each $\mathcal{C}' \in \mathrm{Conj}(C'/A', \mathcal{H})$, let $c_{\theta'_{\mathcal{C}'}} := c_{\theta'_{L'}}$ be the content of $\theta'_{L'}$ in $K[A']$, for $L' \in \mathrm{Fix}(\mathcal{C}')$. Then $c_{\boldsymbol{\theta}'_{\mathcal{H}}} = \prod_{\mathcal{C}' \in \mathrm{Conj}(C'/A', \mathcal{H})} c_{\theta'_{\mathcal{C}'}}$ is the content of $\boldsymbol{\theta}'_{\mathcal{H}}$ in $K[A']$.

For every $M \in \mathcal{F}_{\mathcal{H}}(\mathcal{O})$ and each $\mathbf{a} \in A'(\mathcal{O}_M)$ we write

$$(C'/A', M, \mathbf{a}) \models \boldsymbol{\theta}'_{\mathcal{H}} \Leftrightarrow \mathcal{O}_M \models \exists Z\,[p'_{\mathcal{C}'}(\mathbf{a}, Z) = 0 \wedge \varphi'_{\mathcal{C}'}(\mathbf{a}, Z)]$$

for $\mathcal{C}' = \mathrm{Ar}(A', M, \mathbf{a})$.

We say that the cover-sentence $(C'/A', \boldsymbol{\theta}'_{\mathcal{H}})$ is **induced by τ from** $(C/A, \boldsymbol{\theta}_{\mathcal{H}})$. Also, we say that a cover-sentence $(C'/A', \boldsymbol{\theta}'_{\mathcal{H}})$ is **induced from** $(C/A, \boldsymbol{\theta}_{\mathcal{H}})$ if there

exists a K-homomorphism, $\tau\colon C \to C'$, such that $(C'/A', \boldsymbol{\theta}'_{\mathcal{H}})$ is the cover-sentence which is induced by τ from $(C/A, \boldsymbol{\theta}_{\mathcal{H}})$.

Remark 3.10. Suppose that the cover-sentence pair $(C/A, \boldsymbol{\theta}_{\mathcal{H}})$ is compatible; that is, $c_{\boldsymbol{\theta}_{\mathcal{H}}}$ is invertible in $K[A]$ and, for every $M \in \mathcal{F}_{\mathcal{H}}(\mathcal{O})$ and each $\mathbf{a} \in A(\mathcal{O}_M)$, we have, for $\mathcal{C} = \mathrm{Ar}(A, M, \mathbf{a})$, that $\mathcal{O}_M \models \eta_{\mathcal{C}}(\mathbf{a})$, where

$$\eta_{\mathcal{C}}(\mathbf{X}) : \exists Z[\, p_{\mathcal{C}}(\mathbf{X}, Z) = 0 \wedge \varphi_{\mathcal{C}}(\mathbf{X}, Z)] \to \forall Z[\, p_{\mathcal{C}}(\mathbf{X}, Z) = 0 \to \varphi_{\mathcal{C}}(\mathbf{X}, Z)]\,.$$

Then

a) *$c_{\boldsymbol{\theta}'_{\mathcal{H}}}$ is invertible in $K[A']$.*
Indeed, let $\mathcal{C}' \in \mathrm{Conj}(C'/A', \mathcal{H})$. We shall show that $c_{\theta'_{\mathcal{C}'}}$ is invertible in $K[A']$. Let $\mathcal{C}$ be the conjugacy class of $\mathrm{Gal}(C/A)$ which satisfies that $\mathcal{C}'$ is induced by τ from $\mathcal{C}$, and let $c_{\theta_{\mathcal{C}}}$ be the content of θ_L in $K[A]$, for $L \in \mathrm{Fix}(\mathcal{C})$. Let $L' \in \mathrm{Fix}(\mathcal{C}')$ and $L \in \mathrm{Fix}(\mathcal{C})$ be such that $\tau(L) = L'$. Since $c_{\theta_{\mathcal{C}}}$ is invertible in $K[A]$, it follows that $\tau(c_{\theta_{\mathcal{C}}})$ is invertible in $K[A'] = \tau(K[A])$ and, in particular, that $\tau(c_{\theta_{\mathcal{C}}}) \neq 0$. Hence, since $\theta'_{L'} = \tau(\theta_L)$, it follows that $c_{\theta'_{\mathcal{C}'}} = \tau(c_{\theta_{\mathcal{C}}})$ is invertible in $K[A']$.

b) *The induced cover-sentence (by τ), $(C'/A', \boldsymbol{\theta}'_{\mathcal{H}})$, is also compatible.*
Indeed, it follows from a) that $c_{\boldsymbol{\theta}'_{\mathcal{H}}}$ is invertible in $K[A']$. In addition, let $M \in \mathcal{F}_{\mathcal{H}}(\mathcal{O})$ and $\mathbf{a} \in A'(\mathcal{O}_M)$ and denote $\mathcal{C}' = \mathrm{Ar}(A', M, \mathbf{a})$ and

$\eta'_{\mathcal{C}'}(\mathbf{X})$:
$\exists Z[\, p'_{\mathcal{C}'}(\mathbf{X}, Z) = 0 \wedge \varphi'_{\mathcal{C}'}(\mathbf{X}, Z)] \to \forall Z[\, p'_{\mathcal{C}'}(\mathbf{X}, Z) = 0 \to \varphi'_{\mathcal{C}'}(\mathbf{X}, Z)]\,.$

We have to show that $\mathcal{O}_M \models \eta'_{\mathcal{C}'}(\mathbf{a})$. Indeed, the conjugacy class $\mathcal{C} = \mathrm{Ar}(A, M, \mathbf{a})$ of $\mathrm{Gal}(C/A)$ satisfies that $\tau^*(\mathcal{C}') \subseteq \mathcal{C}$ (Remark 1.21 e)); hence $\mathcal{C}'$ is the conjugacy class of $\mathrm{Gal}(C'/A')$ which is induced by τ from $\mathcal{C}$. Therefore, $\varphi'_{\mathcal{C}'}(\mathbf{X}, Z)$ is the formula $\varphi_{\mathcal{C}}(\mathbf{X}, Z)$.
Suppose that $\mathcal{O}_M \models \exists Z[\, p'_{\mathcal{C}'}(\mathbf{a}, Z) = 0 \wedge \varphi_{\mathcal{C}}(\mathbf{a}, Z)]$. Then, since

$$p'_{\mathcal{C}'}(\mathbf{a}, Z) | p_{\mathcal{C}}(\mathbf{a}, Z) \text{ in } M[Z]$$

(because $p'_{\mathcal{C}'}(\mathbf{x}', Z) | p_{\mathcal{C}}(\mathbf{x}', Z)$ in $K[A'][Z]$), it follows that we have also $\mathcal{O}_M \models \exists Z[\, p_{\mathcal{C}}(\mathbf{a}, Z) = 0 \wedge \varphi_{\mathcal{C}}(\mathbf{a}, Z)]$. Hence, since $(C/A, \boldsymbol{\theta}_{\mathcal{H}})$ is compatible, it follows that $\mathcal{O}_M \models \forall Z[\, p_{\mathcal{C}}(\mathbf{a}, Z) = 0 \to \varphi_{\mathcal{C}}(\mathbf{a}, Z)]$. Therefore, again, since $p'_{\mathcal{C}'}(\mathbf{a}, Z) | p_{\mathcal{C}}(\mathbf{a}, Z)$ in $M[Z]$, it follows that $\mathcal{O}_M \models \forall Z[\, p'_{\mathcal{C}'}(\mathbf{a}, Z) = 0 \to \varphi_{\mathcal{C}}(\mathbf{a}, Z)]$. Thus, $\mathcal{O}_M \models \eta'_{\mathcal{C}'}(\mathbf{a})$, as required.

c) *Let $M \in \mathcal{F}_{\mathcal{H}}(\mathcal{O})$ and $\mathbf{a} \in A'(\mathcal{O}_M)$. Then*

$$(C'/A', M, \mathbf{a}) \models \boldsymbol{\theta}'_{\mathcal{H}} \Leftrightarrow (C/A, M, \mathbf{a}) \models \boldsymbol{\theta}_{\mathcal{H}}\,.$$

Indeed, let $\mathcal{C}' = \mathrm{Ar}(A', M, \mathbf{a})$ and $\mathcal{C} = \mathrm{Ar}(A, M, \mathbf{a})$. Then

$$\begin{aligned}(C'/A', M, \mathbf{a}) \models \boldsymbol{\theta}'_{\mathcal{H}} &\Leftrightarrow \mathcal{O}_M \models \exists Z[\, p'_{\mathcal{C}'}(\mathbf{a}, Z) = 0 \wedge \varphi_{\mathcal{C}}(\mathbf{a}, Z)] \\ &\Rightarrow \mathcal{O}_M \models \exists Z[\, p_{\mathcal{C}}(\mathbf{a}, Z) = 0 \wedge \varphi_{\mathcal{C}}(\mathbf{a}, Z)] \\ &\Leftrightarrow (C/A, M, \mathbf{a}) \models \boldsymbol{\theta}_{\mathcal{H}}\,.\end{aligned}$$

Conversely, since the pair $(C/A, \boldsymbol{\theta}_{\mathcal{H}})$ is compatible and

$$\mathcal{O}_M \models \exists Z[\, p'_{\mathcal{C}'}(\mathbf{a}, Z) = 0]$$

(see Definition 3.5 a)),

$$\begin{aligned}(C/A, M, \mathbf{a}) \models \boldsymbol{\theta}_{\mathcal{H}} &\Leftrightarrow \mathcal{O}_M \models \exists Z[\, p_{\mathcal{C}}(\mathbf{a}, Z) = 0 \wedge \varphi_{\mathcal{C}}(\mathbf{a}, Z)] \\ &\Rightarrow \mathcal{O}_M \models \forall Z[\, p_{\mathcal{C}}(\mathbf{a}, Z) = 0 \to \varphi_{\mathcal{C}}(\mathbf{a}, Z)] \\ &\Rightarrow \mathcal{O}_M \models \forall Z[\, p'_{\mathcal{C}'}(\mathbf{a}, Z) = 0 \to \varphi_{\mathcal{C}}(\mathbf{a}, Z)] \\ &\Rightarrow \mathcal{O}_M \models \exists Z[\, p'_{\mathcal{C}'}(\mathbf{a}, Z) = 0 \wedge \varphi_{\mathcal{C}}(\mathbf{a}, Z)] \\ &\Leftrightarrow (C'/A', M, \mathbf{a}) \models \boldsymbol{\theta}'_{\mathcal{H}}\,.\end{aligned}$$

3.3. **Cover-Sentence under Projection.** We continue the conventions of Subsection 3.2. Let $n \geq 0$ and let $\pi : \mathbb{A}^{n+1} \to \mathbb{A}^n$ be the projection into the first n coordinates. If $n = 0$, then π maps each point of $\mathbb{A}^1$ onto the point, O, of $\mathbb{A}^0$.

Suppose that $A \subseteq \mathbb{A}^{n+1}$ and $B \subseteq \mathbb{A}^n$ are two K-normal basic sets such that $\pi(A) = B$. Suppose also that C/A is a complete Galois ring/set cover over K and $\boldsymbol{\theta}_{\mathcal{H}}$ is a quantifier-free sentence in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}[C/A, \mathcal{H}])$, where $\mathcal{H}$ is a family of finite groups. We shall now construct nonempty K-open subsets A', B' and C' of A, B and C, respectively, a complete Galois ring/set cover D/B' over K, and a quantifier-free sentence $\boldsymbol{\chi}_{\mathcal{H}}$ in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}[D/B', \mathcal{H}])$ such that the pair $(D/B', \boldsymbol{\chi}_{\mathcal{H}})$ is compatible and, for every $M \in \mathcal{F}_{\mathcal{H}}(\mathcal{O})$ and each $\mathbf{b} \in B'(\mathcal{O}_M)$, the following holds: $(D/B', M, \mathbf{b}) \models \boldsymbol{\chi}_{\mathcal{H}}$ if and only if there exists $\mathbf{a} \in A'(\mathcal{O}_M)$ such that $\pi(\mathbf{a}) = \mathbf{b}$ and $(C'/A', M, \mathbf{a}) \models \boldsymbol{\theta}_{\mathcal{H}}$. There are two cases: either $\dim(A) = \dim(B)+1$ or $\dim(A) = \dim(B)$. Lemmas 3.12 and 3.15 treat the first case, Lemma 3.17 the second.

Notation 3.11. Let $A \subseteq \mathbb{A}^{n+1}$ and $B \subseteq \mathbb{A}^n$ be two K-normal basic sets such that $\pi(A) = B$. Let C/A be a complete Galois ring/set cover over K with an $\mathcal{O}[\bar{A}]$-integral primitive element $\mathbf{z}$ and with a corresponding ring of integers $\mathcal{O}[C/A]$, and let $\boldsymbol{\theta}_{\mathcal{H}}$ be a quantifier-free sentence in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}[C/A, \mathcal{H}])$ with a content polynomial $h_{\boldsymbol{\theta}_{\mathcal{H}}} \in \mathcal{O}[X_1, \ldots, X_n, Y]$, where $\mathcal{H}$ is a family of finite groups. We assume that $K(A) = K(B)(y)$, where y is a transcendental element over $K(B)$. Let L be the algebraic closure of $K(B)$ in $K(C)$. Also, let z be a primitive element for the ring cover $C/K[A]$, let $\mathbf{x}$ be a generic point for B, and let $\bar{B}$ be the K-variety generated by $\mathbf{x}$. We assume that $K[B] = K[\mathbf{x}, g_1(\mathbf{x})^{-1}]$ and $K[A] = K[\mathbf{x}, y, g_2(\mathbf{x}, y)^{-1}]$, where $g_1 \in \mathcal{O}[X_1, \ldots, X_n]$ and $g_2 \in \mathcal{O}[X_1, \ldots, X_n, Y]$. We assume, in addition, that $h_{\boldsymbol{\theta}_{\mathcal{H}}}(\mathbf{x}, y)$ (hence also $c_{\boldsymbol{\theta}_{\mathcal{H}}}$) is invertible in $K[A]$.

Lemma 3.12. *In addition to the notations in Notation 3.11, suppose that D/B is a Galois ring/set cover over K such that $L \subseteq K(D)$. Then, there exists a polynomial $h_D \in \mathcal{O}[X_1, \ldots, X_n]$, not vanishing on B, such that if h is a multiple of h_D in $\mathcal{O}[\mathbf{X}]$, then for $C' = C[h(\mathbf{x})^{-1}]$, $A' = A \setminus V(h)$, $D' = D[h(\mathbf{x})^{-1}]$ and $B' = B \setminus V(h)$, we have that the pair $(C'/A', D'/B')$ of Galois ring/set covers is* **specialization compatible**. *That is:*

(1a) *$(D' \cap L)/K[B']$ is a ring cover;*

(1b) *$\pi(A') = B'$; and*

(1c) *Let M be a field extension of K, let y' be a transcendental element over M and let $\varphi\colon C' \to \widetilde{M(y')}$ be a K-homomorphism such that $\varphi(\mathbf{x}) \in B'(M)$ and $\varphi(y) = y'$. Let $N = M[\varphi(D' \cap L)]$ and $F = M(y', \varphi(z))$. Then, $[K(C) : L(y)] = [F : N(y')]$ and N is the algebraic closure of M in F.*

Moreover, in the explicit case, when A, B, C and D are presented, h_D can be computed effectively.

Proof. [FrJ08, p. 711, Lemma 30.2.1]. Let $S = L \cap D$ and find a polynomial $f \in S[Y, Z]$, irreducible over L, such that $f(y, z) = 0$. Since $L(y, z) = K(C)$ is a regular extension of L, $f(Y, Z)$ is absolutely irreducible. The Bertini-Noether theorem [FrJ08, p. 179, Prop. 10.4.2] produces a nonzero element $u \in S$ with this property: if ψ is a homomorphism of S into a field and $\psi(u) \neq 0$, then the polynomial $f^{\psi}(Y, Z)$ is absolutely irreducible and has the same degree in Z as $f(Y, Z)$. Choose $h_D \in \mathcal{O}[X_1, \ldots, X_n]$ so that $h_D(\mathbf{x}) = a g_1(\mathbf{x})^k N_{L/K(B)}(u) \in \mathcal{O}[\mathbf{x}]$ for some $0 \neq a \in \mathcal{O}$ and some integer $k \geq 0$. Further, a multiplication of h_D by an appropriate polynomial in $\mathcal{O}[\mathbf{X}]$ assures that, with D' and B' given in the statement of the lemma, $D' \cap L/K[B']$ is a ring cover (Remark 1.18).

In order to prove that the pair $(C'/A', D'/B')$ of Galois ring/set covers satisfies (1a)–(1c) we have only to check (1c). Indeed, $h_D(\varphi(\mathbf{x})) \neq 0$. Hence, $\varphi(u) \neq 0$ and $f^{\varphi}(Y, Z)$ is absolutely irreducible. Therefore, N is the algebraic closure of M in F and $f^{\varphi}(y', Z)$ is irreducible over $N(y')$. Thus, $[F : N(y')] = \deg_Z f^{\varphi}(y', Z) = \deg_Z f(y, Z) = [K(C) : L(y)]$. □

Definition 3.13. Let $(C/A, \boldsymbol{\theta}_{\mathcal{H}})$ and $(D/B, \boldsymbol{\chi}_{\mathcal{H}})$ be two cover-sentence pairs, in which $A \subseteq \mathbb{A}^{n+1}$ and $B \subseteq \mathbb{A}^n$, C/A and D/B are complete Galois ring/set covers over K with rings of integers $\mathcal{O}[C/A]$ and $\mathcal{O}[D/B]$, respectively, and $\boldsymbol{\theta}_{\mathcal{H}}$ and $\boldsymbol{\chi}_{\mathcal{H}}$ are quantifier-free sentences in the languages $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}[C/A, \mathcal{H}])$ and $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}[D/B, \mathcal{H}])$, respectively. We say that the quadruple

$$(C/A, \boldsymbol{\theta}_{\mathcal{H}}; D/B, \boldsymbol{\chi}_{\mathcal{H}})$$

is **compatible** if the following three conditions are satisfied:

(2a) $\pi(A) = B$;

(2b) the cover-sentence pair $(D/B, \boldsymbol{\chi}_{\mathcal{H}})$ is compatible; and

(2c) for every $M \in \mathcal{F}_{\mathcal{H}}(\mathcal{O})$ and each $\mathbf{b} \in B(\mathcal{O}_M)$ we have $(D/B, M, \mathbf{b}) \models \boldsymbol{\chi}_{\mathcal{H}}$ iff there exists $\mathbf{a} \in A(\mathcal{O}_M)$ such that $\pi(\mathbf{a}) = \mathbf{b}$ and $(C/A, M, \mathbf{a}) \models \boldsymbol{\theta}_{\mathcal{H}}$.

Notation 3.14. Let F/E be a Galois extension and let L' be a subfield of F which satisfies that $L'/L' \cap E$ is a Galois extension. For a collection $\mathcal{D}$ of subgroups of $\mathrm{Gal}(F/E)$ we denote the collection of all groups obtained by restricting elements of $\mathcal{D}$ to L' by $\mathrm{res}_{L'}\mathcal{D}$.

Lemma 3.15. *Let $(C/A, \boldsymbol{\theta}_{\mathcal{H}})$ and B be as in the notations of Notation 3.11. Then, there exists a finite seperable extension P of $K(B)$ such that, for any finite Galois extension Q of $K(B)$ which contains P, for every complete Galois ring/set cover D_0/B_0 over K in which $B_0 = B \smallsetminus V(h_0)$ ($h_0 \in \mathcal{O}[\mathbf{X}]$) is a nonempty K-open subset of B and $K(D_0) = Q$, and for each $\mathcal{O}[\bar{B}]$-integral primitive element $\mathbf{w}$ for the ring/set cover D_0/B_0 with a corresponding ring of integers $\mathcal{O}[D_0/B_0]$, there exist*

(3a) *a quantifier-free sentence $\boldsymbol{\chi}_{\mathcal{H}}$ in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}[D_0/B_0, \mathcal{H}])$, and*

(3b) *a multiple h of h_0 in $\mathcal{O}[\mathbf{X}]$ such that $h(\mathbf{x}) \neq 0$,*

and for $B' = B \smallsetminus V(h)$, $A' = A \smallsetminus V(h)$, $C' = C[h(\mathbf{x})^{-1}]$ and $D = D_0[h(\mathbf{x})^{-1}]$, the quadruple $(C'/A', \boldsymbol{\theta}_{\mathcal{H}}; D/B', \boldsymbol{\chi}_{\mathcal{H}})$ of two cover-sentence pairs is compatible.

Moreover, in the explicit case, when A, B, C, $\mathcal{H}$ and $\boldsymbol{\theta}_{\mathcal{H}}$ are presented, P can be effectively computed, and if also Q and $\mathbf{w}$ are presented, then $\boldsymbol{\chi}_{\mathcal{H}}$ and h can be also computed effectively.

Proof. For each conjugacy class $\mathcal{C}$ in $\mathrm{Conj}(C/A,\mathcal{H})$, let $\varphi_{\mathcal{C}}(\mathbf{X},Y,Z)$ be the quantifier-free formula in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$ which satisfies that $\theta_{L'}=\varphi_{\mathcal{C}}(\mathbf{x},y,z_{L'})$ and let $p_{\mathcal{C}}\in\mathcal{O}[\mathbf{X},Y,Z]$ be a polynomial such that $p_{\mathcal{C}}(\mathbf{x},y,Z)$ is a multiple of $\mathrm{irr}(z_{L'},K(\mathbf{x},y))$ by an invertible element of $K[A]$, for each $L'\in\mathrm{Fix}(\mathcal{C})$. Let $\psi_{\mathcal{C}}(\mathbf{X})$ be the formula

$$\exists Y\exists Z[\,g_2(\mathbf{X},Y)\neq 0\wedge p_{\mathcal{C}}(\mathbf{X},Y,Z)=0\wedge\varphi_{\mathcal{C}}(\mathbf{X},Y,Z)]\,.$$

Let L be field as in Notation 3.11. For each conjugacy class $\mathcal{D}_L$ in $\mathrm{Conj}(L/K(B))$ we denote

$$\mathrm{Conj}_{\mathcal{D}_L}(C/A,\mathcal{H})=\{\mathcal{C}\in\mathrm{Conj}(C/A,\mathcal{H})|\,\mathrm{res}_L\mathcal{C}=\mathcal{D}_L\}$$

and

$$\psi_{\mathcal{D}_L}(\mathbf{X}):=\bigvee_{\mathcal{C}\in\mathrm{Conj}_{\mathcal{D}_L}(C/A,\mathcal{H})}\psi_{\mathcal{C}}(\mathbf{X})\,.$$

If $\mathrm{Conj}_{\mathcal{D}_L}(C/A,\mathcal{H})=\emptyset$, we let $\psi_{\mathcal{D}_L}=\psi_{\mathcal{D}_L}(\mathbf{X})$ be some false sentence in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$. Then, Proposition 2.26 gives a finite Galois extension $P_{\mathcal{D}_L}$ of $K(\mathbf{x})$ and a polynomial $h_{\psi_{\mathcal{D}_L}}$, which does not vanish on $\bar{B}$, such that the pair $(\psi_{\mathcal{D}_L},\bar{B})$ is solvable by the pair $(P_{\mathcal{D}_L},h_{\psi_{\mathcal{D}_L}})$. This proposition allows us to eliminate the quantifiers $\exists Y\,\exists Z$ and to replace them by an "algebraic" quantifier $\exists W$ in the following way.

Let P be the compositum of L with all the $P_{\mathcal{D}_L}$'s and let $h_{\boldsymbol{\psi}}$ be a common multiple of all the $h_{\psi_{\mathcal{D}_L}}$'s in $\mathcal{O}[\mathbf{X}]$, for $\mathcal{D}_L\in\mathrm{Conj}(L/K(B))$. Now, let Q be a finite Galois extension of $K(B)$ which contains P and let D_0/B_0 be a complete Galois ring/set cover such that $B_0=B\smallsetminus V(h_0)$, where $h_0\in\mathcal{O}[\mathbf{X}]$ is a polynomial which does not vanish on $\bar{B}$, and $K(D_0)=Q$. Let $\mathbf{w}$ be an $\mathcal{O}[\mathbf{x}]$-integral primitive element for the ring/set cover D_0/B_0 and let $\mathcal{O}[D_0/B_0]$ be the corresponding ring of integers. For each conjugacy class $\mathcal{D}$ in $\mathrm{Conj}(D_0/B_0,\mathcal{H})$, let $q_{\mathcal{D}}\in\mathcal{O}[\mathbf{X},W]$ be a polynomial which satisfies that $q_{\mathcal{D}}(\mathbf{x},W)$ is a multiple of $\mathrm{irr}(w_{L'},K(\mathbf{x}))$ by an invertible element of $K[B_0]$, for each $L'\in\mathrm{Fix}(\mathcal{D})$. By assumption, D_0/B_0 is a complete Galois ring/set cover over K; in particular, the discriminant of $w_{L'}$ over $K(B_0)$ is invertible in $K[B_0]$.

For each $\mathcal{D}\in\mathrm{Conj}(D_0/B_0,\mathcal{H})$, Proposition 2.26 gives a quantifier-free formula $\overline{\psi}_{\mathcal{D}}(\mathbf{X},W)$ in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$ such that, if $h\in\mathcal{O}[\mathbf{X}]$ is a common multiple of h_0 and $h_{\boldsymbol{\psi}}$, then, for $B'=B\smallsetminus V(h)$ and $D=D_0[h(\mathbf{x})^{-1}]$, the pair $(q_{\mathcal{D}},\overline{\psi}_{\mathcal{D}})$ is a solution for the triple $(\psi_{\mathcal{D}_L},D/B',\mathcal{D})$, where $\mathcal{D}_L=\mathrm{res}_L\mathcal{D}$. For each $L'\in\mathrm{Fix}(\mathcal{D})$ we denote the quantifier-free sentence $\overline{\psi}_{\mathcal{D}}(\mathbf{x},w_{L'})$ in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}[D_0\cap L'])$ by $\chi_{L'}$. Then $\boldsymbol{\chi}_{\mathcal{H}}=(\chi_{L'}\,|\,L'\in\mathrm{Field}(D_0/B_0,\mathcal{H}))$ is a quantifier-free sentence in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}[D_0/B_0,\mathcal{H}])$. Let $h_{\boldsymbol{\chi}_{\mathcal{H}}}\in\mathcal{O}[\mathbf{X}]$ be a content polynomial of $\boldsymbol{\chi}_{\mathcal{H}}$, let $h_{D_0}\in\mathcal{O}[\mathbf{X}]$ be the polynomial that Lemma 3.12 gives, and let $h\in\mathcal{O}[\mathbf{X}]$ be a common multiple of h_0, $h_{\boldsymbol{\psi}}$, $h_{\boldsymbol{\chi}_{\mathcal{H}}}$ and h_{D_0}. We denote $B'=B\smallsetminus V(h)$, $D=D_0[h(\mathbf{x})^{-1}]$, $A'=A\smallsetminus V(h)$ and $C'=C[h(\mathbf{x})^{-1}]$. Then, in particular, $h_{\boldsymbol{\chi}_{\mathcal{H}}}(\mathbf{x})$ (hence also $c_{\boldsymbol{\chi}_{\mathcal{H}}}$) is invertible in $K[B']$ and the pair $(C'/A',D/B')$ is specialization compatible. Also, for every $M\in\mathcal{F}_{\mathcal{H}}(\mathcal{O})$ and each $\mathbf{b}\in B'(\mathcal{O}_M)$, we have, for $\mathcal{D}=\mathrm{Ar}(D/B',M,\mathbf{b})$, that

$$\begin{aligned}(4)\qquad \mathcal{O}_M\models\psi_{\mathcal{D}_L}(\mathbf{b})&\Leftrightarrow\mathcal{O}_M\models\exists W[\,q_{\mathcal{D}}(\mathbf{b},W)=0\wedge\overline{\psi}_{\mathcal{D}}(\mathbf{b},W)]\\&\Leftrightarrow(D/B',M,\mathbf{b})\models\boldsymbol{\chi}_{\mathcal{H}}\end{aligned}$$

and $\mathcal{O}_M\models\exists W[\,q_{\mathcal{D}}(\mathbf{b},W)=0\wedge\overline{\psi}_{\mathcal{D}}(\mathbf{b},W)]\Leftrightarrow\mathcal{O}_M\models\forall W[\,q_{\mathcal{D}}(\mathbf{b},W)=0\rightarrow\overline{\psi}_{\mathcal{D}}(\mathbf{b},W)]$. In particular, the pair $(D/B',\boldsymbol{\chi}_{\mathcal{H}})$ is compatible. It remains to check that (2c) is satisfied for the pairs $(C'/A',\boldsymbol{\theta}_{\mathcal{H}})$ and $(D/B',\boldsymbol{\chi}_{\mathcal{H}})$.

Let $M \in \mathcal{F}_{\mathcal{H}}(\mathcal{O})$ and $\mathbf{b} \in B'(\mathcal{O}_M)$.
Suppose first that there is $\mathbf{a} \in A'(\mathcal{O}_M)$ such that

$$\pi(\mathbf{a}) = \mathbf{b} \text{ and } (C'/A', M, \mathbf{a}) \models \boldsymbol{\theta}_{\mathcal{H}}\,.$$

That is, for $\mathcal{C} = \mathrm{Ar}(A', M, \mathbf{a})$, we have $\mathcal{O}_M \models \exists Z[\, p_{\mathcal{C}}(\mathbf{a}, Z) = 0 \wedge \varphi_{\mathcal{C}}(\mathbf{a}, Z)]\,$. In particular,

$$\mathcal{O}_M \models \psi_{\mathcal{C}}(\mathbf{b})\,. \tag{5}$$

Let φ be a K-homomorphism of C' into $\tilde{M}$ such that $\varphi(\mathbf{x}, y) = \mathbf{a}$. By Remark 1.21 c), $\mathrm{res}_{L(y)}(D_M(\varphi)) = D_M(\mathrm{res}_{L(y)}\varphi)$. Also, for $S = D \cap L$, $S \cdot K[A']/K[A']$ is a Galois ring cover and $L(y)$ is the quotient field of $S \cdot K[A']$. Since $M[\varphi(S \cdot K[A'])] = M[\varphi(S)]$, it follows, by comparing degrees, that $\mathrm{res}_L(D_M(\mathrm{res}_{L(y)}\varphi)) = D_M(\mathrm{res}_L\varphi)$. Thus, $\mathrm{res}_L(D_M(\varphi)) = D_M(\mathrm{res}_L\varphi)$. Since $\varphi(\mathbf{x}) = \mathbf{b}$, this implies that $\mathrm{res}_L\mathcal{C} \subseteq \mathrm{Ar}(S/B', M, \mathbf{b})$. Since the left hand side of the inclusion is a conjugacy domain (i.e. closed under a conjugation by elements of $\mathrm{Gal}(L/K(B'))$) and the right hand side is a conjugacy class of subgroups of $\mathrm{Gal}(L/K(B'))$, they are equal. It follows that $\mathrm{res}_L\mathcal{C} = \mathrm{res}_L\mathcal{D}$, where $\mathcal{D} = \mathrm{Ar}(B', M, \mathbf{b})$. If $G \in \mathcal{D}$, then $G \in \mathrm{Im}(\mathrm{Gal}(M)) = \mathcal{H}$. Hence $\mathcal{D} \in \mathrm{Conj}(D/B', \mathcal{H})$. We denote $\mathcal{D}_L = \mathrm{res}_L\mathcal{D}$. Then, since $\mathcal{C} \in \mathrm{Conj}_{\mathcal{D}_L}(C'/A', \mathcal{H})$, it follows from (5) that $\mathcal{O}_M \models \psi_{\mathcal{D}_L}(\mathbf{b})$ and, therefore, by (4), that $(D/B', M, \mathbf{b}) \models \boldsymbol{\chi}_{\mathcal{H}}$.

Now, suppose that $(D/B', M, \mathbf{b}) \models \boldsymbol{\chi}_{\mathcal{H}}$. That is, $\mathcal{O}_M \models \exists W[\, q_{\mathcal{D}}(\mathbf{b}, W) = 0 \wedge \overline{\psi}_{\mathcal{D}}(\mathbf{b}, W)]$, for $\mathcal{D} = \mathrm{Ar}(B', M, \mathbf{b})$. In particular, it follows from (4) that there exists $\mathcal{C} \in \mathrm{Conj}(C'/A', \mathcal{H})$ such that $\mathrm{res}_L\mathcal{C} = \mathrm{res}_L\mathcal{D}$ and $\mathcal{O}_M \models \psi_{\mathcal{C}}(\mathbf{b})$.

The existence of $\mathbf{a} \in A'(\mathcal{O}_M)$ such that $\pi(\mathbf{a}) = \mathbf{b}$ and $(C'/A', M, \mathbf{a}) \models \boldsymbol{\theta}_{\mathcal{H}}$ hold falls into two parts.

PART A: *Specialization of* $(\mathbf{x}, y)$ *to a point of transcendence degree* 1 *over* M. Without loss assume that $K(D) = L$. Take a transcendental element y' over M and extend the specialization $\mathbf{x} \to \mathbf{b}$ to a K-homomorphism φ of C' into the algebraic closure of $M(y')$ such that $\varphi(y) = y'$. Recall that $K[A'] = K[\mathbf{x}, y, (h(\mathbf{x})g_2(\mathbf{x}, y))^{-1}]$. Since $\pi(A') = B'$, we have $h(\mathbf{b})g_2(\mathbf{b}, y') \neq 0$. Let $z' = \varphi(z)$, $N = M \cdot \varphi(D)$, $R = M[y', g_2(\mathbf{b}, y')^{-1}] = M[\varphi(K[A'])]$, $E = M(y')$ and $F = E(z')$. Then, $R[z']/R$ is a Galois ring cover over M with F/E the corresponding field cover. By the specialization compatibility assumption on $(C'/A', D/B')$, $[F : N(y')] = [K(C) : L(y)]$. Conclude from this that, in the following commutative diagram,

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathrm{Gal}(K(C')/L(y)) & \longrightarrow & \mathrm{Gal}(C'/A') & \xrightarrow{\mathrm{res}} & \mathrm{Gal}(D/B') & \longrightarrow & 1 \\
 & & \uparrow{\scriptstyle \varphi^*} & & \uparrow{\scriptstyle \varphi^*} & & \uparrow{\scriptstyle \varphi^*} & & \\
1 & \longrightarrow & \mathrm{Gal}(F/N(y')) & \longrightarrow & \mathrm{Gal}(F/E) & \xrightarrow{\mathrm{res}} & \mathrm{Gal}(N/M) & \longrightarrow & 1
\end{array}$$

the left vertical arrow is an isomorphism.

PART B: *Application of the Frobenius property.* The conjugacy class $\mathcal{D} = \mathrm{Ar}(B', M, \mathbf{b})$ is generated by $\varphi^*(\mathrm{Gal}(N/M))$. Since $L = K(D)$ and $\varphi^*(\mathrm{Gal}(N/M)) \in \mathcal{D}$, it follows that there exists $H \in \mathcal{C}$ such that $\mathrm{res}_{K(D)}H = \varphi^*(\mathrm{Gal}(N/M))$. Note that $H \in \mathcal{H}$ (because $\mathcal{C} \in \mathrm{Conj}(C'/A', \mathcal{H})$); hence $H \in \mathrm{Im}(\mathrm{Gal}(M))$. The commutativity of the diagram in Part A shows that $\mathrm{res}_{K(D)}(\varphi^*(\mathrm{Gal}(F/E)) = \varphi^*(\mathrm{Gal}(N/M))$. Since the left vertical arrow is surjective, $H \leq \varphi^*(\mathrm{Gal}(F/E))$. Hence, there exists a subgroup H' of $\mathrm{Gal}(F/E)$ such that $\varphi^*(H') = H$. As all the maps denoted by φ^* are injective, conclude that $H' \in \mathrm{Im}(\mathrm{Gal}(M))$ and $\mathrm{res}_N H' = \mathrm{Gal}(N/M)$. Also, by (1c), N is the algebraic closure of M in F.

Let $L' \in \mathrm{Fix}(\mathcal{C})$ be the fixed field of H in $K(C)$, and let $c_{\theta_{L'}}$ be the content of $\theta_{L'}$ in $K[A']$. Since $\mathcal{O}_M \models \psi_{\mathcal{C}}(\mathbf{b})$, it follows that there exist elements $\bar{y}, \bar{z} \in \mathcal{O}_M$

which satisfy $g_2(\mathbf{b},\bar{y}) \neq 0$, $p_{\mathcal{C}}(\mathbf{b},\bar{y},\bar{z}) = 0$ and $\varphi_{\mathcal{C}}(\mathbf{b},\bar{y},\bar{z})$. Hence, there exists an M-homomorphism, $\tau\colon R[z'] \to \tilde{K}$, such that $\tau(y') \in \mathcal{O}_M$, $\tau(z_{L'}) \in \mathcal{O}_M$ and $\mathcal{O}_M \models \tau(\varphi(\theta_{L'}))$. Also, since $h_{\boldsymbol{\theta}_{\mathcal{H}}}(\mathbf{x},y)$ is invertible in $K[A]$ (this is one of the assumptions in Notation 3.11), it follows that $\tau(\varphi(h_{\boldsymbol{\theta}_{\mathcal{H}}}(\mathbf{x},y))) \neq 0$. Hence, $\tau(\varphi(c_{\theta_{L'}})) \neq 0$; therefore, the content, $c_{\varphi(\theta_{L'})} = \varphi(c_{\theta_{L'}})$, of $\varphi(\theta_{L'})$ in R satisfies $\tau(c_{\varphi(\theta_{L'})}) \neq 0$.

As M is a perfect algebraic extension of K which is Frobenius over $\mathcal{O}_M$, Proposition 3.2 produces an M-epimorphism ψ of $R[z']$ onto a Galois extension F' of M that contains N such that $\psi(y') = c \in \mathcal{O}_M$, $\psi(z_{L'}) \in \mathcal{O}_M$, $\mathcal{O}_M \models \psi(\varphi(\theta_{L'}))$ and $D_M(\psi) = \psi^*(\mathrm{Gal}(F'/M)) = H'$. From the definitions, $\varphi^*(D_M(\psi)) \leq D_M(\psi\circ\varphi)$. But, since both $D_M(\psi\circ\varphi)$ and $D_M(\varphi)$ are isomorphic to $\mathrm{Gal}(F'/M)$,

$$H = \varphi^*(D_M(\psi)) = D_M(\psi\circ\varphi)\,.$$

The point $\mathbf{a} = (\mathbf{b},c) = \psi\circ\varphi(\mathbf{x},y)$ belongs to $A'(\mathcal{O}_M)$ and $\pi(\mathbf{a}) = \mathbf{b}$. Hence, $\mathcal{C} = \mathrm{Ar}(A',M,\mathbf{a})$. Also, since $\mathcal{O}_M \models \psi\circ\varphi(\theta_{L'})$, $\mathcal{O}_M \models \exists Z[p_{\mathcal{C}}(\mathbf{a},Z) = 0 \wedge \varphi_{\mathcal{C}}(\mathbf{a},Z)]$. Thus, $(C'/A',M,\mathbf{a}) \models \boldsymbol{\theta}_{\mathcal{H}}$.

This concludes the lemma. □

Notation 3.16. Let $A \subseteq \mathbb{A}^{n+1}$ and $B \subseteq \mathbb{A}^n$ be two K-normal basic sets such that $\pi(A) = B$ and $K(A)$ is an algebraic extension of $K(B)$. Let $(\mathbf{x},y)$ be a generic point for A, where $\mathbf{x}$ is a generic point for B, and let $\bar{B}$ be the K-variety generated by $\mathbf{x}$. We assume that $K[B] = K[\mathbf{x}, g_1(\mathbf{x})^{-1}]$ and $K[A] = K[\mathbf{x},y,g_2(\mathbf{x},y)^{-1}]$, where $g_1 \in \mathcal{O}[X_1,\ldots,X_n]$ and $g_2 \in \mathcal{O}[X_1,\ldots,X_n,Y]$.

Let C/A be a complete Galois ring/set cover over K with an $\mathcal{O}[\bar{A}]$-integral primitive element $\mathbf{z}$ and with a corresponding ring of integers $\mathcal{O}[C/A]$, and let $\boldsymbol{\theta}_{\mathcal{H}}$ be a quantifier-free sentence in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}[C/A,\mathcal{H}])$, where $\mathcal{H}$ is a family of finite groups. Let E (resp., F) be the maximal separable extension of $K(B)$ in $K(A)$ (resp., $K(C)$). Both extensions $K(A)/E$ and $K(C)/F$ are purely inseparable. Hence $K(A)$ and F are linearly disjoint over E and $K(A)\cdot F = K(C)$ (because $K(C)/K(A)$ is separable). If $\mathrm{char}(K) = p \neq 0$, let q be a power of p such that $K(A)^q \subseteq E$ and $K(C)^q \subseteq F$. Then, $K(C)^q/K(A)^q$ is a Galois extension and $E\cdot K(C)^q = F$ (because F is both separable and purely inseparable over $E\cdot K(C)^q$). Therefore, F/E is also a Galois extension and res: $\mathrm{Gal}(C/A) \to \mathrm{Gal}(F/E)$ is an isomorphism.

Lemma 3.17. *Let $(C/A,\boldsymbol{\theta}_{\mathcal{H}})$ and B be as in the notations of Notation 3.16. Then, there exists a finite separable extension P of $K(B)$ such that, for any finite Galois extension Q of $K(B)$ which contains P, for every complete Galois ring/set cover D_0/B_0 over K in which $B_0 = B\smallsetminus V(h_0)$ ($h_0 \in \mathcal{O}[\mathbf{X}]$) is a nonempty K-open subset of B and $K(D_0) = Q$, and for each $\mathcal{O}[\bar{B}]$-integral primitive element $\mathbf{w}$ for the ring/set cover D_0/B_0 with corresponding ring of integers $\mathcal{O}[D_0/B_0]$, there exist*

(3′a) *a quantifier-free sentence $\boldsymbol{\chi}_{\mathcal{H}}$ in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}[D_0/B_0,\mathcal{H}])$, and*

(3′b) *a multiple h of h_0 in $\mathcal{O}[\mathbf{X}]$ such that $h(\mathbf{x}) \neq 0$,*

and for $B' = B\smallsetminus V(h)$, $A' = A\smallsetminus V(h)$, $C' = C[h(\mathbf{x})^{-1}]$ and $D = D_0[h(\mathbf{x})^{-1}]$, the quadruple $(C'/A',\boldsymbol{\theta}_{\mathcal{H}};D/B',\boldsymbol{\chi}_{\mathcal{H}})$ of two cover-sentence pairs is compatible.

Moreover, in the explicit case, when A, B, C, $\mathcal{H}$ and $\boldsymbol{\theta}_{\mathcal{H}}$ are presented, P can be effectively computed, and if also Q and $\mathbf{w}$ are presented, then $\boldsymbol{\chi}_{\mathcal{H}}$ and h can be also computed effectively.

Proof. Let $\bar{A}$ be the K-variety generated by $(\mathbf{x},y)$ and suppose that

$$\bar{A} = \{(\mathbf{x}',y') \in \mathbb{A}^{n+1} \mid f_1(\mathbf{x}',y') = 0,\ldots,f_m(\mathbf{x}',y') = 0\}\,,$$

where $f_1, \dots, f_m \in \mathcal{O}[\mathbf{X}, Y]$. For each $\mathcal{C} \in \mathrm{Conj}(C/A, \mathcal{H})$, let $\varphi_{\mathcal{C}}(\mathbf{X}, Y, Z)$ be the quantifier-free formula in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$ which satisfies that $\theta_{L'} = \varphi_{\mathcal{C}}(\mathbf{x}, y, z_{L'})$ and let $p_{\mathcal{C}} \in \mathcal{O}[\mathbf{X}, Y, Z]$ be a polynomial which satisfies that $p_{\mathcal{C}}(\mathbf{x}, y, Z)$ is a multiple of $\mathrm{irr}(z_{L'}, K(\mathbf{x}, y))$ by an invertible element of $K[A]$, for each $L' \in \mathrm{Fix}(\mathcal{C})$. Let $\psi_{\mathcal{C}}(\mathbf{X})$ be the formula

$$\exists Y \exists Z [\bigwedge_{i=1}^{m} f_i(\mathbf{X}, Y) = 0 \wedge g_2(\mathbf{X}, Y) \neq 0 \wedge p_{\mathcal{C}}(\mathbf{X}, Y, Z) = 0 \wedge \varphi_{\mathcal{C}}(\mathbf{X}, Y, Z)] .$$

Then, Proposition 2.26 gives a finite Galois extension $P_{\mathcal{C}}$ of $K(\mathbf{x})$ and a polynomial $h_{\psi_{\mathcal{C}}}$, which does not vanish on $\bar{B}$, such that the pair $(\psi_{\mathcal{C}}, \bar{B})$ is solvable by the pair $(P_{\mathcal{C}}, h_{\psi_{\mathcal{C}}})$. Let E and F be as in Notation 3.16.

Let P be the compositum of F with all the $P_{\mathcal{C}}$'s and let $h_{\boldsymbol{\psi}}$ be a common multiple of all the $h_{\psi_{\mathcal{C}}}$'s in $\mathcal{O}[\mathbf{X}]$, for $\mathcal{C} \in \mathrm{Conj}(C/A, \mathcal{H})$. Now, let Q be a finite Galois extension of $K(B)$ which contains P and let D_0/B_0 be a complete Galois ring/set cover such that $B_0 = B \smallsetminus V(h_0)$, where $h_0 \in \mathcal{O}[\mathbf{X}]$ is a polynomial which does not vanish on $\bar{B}$, and $K(D_0) = Q$. Let $\mathbf{w}$ be an $\mathcal{O}[\mathbf{x}]$-integral primitive element for the ring/set cover D_0/B_0 and let $\mathcal{O}[D_0/B_0]$ be the corresponding ring of integers. For each conjugacy class $\mathcal{D}$ in $\mathrm{Conj}(D_0/B_0, \mathcal{H})$, let $q_{\mathcal{D}} \in \mathcal{O}[\mathbf{X}, W]$ be a polynomial which satisfies that $q_{\mathcal{D}}(\mathbf{x}, W)$ is a multiple of $\mathrm{irr}(w_{L'}, K(\mathbf{x}))$ by an invertible element of $K[B_0]$, for each $L' \in \mathrm{Fix}(\mathcal{D})$. By assumption, D_0/B_0 is a complete Galois ring/set cover over K; in particular, the discriminant of $w_{L'}$ over $K(B_0)$ is invertible in $K[B_0]$.

For each $\mathcal{D} \in \mathrm{Conj}(D_0/B_0, \mathcal{H})$, the set $\mathrm{res}_F \mathcal{D}$ contains at most one conjugacy class of $\mathrm{Conj}(F/E)$. If there exists $\mathcal{C} \in \mathrm{Conj}(C/A, \mathcal{H})$ such that $\mathrm{res}_F \mathcal{C} \subseteq \mathrm{res}_F \mathcal{D}$, we let $\psi_{\mathcal{D}}(\mathbf{X})$ be the formula $\psi_{\mathcal{C}}(\mathbf{X})$. Otherwise, we let $\psi_{\mathcal{D}} = \psi_{\mathcal{D}}(\mathbf{X})$ be some false sentence in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$. Then, Proposition 2.26 gives a quantifier-free formula $\overline{\psi}_{\mathcal{D}}(\mathbf{X}, W)$ in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$ such that if $h \in \mathcal{O}[\mathbf{X}]$ is a common multiple of h_0 and $h_{\boldsymbol{\psi}}$, then, for $B' = B \smallsetminus V(h)$ and $D = D_0[h(\mathbf{x})^{-1}]$, the pair $(q_{\mathcal{D}}, \overline{\psi}_{\mathcal{D}})$ is a solution for the triple $(\psi_{\mathcal{D}}, D/B', \mathcal{D})$. For each $L' \in \mathrm{Fix}(\mathcal{D})$, we denote the quantifier-free sentence $\overline{\psi}_{\mathcal{D}}(\mathbf{x}, w_{L'})$ in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}[D_0 \cap L'])$ by $\chi_{L'}$. Then, $\boldsymbol{\chi}_{\mathcal{H}} = (\chi_{L'} \mid L' \in \mathrm{Field}(D_0/B_0, \mathcal{H}))$ is a quantifier-free sentence in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}[D_0/B_0, \mathcal{H}])$.

Let $h_{\boldsymbol{\chi}_{\mathcal{H}}} \in \mathcal{O}[\mathbf{X}]$ be a content polynomial of $\boldsymbol{\chi}_{\mathcal{H}}$, let $h_B \in \mathcal{O}[\mathbf{X}]$ be a polynomial which does not vanish on $\bar{B}$ and satisfies that $K[A][h_B(\mathbf{x})^{-1}]$ is integral over $K[B][h_B(\mathbf{x})^{-1}]$, and let $h \in \mathcal{O}[\mathbf{X}]$ be a common multiple of h_0, $h_{\boldsymbol{\psi}}$, $h_{\boldsymbol{\chi}_{\mathcal{H}}}$ and h_B. we denote $B' = B \smallsetminus V(h)$, $D = D_0[h(\mathbf{x})^{-1}]$, $A' = A \smallsetminus V(h)$ and $C' = C[h(\mathbf{x})^{-1}]$. Then, in particular, $h_{\boldsymbol{\chi}_{\mathcal{H}}}(\mathbf{x})$ (hence also $c_{\boldsymbol{\chi}_{\mathcal{H}}}$) is invertible in $K[B']$ and $K[A']$ is integral over $K[B']$. Also, for every $M \in \mathcal{F}_{\mathcal{H}}(\mathcal{O})$ and each $\mathbf{b} \in B'(\mathcal{O}_M)$, we have, for $\mathcal{D} = \mathrm{Ar}(D/B', M, \mathbf{b})$, that

$$(4') \qquad \begin{aligned} \mathcal{O}_M \models \psi_{\mathcal{D}}(\mathbf{b}) &\Leftrightarrow \mathcal{O}_M \models \exists W [\, q_{\mathcal{D}}(\mathbf{b}, W) = 0 \wedge \overline{\psi}_{\mathcal{D}}(\mathbf{b}, W)] \\ &\Leftrightarrow (D/B', M, \mathbf{b}) \models \boldsymbol{\chi}_{\mathcal{H}} \end{aligned}$$

and $\mathcal{O}_M \models \exists W [\, q_{\mathcal{D}}(\mathbf{b}, W) = 0 \wedge \overline{\psi}_{\mathcal{D}}(\mathbf{b}, W)] \Leftrightarrow \mathcal{O}_M \models \forall W [\, q_{\mathcal{D}}(\mathbf{b}, W) = 0 \to \overline{\psi}_{\mathcal{D}}(\mathbf{b}, W)]$. In particular, the pair $(D/B', \boldsymbol{\chi}_{\mathcal{H}})$ is compatible. It remains to check that (2c) is satisfied for the pairs $(C'/A', \boldsymbol{\theta}_{\mathcal{H}})$ and $(D/B', \boldsymbol{\chi}_{\mathcal{H}})$.

Let $M \in \mathcal{F}_{\mathcal{H}}(\mathcal{O})$ and $\mathbf{b} \in B'(\mathcal{O}_M)$. We denote the integral closure of $K[B']$ in E (resp., F) by R (resp., S). Then $R \subseteq K[A']$ and $S \subseteq C' \cap D$.

Suppose first that there is $\mathbf{a} \in A'(\mathcal{O}_M)$ such that

$$\pi(\mathbf{a}) = \mathbf{b} \text{ and } (C'/A', M, \mathbf{a}) \models \boldsymbol{\theta}_{\mathcal{H}} .$$

That is, for $\mathcal{C} = \mathrm{Ar}(A', M, \mathbf{a})$, we have $\mathcal{O}_M \models \exists Z[\, p_{\mathcal{C}}(\mathbf{a}, Z) = 0 \wedge \varphi_{\mathcal{C}}(\mathbf{a}, Z)]$. In particular,

$$\mathcal{O}_M \models \psi_{\mathcal{C}}(\mathbf{b}) . \tag{5'}$$

Let φ be a K-homomorphism of C' into $\tilde{M}$ such that $\varphi(\mathbf{x}, y) = \mathbf{a}$. Since the restriction $\mathrm{res}_F \colon \mathrm{Gal}(C'/A') \to \mathrm{Gal}(F/E)$ is an isomorphism, we have $\mathrm{res}_F(D_M(\varphi)) = D_M(\mathrm{res}_S\varphi)$, and, since $\varphi(\mathbf{x}) = \mathbf{b}$, this implies that $\mathrm{res}_F\mathcal{C} \subseteq \mathrm{Ar}(S/B', M, \mathbf{b})$. It follows that $\mathrm{res}_F\mathcal{C} \subseteq \mathrm{res}_F\mathcal{D}$, where $\mathcal{D} = \mathrm{Ar}(B', M, \mathbf{b})$; hence, by (5'), $\mathcal{O}_M \models \psi_{\mathcal{D}}(\mathbf{b})$. If $G \in \mathcal{D}$, then $G \in \mathrm{Im}(\mathrm{Gal}(M)) = \mathcal{H}$. Therefore, $\mathcal{D} \in \mathrm{Conj}(D/B', \mathcal{H})$. Then, it follows from (4') that $(D/B', M, \mathbf{b}) \models \boldsymbol{\chi}_{\mathcal{H}}$.

Now, suppose that $(D/B', M, \mathbf{b}) \models \boldsymbol{\chi}_{\mathcal{H}}$. That is $\mathcal{O}_M \models \exists W[\, q_{\mathcal{D}}(\mathbf{b}, W) = 0 \wedge \overline{\psi}_{\mathcal{D}}(\mathbf{b}, W)]$ for $\mathcal{D} = \mathrm{Ar}(B', M, \mathbf{b})$. Hence, by (4'), $\mathcal{O}_M \models \psi_{\mathcal{D}}(\mathbf{b})$. It follows that $\psi_{\mathcal{D}}$ is not a contradiction; therefore, there exists $\mathcal{C} \in \mathrm{Conj}(C'/A', \mathcal{H})$ such that $\mathrm{res}_F\mathcal{C} \subseteq \mathrm{res}_F\mathcal{D}$ and $\mathcal{O}_M \models \psi_{\mathcal{C}}(\mathbf{b})$. Thus, there exists $c \in \mathcal{O}_M$ such that

$$\mathcal{O}_M \models \exists Z[\, \bigwedge_{i=1}^{m} f_i(\mathbf{b}, c) = 0 \wedge g_2(\mathbf{b}, c) \neq 0 \wedge p_{\mathcal{C}}(\mathbf{b}, c, Z) = 0 \wedge \varphi_{\mathcal{C}}(\mathbf{b}, c, Z)] .$$

That is, $\mathbf{a} = (\mathbf{b}, c) \in A'(\mathcal{O}_M)$ satisfies that $\pi(\mathbf{a}) = \mathbf{b}$ and

$$\mathcal{O}_M \models \exists Z[\, p_{\mathcal{C}}(\mathbf{a}, Z) = 0 \wedge \varphi_{\mathcal{C}}(\mathbf{a}, Z)] .$$

For each K-homomorphism ψ of C' into $\tilde{K}$ which extends the specialization $(\mathbf{x}, y) \mapsto \mathbf{a}$, we can extend $\mathrm{res}_S\psi$ to a K-homomorphism φ of D into $\tilde{K}$. Hence we have that $\mathrm{res}_F\mathrm{Ar}(A', M, \mathbf{a}) \subseteq \mathrm{res}_F\mathrm{Ar}(B', M, \mathbf{b}) = \mathrm{res}_F\mathcal{D}$. Since $\mathcal{C}$ is the unique conjugacy class of $\mathrm{Gal}(C'/A')$ that satisfies $\mathrm{res}_F\mathcal{C} \subseteq \mathrm{res}_F\mathcal{D}$, it follows that $\mathcal{C} = \mathrm{Ar}(A', M, \mathbf{a})$. Thus, $(C'/A', M, \mathbf{a}) \models \boldsymbol{\theta}_{\mathcal{H}}$. □

Lemma 3.18. *Let $n \geq 0$ and let $\{(C_t/A_t, \boldsymbol{\theta}_{t,\mathcal{H}}) | \, t \in T\}$ be a finite collection of compatible cover-sentence pairs, where $A_t \subseteq \mathbb{A}^{n+1}$, C_t/A_t is a complete Galois ring/set cover over K with a ring of integers $\mathcal{O}[C_t/A_t]$, $\mathcal{H}$ is a family of finite groups, and $\boldsymbol{\theta}_{t,\mathcal{H}}$ is a quantifier-free sentence in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}[C_t/A_t, \mathcal{H}])$, $t \in T$. Let $B \subseteq \mathbb{A}^n$ be a K-normal basic set with $B \subseteq \pi(A_t)$ for each $t \in T$. Then there exist*

(6a) *a nonempty K-open subset B' of B,*

(6b) *complete Galois ring/set covers D/B' and C'_{ti}/A'_{ti} over K with rings of integers $\mathcal{O}[D/B']$ and $\mathcal{O}[C'_{ti}/A'_{ti}]$, respectively, and*

(6c) *quantifier-free sentences $\boldsymbol{\chi}_{ti,\mathcal{H}}$, $\boldsymbol{\theta}_{ti,\mathcal{H}}$ in the languages $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}[D/B', \mathcal{H}])$ and $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}[C'_{ti}/A'_{ti}, \mathcal{H}])$, respectively,*

for i in a finite set $I(t)$, with the following properties:

(7a) *the pair $(C'_{ti}/A'_{ti}, \boldsymbol{\theta}_{ti,\mathcal{H}})$ is induced (Definition 3.9) from $(C_t/A_t, \boldsymbol{\theta}_{t,\mathcal{H}})$;*

(7b) *$\pi^{-1}(B') \cap A_t = \bigcup_{i \in I(t)}^{\cdot} A'_{ti}$ and $\pi(A'_{ti}) = B'$; and*

(7c) *the quadruple $(C'_{ti}/A'_{ti}, \boldsymbol{\theta}_{ti,\mathcal{H}}; D/B', \boldsymbol{\chi}_{ti,\mathcal{H}})$ is compatible.*

Moreover, in the explicit case, if $(C_t/A_t, \boldsymbol{\theta}_{t,\mathcal{H}})$ and B are presented, then $I(t)$, $\boldsymbol{\chi}_{ti,\mathcal{H}}$, $\boldsymbol{\theta}_{ti,\mathcal{H}}$, C'_{ti}/A'_{ti}, $i \in I(t)$, $t \in T$, and D/B' can be effectively computed.

Proof. We apply [FrJ08, p. 427, Prop. 19.7.3] to find a stratification of $A_t \cap \pi^{-1}(B)$ into a disjoint union $\bigcup_{i\in J(t)}^{\cdot} A_{ti}$ of K-normal basic sets, where $J(t)$ is a finite set. In particular, $\pi(A_{ti}) \subseteq B$, for $i \in J(t)$.

Let $I(t) = \{j \in J(t) |\ \dim(\pi(A_{tj})) = \dim(B)\}$ and let $I'(t) = J(t) \setminus I(t)$. Then

$$B_1 = \bigcup_{j\in I(t)} (B \setminus \pi(A_{tj})) \cup \bigcup_{j\in I'(t)} \pi(A_{tj})$$

is of dimension smaller than B. We find a polynomial $f \in \mathcal{O}[X_1, \ldots, X_n]$ that vanishes on B_1 but not on B. Then, for a multiple h of f in $\mathcal{O}[\mathbf{X}]$ which does not vanish on B, we have that $\pi(A_{ti}) \setminus V(h) = B \setminus V(h)$ for each $i \in I(t)$ and $\pi^{-1}(B \setminus V(h)) \cap A_t = \bigcup_{i\in I(t)}^{\cdot} A_{ti} \setminus V(h)$.

For each $t \in T$ and $i \in I(t)$, let $(C_{ti}/A_{ti}, \boldsymbol{\theta}_{ti,\mathcal{H}})$ be the cover-sentence which is induced from the pair $(C_t/A_t, \boldsymbol{\theta}_{t,\mathcal{H}})$ and let P_{ti} be the finite separable extension of $K(B)$ that Lemmas 3.15 and 3.17 give (effectively, in the explicit case, if $(C_{ti}/A_{ti}, \boldsymbol{\theta}_{ti,\mathcal{H}})$ and B are presented). We find a finite Galois extension Q of $K(B)$ which contains all the P_{ti}'s, $i \in I(t)$, $t \in T$, and then we find an integral domain D_0 and a multiple h_0 of f in $\mathcal{O}[\mathbf{X}]$ which does not vanish on B such that $K(D_0) = Q$ and, with $B_0 = B \setminus V(h_0)$, D_0/B_0 is a complete Galois ring/set cover over K. Also, we choose for D_0/B_0 a ring of integers $\mathcal{O}[D_0/B_0]$.

Now, with a generic point $\mathbf{x}$ of B, we find, by Lemmas 3.15 and 3.17, effectively in the explicit case when all is presented,

a) a quantifier-free sentence $\boldsymbol{\chi}_{ti,\mathcal{H}}$ in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}[D_0/B_0, \mathcal{H}])$, $i \in I(t)$, $t \in T$, and
b) a multiple h of h_0 in $\mathcal{O}[\mathbf{X}]$ with $h(\mathbf{x}) \neq 0$,

such that, for $B' = B \setminus V(h)$, $A'_{ti} = A_{ti} \setminus V(h)$, $C'_{ti} = C_{ti}[h(\mathbf{x})^{-1}]$, $i \in I(t)$, $t \in T$, and $D = D_0[h(\mathbf{x})^{-1}]$, we have that the quadruple

$$(C'_{ti}/A'_{ti}, \boldsymbol{\theta}_{ti,\mathcal{H}};\ D/B', \boldsymbol{\chi}_{ti,\mathcal{H}})$$

is compatible, for each $i \in I(t)$, $t \in T$. □

Remark 3.19. Note that the extension P of $K(B)$ in Lemmas 3.15 and 3.17 depends on $\boldsymbol{\theta}_{\mathcal{H}}$ (because the extension P of $K(\mathbf{y})$ in Proposition 2.26 depends on $\psi(\mathbf{Y})$). Hence, the cover D/B' in Lemma 3.18 depends on the system of sentences $(\boldsymbol{\theta}_{t,\mathcal{H}} \,|\, t \in T)$.

3.4. **Elimination of One Variable.**

Definition 3.20. Let $n \geq 0$ and let A be a K-constructible set in $\mathbb{A}^n$.

a) A **complete normal stratification**

$$\mathcal{A} = \langle A, C_i/A_i |\ i \in I\rangle$$

of A over K is a partition $A = \bigcup_{i\in I}^{\cdot} A_i$ of A as a finite union of disjoint K-normal basic sets A_i, each equipped with a complete Galois ring/set cover C_i/A_i with ring of integers $\mathcal{O}[C_i/A_i]$.

b) Let $\mathcal{H}$ be a family of finite groups. If $\boldsymbol{\theta}_{i,\mathcal{H}}$ is a quantifier-free sentence in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}[C_i/A_i, \mathcal{H}])$ such that the pair $(C_i/A_i, \boldsymbol{\theta}_{i,\mathcal{H}})$ is compatible,

$i \in I$, then $\mathcal{A}$ may be augmented to a **radical Galois stratification** (with respect to $\mathcal{H}$) over $\mathcal{O}$:

$$\mathcal{A}(\mathcal{O},\mathcal{H}) = \langle A, C_i/A_i, \boldsymbol{\theta}_{i,\mathcal{H}} | \, i \in I \rangle \, .$$

Then, $\mathcal{A}$ is said to be the **underlying normal stratification of** $\mathcal{A}(\mathcal{O},\mathcal{H})$. We denote the system of sentences $(\boldsymbol{\theta}_{i,\mathcal{H}} | \, i \in I)$ of $\mathcal{A}(\mathcal{O},\mathcal{H})$ by $\mathrm{Sen}(\mathcal{A}(\mathcal{O},\mathcal{H}))$.

c) For $M \in \mathcal{F}_{\mathcal{H}}(\mathcal{O})$ and $\mathbf{a} \in A(\mathcal{O}_M)$, we write $(\mathcal{A}, M, \mathbf{a}) \models \mathrm{Sen}(\mathcal{A}(\mathcal{O},\mathcal{H}))$ if $(C_i/A_i, M, \mathbf{a}) \models \boldsymbol{\theta}_{i,\mathcal{H}}$ for the unique $i \in I$ such that $\mathbf{a} \in A_i$.

d) Suppose that $\mathcal{A}' = \langle A, C'_j/A'_j | \, j \in J \rangle$ is another complete normal stratification of A. We call $\mathcal{A}'$ a **refinement** of $\mathcal{A}$ if for each $j \in J$ there exists a unique $i \in I$ such that $A'_j \subseteq A_i$. If $\mathcal{A}'(\mathcal{O},\mathcal{H}) = \langle A, C'_j/A'_j, \boldsymbol{\theta}'_{j,\mathcal{H}} | \, j \in J \rangle$ is an augmentation of $\mathcal{A}'$ to a radical Galois stratification, then $\mathcal{A}'(\mathcal{O},\mathcal{H})$ is said to be a **refinement** of $\mathcal{A}(\mathcal{O},\mathcal{H})$ if in addition the pair $(C'_j/A'_j, \boldsymbol{\theta}'_{j,\mathcal{H}})$ is induced (Definition 3.9) from the pair $(C_i/A_i, \boldsymbol{\theta}_{i,\mathcal{H}})$ whenever $A'_j \subseteq A_i$. In this case it is clear that if $M \in \mathcal{F}_{\mathcal{H}}(\mathcal{O})$ and $\mathbf{a} \in A(\mathcal{O}_M)$, then $(\mathcal{A}, M, \mathbf{a}) \models \mathrm{Sen}(\mathcal{A}(\mathcal{O},\mathcal{H}))$ if and only if $(\mathcal{A}', M, \mathbf{a}) \models \mathrm{Sen}(\mathcal{A}'(\mathcal{O},\mathcal{H}))$.

The next two lemmas are based on Lemma 3.18. They allow us to eliminate, respectively, one existential or universal quantifier from a given radical Galois formula (Subsection 3.5).

Lemma 3.21. *(The existential elimination lemma.) Let $n \geq 0$ and let $\mathcal{A}(\mathcal{O},\mathcal{H}) = \langle \mathbb{A}^{n+1}, C_i/A_i, \boldsymbol{\theta}_{i,\mathcal{H}} | \, i \in I \rangle$ be a radical Galois stratification of $\mathbb{A}^{n+1}$ over $\mathcal{O}$ with respect to a family $\mathcal{H}$ of finite groups. Then, there exists a radical Galois stratification $\mathcal{B}(\mathcal{O},\mathcal{H}) = \langle \mathbb{A}^n, D_j/B_j, \boldsymbol{\chi}_{j,\mathcal{H}} | \, j \in J \rangle$ of $\mathbb{A}^n$ such that, for every $M \in \mathcal{F}_{\mathcal{H}}(\mathcal{O})$ and each $\mathbf{b} \in \mathbb{A}^n(\mathcal{O}_M)$, we have $(\mathcal{B}, M, \mathbf{b}) \models \mathrm{Sen}(\mathcal{B}(\mathcal{O},\mathcal{H}))$ if and only if there exists $\mathbf{a} \in \mathbb{A}^{n+1}(\mathcal{O}_M)$ such that $\pi(\mathbf{a}) = \mathbf{b}$ and $(\mathcal{A}, M, \mathbf{a}) \models \mathrm{Sen}(\mathcal{A}(\mathcal{O},\mathcal{H}))$.*

Moreover, in the explicit case, if $\mathcal{H}$ is primitive recursive and $\mathcal{A}(\mathcal{O},\mathcal{H})$ is presented, then $\mathcal{B}(\mathcal{O},\mathcal{H})$ can be effectively computed.

Proof. The union of the constructible sets $\pi(A_i)$ is equal to $\mathbb{A}^n$. We apply Lemma 1.19 to stratify $\mathbb{A}^n$ into a union of disjoint K-normal basic sets U_s, $s \in S$, such that, for each $i \in I$ and $s \in S$, either $U_s \subseteq \pi(A_i)$ or $U_s \cap \pi(A_i)$ is empty.

Lemma 3.18 and the stratification lemma (Lemma 1.19), again, allow us to stratify, effectively in the explicit case when $\mathcal{A}(\mathcal{O},\mathcal{H})$ is presented, each U_s separately and then combine the separate stratifications into basic normal stratifications $\mathbb{A}^n = \dot{\bigcup}_{j \in J} B_j$ and $\mathbb{A}^{n+1} = \dot{\bigcup}_{j \in J} \dot{\bigcup}_{k \in K(j)} A_{jk}$ with the following properties:

(1a) each A_{jk} is contained in a unique A_i and has a complete Galois ring/set cover C_{jk}/A_{jk} over K with ring of integers $\mathcal{O}[C_{jk}/A_{jk}]$ and a quantifier-free sentence $\boldsymbol{\theta}_{jk,\mathcal{H}}$ in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}[C_{jk}/A_{jk},\mathcal{H}])$ such that the pair $(C_{jk}/A_{jk}, \boldsymbol{\theta}_{jk,\mathcal{H}})$ is induced from the pair $(C_i/A_i, \boldsymbol{\theta}_{i,\mathcal{H}})$;

(1b) $\pi(A_{jk}) = B_j$ for each $j \in J$, $k \in K(j)$ and $\pi^{-1}(B_j) = \dot{\bigcup}_{k \in K(j)} A_{jk}$;

(1c) each B_j is equipped with a complete Galois ring set cover D_j/B_j over K with ring of integers $\mathcal{O}[D_j/B_j]$ and with quantifier-free sentences $\boldsymbol{\chi}_{jk,\mathcal{H}}$ in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}[D_j/B_j,\mathcal{H}])$ for each $k \in K(j)$, $j \in J$;

(1d) The quadruple $(C_{jk}/A_{jk}, \boldsymbol{\theta}_{jk,\mathcal{H}}; D_j/B_j, \boldsymbol{\chi}_{jk,\mathcal{H}})$ is compatible for each $k \in K(j)$, $j \in J$.

The stratification $\mathcal{A}'(\mathcal{O},\mathcal{H}) = \langle \mathbb{A}^{n+1}, C_{jk}/A_{jk}, \boldsymbol{\theta}_{jk,\mathcal{H}} | \, j \in J,\, k \in K(j)\rangle$ refines $\mathcal{A}(\mathcal{O},\mathcal{H})$. For each $j \in J$ we define $\boldsymbol{\chi}_{j,\mathcal{H}}$ to be $\bigvee_{k\in K(j)} \boldsymbol{\chi}_{jk,\mathcal{H}}$. Since for each $k \in K(j)$ the pair $(D_j/B_j, \boldsymbol{\chi}_{jk,\mathcal{H}})$ is compatible, the pair $(D_j/B_j, \boldsymbol{\chi}_{j,\mathcal{H}})$ is also compatible, $j \in J$. Then, $\mathcal{B}(\mathcal{O},\mathcal{H}) = \langle \mathbb{A}^n, D_j/B_j, \boldsymbol{\chi}_{j,\mathcal{H}} | \, j \in J\rangle$ is a radical Galois stratification of $\mathbb{A}^n$ and it follows from (1d) that, for every $M \in \mathcal{F}_{\mathcal{H}}(\mathcal{O})$ and each $\mathbf{b} \in \mathbb{A}^n(\mathcal{O}_M)$, $(\mathcal{B}, M, \mathbf{b}) \models \mathrm{Sen}(\mathcal{B}(\mathcal{O},\mathcal{H}))$ if and only if there exists $\mathbf{a} \in \mathbb{A}^{n+1}(\mathcal{O}_M)$ such that $\pi(\mathbf{a}) = \mathbf{b}$ and $(\mathcal{A}', M, \mathbf{a}) \models \mathrm{Sen}(\mathcal{A}'(\mathcal{O},\mathcal{H}))$ (hence $(\mathcal{A}, M, \mathbf{a}) \models \mathrm{Sen}(\mathcal{A}(\mathcal{O},\mathcal{H}))$). □

Lemma 3.22. *(The universal elimination lemma.) Let $n \geq 0$ and let*

$$\mathcal{A}(\mathcal{O},\mathcal{H}) = \langle \mathbb{A}^{n+1}, C_i/A_i, \boldsymbol{\theta}_{i,\mathcal{H}} | \, i \in I\rangle$$

be a radical Galois stratification of $\mathbb{A}^{n+1}$ over $\mathcal{O}$ with respect to a family $\mathcal{H}$ of finite groups. Then, there exists a radical Galois stratification

$$\mathcal{B}(\mathcal{O},\mathcal{H}) = \langle \mathbb{A}^n, D_j/B_j, \boldsymbol{\chi}_{j,\mathcal{H}} | \, j \in J\rangle$$

of $\mathbb{A}^n$ such that, for every $M \in \mathcal{F}_{\mathcal{H}}(\mathcal{O})$ and each $\mathbf{b} \in \mathbb{A}^n(\mathcal{O}_M)$, we have $(\mathcal{B}, M, \mathbf{b}) \models \mathrm{Sen}(\mathcal{B}(\mathcal{O},\mathcal{H}))$ if and only if $(\mathcal{A}, M, \mathbf{a}) \models \mathrm{Sen}(\mathcal{A}(\mathcal{O},\mathcal{H}))$ for all $\mathbf{a} \in \mathbb{A}^{n+1}(\mathcal{O}_M)$ such that $\pi(\mathbf{a}) = \mathbf{b}$.

Moreover, in the explicit case, if $\mathcal{H}$ is primitive recursive and $\mathcal{A}(\mathcal{O},\mathcal{H})$ is presented, then $\mathcal{B}(\mathcal{O},\mathcal{H})$ can be effectively computed.

Proof. Let $\mathcal{A}^c(\mathcal{O},\mathcal{H}) = \langle \mathbb{A}^{n+1}, C_i/A_i, \neg\boldsymbol{\theta}_{i,\mathcal{H}} | \, i \in I\rangle$ be the **complementary radical Galois stratification** to $\mathcal{A}(\mathcal{O},\mathcal{H})$ of $\mathbb{A}^{n+1}$. Note that, since $(C_i/A_i, \boldsymbol{\theta}_{i,\mathcal{H}})$ is compatible, it follows from Remark 3.6 that also the pair $(C_i/A_i, \neg\boldsymbol{\theta}_{i,\mathcal{H}})$ is compatible and we have, for every $M \in \mathcal{F}_{\mathcal{H}}(\mathcal{O})$ and each $\mathbf{a} \in A_i(\mathcal{O}_M)$, that

$$(C_i/A_i, M, \mathbf{a}) \models \neg\boldsymbol{\theta}_{i,\mathcal{H}} \Leftrightarrow (C_i/A_i, M, \mathbf{a}) \not\models \boldsymbol{\theta}_{i,\mathcal{H}}\,.$$

We apply Lemma 3.21 to find a radical Galois stratification

$$\mathcal{B}^c(\mathcal{O},\mathcal{H}) = \langle \mathbb{A}^n, D_j/B_j, \neg\boldsymbol{\chi}_{j,\mathcal{H}} | \, j \in J\rangle$$

of $\mathbb{A}^n$ over $\mathcal{O}$ such that, for every $M \in \mathcal{F}_{\mathcal{H}}(\mathcal{O})$ and each $\mathbf{b} \in \mathbb{A}^n(\mathcal{O}_M)$, $(\mathcal{B}^c, M, \mathbf{b}) \models \mathrm{Sen}(\mathcal{B}^c(\mathcal{O},\mathcal{H}))$ if and only if there exists $\mathbf{a} \in \mathbb{A}^{n+1}(\mathcal{O}_M)$ such that $\pi(\mathbf{a}) = \mathbf{b}$ and $(\mathcal{A}^c, M, \mathbf{a}) \models \mathrm{Sen}(\mathcal{A}^c(\mathcal{O},\mathcal{H}))$. The complementary radical Galois stratification to $\mathcal{B}^c(\mathcal{O},\mathcal{H})$ of $\mathbb{A}^n$ satisfies the conclusion of the lemma. □

Remark 3.23. Note that, by Remark 3.19, the underlying normal stratification $\mathcal{B}$ of $\mathcal{B}(\mathcal{O},\mathcal{H})$ depends on the system of sentences $\mathrm{Sen}(\mathcal{A}(\mathcal{O},\mathcal{H}))$. When $\mathcal{O} = K$, we can construct $\mathcal{B}$ such that it does not depend on $\mathrm{Sen}(\mathcal{A}(\mathcal{O},\mathcal{H}))$ (see [FrJ08, pp. 715–719, Lemmas 30.2.6, 30.4.1 and 30.4.2]).

3.5. **The Complete Elimination Procedure.**

Definition 3.24. Let $m, n \geq 0$ be integers, let $Q_1, \ldots, Q_m$ be quantifiers, and let

$$\mathcal{A}(\mathcal{O},\mathcal{H}) = \langle \mathbb{A}^{m+n}, C_i/A_i, \boldsymbol{\theta}_{i,\mathcal{H}} | \, i \in I\rangle$$

be a radical Galois stratification of $\mathbb{A}^{m+n}$ over $\mathcal{O}$ with respect to a family $\mathcal{H}$ of finite groups. Then, the expression

(1) $$(Q_1X_1)\ldots(Q_mX_m)[(\mathcal{A}, (\mathbf{X}, \mathbf{Y})) \models \mathrm{Sen}(\mathcal{A}(\mathcal{O},\mathcal{H}))]\,,$$

with $\mathbf{X} = (X_1, \dots, X_m)$ and $\mathbf{Y} = (Y_1, \dots, Y_n)$, is said to be a **radical Galois formula** (with respect to $\mathcal{A}(\mathcal{O}, \mathcal{H})$) in the free variables $\mathbf{Y}$. We denote it by $\theta = \theta(\mathbf{Y})$. For $M \in \mathcal{F}_{\mathcal{H}}(\mathcal{O})$ and $b_1, \dots, b_n \in \mathcal{O}_M$, we write $\mathcal{O}_M \models \theta(\mathbf{b})$ if $Q_m a_m \in \mathcal{O}_M, \dots, Q_1 a_1 \in \mathcal{O}_M$ such that $(\mathcal{A}, M, (\mathbf{a}, \mathbf{b})) \models \mathrm{Sen}(\mathcal{A}(\mathcal{O}, \mathcal{H}))$. Here we read "$Q_i a_i \in \mathcal{O}_M$" as "there exists a_i in $\mathcal{O}_M$" if Q_i is $\exists$, and as "for each a_i in $\mathcal{O}_M$" if Q_i is $\forall$. In the case that $n = 0$, θ has no free variables and it is called a **radical Galois sentence**.

Remark 3.25. *Each formula in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$ is equivalent to a radical Galois formula over $\mathcal{O}$ with respect to every family $\mathcal{H}$ of finite groups which contains the trivial group.* Indeed, let $\psi(Y_1, \dots, Y_n)$ be a formula in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$. Then, by Remark 2.5 a), $\psi(\mathbf{Y})$ is equivalent to a formula in the language $\mathcal{L}(\mathcal{O})$: That is, there exists a formula $\varphi(\mathbf{Y})$ in the language $\mathcal{L}(\mathcal{O})$ which satisfies that, for every algebraic extension M of K and for each $b_1, \dots, b_n \in \mathcal{O}_M$, we have $\mathcal{O}_M \models \varphi(\mathbf{b})$ if and only if $\mathcal{O}_M \models \psi(\mathbf{b})$. Now, $\varphi(\mathbf{Y})$ can be written (effectively, in the explicit case) in prenex normal form

$$(Q_1 X_1) \dots (Q_m X_m)[\bigvee_{i=1}^{k} \bigwedge_{j=1}^{l} f_{ij}(\mathbf{X}, \mathbf{Y}) = 0 \wedge g_{ij}(\mathbf{X}, \mathbf{Y}) \neq 0] \,,$$

with $f_{ij}, g_{ij} \in \mathcal{O}[\mathbf{X}, \mathbf{Y}]$. The formula in the brackets defines a K-constructible set $A \subseteq \mathbb{A}^{m+n}$. We construct a K-normal basic stratification $\mathbb{A}^{m+n} = \bigcup_{i \in I}^{\cdot} A_i$ such that, for each $i \in I$, either $A_i \subseteq A$ or $A_i \subseteq \mathbb{A}^{m+n} \smallsetminus A$. In the first case, let $C_i = K[A_i]$ and let θ_i be some true quantifier-free sentence in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$, for example $\mathrm{rad}_{1,1}(1, 1, 0, 0)$ (which is equivalent to $0 = 0$). In the second case, let $C_i = K[A_i]$ and let θ_i be some false quantifier-free sentence in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$, for example $\mathrm{rad}_{1,1}(1, 1, 0, 1)$ (which is equivalent to $1 = 0$). The pair $(C_i/A_i, \theta_i)$ is, of course, compatible. Let $\mathcal{H}$ be a family of finite groups which contains the trivial group. The corresponding radical Galois stratification $\mathcal{A}(\mathcal{O}, \mathcal{H})$ defines θ as in (1). Obviously, if $M \in \mathcal{F}_{\mathcal{H}}(\mathcal{O})$ and $\mathbf{b} \in \mathcal{O}_M^n$, then $\mathcal{O}_M \models \theta(\mathbf{b})$ if and only if $\mathcal{O}_M \models \varphi(\mathbf{b})$ (hence, if and only if $\mathcal{O}_M \models \psi(\mathbf{b})$). Thus, each formula in $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$ is equivalent to a radical Galois formula over $\mathcal{O}$ with respect to $\mathcal{H}$.

Application of Lemmas 3.21 and 3.22 to $\theta(\mathbf{Y})$ gives elimination of quantifiers.

Proposition 3.26. *Let $\mathcal{H}$ be a family of finite groups and let $\theta(Y_1, \dots, Y_n)$ be a radical Galois formula,*

$$(Q_1 X_1) \dots (Q_m X_m)[(\mathcal{A}, (\mathbf{X}, \mathbf{Y})) \models \mathrm{Sen}(\mathcal{A}(\mathcal{O}, \mathcal{H}))] \,,$$

with respect to a radical Galois stratification $\mathcal{A}(\mathcal{O}, \mathcal{H})$ of $\mathbb{A}^{m+n}$ over $\mathcal{O}$. Then, there exists a radical Galois stratification $\mathcal{B}(\mathcal{O}, \mathcal{H})$ of $\mathbb{A}^n$ over $\mathcal{O}$ such that, for every $M \in \mathcal{F}_{\mathcal{H}}(\mathcal{O})$ and each $\mathbf{b} \in \mathbb{A}^n(\mathcal{O}_M)$, we have

$$\mathcal{O}_M \models \theta(\mathbf{b}) \Leftrightarrow (\mathcal{B}, M, \mathbf{b}) \models \mathrm{Sen}(\mathcal{B}(\mathcal{O}, \mathcal{H})) \,. \tag{2}$$

In the explicit case, if $\theta(\mathbf{Y})$ is presented and $\mathcal{H}$ is primitive recursive, then $\mathcal{B}(\mathcal{O}, \mathcal{H})$ can be effectively computed.

Proof. Lemmas 3.21 and 3.22 give a radical Galois stratification $\mathcal{A}_{m-1}(\mathcal{O}, \mathcal{H})$ of $\mathbb{A}^{m-1+n}$ (depending on Q_m) s.t., for every $M \in \mathcal{F}_{\mathcal{H}}(\mathcal{O})$ and each $(a_1, \dots, a_{m-1}, \mathbf{b}) \in \mathbb{A}^{m-1+n}(\mathcal{O}_M)$, we have

$$(\mathcal{A}_{m-1}, M, (a_1, \dots, a_{m-1}, \mathbf{b})) \models \mathrm{Sen}(\mathcal{A}_{m-1}(\mathcal{O}, \mathcal{H}))$$

if and only if $Q_m a_m \in \mathcal{O}_M$ such that $(\mathcal{A}, M, (\mathbf{a}, \mathbf{b})) \models \mathrm{Sen}(\mathcal{A}(\mathcal{O}, \mathcal{H}))$.

This eliminates Q_m from θ. We continue to eliminate $Q_{m-1}, \dots, Q_1$, in order, by constructing the corresponding radical Galois stratifications $\mathcal{A}_{m-2}(\mathcal{O}, \mathcal{H}), \dots, \mathcal{A}_0(\mathcal{O}, \mathcal{H})$. Then, $\mathcal{B}(\mathcal{O}, \mathcal{H}) = \mathcal{A}_0(\mathcal{O}, \mathcal{H})$ is the desired radical Galois stratification. □

Remark 3.27. In the case of the usual Galois stratification (when $\mathcal{O} = K$), the normal stratification $\mathcal{B}$ under $\mathcal{B}(\mathcal{O}, \mathcal{H})$ does not depend on $\mathcal{H}$. This fact gives a decision procedure for the family of all perfect Frobenius fields which contain K [FrJ08, p. 722, Thm. 30.6.1]. In the general case this is not so (see Remark 3.23).

The case $n = 0$ is of particular interest: θ is a radical Galois sentence; the normal stratification $\mathcal{B}$ of $\mathbb{A}^0$ is trivial; and $\mathrm{Sen}(\mathcal{B}(\mathcal{O}, \mathcal{H}))$ contains only one quantifier-free sentence $\boldsymbol{\chi}_{\mathcal{H}}$ in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}[L/K, \mathcal{H}])$ with L a finite Galois extension of K. The condition $(\mathcal{B}, M, \mathbf{b}) \models \mathrm{Sen}(\mathcal{B}(\mathcal{O}, \mathcal{H}))$ simplifies to $\mathrm{Gal}(L/L \cap M) \in \mathcal{H}$ and $\mathcal{O}_M \models \chi_{L \cap M}$. Note that $\chi_{L \cap M}$ is a quantifier-free sentence in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}_{L \cap M})$; hence, by Proposition 2.11, $\mathcal{O}_M \models \chi_{L \cap M}$ if and only if $\widetilde{\mathcal{O}} \models \chi_{L \cap M}$. We denote

$$\mathrm{Con}_\theta(\mathcal{H}) = \{\mathrm{Gal}(L/K') \in \mathcal{H} \,|\, K' \text{ is a subextension of } L/K \text{ s.t. } \widetilde{\mathcal{O}} \models \chi_{K'}\}.$$

Then, $\mathrm{Con}_\theta(\mathcal{H})$ is a conjugacy domain of subgroups of $\mathrm{Gal}(L/K)$ which belong to $\mathcal{H}$ (since if K_1' and K_2' are two subextensions of L/K which are conjugate by an element of $\mathrm{Gal}(L/K)$, then there exists $\sigma \in \mathrm{Gal}(L/K)$ which satisfies $K_2' = \sigma K_1'$ and $\chi_{K_2'} = \sigma \chi_{K_1'}$). Moreover, when $\mathcal{O}$ is an effective computability domain, if $\mathcal{H}$ is primitive recursive and θ is presented, then we can find it effectively (because, by Proposition 2.8, the relation $\mathrm{rad}_{k,l}$ on $\widetilde{\mathcal{O}}$ is primitive recursive).

Theorem 3.28. *Let $\mathcal{H}$ be a family of finite groups and let θ be a radical Galois sentence,*

$$(Q_1 X_1) \dots (Q_m X_m)[(\mathcal{A}, \mathbf{X}) \models \mathrm{Sen}(\mathcal{A}(\mathcal{O}, \mathcal{H}))],$$

with respect to a radical Galois stratification $\mathcal{A}(\mathcal{O}, \mathcal{H})$ of $\mathbb{A}^m$ over $\mathcal{O}$. Then, there exists a finite Galois extension L of K and there exists a conjugacy domain $\mathrm{Con}_\theta(\mathcal{H})$ of $\mathrm{Gal}(L/K)$ which contains groups that belong to $\mathcal{H}$ such that, for every $M \in \mathcal{F}_{\mathcal{H}}(\mathcal{O})$, we have

$$\mathcal{O}_M \models \theta \Leftrightarrow \mathrm{Gal}(L/L \cap M) \in \mathrm{Con}_\theta(\mathcal{H}). \tag{3}$$

Moreover, when $\mathcal{O}$ is an effective computability domain, if $\mathcal{H}$ is primitive recursive and θ is presented, then we can effectively construct L and $\mathrm{Con}_\theta(\mathcal{H})$.

The following corollary follows from Theorem 3.28 and Remark 3.25.

Corollary 3.29. *Let $\mathcal{H}$ be a family of finite groups which contains the trivial group and let θ be a sentence in the language $\mathcal{L}(\mathcal{O})$. Then, there exists a finite Galois extension L of K and there exists a conjugacy domain Con of $\mathrm{Gal}(L/K)$ which contains groups that belong to $\mathcal{H}$ such that, for every perfect algebraic extension M of K which is Frobenius over $\mathcal{O}_M$ and $\mathrm{Im}(\mathrm{Gal}(M)) = \mathcal{H}$, we have*

$$\mathcal{O}_M \models \theta \Leftrightarrow \mathrm{Gal}(L/L \cap M) \in \mathrm{Con}.$$

Moreover, when $\mathcal{O}$ is an effective computability domain, if $\mathcal{H}$ is primitive recursive and θ is presented, then we can effectively construct L and Con.

3.6. **Decidability of Large Rings of Algebraic Integers.** When $\mathcal{H}$ consists only of the trivial group, $\mathrm{Im}(\mathrm{Gal}(\tilde{K})) = \mathcal{H}$. In this case Proposition 3.26 is equivalent to the main theorem of v.d. Dries [Dri88]:

Theorem 3.30. *For each formula $\varphi(Y_1, \ldots, Y_n)$ in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$, we can construct an equivalence*

$$\widetilde{\mathcal{O}} \models \varphi(\mathbf{Y}) \leftrightarrow \varphi_1(\mathbf{Y}) \vee \cdots \vee \varphi_d(\mathbf{Y}) \,,$$

in which each disjunct $\varphi_i(\mathbf{Y})$ is of the form

$$\exists Z[\, p_i(\mathbf{Y}, Z) = 0 \wedge \psi_i(\mathbf{Y}, Z)]$$

with $p_i \in \mathcal{O}[\mathbf{Y}, Z]$ a polynomial, monic in Z, and $\psi_i(\mathbf{Y}, Z)$ a quantifier-free formula in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$.

Moreover, in the explicit case, if $\varphi(\mathbf{Y})$ is presented, then we can effectively find $\varphi_i(\mathbf{Y})$ $(1 \leq i \leq d)$.

Proof. Let $\mathcal{H}$ be the family consisting only of the trivial group. We find, by Remark 3.25, a radical Galois formula $\theta(\mathbf{Y})$ over $\mathcal{O}$ with respect to $\mathcal{H}$ such that, for each $b_1, \ldots, b_n \in \widetilde{\mathcal{O}}$,

$$\widetilde{\mathcal{O}} \models \theta(\mathbf{b}) \Leftrightarrow \widetilde{\mathcal{O}} \models \varphi(\mathbf{b}) \,. \tag{1}$$

Proposition 3.26 gives, effectively in the explicit case if $\theta(\mathbf{Y})$ is presented, a radical Galois stratification $\mathcal{B}(\mathcal{O}) = \mathcal{B}(\mathcal{O}, \mathcal{H})$ of $\mathbb{A}^n$ over $\mathcal{O}$ such that, for each $\mathbf{b} \in \mathbb{A}^n(\widetilde{\mathcal{O}})$,

$$\widetilde{\mathcal{O}} \models \theta(\mathbf{b}) \Leftrightarrow (\mathcal{B}, \tilde{K}, \mathbf{b}) \models \mathrm{Sen}(\mathcal{B}(\mathcal{O})) \,. \tag{2}$$

Suppose that $\mathcal{B}(\mathcal{O}) = \langle \mathbb{A}^n, C_i/A_i, \theta_i |\, i \in I \rangle$, where θ_i is a quantifier-free sentence in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O}[C_i])$. For each $i \in I$, let $\mathbf{y}_i$ be a generic point of A_i, let z_i be a primitive element for the Galois ring/set cover C_i/A_i, integral over $\mathcal{O}[\mathbf{y}_i]$, such that $\mathcal{O}[C_i] = \mathcal{O}[\mathbf{y}_i, z_i]$, and let $\chi_i(\mathbf{Y}, Z)$ be a quantifier-free formula in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$ such that $\theta_i = \chi_i(\mathbf{y}_i, z_i)$. Let q_i be a polynomial in $\mathcal{O}[\mathbf{Y}, Z]$ which satisfies that $q_i(\mathbf{y}_i, Z)$ is a multiple of $\mathrm{irr}(z_i, K(\mathbf{y}_i))$ by an invertible element of $K[A_i]$, and let $p_i \in \mathcal{O}[\mathbf{Y}, Z]$ be a polynomial which is monic in Z and satisfies $p_i(\mathbf{y}_i, z_i) = 0$. Then $q_i(\mathbf{y}_i, Z) | p_i(\mathbf{y}_i, Z)$ in $K[A_i][Z]$. Also, for each $b_1, \ldots, b_n \in \widetilde{\mathcal{O}}$,

$$(C_i/A_i, \tilde{K}, \mathbf{b}) \models \theta_i \Leftrightarrow \widetilde{\mathcal{O}} \models \exists Z[\, q_i(\mathbf{b}, Z) = 0 \wedge \chi_i(\mathbf{b}, Z)] \,. \tag{3}$$

We write, for each $i \in I$, $A_i = V_i \smallsetminus V(g_i)$, where $V_i = V(f_{i1}, \ldots, f_{i,\rho(i)})$ is a K-variety on which g_i does not vanish, and $f_{i1}, \ldots, f_{i,\rho(i)}, g_i \in \mathcal{O}[\mathbf{Y}]$. We denote $\mathbf{f}_i(\mathbf{Y}) = (f_{i1}(\mathbf{Y}), \ldots, f_{i,\rho(i)}(\mathbf{Y}))$ and let $\varphi_i(\mathbf{Y})$ be the following formula in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$:

$$\mathbf{f}_i(\mathbf{Y}) = 0 \wedge g_i(\mathbf{Y}) \neq 0 \wedge \exists Z[\, q_i(\mathbf{Y}, Z) = 0 \wedge \chi_i(\mathbf{Y}, Z)] \,.$$

We denote by $\psi_i(\mathbf{Y}, Z)$ the following quantifier-free formula in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$:

$$\mathbf{f}_i(\mathbf{Y}) = 0 \wedge g_i(\mathbf{Y}) \neq 0 \wedge q_i(\mathbf{Y}, Z) = 0 \wedge \chi_i(\mathbf{Y}, Z) \,.$$

Then $\varphi_i(\mathbf{Y})$ is equivalent to $\exists Z[\, p_i(\mathbf{Y}, Z) = 0 \wedge \psi_i(\mathbf{Y}, Z)]$, which is a formula of the desired form.

Let $\mathbf{b} \in \mathbb{A}^n(\widetilde{\mathcal{O}})$ and let i be the unique element in I such that $\mathbf{b} \in A_i(\widetilde{\mathcal{O}})$. It follows from (1), (2), and (3) that

$$\begin{aligned} \widetilde{\mathcal{O}} \models \varphi(\mathbf{b}) \Leftrightarrow \widetilde{\mathcal{O}} \models \theta(\mathbf{b}) &\Leftrightarrow (C_i/A_i, \tilde{K}, \mathbf{b}) \models \theta_i \\ &\Leftrightarrow \widetilde{\mathcal{O}} \models \exists Z[\, q_i(\mathbf{b}, Z) = 0 \wedge \chi_i(\mathbf{b}, Z)] \,. \end{aligned}$$

Hence,

$$\widetilde{\mathcal{O}} \models \varphi(\mathbf{Y}) \leftrightarrow \bigvee_{i\in I} \big(\mathbf{f}_i(\mathbf{Y}) = 0 \wedge g_i(\mathbf{Y}) \neq 0 \wedge \exists Z[\, q_i(\mathbf{Y}, Z) = 0 \wedge \chi_i(\mathbf{Y}, Z)]\big)\,;$$

thus, $\widetilde{\mathcal{O}} \models \varphi(\mathbf{Y}) \leftrightarrow \bigvee_{i\in I} \varphi_i(\mathbf{Y})$. □

Remark 3.31.

a) The proof of this theorem in [Dri88], for $\mathcal{O} = \mathbb{Z}$, uses a compactness argument from model theory [Dri88, Section 1.5], instead of our stratification procedure; hence, the elimination procedure in [Dri88] is not primitive recursive, but only recursive. However, the elimination procedure that we have constructed here is primitive recursive. By the compactness argument, v.d. Dries achives the following result: Let $f_1(\mathbf{X}, \mathbf{Y}), \ldots, f_k(\mathbf{X}, \mathbf{Y}) \in \mathbb{Z}[\mathbf{X}, \mathbf{Y}]$, where $\mathbf{X} = (X_1, \ldots, X_m)$ and $\mathbf{Y} = (Y_1, \ldots, Y_n)$. For every field L and each $\mathbf{y} \in L^n$, we denote $\{\mathbf{x} \in \mathbb{A}^m \,|\, f_1(\mathbf{x}, \mathbf{y}) = 0, \ldots, f_k(\mathbf{x}, \mathbf{y}) = 0\}$ by $V_{L,\mathbf{y}}$. Then, there exist:
   (i) quantifier-free $\mathcal{L}$-formulas $s_i(\mathbf{Y})$, $1 \leq i \leq B$, such that all fields of characteristic zero satisfy $\forall \mathbf{Y}(s_1(\mathbf{Y}) \vee \cdots \vee s_B(\mathbf{Y}))$;
   (ii) for each $i \in \{1, \ldots, B\}$, a tuple $(p_i, \mathbf{f}_{i1}, \ldots, \mathbf{f}_{iJ(i)})$, where $p_i \in \mathbb{Z}[\mathbf{X}, T]$ is monic and of positive degree in T and each $\mathbf{f}_{ij}$ is a tuple of elements of $\mathbb{Z}[\mathbf{X}, \mathbf{Y}, T]$, such that if L is a field of characteristic zero, $\mathbf{y}$ is an element in L^n satisfying $s_i(\mathbf{y})$, and $t \in \tilde{L}$ is a root of $p_i(\mathbf{y}, T)$, then $V_{L,\mathbf{y}} = W_1 \cup \cdots \cup W_{J(i)}$, where each $W_j := \{\mathbf{x} \in \mathbb{A}^m \,|\, \mathbf{f}_{ij}(\mathbf{x}, \mathbf{y}, t) = 0\}$ is an absolutely irreducible variety.

b) L. v.d. Dries proved this theorem in [Dri88] for $\tilde{\mathbb{Z}}$ and generalized it, together with A. Macintyre, in [DrM90] for additional integral domains which satisfy natural (i.e. algebraic) first-order assumptions. They called a ring satisfying the relevant algebraic conditions a **good Rumely domain**; this is by definition a domain R with quotient field E having the following six properties:
   1) E is algebraically closed.
   2) R is a Bezout domain.
   3) If $C \subseteq \mathbb{A}^m$ is a smooth absolutely irreducible curve over E, $f \in E[X_1, \ldots, X_m]$, and $C_f := \{\mathbf{x} \in C \,|\, f(\mathbf{x}) \neq 0\}$ has points in $\mathbb{A}^m(\frac{1}{a}R)$ and in $\mathbb{A}^m(\frac{1}{b}R)$, where $a, b \in R \setminus \{0\}$ have $\gcd(a, b) = 1$, then C_f has a point in $\mathbb{A}^m(R)$.
   4) For all $a, b \in R \setminus \{0\}$ there are $a_1, b_1 \in R$ such that $a = a_1 \cdot b_1$, $\gcd(a_1, b) = 1$, and $b \in \mathrm{rad}_R(b_1 R)$.
   5) Every nonzero nonunit (i.e. non-invertible element) in R is a product of two relatively prime nonunits.
   6) $R \neq E$ and R has Jacobson radical zero.

   They also showed that condition 3) can be replaced by the local-global condition:
   3′) If $V \subseteq \mathbb{A}^m$ is absolutely irreducible variety over E, $f \in E[X_1, \ldots, X_m]$, and $V_f := \{\mathbf{x} \in V \,|\, f(\mathbf{x}) \neq 0\}$ has a point in each $\mathbb{A}^m(R_{\mathfrak{m}})$ ($\mathfrak{m} \in \mathrm{Max}(R)$), then V_f has a point in $\mathbb{A}^m(R)$.

   They proved that if R is a good Rumely domain, then it satisfies the following claim: *Let $V \subseteq \mathbb{A}^m$ be an absolutely irreducible variety over E and let*

$f, g_1, \dots, g_k, h_1, \dots, h_k, p_1, \dots, p_t$ be polynomials in $E[X_1, \dots, X_m]$. Then, in the notations of Subsection 2.3,

$$R \models \exists \mathbf{X}\,[\mathbf{X} \in V \wedge f(\mathbf{X}) \neq 0 \wedge \bigwedge_{i=1}^{k} (g_i(\mathbf{X}) \underline{\mathrm{R}}\, h_i(\mathbf{X})) \wedge \bigwedge_{j=1}^{t} (\underline{\mathrm{NU}}(p_j(\mathbf{X})))]$$

$$\Leftrightarrow (\forall \mathfrak{m} \in \mathrm{Max}(R))\, R_{\mathfrak{m}} \models \exists \mathbf{X}\,[\mathbf{X} \in V \wedge f(\mathbf{X}) \neq 0 \wedge \bigwedge_{i=1}^{k} (g_i(\mathbf{X}) \underline{\mathrm{R}}\, h_i(\mathbf{X}))]$$

$$\wedge \bigwedge_{j=1}^{t} \big((\exists \mathfrak{m} \in \mathrm{Max}(R))\, R_{\mathfrak{m}} \models \exists \mathbf{X}\,[\mathbf{X} \in V \wedge f(\mathbf{X}) \neq 0$$

$$\wedge \bigwedge_{i=1}^{k} (g_i(\mathbf{X}) \underline{\mathrm{R}}\, h_i(\mathbf{X})) \wedge \underline{\mathrm{NU}}(p_j(\mathbf{X}))]\big).$$

This is, in fact, the claim we use in Proposition 2.20. But, in order to prove this claim there, we use the weak approximation theorem for absolutely irreducible varieties, which is more precise than the local-global principle, but is not first order. Also, the proof of Proposition 2.20 depends on the assumption that the Jacobson radical of a nonzero ideal in R and in $R_{\mathfrak{m}}$, for $\mathfrak{m} \in \mathrm{Max}(R)$, equals its nilradical; this property is blatantly not elementary.

Let M be an algebraic extension of K which is PAC over $\mathcal{O}_M$. We have shown, in Theorem 1.12, that if K_1 is a finite subextension of M/K and $\mathfrak{a}$ is an ideal of $\mathcal{O}_{K_1}$, then there exists a finite subextension L of M/K_1 and there exists $c \in \mathcal{O}_L$ such that $\mathfrak{a}\mathcal{O}_L = c\mathcal{O}_L$. In particular, $\mathcal{O}_M$ is a Bezout domain. We shall show now that also properties 4) and 5) are satisfied for $R = \mathcal{O}_M$:

In order to see 4), let $a, b \in \mathcal{O}_{K_1} \setminus \{0\}$, where K_1 is a finite subextension of M/K. We factor the ideals $a\mathcal{O}_{K_1}$ and $b\mathcal{O}_{K_1}$ as follows:

$$a\mathcal{O}_{K_1} = \mathfrak{m}_1^{e_1} \cdots \mathfrak{m}_r^{e_r} \cdot \mathfrak{n}_1^{f_1} \cdots \mathfrak{n}_s^{f_s} \qquad (e_i, f_j > 0)\,,$$
$$b\mathcal{O}_{K_1} = \mathfrak{m}_1^{g_1} \cdots \mathfrak{m}_r^{g_r} \cdot \mathfrak{q}_1^{h_1} \cdots \mathfrak{q}_t^{h_t} \qquad (g_i, h_k > 0)\,,$$

where $\mathfrak{m}_1, \dots, \mathfrak{m}_r, \mathfrak{n}_1, \dots, \mathfrak{n}_s, \mathfrak{q}_1, \dots, \mathfrak{q}_t$ are distinct maximal ideals of $\mathcal{O}_{K_1}$. By Theorem 1.12, we can take a finite subextension L of M/K_1 in which all these maximal ideals become principal, say $\mathfrak{m}_i\mathcal{O}_L = c_i\mathcal{O}_L$, $\mathfrak{n}_j\mathcal{O}_L = d_j\mathcal{O}_L$. Then, $a\mathcal{O}_L = (cd)\mathcal{O}_L$, where $c = c_1^{e_1} \cdots c_r^{e_r}$ and $d = d_1^{f_1} \cdots d_s^{f_s}$. Hence, there exists an invertible element u in $\mathcal{O}_L$ such that $a = cdu$. We denote $a_1 = d$ and $b_1 = cu$. Then, $a = a_1 \cdot b_1$, $\gcd(a_1, b) = 1$, and $b \in \mathrm{rad}_{\mathcal{O}_M}(b_1\mathcal{O}_M)$.

In order to see 5), let $x \neq 0$ be a nonunit in $\mathcal{O}_{K_1}$, where K_1 is a finite subextension of M/K. We write $x\mathcal{O}_{K_1} = \mathfrak{m}_1^{e_1} \cdots \mathfrak{m}_k^{e_k}$, where $e_1, \dots, e_k > 0$ and $\mathfrak{m}_1, \dots, \mathfrak{m}_k$ are distinct maximal ideals of $\mathcal{O}_{K_1}$. Since $\mathfrak{m}_1$ factors in a suitable subextension of M/K_1 (see the proof of Lemma 1.8), we can get $k > 1$ after enlarging K_1, and similarly we can achieve that each $\mathfrak{m}_i$ is principal. From this, a factorization of x into a multiplication of two relatively prime nonunits is clear.

When θ is a sentence in the language $\mathcal{L}(\mathcal{O})$ (or $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$), Theorem 3.30 gives an equivalence

$$\widetilde{\mathcal{O}} \models \theta \leftrightarrow \theta_1 \vee \cdots \vee \theta_d\,,$$

in which each sentence θ_i is of the form

$$\exists Z[\, p_i(Z) = 0 \wedge \psi_i(Z)]$$

with $p_i \in \mathcal{O}[Z]$ a monic polynomial and $\psi_i(Z)$ a quantifier-free formula in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$. Moreover, in the explicit case and when $\mathcal{O}$ is an effective computability domain, if θ is presented, then we can check for each i between 1 and d and each root z_i of $p_i(Z)$ whether $\widetilde{\mathcal{O}} \models \psi_i(z_i)$ (Proposition 2.8). Alternatively, we can arrive to the same conclusion using Theorem 3.28 if we take for $\mathcal{H}$ the family consisting only of the trivial group.

Theorem 3.32. *When $\mathcal{O}$ is an effective computability domain, the ring $\widetilde{\mathcal{O}}$ is decidable.*

Moreover, the theory of $\widetilde{\mathcal{O}}$ is primitive recursive.

We arrive, finally, to the main result in this work. For a positive integer e and for $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e) \in \mathrm{Gal}(K)^e$, we denote the fixed field in $\tilde{K}$ of $\sigma_1, \ldots, \sigma_e$ by $\tilde{K}(\boldsymbol{\sigma})$ and the integral closure of $\mathcal{O}$ in $\tilde{K}(\boldsymbol{\sigma})$ by $\widetilde{\mathcal{O}}(\boldsymbol{\sigma})$. We denote the theory of all sentences of $\mathcal{L}(\mathcal{O})$ which are true in $\widetilde{\mathcal{O}}(\boldsymbol{\sigma})$ for almost all (with respect to the Haar measure) $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ by $\mathrm{Almost}(\mathcal{O}, e)$.

Theorem 3.33. *Let e be a positive integer and let θ be a sentence in the language $\mathcal{L}(\mathcal{O})$. Denote the Haar measure of all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ such that θ is true in $\widetilde{\mathcal{O}}(\boldsymbol{\sigma})$ by α. Then, α is a rational number.*

Moreover, when $\mathcal{O}$ is an effective computability domain (e.g. when $\mathcal{O} = \mathbb{Z}$ and $\mathcal{O} = \mathbb{F}_p[t]$), if θ is presented, then α can be effectively (primitive recursively) computed. The theory $\mathrm{Almost}(\mathcal{O}, e)$ is primitive recursive.

Proof. Let $\mathcal{H}$ be the family of all finite groups H such that $\mathrm{rank}(H) \leq e$. By Remark 3.25, θ is equivalent to a radical Galois sentence over $\mathcal{O}$ with respect to $\mathcal{H}$. Theorem 3.28 gives a finite Galois extension L of K and a conjugacy domain $\mathrm{Con}_\theta(\mathcal{H})$ of $\mathrm{Gal}(L/K)$, which contains only groups that belong to $\mathcal{H}$, such that, for every perfect algebraic extension M of K which is PAC over $\mathcal{O}_M$ and satisfies $\mathrm{Im}(\mathrm{Gal}(M)) = \mathcal{H}$, we have

$$\mathcal{O}_M \models \theta \Leftrightarrow \mathrm{Gal}(L/L \cap M) \in \mathrm{Con}_\theta(\mathcal{H})\,. \tag{4}$$

Note that $\mathrm{Im}(\mathrm{Gal}(M)) = \mathcal{H}$ if and only if $\mathrm{Gal}(M) \cong \hat{F}_e$ [FrJ08, p. 360, Lemma 17.7.1]; therefore, $\mathrm{Gal}(M)$ has the embbeding property [FrJ08, p. 568, Lemma 24.3.3]. Since, in addition, M is PAC over $\mathcal{O}_M$, if follows that M is Frobenius over $\mathcal{O}_M$.

Let k be the number of $\boldsymbol{\sigma}_0 \in \mathrm{Gal}(L/K)^e$ such that $< \boldsymbol{\sigma}_0 > \in \mathrm{Con}_\theta(\mathcal{H})$. Then, by (4), $\alpha = \frac{k}{[L:K]^e}$ is the desired rational number, because, for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, $\tilde{K}(\boldsymbol{\sigma})$ is perfect and PAC over $\widetilde{\mathcal{O}}(\boldsymbol{\sigma})$ (Proposition 1.7) which satisfies $\mathrm{Gal}(\tilde{K}(\boldsymbol{\sigma})) \cong \hat{F}_e$ [FrJ08, p. 379, Thm. 18.5.6]. □

APPENDIX A. IDEAL CALCULUS

Let $\mathcal{O}$ be a Dedekind domain with a quotient field K and let P be the set of all nonzero prime ideals of $\mathcal{O}$. We assume:

a) $\mathcal{O}$ is presented in K [FrJ08, p. 404, Def. 19.1.1];
b) P is presented and each ideal of $\mathcal{O}$ can be effectively written as a product of prime ideals of $\mathcal{O}$;

c) $\mathcal{O}$ is an **Euclidean ring**. That is, there exists a function $\delta : \mathcal{O} \setminus \{0\} \to \mathbb{N}$ which satisfies, for each $a, b \in \mathcal{O} \setminus \{0\}$, that $\delta(ab) = \delta(a)\delta(b)$ and there exist $c, r \in \mathcal{O}$ such that $a = bc + r$ and $\delta(r) < \delta(b)$ or $r = 0$. We define also $\delta(0) = 0$. We assume that δ is presented and that we can effectively perform division with a remainder as above. In particular, we can effectively find, by Euclid's algorithm, a greatest common divisor of two elements in $\mathcal{O}$;
d) For each $n \in \mathbb{N}$, the set $\{a \in \mathcal{O} | \, \delta(a) \leq n\}$ is an explicitly given *finite* subset of $\mathcal{O}$.

Along this appendix, L is a separable extension of K of degree n, $\mathcal{O}_L$ is the integral closure of $\mathcal{O}$ in L, and P_L is the set of all nonzero prime ideals of $\mathcal{O}_L$. Let η be a primitive element for L/K and let $f(X) = \mathrm{irr}(\eta, K)$. We multiply η by a suitable element of $\mathcal{O}$, in order to assume that $\eta \in \mathcal{O}_L$ and f is a monic polynomial in $\mathcal{O}[X]$. L is given, in fact, by the coefficients of f. Also, each element x in $\mathcal{O}_L$ is given by the coefficients of $\mathrm{irr}(x, K)$. We assume, then, along this appendix, that $\eta \in \mathcal{O}_L$ is a primitive element for L/K and $f(X) = \mathrm{irr}(\eta, K)$ is a monic polynomial in $\mathcal{O}[X]$.

Let $x \in \mathcal{O}_L$. We would like to know how to factor $x\mathcal{O}_L$ into a product of prime ideals. We shall show, in fact, how to (effectively) factor each ideal of $\mathcal{O}_L$, presented by a finite number of generators, into a product of prime ideals.

The presentation of an ideal by generators is not suitable for calculations. In Subsection A.1 we shall find an integral basis $\{w_1, \ldots, w_n\}$ of L/K such that $\mathcal{O}_L = \mathcal{O}w_1 + \cdots + \mathcal{O}w_n$ and in Subsection A.2 we shall find, for each ideal $\mathfrak{a}$ in $\mathcal{O}_L$, an $\mathcal{O}$-basis $\{\alpha_1, \ldots, \alpha_n\}$ such that $\mathfrak{a} = \mathcal{O}\alpha_1 + \cdots + \mathcal{O}\alpha_n$. By this presentation we can check whether an element $\beta = \sum_{i=1}^{n} b_i w_i \in \mathcal{O}_L$ belongs to the ideal $\mathfrak{a}$ and hence we can check inclusion between ideals. Finally, in Subsection A.3, we shall show how to find, for $\mathfrak{p} \in P$, all the prime ideals $\mathfrak{P} \in P_L$ which lie above $\mathfrak{p}$ and, as a result, we shall show how to factor each ideal in $\mathcal{O}_L$ into a product of prime ideals.

The references to this appendix are the book *"Algorithmic algebraic number theory"* of Pohst and Zassenhaus [PoZ89] and the book *"Elementary and analytic theory of algebraic numbers"* of Narkiewicz [Nar04]. However, these references deal only with the case $\mathcal{O} = \mathbb{Z}$ while this appendix is written for the general case.

A.1. **Integral Basis.**

Definition A.1. *The discriminant.*

a) Let $\sigma_1, \ldots, \sigma_n$ be the isomorphisms of L into $\tilde{K}$ over K. For each n-tuple $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in L^n$ we define the **discriminant**

$$D_{L/K}(\boldsymbol{\alpha}) = (\det(\sigma_i \alpha_j))^2 .$$

If $\alpha_i = \sum_{j=1}^{n} a_{ij}\beta_j$ with $\beta_j \in L$ and $a_{ij} \in K$, then

$$D_{L/K}(\boldsymbol{\alpha}) = (\det(a_{ij}))^2 D_{L/K}(\boldsymbol{\beta}) .$$

$D_{L/K}(\boldsymbol{\alpha}) \neq 0$ if and only if $\{\alpha_1, \ldots, \alpha_n\}$ is a basis of L/K [Lan70, Prop. 9 in Chapter III].
If $L = K(\alpha)$, then $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis of L/K and we denote

$$D_{L/K}(\alpha) = D_{L/K}(1, \alpha, \ldots, \alpha^{n-1}) .$$

If $\boldsymbol{\alpha} \in \mathcal{O}_L^n$, then $D_{L/K}(\boldsymbol{\alpha}) \in \mathcal{O}$. In particular, $0 \neq D_{L/K}(\eta) \in \mathcal{O}$ and we have

$$D_{L/K}(\eta) = (-1)^{\frac{n(n-1)}{2}} N_{L/K}(f'(\eta))\,.$$

$D_{L/K}(\eta)$ can be effectively computed in the following way: we find $a_{ij} \in K$ such that

$$a^j f'(\eta) = \sum_{i=1}^{n} a_{ij}\eta^i\,, \qquad j = 0, 1, \ldots, n-1\,;$$

then

$$D_{L/K}(\eta) = (-1)^{\frac{n(n-1)}{2}} \det(a_{ij})$$

[Nar04, Prop. 2.9] (see also [FrJ08, §19.2]).

b) If $M \subseteq L$ is a free $\mathcal{O}$-module of rank n and $\{\alpha_1, \ldots, \alpha_n\}$ is a basis of M over $\mathcal{O}$, we denote the fractional ideal $D_{L/K}(\boldsymbol{\alpha})\mathcal{O}$ of $\mathcal{O}$ by $D_{\mathcal{O}_L/\mathcal{O}}(M)$; it can be shown that this notation does not depend on the basis [Lan70, Prop. 10 in Chap. III].

We shall show in Proposition A.3 that $\mathcal{O}_L$ is a free $\mathcal{O}$-module of rank n and hence also each fractional ideal of $\mathcal{O}_L$ is a free $\mathcal{O}$-module of rank n.

Definition A.2. *An integral basis. A set of n elements $w_1, \ldots, w_n$ in $\mathcal{O}_L$ which are linearly independent over K and generate $\mathcal{O}_L$ as an $\mathcal{O}$-module, i.e. $\mathcal{O}_L = \mathcal{O}w_1 + \cdots + \mathcal{O}w_n$, is called an* **integral basis** *for the field L.*

Proposition A.3. *L has an integral basis $\{w_1, \ldots, w_n\}$ which can be found effectively.*

Proof. We denote $\alpha_i = \eta^{i-1}$, $i = 1, \ldots, n$, and let $d = D_{L/K}(\boldsymbol{\alpha}) = D_{L/K}(\eta)$. Then $0 \neq d \in \mathcal{O}$. We denote $M = \mathcal{O}\alpha_1 + \cdots + \mathcal{O}\alpha_n$.

CLAIM: $d\mathcal{O}_L \subseteq M$. Indeed, Let $b \in \mathcal{O}_L$. Then, there exist $c_1, \ldots, c_n \in \mathcal{O}$ with $\gcd(c_1, \ldots, c_n) = 1$ and there exists $0 \neq c_0 \in \mathcal{O}$ such that

$$b = \frac{1}{c_0}(c_1\alpha_1 + \cdots + c_n\alpha_n)\,.$$

Let $\sigma_1, \ldots, \sigma_n$ be the isomorphisms of L into $\tilde{K}$ over K. Then

$$\sigma_j b = \frac{c_1}{c_0}\sigma_j\alpha_1 + \cdots + \frac{c_n}{c_0}\sigma_j\alpha_n\,, \qquad j = 1, \ldots, n\,.$$

That is,

$$\begin{pmatrix} \sigma_1 b \\ \vdots \\ \sigma_n b \end{pmatrix} = \begin{pmatrix} \sigma_1\alpha_1 & \ldots & \sigma_1\alpha_n \\ \vdots & \ddots & \vdots \\ \sigma_n\alpha_1 & \ldots & \sigma_n\alpha_n \end{pmatrix} \begin{pmatrix} \frac{c_1}{c_0} \\ \vdots \\ \frac{c_n}{c_0} \end{pmatrix}\,.$$

Note that $\sigma_j b, \sigma_j\alpha_i \in \widetilde{\mathcal{O}}$, $i, j = 1, \ldots, n$. Let $\Delta = \det(\sigma_j\alpha_i)$. Then $\Delta \in \widetilde{\mathcal{O}}$ and $\Delta^2 = d$.

We denote

$$\Delta_j = \det \begin{pmatrix} \sigma_1\alpha_1 & \ldots & \overset{j}{\sigma_1 b} & \ldots & \sigma_1\alpha_n \\ \vdots & & \vdots & & \vdots \\ \sigma_n\alpha_n & \ldots & \sigma_n b & \ldots & \sigma_n\alpha_n \end{pmatrix}, \qquad j = 1, \ldots, n\,.$$

Then $\Delta_j \in \widetilde{\mathcal{O}}$ and it follows, by Kramer's rule, that $\frac{c_j}{c_0} = \frac{\Delta_j}{\Delta}$, $j = 1, \ldots, n$. Hence

$$\Delta\Delta_j = \Delta^2\frac{\Delta_j}{\Delta} = d\frac{c_j}{c_0} \in \widetilde{\mathcal{O}} \cap K = \mathcal{O}\,,$$

and therefore $c_0|dc_j$, $j=1,\dots,n$. Since $\gcd(c_1,\dots,c_n)=1$, there exist $d_1,\dots,d_n\in\mathcal{O}$ such that $c_1d_1+\cdots+c_nd_n=1$ and hence $d=(dc_1)d_1+\cdots+(dc_n)d_n$. Therefore $c_0|d$; thus, $db=\frac{d}{c_0}(c_1\alpha_1+\cdots+c_n\alpha_n)\in\mathcal{O}\alpha_1+\cdots+\mathcal{O}\alpha_n=M$, and the claim is proved.

For each i between 1 and n, we let D_i be the set

$$\{d_i\in\mathcal{O}\,|\,d_i\neq 0 \text{ and } \exists\, d_1,\dots,d_{i-1}\in\mathcal{O} \text{ s.t. } \frac{1}{d}(d_1\alpha_1+\cdots+d_i\alpha_i)\in\mathcal{O}_L\}\,.$$

$D_i\neq\emptyset$ because $d\in D_i$: $\frac{1}{d}(d\alpha_1+\cdots+d\alpha_i)=\alpha_1+\cdots+\alpha_i\in\mathcal{O}_L$. We denote $m_i=\min\limits_{d_i\in D_i}\delta(d_i)$ and let $d_{ii}\in\mathcal{O}$ be such that $\delta(d_{ii})=m_i$. We can effectively find such d_{ii} as follows: Since $\mathcal{O}$ is an Euclidean ring of finite type, the set $C=\{c\in\mathcal{O}|\,\delta(c)\leq\delta(d)\}$ is finite. If $\frac{1}{d}(d_1\alpha_1+\cdots+d_i\alpha_i)\in\mathcal{O}_L$ and $d'_j\equiv d_j(\mathrm{mod}\,d)$ (i.e., there exists $b_j\in\mathcal{O}$ such that $d_j=b_jd+d'_j$ and $\delta(d'_j)<\delta(d)$), $j=1,\dots,i$, then also $\frac{1}{d}(d'_1\alpha_1+\cdots+d'_i\alpha_i)\in\mathcal{O}_L$. Hence, we can go over the finite set C^i and check, for each $(d_1,\dots,d_i)\in C^i$ with $d_i\neq 0$, whether $\frac{1}{d}(d_1\alpha_1+\cdots+d_i\alpha_i)$ is integral over $\mathcal{O}$.

For each i between 1 and n, we find $d_{i1},\dots,d_{i,i-1}\in\mathcal{O}$ such that

$$w_i=\frac{1}{d}(d_{i1}\alpha_1+\cdots+d_{ii}\alpha_i)$$

belongs to $\mathcal{O}_L$. Then,

$$D_{L/K}(\mathbf{w})=(\det(\frac{d_{ij}}{d}))^2D_{L/K}(\boldsymbol{\alpha})\neq 0\,,$$

because $d=D_{L/K}(\boldsymbol{\alpha})\neq 0$ and $\det(\frac{d_{ij}}{d})=\frac{1}{d^n}\det(d_{ij})=\frac{d_{11}\cdots d_{nn}}{d^n}\neq 0$. Hence $\{w_1,\dots,w_n\}$ forms a basis for L/K. We shall prove that it is also an integral basis for L, that is, $\mathcal{O}_L=\mathcal{O}w_1+\cdots+\mathcal{O}w_n$. Note first that if an element $c\in\mathcal{O}_L$ can be written as $c=\frac{1}{d}(c_1\alpha_1+\cdots+c_j\alpha_j)$ with j between 1 and n and $c_i\in\mathcal{O}$, $i=1,\dots,j$, then d_{jj} divides c_j. Indeed, if $c_j=sd_{jj}+r$, where $s,r\in\mathcal{O}$ and $0<\delta(r)<\delta(d_{jj})$, then $c-sw_j\in\mathcal{O}_L$ and

$$c-sw_j=\frac{1}{d}((c_1-sd_{j1})\alpha_1+\cdots+(c_{j-1}-sd_{j,j-1})\alpha_{j-1}+r\alpha_j)\,,$$

in contradiction to the choice of d_{jj}.

We denote $M_0=\mathcal{O}w_1+\cdots+\mathcal{O}w_n$. We shall prove by induction on j that each element of $\mathcal{O}_L$ of the form $\frac{1}{d}(x_1\alpha_1+\cdots+x_j\alpha_j)$, with $x_j\in\mathcal{O}$, belongs to M_0. For $j=n$ this gives $\mathcal{O}_L=\mathcal{O}_L\cap\frac{1}{d}M\subseteq M_0$, and hence $\mathcal{O}_L=M_0$. Suppose that we have proved this claim for $j-1$ and let $y=\frac{1}{d}(x_1\alpha_1+\cdots+x_j\alpha_j)$ with $x_j\in\mathcal{O}$ such that $y\in\mathcal{O}_L$. Then, there exists $a\in\mathcal{O}$ such that $x_j=ad_{jj}$; therefore, $y-aw_j\in\mathcal{O}_L$ and, by the induction's assumption,

$$y-aw_j=\frac{1}{d}((x_1-ad_{j1})\alpha_1+\cdots+(x_{j-1}-ad_{j,j-1}))\in M_0\,.$$

Thus, since $aw_j\in M_0$, also $y\in M_0$, as required. □

A.2. **Presentation of Ideals.** We denote the group of invertible matrices in $M_n(\mathcal{O})$ by $\mathrm{GL}(n,\mathcal{O})$. Then $A\in\mathrm{GL}(n,\mathcal{O})$ if and only if $\det A$ is an invertible element in $\mathcal{O}$.

Remark A.4. *Let M be a free $\mathcal{O}$-module of rank n and let $\{b_1,\dots,b_n\}$ and $\{c_1,\dots,c_n\}$ be two $\mathcal{O}$-bases of M. Then, there exists $U\in\mathrm{GL}(n,\mathcal{O})$ which satisfies $(b_1,\dots,b_n)=(c_1,\dots,c_n)U$.* Indeed, since $\mathcal{O}b_1+\cdots+\mathcal{O}b_n=M=\mathcal{O}c_1+\cdots+\mathcal{O}c_n$, there

exist $U, V \in M_n(\mathcal{O})$ such that $(b_1, \dots, b_n) = (c_1, \dots, c_n)U$ and $(c_1, \dots, c_n) = (b_1, \dots, b_n)V$. Hence,

$$(c_1, \dots, c_n) = (c_1, \dots, c_n)UV\,;$$

therefore, by the uniqueness of representation, $UV = I_n$.

Lemma A.5. *Let $a_1, \dots, a_n \in \mathcal{O}$. Then, one can effectively find a matrix $A = (a_{ij})$ in $M_n(\mathcal{O})$ such that $a_{1j} = a_j$, $j = 1, \dots, n$, and $\det A = \gcd(a_1, \dots, a_n)$.*

Proof. We denote $d_i = \gcd(a_1, \dots, a_i)$, $i = 1, \dots, n$. We do an induction on n. The case $n = 1$ is trivial. Suppose, then, that there exists a matrix $\tilde{A} = (\tilde{a}_{ij}) \in M_{n-1}(\mathcal{O})$ which satisfies $\tilde{a}_{1j} = a_j$, $j = 1, \dots, n-1$, and $\det\tilde{A} = d_{n-1}$. Since $d_n = \gcd(d_{n-1}, a_n)$, there exist $u, v \in \mathcal{O}$ such that $d_n = ud_{n-1} + va_n$. Suppose that $\tilde{A} = \left(\begin{array}{c|c} a_1 \cdots a_{n-1} & \\ \hline & \\ B & \end{array}\right)$, and let

$$A = \left(\begin{array}{c|c} & a_n \\ & 0 \\ \tilde{A} & \vdots \\ & 0 \\ \hline \frac{a_1}{d_{n-1}}v \dots \frac{a_{n-1}}{d_{n-1}}v & u \end{array}\right) = \left(\begin{array}{c|c} a_1 \quad \dots \quad a_{n-1} & a_n \\ \hline & 0 \\ & \vdots \\ B & \\ & 0 \\ \hline \frac{a_1}{d_{n-1}}v \dots \frac{a_{n-1}}{d_{n-1}}v & u \end{array}\right).$$

Then, $A_{1j} = a_j$, $j = 1, \dots, n$, and, by developing $\det A$ by the last column,

$$\det A = (-1)^{1+n}a_n \cdot \det \left(\begin{array}{c} B \\ \hline \frac{a_1}{d_{n-1}}v \cdots \frac{a_{n-1}}{d_{n-1}}v \end{array}\right) + (-1)^{n+n}u \cdot \det\tilde{A}$$

$$= (-1)^{1+n}a_n \cdot \tfrac{v}{d_{n-1}}(-1)^{n-1}\det \left(\begin{array}{c} a_1 \cdots a_{n-1} \\ \hline \\ B \end{array}\right) + u \cdot d_{n-1}$$

$$= \tfrac{va_n}{d_{n-1}}\det\tilde{A} + ud_{n-1} = va_n + ud_{n-1} = d_n\,,$$

as required. □

Lemma A.6. *Let $a_1, \dots, a_n \in \mathcal{O}$ and denote $d = \gcd(a_1, \dots, a_n)$. Then, one can effectively find $U \in \mathrm{GL}(n, \mathcal{O})$ which satisfies*

$$(a_1, \dots, a_n)U = (d, 0, \dots, 0)\,.$$

Proof. By Lemma A.5 we can find $A = (a_{ij}) \in M_n(\mathcal{O})$ which satisfies $a_{1j} = a_j$, $j = 1, \dots, n$, and $\det A = d$. Suppose that $A = \left(\begin{array}{c} a_1 \cdots a_n \\ \hline \\ B \end{array}\right)$ and let $\tilde{A} = \left(\begin{array}{c} \frac{a_1}{d} \cdots \frac{a_n}{d} \\ \hline \\ B \end{array}\right)$. Then, $\tilde{A} \in M_n(\mathcal{O})$ and $\det\tilde{A} = \frac{1}{d}\det A = 1$; therefore, $\tilde{A} \in \mathrm{GL}(n, \mathcal{O})$. Also, $(d, 0, \dots, 0)\tilde{A} = (a_1, \dots, a_n)$. Hence, $U = \tilde{A}^{-1}$ is the desired matrix. □

A matrix $A = (a_{ij})$ in $M_{m\times n}(\mathcal{O})$ is a **lower triangular matrix** if $a_{ij} = 0$ for each $i < j$.

Proposition A.7. *For each matrix A in $M_{m\times n}(\mathcal{O})$, one can effectively find a matrix $U\in \mathrm{GL}(n,\mathcal{O})$ such that AU is a lower triangular matrix.*

Proof. Suppose that $A=(a_{ij})$ and denote $d=\gcd(a_{11},\dots,a_{1n})$. We shall prove the proposition by induction on n. Let $n>1$ and suppose that the proposition is true for matrices in $M_{m\times k}(\mathcal{O})$, for each positive integer m and each k between 1 and $n-1$. We find, by Lemma A.6, a matrix $U\in\mathrm{GL}(n,\mathcal{O})$ such that $(a_{11},\dots,a_{1n})U=(d,0,\dots,0)$. Then, AU is a matrix of the form

$$\left(\begin{array}{c|c} d & 0\cdots 0 \\ \hline c_2 & \\ \vdots & B \\ c_n & \end{array}\right).$$

If $m=1$, then we are done. For $m>1$ we apply induction on m on the matrix $B\in M_{m-1\times n-1}(\mathcal{O})$ and conclude that there exists a matrix $\tilde{V}\in\mathrm{GL}(n-1,\mathcal{O})$ such that $B\tilde{V}$ is a lower triangular matrix. The matrix $V=\left(\begin{array}{c|c} 1 & 0\cdots 0 \\ \hline 0 & \\ \vdots & \tilde{V} \\ 0 & \end{array}\right)$ belongs to $\mathrm{GL}(n,\mathcal{O})$ and satisfies that $AUV=\left(\begin{array}{c|c} d & 0\cdots 0 \\ \hline c_2 & \\ \vdots & B\tilde{V} \\ c_n & \end{array}\right)$ is a lower triangular matrix. □

Corollary A.8. *Let $\{w_1,\dots,w_n\}$ be an integral basis for L and $\mathfrak{a}=(x_1,\dots,x_k)\mathcal{O}_L$ be a nonzero ideal of $\mathcal{O}_L$.*

Then, one can effectively find a lower triangular matrix H in $M_n(\mathcal{O})$ such that $\det H\neq 0$ *and, for $(\alpha_1,\dots,\alpha_n)=(w_1,\dots,w_n)H$,*

$$\mathfrak{a}=\mathcal{O}\alpha_1+\cdots+\mathcal{O}\alpha_n\,.$$

Proof. Since $\mathcal{O}_L=\mathcal{O}w_1+\cdots+\mathcal{O}w_n$, it follows that

$$\mathfrak{a}=x_1\mathcal{O}_L+\cdots+x_k\mathcal{O}_L=\mathcal{O}x_1w_1+\cdots+\mathcal{O}x_1w_n+\cdots+\mathcal{O}x_kw_1+\cdots+\mathcal{O}x_kw_n\,.$$

Suppose, without loss, that $x_i\neq 0$ for each i. For all i between 1 and k, we can find (since $x_i\in\mathcal{O}_L$) a matrix A_i in $M_n(\mathcal{O})$ such that $(x_iw_1,\dots,x_iw_n)=(w_1,\dots,w_n)A_i$; since $\{x_iw_1,\dots,x_iw_n\}$ is a basis for L/K, the matrix A_i is invertible in $M_n(K)$ and therefore $\mathrm{rank}A_i=n$. We denote

$$A=(A_1\vdots\cdots\vdots A_k)\,.$$

By Proposition A.7, we find a matrix $U\in\mathrm{GL}(kn,\mathcal{O})$ such that $\tilde{H}=AU$ is a lower triangular matrix. Then $\tilde{H}=(H\vdots 0)$, where $H\in M_n(\mathcal{O})$ is a lower triangular matrix, and we have that $n\geq\mathrm{rank}H=\mathrm{rank}\tilde{H}=\mathrm{rank}(AU)=\mathrm{rank}A\geq\mathrm{rank}A_1=n$. Hence $\mathrm{rank}H=n$ and therefore $\det H\neq 0$. Also, $(H\vdots 0)=AU$ and $A=(H\vdots 0)U^{-1}$. We denote $(\alpha_1,\dots,\alpha_n)=(w_1,\dots,w_n)H$. Then,

$$\begin{aligned}(x_1w_1,\dots,x_1w_n,\dots,x_kw_1,\dots,x_kw_n)&=(w_1,\dots,w_n)A\\&=(w_1,\dots,w_n)(H\vdots 0)U^{-1}\\&=(\alpha_1,\dots,\alpha_n,0,\dots,0)U^{-1}\,.\end{aligned}$$

Thus,

$$\begin{aligned}\mathfrak{a} = x_1\mathcal{O}_L + \cdots + x_k\mathcal{O}_L &= \mathrm{Span}_{\mathcal{O}}\{x_1w_1, \ldots, x_1w_n, \ldots, x_kw_1, \ldots, x_kw_n\} \\ &= \mathrm{Span}_{\mathcal{O}}\{\alpha_1, \ldots, \alpha_n\}\,,\end{aligned}$$

as required. □

For an ideal $\mathfrak{a}$ of $\mathcal{O}_L$, we denote the **norm** of $\mathfrak{a}$ [Lan70, Section 7 in Chapter I] by $N_{L/K}(\mathfrak{a})$.

Lemma A.9. *Let $\mathfrak{a} = (x_1, \ldots, x_k)\mathcal{O}_L$ be a nonzero ideal of $\mathcal{O}_L$. Then, one can effectively compute $N_{L/K}(\mathfrak{a})$.*

Proof. We find, by Proposition A.3, an integral basis $\{w_1, \ldots, w_n\}$ for L. By Corollary A.8, we find a lower triangular matrix $H = (h_{ij})$ in $M_n(\mathcal{O})$ such that $\det H = h_{11}\cdots h_{nn} \neq 0$ and, for $(\alpha_1, \ldots, \alpha_n) = (w_1, \ldots, w_n)H$, $\mathfrak{a} = \mathcal{O}\alpha_1 + \cdots + \mathcal{O}\alpha_n$. Then

$$D_{\mathcal{O}_L/\mathcal{O}}(\mathfrak{a}) = D_{L/K}(\boldsymbol{\alpha})\mathcal{O} = (\det H)^2 D_{L/K}(\mathbf{w})\mathcal{O} = (\det H)^2 D_{\mathcal{O}_L/\mathcal{O}}(\mathcal{O}_L)\,.$$

On the other hand, by [Lan70, Prop. 13 in Chapter III],

$$D_{\mathcal{O}_L/\mathcal{O}}(\mathfrak{a}) = (N_{L/K}(\mathfrak{a}))^2 D_{\mathcal{O}_L/\mathcal{O}}(\mathcal{O}_L)\,.$$

Hence

$$N_{L/K}(\mathfrak{a}) = (\det H)\mathcal{O}\,.$$

□

Corollary A.10. *Let $\mathfrak{a} = (x_1, \ldots, x_k)\mathcal{O}_L$ be an ideal of $\mathcal{O}_L$ and let $\beta \in \mathcal{O}_L$. Then, one can effectively check whether $\beta \in \mathfrak{a}$.*

Proof. If $\mathfrak{a} = 0$, the claim is clear. Suppose then, without loss, that $x_i \neq 0$, $i = 1, \ldots, k$. We find, by Proposition A.3, an integral basis $\{w_1, \ldots, w_n\}$ for L and we present β in the form $\beta = \sum_{j=1}^{n} b_j w_j$ with $b_j \in \mathcal{O}$. Also, by Corollary A.8, we find a lower triangular matrix $H = (h_{ij})$ in $M_n(\mathcal{O})$ such that $h_{11}\cdots h_{nn} = \det H \neq 0$ and, for $\alpha_i = \sum_{j=i}^{n} h_{ji}w_j$ $(i = 1, \ldots, n)$, $\mathfrak{a} = \mathcal{O}\alpha_1 + \cdots + \mathcal{O}\alpha_n$. Then, $\beta \in \mathfrak{a}$ if and only if there exist $y_1, \ldots, y_n \in \mathcal{O}$ which satisfy

$$\sum_{j=1}^{n} b_j w_j = \beta = \sum_{i=1}^{n} y_i\alpha_i = \sum_{i=1}^{n} y_i \sum_{j=1}^{n} h_{ji}w_j = \sum_{j=1}^{n} w_j \Big(\sum_{i=1}^{j} h_{ji}y_i\Big)\,.$$

Hence, $\beta \in \mathfrak{a}$ if and only if there exist $y_1, \ldots, y_n \in \mathcal{O}$ such that

$$b_j = \sum_{i=1}^{j} h_{ji}y_i\,, \qquad j = 1, \ldots, n\,. \tag{1}$$

We define $\bar{y}_j \in K$ by induction: $\bar{y}_1 = \frac{b_1}{h_{11}}$ and $\bar{y}_j = \frac{1}{h_{jj}}(b_j - \sum_{i=1}^{j-1} h_{ji}\bar{y}_i)$, $j = 1, \ldots, n$. Then $(\bar{y}_1, \ldots, \bar{y}_n)$ is the unique solution to the system of equations (1). Therefore, $\beta \in \mathfrak{a}$ if and only if $\bar{y}_i \in \mathcal{O}$, $i = 1, \ldots, n$. □

Corollary A.11. *Let $\mathfrak{a} = (x_1, \ldots, x_k)\mathcal{O}_L$ and $\mathfrak{b} = (y_1, \ldots, y_l)\mathcal{O}_L$ be two ideals of $\mathcal{O}_L$. Then, one can effectively check whether $\mathfrak{b} \subseteq \mathfrak{a}$.*

Lemma A.12. *Let $\mathfrak{a} = (x_1, \dots, x_k)\mathcal{O}_L$ be a nonzero ideal of $\mathcal{O}_L$. Then, one can effectively find a system of representatives for $\mathcal{O}_L/\mathfrak{a}$.*

Proof. We find, by Proposition A.3, an integral basis for $\{w_1, \dots, w_n\}$ L. By Corollary A.8, we find a lower triangular matrix $H = (h_{ij})$ in $M_n(\mathcal{O})$ such that $h_{11} \cdots h_{nn} = \det H \neq 0$ and, for $\alpha_i = \sum_{j=i}^{n} h_{ji} w_j$ $(i = 1, \dots, n)$, $\mathfrak{a} = \mathcal{O}\alpha_1 + \cdots + \mathcal{O}\alpha_n$.

For each i between 1 and n, let $C_i = \{ z \in \mathcal{O} \mid \delta(z) < \delta(h_{ii}) \}$. Let

$$R = \{ \sum_{i=1}^{n} z_i w_i \mid z_i \in C_i \}.$$

Then, R is a system of representatives for $\mathcal{O}_L/\mathfrak{a}$. Indeed, let $\beta \in \mathcal{O}_L$. We have to show that there exists $r \in R$ such that $\beta - r \in \mathfrak{a}$. Suppose that $\beta = \sum_{j=1}^{n} b_j w_j$ with $b_j \in \mathcal{O}$. We find, by induction, $\bar{y}_j \in \mathcal{O}$ and $c_j \in C_j$ such that $b_1 = h_{11}\bar{y}_1 + c_1$ and $b_j - \sum_{i=1}^{j-1} h_{ji}\bar{y}_i = h_{jj}\bar{y}_j + c_j$, $j = 1, \dots, n$. We denote $r = \sum_{j=1}^{n} c_j w_j$ and $\overline{\beta} = \sum_{j=1}^{n} w_j (\sum_{i=1}^{j} h_{ji}\bar{y}_i)$. Then $r \in R$ and, as in the proof of Corollary A.10, it follows that $\beta - r = \overline{\beta} \in \mathfrak{a}$. □

We can even find a **complete** system of representatives in the following case.

Remark A.13. Suppose that there exists a presented subset $\mathcal{O}_+$ of $\mathcal{O}$ which satisfies, for each $a, b \in \mathcal{O}$ with $b \neq 0$, that there exist *unique* $c \in \mathcal{O}$ and $r \in \mathcal{O}_+$ such that $a = bc + r$ and $\delta(r) < \delta(b)$. In this case we say that $\mathcal{O}$ is a **nice** Euclidean ring. For example, $\mathbb{Z}$ with $\mathbb{Z}_+ = \mathbb{N} \cup \{0\}$ and $\mathbb{F}_p[t]$ with $\mathbb{F}_p[t]_+ = \mathbb{F}_p[t]$ are nice Euclidean rings.

A nice Euclidean ring satisfies, for each $n \in \mathbb{N}$ and each $a, b \in \mathcal{O}_+$ with $\delta(a) < n$ and $\delta(b) < n$, that $\delta(a - b) < n$. Indeed, suppose on the contrary that there exist $a, b \in \mathcal{O}_+$ such that $\delta(a) < n$, $\delta(b) < n$, and $\delta(a - b) \geq n$. Then, $a - b \neq 0$ and there exist two different divisions with a remainder of a in $a - b$:

$$a = (a - b) \cdot 1 + b \quad (b \in \mathcal{O}_+ \text{ satisfies } \delta(b) < n \leq \delta(a - b)) \text{ and}$$

$$a = (a - b) \cdot 0 + a \quad (a \in \mathcal{O}_+ \text{ satisfies } \delta(a) < n \leq \delta(a - b)),$$

in contradiction to the assumption that $\mathcal{O}$ is a nice Euclidean ring.

We return now to the notations in the proof of Lemma A.12 and for each i between 1 and n we replace C_i by the set $\{z \in \mathcal{O}_+ \,|\, \delta(z) < \delta(h_{ii})\}$. Then, the same proof of Lemma A.12 gives that $R = \{\sum_{i=1}^{n} z_i w_i \,|\, z_i \in C_i\}$ is a system of representatives for $\mathcal{O}_L/\mathfrak{a}$. We claim that R is even a complete system of representatives for $\mathcal{O}_L/\mathfrak{a}$. That is, for each $r_1, r_2 \in R$ such that $r_1 \neq r_2$ we have $r_1 - r_2 \notin \mathfrak{a}$.

To this end, let $\beta \in \mathcal{O}_L$ be a nonzero element and suppose that $\beta = \sum_{j=1}^{n} b_j w_j$ with $b_j \in \mathcal{O}$. Then, if $\beta \in \mathfrak{a}$, then there exists j between 1 and n such that $\delta(b_j) \geq \delta(h_{jj})$. Indeed, suppose on the contrary that $\delta(b_j) < \delta(h_{jj})$, $j = 1, \dots, n$.

It follows from the proof of Corollary A.10 that $b_j = \sum_{i=1}^{j} h_{ji}\bar{y}_i$, where $\bar{y}_j \in \mathcal{O}$ are defined by induction: $\bar{y}_1 = \frac{b_1}{h_{11}}$ and $\bar{y}_j = \frac{1}{h_{jj}}(b_j - \sum_{i=1}^{j-1} h_{ji}\bar{y}_i)$, $j = 1, \ldots, n$. We shall prove by induction on j that $b_j = 0$, $j = 1, \ldots, n$, and therefore arrive to the contradiction $\beta = 0$. If $j = 1$, then $h_{11}|b_1$; hence, since $\delta(b_1) < \delta(h_{11})$, $b_1 = 0$. Suppose that $j > 1$ and that $b_1 = \cdots = b_{j-1} = 0$. Then also $\bar{y}_1 = \cdots = \bar{y}_{j-1} = 0$ and therefore $\bar{y}_j = \frac{b_j}{h_{jj}}$. Hence $h_{jj}|b_j$; thus, since $\delta(b_j) < \delta(h_{jj})$, $b_j = 0$.

Now, let $r_1, r_2 \in R$ be such that $r_1 \neq r_2$. Suppose that $r_j = \sum_{i=1}^{n} z_{ji}w_i$ with $z_{ji} \in C_i$, $j = 1, 2$. Then $0 \neq r_1 - r_2 = \sum_{i=1}^{n}(z_{1i} - z_{2i})w_i$ and for each i between 1 and n, $\delta(z_{1i} - z_{2i}) < \delta(h_{ii})$ (because $\mathcal{O}$ is a nice Euclidean ring). Hence, it follows from the preceding pharagraph that $r_1 - r_2 \notin \mathfrak{a}$.

Lemma A.14. *Let $\mathfrak{a} = (x_1, \ldots, x_k)\mathcal{O}_L$ be an ideal of $\mathcal{O}_L$. Then, one can effectively check whether $\mathfrak{a}$ is a prime ideal of $\mathcal{O}_L$. If $\mathfrak{a}$ is not a prime ideal, then one can effectively find all the prime ideals of $\mathcal{O}_L$ which contain $\mathfrak{a}$.*

Proof. An ideal $\mathfrak{P}$ in $\mathcal{O}_L$ is prime if and only if it is maximal. Therefore, $\mathfrak{a}$ is a prime ideal if and only if $\mathfrak{a} \neq \mathcal{O}_L$ and $\mathfrak{a} + x\mathcal{O}_L = \mathcal{O}_L$ for each $x \in \mathcal{O}_L \setminus \mathfrak{a}$. We find, by Lemma A.12, a system of representatives (even complete if $\mathcal{O}$ is a nice Euclidean ring) R for $\mathcal{O}_L/\mathfrak{a}$. Then, since for every $y, z \in \mathcal{O}_L$, $y - z \in \mathfrak{a}$ if and only if $y\mathcal{O}_L + \mathfrak{a} = z\mathcal{O}_L + \mathfrak{a}$, it follows that $\mathfrak{a}$ is a prime ideal if and only if $\mathfrak{a} \neq \mathcal{O}_L$ and $\mathfrak{a} + x\mathcal{O}_L = \mathcal{O}_L$ for each $x \in R$. Hence, by Corollary A.11, we can effectively check whether $\mathfrak{a}$ is a prime ideal.

If $\mathfrak{a}$ is not a prime ideal, we find all the x's in R such that $\mathfrak{a} + x\mathcal{O}_L \neq \mathcal{O}_L$. These are (in fact all) proper ideals of $\mathcal{O}_L$ which contain $\mathfrak{a}$ properly. We find, by induction, all the prime ideals $\mathfrak{P} \in P_L$ which contain one of the ideals $\mathfrak{a} + x\mathcal{O}_L$. These are all the prime ideals $\mathfrak{P} \in P_L$ which contain $\mathfrak{a}$. □

A.3. **Factorization of an Ideal into a Product of Prime Ideals.** By Lemma A.14 we get

Proposition A.15. *For each $\mathfrak{p} \in P$, one can effectively find all the prime ideals of $\mathcal{O}_L$ which contain $\mathfrak{p}\mathcal{O}_L$.*

We can cut the number of calculations needed for the above procedure in the following case.

Remark A.16. Suppose that, for each $\mathfrak{p} \in P$, the field $\bar{K}_\mathfrak{p} = \mathcal{O}/\mathfrak{p}$ is presented with a **splitting algorithm** [FrJ08, p. 405, Def. 19.1.2]. For example, this situation is satisfied if K is a global field and, for each $\mathfrak{p} \in P$, one can effectively compute $(\mathcal{O} : \mathfrak{p})$ (i.e., the field $\bar{K}_\mathfrak{p}$ is an explicitly given finite field). In this case we can save in the number of calculations that are needed for finding all the prime ideals of $\mathcal{O}_L$ which lie over $\mathfrak{p} \in P$ in the following way.

Let f and η be as in the introduction. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$, let $\bar{f}$ be the reduction of f modulo $\mathfrak{p}$ and let

$$\bar{f}(X) = \bar{P}_1(X)^{e_1} \cdots \bar{P}_r(X)^{e_r}$$

be the factorization of $\bar{f}$ into a multiplication of powers of distinct monic and irreducible polynomials over $\bar{K}_{\mathfrak{p}} = \mathcal{O}/\mathfrak{p}$. For each i between 1 and r, we find a monic polynomial $P_i \in \mathcal{O}[X]$ such that its reduction modulo $\mathfrak{p}$ is $\bar{P}_i$. We denote

$$\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_L + P_i(\eta)\mathcal{O}_L\,, \qquad i = 1, \ldots, r\,.$$

It follows from [Lan70, Prop. 16 in Chapter III] that $I = D_{L/K}(\eta)A \cdot D_{\mathcal{O}_L/\mathcal{O}}(\mathcal{O}_L)^{-1}$ is an (integral) ideal of $\mathcal{O}$ and if $\mathfrak{p} \nmid I$, then $\mathcal{O}_{L,\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}[\eta]$. Hence, it follows from [Lan70, Prop. 25 in Chapter I] that $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ are distinct prime ideals of $\mathcal{O}_L$, with $f(\mathfrak{P}_i/\mathfrak{p}) = \deg P_i$, such that

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_r} \cdots \mathfrak{P}_r^{e_r}\,.$$

If $\mathfrak{p} \mid I$, then the $\mathfrak{P}_i$'s are not necessarily prime ideals of $\mathcal{O}_L$ and they even can be the ring $\mathcal{O}_L$ itself. But, still, we have, for a proper ideal $\mathfrak{P}$ of $\mathcal{O}_L$, that $\mathfrak{P}$ is a prime ideal of $\mathcal{O}_L$ which contains $\mathfrak{p}$ if and only if there exists i between 1 and r such that $\mathfrak{P}$ contains $\mathfrak{P}_i$:

CLAIM: *For each $i \neq j$ $\mathfrak{P}_i \neq \mathfrak{P}_j$ or $\mathfrak{P}_i = \mathcal{O}_L = \mathfrak{P}_j$. Moreover $\mathfrak{p}\mathcal{O}_L \subseteq \mathfrak{P}_i$ $(1 \leq i \leq r)$, and $\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} \subseteq \mathfrak{p}\mathcal{O}_L$.*

PROOF: Let $i \neq j$ be between 1 and r and suppose that $\mathfrak{P}_i = \mathfrak{P}_j$. Since $\bar{P}_i(X)$ and $\bar{P}_j(X)$ are distinct monic irreducible polynomials over $\bar{K}_{\mathfrak{p}}$, $\gcd(\bar{P}_i(X), \bar{P}_j(X)) = 1$. Therefore, there exist polynomials $\bar{u}, \bar{v} \in \bar{K}_{\mathfrak{p}}[X]$ such that $\bar{u}\bar{P}_i + \bar{v}\bar{P}_j = 1$. Hence, there exist polynomials $u, v \in \mathcal{O}[X]$ and a polynomial $w \in \mathfrak{p}[X]$ such that $u(X)P_i(X) + v(X)P_j(X) = 1 + w(X)$. Thus, since $u(\eta)P_i(\eta) \in \mathfrak{P}_i$, $v(\eta)P_j(\eta) \in \mathfrak{P}_j$ and $w(\eta) \in \mathfrak{p}\mathcal{O}_L$, it follows from the assumption that $1 = u(\eta)P_i(\eta) + v(\eta)P_j(\eta) - w(\eta) \in \mathfrak{P}_i$, and therefore $\mathfrak{P}_i = \mathfrak{P}_j = \mathcal{O}_L$.

It is clear that $\mathfrak{p}\mathcal{O}_L \subseteq \mathfrak{p}\mathcal{O}_L + P_i(\eta)\mathcal{O}_L = \mathfrak{P}_i, \quad i = 1, \ldots, r.$

Finally, since $f(X) - P_1(X)^{e_1} \cdots P_r(X)^{e_r} \in \mathfrak{p}[X]$ and $f(\eta) = 0$,

$$P_1(\eta)^{e_1} \cdots P_r(\eta)^{e_r} \in \mathfrak{p}\mathcal{O}_L\,.$$

Also, $\mathfrak{P}_i^{e_i} \subseteq \mathfrak{p}\mathcal{O}_L + P_i(\eta)^{e_i}\mathcal{O}_L$, $i = 1, \ldots, r$. Hence,

$$\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} \subseteq \mathfrak{p}\mathcal{O}_L + P_1(\eta)^{e_1} \cdots P_r(\eta)^{e_r}\mathcal{O}_L \subseteq \mathfrak{p}\mathcal{O}_L\,,$$

and the claim is proved.

Now, let $\mathfrak{p} \in P$ and find $\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_L + P_i(\eta)\mathcal{O}_L$, $i = 1, \ldots, r$, and I as above. If $\mathfrak{p} \nmid I$, i.e if $I \not\subseteq \mathfrak{p}$, then we have finished. Otherwise, we throw out all the $\mathfrak{P}_i = \mathcal{O}_L$ in order to assume that $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ are distinct proper ideals of $\mathcal{O}_L$. It follows from the claim that the set of all prime ideals $\mathfrak{P} \in P_L$ which lie over $\mathfrak{p}$ is the set of all prime ideals of $\mathcal{O}_L$ which contain one of the ideals $\mathfrak{P}_i$, $i = 1, \ldots, r$. By Lemma A.14 we find all the prime ideals $\mathfrak{P} \in P_L$ which contain one of the ideals $\mathfrak{P}_i$. These are all the prime ideals $\mathfrak{P} \in P_L$ which lie over $\mathfrak{p}$

Proposition A.17. *Let $\mathfrak{a} = (x_1, \ldots, x_k)\mathcal{O}_L$ be an ideal of $\mathcal{O}_L$. Then, one can effectively factor $\mathfrak{a}$ into a product of prime ideals of $\mathcal{O}_L$.*

Proof. We find, by Lemma 2.13, the norm $N_{L/K}(\mathfrak{a})$ and factor it into a product of prime ideals $\mathfrak{p} \in P$. For each $\mathfrak{p} \in P$ such that $\mathfrak{p} \mid N_{L/K}(\mathfrak{a})$ we find, by Proposition A.15, the set $I_{\mathfrak{p}} = \{\mathfrak{P} \in P_L \mid \mathfrak{P} \supseteq \mathfrak{p}\mathcal{O}_L\}$ and denote $A = \bigcup_{\mathfrak{p} \mid N_{L/K}(\mathfrak{a})} I_{\mathfrak{p}}$. Then, if $\mathfrak{P} \in P_L$ contains $\mathfrak{a}$, then it is necessarily in A. By Corollary A.11, we find, for each $\mathfrak{P} \in A$, the multiplicity $e = e_{\mathfrak{P}}$, $e \geq 0$, of $\mathfrak{P}$ in $\mathfrak{a}$ by checking $\mathfrak{a} \subseteq \mathfrak{P}^i$, $i = 0, 1, \ldots, e$, and $\mathfrak{a} \not\subseteq \mathfrak{P}^{e+1}$. Since $e \leq n$, the number of checks is finite. Then $\mathfrak{a} = \prod_{\mathfrak{P} \in A} \mathfrak{P}^{e_{\mathfrak{P}}}$. $\square$

Remark A.18. Each ideal in a Dedekind ring is generated by two generators that one of them is an arbitrary element of the ideal. In [PoZ89, Section 6.3] they use this fact in order to represent, in more economic way, each ideal of $\mathcal{O}_L$ by two generators that one of them is in $\mathcal{O}$. Also, if $\mathfrak{a} = a\mathcal{O}_L + \alpha\mathcal{O}_L$ and $\mathfrak{b} = b\mathcal{O}_L + \beta\mathcal{O}_L$, with $a, b \in \mathcal{O}$ and $\alpha, \beta \in \mathcal{O}_L$, then, under suitable conditions, we have $\mathfrak{ab} = ab\mathcal{O}_L + \alpha\beta\mathcal{O}_L$.

The difficulty in this technique is that in order to represent an ideal which is given in the form $(x_1, \ldots, x_k)\mathcal{O}_L$ with $k > 2$ by two generators, one must know how to find, for each $a \in \mathcal{O}$, all the α's in $\mathcal{O}_L$ such that $N_{L/K}(\alpha) = a\mathcal{O}$ [PoZ89, Thm. (4.2) in Section 6.4]. The advantage of this technique, however, is that it is more economic in the number of calculations needed to factor an ideal in $\mathcal{O}_L$ into a product of prime ideals.

APPENDIX B. QUANTIFIER'S ELIMINATION IN THE THEORY OF VALUATION RINGS WITH ALGEBRAICALLY CLOSED FRACTION FIELDS

The purpose of this appendix is to show that there exists a primitive recursive procedure of quantifier's elimination in the theory of valuation rings which are not fields and have algebraically closed quotient fields, in the language $\mathcal{L}_{\text{div}}$ which is the language of rings augmented by a binary relation standing for divisibility (Theorem B.24) [Wei84, p. 434, Cor. 3.4(i)]. Subsections B.2, B.3 and B.4 in this appendix are an elaboration of Sections 2 and 3 in the article *"Quantifier elimination and decision procedure for valued fields"* of Weispfenning [Wei84, pp. 428–439].

Subsection B.2 shows how to eliminate (primitive recursively) field-quantifiers from "linear formulas" in the language of valued rings, and in Subsection B.3 we extend the elimination procedure to any formula in the theory of algebraically closed valued fields. The valuation group Γ of an algebraically closed (non trivial) valued field is a non trivial commutative group which is ordered and divisible. In Subsection B.1 we show how to eliminate (in a primitive recursive way) quantifiers in the theory DOG_∞ of non trivial divisible ordered abelian groups with a top element ∞. We are using this result in Subsection B.3 to eliminate the valuation group-quantifiers that were left in the formulas after we have eliminated the field-quantifiers, in order to get a complete and primitive recursive elimination theory of quantifiers in the theory of algebraically closed (non trivial) valued fields. Finally, in Subsection B.4, we reformulate this result in terms of valuation rings.

This work is written, generally, for valuation rings which contain a homomorphic image $\bar{R}$ of a ring R. The procedure of quantifier elimination, which is carried out in the language $\mathcal{L}_{\text{div}}(R)$, is primitive recursive when R is a presented ring, in the definitions of Chapter 19 in the book *"Field Arithmetic"* of Fried and Jarden [FrJ08]. The only reference to this appendix is the article of Weispfenning. Here, however, we are working with the language of rings instead of the language of fields as in Weispfenning.

B.1. **Divisible Ordered Abelian Groups.**

Definition B.1. An abelian group Γ (with an action of addition) is called **divisible** if for every positive integer m and each $y \in \Gamma$ there exists $x \in \Gamma$ such that $y = mx$.

Definition B.2.

a) $\mathcal{L}_\Gamma = \{0, \infty, +, <\}$ is the language of ordered abelian groups with a top element ∞.

b) DOG_∞ is the theory of non trivial (=non zero) divisible ordered abelian groups with top element ∞ in $\mathcal{L}_\Gamma$. The axioms of the theory include, in particular, the axioms $x+\infty=\infty$ for every x and $x<\infty$ if and only if $x\neq\infty$, the axioms of divisibility $(\forall Y)(\exists X)[\,Y=mX\,]$, $m=1,2,\dots$, the axiom that state that the group is not trivial, $\exists X\,[\,X<\infty\wedge X>0\,]$, and the axioms of order,
$X<\infty\wedge Y<Z\to X+Y<X+Z$ and $X<Y\wedge Y<Z\to X<Z$.

Theorem B.3. *There exists a primitive recursive procedure of quantifier elimination in the theory DOG_∞.*

Proof. Let $\varphi(Z_1,\dots,Z_n)$ be a formula in $\mathcal{L}_\Gamma$. By induction on the number of quantifiers in φ it suffices to handle the case when φ is of the form $(\exists X)\psi(X,\mathbf{Z})$, where ψ is quantifier-free. Each term $\alpha=\alpha(X,\mathbf{Z})$ of $\mathcal{L}_\Gamma$ in ψ is of the form $mX+k_1Z_1+\cdots+k_nZ_n$ or of the form $mX+k_1Z_1+\cdots+k_nZ_n+\infty$, where $m,k_1,\dots,k_n\in\mathbb{N}\cup\{0\}$. In the later case $DOG_\infty\models\alpha=\infty$. Hence, ψ is a disjunction of expressions of the form

$$\bigwedge_{i\in\mathcal{I}}\alpha_i(X,\mathbf{Z})=\beta_i(X,\mathbf{Z})\wedge\bigwedge_{j\in\mathcal{J}}\gamma_j(X,\mathbf{Z})<\delta_j(X,\mathbf{Z})\,, \tag{1}$$

where $\alpha_i,\beta_i,\gamma_j,\delta_j$ are terms of $\mathcal{L}_\Gamma$. Note that $DOG_\infty\models\alpha\neq\beta\leftrightarrow(\alpha>\beta\vee\alpha<\beta)$. We replace ψ by the following disjunction of conjunctions

$$[X=\infty\wedge\psi(X,\mathbf{Z})]\vee\bigvee_{I\subseteq\{1,\dots,n\}}[X<\infty\wedge\bigwedge_{i\in I}Z_i<\infty\wedge\bigwedge_{j\in I'}Z_j=\infty\wedge\psi(X,\mathbf{Z})]\,,$$

where $I'=\{1,\dots,n\}\setminus I$. If a term of the form $mX+k_1Z_1+\cdots+k_nZ_n$ with $m\neq0$ (resp., $k_i\neq0$) appears in the conjunction (1) and one of the conjuncts is $X=\infty$ (resp., $Z_i=\infty$), we replace the term by ∞.

We introduce the symbol $\triangleleft$ to stand for one of the three relations $=$, $<$ or $>$. If the conjunction (1) contains the conjunction $(X<\infty)\wedge\bigwedge_{i\in I}(Z_i<\infty)$, then each term of the form $\alpha(X,\mathbf{Z})\triangleleft\beta(X,\mathbf{Z})$ which occurs in (1), that does not contain Z_j for every $j\in I'$, can be replaced, using a transfer from one side to another, by an expression of the form

$$mX+\gamma(\mathbf{Z})\triangleleft\gamma'(\mathbf{Z})\,,$$

where $m\in\mathbb{N}\cup\{0\}$, $\gamma(\mathbf{Z})=\sum_{i\in I}k_iZ_i$ and $\gamma'(\mathbf{Z})=\sum_{i\in I}k'_iZ_i$ with $k_i,k'_i\in\mathbb{N}\cup\{0\}$. Hence, modulo DOG_∞, ψ is a disjunction of an expression of the form $X=\infty\wedge\theta(\mathbf{Z})$, where θ is a quantifier-free formula which does not contain X, and expressions of the form

$$\begin{aligned}&X<\infty\wedge\bigwedge_{i\in I}Z_i<\infty\wedge\bigwedge_{j\in I'}Z_j=\infty\\&\wedge\bigwedge_{i\in\mathcal{I}}m_iX+\alpha_i(\mathbf{Z}_I)=\alpha'_i(\mathbf{Z}_I)\wedge\bigwedge_{j\in\mathcal{J}}m_jX+\beta_j(\mathbf{Z}_I)<\beta'_j(\mathbf{Z}_I)\\&\wedge\bigwedge_{k\in\mathcal{K}}m_kX+\gamma_k(\mathbf{Z}_I)>\gamma'_k(\mathbf{Z}_I)\wedge\theta(\mathbf{Z}_I)\,,\end{aligned} \tag{2}$$

where $m_l\in\mathbb{N}$; $\mathbf{Z}_I=(Z_i|\,i\in I)$; $\alpha_i,\beta_j,\gamma_k$ are expressions of the form $\sum_{l\in I}k_lZ_l$ with $k_l\in\mathbb{N}\cup\{0\}$; $\alpha'_i,\beta'_j,\gamma'_k$ are expressions of the form $\sum_{l\in I}k'_lZ_l$ with $k'_l\in\mathbb{N}\cup\{0\}$ or ∞;

and θ is a quantifier-free formula which does not contain X. Let m be a common multiple of all the m_l's. Then (2) is equivalent to the expression

$$\begin{aligned} & X < \infty \wedge \bigwedge_{i\in I} Z_i < \infty \wedge \bigwedge_{j\in I'} Z_j = \infty \\ \wedge & \bigwedge_{i\in\mathcal{I}} mX + \frac{m}{m_i}\alpha_i(\mathbf{Z}_I) = \frac{m}{m_i}\alpha_i'(\mathbf{Z}_I) \wedge \bigwedge_{j\in\mathcal{J}} mX + \frac{m}{m_j}\beta_j(\mathbf{Z}_I) < \frac{m}{m_j}\beta_j'(\mathbf{Z}_I) \\ \wedge & \bigwedge_{k\in\mathcal{K}} mX + \frac{m}{m_k}\gamma_k(\mathbf{Z}_I) > \frac{m}{m_k}\gamma_k'(\mathbf{Z}_I) \wedge \theta(\mathbf{Z}_I)\,. \end{aligned}$$

It suffices to handle, then, the case when φ is of the form

$$\begin{aligned} (3)\quad (\exists X)[X < \infty \wedge & \bigwedge_{i\in I} Z_i < \infty \wedge \bigwedge_{j\in I'} Z_j = \infty \\ & \wedge \bigwedge_{i\in\mathcal{I}} mX + \alpha_i(\mathbf{Z}_I) = \alpha_i'(\mathbf{Z}_I) \wedge \bigwedge_{j\in\mathcal{J}} mX + \beta_j(\mathbf{Z}_I) < \beta_j'(\mathbf{Z}_I) \\ & \wedge \bigwedge_{k\in\mathcal{K}} mX + \gamma_k(\mathbf{Z}_I) > \gamma_k'(\mathbf{Z}_I) \wedge \theta(\mathbf{Z}_I)]\,, \end{aligned}$$

where $m \in \mathbb{N}$ and $\alpha_i, \alpha_i', \beta_j, \beta_j', \gamma_k, \gamma_k'$ and θ are as above.

Let $\psi(X, \mathbf{Z})$ be the formula

$$\begin{aligned} (4)\qquad & X < \infty \wedge \bigwedge_{i\in I} Z_i < \infty \wedge \bigwedge_{j\in I'} Z_j = \infty \\ \wedge & \bigwedge_{i\in\mathcal{I}} X + \alpha_i(\mathbf{Z}_I) = \alpha_i'(\mathbf{Z}_I) \wedge \bigwedge_{j\in\mathcal{J}} X + \beta_j(\mathbf{Z}_I) < \beta_j'(\mathbf{Z}_I) \\ \wedge & \bigwedge_{k\in\mathcal{K}} X + \gamma_k(\mathbf{Z}_I) > \gamma_k'(\mathbf{Z}_I) \wedge \theta(\mathbf{Z}_I)\,. \end{aligned}$$

It follows, by the divisibility axiom $(\forall Y)(\exists X)[mX = Y]$ in DOG_∞, that

$$DOG_\infty \models \varphi(\mathbf{Z}) \leftrightarrow (\exists X)[\psi(mX, \mathbf{Z})] \leftrightarrow (\exists Y)[\psi(Y, \mathbf{Z})]\,.$$

Hence we can assume, without loss, that $m = 1$ and $\varphi(\mathbf{Z})$ is the formula $(\exists X)\psi(X, \mathbf{Z})$. We denote the following quantifier-free formula in $\mathcal{L}_\Gamma$ by $\chi(\mathbf{Z})$:

$$\begin{aligned} & \bigwedge_{i\in I} Z_i < \infty \wedge \bigwedge_{j\in I'} Z_i = \infty \wedge \theta(\mathbf{Z}_I) \wedge \bigwedge_{i\in\mathcal{I}} \alpha_i'(\mathbf{Z}_I) < \infty \wedge \bigwedge_{k\in\mathcal{K}} \gamma_k'(\mathbf{Z}_I) < \infty \\ \wedge & \bigwedge_{(i,l)\in\mathcal{I}^2} (\alpha_i'(\mathbf{Z}_I) + \alpha_l(\mathbf{Z}_I) = \alpha_i(\mathbf{Z}_I) + \alpha_l'(\mathbf{Z}_I)) \\ \wedge & \bigwedge_{(i,j)\in\mathcal{I}\times\mathcal{J}} (\alpha_i'(\mathbf{Z}_I) + \beta_j(\mathbf{Z}_I) < \alpha_i(\mathbf{Z}_I) + \beta_j'(\mathbf{Z}_I)) \\ \wedge & \bigwedge_{(i,k)\in\mathcal{I}\times\mathcal{K}} (\alpha_i'(\mathbf{Z}_I) + \gamma_k(\mathbf{Z}_I) > \alpha_i(\mathbf{Z}_I) + \gamma_k'(\mathbf{Z}_I)) \\ \wedge & \bigwedge_{(j,k)\in\mathcal{J}\times\mathcal{K}} (\beta_j'(\mathbf{Z}_I) + \gamma_k(\mathbf{Z}_I) > \beta_j(\mathbf{Z}_I) + \gamma_k'(\mathbf{Z}_I))\,. \end{aligned}$$

CLAIM: $DOG_\infty \models \varphi(\mathbf{Z}) \leftrightarrow \chi(\mathbf{Z})$. Indeed, it is clear that $DOG_\infty \models \varphi(\mathbf{Z}) \rightarrow \chi(\mathbf{Z})$. Conversely, let $\Gamma \cup \{\infty\}$ be a model of DOG_∞, where Γ is a non trivial divisible ordered abelian group, and let $z_1, \ldots, z_n \in \Gamma \cup \{\infty\}$ be such that $\Gamma \cup \{\infty\} \models \chi(\mathbf{Z})$. In particular, $z_i \in \Gamma$ for each $i \in I$ and $z_j = \infty$ for each $j \in I'$. We have to show that there exists $x \in \Gamma$ such that $\Gamma \cup \{\infty\} \models \psi(x, \mathbf{z})$. We denote $\mathbf{z}_I = (z_i | \, i \in I)$; then $\alpha_i'(\mathbf{z}_I) < \infty$ for each $i \in \mathcal{I}$ and $\gamma_k'(\mathbf{z}_I) < \infty$ for each $k \in \mathcal{K}$.

If $\mathcal{I} \neq \emptyset$ we choose $i_0 \in \mathcal{I}$. Then, with $x = \alpha'_{i_0}(\mathbf{z}_I) - \alpha_{i_0}(\mathbf{z})$, $\Gamma \cup \{\infty\} \models \psi(x, \mathbf{z})$. Suppose, then, that $\mathcal{I} = \emptyset$. In this case $\chi(\mathbf{Z})$ reduces to the conjunction

$$\bigwedge_{i\in I} Z_i < \infty \wedge \bigwedge_{j\in I'} Z_i = \infty \wedge \theta(\mathbf{Z}_I) \wedge \bigwedge_{k\in\mathcal{K}} \gamma'_k(\mathbf{Z}_I) < \infty$$
$$\wedge \bigwedge_{(j,k)\in\mathcal{J}\times\mathcal{K}} (\beta'_j(\mathbf{Z}_I) + \gamma_k(\mathbf{Z}_I) > \beta_j(\mathbf{Z}_I) + \gamma'_k(\mathbf{Z}_I)) .$$

Suppose first that $\mathcal{J} \neq \emptyset$ and $\mathcal{K} \neq \emptyset$. We denote $\beta = \min_{j\in\mathcal{J}}\{\beta'_j(\mathbf{z}_I) - \beta_j(\mathbf{z}_I)\}$ and $\gamma = \max_{k\in\mathcal{K}}\{\gamma'_k(\mathbf{z}_I) - \gamma_k(\mathbf{z}_I)\}$. Then $\gamma < \beta$. If $\beta < \infty$, then, since Γ is a divisible group, there exists $x \in \Gamma$ such that $2x = \beta + \gamma$. This x satisfies $\gamma'_k(\mathbf{z}_I) - \gamma_k(\mathbf{z}_I) \leq \gamma < x < \beta \leq \beta'_j(\mathbf{z}_I) - \beta_j(\mathbf{z}_I)$ for each $j \in \mathcal{J}$ and $k \in \mathcal{K}$ and therefore $\Gamma \cup \{\infty\} \models \psi(x, \mathbf{z})$. If $\beta = \infty$, then $x = 2 \cdot \max\{\gamma, -\gamma\}$ satisfies $\gamma'_k(\mathbf{z}_I) - \gamma_k(\mathbf{z}_I) \leq \gamma < x < \infty = \beta'_j(\mathbf{z}_I) - \beta_j(\mathbf{z}_I)$ for each $j \in \mathcal{J}$ and $k \in \mathcal{K}$; hence, again, $\Gamma \cup \{\infty\} \models \psi(x, \mathbf{z})$.

Suppose now that $\mathcal{J} = \emptyset$ and $\mathcal{K} \neq \emptyset$. In this case $\chi(\mathbf{Z})$ is

$$\bigwedge_{i\in I} Z_i < \infty \wedge \bigwedge_{j\in I'} Z_i = \infty \wedge \theta(\mathbf{Z}_I) \wedge \bigwedge_{k\in\mathcal{K}} \gamma'_k(\mathbf{Z}_I) < \infty .$$

We denote $\gamma = \max_{k\in\mathcal{K}}\{\gamma'_k(\mathbf{z}_I) - \gamma_k(\mathbf{z}_I)\}$. Since Γ is not trivial, there exists $0 < \delta \in \Gamma$. Hence $x = \gamma + \delta$ satisfies $x > \gamma'_k(\mathbf{z}_I) - \gamma_k(\mathbf{z}_I)$ for each $k \in \mathcal{K}$ and thus $\Gamma \cup \{\infty\} \models \psi(x, \mathbf{z})$.

Finally, suppose that $\mathcal{J} \neq \emptyset$ and $\mathcal{K} = \emptyset$. We denote $\beta = \min_{j\in\mathcal{J}}\{\beta'_j(\mathbf{z}_I) - \beta_j(\mathbf{z}_I)\}$. If $\beta = \infty$ we choose $x = 0$ and if $\beta < \infty$ we choose $x = \beta - \delta$, where $0 < \delta \in \Gamma$ is some element. In any case, $x < \beta \leq \beta'_j(\mathbf{z}_I) - \beta_j(\mathbf{z}_I)$ for each $j \in \mathcal{J}$ and therefore $\Gamma \cup \{\infty\} \models \psi(x, \mathbf{z})$. The case $\mathcal{J} = \mathcal{K} = \emptyset$ is trivial. □

B.2. **Linear Problems in Valued Fields.**

Definition B.4.

a) $\mathcal{L} = \{0, 1, +, -, \cdot\}$ is the language of rings.
For a ring R we denote the language $\mathcal{L}$ augmented by a constant symbol for each element of R by $\mathcal{L}(R)$. In every ring which contains a homomorphic image $\bar{R}$ of R, these symbols are interpreted as elements of $\bar{R}$ which satisfy the additive and multiplicative tables of corresponding elements of R.

b) $\mathcal{L}_{\mathrm{VR}} = (\mathcal{L}, \mathcal{L}_\Gamma, v)$ is the language of valued rings.
For a ring R, $\mathcal{L}_{\mathrm{VR}}(R) = (\mathcal{L}(R), \mathcal{L}_\Gamma, v)$.

c) VF is the theory of valued fields in the language $\mathcal{L}_{\mathrm{VR}}$. In each valued field, (F, v_F), the function symbol v is interpreted as the valuation v_F. We denote the valuation group $v_F(F^\times)$ of F by Γ_F. Then, Γ_F is an ordered abelian group and $v_F : F \to \Gamma_F \cup \{\infty\}$ is surjective.

d) For a ring R, we denote by $VF(R)$ the theory, in the language $\mathcal{L}_{\mathrm{VR}}(R)$, whose models are valued fields (F, v_F) such that F contains a homomorphic image $\bar{R}$ of R and v_F is integral on $\bar{R}$. That is, $VF(R)$ contains in addition the axioms $v(a) \geq 0$ for each $a \in R$.

e) If (F, v) is a model of VF, we denote the residue field of F at v by $\bar{F} = \bar{F}_v$. If x is an element of F such that $v(x) \geq 0$, we denote the reduction modulo v by $\bar{x}$. If $f(X) = a_nX^n + \cdots + a_1X + a_0$ is a polynomial in $F[X]$, we denote $v(f) = \min_{0\leq i\leq n}\{v(a_i)\}$. If $v(f) \geq 0$, we denote $\bar{f}(X) = \bar{a}_nX^n + \cdots + \bar{a}_1X + \bar{a}_0$.

f) $\mathcal{L}_{\mathrm{VR}}^{E}$ (resp., $\mathcal{L}_{\mathrm{VR}}^{E}(R)$) is the language $\mathcal{L}_{\mathrm{VR}}$ (resp., $\mathcal{L}_{\mathrm{VR}}(R)$) augmented by the symbols E_n, for each positive integer n, to be interpreted in every valued field (F, v) by

$$|\bar{F}| \geq n \Leftrightarrow (F, v) \models E_n \,.$$

E_n can be defined in the language $\mathcal{L}_{\mathrm{VR}}$ by the sentence

$$\epsilon_n : (\exists X_1)\cdots(\exists X_{n-1})[\bigwedge_{i=1}^{n-1} v(X_i) = 0 \wedge \bigwedge_{1\leq i<j\leq n-1} v(X_i - X_j) = 0\,].$$

Indeed, in every valued field (F, v), $(F, v) \models \epsilon_n$ if and only if $|\bar{F}^{\times}| \geq n-1$ (or $|\bar{F}| \geq n$).

Notation B.5. We denote $\mathcal{L}$-variables (which will be called field-variables or F-variables) by $X, Y, \ldots$, $\mathcal{L}(R)$-terms (which will be called F-terms) by $a, b, \ldots$, $\mathcal{L}_\Gamma$-variables (Γ-variables) by $\xi, \eta, \ldots$, and Γ-terms in $\mathcal{L}_{\mathrm{VR}}(R)$ (including Γ-terms in $\mathcal{L}_\Gamma$) by $\alpha, \beta, \ldots$. F-quantifiers (i.e. $\mathcal{L}$-quantifiers) are quantifiers of the form $\exists X, \forall X$ and Γ-quantifiers ($\mathcal{L}_\Gamma$-quantifiers) are quantifiers of the form $\exists\xi, \forall\xi$.

Remark B.6.

a) *let $\varphi(X_1, \ldots, X_n, \eta_1, \ldots, \eta_k)$ be a quantifier-free formula in the language $\mathcal{L}_{\mathrm{VR}}(R)$. Then there exist a positive integer m, polynomials $a_1, \ldots, a_m \in R[X_1, \ldots, X_n]$, and a quantifier-free formula*

$$\psi(\xi_1, \ldots, \xi_m, \eta_1, \ldots, \eta_k)$$

in the language $\mathcal{L}_\Gamma$ such that

$$VF(R) \models \varphi(\mathbf{X}, \boldsymbol{\eta}) \leftrightarrow (\exists\boldsymbol{\xi})[\,\psi(\boldsymbol{\xi}, \boldsymbol{\eta}) \wedge \bigwedge_{i=1}^{m} v(a_i(\mathbf{X})) = \xi_i\,].$$

Indeed, note that each F-term a is a polynomial and that $a = 0 \leftrightarrow v(a) = \infty$. Hence, we can write φ in the form

$$\psi(v(a_1(\mathbf{X})), \ldots, v(a_m(\mathbf{X})), \boldsymbol{\eta})\,,$$

where $a_1, \ldots, a_m$ are all the F-terms that occur in φ and $\psi(\xi_1, \ldots, \xi_m, \boldsymbol{\eta})$ is a quantifier-free formula in the language $\mathcal{L}_\Gamma$. Thus φ is equivalent to the desired formula modulo $VF(R)$.

b) *Let $\varphi(T, X_1, \ldots, X_n, \eta_1, \ldots, \eta_k)$ be an F-quantifier-free formula in $\mathcal{L}_{\mathrm{VR}}(R)$. Then, there is an F-quantifier-free formula $\varphi'(X_1, \ldots, X_n, Y, Z, \eta_1, \ldots, \eta_k)$ in the language $\mathcal{L}_{\mathrm{VR}}(R)$ such that*

$$VF(R) \models Z \neq 0 \wedge (\exists T)[\,Y = ZT \wedge \varphi(T, \mathbf{X}, \boldsymbol{\eta})\,] \leftrightarrow \varphi'(\mathbf{X}, Y, Z, \boldsymbol{\eta})\,.$$

Indeed, by a), we can assume that $\varphi(T, \mathbf{X}, \boldsymbol{\eta})$ is the formula

$$(\exists\boldsymbol{\xi})[\,\psi(\boldsymbol{\xi}, \boldsymbol{\eta}) \wedge \bigwedge_{i=1}^{m} v(\sum_{j=0}^{n_i} a_{ij}(\mathbf{X})T^j) = \xi_i\,],$$

where $a_{ij} \in R[\mathbf{X}]$ and ψ is a formula in the language $\mathcal{L}_\Gamma$. Hence

$$\begin{aligned} VF(R) \models\ & Z \neq 0 \wedge (\exists T)[\,Y = ZT \wedge \varphi(T, \mathbf{X}, \boldsymbol{\eta})\,] \leftrightarrow \\ & Z \neq 0 \wedge (\exists\boldsymbol{\xi})[\,\psi(\boldsymbol{\xi}, \boldsymbol{\eta}) \wedge \bigwedge_{i=1}^{m} v(\sum_{j=0}^{n_i} a_{ij}(\mathbf{X})Y^j Z^{n_i-j}) = \xi_i + n_i v(Z)\,]\,. \end{aligned}$$

Definition B.7. Let $\mathbf{X} = (X_1, \ldots, X_n)$ be a tuple of F-variables. We say that an F-term a of $\mathcal{L}(R)$ is **linear in X** if a is of the form $a = a_1X_1 + \cdots + a_nX_n + a'$, where $a_1, \ldots, a_n, a'$ are F-terms in which $\mathbf{X}$, i.e. each X_i, does not occur. We say that a Γ-term α of $\mathcal{L}_{\mathrm{VR}}(R)$ is **linear in X** if α is of the form $\alpha = \beta(v(a_1), \ldots, v(a_m), \eta_1, \ldots, \eta_k)$, where $\beta(\xi_1, \ldots, \xi_m, \eta_1, \ldots, \eta_k)$ is an $\mathcal{L}_\Gamma$-term and $a_1, \ldots, a_m$ are F-term which are linear in $\mathbf{X}$. We say that a formula φ of $\mathcal{L}_{\mathrm{VR}}(R)$ is **linear in X** if each term which occurs in φ is linear in $\mathbf{X}$. Finally, we call a fomula φ of $\mathcal{L}_{\mathrm{VR}}(R)$ a **linear formula** if φ is linear in the tuple of all F-variable bounded in it.

Lemma B.8. *There is a primitive recursive procedure assigning to any $\mathcal{L}_{\mathrm{VR}}$-formula φ of the form*

$$\bigwedge_{i=1}^{n} [\, \xi_i < \infty \wedge Y_i \neq 0 \wedge v(Y_iX - Z_i) = \xi_i \,]$$

an $\mathcal{L}_{\mathrm{VR}}$-formula φ' and an $\mathcal{L}^E_{\mathrm{VR}}$-formula φ'' such that:

a) $VF \models \varphi \leftrightarrow \varphi' \quad$ *and* $\quad VF \models (\exists X)\varphi \leftrightarrow \varphi''$ *;*
b) *φ' and φ'' are quantifier-free and linear in $\mathbf{Z}$; and*
c) *φ' is the formula*

$$a \neq 0 \wedge \bigvee_{\emptyset \neq I \subseteq \{1,\ldots,n\}} [\, \alpha_I < \infty \wedge \bigwedge_{i \in I} (\alpha_i = \alpha_I) \wedge \bigwedge_{i \in I} (v(aX - b_i) = \alpha_I) \wedge \bigwedge_{\substack{(i,j) \in I^2 \\ i \neq j}} (v(b_i - b_j) = \alpha_I) \wedge \chi_I \,],$$

where $a = \prod_{i=1}^{n} Y_i$; with $a_i = \prod_{\substack{j=1 \\ j \neq i}}^{n} Y_j$, $b_i = a_iZ_i$ and $\alpha_i = \xi_i + v(a_i)$, $i = 1, \ldots, n$; and, for $\emptyset \neq I \subseteq \{1, \ldots, n\}$, α_I is any element in $\{\alpha_i \mid i \in I\}$ and χ_I is a quantifier-free $\mathcal{L}_{\mathrm{VR}}$-formula in which X does not occur.

Hence, φ' is a disjunction of formulas of the form

$$(1) \qquad a \neq 0 \wedge \alpha_I < \infty \wedge \bigwedge_{i \in I} (v(aX - b_i) = \alpha_I) \wedge \bigwedge_{\substack{(i,j) \in I^2 \\ i \neq j}} (v(b_i - b_j) = \alpha_I) \wedge \chi'_I \,,$$

where χ'_I is a quantifier-free $\mathcal{L}_{\mathrm{VR}}$-formula; the variables Z_i do not occur in a; and X does not occur in a, b_i $(i \in I)$, α_I and χ'_I.

Proof. *φ is equivalent to the formula $a \neq 0 \wedge \bigwedge_{i=1}^{n} [\, \alpha_i < \infty \wedge v(aX - b_i) = \alpha_i \,]$.* Indeed, modulo VF,

1. $\bigwedge_{i=1}^{n} Y_i \neq 0 \leftrightarrow a \neq 0$;
2. For each i between 1 and n, $\alpha_i < \infty \to \xi_i < \infty$. Conversely, for each i between 1 and n,

$$[\, (\bigwedge_{j=1}^{n} Y_j \neq 0 \to a_i \neq 0) \wedge (a_i \neq 0 \to v(a_i) < \infty) \wedge (\xi_i < \infty) \,] \to \alpha_i < \infty \,;$$

3. For each i between 1 and n,

$$v(Y_iX - Z_i) = \xi_i \leftrightarrow v(a_iY_iX - a_iZ_i) = \xi_i + v(a_i) \leftrightarrow v(aX - b_i) = \alpha_i\,.$$

We adjoin to φ a disjunction over the possible orderings of the α_i's:

$$\varphi \leftrightarrow \bigvee_{\emptyset\neq I\subseteq\{1,\dots,n\}} [\,\varphi \wedge \bigwedge_{i\in I}(\alpha_i = \alpha_I) \wedge \bigwedge_{i'\in I'}(\alpha_{i'} < \alpha_I)\,]\,,$$

where $I' = \{1,\dots,n\} \smallsetminus I$ and α_I is any element in $\{\alpha_i \,|\, i \in I\}$. Then, *$\varphi$ is equivalent to the disjunction* $\bigvee_{\emptyset\neq I\subseteq\{1,\dots,n\}} (\varphi_I \wedge \psi_I)$, *where*

$$\begin{aligned} (2)\qquad \varphi_I :&\ a \neq 0 \wedge \alpha_I < \infty \wedge \bigwedge_{i\in I}[\,(\alpha_i = \alpha_I) \wedge v(aX - b_i) = \alpha_I\,]\,,\\ \psi_I :&\ \bigwedge_{i'\in I'}[\,(\alpha_{i'} < \alpha_I) \wedge v(b_{i'} - b_I) = \alpha_{i'}\,]\,, \end{aligned}$$

and b_I is any element in $\{b_i \,|\, i \in I\}$.

Indeed, for $i' \in I'$,

$$\begin{aligned} VF \models [\,(\alpha_{i'} < \alpha_I) \wedge v(aX - b_I) = \alpha_I\,] \rightarrow\\ [\,v(aX - b_{i'}) = \alpha_{i'} \leftrightarrow v(b_{i'} - b_I) = \alpha_{i'}\,]\,, \end{aligned}$$

since, if $v(b_{i'} - b_I) = \alpha_{i'}$, then $v(aX - b_{i'}) = v((aX - b_I) - (b_{i'} - b_I)) = \alpha_{i'}$ and if $v(aX - b_{i'}) = \alpha_{i'}$, then $v(b_{i'} - b_I) = v((aX - b_I) - (aX - b_{i'})) = \alpha_{i'}$.

Let $\emptyset \neq I \subseteq \{1,\dots,n\}$; for each $(i,j) \in I^2$, $v(b_j - b_i) = v((aX - b_i) - (aX - b_j)) \geq \alpha_I$. We adjoin to φ_I a disjunction over the possible values of $v(b_j - b_i)$ for $i, j \in I$:

$$\varphi_I \leftrightarrow \bigvee_{\emptyset\neq J\subseteq I} [\,\varphi_I \wedge \bigwedge_{\substack{(j,j')\in J^2\\ j\neq j'}} (v(b_j - b_{j'}) = \alpha_I) \wedge \bigwedge_{i\in I\smallsetminus J} (\bigvee_{j\in J}(v(b_j - b_i) > \alpha_I))\,]\,.$$

Then, *φ_I is equivalent to the disjunction* $\bigvee_{\emptyset\neq J\subseteq I} (\varphi'_J \wedge \psi'_{I,J})$, *where*

$$\begin{aligned} (3)\qquad \varphi'_J :&\ a \neq 0 \wedge \alpha_J < \infty \wedge \bigwedge_{j\in J}[\,(\alpha_j = \alpha_J) \wedge v(aX - b_j) = \alpha_J\,]\\ &\wedge \bigwedge_{\substack{(j,j')\in J^2\\ j\neq j'}} v(b_j - b_{j'}) = \alpha_J \end{aligned}$$

and

$$\psi'_{I,J} :\ \bigwedge_{i\in I\smallsetminus J} (\alpha_i = \alpha_J) \wedge (\bigvee_{j\in J} v(b_j - b_i) > \alpha_J)\,.$$

Indeed, let $\emptyset \neq J \subseteq I$ and suppose that for each $j \in J$, $v(aX - b_j) = \alpha_J$, and for each $i \in I \smallsetminus J$ there exists $j \in J$ such that $v(b_j - b_i) > \alpha_J$. Then $v(aX - b_i) = v((aX - b_j) + (b_j - b_i)) = \alpha_J$.

We add (2) and (3) and get, modulo VF, that

$$\begin{aligned} \varphi &\leftrightarrow \bigvee_{\emptyset\neq I\subseteq\{1,\dots,n\}} (\varphi_I \wedge \psi_I) \leftrightarrow \bigvee_{\emptyset\neq I\subseteq\{1,\dots,n\}}\ [\ \bigvee_{\emptyset\neq J\subseteq I} (\varphi'_J \wedge \psi'_{I,J}) \wedge \psi_I\,]\\ &\leftrightarrow \bigvee_{\emptyset\neq J\subseteq\{1,\dots,n\}} (\varphi'_J \wedge \chi_J)\,, \end{aligned}$$

where $\chi_J : \bigvee_{J\subseteq I\subseteq\{1,\dots,n\}} (\psi'_{I,J} \wedge \psi_I)$ is a quantifier-free $\mathcal{L}_{\mathrm{VR}}$-formula in which X does not occur. Then

$$\varphi' : \bigvee_{\emptyset\neq I\subseteq\{1,\dots,n\}} (\varphi'_I \wedge \chi_I)$$

is the desired formula. Since Z_i occurs only in $b_i = a_i Z_i$ and the terms containing the b_i's are only of the form $v(aX - b_i)$ and $v(b_j - b_i)$, it follows that φ' is linear in $\mathbf{Z}$.

It is left to construct the formula φ'' in the language $\mathcal{L}^E_{\mathrm{VR}}$ such that $VF \models (\exists X)\varphi \leftrightarrow \varphi''$. For $\emptyset \neq I \subseteq \{1,\dots,n\}$, we denote

$$\varphi''_I : E_{|I|+1} \wedge a \neq 0 \wedge \alpha_I < \infty \wedge \bigwedge_{i\in I}(\alpha_i = \alpha_I) \wedge \bigwedge_{\substack{(i,j)\in I^2\\ i\neq j}} v(b_i - b_j) = \alpha_I \,.$$

Then φ''_I is a quantifier-free formula in the language $\mathcal{L}^E_{\mathrm{VR}}$ and φ''_I is linear in $\mathbf{Z}$.

CLAIM: $VF \models (\exists X)\varphi'_I \leftrightarrow \varphi''_I$. Indeed, let (F, v) be a valued field with valuation group Γ, let $\alpha \in \Gamma$, let $0 \neq a \in F$, and let $b_i \in F$ $(i \in I)$ be such that $v(b_i - b_j) = \alpha$ for $i \neq j$. We have to show that

$$(F, v) \models (\exists X)[\bigwedge_{i\in I} v(aX - b_i) = \alpha\,] \leftrightarrow E_{|I|+1}\,.$$

Let $0 \neq b \in F$ be such that $v(b) = \alpha - v(a)$. Then,

$$\begin{aligned}(\exists X)[\bigwedge_{i\in I} v(aX - b_i) = \alpha\,] &\leftrightarrow (\exists X)[\bigwedge_{i\in I} v(X - \frac{b_i}{a}) = \alpha - v(a)\,]\\ &\leftrightarrow (\exists X)[\bigwedge_{i\in I} v(\frac{X}{b} - \frac{b_i}{ab}) = 0\,]\\ &\leftrightarrow (\exists Y)[\bigwedge_{i\in I} v(Y - c_i) = 0\,],\end{aligned}$$

where $c_i = \frac{b_i}{ab}$, $i \in I$. Also, for $i \neq j$,

$$v(c_i - c_j) = v(\frac{b_i}{ab} - \frac{b_j}{ab}) = v(b_i - b_j) - v(a) - v(b) = \alpha - v(a) - v(b) = 0\,.$$

It suffices, then, to show that

$$(F, v) \models (\exists X)[\bigwedge_{i\in I} v(X - c_i) = 0\,] \leftrightarrow E_{|I|+1}\,.$$

Let i_0 be any element in I and let $I' = I \smallsetminus \{i_0\}$. For each $i \in I'$ we denote $d_i = c_i - c_{i_0}$. Then $v(d_i) = 0$ and, for each $i \neq j$ in I',

$$v(d_i - d_j) = v((c_i - c_{i_0}) - (c_j - c_{i_0})) = v(c_i - c_j) = 0\,.$$

That is, the set $\{\bar{d}_i \,|\, i \in I'\}$ has $|I'| = |I| - 1$ distinct elements in $\bar{F}^\times$. Hence

(4) $(F, v) \models E_{|I|+1} \Leftrightarrow \exists\, \bar{d} \in \bar{F}^\times$ s.t. $\bar{d} \notin \{\bar{d}_i \,|\, i \in I'\}$

$$\Leftrightarrow \exists\, d \in F \text{ s.t. } v(d) = 0 \text{ and } v(d - d_i) = 0 \quad \forall\, i \in I'\,.$$

Suppose first that $(F, v) \models E_{|I|+1}$. Then, it follows from (4) that there exists $d \in F$ such that $v(d) = 0$ and $v(d - d_i) = 0$ for each $i \in I'$. Then $x = d + c_{i_0}$ satisfies, for each $i \in I'$,

$$v(x - c_i) = v(d + c_{i_0} - c_i) = v(d - d_i) = 0\,.$$

Also, $v(x - c_{i_0}) = v(d) = 0$; therefore, $v(x - c_i) = 0$ for each $i \in I$.

Conversely, suppose that there exists $x \in F$ such that $v(x-c_i) = 0$ for each $i \in I$. Then $d = x - c_{i_0}$ satisfies that $v(d) = v(x - c_{i_0}) = 0$ and $v(d - d_i) = v(x - c_i) = 0$ for each $i \in I'$. Hence, by (4), $(F, v) \models E_{|I|+1}$. This proves the claim.

Now, $\varphi'' : \bigvee_{\emptyset \neq I \subseteq \{1,\dots,n\}} (\varphi''_I \wedge \chi_I)$ is the desired formula. □

In Subsection B.3 we shall need only the above lemma. However, an immediate corollary from this lemma is

Theorem B.9. *Each linear formula φ in $\mathcal{L}^E_{\mathrm{VR}}(R)$ has an F-quantifier-free linear formula φ' in $\mathcal{L}^E_{\mathrm{VR}}(R)$ such that $VF(R) \models \varphi \leftrightarrow \varphi'$.*

Moreover, if R is a presented ring and φ is a presented formula, then we can effectively find φ'.

Proof. By induction on the number of F-quantifiers in φ, it suffices to handle the case when φ is a formula of the form $(\exists X)\varphi^*(X, \mathbf{Z}, \boldsymbol{\eta})$, where $\mathbf{Z} = (Z_1, \dots, Z_n)$, $\boldsymbol{\eta} = (\eta_1, \dots, \eta_k)$, and $\varphi^*(X, \mathbf{Z}, \boldsymbol{\eta})$ is an $\mathcal{L}_{\mathrm{VR}}(R)$-formula which is F-quantifier-free and linear in $(X, \mathbf{Z})$. By Remark B.6 a), we can assume that φ^* is of the form

$$(\exists \boldsymbol{\xi})[\, \psi(\boldsymbol{\xi}, \boldsymbol{\eta}) \wedge \bigwedge_{i=1}^{m} v(a_i(X, \mathbf{Z})) = \xi_i \,],$$

where $\boldsymbol{\xi} = (\xi_1, \dots, \xi_m)$, $a_i(X, \mathbf{Z}) \in R[X, \mathbf{Z}]$, $i = 1, \dots, m$, and $\psi(\boldsymbol{\xi}, \boldsymbol{\eta})$ is an $\mathcal{L}_\Gamma$-formula. Hence we may assume, without loss, that φ is of the form

$$(\exists X)[\, \bigwedge_{i=1}^{m} v(a_i(X, \mathbf{Z})) = \xi_i \,].$$

Since φ is linear in $(X, \mathbf{Z})$, it follows that a_i is linear in $(X, \mathbf{Z})$, $i = 1, \dots, m$. That is, $a_i(X, \mathbf{Z})$ is of the form

$$a_i(X, \mathbf{Z}) = b_i X + c_i(\mathbf{Z}),$$

where $b_i \in R$, $c_i(\mathbf{Z}) \in R[\mathbf{Z}]$ and c_i is linear in $\mathbf{Z}$, $i = 1, \dots, m$. Hence, modulo $VF(R)$,

$$\begin{aligned} v(a_i(X, \mathbf{Z})) = \xi_i \leftrightarrow{}& (a_i(X, \mathbf{Z}) = 0 \wedge \xi_i = \infty) \vee (\xi_i < \infty \wedge v(a_i(X, \mathbf{Z})) = \xi_i) \\ \leftrightarrow{}& (\,[\,(b_i = 0 \wedge c_i(\mathbf{Z}) = 0) \vee (b_i \neq 0 \wedge b_i X = -c_i(\mathbf{Z}))\,] \\ & \wedge \xi_i = \infty) \vee (\xi_i < \infty \wedge v(b_i X + c_i(\mathbf{Z})) = \xi_i), \end{aligned}$$

and therefore we can reduce to the case that φ is of the form

$$(\exists X)[\, \bigwedge_{i' \in I'} (b_{i'} \neq 0 \wedge b_{i'} X = -c_{i'}(\mathbf{Z})) \wedge \bigwedge_{i \in I} (\xi_i < \infty \wedge v(b_i X + c_i(\mathbf{Z})) = \xi_i)\,],$$

where $I \subseteq \{1, \dots, m\}$ and $I' = \{1, \dots, m\} \setminus I$.

If $I' \neq \emptyset$, we choose $i_0 \in I'$. Then φ is equivalent to the formula

$$\begin{aligned} & \bigwedge_{i' \in I'} (b_{i'} \neq 0 \wedge b_{i_0} c_{i'}(\mathbf{Z}) = b_{i'} c_{i_0}(\mathbf{Z})) \wedge \\ & \bigwedge_{i \in I} (\xi_i < \infty \wedge v(-b_i c_{i_0}(\mathbf{Z}) + b_{i_0} c_i(\mathbf{Z})) = \xi_i + v(b_{i_0})) \end{aligned}$$

which is a quantifier-free formula in $\mathcal{L}_{\mathrm{VR}}(R)$. If $I' = \emptyset$, then φ is the formula

$$(\exists X)[\, \bigwedge_{i \in I} (\xi_i < \infty \wedge v(b_i X + c_i(\mathbf{Z})) = \xi_i)\,].$$

We adjoin to φ a disjunction over the possible options $b_j = 0$ or $b_j \neq 0$:

$$\varphi \leftrightarrow (\exists X)\{\bigwedge_{i\in I} \xi_i < \infty \wedge [\,(b_i = 0 \wedge v(c_i(\mathbf{Z})) = \xi_i) \\ \vee (b_i \neq 0 \wedge v(b_i X + c_i(\mathbf{Z})) = \xi_i)\,]\,\},$$

in order to reduce to the case that φ is the formula

$$(\exists X)(\bigwedge_{i\in I}[\,(\xi_i < \infty) \wedge (b_i \neq 0) \wedge (v(b_i X + c_i(\mathbf{Z})) = \xi_i)\,]\,).$$

Now, we can eliminate the quantifier $\exists X$ using Lemma B.8. □

B.3. **Algebraically Closed Valued Fields.** We continue to hold the notations of Subsection B.2.

Definition B.10.

a) $ACVF$ is the theory of algebraically closed, nontrivially valued fields in the language $\mathcal{L}_{\mathrm{VR}}$.
b) For a ring R, $ACVF(R)$ is the theory, in the language $\mathcal{L}_{\mathrm{VR}}(R)$, whose models are valued field (F, v) which contain a homomorphic image $\bar{R}$ of R and satisfy $(F, v) \models ACVF$ and $(F, v) \models VF(R)$.

Remark B.11. Let (F, v) be a model of $ACVF$ with a valuation group Γ. Then

a) Γ is not trivial, i.e. $\Gamma \neq 0$;
b) $\bar{F}_v$ is an algebraically closed field and, in particular, infinite. Hence, the predicates E_n of Subsection 2 (Definition B.4 f)) are true modulo $ACVF$;
c) Γ is a divisible group (Definition B.1). Indeed, let m be a positive integer and let $\beta \in \Gamma$. We have to show that there exists $\xi \in \Gamma$ such that $\beta = m\xi$. Let $b \in F^\times$ be such that $v(b) = \beta$. Since F is algebraically closed, there exists $x \in F^\times$ such that $x^m = b$. Then, with $\xi = v(x)$, $\beta = v(b) = v(x^m) = mv(x) = m\xi$.

Definition B.12. It is convenient to enlarge the language $\mathcal{L}_\Gamma$ by the n-ary operation symbol $\min_n$, for each positive integer n, which is defined by

$$\min_n(\xi_1, \ldots, \xi_n) = \xi \leftrightarrow \bigvee_{i=1}^{n} (\xi = \xi_i \wedge \bigwedge_{j=1}^{n} \xi \leq \xi_j)\,. \tag{1}$$

So, in any ordered abelian group Γ and for each $\alpha_1, \ldots, \alpha_n \in \Gamma$, $\min_n(\alpha_1, \ldots, \alpha_n)$ is interpreted as the minimal element in the set $\{\alpha_1, \ldots, \alpha_n\}$.

Since these operations can be eliminated in formulas by (1) without introducing new quantifiers, they do not affect the quantifier elimination procedure in the theory DOG_∞ (see Theorem B.3).

Definition B.13.

a) a **formal polynomial in** X of degree $n = \deg(f)$ is an F-term (in the language $\mathcal{L}(R)$) $f(X)$ of the form $\sum_{i=0}^{n} f_i X^i$, where the f_i's are F-terms which do not contain the variable X and f_n is not identically zero (modulo $VF(R)$); f is **monic** if $f_n = 1$. We denote polynomials by $f(X), g(X), h(X), \ldots$; the corresponding tuples of coefficients are then $\mathbf{f} = (f_0, \ldots, f_n), \mathbf{g}, \mathbf{h}, \ldots$.

b) $T(\mathbf{f}, a)$ is the tuple of coefficients of the **Taylor expansion** of $f(X)$ at a; that is, $T(\mathbf{f}, a) = (f_0^*, \dots, f_n^*)$ with $f_k^* = \sum_{i=k}^{n} \binom{i}{k} f_i a^{i-k}$, and the equation $f(X) = f^*(X - a)$ is true in every field which contains a homomorphic image of R.

c) Let $f(X)$ and $g(X)$ be two formal polynomial in X of degrees n and m, respectively. $Q(f, g)$ (resp., $R(f, g)$) is the tuple of coefficients of the **quotient** (resp., **remainder**) of $f(X)$ when formally divided by $g(X)$; i.e., if $Q(f, g) = \mathbf{q}$ and $R(f, g) = \mathbf{r}$, then $q(X)$ is a polynomial of degree $\max\{0, n - m\}$, $r(X)$ is a polynomial of degree $\leq \max\{0, m - 1\}$, and the formula

(2) $$g_m \neq 0 \to f(X) = q(X)g(X) + r(X)$$

is true in every field which contains a homomorphic image of R.

Notation B.14. For a tuple $\mathbf{c} = (c_1, \dots, c_n)$ of F-terms, we denote

$$v(\mathbf{c}) = \min_n(v(c_1), \dots, v(c_n)) .$$

In particular, if f is a formal polynomial in X of degree n, then

$$v(\mathbf{f}) = \min_{n+1}(v(f_0), \dots, v(f_n)) .$$

If, in addition, a is an F-term, we denote $\underline{fa} = (f_0, f_1 a, \dots, f_n a^n)$. Hence

$$v(\underline{fa}) = \min_{n+1}(v(f_0), v(f_1 a), \dots, v(f_n a^n)) .$$

Lemma B.15. *Let $f(X)$ be a monic formal polynomial in X of degree n. Then, the following equivalences hold in $ACVF(R)$:*

(a) $$(\alpha < \infty \wedge v(a) = \alpha) \to [\,(\exists X)(v(X - a) > \alpha \wedge f(X) = 0) \leftrightarrow v(f(a)) > v(\underline{fa})\,] ;$$

(b) $$\alpha < \infty \to [\,(\exists X)(v(X) = \alpha \wedge f(X) = 0) \leftrightarrow \bigvee_{0 \leq i < j \leq n} v(f_i) + i\alpha = v(f_j) + j\alpha = \min_{n+1}(v(f_0), v(f_1) + \alpha, \dots, v(f_n) + n\alpha)\,] .$$

Proof of (a). Let α be a finite $\mathcal{L}_\Gamma$-term and let a be an F-term such that $v(a) = \alpha$. In particular, $a \neq 0$. Let $g(X) = \sum_{i=0}^{n} (f_i a^i) X^i = \sum_{i=0}^{n} g_i X^i$. Then $g_n = a^n \neq 0$, $\mathbf{g} = \underline{fa}$, $g(X) = f(aX)$ and therefore $g(1) = f(a)$. It follows by the subtitution $X = aY$ that, modulo $VF(R)$,

$$(\exists X)[\,v(X - a) > \alpha \wedge f(X) = 0\,] \leftrightarrow (\exists Y)[\,v(a(Y - 1)) > \alpha \wedge f(aY) = 0\,] \leftrightarrow (\exists Y)[\,v(Y - 1) > 0 \wedge g(Y) = 0\,] .$$

Hence it suffices to show that, modulo $ACVF(R)$,

(3) $$(\exists X)[\,v(X - 1) > 0 \wedge g(X) = 0\,] \leftrightarrow v(g(1)) > v(\mathbf{g}) .$$

Indeed, suppose first that the left hand side of (3) holds. Then, modulo $VF(R)$,

$$v(g(1)) = v(0 - g(1)) = v(g(X) - g(1)) = v(\sum_{i=0}^{n} g_i(X^i - 1)) \geq \min_{0 \leq i \leq n} \{v(g_i(X^i - 1))\} > v(\mathbf{g}) ,$$

since $VF \models v(X^i-1) = v(X-1)+v(1+\cdots+X^{i-1}) > 0$; note that $VF \models v(X-1)>0 \to v(X)=0$.

Conversely, let (F,v) be a model of $ACVF(R)$, let $g(X)$ be a (usual) polynomial in $F[X]$ of degree n ($g_n \neq 0$) and suppose that the left hand side of (3) does not hold. Let $c \in F$ be such that $v(c)=v(\mathbf{g})$. Then $c \neq 0$ (since $v(\mathbf{g}) \leq v(g_n) < \infty$) and the polynomial $g'(X) = \frac{1}{c}g(X)$ satisfies $v(\mathbf{g}')=0$. Since $\bar{F}_v$ is infinite (Remark B.11 b)), there exists $\bar{b} \in \bar{F}_v^{\times}$ such that $\overline{g'}(\bar{b}) \neq 0$ and therefore there exists $b \in F$ such that $v(b)=0$ and $v(g'(b))=0$. That is, there exists $b \in F$ which satisfies

$$v(b)=0 \wedge v(g(b)) = v(\mathbf{g})\,. \tag{4}$$

Let

$$g^*(X) = g(X+b) = g_n \cdot (X-c_1)\cdots(X-c_n)$$

with $c_i \in F$ (F is an algebraically closed field). Then

$$g(X) = g^*(X-b) = g_n \cdot (X-(c_1+b))\cdots(X-(c_n+b))\,;$$

hence, $\neg(\exists X)[\, v(X-1)>0 \wedge g(X)=0\,]$ implies

$$\bigwedge_{i=1}^{n} v(c_i+b-1) \leq 0\,. \tag{5}$$

If $v(c_i) \geq 0$, then, by (5), $v(c_i+b-1) \leq v(c_i)$, and if $v(c_i)<0$, then, since $v(b)=0$, $v(c_i+b-1)=v(c_i)$. Thus, in any case,

$$\bigwedge_{i=1}^{n} v(c_i+b-1) \leq v(c_i)\,. \tag{6}$$

Finally, by (6) and (4),

$$\begin{aligned} v(g(1)) = v(g^*(1-b)) &= v(g_n) + \sum_{i=1}^{n} v(1-b-c_i) \\ &\leq v(g_n) + \sum_{i=1}^{n} v(c_i) = v(g_n c_1 \cdots c_n) = v(g_0^*) \\ &= v(g^*(0)) = v(g(b)) = v(\mathbf{g}) \end{aligned}$$

and the right hand side of (3) does not hold.

Proof of (b). Let (F,v) be a model of $ACVF(R)$ and let Γ be the corresponding valuation group. Let $\alpha \in \Gamma$ and let $f(X)$ be a monic polynomial in $F[X]$ of degree n (in particular, $v(\mathbf{f}) \leq v(f_n) = v(1) = 0 < \infty$).

Suppose first that the left hand side of (b) holds. That is, there exists $x \in F$ such that $v(x)=\alpha$ and $f(x)=0$. In particular, $x \neq 0$ (hence $v(x)<\infty$) and $v(f(x)) = \infty$. Therefore $v(f(x)) = \infty > v(\underline{fx})$. If the value $v(\underline{fx}) = \min\limits_{0\leq i\leq n}\{v(f_i x^i)\}$ would have been achieved only by one of the values $v(f_0),\ldots,v(f_n x^n)$, then $v(f(x)) = v(\underline{fx})$, a contradiction. Hence, there exist $0 \leq i < j \leq n$ such that $v(f_i x^i) = v(f_j x^j) = v(\underline{fx})$. Thus

$$v(f_i)+i\alpha = v(f_j)+j\alpha = \min_{n+1}(v(f_0), v(f_1)+\alpha, \ldots, v(f_n)+n\alpha)\,.$$

Conversely, we choose $a \in F$ with $v(a)=\alpha$ (in particular, $a \neq 0$) and define $g(X) = \sum\limits_{i=0}^{n}(f_i a^i)X^i$. Then $g(X) = f(aX)$ and $v(g_k) = v(f_k a^k) = v(f_k)+k\alpha$,

$k = 0, \dots, n$. If, for $0 \le i < j \le n$, $v(f_i) + i\alpha = v(f_j) + j\alpha = \min_{0 \le k \le n} \{v(f_k) + k\alpha\}$, then, since $v(\mathbf{f}) < \infty$,

$$v(g_i) = v(g_j) = v(\mathbf{g}) < \infty \,. \tag{7}$$

We choose $b \in F$ with $v(b) = v(\mathbf{g})$ and define $h(X) = b^{-1}g(X)$. Then, by (7), $v(h_i) = v(h_j) = v(\mathbf{h}) = 0$. Since $\bar{F}_v$ is algebraically closed and $\bar{h}_i, \bar{h}_j \neq 0$, it follows that there exists $0 \neq \bar{c} \in \bar{F}_v$ such that $\bar{h}(\bar{c}) = \sum_{i=0}^{n} \bar{h}_i \bar{c}^i = 0$ (if $\bar{h}(X)$ would have no nonzero roots, then $\bar{h}(X)$ would have been of the form $\bar{h}_k X^k$, with k between 0 and n, in contradiction to the fact that there exist $0 \le i < j \le n$ such that $\bar{h}_i, \bar{h}_j \neq 0$). Hence, there exists $c \in F$ such that $v(c) = 0$ and $v(h(c)) > 0$. That is, there exists $c \in F$ which satisfies

$$v(c) = 0 \wedge v(g(c)) > v(\mathbf{g}) \,.$$

By (a), with $\alpha = 0$, g instead of f and c instead of a, there exists $d \in F$ such that

$$v(d - c) > 0 \wedge g(d) = 0 \,.$$

Hence $f(ad) = g(d) = 0$, $v(d) = v(c) = 0$, and $v(ad) = v(a) = \alpha$. Thus

$$(F, v) \models (\exists X)[\, v(X) = \alpha \wedge f(X) = 0 \,] \,.$$

Lemma B.16. *$ACVF(R)$ admits quantifier elimination, in the language $\mathcal{L}_{\mathrm{VR}}(R)$, for formulas of the form*

$$(\exists X)[\, \bigwedge_{i=1}^{n} v(X - a_i) = \alpha_i \,] \quad \text{and} \tag{a}$$

$$(\exists X)[\, f(X) = 0 \wedge \bigwedge_{i=1}^{n} v(X - a_i) = \alpha_i \,] \,, \tag{b}$$

where the variable X does not occur in α_i, a_i, $i = 1, \dots, n$, and $f(X)$ is a monic formal polynomial of degree m.

Moreover, if R is a presented ring, then there is a primitive recursive procedure of quantifier elimination in the theory $ACVF(R)$ for formulas of the above forms in the language $\mathcal{L}_{\mathrm{VR}}(R)$.

Proof. If there exists i between 1 and n such that $\alpha_i = \infty$, then $X = a_i$ and hence (a) is equivalent to the quantifier-free formula $\bigwedge_{\substack{j=1 \\ j \neq i}}^{n} v(a_i - a_j) = \alpha_j$ and (b) is equivalent to the quantifier-free formula $f(a_i) = 0 \wedge \bigwedge_{\substack{j=1 \\ j \neq i}}^{n} v(a_i - a_j) = \alpha_j$.

Suppose then that $\alpha_i < \infty$, $i = 1, \dots, n$. Then, the elimination of the quantifier from formulas of type (a) is an immediate consequence of Lemma B.8 a), b) and Remark B.11 b). Also, the quantifier elimination for formulas of type (b) reduces, by Lemma B.8 c), to formulas of the form

$$\psi \wedge (\exists X)[\, f(X) = 0 \wedge \bigwedge_{i=1}^{n'} v(X - a'_i) = \alpha \wedge \bigwedge_{1 \le i < j \le n'} v(a'_i - a'_j) = \alpha \,] \,, \tag{8}$$

where $\psi : \alpha < \infty \wedge \chi$, χ is a quantifier-free $\mathcal{L}_{\mathrm{VR}}(R)$-formula which does not contain X, and X does not occur in a'_i, $i = 1, \dots, n'$.

We denote $\mathbf{f}^* = T(\mathbf{f}, a'_1)$ (Definition B.13 b)). Then $f^*_m = 1$, and with $f^*(X) = \sum_{i=0}^{m} f^*_i X^i$, $f(X) = f^*(X - a'_1)$. If $n' = 1$, then, by the subtitution $X' = X - a'_1$, the formula (8) is equivalent to the formula

$$\psi \wedge (\exists X')[\, f^*(X') = 0 \wedge v(X') = \alpha \,]$$

and by Lemma B.15 (b) we can eliminate the quantifier $\exists X'$.

Suppose now that $n' > 1$ and let $b_i = a'_i - a'_1$, $i = 2, \dots, n'$. Then, by the subtitution $X' = X - a'_1$, the formula (8) is equivalent to the formula

$$\psi \wedge \bigwedge_{i=2}^{n'} v(b_i) = \alpha \wedge \bigwedge_{2 \le i < j \le n'} v(b_i - b_j) = \alpha \tag{9}$$
$$\wedge (\exists X')[\, f^*(X') = 0 \wedge v(X') = \alpha \wedge \bigwedge_{i=2}^{n'} v(X' - b_i) = \alpha \,].$$

Let

$$\psi' : \psi \wedge \bigwedge_{i=2}^{n'} v(b_i) = \alpha \wedge \bigwedge_{2 \le i < j \le n'} v(b_i - b_j) = \alpha\,.$$

Then, the formula (9) is equivalent, modulo $ACVF(R)$, to the formula

$$\psi' \wedge (\exists Y)\{\, v(Y) = \alpha \wedge (\exists X')[\, v(X' - Y) > \alpha \wedge f^*(X') = 0 \,] \wedge \tag{10}$$
$$\bigwedge_{i=2}^{n'} v(Y - b_i) = \alpha \,\}\,.$$

Indeed, let (F, v) be a model of $ACVF(R)$ with a valuation group Γ and let $\alpha \in \Gamma$ and $b_2, \dots, b_{n'} \in F$. Suppose first that (9) holds. Then there exists $x' \in F$ such that $f^*(x') = 0$, $v(x') = \alpha$, and $v(x' - b_i) = \alpha$, $i = 2, \dots, n'$. Let $d \in F$ be such that $v(d) > 0$ and let $c = 1 - d$. Then $v(c) = 0$ and $y = cx'$ satisfies that $v(y) = \alpha$, $v(x' - y) = v(dx') > \alpha$, and $v(y - b_i) = v((x' - b_i) - (x' - y)) = \alpha$, $i = 2, \dots, n'$.

Conversely, suppose that (10) holds. Then there exist $y, x' \in F$ such that $f^*(x') = 0$, $v(y) = \alpha$, $v(x' - y) > \alpha$, and $v(y - b_i) = \alpha$, $i = 2, \dots, n'$. Then $v(x') = v((x' - y) + y) = \alpha$ and $v(x' - b_i) = v((x' - y) + (y - b_i)) = \alpha$, $i = 2, \dots, n'$.

Now, by Lemma B.15 (a), the formula (10) is equivalent to the formula

$$\psi' \wedge (\exists Y)[\, v(Y) = \alpha \wedge v(f^*(Y)) > v(\underline{f^* Y}) \wedge \bigwedge_{i=2}^{n'} v(Y - b_i) = \alpha \,]\,. \tag{11}$$

CASE A: $\alpha = 0$. Let φ be the formula

$$\psi'_0 \wedge v(\mathbf{g}) < \infty \wedge (\exists X)[\, v(X) = 0 \wedge v(g(X)) > v(\mathbf{g}) \wedge \bigwedge_{i=1}^{\ell} v(X - c_i) = 0 \,]\,, \tag{12}$$

where $g(X)$ is a formal polynomial in X of degree m and

$$\psi'_0 : \bigwedge_{i=1}^{\ell} v(c_i) = 0 \wedge \bigwedge_{1 \le i < j \le \ell} v(c_i - c_j) = 0\,.$$

Let $h(X)$ be the formal polynomial which corresponds to $(X - c_1) \cdots (X - c_\ell)$. Then, modulo $VF(R)$, φ is equivalent to the formula

(13) $$\psi_0' \wedge (\exists X)[\, v(X) = 0 \wedge v(g(X)) > v(\mathbf{g}) \wedge v(h(X)) = 0\,]\,,$$

because

$$VF(R) \models v(X) = 0 \wedge \bigwedge_{i=1}^{\ell} v(c_i) = 0 \to [\, \bigwedge_{i=1}^{\ell} v(X - c_i) = 0 \leftrightarrow v(h(X)) = 0\,]\,.$$

Note that

$$VF(R) \models (h_\ell = 1 \wedge \bigwedge_{i=1}^{\ell} v(c_i) = 0) \to v(\mathbf{h}) = 0\,.$$

CASE A1: *$g(X)$ is monic and $v(\mathbf{g}) = 0$.* Suppose that φ is the formula

(14) $$g_m = 1 \wedge v(\mathbf{g}) = 0 \wedge v(\mathbf{h}) = 0 \wedge (\exists X)[\, v(X) = 0 \wedge v(h(X)) = 0 \wedge v(g(X)) > 0\,]\,.$$

Let $k(X)$ be the formal polynomial which corresponds to $(Xh(X))^m$ and let $\mathbf{q} = Q(k, g)$ and $\mathbf{r} = R(k, g)$ (Definition B.13 c)). Then, the degree of r is smaller than m and, by (2),

(15) $$(Xh(X))^m = g(X)q(X) + r(X)\,.$$

CLAIM: $ACVF(R) \models \varphi \leftrightarrow g_m = 1 \wedge v(\mathbf{g}) = 0 \wedge v(\mathbf{h}) = 0 \wedge v(\mathbf{r}) = 0\,.$

Indeed, let (F, v) be a model of $ACVF(R)$, and let $g(X)$ and $h(X)$ be monic polynomials in $F[X]$ of degrees m and ℓ, respectively, such that $v(\mathbf{g}) = 0$ and $v(\mathbf{h}) = 0$. Then, it follows from the construction of $q(X)$ and $r(X)$, that q is monic, $v(\mathbf{q}) = 0$ and $v(\mathbf{r}) \geq 0$. Hence, it follows from (15) that in $\bar{F}_v$

(16) $$(X\bar{h}(X))^m = \bar{g}(X)\bar{q}(X) + \bar{r}(X)\,.$$

By (14), we need to show that there exists $x \in F$ such that $v(x) = 0$, $v(h(x)) = 0$, and $v(g(x)) > 0$ if and only if $v(\mathbf{r}) = 0$. An equivalent formulation in $\bar{F}_v$ is:

$$\text{there exists } 0 \neq \bar{x} \in \bar{F}_v \text{ s.t. } \bar{h}(\bar{x}) \neq 0 \text{ and } \bar{g}(\bar{x}) = 0 \text{ iff } \bar{r} \neq 0\,.$$

Suppose first that there exists $0 \neq \bar{x} \in \bar{F}_v$ such that $\bar{h}(\bar{x}) \neq 0$ and $\bar{g}(\bar{x}) = 0$. Then it follows from (16) that $\bar{r}(\bar{x}) = (\bar{x}\bar{h}(\bar{x}))^m \neq 0$ and, in particular, that $\bar{r} \neq 0$.

Conversely, suppose that each root $\bar{x}$ of $\bar{g}(X)$ in $\bar{F}_v$ satisfies $\bar{x}\bar{h}(\bar{x}) = 0$. Then, since $\bar{F}_v$ is algebraically closed, $\bar{g}(X)$ divides $(X\bar{h}(X))^m$ and therefore $\bar{r} = 0$. This proves the claim.

CASE A2: *$g(X)$ is any formal polynomial of degree m such that $v(\mathbf{g}) < \infty$.* Suppose now that φ is the formula

(17) $$v(\mathbf{g}) < \infty \wedge v(\mathbf{h}) = 0 \wedge (\exists X)[\, v(X) = 0 \wedge v(g(X)) > v(\mathbf{g}) \wedge v(h(X)) = 0\,]\,.$$

We adjoin to φ a disjunction over the possible values of the $v(g_i)$'s: modulo $VF(R)$,

(18) $$\varphi \leftrightarrow \bigvee_{i=0}^{m} [\, \varphi \wedge \bigwedge_{j=i+1}^{m} (v(g_j) > v(\mathbf{g})) \wedge (v(g_i) = v(\mathbf{g}))\,]\,.$$

For each i between 0 and m, let $g^{(i)}(X)$ be the formal polynomial which corresponds to $\sum_{j=0}^{i} T_{i,j} X^j$, where $\mathbf{T}_i = (T_{i,0}, \ldots, T_{i,i})$ is a new tuple of F-variables. Then, modulo $VF(R)$,

$$(19)\quad (v(\mathbf{g}) <\infty \wedge v(X)=0 \wedge \bigwedge_{j=i+1}^{m} v(g_j) > v(\mathbf{g}) \wedge v(g_i)=v(\mathbf{g})) \longrightarrow$$
$$[\, v(g(X)) > v(\mathbf{g}) \leftrightarrow (\exists \mathbf{T}_i)(\bigwedge_{j=0}^{i} g_j = g_i T_{i,j} \wedge v(g^{(i)}(X)) > 0)\,]\,.$$

Indeed, suppose the top line in (19) holds. Then, modulo $VF(R)$, $v(\sum_{j=i+1}^{m} g_j X^j) > v(\mathbf{g})$ and $v(\sum_{j=0}^{i} g_j X^j) \geq v(\mathbf{g})$. Hence in this case, modulo $VF(R)$,

$$v(g(X)) > v(\mathbf{g}) \leftrightarrow v(\sum_{j=0}^{i} g_j X^j) > v(\mathbf{g})$$
$$\leftrightarrow (\exists \mathbf{T}_i)(\bigwedge_{j=0}^{i} g_j = g_i T_{i,j} \wedge v(g^{(i)}(X)) > 0)\,.$$

Note that if $v(g_i) = v(\mathbf{g})$, then (modulo $VF(R)$), since $v(\mathbf{g}) < \infty$, it follows that $g_i \neq 0$ and $v(g_j) \geq v(g_i)$, $j = 0, \ldots, m$, and therefore $g_i^{(i)} = 1$ and $v(\mathbf{g}^{(i)}) = 0$.

It follows from (18) and (19) that in order to eliminate the quantifier $\exists X$ from (17), it suffices to know how to eliminate, for each i between 0 and m, the F-quantifiers from the formula

$$g_i \neq 0 \wedge v(\mathbf{h}) = 0 \wedge (\exists \mathbf{T}_i)\{ \bigwedge_{j=0}^{i} g_j = g_i T_{i,j} \wedge g_i^{(i)} = 1 \wedge v(\mathbf{g}^{(i)}) = 0$$
$$\wedge\, (\exists X)[\, v(X) = 0 \wedge v(h(X)) = 0 \wedge v(g^{(i)}(X)) > 0\,]\,\}\,.$$

We can eliminate the quantifier $\exists X$ using Case A1, and afterwards we can eliminate the quantifiers $\exists T_{i,0}, \ldots, \exists T_{i,i}$ using Remark B.6 b).

CASE B: *α is any $\mathcal{L}_\Gamma$-term such that $v(\alpha) < \infty$.* We eliminate now the quantifier $\exists Y$ from formula (11). Let $g(X) = \sum_{i=0}^{m} (f_i^* b_2^i) X^i = \sum_{i=0}^{m} g_i X^i$. Then formula (11) is equivalent, modulo $VF(R)$, to the formula

$$(20)\quad \psi' \wedge \exists \mathbf{T}\{ \bigwedge_{i=2}^{n'} b_i = b_2 T_i \wedge (\exists X)[\, v(X) = 0 \wedge v(g(X)) > v(\mathbf{g}) \wedge$$
$$\bigwedge_{i=2}^{n'} v(X - T_i) = 0\,]\,\}\,,$$

where $\mathbf{T} = (T_2, \ldots, T_{n'})$ is a new tuple of F-variables.

Indeed, let (F, v) be a model of $VF(R)$ with a valuation group Γ and let $\alpha \in \Gamma$ and $b_2, \ldots, b_{n'} \in F$ be such that $v(b_i) = \alpha$, $i = 2, \ldots, n'$. Note, since $v(\alpha) < \infty$, that $b_2 \neq 0$ and therefore $v(\mathbf{g}) < \infty$. We denote $c_i = \frac{b_i}{b_2}$ (hence $v(c_i) = 0$), $i = 2, \ldots, n'$. Suppose first that (11) holds. Then there exists $y \in F$ such that $v(y) = \alpha$, $v(f^*(y)) > v(f^* y)$, and $v(y - b_i) = \alpha$, $i = 2, \ldots, n'$. Therefore $x = \frac{y}{b_2}$ satisfies $v(x) = v(y) - v(b_2) = \alpha - \alpha = 0$, $v(g(x)) = v(f^*(b_2 x)) = v(f^*(y)) >$

$v(\underline{f^*y}) = v(\mathbf{g})$, and for each i between 2 and n',

$$v(x - c_i) = v(\frac{y - b_i}{b_2}) = v(y - b_i) - v(b_2) = \alpha - \alpha = 0\,.$$

Conversely, suppose that (20) holds. Then there exists $x \in F$ such that $v(x) = 0$, $v(g(x)) > v(\mathbf{g})$, and for each i between 2 and n', $v(x - c_i) = 0$. Hence $y = b_2 x$ satisfies $v(y) = v(b_2) + v(x) = \alpha$,

$$v(f^*(y)) = v(f^*(b_2 x)) = v(g(x)) > v(\mathbf{g}) = v(\underline{f^*y})\,,$$

and

$$v(y - b_i) = v(b_2 \cdot (x - c_i)) = v(b_2) + v(x - c_i) = \alpha\,, i = 2, \ldots, n'\,.$$

Now, we can eliminate the quantifier $\exists X$ from formula (20) using Case A, and afterwards the quantifiers $\exists T_2, \ldots, \exists T_{n'}$ using Remark B.6 b). This concludes the proof of the lemma. □

Notation B.17.

a) $\mathrm{Ft}(W_1, \ldots, W_r)$ is the set of all F-terms in $\mathcal{L}(R)$ whose variables belong to the set $\{W_1, \ldots, W_r\}$.

b) $\mathcal{Z}_{\mathbf{g}}(\mathbf{W}; \mathbf{Z})$ ($\mathcal{Z}$ = Zeros) denotes a formula of the form $\bigwedge_{i=1}^{n} g_i(Z_i) = 0$, where $\mathbf{g} = (g_1, \ldots, g_n)$ and $g_i(Z_i)$ is a monic formal polynomial in Z_i with coefficients $g_{ij} \in \mathrm{Ft}(\mathbf{W}, Z_1, \ldots, Z_{i-1})$, $i = 1, \ldots, n$. ($\mathbf{Z}$ is a tuple of zeros of polynomials with parameters $\mathbf{W}$.)

c) $\deg \mathcal{Z}_{\mathbf{g}}(\mathbf{W}; \mathbf{Z}) = \max\limits_{1 \le i \le n} \{ \deg g_i(Z_i) \}$.

Lemma B.18. *To any formula* $\varphi : \bigwedge_{i=1}^{n} v(f_i(X)) = \alpha_i$, *where* α_i *is an* $\mathcal{L}_\Gamma$*-term and* $f_i(X)$ *is a monic formal polynomial with coefficients in* $\mathrm{Ft}(\mathbf{W})$, $i = 1, \ldots, n$, *one can assign a formula*

$$\varphi' : (\exists \boldsymbol{\xi})\{ (\exists \mathbf{Z})[\, \mathcal{Z}_{\mathbf{g}}(\mathbf{W}; \mathbf{Z}) \wedge \bigwedge_{i=1}^{n'} v(X - a_i) = \alpha_i' \,] \wedge \chi \}\,,$$

where $a_i \in \mathrm{Ft}(\mathbf{Z})$, α_i' *is an* $\mathcal{L}_\Gamma$*-term,* $i = 1, \ldots, n'$, χ *is a quantifier-free* $\mathcal{L}_\Gamma$*-formula and* $\deg \mathcal{Z}_{\mathbf{g}}(\mathbf{W}; \mathbf{Z}) \le \max\limits_{1 \le i \le n} \{\deg f_i(X)\}$, *such that*

$$ACVF(R) \models \varphi \leftrightarrow \varphi'\,.$$

Moreover, if R *is a presented ring and* φ *is a presented formula, then we can effectively (primitive recursively) find* φ'.

Proof. We shall prove the lemma by induction on $k = \sum\limits_{\substack{1 \le i \le n \\ \deg f_i > 1}} \deg f_i$. If $k = 0$, then all the f_i's are linear polynomials and we are done. We suppose that $k > 0$ and choose $f_j(X)$ with $\deg f_j > 1$. Let $\mathbf{f}^* = T(\mathbf{f}_j, Z')$ (Definition B.13 b)). That is, $f_j(X) = f^*(X - Z')$. In particular, $f_0^* = f^*(0) = f_j(Z')$. Let

$$g(X) = \sum_{i=1}^{\deg f^*} f_i^* X^{i-1}\,.$$

Then $f^*(X) = f_0^* + X \cdot g(X)$. We also denote $h(X) = g(X - Z')$. Then

$$h_i \in \mathrm{Ft}(\mathbf{W}, Z')\,, \quad i = 0, \dots, \deg h\,, \tag{21}$$
$$\deg h = \deg g < \deg f^* = \deg f_j\,,$$

and

$$f_j(X) = f^*(X - Z') = f_0^* + (X - Z')g(X - Z') = f_j(Z') + (X - Z')h(X)\,.$$

Hence, since the models of $ACVF(R)$ are algebraically closed fields,

$$ACVF(R) \models v(f_j(X)) = \alpha_j \leftrightarrow (\exists Z')[\, f_j(Z') = 0 \wedge (v(X - Z') + v(h(X)) = \alpha_j)\,]\,.$$

Thus, modulo $ACVF(R)$,

$$\varphi \leftrightarrow (\exists\eta)(\exists\zeta)(\exists Z')[\, f_j(Z') = 0 \wedge v(X - Z') = \eta \wedge v(h(X)) = \zeta \wedge \bigwedge_{\substack{1\le i\le n\\ i\ne j}} v(f_i(X)) = \alpha_i \wedge (\eta + \zeta = \alpha_j)\,]\,. \tag{22}$$

It follows from (21) that we can apply the induction assumption on the formula

$$\psi:\ v(h(X)) = \zeta \wedge \bigwedge_{\substack{1\le i\le n\\ i\ne j}} v(f_i(X)) = \alpha_i\,,$$

for the tuple of variables $(\mathbf{W}, Z')$ instead of the tuple $\mathbf{W}$, and to get a formula

$$\psi':\ (\exists\boldsymbol{\xi})\{\,(\exists\mathbf{Z})[\,\mathcal{Z}_{\mathbf{g}}(\mathbf{W}, Z'; \mathbf{Z}) \wedge \bigwedge_{i=1}^{n_\psi} v(X - a_i) = \alpha_i'\,] \wedge \chi'\,\}\,, \tag{23}$$

such that $ACVF(R) \models \psi \leftrightarrow \psi'$, where $\mathbf{Z} = (Z_1, \dots, Z_m)$, $a_i \in \mathrm{Ft}(\mathbf{Z})$, α_i' is an $\mathcal{L}_\Gamma$-term, $i = 1, \dots, n_\psi$, χ' is a quantifier-free $\mathcal{L}_\Gamma$-formula, and $\mathcal{Z}_{\mathbf{g}}(\mathbf{W}, Z'; \mathbf{Z}) : \bigwedge_{i=1}^{m} g_i(Z_i) = 0$ with monic formal polynomials $g_i(Z_i)$ such that the coefficients g_{ij} belong to $\mathrm{Ft}(\mathbf{W}, Z', Z_1, \dots, Z_{i-1})$ and, by (21),

$$\begin{aligned}\deg \mathcal{Z}_{\mathbf{g}}(\mathbf{W}, Z'; \mathbf{Z}) &= \max_{1\le i\le m}\{\deg g_i(Z_i)\}\\ &\le \max\{\deg h(X), \max_{\substack{1\le i\le n\\ i\ne j}}\{\deg f_i(X)\}\} \le \max_{1\le i\le n}\{\deg f_i(X)\}\,.\end{aligned} \tag{24}$$

We put (23) in (22) and get, modulo $ACVF(R)$, that φ is equivalent to the formula:

$$(\exists\eta)(\exists\zeta)(\exists\boldsymbol{\xi})\{\,(\exists Z')(\exists\mathbf{Z})[\,\mathcal{Z}_{(f_j,\mathbf{g})}(\mathbf{W}; Z', \mathbf{Z}) \wedge v(X - Z') = \eta \wedge \bigwedge_{i=1}^{n_\psi} v(X - a_i) = \alpha_i'\,] \wedge \chi\,\}\,,$$

where

$$\chi:\ \chi' \wedge (\eta + \zeta = \alpha_j)$$

and

$$\mathcal{Z}_{(f_j,\mathbf{g})}(\mathbf{W}; Z', \mathbf{Z}):\ f_j(Z') = 0 \wedge \bigwedge_{i=1}^{m} g_i(Z_i) = 0\,.$$

Note that $f_j(Z')$ is a monic formal polynomial and its coefficients belong to $\mathrm{Ft}(\mathbf{W})$. Also, by (24), $\deg \mathcal{Z}_{(f_j,\mathbf{g})}(\mathbf{W}; Z', \mathbf{Z}) \le \max_{1\le i\le n}\{\deg f_i(X)\}$. We have found then a formula equivalent to φ, modulo $ACVF(R)$, of the desired form. □

Corollary B.19. *Let φ be the formula of Lemma B.18. Then, modulo $ACVF(R)$, $(\exists X)\varphi$ is equivalent to a formula of the form*

$$(\exists \boldsymbol{\xi})(\exists \mathbf{Z})[\, \mathcal{Z}_{\mathbf{g}}(\mathbf{W};\mathbf{Z}) \wedge \psi\,]$$

with $\mathcal{Z}_{\mathbf{g}}(\mathbf{W};\mathbf{Z})$ as in Lemma B.18 and ψ a quantifier-free $\mathcal{L}_{\mathrm{VR}}(R)$-formula.

Moreover, if R is a presented ring and φ is a presented formula, then we can effectively find $\mathcal{Z}_{\mathbf{g}}$ and ψ.

Proof. Combine Lemma B.18 with Lemma B.16 (a). □

The elimination of the quantifier $\exists X$ for formulas $(\exists X)\varphi$, as in Corollary B.19, looks like a bad deal: to eliminate $\exists X$, a tuple of a new F-quantifiers, $\exists \mathbf{Z}$, had to be introduced. Nevertheless, the additional condition on $\mathbf{Z}$ expressed by the formula $\mathcal{Z}_{\mathbf{g}}(\mathbf{W};\mathbf{Z})$ will make sure that the elimination of the quantifiers $\exists \mathbf{Z}$ will come to an end after finitely many steps.

Lemma B.20. *Let φ be a formula of the form*

$$(\exists \mathbf{Z})[\, \mathcal{Z}_{\mathbf{g}}(\mathbf{W};\mathbf{Z}) \wedge \psi(\mathbf{W},\mathbf{Z})\,]\,, \tag{25}$$

where $\psi(\mathbf{W},\mathbf{Z})$ is an F-quantifier-free $\mathcal{L}_{\mathrm{VR}}(R)$-formula. Then, there exists an F-quantifier-free $\mathcal{L}_{\mathrm{VR}}(R)$-formula φ' such that

$$ACVF(R) \models \varphi \leftrightarrow \varphi'\,.$$

Moreover, if R is a presented ring and φ is a presented formula, then we can effectively find φ'.

Proof. Suppose that $\mathbf{Z} = (Z_1,\dots,Z_m)$ and $\mathcal{Z}_{\mathbf{g}}(\mathbf{W};\mathbf{Z}) : \bigwedge_{i=1}^{m} g_i(Z_i) = 0$, where $g_i(Z_i)$ is a monic formal polynomial in Z_i with coefficients in

$$\mathrm{Ft}(\mathbf{W}, Z_1,\dots,Z_{i-1}), \quad i = 1,\dots,m\,.$$

Let

$$n = \deg \mathcal{Z}_{\mathbf{g}}(\mathbf{W};\mathbf{Z}) = \max_{1\le i\le m} \{\deg g_i(Z_i)\}\,.$$

We shall prove the lemma by induction on the degree of the formulas, n, of the type $\mathcal{Z}_{\mathbf{g}}(\mathbf{W};\mathbf{Z})$. if $n = 1$ (and m arbitrary), then each $g_i(Z_i)$ is of the form $Z_i - b_i$, where $b_i \in \mathrm{Ft}(\mathbf{W}, Z_1,\dots,Z_{i-1})$. Therefore, the substitutions $Z_m = b_m(\mathbf{W}, Z_1,\dots,Z_{m-1}),\dots,Z_1 = b_1(\mathbf{W})$, in order, in φ bring it to a quantifier-free formula.

Suppose now that $n > 1$. We denote $\mathbf{Z}' = (Z_1,\dots,Z_{m-1})$.

CASE A: *$\psi(\mathbf{W},\mathbf{Z})$ is a formula of the form*

$$\bigwedge_{i=1}^{r} v(f_i(Z_m)) = \alpha_i\,,$$

where α_i is an $\mathcal{L}_\Gamma$-term and $f_i(Z_m)$ is a monic formal polynomial with coefficients in $\mathrm{Ft}(\mathbf{W},\mathbf{Z}')$, $i = 1,\dots,r$. By the division algorithm for formal polynomials (Definition B.13 c)), we may assume, without loss, that

$$\deg f_i(Z_m) < \deg g_m(Z_m) \le n\,, \qquad i = 1,\dots,r\,.$$

Now, by Lemma B.18, we find a tuple $\mathbf{Y}$ of F-variables and a tuple $\boldsymbol{\xi}$ of Γ-variables, F-terms $a_i \in \mathrm{Ft}(\mathbf{Y})$, $\mathcal{L}_\Gamma$-terms α_i', $i = 1,\dots,r'$, a formula $\mathcal{Z}_{\mathbf{h}}(\mathbf{W},\mathbf{Z}';\mathbf{Y})$ of the type of Notation B.17 b) with

$$\deg \mathcal{Z}_{\mathbf{h}}(\mathbf{W},\mathbf{Z}';\mathbf{Y}) \leq \max_{1\leq i\leq r}\{\deg f_i(Z_m)\} < n \tag{26}$$

and a quantifier-free $\mathcal{L}_\Gamma$-formula χ such that

$$ACVF(R) \models \bigwedge_{i=1}^{r} v(f_i(Z_m)) = \alpha_i \leftrightarrow (\exists \boldsymbol{\xi})\{\,(\exists \mathbf{Y})[\,\mathcal{Z}_{\mathbf{h}}(\mathbf{W},\mathbf{Z}';\mathbf{Y}) \wedge \bigwedge_{i=1}^{r'} v(Z_m - a_i) = \alpha_i'\,] \wedge \chi\,\}\,.$$

Hence we may assume that $\psi(\mathbf{W},\mathbf{Z})$ is the formula written in the above line and reduce φ to the formula

$$(\exists Z_1)\cdots(\exists Z_{m-1})\Big(\bigwedge_{i=1}^{m-1} g_i(Z_i) = 0 \wedge (\exists \boldsymbol{\xi})\{\,(\exists \mathbf{Y})[\,\mathcal{Z}_{\mathbf{h}}(\mathbf{W},\mathbf{Z}';\mathbf{Y}) \wedge (\exists Z_m)\big(\,g_m(Z_m) = 0 \wedge \bigwedge_{i=1}^{r'} v(Z_m - a_i) = \alpha_i'\,\big)\,] \wedge \chi\,\}\Big)\,.$$

By Lemma B.16 (b) we find a quantifier-free $\mathcal{L}_{\mathrm{VR}}(R)$-formula $\psi'(\mathbf{W},\mathbf{Z}',\mathbf{Y})$ such that

$$ACVF(R) \models (\exists Z_m)\big(\,g_m(Z_m) = 0 \wedge \bigwedge_{i=1}^{r'} v(Z_m - a_i) = \alpha_i'\,\big) \leftrightarrow \psi'(\mathbf{W},\mathbf{Z}',\mathbf{Y})\,.$$

Now, by (26) and the induction assumption, we find an F-quantifier-free $\mathcal{L}_{\mathrm{VR}}(R)$-formula $\psi''(\mathbf{W},\mathbf{Z}')$ such that

$$ACVF(R) \models (\exists \mathbf{Y})[\,\mathcal{Z}_{\mathbf{h}}(\mathbf{W},\mathbf{Z}';\mathbf{Y}) \wedge \psi'(\mathbf{W},\mathbf{Z}',\mathbf{Y})\,] \leftrightarrow \psi''(\mathbf{W},\mathbf{Z}')\,.$$

This reduces φ to the formula

$$(\exists \mathbf{Z}')\Big(\bigwedge_{i=1}^{m-1} g_i(Z_i) = 0 \wedge (\exists \boldsymbol{\xi})\{\,\psi''(\mathbf{W},\mathbf{Z}')\,\}\Big)\,.$$

We denote

$$\psi^{(m-1)}(\mathbf{W},\mathbf{Z}') : (\exists \boldsymbol{\xi})\{\,\psi''(\mathbf{W},\mathbf{Z}')\,\}$$

and

$$\mathcal{Z}_{\mathbf{g}'}(\mathbf{W};\mathbf{Z}') : \bigwedge_{i=1}^{m-1} g_i(Z_i) = 0\,,$$

where $\mathbf{g}' = (g_1,\ldots,g_{m-1})$. Then φ is equivalent, modulo $ACVF(R)$, to the formula

$$(\exists \mathbf{Z}')[\,\mathcal{Z}_{\mathbf{g}'}(\mathbf{W};\mathbf{Z}') \wedge \psi^{(m-1)}(\mathbf{W},\mathbf{Z}')\,]$$

which is a formula of the form (25).

Now, by induction on m, we can eliminate the quantifiers $\exists Z_{m-1},\ldots,\exists Z_1$, in order, and arrive to an F-quantifier-free $\mathcal{L}_{\mathrm{VR}}(R)$-formula which is equivalent to φ modulo $ACVF(R)$.

CASE B: *$\psi(\mathbf{W},\mathbf{Z})$ is any F-quantifier-free $\mathcal{L}_{\mathrm{VR}}(R)$-formula.* By Remark B.6 a) we may assume, without loss, that $\psi(\mathbf{W},\mathbf{Z})$ is of the form $\bigwedge_{i=1}^{r} v(b_i(\mathbf{W},\mathbf{Z})) = \beta_i$,

where $b_1, \dots, b_r \in R[\mathbf{W}, \mathbf{Z}]$ and $\beta_1, \dots, \beta_r$ are Γ-terms. Let $n_i = \deg_{Z_m} b_i$, $i = 1, \dots, r$, and write

$$b_i(\mathbf{W}, \mathbf{Z}) = \sum_{j=0}^{n_i} b_{ij}(\mathbf{W}, \mathbf{Z}') Z_m^j \,,$$

with $b_{ij} \in R[\mathbf{W}, \mathbf{Z}']$. Then

$$v(b_i(\mathbf{W}, \mathbf{Z})) = \beta_i \leftrightarrow \bigwedge_{\ell=0}^{n_i} (b_{i\ell}(\mathbf{W}, \mathbf{Z}') = 0 \wedge \beta_i = \infty) \vee$$
$$\bigvee_{j=0}^{n_i} [\bigwedge_{\ell=j+1}^{n_i} b_{i\ell}(\mathbf{W}, \mathbf{Z}') = 0 \wedge b_{ij}(\mathbf{W}, \mathbf{Z}') \neq 0 \wedge v(\sum_{\ell=0}^{j} b_{i\ell}(\mathbf{W}, \mathbf{Z}') Z_m^\ell) = \beta_i \,] \,.$$

Hence we may assume, without loss, that $\psi(\mathbf{W}, \mathbf{Z})$ is the formula

$$\bigwedge_{i=1}^{r} b_{i,n_i}(\mathbf{W}, \mathbf{Z}') \neq 0 \wedge v(b_i(\mathbf{W}, \mathbf{Z})) = \beta_i \,.$$

Let $f_i(Z_m)$ be the formal polynomial which corresponds to

$$Z_m^{n_i} + T_{n_i-1} Z_m^{n_i-1} + \cdots + T_1 Z_m + T_0 \,,$$

where $\mathbf{T}_i = (T_0, \dots, T_{n_i-1})$ is a new tuple of F-variables. Then, modulo $VF(R)$,

$$b_{i,n_i}(\mathbf{W}, \mathbf{Z}') \neq 0 \wedge v(b_i(\mathbf{W}, \mathbf{Z})) = \beta_i \leftrightarrow$$
$$(\exists \xi_i) \{ \, v(b_{i,n_i}(\mathbf{W}, \mathbf{Z}')) + \xi_i = \beta_i \, \wedge b_{i,n_i}(\mathbf{W}, \mathbf{Z}') \neq 0 \wedge$$
$$(\exists \mathbf{T}_i) [\bigwedge_{j=0}^{n_i-1} b_{ij}(\mathbf{W}, \mathbf{Z}') = b_{i,n_i}(\mathbf{W}, \mathbf{Z}') \cdot T_{ij} \wedge v(f_i(Z_m)) = \xi_i \,] \, \} \,.$$

Hence, we may assume that φ is the formula

$$(\exists \mathbf{T}_1) \cdots (\exists \mathbf{T}_r) \{ \, (\bigwedge_{i=1}^{r} b_{i,n_i} \neq 0 \wedge \bigwedge_{j=0}^{n_i-1} b_{ij} = b_{i,n_i} T_{ij}) \wedge$$
$$(\exists \mathbf{Z}) [\, \mathcal{Z}_{\mathbf{g}} \wedge \bigwedge_{i=1}^{r} v(f_i(Z_m)) = \xi_i \,] \, \} \,.$$

Now, we can eliminate the quantifiers $\exists \mathbf{Z}$ using Case A, and afterwards the quantifiers $\exists \mathbf{T}_1, \dots, \exists \mathbf{T}_r$ using Remark B.6 b). □

Theorem B.21. *For any $\mathcal{L}_{\mathrm{VR}}(R)$-formula φ we can assign an F-quantifier-free $\mathcal{L}_{\mathrm{VR}}(R)$-formula φ' such that*

$$ACVF(R) \models \varphi \leftrightarrow \varphi' \,.$$

Moreover, if R is a presented ring and φ is a presented formula, then we can effectively find φ'.

Proof. By induction on the number of F-quantifiers in an $\mathcal{L}_{\mathrm{VR}}(R)$-formula, it suffices to eliminate the quantifier $\exists X$ from formulas of the form $(\exists X)[\widetilde{\varphi}(X)]$ with an F-quantifier-free $\mathcal{L}_{\mathrm{VR}}(R)$-formula $\widetilde{\varphi}(X)$. By Remark B.6 a) we may assume, without loss, that $\widetilde{\varphi}(X)$ is of the form $\bigwedge_{i=1}^{n} v(f_i(X)) = \alpha_i$, where α_i is an $\mathcal{L}_\Gamma$-term

and $f_i(X)$ is a formal polynomial in X with coefficients in $\mathrm{Ft}(\mathbf{W})$, $i = 1, \ldots, n$. As in the proof of Lemma B.20, we may assume that $f_i(X)$ is monic, $i = 1, \ldots, n$.

Now, by Corollary B.19, we can find a tuple $\mathbf{Z}$ of F-variables, a tuple $\boldsymbol{\xi}$ of $\mathcal{L}_\Gamma$-variables, a formula $\mathcal{Z}_{\mathbf{g}}(\mathbf{W}; \mathbf{Z})$ of the type of Notation B.17 b), and a quantifier-free $\mathcal{L}_{\mathrm{VR}}(R)$-formula $\psi(\mathbf{W}, \mathbf{Z})$ such that

$$ACVF(R) \models (\exists X)[\widetilde{\varphi}(X)] \leftrightarrow (\exists \boldsymbol{\xi})(\exists \mathbf{Z})[\, \mathcal{Z}_{\mathbf{g}}(\mathbf{W}; \mathbf{Z}) \wedge \psi(\mathbf{W}, \mathbf{Z})\,] \,.$$

Next, by Lemma B.20, we can find an F-quantifier-free $\mathcal{L}_{\mathrm{VR}}(R)$-formula $\psi'(\mathbf{W})$ such that

$$ACVF(R) \models (\exists \mathbf{Z})[\, \mathcal{Z}_{\mathbf{g}}(\mathbf{W}; \mathbf{Z}) \wedge \psi(\mathbf{W}, \mathbf{Z})\,] \leftrightarrow \psi'(\mathbf{W}) \,.$$

Thus, $\varphi' : (\exists \boldsymbol{\xi})[\psi'(\mathbf{W})]$ is the desired formula. □

Theorem B.22. *For any $\mathcal{L}_{\mathrm{VR}}(R)$-formula φ we can assign a quantifier-free $\mathcal{L}_{\mathrm{VR}}(R)$-formula φ' such that*

$$ACVF(R) \models \varphi \leftrightarrow \varphi' \,.$$

Moreover, if R is a presented ring and φ is a presented formula, then we can effectively find φ' . That is, the theory $ACVF(R)$ admits a primitive recursive procedure of quantifier elimination in the language $\mathcal{L}_{\mathrm{VR}}(R)$.

Proof. By Theorem B.21, it is left to eliminate only Γ-quantifiers from F-quantifier-free $\mathcal{L}_{\mathrm{VR}}(R)$-formulas. Hence, it suffices to know how to eliminate Γ-quantifiers from $\mathcal{L}_\Gamma$-formulas.

If (F, v) is a model of $ACVF(R)$ and Γ is the corresponding valuation group, then, by Remark B.11 a) and c), $\Gamma \cup \{\infty\}$ is a model of DOG_∞ (Definition B.2 b)). Hence, by Theorem B.3, we can eliminate also the Γ-quantifiers from the formulas and arrive to quantifier-free formulas. □

B.4. **Monically Closed Valuation Domains.**

Definition B.23.

a) $\mathcal{L}_{\mathrm{div}} = \{\, 0, 1, +, -, \cdot, |\,\}$ is the language of rings augmented by the symbol $|$ of a binary relation which is interpreted in every ring as divisibility: $x|y \leftrightarrow (\exists z)[xz = y]$.

b) For a ring R, we denote by $\mathcal{L}_{\mathrm{div}}(R)$ the language $\mathcal{L}_{\mathrm{div}}$ augmented by a constant symbol for each element of R. In every ring which contain a homomorphic image $\bar{R}$ of R, these symbols are interpreted as elements of $\bar{R}$ which satisfy the additive and multiplicative tables of corresponding elements in R.

c) VD is the theory of valuation domains in the language $\mathcal{L}_{\mathrm{div}}$. That is, in addition to the ring-axioms in the language $\mathcal{L}$, VD contains the axiom

$$(\forall X)(\forall Y)[\, X|Y \vee Y|X\,] \,.$$

d) $MCVD$ (MCVD = Monically-Closed Valuation Domains) is the theory, in the language $\mathcal{L}_{\mathrm{div}}$, whose models are valuation domains which are not fields and have algebraically closed quotient fields. Alternatively, we say that a ring R is **monically closed** if each monic polynomial in $R[X]$ has a root in R. Then, the models of $MCVD$ are monically closed valuation domains which are not fields. The axioms of the monically closeness are:

$$(\forall Z_0) \cdots (\forall Z_{n-1})(\exists X)[\, X^n + Z_{n-1}X^{n-1} + \cdots + Z_0 = 0\,], \quad n = 1, 2, \ldots \,.$$

e) $VD(R)$ and $MCVD(R)$ are the theories, in the language $\mathcal{L}_{\mathrm{div}}(R)$, whose models are valuation domains A which contain a homomorphic image $\bar{R}$ of R and satisfy $A \models VD$ and $A \models MCVD$, respectively.

Theorem B.24. *To any $\mathcal{L}_{\mathrm{div}}(R)$-formula φ we can assign a quantifier-free $\mathcal{L}_{\mathrm{div}}(R)$-formula φ' such that*

$$MCVD(R) \models \varphi \leftrightarrow \varphi' .$$

Moreover, if R is a presented ring and φ is a presented formula, then we can effectively find φ'. That is, the theory $MCVD(R)$ admits a primitive recursive procedure of quantifier elimination in the language $\mathcal{L}_{\mathrm{div}}(R)$.

Proof. We shall show first that there is a one-to-one correspondence between models of $VD(R)$ and models of $VF(R)$. Indeed, if A is a valuation domain containing a homomorphic image $\bar{R}$ of R with quotient field F, then there is a unique valuation v of F (up to an equivalence of valuations) which satisfies, for each $a \in F$, $a \in A \Leftrightarrow v(a) \geq 0$. In particular, $v(a) \geq 0$ for each $a \in \bar{R}$, as required in Definition B.4 d). Conversely, if (F, v) is a valued field containing a homomorphic image $\bar{R}$ of R such that $v(a) \geq 0$ for each $a \in \bar{R}$, then $A = \{\, a \in F \mid v(a) \geq 0 \,\}$ is a valuation domain which contains $\bar{R}$.

We translate each expression of the form $a|b$ in the language $\mathcal{L}_{\mathrm{div}}(R)$ to the expression $v(b) \geq v(a)$ in the language $\mathcal{L}_{\mathrm{VR}}(R)$. (Note that equations can be eliminated in favour of divisibilities using $a = 0 \leftrightarrow 0|a$.) In this way we code each formula $\varphi(X_1, \ldots, X_n)$ in the language $\mathcal{L}_{\mathrm{div}}(R)$ into a formula $\varphi^*(X_1, \ldots, X_n)$ in the language $\mathcal{L}_{\mathrm{VR}}(R)$ without Γ-variables, such that if (F, v) is a valued field with a valuation domain A which contains a homomorphic image of R, then for each $a_1, \ldots, a_n \in A$,

$$A \models \varphi(\mathbf{a}) \Leftrightarrow (F, v) \models \varphi^*(\mathbf{a}) . \tag{1}$$

Conversely, we translate each expression of the form $v(b) \geq v(a)$ in the language $\mathcal{L}_{\mathrm{VR}}(R)$ to the expression $a|b$ in the language $\mathcal{L}_{\mathrm{div}}(R)$. (Note that $VF(R) \models v(a) = v(b) \leftrightarrow v(a) \geq v(b) \wedge v(b) \geq v(a)$.) In this way we code each quantifier-free $\mathcal{L}_{\mathrm{VR}}(R)$-formula $\psi(X_1, \ldots, X_n)$ without Γ-variables into a quantifier-free formula $\hat{\psi}(X_1, \ldots, X_n)$ in the language $\mathcal{L}_{\mathrm{div}}(R)$, such that if (F, v) is a valued field with a valuation domain A which contains a homomorphic image of R, then for each $a_1, \ldots, a_n \in A$,

$$(F, v) \models \psi(\mathbf{a}) \Leftrightarrow A \models \hat{\psi}(\mathbf{a}) . \tag{2}$$

Note also that there is a one-to-one correspondence between models of $MCVD(R)$ and models of $ACVF(R)$. Indeed, if (F, v) is a valued field with a valuation domain A which contains a homomorphic image of R, then F is algebraically closed if and only if A is monically closed, and v is not trivial on F if and only if A is not a field.

Let now $\varphi(X_1, \ldots, X_n)$ be an $\mathcal{L}_{\mathrm{div}}(R)$-formula. Then $\varphi^*(X_1, \ldots, X_n)$ is an $\mathcal{L}_{\mathrm{VR}}(R)$-formula without Γ-variables. We find, by Theorem B.22, a quantifier-free $\mathcal{L}_{\mathrm{VR}}(R)$-formula $\psi(X_1, \ldots, X_n)$ without Γ-variables such that

$$ACVF(R) \models \varphi^*(\mathbf{X}) \leftrightarrow \psi(\mathbf{X}) . \tag{3}$$

The formula $\hat{\psi}(X_1, \ldots, X_n)$ is a quantifier-free $\mathcal{L}_{\mathrm{div}}(R)$-formula which satisfies

$$MCVD(R) \models \varphi(\mathbf{X}) \leftrightarrow \hat{\psi}(\mathbf{X}) .$$

Indeed, let A be a model of $MCVD(R)$, let F be the quotient field of A, and let v be the corresponding valuation of F. Then, for each $a_1, \ldots, a_n \in F$, it follows

from (1), (3), and (2) that

$$A \models \varphi(\mathbf{a}) \Leftrightarrow (F, v) \models \varphi^*(\mathbf{a}) \Leftrightarrow (F, v) \models \psi(\mathbf{a}) \Leftrightarrow A \models \hat{\psi}(\mathbf{a})\,.$$

□

REFERENCES

[Bir85] B.J. Birch, *When does an affine curve have an algebraic integer point?* Glasgow Math. J. **27** (1985), 1–4.

[Dri88] L. van den Dries, *Elimination theory for the ring of algebraic integers*, J. reine angew. Math. **388** (1988), 189–205.

[DrM90] L. van den Dries and A. Macintyre, *The logic of Rumely's local-global principle*, J. reine angew. Math. **407** (1990), 33–56.

[FrJ08] M. Fried and M. Jarden, *Field Arithmetic* (third edition), Ergebnisse der Mathematik (3), **11**, Springer, Heidelberg, 2008.

[JaR94] M. Jarden and A. Razon, *Pseudo algebraically closed fields over rings*, Israel Journal of Mathematics **86** (1994), 25–59.

[JaR95] M. Jarden and A. Razon, *Skolem density problems over algebraic PAC fields over rings*, Nieuw Archief voor Wiskunde **13** (1995), 381–399.

[JaR98] M. Jarden and A. Razon, *Rumely's local-global principle for algebraic PSC fields over rings*, Transactions of AMS **350** (1998), 55–85.

[Lan64] S. Lang, *Introduction to Algebraic Geometry*, Interscience Punoindentshers, New York, 1964.

[Lan70] S. Lang, *Algebraic Number Theory*, Springer 1970.

[MMD83] A. Macintyre, K. McKenna and L. van den Dries, *Elimination of quantifiers in algebraic structures*, Adv. in Math. **47** (1983), 76–87.

[Mat86] H. Matsumura, *Commutative ring theory*, Cambridge studies in advanced mathematics 8, 1986.

[Nar04] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers (3rd Edition)*, Warszawa, 2004.

[PoZ89] M. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, Cambridge, 1989.

[Rob56] A. Robinson, *Complete theories*, Amsterdam, 1956.

[Rum86] R. Rumely, *Arithmetic over the ring of all algebraic integers*, J. reine angew. Math. **368** (1986), 127–133.

[Sko34] T. Skolem, *Lösung gewisser Gleichungen in ganzen algebraischen Zahlen*, insbesondere in Einheiten, Skrifter Norske Videnskaps Akademi Oslo, Mat. Nature K1. **10** (1934).

[Wei84] V. Weispfenning, *Quantifier elimination and decision procedure for valued fields*, in Models and Sets, LNM **1103**, 1984, 419–472.