Fields Institute Communications
Volume **00**, 0000

The theorem of Grunwald-Wang in the setting of valuation theory

Falko Lorenz
Mathematisches Institut
Universität Münster (Germany)
lorenz@math.uni-muenster.de

Peter Roquette
Mathematisches Institut
Universität Heidelberg (Germany)
roquette@uni-hd.de

Abstract. Given a field K with finitely many valuations; does there exist an extension of K which at these valuations has a prescribed local behavior? The Grunwald-Wang theorem answers this question in the case of abelian field extensions. Originally developed for algebraic number fields in the context of class field theory, it has turned out that it is valid quite generally, for arbitrary multi-valued fields, provided the valuations are of rank one or, more generally, are mutually independent and dense in their respective henselizations. In this paper we present a simple proof which is based on Kummer theory for cyclic Galois algebras, and on Witt theory in case of characteristic p.

Contents

1991 *Mathematics Subject Classification.* Primary 12J10; Secondary 11R37.

1 Introduction

1.1 Statement of main results. A field K, equipped with a finite non-empty set V of inequivalent valuations, archimedean or non-archimedean, is called a **multi-valued field**. [1] Since we include the archimedean case we write the valuations multiplicatively; if $a \in K$ and $v \in V$ then $|a|_v \in \mathbb{R}$ denotes the corresponding value, $|a|_v \geq 0$. We put

$$|a|_V = \max_{v\in V} |a|_v .$$

This defines a metric topology on K. Let $\widehat{K}_V$ denote the corresponding completion. If it is clear from the context which set V we are referring to, then we omit the subscript V and write simply $\widehat{K}$. Since the valuations $v \in V$ are independent, $\widehat{K}$ splits into the direct product of complete fields:

$$\widehat{K} = \prod_{v\in V} \widehat{K}_v \, . \tag{1}$$

We see that $\widehat{K}$ is a commutative semisimple K-algebra. [2]

Now let $L|K$ be a finite Galois extension with Galois group G. Every valuation $v \in V$ has finitely many extensions to L, and so we obtain a finite set of valuations w of L. Thus L, as an extension of the multi-valued field K, is again multi-valued in a canonical way. We have

$$\widehat{L} = \prod_{v\in V} \widehat{L}_v \qquad \text{with} \qquad \widehat{L}_v = \prod_{w|v} \widehat{L}_w \tag{2}$$

where $w|v$ indicates that w is an extension of v. Note that $\widehat{L}_v = L \otimes_K \widehat{K}_v$ since $L|K$ is separable. Hence

$$\widehat{L} = L \otimes_K \widehat{K} \tag{3}$$

The Galois group G acts on the left factor of this tensor product and hence on $\widehat{L}$. With respect to this action $\widehat{L}$ becomes a **Galois G-algebra** over $\widehat{K}$. [3]

The structure of $\widehat{L}$ as a Galois G-algebra over $\widehat{K}$ describes *the local behavior* of the valuations $v \in V$ in the Galois extension $L|K$. For instance, the *decomposition groups* $G_v \subset G$ of the valuations $v \in V$ in the sense of valuation theory can

[1] In this paper all valuations are supposed to be of rank one, i.e., the values are real numbers. More generally, as the reader will observe, our arguments remain valid for finitely many independent Krull valuations of K such that K is dense in the respective henselizations.

[2] We use the terminology "semisimple algebra" in the sense that it implies the algebra to be Artinian. Hence a commutative semisimple algebra is a direct sum of finitely many fields, and conversely.

[3] See **A.10**. For the convenience of the reader, the definitions and basic facts concerning Galois algebras are recalled in the appendix. References to the appendix are prefaced by capital **A**. Thus **A.10** refers to statement **A.10** of the appendix.

be identified with the decomposition groups of the Galois G-algebra $\widehat{L}|\widehat{K}$. [4] There arises the question whether for a given finite group G, there exists a Galois extension $L|K$ with Galois group G with prescribed local behavior at the valuations $v \in V$. In other words:

Given a finite group G and a Galois G-algebra A over $\widehat{K}$, does there exist a Galois extension field $L|K$ on which G acts as Galois group, such that $\widehat{L}$ is isomorphic to A as a Galois G-algebra over $\widehat{K}$?

$$\begin{tikzcd}
 & \widehat{L} \approx A \arrow[dd, dash, "G"] \\
?\, L \arrow[ur, dash] \arrow[dd, dash, "G"'] & \\
 & \widehat{K} \\
K \arrow[ur, dash] &
\end{tikzcd}$$

If G is an abelian group then the above question has been studied by W. Grunwald, a student of Hasse, in his 1933 paper [2], in the case when K is an algebraic number field of finite degree. He assumed that G is generated by the decomposition groups G_v for $v \in V$ [5] and then claimed that, indeed, such $L|K$ does exist. His proof was based on class field theory.

Grunwald's theorem became important in the context of class field theory and the arithmetic theory of central simple algebras. In 1942 G. Whaples [13] presented a new proof which was based on class field theory too but did not use analytic methods, as it had been necessary in Grunwald's time. [6]

However in 1948 Sh. Wang [10] presented a counter-example to Grunwald's theorem, and 1950 in his thesis [11] he corrected the error in Grunwald's (as well as in Whaples') paper, giving precise conditions under which Grunwald's theorem holds for an algebraic number field. It turned out that there are only certain "special" cases of number fields in which Grunwald's theorem may fail to hold without further conditions, but that in all "non-special" cases the theorem holds as had been stated by Grunwald. Those "special" cases can occur only if the exponent of G is divisible by 8, and they depend on the behavior of the field of 2-power roots of unity over K.

Since then the theorem is called the Grunwald-Wang theorem.

In the same year 1950, H. Hasse [4] also presented a correction of Grunwald's theorem in the context of class field theory; Hasse had known Wang's counter-example but not his thesis [11]. See also Chap. X of the Artin-Tate notes [1] on class

[4] For the notions and facts about decomposition groups of Galois G-algebras see the appendix, in particular **A.6**.

[5] In case of a number field Grunwald's assumption is no essential restriction; see Corollary 3 below.

[6] Whaples erroneously called it "Gruenwald's theorem" but the correct name is "Grunwald".

field theory for a discussion of the Grunwald-Wang theorem. Hasse asked whether a proof of the Grunwald-Wang theorem could be given by means of Kummer theory, independent of class field theory.

Here we shall answer Hasse's question and prove, on the basis of Kummer theory for Galois algebras, that the Grunwald-Wang theorem is valid for arbitrary multi-valued fields. (In case of characteristic p we use the additive theory of Witt vectors instead of the multiplicative Kummer theory.)

In this generality, however, the existence of a Galois *field extension* with group G cannot be expected (not for instance, if K is algebraically closed). Instead, we can only assert the existence of a *Galois G-algebra $L|K$* whose completion is isomorphic to A. The easiest way to define the completion $\widehat{L}$ of a Galois G-algebra $L|K$ over a multi-valued field K is by using the formula (3); in the case of a multi-valued field extension this coincides with the definition given above. In any case, formula (3) is what we will refer to in our proof.

Before stating our main result we have to give the definition of "non-special". Let n be an integer. Following Artin-Tate [1] we shall call a field "non-special" with respect to n if it satisfies the following

Wang condition: *Let 2^ν denote the highest power of 2 dividing n; then the field of 2^ν-th roots of unity is cyclic over K.* [7]

If K is of prime characteristic > 0 then the Wang condition is always satisfied, for every n. If $\mathrm{char}(K) = 0$ and n is odd then, again, the Wang condition is satisfied; more generally this holds for $\nu \leq 2$. However, if $\nu \geq 3$ then, for instance, the rational number field $\mathbb{Q}$ does not satisfy the Wang condition. The field of 8-th roots of unity over $\mathbb{Q}$ is of degree 4 and generated by square roots:

$$\mathbb{Q}(\sqrt[8]{1}) = \mathbb{Q}(\sqrt{-1}, \sqrt{-2})\,.$$

Its Galois group is not cyclic. This fact was essential in Wang's counter-example: He worked with $K = \mathbb{Q}$ as base field, and with V consisting solely of the 2-adic valuation of $\mathbb{Q}$. Wang showed, and this is not difficult, that there does not exist a cyclic extension $L|\mathbb{Q}$ of degree 8 such that $\widehat{L}_2|\widehat{\mathbb{Q}}_2$ is the unramified field extension of degree 8.

If a field K contains at least one of the square roots $\sqrt{-1}$, $\sqrt{-2}$ then again, K satisfies the Wang condition, for all n.

For a detailed description of the special cases we refer to the literature, e.g., to Artin-Tate [1] Chap.X.

Our main result can now be stated as follows:

Theorem 1 (General Grunwald-Wang theorem) **(i)** *Let (K, V) be a multi-valued field with completion $\widehat{K}$. Let G be a finite abelian group, of exponent n, and let a Galois G-algebra A over $\widehat{K}$ be given. Then there exists a Galois G-algebra $L|K$ such that its completion $\widehat{L}$ is isomorphic to A as a Galois G-algebra over $\widehat{K}$ – provided K satisfies the Wang condition with respect to n.*

(ii) *It suffices already that every completion $\widehat{K}_v$ for $v \in V$ satisfies the Wang condition with respect to n.*

From the definition we see that the Wang condition for K implies the Wang condition for every overfield of K, in particular for the completions $\widehat{K}_v$ $(v \in V)$.

[7] This should include the case $\mathrm{char}(K) = 2$ when there are no proper roots of unity of 2-power order.

Hence the statement (ii) contains (i) but is more general. We have separated (ii) from (i) because this reflects our proof: First we shall prove Theorem 1 under the assumption that K satisfies the Wang condition and then we amend our proof such as to cover also the more general case (ii); this will be done in section 3. Note that if n is odd then the Wang condition is always satisfied, hence the odd case is covered by statement (i).

Remark: If a valuation v is non-archimedean of residue characteristic > 2 then its completion $\widehat{K}_v$ satisfies the Wang condition; same for an archimedean valuation. Consequently, if V contains valuations v of this kind only, then (ii) shows that the conclusion of the Grunwald-Wang theorem does hold without mentioning any extra condition.

As said above already, the existence of a Galois *field extension* $L|K$ cannot be expected in the general situation of Theorem 1. However, if we assume (like Grunwald has done) that the decomposition groups of A generate G then it turns out that, indeed, $L|K$ is a Galois field extension. This is easy to see. For, as explained in the appendix, the Galois G-algebra $L|K$ has only one decomposition group $H \subset G$ since its base K is a field. From $L \otimes_K \widehat{K} \approx A$ it follows that the decomposition groups of A are subgroups of H (see **A.10**). If these subgroups generate G then it follows $H = G$ and, hence, $L|K$ is a field. Thus we can state the following result as an addition to the general Grunwald-Wang theorem.

Theorem 2 (Irreducibility theorem) *Consider the same situation as in Theorem* 1*. Suppose that the decomposition groups of the given Galois G-algebra $A|\widehat{K}$ generate the group G. Then the Galois G-algebra $L|K$ as announced in that theorem is in fact a Galois field extension.*

We have called this the “Irreducibility theorem” since a Galois algebra is said to be irreducible if it is not properly decomposable into a direct sum, i.e., if it is a Galois extension of fields.

Corollary 3 (Number field case) *Suppose that K is a number field of finite degree. Then the Grunwald-Wang theorem can be sharpened, to the effect that the Galois G-algebra $L|K$ as announced in that theorem, can be chosen to be a Galois field extension – regardless of whether the decomposition groups of $A|\widehat{K}$ generate G or not.*

Proof: Suppose the decomposition groups of $A|\widehat{K}$ do not generate G. Then we choose a cyclic subgroup $H \subset G$ which is not contained in the group generated by the decomposition groups of A. We enlarge the given set V of valuations of K by adding a non-archimedean valuation v of K, independent of the valuations in V. We take care that $\widehat{K}_v$ satisfies the Wang condition, e.g., by choosing v such that the residue characteristic is $\neq 2$. There exists a cyclic extension $M_v|\widehat{K}_v$ of degree $|H|$, e.g., the unique unramified extension of degree $|H|$. There exists an isomorphism of the Galois group of $M_v|\widehat{K}_v$ with H. In other words: we have an injection $\mathrm{Gal}(M_v|\widehat{K}_v) \hookrightarrow G$ with image H. This injection gives rise to a Galois G-algebra $A_v|\widehat{K}_v$ by means of the induction process from H to G (see **A.7**). By construction, the decomposition group of $A_v|\widehat{K}_v$ is H.

Now let $V' := V \cup \{v\}$. This is a finite set of valuations of K. Its completion is $\widehat{K}_{V'} = \widehat{K}_V \times \widehat{K}_v$. If we put $A' = A \times A_v$, then A' is a Galois G-algebra over $\widehat{K}_{V'}$ and the set of decomposition groups of A' contains H, besides of the decomposition groups of A. Thus the subgroup of G generated by the decomposition groups of A' is larger than that with respect to A. Repeating this process we finally obtain a finite set of valuations $V' \supset V$ and a Galois G-algebra $A'|\widehat{K}_{V'}$ whose decomposition groups generate G; moreover, A' contains the given A as a direct factor. Applying Theorem 2 to V' and A' we obtain a Galois field extension $L|K$ with group G such that $\widehat{L}_{V'} \approx A'$. By construction, this implies $\widehat{L}_V \approx A$.

□

Remark: The same argument works not only for a number field of finite degree, but for any field K which carries infinitely many independent valuations v whose completions $\widehat{K}_v$ satisfy Wang's condition and admit cyclic field extensions of a given degree m. For instance, K may be an algebraic function field of one or several variables over some subfield.

1.2 Reduction to cyclic groups of prime power order. If the group G is a direct product $G = G_1 \times G_2$ then the Galois G-algebra $A|\widehat{K}$ is isomorphic to a tensor product $A = A_1 \otimes_{\widehat{K}} A_2$ of a Galois G_1-algebra $A_1|\widehat{K}$ with a Galois G_2-algebra $A_2|\widehat{K}$ (see **A.11**). It suffices to prove the Grunwald-Wang theorem for each of the factors A_1, A_2.

For, if there exists a Galois G_1-algebra L_1 over K such that $\widehat{L}_1 \approx A_1$, and similarly $\widehat{L}_2 \approx A_2$, then $L = L_1 \otimes_K L_2$ is a Galois G-algebra over K (see **A.11** again) and $\widehat{L} = \widehat{L}_1 \otimes_{\widehat{K}} \widehat{L}_2 \approx A_1 \otimes_{\widehat{K}} A_2 = A$. Observe that the exponent n of G is the least common multiple of the exponents n_1, n_2 of G_1 and G_2. Hence if K satisfies the Wang condition with respect to n then it does so for n_1 and n_2 too.

Accordingly, we assume from now on that G is not decomposable as a direct product. Since G is assumed to be abelian this implies that G is cyclic of prime power order. The order of G is denoted by

$$|G| = n = p^\nu .$$

The Wang condition can now be formulated to say that the field $K(\sqrt[n]{1})$ of n-th roots of unity should be cyclic over K. As said above, this is always satisfied if $p > 2$, or if $\mathrm{char}(K) > 0$, or if at least one of the square roots $\sqrt{-1}$, $\sqrt{-2}$ is contained in K.

1.3 Plan of work. Our main idea of proof is to use a *parametrization* of Galois G-algebras for a cyclic group G of prime power order $n = p^\nu$. If the given Galois G-algebra $A|\widehat{K}$ is described by parameters in $\widehat{K}$ then after a small perturbation of those parameters one can assume that they are contained in K already. But in K they define a Galois G-algebra over $L|K$ which then turns out to be a solution of the Grunwald-Wang problem.

This simple idea works well in the case when $p \neq \mathrm{char}(K)$ and the n-th roots of unity are contained in K. For in this case we can use Kummer theory of Galois G-algebras; these can be parametrized by their Kummer radicands. We have to use Kummer theory over commutative semisimple algebras and not only over fields; for the convenience of the reader we include a short presentation of Kummer theory in this framework. See section 2.1.

But if the n-th roots of unity are not in K then the situation becomes a little more involved. Our idea is first to adjoin the n-th roots of unity to K, and then characterize those Kummer radicands whose corresponding Galois G-algebra has been obtained by base extension. It is here where we have to impose the Wang condition with respect to the group order $n = p^\nu$. If the Wang condition is not satisfied (and hence $p = 2$) then a parametrization of the Galois G-algebras is still possible but not in a form which allows the use of the perturbation idea mentioned above. In fact, Wang's counter-example shows that this is not a failure of the method but that the theorem fails to hold in general.

But even if the Wang condition is satisfied there is a certain exception. Whereas "in general" the Galois G-algebras can be parametrized by just one parameter (which we call "Kummer parameter", see Prop. 8 in section 2.3) there are certain exceptions where two parameters are needed. These exceptions arise when $p = 2$ and $\sqrt{-1} \notin K$. Although in this exceptional case our main idea is still applicable, we have to treat both cases separately. Thus we first deal with the non-exceptional case in section 2.3. The exceptional case, where $p = 2$, is treated in section 3, together with the proof of statement (ii) of the theorem.

Once the basic facts on the Kummer parametrization of cyclic Galois algebras are available, the proof of the Grunwald-Wang theorem turns out to be quite short and straightforward (see sections 2.4 and 3.2).

Finally, there is the case $p = \mathrm{char}(K)$. This case can be treated without problems by using Witt's parametrization of cyclic Galois G-algebras of p-power rank. Witt has developed this theory for cyclic field extensions only; hence we shall briefly treat Witt's theory in the framework of Galois G-algebras. See section 4.

1.4 Further comments. (1) Connection to embedding problem: The larger part of our paper is concerned with the presentation of Kummer parametrization and, in the case of $p = \mathrm{char}(K)$, of Witt parametrization. We would like to point out that this may be regarded as "well known" in the sense, that it can be extracted from the general theory of embedding problem for Galois G-algebras with abelian groups G. This theory has been started from a systematic point of view by Hasse [3] in a series of three papers on this subject. In modern language, the parametrization of such algebras can be described by certain cohomology invariants. But it would have taken some space and effort to show that those cohomology invariants can be parametrized by elements in the base algebra, in the way which we need for our proof of the Grunwald-Wang theorem. Hence we have decided to give a direct and relatively short presentation of the material, in a form which is suitable for our purpose. In order to put the simplicity of our method into evidence, we have tried to assume not too many prerequisites from algebra or cohomology theory. We have in mind a reader with the knowledge from an algebra course, say, [6].

(2) Historical remarks: We would like to point out that Miki [8] in 1978 had been the first who followed Hasse's suggestion and proved Grunwald's theorem in the setting of valuation theory, using Kummer theory as we do. His methods appear to be similar to ours, but he discussed discrete valuations only. And he imposed quite strong conditions concerning the "special" case, which later were relaxed by Sueyoshi [12] in 1980 but they are still more restrictive than ours. We believe that our method of putting the theorem in the framework of *Galois algebras* instead of *Galois field extensions* is more adapted to the problem. In fact, it puts into evidence that the discreteness of the valuations is not needed at all.

A completely new idea was introduced into the subject by the interesting paper of Saltman [9]. He approached the problem of the Grunwald-Wang theorem by means of his theory of generic Galois polynomials. In fact, our work started after reading Saltman's paper; although the theory of generic Galois polynomials is of interest there arose the question whether his ideas of specialization could be transformed into parametrization. Although we do not do it explicitly in our paper, the reader will notice that if the Kummer parameter of a Galois G-algebra is transcendental over R in a suitable sense, then every Galois G-algebra over R is a specialization of that transcendental algebra.

(3) Open problem: In this paper we deal with the non-special case only. Over a number field, however, the "special" case is also discussed in the framework of class field theory, giving necessary and sufficient conditions for a Galois G-algebra $A|\widehat{K}$ to be the completion of a Galois G-algebra $L|K$. Those conditions refer to the behavior of local norm residue symbols of the field of roots of unity of 2-power order, locally at the critical valuations. There arises the question whether conditions of such type can be given in terms of Kummer parameters or similar invariants, over an arbitary multi-valued field. We leave it as an open problem to find such conditions.

2 Parametrization of cyclic Galois algebras

As said above, G is now supposed to be a cyclic group of prime power order $n = p^\nu$. Let K be a field. Until section 4 it is assumed that $p \neq \operatorname{char}(K)$.

2.1 Kummer theory. In the present section we assume in addition that the n-th roots of unity are contained in K. Let $\mu_n \subset K^\times$ denote the group of n-th roots of unity and

$$\chi\colon G \to \mu_n \tag{4}$$

an isomorphism from G to μ_n. This isomorphism is kept fixed in the sequel and all statements refer to the given χ although this is not mentioned explicitly.

Let R be a semisimple commutative K-algebra. Our aim is to give a description of the Galois G-algebras over R.

$R^\times$ denotes the multiplicative group of units, i.e., invertible elements, in R. Let $a \in R^\times$. Consider an R-algebra $A_a = R[x]$ which is generated by an element x satisfying

$$x^n = a \tag{5}$$

as a *defining relation* over R. This means that any other polynomial relation for x over R is a consequence of the relation (5). In other words: Let $R[X]$ denote the polynomial algebra over R and consider the map $R[X] \to A_a$ given by $X \mapsto x$, then the kernel of this map should be the ideal generated by the polynomial $X^n - a$, so that we obtain an isomorphism

$$R[X]/(X^n - a) \approx A_a \tag{6}$$

of R-algebras. If $y \in A_a$ is any other element satisfying $y^n = a$ then there is a unique R-algebra homomorphism $A_a \to A_a$ such that x maps onto y.

Let $\sigma \in G$. We have $(\chi(\sigma)x)^n = x^n = a$; hence there is a unique R-algebra homomorphism $\sigma\colon A_a \to A_a$ which takes x into

$$x^\sigma = \chi(\sigma)x \qquad (\sigma \in G)\,. \tag{7}$$

The homomorphism property $\chi(\sigma\tau) = \chi(\sigma)\chi(\tau)$ yields $x^{\sigma\tau} = (x^\sigma)^\tau$. In this way A_a becomes a G-algebra. By construction, it is uniquely determined by a (up to isomorphisms of G-algebras over R).

Proposition 4 (Kummer Theory for Galois algebras) **(i)** *Let $a \in R^\times$. Any G-algebra $A|R$ generated by an element $x \in A$ satisfying the relations* (5),(7) *is a Galois G-algebra over R, and A is isomorphic to A_a.*

(ii) *If $a \equiv b \mod R^{\times n}$, i.e., if $a = b \cdot u^n$ with $u \in R^\times$, then A_a is isomorphic to A_b, and conversely.*

(iii) *Every Galois G-algebra $A|R$ is isomorphic to A_a for suitable $a \in R^\times$. Such element a is called a* **Kummer radicand** *of A, and the corresponding x is called a* **Kummer radical** *of A.*

Proof of (i): First we show that A_a is a Galois G-algebra. We decompose R into a direct product of fields; using **A.3** we see that it suffices to prove the assertion for each direct factor separately. In other words: we may assume that R is a field. We use **A.4** and see that we have to prove the following:

(a) *A_a is semisimple.*
(b) $\mathrm{Fix}(G, A_a) = R$.
(c) $[A_a : R] = n$.

Statement (a) follows from (6) since the polynomial $X^n - a$ has no multiple roots. Note that $a \neq 0$, and that n is not divisible by the characteristic of the field R.

Statement (c) follows also from (6) since the n elements $1, x, \dots, x^{n-1}$ form an R-basis of A_a.

As to statement (b), let $u \in A_a$ and write

$$u = \sum_{0 \le i \le n-1} c_i x^i \qquad \text{with} \qquad c_i \in R.$$

For $\sigma \in G$ we have according to (7):

$$u^\sigma = \sum_{0 \le i \le n-1} c_i \chi(\sigma)^i x^i \,.$$

Hence if u is fixed under σ then by comparing coefficients we obtain $c_i = c_i \chi(\sigma^i)$. Now take σ to be a generator of the cyclic group G; then we have $\chi(\sigma^i) \neq 1$ for $1 \le i \le n-1$ since χ is an ismomorphism. It follows $c_i = 0$ for those i (since R is a field) and hence $u = c_0 \in R$.

Now let A be an arbitrary G-algebra over R, generated by an element x satisfying (5) and (7). We do not require *a priori* that the relation (5) is a *defining relation* for x over R. In any case, we have a unique R-homomorphism $R[X] \to A$ mapping X to $x \in A$. This is surjective because A is generated by x. In view of (5) this factors through the residue class algebra modulo $X^n - a$, and we obtain a homomorphism $R(X)/(X^n - a) \to A$ as R-algebras, mapping the residue class of X to x. In view of (7) this is a homomorphism of G-algebras.

Now, we know from the above that $A_a = R(X)/(X^n - a)$ is a *Galois* G-algebra. Hence the map $A_a \to A$ is injective; see **A.12**. Since it is surjetive by construction, it is an isomorphism. (And, hence, the relation (5) is indeed a defining relation for x over R.)

Proof of **(ii)**: Consider the Galois G-algebra $A_a = R[x]$ with (5) and (7), and similarly $A_b = R[y]$. Suppose that $a = bu^n$ with $u \in R^\times$. We are going to establish an isomorphism $\varphi : A_a \to A_b$ as G-algebras over R.

The relation $x^n = a$ is a *defining relation* for x over R. Hence, in order to obtain an homomorphism $\varphi : A_a \to A_b$ as R-algebras, it is sufficient to assign to

x some element $z \in A_b$ such that z satisfies the same relation $z^n = a$ as x does. Clearly this holds for $z := yu$ (since $bu^n = a$).

Hence we have a uniquely defined homomorphism $\varphi : A_a \to A_b$ as R-algebras, such that $x^\varphi = yu$. We claim that this is a homomorphism as G-algebras, which means that $\sigma\varphi = \varphi\sigma$ for $\sigma \in G$. Indeed: $x^{\sigma\varphi} = (\chi(\sigma)x)^\varphi = \chi(\sigma)x^\varphi = \chi(\sigma)yu = y^\sigma u = (yu)^\sigma = x^{\varphi\sigma}$ since σ acts trivially on $u \in R$.

Since both A_a and A_b are Galois G-algebras over R it follows that $\varphi : A_a \to A_b$ is an isomorphism. (See **A.12**.)

Conversely, assume that $A_a \approx A_b$. Let us identify $A_a = A_b = A$ by means of that isomorphism. Thus on the one hand, $A = R[x]$ with the relations (5), (7), and on the other hand $A = R[y]$ with corresponding relations for y and b. When applying $\sigma \in G$ both x and y take the same factor, namely $\chi(\sigma)$. Let us put $u := yx^{-1}$; this is fixed under G and hence $u \in R$. Note that x is a unit in A since x^n is a unit in R; similarly we have $y \in A^\times$. It follows $u \in R^\times$. From $y = xu$ we compute $b = y^n = x^n u^n = au^n \equiv a \mod R^{\times n}$.

Proof of (iii): Now consider an arbitrary Galois G-algebra A over R; we have to find $x \in A^\times$ and $a \in R^\times$ satisfying the relations (5), (7) and such that A is generated over R by x. Since A is a Galois G-algebra it admits a normal basis over R. Let $u \in A$ generate such a normal basis. Starting from such u we consider the "Lagrange resolvent"

$$x := \sum_{\tau \in G} \chi(\tau)^{-1} u^\tau .$$

A straightforward computation shows that $x^\sigma = \chi(\sigma)x$, for $\sigma \in G$. Let us put $a := x^n$. Then $a^\sigma = x^{\sigma n} = (\chi(\sigma)x)^n = x^n = a$. Hence a is fixed under G and therefore contained in R.

If a would not be a unit in R then there would exist a primitive idempotent $e \neq 0$ in R such that $ea = 0$. (Observe that R is supposed to be semisimple.) It follows $(ex)^n = e^n x^n = ea = 0$ and hence $ex = 0$, since A is commutative and semi-simple and therefore has no nilpotent elements $\neq 0$. We have $0 = ex = \sum_{\sigma \in G} e\chi(\sigma^{-1})u^\sigma$. Since the u^σ form an R-basis of A we conclude that $e\chi(\sigma^{-1}) = 0$ for all $\sigma \in G$. Taking $\sigma = 1$ we obtain $e = 0$, a contradiction. Thus indeed $a \in R^\times$. Since $x^n = a$ we conclude $x \in A^\times$.

Thus $x \in A^\times$ satisfies relations of the form (5), (7). From (i) we conclude that the algebra $R[x]$ is a Galois G-algebra, with the action of G induced by its action on A. The inclusion map $R[x] \hookrightarrow A$ is a homomorphism of Galois G-algebras over R, hence an isomorphism by **A.12**. Thus $R[x] = A$.

□

We can reformulate Proposition 4 as follows:

Every element $a \in R^\times$ defines (uniquely up to isomorphisms) a Galois G-algebra $A|R$ such that a is a Kummer radicand of A. The structure of A depends only on the residue class of a modulo n-th powers in $R^\times$. Conversely, every Galois G-algebra $A|R$ admits an element $a \in R^\times$ as its Kummer radicand.

Remark: Let $A|R$ be a Galois G-algebra and $a \in R^\times$ a Kummer radicand of A. The corresponding Kummer radical $x \in A$ of a is not uniquely determined. An element $y \in A$ is another Kummer radical of a if and only if $y = \zeta x$ with $\zeta \in R$ and $\zeta^n = 1$. If R is a direct product of d fields then there are n^d such elements ζ. The n^d substitutions $x \mapsto \zeta x$ yield n^d automorphisms of A as Galois G-algebra over R, and every automorphism of A is of this form.

2.2 Galois action on the n-th roots of unity. Now we drop the assumption that the n-th roots of unity are contained in K.

Let $K' = K(\sqrt[n]{1})$ be the field of n-th roots of unity over K. As in (4) we fix an isomorphism χ of G onto the group $\mu_n \subset K'^{\times}$ of n-th roots of unity Let $\mathfrak{g}$ denote the Galois group of $K'|K$. Every automorphism $\tau \in \mathfrak{g}$ is uniquely determined by its action on μ_n. There exists $t \in \mathbb{Z}$ such that

$$\chi(\sigma)^{\tau} = \chi(\sigma)^{t} \qquad (\sigma \in G)\,. \tag{8}$$

The exponent t modulo n is uniquely determined by τ . The mapping $\tau \mapsto t$ gives an injection of the Galois group $\mathfrak{g}$ into the group $(\mathbb{Z}/n)^{\times}$.

Let s denote the order of τ. We have

$$\tau^s = 1 \qquad \text{hence} \qquad t^s \equiv 1 \bmod n\,.$$

Let $\ell \in \mathbb{Z}$ be defined as

$$\ell = \frac{t^s - 1}{n}\,. \tag{9}$$

At this point we use the assumption introduced in section 1.2 that $n = p^{\nu}$ is a prime power, $p \neq \operatorname{char}(K)$. We shall need it in the proof of the following lemma. [8]

Lemma 5 (Normalization) *Let $\tau \in \mathfrak{g}$. The exponent $t \in \mathbb{Z}$ can be normalized in its residue class modulo n such that* $\gcd(\ell, n) = 1$ *except in the case when $p = 2$, $s = 2$, $t \equiv -1 \bmod n$. In this exceptional case we normalize $t = -1$ hence $\ell = 0$.*

Proof: $n = p^{\nu}$ is a p-power. The condition $\gcd(\ell, n) = 1$ is satisfied if

$$t^s \not\equiv 1 \bmod p^{\nu+1}\,. \tag{10}$$

Suppose that $t^s \equiv 1 \bmod p^{\nu+1}$, then we try to replace t by $t + p^{\nu}$. We have

$$(t + p^{\nu})^s \equiv 1 + st^{s-1}p^{\nu} \bmod p^{\nu+1}\,.$$

If $s \not\equiv 0 \bmod p$ then we see that $t + p^{\nu}$ satisfies (10). If however $s \equiv 0 \bmod p$ then we argue as follows: $t^{s/p}$ is of order p modulo p^{ν}. If $p > 2$ the group $(\mathbb{Z}/p^{\nu})^{\times}$ is cyclic and, hence, it admits only one subgroup of order p. This subgroup consists of the p elements $1 + ip^{\nu-1}$ for $0 \le i \le p - 1$. Hence

$$t^{s/p} \equiv 1 + ip^{\nu-1} \bmod p^{\nu} \qquad \text{for some} \qquad i \not\equiv 0 \bmod p\,.$$

Taking p-th powers we conclude that $t^s \equiv 1 + ip^{\nu} \bmod p^{\nu+1}$ and hence (10).

Now let $p = 2$. Every element in $(\mathbb{Z}/2^{\nu})^{\times}$ has order a power of 2. If $\nu \ge 3$ then there are 3 elements of order 2 in $(\mathbb{Z}/2^{\nu})^{\times}$, namely -1 and $\pm 1 + 2^{\nu-1}$. If $t^{s/2} \equiv \pm 1 + 2^{\nu-1} \bmod 2^{\nu}$ then after squaring we obtain $t^s \equiv 1 + 2^{\nu} \bmod 2^{\nu+1}$, thus again (10). The exceptional case $t^{s/2} \equiv -1 \bmod 2^{\nu}$ can occur only if $s = 2$ since -1 is not a square in $(\mathbb{Z}/2^{\nu})^{\times}$.

□

In the following we assume that the exponent t is normalized in the above sense. We define τ to be **non-exceptional** if indeed $\gcd(\ell, n) = 1$, and otherwise **exceptional**. If τ is exceptional then $\ell = 0$.

Perhaps it is not unnecessary to mention that the trivial automorphism $\tau = 1$ is non-exceptional; in this case we normalize t to be $t = 1 + n$ and hence $\ell = 1$.

Definition. $\mathfrak{g}$ *is called exceptional if it contains an exceptional automorphism.*

[8] This is taken from Saltman [9].

If this is the case then necessarily $p = 2$ and there is only one exceptional automorphism in $\mathfrak{g}$, namely the automorphism of order $s = 2$ which keeps the elements in K fixed and maps every n-th root of unity into its inverse.

Lemma 6 *If $\mathfrak{g}$ is non-exceptional then $\mathfrak{g}$ is cyclic, hence K satisfies the Wang condition with respect to n.*

Proof: If $\mathfrak{g}$ is non-cyclic then necessarily $p = 2$ and $\mathfrak{g}$ is isomorphic to a subgroup of $(\mathbb{Z}/2^\nu)^\times$. The group $(\mathbb{Z}/2^\nu)^\times$ is non-cyclic if $\nu \geq 3$, and then it is generated by -1 (of order 2) and 5 (of order $2^{\nu-2}$):

$$(\mathbb{Z}/2^\nu)^\times = \langle -1 \rangle \times \langle 5 \rangle \,. \tag{11}$$

Every non-cyclic subgroup of $(\mathbb{Z}/2^\nu)^\times$ necessarily contains -1, and this corresponds to the exceptional automorphism of $\mathfrak{g}$.

□

Remark: The invariants s, t, ℓ describe the action of $\tau \in \mathfrak{g}$ on the n-th roots of unity. If we wish to indicate which automorphism τ they belong to then we write more precisely $s_\tau, t_\tau, \ell_\tau$. But for simplicity of notation we mostly drop the index τ if it is clear from the context which automorphism τ we are referring to.

In addition we will have to use the operator $N = N_\tau$ as follows:

$$N = t^{s-1} + t^{s-2}\tau + \cdots + t\tau^{s-2} + \tau^{s-1} \,. \tag{12}$$

N operates on any module on which τ operates. We have $(t-\tau)N = t^s - \tau^s = t^s - 1$ and hence, using the definition (9) of ℓ:

$$(t - \tau)N = \ell n \,. \tag{13}$$

We will use this relation several times in the sequel. [9]

2.3 Parametrization in the non-exceptional case. Let R be a commutative semisimple K-algebra. As above, K' denotes the field of n-th roots of unity over K. We put

$$R' = K' \otimes_K R \tag{14}$$

and call R' the "algebra of n-th roots of unity" over R. The Galois group $\mathfrak{g}$ of $K'|K$ acts on the left hand side of the tensor product, and by this action R' becomes a Galois $\mathfrak{g}$-algebra over R (see **A.10**). On the other hand, R' can be regarded as a commutative semisimple algebra over K', and since K' contains the n-th roots of unity, the Kummer Theory of Proposition 4 can be applied to Galois G-algebras over R'.

[9] The notation N for the operator on the right hand side of (12) has been chosen to indicate that it behaves somewhat like the norm operator in cohomology theory. In fact, if we introduce the so-called "twist" $\overline{\tau} = t\tau^{-1}$ and its norm $\overline{N} = \overline{\tau}^{s-1} + \overline{\tau}^{s-2} + \cdots + 1$ then $N = \tau^{(s-1)}\overline{N}$. By using the twist $\overline{\tau}$ instead of τ it would have been possible to put our following discussion into a more systematic and general framework of cohomology theory. For, the condition of Prop. 7 below can be stated to the effect that a', if regarded in the factor group $R'^\times/R'^{\times n}$, should be a norm with respect to the twist $\overline{\tau}$, which can be interpreted that the comology class determined by a' in $H^0(\overline{\mathfrak{g}}, R'^\times/R'^{\times n})$ is trivial. In this form, Prop.7 can be regarded as a very special case of Hasse's general theory of abelian algebras [3], as we have already mentioned in the introduction. (However, Hasse's theory would first have to be extended, such as to cover not only abelian algebras over a field but also over a semisimple algebra as a base.) After some deliberation we have decided not to work with the twist (which nowadays is also called "Tate twist") because it seems not to be relevant for our purpose, namely the parametrization of Galois G-algebras for cyclic G.

Consider a Galois G-algebra A over R and put

$$A' = A \otimes_R R' . \tag{15}$$

Then A' is a Galois G-algebra over R' (see **A.10**). It is obtained from A by extending the base algebra from R to R'. Let $a' \in R'^{\times}$ be a Kummer radicand of A'. We ask:

What are the properties of a' which express the fact that A' is obtained from the Galois G-algebra A over R by base extension from R to R' ?

$$\begin{tikzcd}
 & A \otimes_R R' = A' \arrow[dd, dash, "G"] \\
? \, A \arrow[ur, dash, "\mathfrak{g}"] \arrow[dd, dash, "G"'] & \\
 & R' \\
R \arrow[ur, dash, "\mathfrak{g}"'] &
\end{tikzcd}$$

In this section we treat the case that $\mathfrak{g}$ is non-exceptional in the sense as defined in section 2.2. By Lemma 6 this implies that $\mathfrak{g}$ is cyclic. Let us choose a generator $\tau \in \mathfrak{g}$, so that

$$\mathfrak{g} = \langle \tau \rangle .$$

τ is a non-exceptional automorphism in $\mathfrak{g}$. The invariants s, t, ℓ, N belonging to τ have been introduced in section 2.2.

Proposition 7 *Suppose that $\mathfrak{g} = \langle \tau \rangle$ is non-exceptional. Let $A'|R'$ be a Galois G-algebra with Kummer radicand $a' \in R'^{\times}$. If there exists $a \in R'^{\times}$ such that $a' \equiv a^N \mod R'^{\times n}$ then A' is representable as a tensor product $A' = A \otimes_R R'$ with some Galois G-algebra $A|R$. And conversely.*

This is immediate from the following result which gives a complete parametrization of the Galois G-algebras $A|R$.

Proposition 8 (Parametrization, non-exceptional case) *Suppose that $\mathfrak{g}$ is non-exceptional and that $\mathfrak{g} = \langle \tau \rangle$. Then:*

(i) *Every element $a \in R'^{\times}$ determines a Galois G-algebra $A(a)$ over R by way of the following two-step construction.*

Step 1:: *Construct the Galois G-algebra A' over R' with a^N as its Kummer radicand. Hence $A' = R'[x]$ with $x^n = a^N$ and $x^{\sigma - 1} = \chi(\sigma)$.*

Step 2:: *Extend the action of $\mathfrak{g}$ on R' to an action of $\mathfrak{g}$ on A' such that $x^{t-\tau} = a^{\ell}$. This extension is possible and unique. Then put $A(a) := \mathrm{Fix}(\mathfrak{g}, A')$; this is a Galois G-algebra over R. Moreover, $A(a) \otimes_R R' \approx A'$.*

(ii) *If $a \equiv b \mod R'^{\times n}$ then $A(a) \approx A(b)$.*

(iii) *Every Galois G-algebra A over R is isomorphic to $A(a)$ for suitable $a \in R'^{\times}$. Such an element a is called a* **Kummer parameter** *for A.*

Remark: We can reformulate Proposition 8 as follows:

If $\mathfrak{g}$ is non-exceptional then the elements $a \in R'^{\times}$ parametrize the Galois G-algebras $A|R$ (up to isomorphisms) as their Kummer parameters. Elements which differ by n-th power factors parametrize isomorphic Galois G-algebras.

Note that we do not claim the Kummer parameter a to be uniquely determined modulo n-th powers. It may well be that $A(a) \approx A(b)$ but $a \not\equiv b \mod R'^{\times n}$. If however K contains the n-th roots of unity then $K' = K$ and $\mathfrak{g} = 1$, and the Kummer parameters coincide with the Kummer radicands, i.e., $A(a) = A_a$ in the sense of Proposition 4.

Proof of (i): Let A' be constructed as in Step 1. We try to extend the action of τ on R' to an action on A'.

We recall from Kummer Theory (Prop. 4) that the relation $x^n = a^N$ is a *defining relation* for x over R'. Consequently, in order to extend the action of τ to an algebra homomorphism of A' it suffices to assign to x an element $y \in A'$ which satisfies the image of that relation under τ, which is to say $y^n = a^{N\tau}$. We claim that this holds for $y = x^t a^{-\ell}$. Indeed, we compute using (13): $\left(x^t a^{-\ell}\right)^n = a^{Nt} a^{-\ell n} = a^{Nt-\ell n} = a^{N\tau}$. We conclude:

There is a unique algebra homomorphism τ of A' into itself, extending the given algebra automorphism τ of R' and satisfying

$$x^{\tau} = x^t a^{-\ell} \qquad \text{or, equivalently} \qquad x^{t-\tau} = a^{\ell}\,. \tag{16}$$

Next we claim that $\tau^s = 1$, i.e., *τ has order s not only as an operator on R' but also on A'.* Since this relation holds on R' it suffices to verify it when applied to the generator x of $A'|R'$. Now, as operators on the unit group $A'^{\times}$ we have $\tau^s - 1 = (t^s - 1) - (t^s - \tau^s) = \ell n - (t-\tau)N$; remember the definitions (9) of ℓ and (12) of N. Thus $\tau^s = 1$ is equivalent to $(t-\tau)N = \ell n$. We have to verify this when applied to x. Indeed, using (16) we have: $x^{(t-\tau)N} = a^{\ell N}$, and on the other hand: $x^{n\ell} = a^{N\ell}$ since $x^n = a^N$.

Next we show that the action of τ on A' commutes with the action of G, i.e. that $\sigma\tau = \tau\sigma$ holds on A'. Again, this relation holds on R' (because σ acts trivially on R') and therefore it suffices to verify this when applied to x. Indeed: $x^{\sigma(t-\tau)} = (\chi(\sigma)x)^{t-\tau} = x^{t-\tau} = a^{\ell}$ since τ acts on $\chi(\sigma)$ as the exponentiation with t. On the other hand, $x^{(t-\tau)\sigma} = a^{\ell\sigma} = a^{\ell}$ since σ acts trivially on $a^{\ell} \in R'$. Thus $x^{\sigma(t-\tau)} = x^{(t-\tau)\sigma}$ and therefore $x^{\sigma\tau} = x^{\tau\sigma}$.

We have proved the following

Statement (i):[10] *The relation* (16) *establishes uniquely an action of the cyclic group $\langle\tau\rangle$ as a group of G-algebra automorphisms of A', extending the action of $\langle\tau\rangle$ on R'.*

Now, according to the hypothesis of the Proposition, $\langle\tau\rangle = \mathfrak{g}$ and hence A' appears as a $\mathfrak{g}$-algebra. In fact, A' is a $G \times \mathfrak{g}$-algebra since the actions of G and of $\mathfrak{g}$ on A' commute elementwise. From the general theory we conclude that $A'|R$ is in fact a *Galois* $G \times \mathfrak{g}$-algebra (since $R'|R$ is a Galois $\mathfrak{g}$-algebra and $A'|R'$ is a Galois G-algebra; see **A.13**). From this the other assertions of (i) follow, namely: the fixed algebra $A(a) = \mathrm{Fix}(\mathfrak{g}, A')$ is a Galois G-algebra over R, and $A(a) \otimes_R R'$ is isomorphic to A' (see **A.11**).

[10] For later reference we observe that, in this part of proof, until now we have not used the fact that $\mathfrak{g} = \langle\tau\rangle$. Hence this statement remains valid for an arbitrary cyclic subgroup $\langle\tau\rangle$ of $\mathfrak{g}$. The group $\mathfrak{g}$ may be exceptional or not.

Proof of (ii): As above, A' denotes the Galois G-algebra over R' with Kummer radicand a^N; thus $A' = R'[x]$ with $x^n = a^N$. Similarly let $B' = R'[y]$ with $y^n = b^N$. Suppose that $a = bu^n$ with $u \in R'^{\times}$. We are going to establish an isomorphism $\varphi : A' \to B'$.

We have shown in part (ii) of the proof of Prop. 4 that the assignment

$$x^{\varphi} = yu^N \tag{17}$$

defines uniquely a G-isomorphism $A' \to B'$ over R'. Now we claim that, in addition, φ is compatible with the action of τ, i.e., that $\tau\varphi = \varphi\tau$. This holds on R' since φ leaves the elements of R' fixed. Hence again, it is sufficient to verify this when applied to x. Now from (16) we see that $x^{(t-\tau)\varphi} = a^{\ell\varphi} = a^{\ell}$; and on the other hand: $x^{\varphi(t-\tau)} = (yu^N)^{t-\tau} = b^{\ell}u^{N(t-\tau)} = b^{\ell}u^{\ell n} = a^{\ell}$, where we have used (13). Thus $x^{(t-\tau)\varphi} = x^{\varphi(t-\tau)}$ and therefore $x^{\tau\varphi} = x^{\varphi\tau}$. We have now shown the validity of

Statement (ii):[10] *Suppose $a = bu^n$ with $u \in R'^{\times}$. Then the relation* (17) *establishes an R'-algebra isomorphism $\varphi : A' \to B'$ which is compatible with the action of G and of τ.*

Now, according to the hypothesis of the Proposition, τ generates $\mathfrak{g}$. Hence $\varphi : A' \to B'$ is an isomorphism of G-algebras and of $\mathfrak{g}$-algebras, i.e., of $G \times \mathfrak{g}$-algebras. It follows that φ maps the fixed algebra $A(a) = \mathrm{Fix}(\mathfrak{g}, A')$ onto $A(b) = \mathrm{Fix}(\mathfrak{g}, B')$.

Proof of (iii): Now let $A|R$ be an arbitrary Galois G-algebra. Let us put $A' := A \otimes_R R'$. This is a Galois $G \times \mathfrak{g}$-algebra and we have $A = \mathrm{Fix}(\mathfrak{g}, A')$ (see **A.11**). In particular, τ acts on A', and this action commutes with every $\sigma \in G$. We are going to construct a Kummer radical x of $A'|R'$ such that, firstly, $x^n = a^N$ with $a \in A'^{\times}$, and secondly the relation (16) holds: $x^{t-\tau} = a^{\ell}$.

We start with an arbitrary Kummer radical $x \in A'^{\times}$. Since τ commutes with $\sigma \in G$ we have $x^{(t-\tau)\sigma} = x^{\sigma(t-\tau)} = \chi(\sigma)^{t-\tau}x^{t-\tau} = x^{t-\tau}$. Hence the element $u := x^{t-\tau}$ is kept fixed by all $\sigma \in G$ and therefore $u \in R'^{\times}$.

Now we use the fact that τ is non-exceptional, which by definition means that ℓ is relatively prime to n. Let $m \in \mathbb{Z}$ be a multiple of ℓ such that $m \equiv 1 \mod n$. Then $x^{m-1} \in R'^{\times}$ since $x^n \in R'^{\times}$ and $n|m-1$. Hence $x^m = x \cdot x^{m-1}$ differs from x by a factor from $R'^{\times}$, and therefore x^m too is a Kummer radical of $A'|R'$. We put $a = u^{m/\ell}$ and compute: $(x^m)^{(t-\tau)} = u^m = a^{\ell}$, and $(x^m)^n = x^{\ell n(m/\ell)} = x^{(t-\tau)N\cdot(m/\ell)} = u^{N\cdot(m/\ell)} = a^N$, where we have used (13). We have shown:

Statement (iii):[10] *For any Kummer radical x of $A'|R'$ the element $u := x^{t-\tau}$ is contained in $R'^{\times}$. Let $m \in \mathbb{Z}$ be a multiple of ℓ such that $m \equiv 1 \mod n$ (such m exists since τ is assumed to be non-exceptional). Then the m-th power x^m is also a Kummer radical of $A'|R'$. Its radicand is $(x^m)^n = a^N$ where $a := u^{m/\ell}$. Moreover, we have $(x^m)^{(t-\tau)} = a^{\ell}$.*

Now, changing notation we write again x instead of x^m. We have found a Kummer radical x of $A'|R'$ such that $x^n = a^N$ and $x^{t-\tau} = a^{\ell}$ for some $a \in R'^{\times}$, as required.

□

We shall have occasion to consider base extensions. Suppose that R is contained in the semisimple commutative K-algebra S. We assume that the unit element of R is also the unit element of S. Let $A|R$ be a Galois G-algebra, and consider the

Galois G-algebra $A_S := A \otimes_R S$ over S.[11] We say that A_S is obtained from A by *base extension* from R to S.

Let a be a Kummer parameter for A, so that $A = A(a)$. We claim that a is also a Kummer parameter for A_S. To see this, consider the diagram of R-algebras, with $A' = A \otimes_R R'$:

$$\begin{tikzcd}
 & A' \arrow[dd, dash, "G"'] \\
A \arrow[ur, dash, "\mathfrak{g}"] \arrow[dd, dash, "G"'] & \\
 & R' \\
R \arrow[ur, dash, "\mathfrak{g}"] &
\end{tikzcd}$$

Within A', the algebra A is characterized as the fixed algebra $A = \mathrm{Fix}(\mathfrak{g}, A')$. By tensoring with S we obtain the diagram

$$\begin{tikzcd}
 & A'_S \arrow[dd, dash, "G"'] \\
A_S \arrow[ur, dash, "\mathfrak{g}"] \arrow[dd, dash, "G"'] & \\
 & R'_S \\
R_S \arrow[ur, dash, "\mathfrak{g}"] &
\end{tikzcd}$$

where $A'_S = A' \otimes_R S$ and similarly A_S, R_S, R'_S. Again, we have $A_S = \mathrm{Fix}(\mathfrak{g}, A'_S)$ (see **A.10**). The action of $\mathfrak{g} = \langle \tau \rangle$ on A' is given by the formulas

$$x^n = a^N \tag{18}$$

$$x^{\sigma - 1} = \chi(\sigma) \quad (\text{for } \sigma \in G) \tag{19}$$

$$x^{t - \tau} = a^\ell \tag{20}$$

where $A' = R'[x]$; this establishes a as a Kummer parameter of A. Now, the same formulas hold in $A'_S = R'_S[x]$, and hence a is also a Kummer parameter of A_S. Thus we have:

Lemma 9 (Base extension) *Let A be a Galois G-algebra over R with Kummer parameter $a \in R'^\times$. If a is considered as an element in $S'^\times$, then it is a Kummer parameter for the Galois G-algebra $A_S = A \otimes_R S$ over S, which is obtained from A by base extension from R to S.*

2.4 Proof of Grunwald-Wang theorem. Based on the above parametrization we will now give a simple proof of the Grunwald-Wang theorem. This proof is restricted to the non-exceptional case since we shall use Kummer parameters according to Proposition 8. The exceptional case will be treated in the next section.

[11] See **A.10** for the fact that $A \otimes_R S$ is a Galois G-algebra over S.

We consider the situation of the Grunwald-Wang theorem; thus K is a multivalued field and $\widehat{K}$ its completion. We have to use the following Lemma. Of course this is well known; we present the proof for the convenience of the reader.

Lemma 10 *Suppose that n is not divisible by the characteristic of $\widehat{K}$. If $z \in \widehat{K}$ is sufficiently close to 1 then $z = u^n$ is an n-th power, with $u \in \widehat{K}^\times$.*

Proof: $\widehat{K}$ is a direct product of the complete fields $\widehat{K}_v$. It suffices to discuss each factor $\widehat{K}_v$ separately. In other words: we may assume that $\widehat{K}$ is a field with a single valuation $|\cdot|$.

If the valuation of $\widehat{K}$ is archimedean, then either $\widehat{K} = \mathbb{R}$ or $\widehat{K} = \mathbb{C}$. In this case the assertion is clear.

If $\widehat{K}$ is non-archimedean then we use the so-called Hensel-Rychlik Lemma. [12] Consider the polynomial $f(X) = X^n - z$; the condition $u^n = z$ is equivalent to $f(u) = 0$. We have

$$|f(1)| = |z-1| \qquad \text{and} \qquad |f'(1)| = |n| \le 1.$$

Note that $|n| > 0$ since n is not divisible by the characteristic of $\widehat{K}$. Therefore, if

$$|z-1| < |n|^2 \tag{21}$$

then the Hensel-Rychlik Lemma guarantees the existence of $u \in \widehat{K}$ such that

$$f(u) = 0 \qquad \text{and} \qquad |u-1| < |n|\,.$$

□

Proof of Grunwald-Wang theorem:

Besides of K we consider $K' = K(\sqrt[n]{1})$ and its completion $\widehat{K}' = K' \otimes_K \widehat{K}$. We apply Prop. 8 to Galois G-algebras over $R = \widehat{K}$.

Let A be a Galois G-algebra over $\widehat{K}$, and let $a \in \widehat{K}'^\times$ be a Kummer parameter for A, according to Proposition 8. We observe that K' is dense in $\widehat{K}'$; hence there are elements $b \in K'$ which are arbitrarily close to a. Then $a^{-1}b$ is close to 1 and we infer from Lemma 10 (applied to $\widehat{K}'$ instead of $\widehat{K}$) that $a^{-1}b \equiv 1 \mod \widehat{K}'^{\times n}$. Hence by Proposition 8, b is also a Kummer parameter for A. We change notation and write again a instead of b. We have seen:

There exists a Kummer parameter a for $A|\widehat{K}$ which is contained in K'.

Now we use again Proposition 8, but over K instead of $\widehat{K}$. Hence a is the Kummer parameter of a certain Galois G-algebra L over K. We apply Lemma 9 with respect to the base extension $K \subset \widehat{K}$ and conclude that $L \otimes_K \widehat{K} \approx A$. In view of (3) we see that $\widehat{L} \approx A$.

□

3 The exceptional case

In this section we consider the case when $\mathfrak{g}$ is exceptional in the sense as defined in connection with Lemma 5. Then we have necessarily $p = 2$ and $n = 2^\nu \ge 2$. The group $\mathfrak{g}$ contains a unique exceptional automorphism; this will be denoted by ε. By definition, ε acts on the roots of unity as the inverse operator: $\chi(\sigma)^\varepsilon = \chi(\sigma)^{-1}$.

$\mathfrak{g}$ is the direct product of the subgroup $\langle\varepsilon\rangle$ of order 2 and a cyclic group generated by a non-exceptional automorphism τ:

$$\mathfrak{g} = \langle\tau\rangle \times \langle\varepsilon\rangle\,. \tag{22}$$

[12] For this we refer to [6] II, §23, F14.

This follows from the fact that $\mathfrak{g}$ is isomorphic to a subgroup of $(\mathbb{Z}/2^\nu)^\times$ which has the product decomposition (11), and ε corresponds to -1 in this isomorphism.

We do not exclude the case $\tau = 1$ in which case $\mathfrak{g} = \langle\varepsilon\rangle$ is cyclic and hence K satisfies the Wang condition with respect to n.

Let s denote the order of τ. The *defining relations* for τ and ε as generators of $\mathfrak{g}$ are

$$\tau^s = 1\,, \qquad \varepsilon^2 = 1\,, \qquad \tau\varepsilon = \varepsilon\tau\,. \tag{23}$$

The invariants $s_\tau, t_\tau, \ell_\tau, N_\tau$ referring to τ will simply be denoted by s, t, ℓ, N, as in the foregoing section. The corresponding invariants for ε are

$$s_\varepsilon = 2, \quad t_\varepsilon = -1, \quad \ell_\varepsilon = 0, \quad N_\varepsilon = \varepsilon - 1\,.$$

We shall denote by K'_ε the fixed field of ε within K'. Thus $K'|K'_\varepsilon$ is a quadratic field extension.

3.1 Parametrization in the exceptional case. Again, let R be a commutative semisimple K-algebra, and consider the Galois $\mathfrak{g}$-algebra $R' = K' \otimes_K R$ of n-th roots of unity over R. Let

$$R'_\varepsilon = \mathrm{Fix}(\varepsilon, R') = K'_\varepsilon \otimes_K R$$

denote the subalgebra of the elements which are fixed under ε. Then R' is a Galois $\langle\varepsilon\rangle$-algebra over R'_ε and R'_ε is a Galois $\langle\tau\rangle$-algebra over R; see **A.9**. The map $z \mapsto z^{\varepsilon+1}$ is the ordinary norm map from the algebra R' to R'_ε.

In the exceptional case it will turn out that not every $a \in R'^\times$ is admissible as a Kummer parameter for Galois G-algebras.

Definition: An element $a \in R'^\times$ is called **admissible** if its ε-norm $a^{\varepsilon+1}$ is an n-th power in $R'^\times_\varepsilon$, i.e., if there exists $c \in R'^\times$ such that

$$a^{\varepsilon+1} = c^n \qquad \text{and} \qquad c^{\varepsilon-1} = 1\,. \tag{24}$$

If this is the case then (a, c) is called an **admissible pair**. The admissible pairs form a multiplicative subgroup $W \subset R'^\times \times R'^\times_\varepsilon$.

In the exceptional case, the following propositions are analogous to Propositions 7 and 8.

Proposition 11 *Suppose $\mathfrak{g} = \langle\tau\rangle \times \langle\varepsilon\rangle$ is exceptional. Let $A'|R'$ be a Galois G-algebra and $a' \in R'^\times$ a Kummer radicand of A'. If there exists an admissible $a \in R'^\times$ with $a' \equiv a^N \mod R'^{\times n}$ then there exists a Galois G-algebra A over R such that $A' = A \otimes_R R'$. The converse does also hold – provided the decomposition groups of the Galois $\mathfrak{g}$-algebra $R'|R$ are cyclic.*

This is an immediate consequence of

Proposition 12 (Parametrization; exceptional case) *Suppose $\mathfrak{g}$ is exceptional, and write $\mathfrak{g} = \langle\tau\rangle \times \langle\varepsilon\rangle$ as explained above.*

(i) *Every admissible pair $(a, c) \in W$ determines a Galois G-algebra $A(a, c)$ over R by means of the following two-step construction.*

Step 1:: *Construct the Galois G-algebra $A'|R'$ with the Kummer radicand a^N. Hence $A' = R'[x]$ with $x^n = a^N$ and $x^{\sigma-1} = \chi(\sigma)$.*

Step 2:: *Extend the action of $\mathfrak{g}$ on R' to an action of $\mathfrak{g}$ on A' such that $x^{t-\tau} = a^\ell$ and $x^{\varepsilon+1} = c^N$. This extension is possible and unique. Then put $A(a, c) := \mathrm{Fix}(\mathfrak{g}, A')$. This is a Galois G-algebra over R and $A(a, c) \otimes_R R' \approx A'$.*

(ii) *If (b,d) is another admissible pair and $(a,c) \equiv (b,d) \mod W^n$ then $A(a,c) \approx A(b,d)$.*

(iii) *Suppose that the decomposition groups of the Galois $\mathfrak{g}$-algebra $R'|R$ are cyclic. Then every Galois G-algebra A over R is isomorphic to $A(a,c)$ for a suitable admissible pair $(a,c) \in W$. Such a pair is called a* **Kummer parameter pair** *for A.*

Remark: We can reformulate Prop.8 as follows:

Let $\mathfrak{g}$ be exceptional. Suppose the decomposition groups of $R'|R$ are cyclic. Then the admissible pairs $(a,c) \in W$ parametrize the Galois G-algebras $A|R$ (up to isomorphisms). Pairs which differ by n-th power factors from W parametrize isomorphic Galois G-algebras.

The proof of parts (i),(ii) will be quite analogous to the proof in the non-exceptional case, the only difference being that now, besides of τ, also the exceptional automorphism ε has to be considered. In part (iii) there will be some new consideration necessary, taking into account the hypothesis about the decomposition groups of $R'|R$.

Proof of (i): Let A' be constructed as in Step 1. We try to extend the actions of both τ and ε on R' to actions as G-algebra automorphisms of A'.

As to τ, we have done this in the proof of Prop. 8 already; see Statement (i) there. (Observe footnote 10.) Accordingly, the action of $\langle\tau\rangle$ on R' extends uniquely to an action of $\langle\tau\rangle$ on A' such that $x^{t-\tau} = a^{\ell}$.

As to ε, we argue as follows. In order to extend the action of ε to an algebra homomorphism of A' it suffices to assign to x some element $z \in A'$ which satisfies the relations $z^n = a^{N\varepsilon}$. This holds for $z = x^{-1}c^N$. Indeed: we compute $(x^{-1}c^N)^n = a^{-N}c^{nN} = (a^{-1}c^n)^N = a^{\varepsilon N}$ where we have used the relation (24) which expresses admissibility of the pair (a,c).

As operator on A', ε remains to be of order 2, for: $x^{\varepsilon^2-1} = x^{(\varepsilon+1)(\varepsilon-1)} = c^{N(\varepsilon-1)} = c^{(\varepsilon-1)N} = 1$ since c is fixed by ε in view of (24). Note that as operators on R' we have $\tau\varepsilon = \varepsilon\tau$ and hence $N\varepsilon = \varepsilon N$.

But we also have $\tau\varepsilon = \varepsilon\tau$ on A'. To see this we compute: $x^{(t-\tau)(\varepsilon+1)} = a^{\ell(\varepsilon+1)} = c^{\ell n}$ in view of (24), and on the other hand $x^{(\varepsilon+1)(t-\tau)} = c^{N(t-\tau)} = c^{\ell n}$ where we have used (13).

We have shown that the extended actions of τ, ε satisfy the defining relations (23) of the group $\mathfrak{g}$. In other words: *The formulas*

$$x^{t-\tau} = a^{\ell} \qquad \text{and} \qquad x^{\varepsilon+1} = c^N \tag{25}$$

define uniquely an extension of the action of $\mathfrak{g} = \langle\tau\rangle \times \langle\varepsilon\rangle$ on R' to an action of $\mathfrak{g}$ as R-algebra automorphisms on A'.

Next we claim that $\mathfrak{g}$ acts on A' by G-automorphisms, which is to say that τ as well as ε commute with each $\sigma \in G$. As to τ, we again refer to Statement (i) in the proof of Prop. 8. For ε we verify: $x^{\sigma(\varepsilon+1)} = (\chi(\sigma)x)^{\varepsilon+1} = x^{\varepsilon+1} = c^N$ since ε acts on $\chi(\sigma)$ as the exponentiation with -1. On the other hand, $x^{(\varepsilon+1)\sigma} = c^{N\sigma} = c^N$ since σ leaves $c^N \in R'$ fixed.

We have seen:

The action of $\mathfrak{g}$ on A' given by (25) commutes elementwise with the action of G.

Hence A' now becomes a $G \times \mathfrak{g}$-algebra. Again, as in the non-exceptional case, we conclude that A' is a Galois $G \times \mathfrak{g}$-algebra over R (since $R'|R$ is a Galois $\mathfrak{g}$-algebra and $A'|R'$ a Galois G-algebra; see **A.13**). From this it follows that $A(a,c) = \mathrm{Fix}(\mathfrak{g}, A')$ is a Galois G-algebra over R and that $A(a,c) \otimes_R R' \approx A'$ (see **A.11**).

Proof of (ii): As in the proof of Prop. 8(ii) we let $A' = R'[x]$ with $x^n = a^N$ and $B' = R'[y]$ with $y^n = b^N$. Again, we have to exhibit an R'-isomorphism $\varphi : A' \to B'$ which is an isomorphism as $G \times \mathfrak{g}$-algebras. Suppose that $a = bu^n$ and $c = dv^n$ with $(u, v) \in W$. Then we define φ by the same formula (17) as in the proof of prop. 8. According to Statement (ii) there, this indeed defines an R'-algebra isomorphism, and it is compatible with the action of τ and of each $\sigma \in G$ (see footnote 10). It remains to verify that it is also compatible with ε. To this end we compute: $x^{(\varepsilon+1)\varphi} = c^{N\varphi} = c^N$ since φ acts as the identity operator on R'; on the other hand $x^{\varphi(\varepsilon+1)} = (yu^N)^{\varepsilon+1} = d^N u^{(\varepsilon+1)N} = (dv^n)^N = c^N$ where we have used that the pair (u, v) is admissible and hence $u^{\varepsilon+1} = v^n$.

Proof of (iii): In this part of proof we suppose that the decomposition groups of $R'|R$ are cyclic.

R is the direct product of the fields eR where e ranges over the set $P(R)$ of primitive idempotents of R. For each e we have $eR' = K' \otimes_K eR$, thus we see that eR' is the algebra of roots of unity over eR. If $A|R$ is a Galois G-algebra then $eA|eR$ is a Galois G-algebra too (see **A.3**). Accordingly it suffices for each e to exhibit an admissible pair in eW with respect to eA; since W is the direct product of the eW we obtain an admissible pair for A.

Consequently, we may assume from now on that R is a field.

Therefore there is only one decomposition group of $R'|R$, say $\mathfrak{h}$ (see **A.6**). $\mathfrak{h}$ is a subgroup of $\mathfrak{g}$, and $\mathfrak{h}$ is cyclic by hypothesis. In our discussion we will have to distinguish the cases $\varepsilon \notin \mathfrak{h}$ and $\varepsilon \in \mathfrak{h}$. In each of these cases, given a Galois G-algebra $A|R$ we have to construct a Kummer radical x of $A' := A \otimes_R R'$ such that $x^n = a^N$ for some admissible $a \in R'^\times$, and that in addition (25) holds for some $c \in R'^\times$ for which (a, c) is an admissible pair. Note that A' is a Galois $G \times \mathfrak{g}$-algebra, and hence τ, ε act on A' as G-algebra automorphisms.

Case 1: $\varepsilon \notin \mathfrak{h}$.

We first claim: *If $u \in R'^\times$ is fixed under ε then there exists $v \in R'^\times$ such that* $u = v^{\varepsilon+1}$. In other words: *The norm map $v \mapsto v^{\varepsilon+1}$ from $R'^\times$ to $R'^\times_\varepsilon$ is surjective.*

Proof: Consider the set $P(R')$ of primitive idempotents of R'. Since R is a field, $\mathfrak{g}$ acts transitively on $P(R')$. (See **A.5**.) The decomposition group $\mathfrak{h}$ is defined to be the stabilizer of an idempotent in $P(R')$. This does not depend on the choice of this idempotent since $\mathfrak{g}$ is abelian. Consequently, the assumption that $\varepsilon \notin \mathfrak{h}$ implies that ε does not leave any primitive idempotent in $P(R')$ fixed. Accordingly $P(R')$ splits into pairs of idempotents which are mutually conjugate under ε. Let $\mathcal{E}$ be a set of representatives of those pairs, so that

$$P(R') = \mathcal{E} \cup \mathcal{E}^\varepsilon\,, \qquad \mathcal{E} \cap \mathcal{E}^\varepsilon = \emptyset\,.$$

Let e denote the sum of the primitive idempotents in $\mathcal{E}$. Then e is an idempotent of R' (not primitive in general) and we have

$$1 = e + e^\varepsilon\,, \qquad e \cdot e^\varepsilon = 0\,.$$

This leads to a direct product decomposition

$$\begin{aligned} R' &= eR' \times e^{\varepsilon} R' \\ &= eR' \times (eR')^{\varepsilon} \\ &\approx S' \times S' \qquad \text{where} \quad S' := eR' . \end{aligned} \tag{26}$$

Using this isomorphism, every $u \in R'^{\times}$ can be written as a vector in the form $u = (u_1, u_2)$ with $u_1, u_2 \in S'^{\times}$. We have $e = (1,0)$ and $e^{\varepsilon} = (0,1)$. The automorphism ε acts on vectors by interchanging the components:

$$(u_1, u_2)^{\varepsilon} = (u_2, u_1) .$$

If $u^{\varepsilon} = u$ then $u_1 = u_2$. Hence, putting $v := (1, u_1)$ we have $v^{\varepsilon+1} = (u_1, 1)(1, u_1) = (u_1, u_1) = u$.

Our claim is proved.

Now let $A|R$ be any Galois G-algebra, and $A' = A \otimes_R R'$. We are looking for a Kummer radical x of $A'|R'$ such that $x^n = a^N$, and that (25) holds for some admissible pair (a,c).

We start with an arbitrary Kummer radical $x \in A'^{\times}$. Since ε commutes with $\sigma \in G$ we compute

$$x^{(\varepsilon+1)\sigma} = x^{\sigma(\varepsilon+1)} = \chi(\sigma)^{\varepsilon+1} x^{\varepsilon+1} = x^{\varepsilon+1} , \tag{27}$$

because ε acts on $\chi(\sigma)$ as the inverse operator. Thus $x^{\varepsilon+1}$ is stable under G and therefore $x^{\varepsilon+1} =: u \in R'^{\times}$. It follows $u^{\varepsilon-1} = x^{\varepsilon^2-1} = 1$ and therefore, as shown above, $u = v^{\varepsilon+1}$ with some $v \in R'^{\times}$. Hence $(xv^{-1})^{\varepsilon+1} = 1$. Changing notation and writing again x instead of xv^{-1} we have shown:

There exists a Kummer radical x of $A'|R'$ such that $x^{\varepsilon+1} = 1$.

With this Kummer radical x we now use the Statement (iii) as formulated in the proof of Prop. 8 (see footnote 10). We conclude that x^m is another Kummer radical of $A'|R'$, and that for certain $a \in R'^{\times}$ we have $(x^m)^n = a^N$ and $(x^m)^{t-\tau} = a^{\ell}$. Explicitly, a is given as $a = x^{(t-\tau)m/\ell}$, from which we conclude that $a^{\varepsilon+1} = 1$. In addition, $(x^m)^{\varepsilon+1} = 1$. Changing notation, we write again x instead of x^m. Thus we have produced a Kummer radical x of $A'|R'$ with the properties:

$$x^n = a^N \qquad \text{and} \qquad x^{t-\tau} = a^{\ell} \qquad \text{and} \qquad x^{\varepsilon+1} = 1 .$$

In addition we have $a^{\varepsilon+1} = 1$ which shows that the pair $(a,1)$ is admissible, as required.

Case 2: $\varepsilon \in \mathfrak{h}$.

In this case we have to invoke our hypothesis that the decomposition group $\mathfrak{h}$ is cyclic. Hence, since ε is not a square in $\mathfrak{h}$ we conclude that $\mathfrak{h} = \langle\varepsilon\rangle$ is of order 2.

The powers $1, \tau, \tau^2, \ldots, \tau^{s-1}$ represent the cosets of $\mathfrak{g}$ modulo $\mathfrak{h} = \langle\varepsilon\rangle$. Let e be a primitive idempotent of R'. The stabilizer of e in $\mathfrak{g}$ is the decomposition group $\mathfrak{h}$, and the conjugates $e, e^{\tau}, e^{\tau^2}, \ldots, e^{\tau^{s-1}}$ are precisely the different primitive idempotents of R'. The decomposition

$$1 = e + e^{\tau} + \cdots + e^{\tau^{s-1}} \tag{28}$$

into orthogonal primitive idempotents leads to a direct decomposition

$$\begin{aligned} R' &= eR' \times e^{\tau}R' \times \cdots \times e^{\tau^{s-1}}R' \\ &= eR' \times (eR')^{\tau} \times \cdots \times (eR')^{\tau^{s-1}} \\ &\approx S' \times S' \times \cdots \times S' \qquad \text{with } \ S' := eR' \end{aligned} \tag{29}$$

This decomposition is the analogue, in Case 2, of the decomposition (26) which we have used in Case 1.

Now let $A|R$ be a Galois G-algebra and $A' = A \otimes_R R'$. Then $\mathfrak{g}$ acts on A' such that $A = \mathrm{Fix}(\mathfrak{g}, A')$. We claim:

There exists a Kummer radical x of $A'|R'$ such that $x = y^N$ with $y \in A'^{\times}$.

This can be seen as follows: The primitive idempotent $e \in R'$ may not be primitive in A'. Nevertheless, the decomposition (28) yields a decomposition of A' similarly to (29), namely:

$$\begin{aligned} A' &= eA' \times e^{\tau}A' \times \cdots \times e^{\tau^{s-1}}A' \\ &= eA' \times (eA')^{\tau} \times \cdots \times (eA')^{\tau^{s-1}} \\ &\approx B' \times B' \times \cdots \times B' \qquad \text{with } \ B' := eA' \,. \end{aligned} \tag{30}$$

According to this decomposition, every element $x \in A'$ can be written as a vector

$$x = (x_0, x_1, \ldots, x_{s-1}) \qquad \text{with} \qquad x_i \in B' \,. \tag{31}$$

In this representation the automorphism τ acts as the right shift:

$$x^{\tau} = (x_{s-1}, x_0, x_1, \ldots) \,.$$

The automorphism ε acts component-wise:

$$x^{\varepsilon} = (x_0^{\varepsilon}, \ldots, x_{s-1}^{\varepsilon}) \,.$$

Note that $B' = eA'$ is stable under ε since e is.

We start with an arbitray Kummer radical x of $A'|R'$. We refer to Statement (iii) of the proof of Prop. 8 for the fact that the element $u := x^{t-\tau}$ is contained in $R'^{\times}$ (see footnote 10). We write x in the form (31) and similarly u; we conclude that $x_i^t x_{i-1}^{-1} = u_i \in S'^{\times}$. By induction it follows $x_{s-1}^{t^{s-1-i}} = x_i v_i$ $(0 \leq i \leq s-1)$ where the elements v_i are power products of the u_i; for our purpose it is sufficient to know that $v_i \in S'^{\times}$ and hence $v = (v_0, v_1, \ldots, v_{s-1}) \in R'^{\times}$. Putting $y := x_{s-1}$, we conclude

$$\left(y^{t^{s-1}}, y^{t^{s-2}}, \ldots, y^t, y\right) = (x_0, x_1, \ldots, x_{s-1})(v_0, v_1, \ldots, v_{s-1}) = x \cdot v \,. \tag{32}$$

The vector on the left hand side can be written as y^N if we identify $B'^{\times}$ with the first factor of the product $B'^{\times} \times \cdots \times B'^{\times}$, so that y is identified with the vector $(y, 1, 1, \ldots, 1)$. Indeed, the definition of the operator N reads $N = t^{s-1} + t^{s-2}\tau + \cdots + \tau^{s-1}$ and if we apply this operator to $(y, 1, 1, \ldots, 1)$ we obtain the vector on the left hand side in (32) since τ acts as the shift. So we have

$$y^N = x \cdot v \,.$$

Since x is a Kummer radical of $A'|R'$ and $v \in R'^{\times}$, it follows that xv is a Kummer radical too. Changing notation, we write again x instead of xv and thus have obtained a Kummer radical x such that $x = y^N$.

Our above claim is proved. But we have obtained more information. Namely, since $y = x_{s-1}$ appears as the last component of x, it follows that y^n is the last component of x^n. Since $x^n \in R'^{\times}$ it follows $y^n \in S'^{\times}$. Let us put $a := y^n \in S'^{\times} \subset R'^{\times}$.

Moreover, we know from (27) that $x^{\varepsilon+1}$ is contained in $R'^{\times}$. [13] Now, $y^{\varepsilon+1}$ is the last component of $x^{\varepsilon+1}$ and therefore it follows that $y^{\varepsilon+1} \in S'^{\times} \subset R'^{\times}$. Let us put $c := y^{\varepsilon+1}$.

We have proved:

There exists a Kummer radical x of $A'|R'$ such that $x = y^N$ for some $y \in A'^{\times}$. Moreover, $y^n = a$ and $y^{\varepsilon+1} = c$ with $a, c \in R'^{\times}$.

For this Kummer radical we compute:

$$\begin{aligned} x^n &= y^{nN} = a^N \\ x^{t-\tau} &= y^{(t-\tau)N} = y^{\ell n} = a^{\ell} \\ x^{\varepsilon+1} &= y^{(\varepsilon+1)N} = c^N\,, \end{aligned}$$

these are the relations (25), and

$$\begin{aligned} a^{\varepsilon+1} &= y^{(\varepsilon+1)n} = c^n \\ c^{\varepsilon-1} &= y^{(\varepsilon+1)(\varepsilon-1)} = 1\,. \end{aligned}$$

this shows that the pair (a, c) is admissible.

□

Proposition 12 is proved.

Again we shall have occasion to consider base extension. Suppose that R is contained in the semi-simple commutative K-algebra S. We assume that the unit element of R is also the unit element of S, hence $R^{\times} \subset S^{\times}$. Moreover, $R' = K' \otimes_K R$ is contained in $S' = K' \otimes_K S$ and $R'^{\times} \subset S'^{\times}$. In this situation we have in the exceptional case too:

Lemma 13 (Base extension) *Suppose that $\mathfrak{g}$ is exceptional, and that the decomposition groups of the Galois $\mathfrak{g}$-algebra $R'|R$ are cyclic. Let A be a Galois G-algebra over R with Kummer parameter pair (a, c). If a and c are considered as elements in $S'^{\times}$, then (a, c) is a Kummer parameter pair for the Galois G-algebra $A \otimes_R S$ over S, which is obtained from A by base extension $R \subset S$.*

The proof proceeds as in the non-exceptional case.

The following Lemma gives a method to generate admissible pairs. As introduced above, $R'_{\varepsilon} = \mathrm{Fix}(\varepsilon, R')$ denotes the subalgebra of elements which are fixed under the exceptional automorphism ε.

Lemma 14 *If $(a, c) \in R'^{\times} \times R'^{\times}_{\varepsilon}$ is admissible then a can be written in the form $a = \widetilde{a}^{\varepsilon-1} c^{n/2}$ with $\widetilde{a} \in R'^{\times}$. Conversely, if $\widetilde{a} \in R'^{\times}$ and $c \in R'^{\times}_{\varepsilon}$ are arbitrary, then by putting $a = \widetilde{a}^{\varepsilon-1} c^{n/2}$, the pair pair (a, c) is admissible.*

In other words: *The map $(\widetilde{a}, c) \mapsto (a, c)$ as described above is a surjective homomorphism from $R'^{\times} \times R'^{\times}_{\varepsilon}$ onto the group W of admissible pairs.*

Proof: (a, c) to be admissible means that $a^{\varepsilon+1} = c^n$ and $c^{\varepsilon} = c$. From this it follows $(ac^{-n/2})^{\varepsilon+1} = 1$. We apply "Hilbert's Theorem 90" (see **A.14**) to the Galois $\langle\varepsilon\rangle$-algebra $R'|R'_{\varepsilon}$. We conclude that there exists $\widetilde{a} \in R'^{\times}$ such that $ac^{-n/2} = \widetilde{a}^{\varepsilon-1}$, hence $a = \widetilde{a}^{\varepsilon-1} c^{n/2}$.

[13] In (27) we have only used that ε commutes with every automorphism of G; this is true in both cases, Case 1 and Case 2.

The converse is directly verified.

□

3.2 Proof of Grunwald-Wang theorem. We consider the situation of Theorem 1 in the exceptional case; this implies in particular that $n = 2^\nu$ is a power of 2.

Again, $K' = K(\sqrt[n]{1})$ denotes the field of n-th roots of unity over K. Let $K'_\varepsilon = \mathrm{Fix}(\varepsilon, K')$ denote the fixed field of the exceptional automorphism ε. Let Let $\widehat{K}$, $\widehat{K}'_\varepsilon$, $\widehat{K}'$ be the completions of K, K'_ε, K' respectively.

The decomposition groups in K' of the valuations $v \in V$ are precisely the decomposition groups of the Galois $\mathfrak{g}$-algebra $\widehat{K}'$ over $\widehat{K}$. We assume that all those decomposition groups are cyclic. According to Proposition 12 this implies that every Galois G-algebra A over $\widehat{K}$ admits a Kummer parameter pair (a, c).

Similarly as in the non-exceptional case we try to choose a Kummer parameter pair (a, c) for A such that $a, c \in K'^\times$.

We start with an arbitrary parameter pair (a, c) for A and write $a = \widetilde{a}^{\varepsilon-1}c^{n/2}$ as in Lemma 14. Since K' is dense in $\widehat{K}'$ there exists $\widetilde{b} \in K'$ which is close to $\widetilde{a}$. Applying Lemma 10 we conclude that

$$\widetilde{a} \equiv \widetilde{b} \mod \widehat{K}'^{\times n}.$$

Similarly, since K'_ε is dense in $\widehat{K}'_\varepsilon$, we find $d \in K'_\varepsilon$ close to c, and conclude

$$c \equiv d \mod \widehat{K}'^{\times n}_\varepsilon.$$

Putting $b = \widetilde{b}^{\varepsilon-1}d^{n/2}$ we obtain an admissable pair (b, d) (by Lemma 14) and we have $b \in K'$ and $d \in K'_\varepsilon$. Moreover, Lemma 14 shows that we have

$$(a, c) \equiv (b, d) \mod W^n.$$

Consequently, Proposition 12(ii) says that the admissible pair (b, d) parametrizes the same algebra A as (a, c).

We change notation and write again (a, c) instead of (b, d). We have shown:

There exists a Kummer parameter pair (a, c) for $A|\widehat{K}$ such that $a \in K'^\times$ and $c \in K'^\times_\varepsilon$.

Now we use Proposition 12(i), but over K instead of $\widehat{K}$. Hence (a, c) is a pair of Kummer parameters of a certain Galois G-algebra L over K. We apply Lemma 13 with respect to the base extension $K \subset \widehat{K}$ and conclude that $L \otimes_K \widehat{K} \approx A$. In view of (3) we see that $\widehat{L} \approx A$.

□

4 The case of characteristic p

As before, G is a cyclic group of prime power order $n = p^\nu$, and K is a field. Now we consider the case that $\mathrm{char}(K) = p$.

4.1 Preliminaries on Witt vectors. Let A be a commutative ring with unit element such that $pA = 0$; thus A is an $\mathbb{F}_p$-algebra. We denote by $W_\nu(A)$ the ring of Witt vectors $x = (x_0, \ldots, x_{\nu-1})$ of length ν over A. [14] Addition and multiplication of those vectors are defined by polynomials. More precisely, if the Witt vector z is

[14] For the basic facts about Witt vectors we refer to [6] II. § 26.

the sum (or product) of x and y then the i-th component z_i is a certain polynomial, with integer coefficients, in $x_0, \ldots x_i, y_0, \ldots, y_i$. [15]

The Frobenius operator F on $W_\nu(A)$ is defined by

$$F(x) = (x_0^p, x_1^p, \ldots)\,;$$

this is an endomorphism of the ring $W_\nu(A)$. The Artin-Schreier map $\wp$ on $W_\nu(A)$ is defined by

$$\wp(x) = F(x) - x\,.$$

This map is additive. For $\nu \geq 1$ the shift operator $V\colon W_{\nu-1}(A) \to W_\nu(A)$ is defined by

$$V(x_0, x_1, \ldots, x_{\nu-2}) = (0, x_0, x_1, \ldots, x_{\nu-2})\,.$$

This map is useful for induction arguments. [16] V is additive and injective, and it satisfies $FV = VF$. It follows $\wp V = V\wp$. The image of V is the kernel of the canonical homomorphism $W_\nu(A) \to A$ which maps every vector x onto its first component x_0. Thus we have the exact sequence

$$0 \to W_{\nu-1}(A) \xrightarrow{V} W_\nu(A) \longrightarrow A \to 0$$

For $x_0 \in A$ we denote by $\{x_0\}$ the vector [17]

$$\{x_0\} = (x_0, 0, 0, \ldots, 0)\,.$$

The map $x_0 \mapsto \{x_0\}$ is a section for the projection homomorphism $W_\nu(A) \to A$; it is multiplicative but not additive. The fundamental rules for the addition of Witt vectors imply [18] for $x = (x_0, x_1, \ldots, x_{\nu-1})$ that

$$x = \{x_0\} + V\widetilde{x} \qquad \text{with} \qquad \widetilde{x} = (x_1, x_2, \ldots, x_{\nu-1}) \in W_{\nu-1}(A)\,. \tag{33}$$

We shall have to use this formula in the sequel.

4.2 Witt radicals for cyclic Galois algebras. Now let R be a semisimple commutative K-algebra. We want to give a description of the Galois G-algebras over R.

We consider $W_\nu(\mathbb{F}_p)$ as a subring of $W_\nu(R)$. The additive group $W_\nu(\mathbb{F}_p)^+$ is well known to be cyclic of order p^ν (see [6] II. § 26 p.147). We choose an isomorphism

$$\chi\colon G \to W_\nu(\mathbb{F}_p)^+\,.$$

This isomorphism is kept fixed throughout and all statements in the sequel refer to the given χ.

Let $a = (a_0, \ldots, a_{\nu-1}) \in W_\nu(R)$. Consider the R-algebra $A = R[x]$ generated by ν elements $x_0, \ldots, x_{\nu-1}$ which, when interpreted as a vector $x = (x_0, \ldots, x_{\nu-1}) \in W_\nu(A)$, satisfy

$$\wp(x) = a \tag{34}$$

as their *defining relations*. This means that A is isomorphic to the factor algebra of the polynomial algebra $R[X] = R[X_0, \ldots, X_{\nu-1}]$ modulo the ideal I generated by the polynomials $f_0, \ldots, f_{\nu-1} \in R[X]$ which describe the relation (34), i.e.,

$$\wp(X) - a = (f_0(X), \ldots, f_{\nu-1}(X)) \qquad \text{in} \qquad W_\nu(R[X])\,;$$

[15] For later use we note that these polynomials have vanishing constant coefficients.

[16] In our notation of F,V and $\wp$ we suppress the dependence on ν; even for different ν we shall use the same symbols F,V and $\wp$.

[17] This is Witt's original notation [14].

[18] See [6] II. § 26 p.140

and x_i denotes the image of X_i in A $(0 \le i \le \nu - 1)$. In this sense, the relation (34) in $W_\nu(A)$ is to be interpreted as a system of polynomial relations

$$f_i(x_0, \ldots, x_{\nu-1}) = 0 \qquad\qquad (0 \le i \le \nu - 1)$$

and these are *defining relations* for the generators $x_0, \ldots, x_{\nu-1}$ of $A|R$.

If we assign to the generating vector $x = (x_0, \ldots, x_{\nu-1})$ some vector $y = (y_0, \ldots, y_{\nu-1})$ with components $y_i \in A$ satisfying the same relation $\wp(y) = a$, then this defines uniquely an R-algebra homomorphism of A into itself which maps the x_i onto the y_i. [19] Let $\sigma \in G$. We have $\wp(\chi(\sigma)) = 0$ since $\chi(\sigma) \in W_\nu(\mathbb{F}_p)$. Hence for $y = x + \chi(\sigma)$ we have $\wp(y) = \wp(x) = a$. Thus σ defines an R-algebra homomorphism of A into itself. By general functorial properties of Witt vectors, this extends canonically to a ring homomorphism of $W_\nu(A)$ into itself, denoted also by σ, and we have

$$x^\sigma = (x_0^\sigma, \ldots, x_{\nu-1}^\sigma)\,. \tag{35}$$

So the definition of the action of σ on A can be put into the formula

$$x^\sigma = x + \chi(\sigma) \qquad\qquad (\sigma \in G) \tag{36}$$

(which again is to be interpreted as a system of polynomial equations for the components of the respective vectors). The homomorphism property $\chi(\sigma\tau) = \chi(\sigma) + \chi(\tau)$ yields $x^{\sigma\tau} = (x^\sigma)^\tau$. In this way we see that G acts on A and also on $W_\nu(A)$.

Thus the relations (36) define on A the structure of G-algebra over R. We denote this algebra by A_a since it is uniquely determined by the Witt vector $a \in W_\nu(R)$.

The following result, valid in characteristic p, is Witt's additive analogue to the multiplicative Kummer Theory of Proposition 4.

Proposition 15 (Witt Theory for Galois algebras) **(i)** *Let $a \in W_\nu(R)$. Then any G-algebra $A|R$ generated by the components of some Witt vector $x \in W_\nu(A)$ satisfying the relations*

$$\wp(x) = a \qquad \text{and} \qquad x^\sigma = x + \chi(\sigma)\,, \qquad (\sigma \in G) \tag{37}$$

is a Galois G-algebra, and A is isomorphic to A_a (as G-algebras over R).

(ii) *If $a \equiv b \mod \wp W_\nu(R)$, i.e., if $a = b + \wp(u)$ with $u \in W_\nu(R)$ then the Galois G-algebra A_a determined by a is isomorphic to the Galois G-algebra A_b determined by b. And conversely.*

(iii) *Every Galois G-algebra $A|R$ is of the type described in* (i)*, i.e., A is isomorphic to A_a (as Galois G-algebra over R) for suitable $a \in W_\nu(R)$. Such a Witt vector a is called a* **Witt radicand** *of A, and the corresponding x is a* **Witt radical** *of A.*

Remark: We can reformulate Proposition 15 as follows:

Every Witt vector $a \in W_\nu(R)$ defines (uniquely up to isomorphisms) a Galois G-algebra $A|R$ such that a is a Witt radicand of A. The structure of A depends only on the (additive) residue class of a modulo $\wp W_\nu(R)$. Conversely, every Galois G-algebra $A|R$ admits a vector $a \in W_\nu(R)$ as its Witt radicand.

Proof of (i): We shall use induction with respect to ν.

[19] In other words: the map $R[X] \to A$ given by $X_i \mapsto y_i$ $(0 \le i \le \nu - 1)$ can be factored through $R[X]/I \approx R[x]$.

Using **A.3** (and basic functorial properties of Witt vectors) we may suppose that R is a field. To show that A is a Galois G-algebra we use **A.4**. Hence we have to show that

(a) *A is semisimple.*
(b) $\mathrm{Fix}(G, A) = R$.
(d) G acts faithfully on A.

Statement (d) is immediate from the second relation in (37). It remains to verify (a) and (b).

First consider the case $\nu = 1$. Then $W_1(A)$ can be identified with A itself; in the relation (37) we now have $x \in A$ and $a \in R$. Thus the generator x of $A|R$ satisfies an Artin-Schreier equation in the usual sense: $x^p - x = a$. Let $f(X) = X^p - X - a \in R[X]$ (one variable X). Then we have $A_a \approx R[X]/f(X)$. Since $f(X)$ is separable (i.e., it has no multiple roots), it follows that A_a is semisimple; this gives (a) for A_a. If $f(X)$ is irreducible over R then $A_a|R$ is a Galois extension of fields of degree p, and assertion (b) follows for A_a. If $f(X)$ is not irreducible over R then it splits completely in $R[X]$:

$$f(X) = (x - \vartheta_1) \cdots (x - \vartheta_p)$$

where $\vartheta_1, \ldots, \vartheta_p \in R$ are the roots of $f(X)$. It follows that

$$A_a \approx R \times \cdots \times R$$

this decomposition is defined by assigning to x the vector $(\vartheta_1, \ldots, \vartheta_p)$ and, accordingly, to every polynomial $h(x) \in R[x] = A_a$ the vector $(h(\vartheta_1), \ldots, h(\vartheta_p))$. Here, $h(x)$ may be assumed to be of degree $< p$. The automorphisms $\sigma \in G$ permute the ϑ_i cyclically. If $h(x)$ is fixed under all $\sigma \in G$ then $h(\vartheta_i) = h(\vartheta_1)$ for all i. It follows that $h(x)$ is a constant polynomial, i.e., $h(x) \in R$. Thus we have (b) for A_a.

We have now shown (for $\nu = 1$) that A_a is a Galois G-algebra over R. As to A, since it is generated by x over R, there is a natural *surjective* G-homomorphism $A_a \to A$ as G-algebras; applying **A.12** it follows that this is an isomorphism and, hence, A too is a Galois G-algebra.

Now suppose $\nu > 1$. Consider the projection homomorphism $W_\nu(A) \to A$ given by $(x_0, \ldots, x_{\nu-1}) \mapsto x_0$. Then $A = R[x]$ is projected onto $A_0 = R[x_0]$ with the relations

$$\wp(x_0) = a_0 \qquad \text{and} \qquad x_0^\sigma = x_0 + \chi_0(\sigma) \qquad (\sigma \in G)$$

where $\chi_0(\sigma) \in \mathbb{F}_p$ denotes the first component of the Witt vector

$$\chi(\sigma) = (\chi_0(\sigma), \ldots, \chi_{\nu-1}(\sigma))\,.$$

We have $\chi_0(\sigma^i) = i \cdot \chi_0(\sigma) = 0$ if and only if $i \equiv 0 \mod p$. Hence the group G^p of p-th powers in G acts trivially on A_0 while the factor group G/G^p acts faithfully on A_0. By what we have seen in the case $\nu = 1$, A_0 is a Galois G/G^p-algebra over R. In particular, A_0 is semisimple and we have

$$\mathrm{Fix}(G/G^p, A_0) = R\,. \tag{38}$$

Now consider A as a G^p-algebra over A_0. We claim that $A|A_0$ is a Galois G^p-algebra.

A is generated over $A_0 = R[x_0]$ by $x_1, \ldots, x_{\nu-1}$ which we regard as the components of the Witt vector $\widetilde{x} = (x_1, \ldots, x_{\nu-1}) \in W_{\nu-1}(A)$, of length $\nu - 1$. Let us put $b := \wp(\widetilde{x})$. Using (33) we compute

$$Vb = V\wp(\widetilde{x}) = \wp V(\widetilde{x}) = \wp(x - \{x_0\}) = a - \wp\{x_0\}$$

from which we infer that the components of Vb, hence those of b, are polynomials (with integer coefficients) in $a_0, a_1, \ldots, a_{\nu-1}$ and x_0. We conclude that the components of b are contained in $A_0 = R[x_0]$. Thus we have

$$\wp(\widetilde{x}) = b \in W_{\nu-1}(A_0).$$

A similar computation for the action of an automorphism $\tau \in G^p$ leads to the following: We have already seen above that the first component $\chi_0(\tau) = 0$ since $\tau = \sigma^p \in G^p$. Thus

$$\chi(\tau) = (0, \chi_1(\tau), \ldots, \chi_{\nu-1}(\tau)) = V\widetilde{\chi}(\tau)$$

where $\widetilde{\chi}(\tau) = (\chi_1(\tau), \ldots, \chi_{\nu-1}(\tau)) \in W_{\nu-1}(\mathbb{F}_p)$. Now we observe that the operator τ acts componentwise, i.e., $x^\tau = (x_0^\tau, \ldots, x_{\nu-1}^\tau)$. We have seen above already that $\tau \in G^p$ acts trivially on A_0, hence $x_0^\tau = x_0$. We compute, using (33):

$$\begin{aligned} V\widetilde{x}^{\,\tau} &= x^\tau - \{x_0^\tau\} = x + \chi(\tau) - \{x_0\} \\ &= (x - \{x_0\}) + \chi(\tau) \\ &= V\widetilde{x} + V\widetilde{\chi}(\tau) = V(\widetilde{x} + \widetilde{\chi}(\tau)) \end{aligned}$$

and hence

$$\widetilde{x}^{\,\tau} = \widetilde{x} + \widetilde{\chi}(\tau)\,.$$

We have seen that A, as a G^p-algebra over A_0, is generated by the components of the Witt vector $\widetilde{x}$ of length $\nu - 1$, satisfying relations of the same form as does x over R, namely:

$$\wp(\widetilde{x}) = b \in W_{\nu-1}(A_0) \qquad \text{and} \qquad \widetilde{x}^{\,\tau} = \widetilde{x} + \widetilde{\chi}(\tau)\,, \quad (\tau \in G^p)\,.$$

By induction hypothesis we conclude that, indeed, A is a Galois G^p-algebra over A_0.

In particular A is semisimple, which gives (a). Moreover, $A_0 = \mathrm{Fix}(G^p, A)$ and hence, using (38):

$$\mathrm{Fix}(G, A) = \mathrm{Fix}(G, A_0) = \mathrm{Fix}(G/G^p, A_0) = R\,.$$

This gives (b).

We have now shown that A is a Galois G-algebra over R. It follows that A_a too is a Galois G-algebra over R, since A_a satisfies the same hypotheses as announced in the statement of the proposition. Now again, since A is generated by x there is a natural surjection $A_a \to A$, and we infer from **A.12** that this is an isomorphism.

Proof of (ii): Consider the algebra $A_a = R[a]$ with (37), and similarly $A_b = R[y]$. Suppose that $a = b + \wp(u)$ with $u \in W_\nu(R)$. We are going to establish an isomorphism $\varphi : A_a \to A_b$ as G-algebras over R.

The relation $\wp(x) = a$ is a *defining relation* for x over R. Hence, in order to obtain a homomorphism $\varphi : A_a \to A_b$ as R-algebras, it is sufficient to assign to x some vector $z \in W_\nu(A)$ such that z satisfies the same relation $\wp(z) = a$ as x does. Clearly this holds for $z := y + u$ since $\wp(y + u) = b + \wp(u) = a$.

Hence we have a uniquely defined R-algebra homomorphism $\varphi : A_a \to A_b$ such that $x^\varphi = y + u$. We claim that this is a homomorphism as G-algebras. Indeed: for $\sigma \in G$ we have $x^{\sigma\varphi} = (x + \chi(\sigma))^\varphi = x^\varphi + \chi(\sigma) = y + u + \chi(\sigma) = y^\sigma + u = (y + u)^\sigma = x^{\varphi\sigma}$ since σ acts trivially on $u \in W_\nu(R)$.

Since both A_a and A_b are Galois G-algebras over R it follows that $\varphi : A_a \to A_b$ is an isomorphism. (See **A.12**.)

Conversely, assume that A_a and A_b are isomorphic Galois G-algebras. Let us identify $A_a = A_b = A$ by that isomorphism. Thus on the one hand, $A_a = R[x]$ with (37), and on the other hand $A_a = A_b = R[y]$ with corresponding relations for y and b. When applying $\sigma \in G$ both x and y take the same additive summand, namely $\chi(\sigma)$. We conclude $(y-x)^\sigma = y - x$ for all $\sigma \in G$. It follows that the coordinates of the vector $u := y - x$ are contained in R, i.e., $u \in W_\nu(R)$. We have $b = \wp(y) = \wp(x) + \wp(u) = a + \wp(u) \equiv a \mod \wp R$.

Proof of (iii): Now let A be an arbitrary Galois G-algebra over R. We have to find $x \in W_\nu(A)$ and $a \in W_\nu(R)$ satisfying the relations (37), and such that A is generated over R by the components of x.

Since G acts on A it also acts on the ring $W_\nu(A)$ of Witt vectors by means of (35). Consider the trace operator S on $W_\nu(A)$ defined by

$$S(u) = \sum_{\tau \in G} u^\tau \qquad \text{for} \qquad u \in W_\nu(A)\,.$$

Since the vector $S(u)$ is fixed by every $\sigma \in G$, its components are fixed by G and hence are contained in R; we conclude that $S(u) \in W_\nu(R)$. We claim: *There exists $u \in W_\nu(A)$ such that $S(u)$ is a unit in $W_\nu(R)$.*

To see this we recall that a vector is a unit in $W_\nu(R)$ if and only if its first component is a unit in R. [20] Now the first component of $S(u)$ is $S(u_0)$ where $u_0 \in A$ is the first component of u. Since A is a Galois G-algebra it admits a normal basis over R. If we choose $u_0 \in A$ as a generator of such a normal basis then $S(u_0) \in R^\times$. For, if this were not the case then there would exist $c \neq 0$ in R such that

$$c \cdot S(u_0) = \sum_\tau c \cdot u_0^\tau = 0$$

which contradicts the fact that the u_0^τ form a basis of A over R.

Thus indeed, there exists a vector $u \in W_\nu(A)$ such that $S(u) \in W_\nu(R)^\times$; we have to choose u such that its first component u_0 is a generator of a normal basis of $A|R$. After replacing u by $S(u)^{-1}u$ we may assume that

$$S(u) = 1\,.$$

We start from such u and put

$$x := \sum_{\tau \in G} \chi(\tau^{-1}) u^\tau\,,$$

like we did in the multiplicative Kummer theory. We compute for $\sigma \in G$:

$$\begin{aligned} x^\sigma &= \sum_{\tau \in G} \chi(\tau^{-1}) u^{\tau\sigma} = \sum_{\tau \in G} \chi(\tau^{-1}\sigma) u^\tau \\ &= \sum_{\tau \in G} (\chi(\tau^{-1}) + \chi(\sigma)) u^\tau \\ &= \sum_{\tau \in G} \chi(\tau^{-1}) u^\tau + \chi(\sigma) \sum_{\tau \in G} u^\tau \\ &= x + \chi(\sigma)\,. \end{aligned}$$

Let us put $a := \wp(x)$. Then we compute

$$a^\sigma = \wp(x^\sigma) = \wp(x + \chi(\sigma)) = \wp(x) = a$$

[20] See e.g., Witt [14], p.131, Satz 5.

since $\wp(\chi(\sigma)) = 0$. Hence the components of a are fixed under G and therefore contained in R; it follows $a \in W_\nu(R)$.

Thus the vector $x \in W_\nu(A)$ satisfies relations of the form (37). From (i) we conclude that the subalgebra $R[x] \subset A$ is a Galois G-algebra, with the action of G on $R[x]$ induced by the action of G on A. The inclusion map $R[x] \hookrightarrow A$ is a map of Galois G-algebras and hence an isomorphism by **A.12**; this shows that $R[x] = A$. □

Remark: Let $A|R$ be a Galois G-algebra and $a \in W_\nu(R)$ a Witt radicand of A. The corresponding Witt radical $x \in W_\nu(A)$ of a is not uniquely determined. An element $y \in W_\nu(A)$ is another Witt radical of a if and only if $y = x + c$ with $c \in W_\nu(R)$ and $\wp(c) = 0$. If R is a direct product of d fields then there are n^d such elements c. The n^d substitutions $x \mapsto x + c$ yield n^d automorphisms of A as Galois G-algebra over R, and every automorphism of A is of this form.

Similarly as in multiplicative Kummer theory, we shall need the following lemma concerning base extension. Suppose that R is contained in the semi-simple commutative K-algebra S. We assume that the unit element of R is also the unit element of S. Then $W_\nu(R) \subset W_\nu(S)$. In this situation we have:

Lemma 16 (Base extension) *Let A be a Galois G-algebra over R with Witt radicand $a \in W_\nu(R)$. If a is considered as a vector in $W_\nu(S)$, then it is a Kummer parameter for the Galois G-algebra $A \otimes_R S$ over S, which is obtained from A by base extension $R \subset S$.* [21]

The proof is again immediate: We have $A \subset A \otimes_R S$ and hence $W_\nu(A) \subset W_\nu(A \otimes_R S)$. If $x \in W_\nu(A)$ satisfies the relations (37) then it satisfies the same relations when considered as a vector in $W_\nu(A \otimes_R S)$.

4.3 Proof of Grunwald-Wang theorem. We consider the situation of the Grunwald-Wang theorem; thus K is a multi-valued field and $\widehat{K}$ its completion. We assume that $\mathrm{char}(K) = p$. We have to use the following Lemma, which is the additive analogue to the corresponding Lemma 10 in the multiplicative case.

Lemma 17 *Suppose that $n = p^\nu$ where p is the characteristic of K. If the components $z_i \in \widehat{K}$ of the Witt vector $z \in W_\nu(\widehat{K})$ are sufficiently close to 0 then there exists $u \in W_\nu(\widehat{K})$ such that $z = \wp(u)$.*

Proof: $\widehat{K}$ is a direct product of the complete fields $\widehat{K}_v$. It suffices to discuss each factor $\widehat{K}_v$ separately. In other words: we may assume $\widehat{K}$ to be a complete field with a single valuation $|\cdot|$. Note that the valuation is non-archimedean since $\mathrm{char}(K) = p$.

We claim that the condition

$$|z_i| < 1 \qquad \text{for} \qquad 0 \le i \le \nu - 1$$

is already sufficient: if this condition is satisfied then we claim there exists a vector $u = (u_0, \ldots, u_{\nu-1}) \in W_\nu(\widehat{K})$ with $\wp(u) = z$. Moreover, u can be chosen such that $|u_i| < 1$ for $0 \le i \le \nu - 1$. We use induction on ν.

If $\nu = 1$ we have $W_1(\widehat{K}) = \widehat{K}$. We use Hensel's lemma for the polynomial $f(X) = X^p - X - z \in \widehat{K}[X]$. If u is a zero of $f(X)$ then $z = \wp(u)$. We have

$$|f(0)| = |z| \qquad \text{and} \qquad |f'(0)| = 1.$$

[21] See **A.10** for the fact that $A \otimes_R S$ is a Galois G-algebra over S.

Therefore, if $|z| < 1$ then Hensel's lemma guarantees the existence of a unique $u \in \widehat{K}$ such that $f(u) = 0$ and $|u| < 1$.

Now suppose $\nu > 1$ and write (see (33)):

$$z = \{z_0\} + V\widetilde{z}\,.$$

Using what we have just seen for $\nu = 1$, we let $u_0 \in \widehat{K}$ with $|u_0| < 1$ such that $\wp(u_0) = z_0$. Using the induction hypothesis we find $\widetilde{u} \in W_{\nu-1}(\widehat{K})$ such that $\wp(\widetilde{u}) = \widetilde{z}$, and each component of $\widetilde{u}$ has value < 1. Now we write

$$\begin{aligned} z &= \{\wp\, u_0\} + V\wp(\widetilde{u}) \\ &= \wp\left(\{u_0\} + V\widetilde{u}\right) + \left(\{\wp\, u_0\} - \wp\{u_0\}\right) \\ &= \wp u + t \end{aligned}$$

if we put

$$u := \{u_0\} + V\widetilde{u} \qquad \text{and} \qquad t := \{\wp\, u_0\} - \wp\{u_0\}\,.$$

Thus the vector u as constructed does not yet solve our requirements; we still have to discuss the remainder t.

Let us write $t = \{t_0\} + V\widetilde{t}$. By definition of t we have $t_0 = \wp(u_0) - \wp(u_0) = 0$ and therefore $t = V\widetilde{t}$ with $\widetilde{t} = (t_1, \ldots, t_{\nu-1}) \in W_{\nu-1}(\widehat{K})$. We can use the induction hypothesis and conclude that $\widetilde{t} = \wp(u')$ with $u' \in W_{\nu-1}(\widehat{K})$ – *provided* we know that $|t_i| < 1$ for all i. Now, from the definition of t we see that each t_i is a polynomial in u_0 with integer coefficients. Since these polynomials do not have constant coefficients [22] and since $|u_0| < 1$ we conclude that each $|t_i| < 1$. Recall that the valuation of $\widehat{K}$ is non-archimedean.

Thus by the induction hypothesis we have $\widetilde{t} = \wp(u')$ with $u' \in W_{\nu-1}(\widehat{K})$, and all components of u' have value $|u'_i| < 1$. It follows $t = V\wp(u') = \wp(Vu')$ and hence

$$z = \wp(u) + \wp(Vu') = \wp(u + Vu')\,.$$

This proves our assertion since, by footnote 15 again, all components of $u + Vu'$ have value < 1.

□

Proof of Grunwald-Wang theorem:

Besides of K we consider its completion $\widehat{K}$. We apply Prop.15 to Galois G-algebras over $R = \widehat{K}$.

Let A be a Galois G-algebra over $\widehat{K}$, and let $a \in W_\nu(\widehat{K})$ be a Witt radicand for A, according to Prop.15(iii). We observe that K is dense in $\widehat{K}$; hence there are elements $b_i \in K$ which are arbitrarily close to the components a_i of a ($0 \le i \le \nu-1$). Then the $a_i - b_i$ are close to 0 and we infer from Lemma 17 that $b - a \equiv 0 \mod \wp W_\nu(\widehat{K})$. Hence by Prop.15(ii), $b = (b_0, \ldots, b_{\nu-1})$ is also a Witt radicand for A. Changing notation, we have seen:

There exists a Witt radicand a for $A|\widehat{K}$ which is contained in $W_\nu(K)$.

Now, we use Prop.15(i), but over K instead of $\widehat{K}$. Hence a is a Witt radicand of a certain Galois G-algebra L over K. We apply Lemma 16 with respect to the base extension $K \subset \widehat{K}$ and conclude that $L \otimes_K \widehat{K} \approx A$. In view of (3) we see that $\widehat{L} \approx A$.

□

[22] See footnote 15.

5 Appendix: On Galois algebras

All algebras considered here are supposed to be algebras over a field, and to have a unit element. [23]

Let R be a semisimple commutative algebra and G a finite group. A *G-algebra over R* is defined to be a commutative R-algebra A, together with an action of G on A, such that every $\sigma \in G$ acts as an R-algebra automorphism of A. We use the exponential notation for this action, thus x^σ denotes the image of $x \in A$ under the action of $\sigma \in G$. Every such G-algebra carries the structure of a right RG-module, where RG denotes the group ring of G over R.

A.1 Definition: *A G-algebra $A|R$ is called* **Galois G-algebra** *if the following two conditions are satisfied:*

(a) A is semisimple.
(b) A is a free RG-module of rank 1.

Property (b) is equivalent to the existence of a **normal basis** for $A|R$, i.e., the existence of an element $u \in A$ such that its G-images u^σ $(\sigma \in G)$ form an R-basis of A. In particular it follows that G acts faithfully on A. Moreover, the existence of an R-basis of A implies that we can identify $R = R \cdot 1_A$ with a subalgebra of A. Then $R = \operatorname{Fix}(G, A)$, the *fixed algebra* of G in A, consisting of those $x \in A$ which are fixed under all $\sigma \in G$.

A.2 Note: *Every Galois extension of fields $L|K$ with Galois group G is a Galois G-algebra in a natural way.* (Normal Basis theorem, cf. [6] §12.)

Any commutative semisimple algebra R is the direct product of fields:

$$R = K_1 \times \cdots \times K_m$$

where the component fields K_i are uniquely determined as subsets of R (cf. [6], §29). If e_i denotes the unit element of K_i, then

$$1 = e_1 + \cdots + e_m \qquad \text{with} \qquad e_ie_j = \begin{cases} e_i & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

We have $K_i = e_iR$, and as an R-module we have the direct sum decomposition

$$R = e_1R \oplus \cdots \oplus e_mR = K_1 \oplus \cdots \oplus K_m\,.$$

Every idempotent $e \in R$ is a partial sum of $e_1, \ldots, e_m$. An idempotent of R is called *primitive* if it cannot be written as a sum of two orthogonal idempotents of R. The e_i are precisely the primitive idempotents of R. In the following we use the notation

$$P(R) := \{e_1, \ldots, e_m\}$$

for the set of all primitive idempotents in R.

A.3 Reduction Lemma: *Let $A|R$ be a G-algebra. Consider the direct product decomposition*

$$A = \prod_{e \in P(R)} eA\,. \tag{A1}$$

For $A|R$ to be a Galois G-algebra it is necessary and sufficient that $eA|eR$ is a Galois G-algebra for each $e \in P(R)$.

[23] For the general terminology and the basic facts which are used without citation we refer to [6], in particular §§28–29.

For the proof one observes that each of the definining conditions (a) and (b) is satisfied for $A|R$ if and only if it is satisfied for all components $eA|eR$ in (A1).

Note that for the algebra $eA|eR$ the ground ring eR is a *field*. Hence, in the discussion of Galois G-algebras $A|R$, Lemma **A.3** will often allow us to reduce the discussion to the case when R is a field; this explains the name "Reduction Lemma."

Remark: In the situation of **A.3** each eA is also an R-subalgebra of A. However, if R is not a field (i.e., if $e \neq 1$) then $eA|R$ is not a Galois G-algebra.

A.4 Galois algebras over a field: *Suppose $R = K$ is a field. Let $A|K$ be a G-algebra satisfying the following three conditions:*

(a) *A is semisimple*
(b) $\mathrm{Fix}(G, A) = K$
(c) $[A : K] \geq |G|$

where $[A : K]$ denotes the K-dimension of A, and $|G|$ the order of G. Then $A|K$ is a Galois G-algebra and, in fact, we have $[A : K] = |G|$. If G is abelian then the condition (c) *can be replaced by the following condition:*

(d) *G acts faithfully on A.*

We shall prove this together with the following structure theorem for Galois algebras. In fact, we shall give the proof of the structure theorem under the hypotheses of **A.4**, and then conclude that A is indeed a Galois G-algebra.

A.5 Structure of Galois algebras over a field. *Suppose $R = K$ is a field. Let $A|K$ be a G-algebra satisfying* (a), (b), (c) *above* (*or* (a), (b), (d) *if G is abelian*). *Then G acts transitively on the set $P(A)$ of primitive idempotents of A. Let $e \in P(A)$ and put $L := eA$; this is a field. Then*

$$A = \prod_{\sigma \in G \bmod G_e} L^{\sigma} \,. \tag{A2}$$

Here, G_e denotes the subgroup of those elements in G which leave e fixed, and σ ranges over a set of representatives of left cosets $G_e\sigma$ of G.

The group G_e operates on L and with this operation, L is a Galois G_e-algebra over eK. In other words*: If L is regarded as an extension field of K* (*by identifiying $K = eK$*)*, then L is Galois over K and the action of G_e on L yields an isomorphism $G_e \approx \mathrm{Gal}(L|K)$.*

Proof: The sum $s = \sum_{\sigma \in G \bmod G_e} e^{\sigma}$ is left fixed by G. Using (b) we conclude $s \in K$. Since s is an idempotent and K is a field it follows $s = 1$. Hence $1 \in A$ is the sum of the distinct primitive idempotents e^{σ}. It follows

$$P(A) = \{e^{\sigma} : \sigma \in G \bmod G_e\}$$

and we obtain the decomposition (A2). The fact that eA is a field follows from hypothesis (a), that A is semi-simple.

Suppose $a \in L$ is left fixed by G_e. Then $b := \sum_{\sigma \in G \bmod G_e} a^{\sigma}$ is left fixed by G. From (b) it follows $b \in K$ and hence $a = eb \in eK$. Thus $eK = \mathrm{Fix}(G_e, L)$. It follows that $L|eK$ is a Galois extension of fields, and its Galois group is induced by the action of G_e on L. Thus the Galois group of $L|eK$ is a homomorphic image of G_e and therefore

$$[L : K] \leq |G_e| \,. \tag{A3}$$

It remains to show that G_e acts *faithfully* on L, which by Galois theory is equivalent to $[L:K]=|G_e|$. If we consider A as a K-module then

$$A = \oplus \sum_{\sigma\in G \bmod G_e} L^\sigma\,, \tag{A4}$$

the direct sum of the K-modules L^σ. Comparing K-dimensions we get from (A3)

$$[A:K]=(G:G_e)\cdot[L:K]\le(G:G_e)\cdot|G_e|=|G|\,.$$

From (c) we obtain $[L:K]=|G_e|$.

If G is abelian then, using (d) we have the following argument to show that G_e acts faithfully on L: Let $\tau\in G_e$ and suppose that $a^\tau=a$ for each $a\in L$. Then for any $\sigma\in G$ we have $a^{\sigma\tau}=a^{\tau\sigma}=a^\sigma$, and hence τ leaves every a^σ fixed ($a\in L$, $\sigma\in G$). From (A4) we conclude that τ leaves every element in A fixed. Hence from (d): $\tau=1$.

□

Proof of A.4: We have to verify that A admits a G-normal basis over K. We use the structure theorem **A.5** which we have proved under the hypotheses of **A.4**. The field L as defined by the structure theorem is a Galois field extension of K whose Galois group we may identify with G_e. There exists a normal basis of $L|K$. Accordingly let $u\in L$ be such that the u^τ with $\tau\in G_e$ form a basis of $L|K$. Each element in G has a unique representation of the form $\tau\sigma$ with $\tau\in G_e$, and σ ranging over a set of representatives of left cosets of G modulo G_e. Looking at (A4) we see that the $u^{\tau\sigma}$ form a K-basis of A.

□

A.6 Decomposition groups. *The subgroup $G_e\subset G$ in* **A.5** *is called the decomposition group of $A|K$ associated to the primitive idempotent e.*

The decomposition group associated to e^σ is $\sigma^{-1}G_e\sigma$. Hence the Galois G-algebra $A|K$ determines a class of conjugate subgroups of G as its decomposition groups. If G is abelian then the decomposition group is uniquely determined by A and is called the decomposition group of the Galois G-algebra $A|K$; it is denoted by G_A.

This definition applies only if the ground ring of A is a field. For a Galois G-algebra $A|R$ over an arbitrary semisimple algebra R, we consider the decomposition (A1). The primitive idempotents of R will now be denoted by ε. Thus A is the direct product of the Galois G-algebras $\varepsilon A|\varepsilon R$, $\varepsilon\in P(R)$. Each εR is a field, and hence $\varepsilon A|\varepsilon R$ determines a decomposition group contained in G, unique up to conjugates. Thus, any Galois G-algebra $A|R$ determines finitely many classes of conjugate decomposition groups in G. Every such class corresponds to a primitive idempotent $\varepsilon\in P(R)$.

A.7 Induced algebras: Let $A|K$ be a Galois G-algebra over a field K. The formula (A2) shows that as G-algebra over K, A is "*induced*" by the G_e-algebra $L|K$ [24] which in turn is a Galois extension of fields whose Galois group is isomorphic

[24] Here we use the notion of "induced G-algebra" in a similar way as the notion of "induced G-module" is used in representation theory. For the latter, we have to regard A as a G-module over K and the formula (A4) shows that and how A is obtained from the G_e-module L over K. If, besides of the addition in A we consider also the multiplication, i.e., if we consider A not only as G-module over K but also as G-algebra over K, and similarly for L, then we speak of "induced G-algebra". In this case we prefer to use the notation of direct product instead of direct sum, i.e., we use formula (A2) instead of (A4).

to G_e. In particular we see that A as G-algebra over K is uniquely determined by the Galois field extension $L|K$ and the isomorphism $\mathrm{Gal}(L|K) \approx G_e \subset G$.

Conversely, if $L|K$ is an arbitrary Galois extension of fields and $\mathrm{Gal}(L|K) \hookrightarrow G$ is any injection of its Galois group into G then the construction (A2) yields a G-algebra $A|K$; this is a Galois G-algebra as follows from Proposition **A.2**. Its decomposition group is, up to conjugates, the image of $\mathrm{Gal}(L|K)$ in G. In this sense, the theory of Galois G-algebras over a field K is essentially the same as the theory of Galois extensions $L|K$, together with an injection $\mathrm{Gal}(L|K) \hookrightarrow G$.

A.8 Subalgebras: *If $A|R$ is a Galois G-algebra, then every R-subalgebra $B \subset A$ is semisimple.*

To see this, we observe that B is commutative, has no nilpotent elements and is finitely generated over R (hence Artinian) since A has these properties. [25]

A.9 Fixed subalgebras: *Let $A|R$ be a G-algebra. For a normal subgroup $H \subset G$ let $B := \mathrm{Fix}(H, A)$ be the corresponding fixed algebra. B is naturally a G/H-algebra over R, and A an H-algebra over B. We claim: If $A|R$ is a Galois G-algebra then:*

(i) *$B|R$ is a Galois G/H-algebra,*
(ii) *$A|B$ is a Galois H-algebra.*

Proof: (i) Choose a normal basis u^σ $(\sigma \in G)$ of $A|R$. Let ϱ run through a set of representatives for the cosets ϱH of G modulo H. The elements $u_\varrho := \sum_{\tau \in H} u^{\varrho\tau}$ are fixed under H and hence contained in B. A direct verification shows that these u_ϱ form an R-basis of B. Since H is normal in G, the left and right cosets of G modulo H coincide: $\varrho H = H\varrho$. Hence for the basis constructed above, we have $u_\varrho = u_1^\varrho$. Thus the u_ϱ form a G/H-normal basis of $B|R$. Since B is semisimple by **A.8**, it follows that $B|R$ is a Galois G/H-algebra.

(ii) Next we show that A is a Galois H-algebra over B. In view of the reduction lemma **A.3** we may assume from the start that $R = K$ is a field.

(iia) If B is a field too then we simply apply **A.4** to the H-algebra A over the field B. In our case, condition (c) of **A.4** reads $[A : B] \geq |H|$. This condition is satisfied because on the one hand $|G| = [A : K] = [A : B] \cdot [B : K]$, and on the other hand we know from (i) that $[B : K] = (G : H)$ (since B admits the K-basis u_ϱ corresponding to the cosets ϱH of G modulo H); it follows $[A : B] = |H|$.

(iib) In general, however, B is not a field and we have to discuss the structure of B in more detail. Again using **A.3** it suffices to show that for every primitive idempotent $\varepsilon \in P(B)$ the H-algebra εA is a Galois H-algebra over εB. Here, εB is a field. We also note that $\varepsilon B = \varepsilon \mathrm{Fix}(H, A) = \mathrm{Fix}(H, \varepsilon A)$. We shall see in (iic) that $\varepsilon A|\varepsilon K$ is a Galois G_ε-algebra for some subgroup $G_\varepsilon \subset G$ containing H. Thus for εA and the group G_ε we have precisely the situation as discussed above in (iia), and we conclude that, indeed, εA is a Galois H-algebra over εB.

(iic) The primitive idempotent ε of B need not be primitive in A. In any case ε is a sum of orthogonal primitive idempotents of A; let e be one of them. Since ε is fixed under H, all H-conjugates e^τ with $\tau \in H$ are also summands of ε. Consider the sum $\sum'_{\tau \in H} e^\tau$ where the prime indicates that each H-conjugate of e appears only once. The above sum is an idempotent fixed under H, hence is contained in

[25] See [6] §29, Satz 2.

B. Since ε is primitive in B it follows

$$\varepsilon = \sum_{\tau \in H}{}' e^{\tau} \,. \tag{A5}$$

To say that each H-conjugate of e appears only once in ε, is equivalent to saying that τ ranges over a set of coset representatives of H modulo $G_e \cap H$. Here, the notation is the same as in **A.5**, namely $G_e = \mathrm{Fix}(e, G)$. These τ form a set of representatives of $G_e H$ modulo G_e; note that $G_e H$ is a group since H is normal in G. We put $G_\varepsilon := G_e H$. It is straightforward to verify that $G_\varepsilon = \mathrm{Fix}(\varepsilon, G)$.

εA is naturally a G_ε-algebra, and we have from (A5)

$$\varepsilon A = \prod_{\tau \in G_\varepsilon \bmod G_e} e^{\tau} A = \prod_{\tau \in G_\varepsilon \bmod G_e} L^{\tau} \tag{A6}$$

where we have put $L := eA$; this is a field. We conclude that the G_ε-algebra εA is *induced* from the G_e-algebra $L|eK$, the latter being a Galois extension of fields with Galois group G_e according to **A.5** (applied to the original Galois G-algebra A over K). We conclude from **A.7** that εA is a Galois G_ε-algebra over εK, as contended.

□

A.10 Base extension: *Let $A|R$ be a Galois G-algebra. Let S be a commutative semisimple R-algebra. Then $A \otimes_R S$ is a Galois G-algebra over S, the action of G on $A \otimes_R S$ being defined by $(x \otimes y)^\sigma = x^\sigma \otimes y$. Moreover:*

(i) *For any subgroup $H \subset G$ we have* $\mathrm{Fix}(H, A \otimes_R S) = \mathrm{Fix}(H, A) \otimes_R S$.

(ii) *Each of the decomposition groups of $A \otimes_R S$ is contained in some decomposition group of A.*

Proof: Starting with a normal R-basis u^σ $(\sigma \in G)$ for A we obtain a normal S-basis $u^\sigma \otimes 1$ for $A \otimes_R S$.

For a subgroup $H \subset G$ we use the notation of the proof of **A.9**; the u_ϱ as defined there form an R-basis of $\mathrm{Fix}(H, A)$ and the $u_\varrho \otimes 1$ an S-basis of $\mathrm{Fix}(H, A) \otimes_R S$, where ϱ ranges over a set of representatives of the cosets of G modulo H.

To show that $A \otimes_R S$ is semisimple, we first decompose S into a direct product of fields; note that S is assumed to be semisimple. This reduces the proof to the case where S, and hence R too, is a field.

Secondly, we decompose A into a direct product of fields: $A = \prod_{e \in P(A)} eA$. By the structure theorem, each eA is a Galois field extension of eR, and its Galois group is one of the decomposition groups of $A|R$. This reduces the proof to the case where $A|R$ is a Galois extension of fields, and G the Galois group of this extension.

Now, the tensor product $A \otimes_R S$ of two field extensions $A|R$ and $S|R$, one of which is algebraic, separable and of finite degree, is well known to be a direct product of finitely many fields. Hence $A \otimes_R S$ is semisimple. In fact, each direct field component of $A \otimes_R S$ is the field compositum $A \cdot S$ after an embedding of A into an algebraically closed overfield of S. It is well known that $A \cdot S$ is a Galois extension of S, its Galois group being naturally isomorphic to the Galois group of $A|A \cap S$, hence a subgroup of G.

□

A.11 Tensor products: (i) *If $A|R$ is a Galois G-algebra and $B|R$ a Galois H-algebra then $A \otimes_R B$ is a Galois $G \times H$-algebra. Here, the action of $G \times H$ on $A \otimes_R B$ is defined by $(x \otimes y)^{(\sigma,\tau)} = x^\sigma \otimes y^\tau$.*

(ii) *Conversely, every Galois $G \times H$-algebra C over R is isomorphic to the tensor product $A \otimes_R B$ of the Galois G-algebra $A := \mathrm{Fix}(H, C)$ with the Galois H-algebra $B := \mathrm{Fix}(G, C)$.*

Proof: (i) By **A.10** $A \otimes_R B$ is semi-simple. If $u \in A$ generates a G-normal basis of A over R and $v \in B$ generates an H-normal basis of B over R then $u \otimes v$ generates a normal $G \times H$-basis of $A \otimes_R B$ over R. Hence $A \otimes_R B$ is a Galois $G \times H$-algebra.

(ii) Since G and H are normal in $G \times H$ we see from **A.9** that A is a Galois G-algebra and B is a Galois H-algebra over R. Hence $A \otimes_R B$ is a Galois $G \times H$-algebra over R, as shown in (i). The natural map $A \otimes_R B \to C$ is a map of $G \times H$-algebras over R. The following lemma shows that this is an isomorphism.

□

A.12 Lemma: *Suppose $A|R$ is a Galois G-algebra and $B|R$ is any G-algebra. Let $f : A \to B$ be a homomorphism of G-algebras over R* (i.e., a homomorphism of R-algebras which is also a homomorphism of G-modules)*. Then f is injective. If B too is a Galois G-algebra over R then f is an isomorphism.*

Proof: It is enough to prove, for each $e \in P(R)$, that the restriction $eA \to eB$ is injective. Thus we may suppose $R = K$ to be a field.

In this case we know from the Structure Theorem **A.5** that the primitive idempotents of A are permuted *transitively* by G. Hence the kernel of f cannot contain any primitive idempotent of A. For, if this would be the case then $\mathrm{Ker}(f)$ (which is stable under G) would contain all primitive idempotents, hence their sum 1, which gives a contradiction. Since A is semisimple we conclude $\mathrm{Ker}(f) = 0$. Thus f is injective. If B too is a Galois G-algebra over K then both A and B have the same dimension over K and hence $f(A) = B$.

□

A.13 Tower of Galois algebras: *Let $\mathfrak{g}$ and G be two finite groups. Let $R'|R$ be a Galois $\mathfrak{g}$-algebra and $A'|R'$ be a Galois G-algebra. Suppose the action of $\mathfrak{g}$ on R' is extended to an action of $\mathfrak{g}$ on the R-algebra A' in such a way that as operator group on A', $\mathfrak{g}$ commutes elementwise with G.* (Thus $A'|R$ can be viewed as $G \times \mathfrak{g}$-algebra.) *Put $A := \mathrm{Fix}(\mathfrak{g}, A')$.* (Because of the imposed commuting condition A is a G-algebra over R.) *Then we have:*

(i) *$A'|R$ is a Galois $G \times \mathfrak{g}$-algebra.*
(ii) *$A|R$ is a Galois G-algebra.*
(iii) *The natural map $A \otimes_R R' \to A'$ is an isomorphism of $G \times \mathfrak{g}$-algebras.*

$$\begin{tikzcd}
& A' \approx A \otimes_R R' \arrow[dl, dash, "\mathfrak{g}"'] \arrow[dd, dash, "G"'] \\
A = \mathrm{Fix}(\mathfrak{g}, A') \arrow[dd, dash, "G"'] & \\
& R' \arrow[dl, dash, "\mathfrak{g}"'] \\
R &
\end{tikzcd}$$

Proof: (i) We again refer to **A.3**. So it suffices to show, for a given $e \in P(R)$, that the $G \times \mathfrak{g}$-algebra $eA'|eR$ is Galois; after changing notation we thus may assume that $R = K$ is a field.

Since $A'|R'$ is a Galois G-algebra, it is a free R'-module of rank $|G|$. Similarly, $[R' : K] = |\mathfrak{g}|$. It follows

$$[A' : K] = |G| \cdot |\mathfrak{g}| = |G \times \mathfrak{g}| \,. \tag{A7}$$

Now the assertion follows from **A.4**, applied to the $G \times \mathfrak{g}$-algebra $A'|R$; note that $\mathrm{Fix}(G \times \mathfrak{g}, A') = R = K$.

(ii) and (iii) follow from (i), see Lemma **A.12**. □

Hilbert's Theorem 90: This theorem holds for arbitrary Galois G-algebras. However, we need it in this paper for a very special case only, namely for *quadratic* Galois G-algebras, which means that the group G is of order 2. In that case the statement and proof is rather trivial. For the convenience of the reader we shall present it here.

A.14 Lemma*:* Suppose $A|R$ is a Galois G-algebra for a group G of order 2, i.e., $G = \langle\sigma\rangle$ and $\sigma^2 = 1$. Let $a \in A^\times$. If $a^{\sigma+1} = 1$ then there exists $b \in A^\times$ such that $a = b^{\sigma-1}$. And conversely.

Proof: Using **A.3** we may suppose that $R = K$ is a field. If we put $b := 1 + a^{-1}$ then we compute $b^\sigma = a \cdot b$ using $a^\sigma = a^{-1}$. Hence if b is a unit in A then b is a solution of the problem.

If b is not a unit in A then $b^{\sigma+1}$ is not a unit either; since $b^{\sigma+1}$ is contained in the field K it follows $b^{\sigma+1} = 0$. But $b^{\sigma+1} = ab^2$ and since a is a unit we have $b^2 = 0$, hence $b = 0$ because A does not contain nilpotent elements. We conclude $a = -1$.

Thus if $a = -1$ then the above definition of b has to be modified. In that case we put $b := u - u^\sigma$ where $u \in A$ is chosen such that u, u^σ are linearly independent over K (normal basis). Then again, $b^\sigma = -b = a \cdot b$. This time we can be sure that b is a unit: otherwise $b = 0$ (as above) which would imply that u and u^σ are linearly dependent over K.

The converse is directly verified.

□

References

[1] E. Artin, J. Tate, *Class field theory.* Lecture Notes from the Artin-Tate seminar 1951-52, Princeton University. Reprinted by Addison-Wesley (1990) 3, 4

[2] W. Grunwald, *Ein allgemeines Existenztheorem für algebraische Zahlkörper.* Journ. f.d. reine u. angewandte Math. 169 (1933) 103–107 3

[3] H. Hasse, *Existenz und Mannigfaltigkeit abelscher Algebren mit vorgegebener Galoisgruppe über einem Teilkörper des Grundkörpers.* Math. Nachrichten 1 (1948) I: 40–61, II: 213–217, III: 277–283 7, 12

[4] H. Hasse, *Zum Existenzsatz von Grunwald in der Klassenkörpertheorie.* Journ. f.d. reine u. angewandte Math. 188 (1950) 3

[5] K. Hensel, *Zahlentheorie.* (Leipzig 1913)

[6] F. Lorenz, *Einführung in die Algebra.* Bd. I (3. Aufl. 1996), Bd. II (2. Aufl. 1997) 7, 17, 24, 25, 32, 35

[7] F. Lorenz, *Algebraische Zahlentheorie.* Heidelberg: Spektrum Akademischer Verlag (1993)

[8] H. Miki, *On Grunwald-Hasse-Wang's theorem.* Journ. Math. Soc. Japan 30 (1978) 313–325 7

[9] D. Saltman, *Generic Galois extensions, Advances in Math. 43 (1982).* 7, 11

[10] Sh. Wang, *A counter example to Grunwald's theorem.* Annals of Math. 49 (1948) 1008–1009 3

[11] Sh. Wang, *On Grunwald's theorem.* Annals of Math. 51 (1950) 471–484 3

[12] Y. Sueyoshi, *A note on Miki's generalization of the Grunwald-Hasse-Wang theorem.* Mem. Fac. Sci. Kyushu Univ. Ser.A 35 (1981) 229-234 7

[13] G. Whaples, *Non-analytic class field theory and Gruenwald's theorem.* Duke Math. J. 9 (1942) 455-473 3

[14] E. Witt, *Zyklische Körper und Algebren der Charakteristik p vom Grad p^n, Struktur diskret bewerteter Körper mit vollkommenem Restklassenkörper der Charakteristik p .* Journ. f.d. reine u. angewandte Math. 176 (1937) 126–140 25, 29