ISRAEL JOURNAL OF MATHEMATICS, Vol. 50, Nos. 1–2, 1985

KUMMER SUBFIELDS OF MALCEV–NEUMANN DIVISION ALGEBRAS

BY

J.-P. TIGNOL[a,†] AND S. A. AMITSUR[b]

[a]*Department of Mathematics, Université Catholique de Louvain, B-1348 Louvain-la-Neuve, Belgium*; and [b]*Institute of Mathematics, The Hebrew University of Jerusalem, Jerusalem 91904, Israel*

ABSTRACT

The abelian Galois subfields of Malcev–Neumann formal series division rings are determined. The results obtained in this paper lead to a lower bound for the rank of Galois splitting fields of universal division algebras.

Introduction

Malcev–Neumann rings of formal series in non-commuting variables provide an interesting class of examples of division rings: for instance, the second author has shown in [3, §2], as part of his solution of the crossed product problem that some of these rings are crossed products only of groups which are direct products of cyclic groups of prime order.

In the present paper, Neumann's definition of formal series division rings, which uses a cocycle f to twist the multiplication of indeterminates, is restricted in such a way that the resulting division rings $\mathscr{D}_f$ are finite-dimensional over their center (see §2). Under this mild restriction, we obtain in §3 a complete description of the subfields of $\mathscr{D}_f$ which are Kummer extensions of the center (i.e. abelian Galois over the center, which is assumed to contain sufficiently many roots of unity). The general results of §3 are specialized in §§4 and 5 to the case of iterated Laurent power series. We thus generalize the results of [3, §2].

In §6, we obtain some information on simultaneous crossed products. Roughly speaking, the problem we deal with can be formulated as follows: suppose a

† The research leading to this paper was begun while the first author was visiting the Hebrew University of Jerusalem, whose hospitality is gratefully acknowledged.

Received May 10, 1984

central simple algebra is a crossed product of some group G; is it then necessarily similar to a crossed product of some other group H? (Precise definitions are given in 6.1.) As an application of the preceding results, we obtain some relations on the invariant factors of abelian groups G and H for which this property holds. Previously known results on simultaneous crossed products are quoted without proof in §8.

A further application is given in §7, where a lower bound for the rank of Galois splitting fields of universal division algebras is obtained.

1. Cohomology of trivial modules and skew-symmetric forms

1.1. Let G and A be abelian groups. We shall use the additive notation for A and the multiplicative notation for G (though subsequently the results of this section will be applied in an opposite situation, where $A = K^*$ is the multiplicative group of a field and G is an additive abelian group).

A *skew-symmetric* map from $G \times G$ to A is a map

$$a : G \times G \to A$$

which is $\mathbf{Z}$-bilinear and such that $a(\sigma, \sigma) = 0$ for all $\sigma \in G$; therefore, $a(\sigma, \tau) = -a(\tau, \sigma)$ for all $\sigma, \tau \in G$. The set of all such maps is an abelian group which will be denoted by $\mathrm{Skew}(G, A)$.

1.2. Skew-symmetric maps can be constructed from 2-cocylces $f \in Z^2(G, A)$, for *the trivial action* of G on A (i.e. $\sigma(u) = u$ for all $u \in A$), as follows: recall that a map $f : G \times G \to A$ is a 2-cocycle if it satisfies the cocycle condition, which in the case of trivial action is of the form:

$$\partial f(\sigma, \tau, \rho) = f(\tau, \rho) - f(\sigma\tau, \rho) + f(\sigma, \tau\rho) - f(\sigma, \tau) = 0 \quad \text{for all } \sigma, \tau, \rho \in G;$$

for $f \in Z^2(G, A)$, we define a map $a_f : G \times G \to A$ by:

$$a_f(\sigma, \tau) = f(\sigma, \tau) - f(\tau, \sigma).$$

Clearly, $a_f(\sigma, \sigma) = 0$, but moreover, since G is abelian, a straightforward computation yields:

$$a_f(\sigma, \rho) + a_f(\tau, \rho) - a_f(\sigma\tau, \rho) = \partial f(\sigma, \tau, \rho) - \partial f(\sigma, \rho, \tau) + \partial f(\rho, \sigma, \tau) = 0,$$

which proves that a_f is $\mathbf{Z}$-bilinear; thus, $a_f \in \mathrm{Skew}(G, A)$.

If $f \in B^2(G, A)$, i.e. $f(\sigma, \tau) = g(\tau) - g(\sigma\tau) + g(\sigma)$ for some map $g : G \to A$, then it is easily seen that $a_f = 0$, whence the map $f \to a_f$ induces a homomorphism

$$\Psi : H^2(G, A) \to \mathrm{Skew}(G, A).$$

The kernel of Ψ obviously contains $H^2(G, A)_{\mathrm{sym}}$, the group of cohomology classes which are represented by symmetric cocycles, i.e. cocycles f such that $f(\sigma, \tau) = f(\tau, \sigma)$ for all $\sigma, \tau \in G$. (Note that this definition of $H^2(G, A)_{\mathrm{sym}}$ makes sense (and will be used) even if the action of G on A is not trivial. In the case of trivial action, every coboundary is symmetric, whence $H^2(G, A)_{\mathrm{sym}} = Z^2(G, A)_{\mathrm{sym}}/B^2(G, A)$.)

1.3. PROPOSITION. *If G is abelian and acts trivially on A, then there is a split exact sequence*:

$$0 \to H^2(G, A)_{\mathrm{sym}} \to H^2(G, A) \xrightarrow{\Psi} \mathrm{Skew}(G, A) \to 0.$$

PROOF. It is easy to see that the kernel of Ψ is $H^2(G, A)_{\mathrm{sym}}$. To prove the rest, we construct a splitting map $\theta : \mathrm{Skew}(G, A) \to H^2(G, A)$, as follows: Choose a basis $\sigma_1, \ldots, \sigma_r$ of G, so that $G = \langle \sigma_1 \rangle \oplus \cdots \oplus \langle \sigma_r \rangle$, and denote $\sigma^\mu = \sigma_1^{\mu_1} \cdots \sigma_r^{\mu_r}$ if $\mu = (\mu_1, \ldots, \mu_r)$. For any $a \in \mathrm{Skew}(G, A)$, define

$$\theta(a)(\sigma^\mu, \sigma^\nu) = \sum_{i>j} \mu_i \nu_j a(\sigma_i, \sigma_j).$$

A straightforward computation shows that $\theta(a)$ is well-defined and that $\theta(a) \in Z^2(G, A)$. Moreover, since a is skew and bilinear,

$$\Psi\theta(a)(\sigma^\mu, \sigma^\nu) = \sum_{i>j} \mu_i \nu_j a(\sigma_i, \sigma_j) + \sum_{i<j} \mu_i \nu_j a(\sigma_i, \sigma_j) = a(\sigma^\mu, \sigma^\nu),$$

whence $\Psi\theta = 1$.

An alternative (non-computational) proof is to use the universal coefficient theorem for cohomology (see e.g. [8, p. 77]), which provides a split exact sequence:

$$0 \to \mathrm{Ext}^1_{\mathbf{Z}}(H_1(G, \mathbf{Z}), A) \to H^2(G, A) \xrightarrow{\phi} \mathrm{Hom}(H_2(G, \mathbf{Z}), A) \to 0.$$

Since G is abelian, we have $H_1(G, \mathbf{Z}) = G$. Moreover, since the action of G on A is trivial, $\mathrm{Ext}^1_{\mathbf{Z}}(G, A)$ and $H^2(G, A)_{\mathrm{sym}}$ are naturally isomorphic, since they both classify the abelian group extensions of A by G. Therefore,

$$\mathrm{Ext}^1_{\mathbf{Z}}(H_1(G, \mathbf{Z}), A) \simeq H^2(G, A)_{\mathrm{sym}}.$$

On the other hand, by theorem 3 of [9, p. 595], there is a natural isomorphism: $H_2(G, \mathbf{Z}) \simeq G \wedge G$, where $G \wedge G$ denotes the second exterior power of G (as a $\mathbf{Z}$-module).

Clearly, $\mathrm{Hom}_{\mathbf{Z}}(G \wedge G, A) = \mathrm{Skew}(G, A)$, whence we may identify:

$$\mathrm{Hom}(H_2(G, \mathbf{Z}), A) = \mathrm{Skew}(G, A)$$

and it is easy to check that under this identification, $\phi = \Psi$.

1.4. Henceforth, we consider the case where G is a *finite* abelian group and $A = \mathbf{Q}/\mathbf{Z}$. In this case, we refer to the elements of $\mathrm{Skew}(G, \mathbf{Q}/\mathbf{Z})$ as skew-symmetric *forms*. Each such form a induces a homomorphism $\hat{a} : G \to \hat{G}$ from G to its character group $\hat{G}$, by letting $\hat{a}(\sigma)(\tau) = a(\sigma, \tau)$.

The skew symmetric form a is called *regular* if $\hat{a}$ is injective (whence also surjective, since G and $\hat{G}$ have the same order), or in other words, if $a(\sigma, \tau) = 0$ for all $\tau \in G$ implies $\sigma = 0$.

If G is a finite abelian group and a is a regular skew-symmetric form on G, the pair (G, a) is called a *symplectic* (**Z**-)*module*. The structure of symplectic modules is easily determined (see e.g. [11, §19] or [21, §4]):

THEOREM. *If (G, a) is a symplectic module, then $G = S \oplus T$, a direct sum of two isomorphic subgroups. Moreover, there is a basis $(\sigma_1, \ldots, \sigma_n)$ of S and a basis $(\tau_1, \ldots, \tau_n)$ of T such that for each i, σ_i and τ_i have the same order r_i. Furthermore, r_{i+1} divides r_i for $i = 1, \ldots, n-1$, and the form a satisfies:*

(1) $a(\sigma_i, \sigma_j) = a(\tau_i, \tau_j) = 0$ *for all* $i, j = 1, \ldots, n$.

(2) $a(\sigma_i, \tau_j) = 0$ *if* $i \neq j$.

(3) $a(\sigma_i, \tau_i) = r_i^{-1} \pmod{\mathbf{Z}}$ *for* $i = 1, \ldots, n$.

Conversely, if $r_1, \ldots, r_n$ is a sequence of integers and if

$$G = (\mathbf{Z}/r_1\mathbf{Z})^2 \times \cdots \times (\mathbf{Z}/r_n\mathbf{Z})^2,$$

then, letting $\sigma_1, \tau_1, \ldots, \sigma_n, \tau_n$ denote the standard basis of G, relations (1), (2), (3) above define a regular skew-symmetric form on G.

COROLLARY. *If (G, a) is a symplectic module, then the invariant factors of G appear in pairs: $(r_1, r_1, r_2, r_2, \ldots, r_n, r_n)$. Hence, the rank of G is even, and its order is a square: $|G| = (r_1 \cdots r_n)^2$.*

1.5. Let (G, a) be a symplectic module. For any subgroup $H \subset G$, we denote

$$H^{\perp} = \{\sigma \in G \mid a(\sigma, \tau) = 0 \text{ for all } \tau \in H\}.$$

A subgroup H is called *isotropic* if $H \subset H^{\perp}$, i.e. $a(H, H) = 0$, and it is called *Lagrangian* if it is maximal isotropic, i.e. $H = H^{\perp}$. For instance, the subgroups S and T of Theorem 1.4 are Lagrangians of (G, a).

At a later stage in this paper, we shall translate a problem of splitting fields to a problem about Lagrangians of certain symplectic modules.

To determine the Lagrangians of a given (arbitrary) symplectic module seems to be rather difficult. However, this determination is easy in two cases: when G is elementary abelian (i.e. a direct sum of cyclic groups of prime order) and when G has rank 2 (i.e. G is a direct sum of two cyclic groups).

LEMMA. *For any subgroup H of a symplectic module (G, a), we have: $G/H^{\perp} \simeq H$ (not canonically). If H is a Lagrangian, then $|G| = |H|^2$, and* $\operatorname{rk} H \leqq \operatorname{rk} G \leqq 2 \operatorname{rk} H$.

PROOF. Let $\lambda : G \to \hat{H} = \operatorname{Hom}(H, \mathbf{Q}/\mathbf{Z})$ be the composite map of $\hat{a} : G \to \hat{G}$ and of the restriction map $\rho : \hat{G} \to \hat{H}$. Since $\hat{a}$ is an isomorphism and since ρ is surjective, λ is surjective. Moreover, its kernel is $H^{\perp}$, since $\lambda(\sigma) = 0$ is equivalent to $a(\sigma, H) = 0$. Hence, λ induces an isomorphism: $G/H^{\perp} \simeq \hat{H}$. If H is a Lagrangian, then $H^{\perp} = H$ and this equality yields the rest of the lemma.

1.6. PROPOSITION. *Let (G, a) be a symplectic module. If G is an elementary abelian group of rank $2r$, then all Lagrangians of (G, a) are elementary abelian of rank r, hence isomorphic to each other.*

PROOF. This follows immediately form the fact that subgroups of elementary abelian groups are elementary abelian and from the preceding lemma.

1.7. Suppose now that $G = S \oplus T$, where $S = \langle \sigma \rangle$ and $T = \langle \tau \rangle$ are isomorphic cyclic groups of order r, and that a symplectic structure on G is defined by: $a(\sigma, \tau) = r^{-1} \pmod{\mathbf{Z}}$. (Compare 1.4.) Then we can prove:

PROPOSITION. *The Lagrangians of (G, a) are isomorphic to direct sums of cyclic groups, $\langle \mu \rangle \oplus \langle \nu \rangle$ where μ is of order s, ν of order t and $r = st$. Conversely, for every factorization $r = st$ there is a Lagrangian of this type.*

PROOF. If $r = st$, one readily verifies that $\mu = \sigma^t$ and $\nu = \tau^s$ generate a Lagrangian of the required type. The rest follows from Lemma 1.5.

2. Malcev–Neumann division rings

2.1. Let G be a finite abelian group acting on a field K by automorphisms and let $F = K^G$ be the subfield of K fixed (elementwise) by G. Note that G is not required to be a group of automorphisms of K, so that generally $[K : F]$ divides $|G|$, but $[K : F] \neq |G|$; in fact, if G acts trivially on K, then $F = K$.

Let $\varepsilon : \mathbf{Z}^n \to G$ be a surjective homomorphism of the free abelian group $\mathbf{Z}^n$

onto G (for some n). Then $\mathbf{Z}^n$ also acts on K through ε, namely: for $\alpha \in \mathbf{Z}^n$ and $a \in K$, $\alpha(a) = \varepsilon(\alpha)(a)$.

Let $f \in Z^2(G, K^*)$ be a normalized 2-cocycle, i.e. $f(1, \sigma) = f(\sigma, 1) = 1$ for all $\sigma \in G$. The inflation map induced by ε raises the cocycle f to a cocycle in $Z^2(\mathbf{Z}^n, K^*)$ which for simplicity we shall also denote by f. In other words, by definition:

$$f(\alpha, \beta) = f(\varepsilon\alpha, \varepsilon\beta) \qquad \text{for } \alpha, \beta \in \mathbf{Z}^n.$$

Given K, G, f and ε as above, we construct the Malcev–Neumann ring of formal series $\mathcal{D}(K, G, f, \varepsilon)$ as follows: its elements are the formal series

$$s = \sum_{\alpha \in \mathbf{Z}^n} a_\alpha z_\alpha \qquad (a_\alpha \in K)$$

whose support $\operatorname{supp}(s) = \{\alpha \in \mathbf{Z}^n \mid a_\alpha \neq 0\}$ is a well-ordered subset of $\mathbf{Z}^n$ for the anti-lexicographic ordering, i.e. the ordering for which the positive elements are the n-tuples $(\alpha_1, \ldots, \alpha_n)$ such that, for some i, $\alpha_i > 0$ and $\alpha_j = 0$ for $j > i$.

Addition in $\mathcal{D}(K, G, f, \varepsilon)$ has the usual meaning, and multiplication is defined by the relations:

$$z_\alpha a = \alpha(a) z_\alpha \qquad \text{for } a \in K \text{ and } \alpha \in \mathbf{Z}^n, \tag{2.1.1}$$

$$z_\alpha z_\beta = f(\alpha, \beta) z_{\alpha+\beta} \qquad \text{for } \alpha, \beta \in \mathbf{Z}^n. \tag{2.1.2}$$

The multiplication is associative since $f \in Z^2(\mathbf{Z}^n, K^*)$ and its unit is z_0 since f is normalized. We shall identify z_0 with $1 \in K$ and $az_0 \in \mathcal{D}(K, G, f, \varepsilon)$ with $a \in K$. It is well-known that $\mathcal{D}(K, G, f, \varepsilon)$ is a division ring [10, Theorem 5.7].

2.2. REMARK. In [10, §5], B.H. Neumann considered a more general construction, using an arbitrary cocycle $f \in Z^2(\mathbf{Z}^n, K^*)$. In the present paper, we consider only cocycles which arise by inflation from $Z^2(G, K^*)$, in order to obtain finite-dimensional central division algebras: see 2.5 below.

Although the following observation is not used in the present paper, it is worth noting that Neumann's construction only depends on the cohomology class of the cocycle f in $H^2(\mathbf{Z}^n, K^*)$. Therefore, the ring $\mathcal{D}(K, G, f, \varepsilon)$ only depends, up to isomorphism, on the image of $f \in Z^2(G, K^*)$ in $H^2(G, K^*)/H^2(G, K^*)_{\text{sym}}$, since we have the following result:

PROPOSITION. *The following sequence is exact*:

$$1 \to H^2(G, K^*)_{\text{sym}} \to H^2(G, K^*) \xrightarrow{\text{inf}} H^2(\mathbf{Z}^n, K^*).$$

A proof is given in the appendix.

2.3. The division ring $\mathcal{D}(K, G, f, \varepsilon)$ can also be considered as an iterated Laurent series ring in the indeterminates $z_i = z_{\beta_i}$, where β_i is the i-th element of the standard basis of $\mathbf{Z}^n$. Indeed, if $\alpha = (\alpha_1, \ldots, \alpha_n) = \Sigma \alpha_i \beta_i$, we get

$$z_\alpha = k_\alpha z_1^{\alpha_1} z_2^{\alpha_2} \cdots z_n^{\alpha_n} \tag{2.3.1}$$

for some $k_\alpha \in K^*$, and we have the following relations:

$$z_i a = \beta_i(a) z_i \quad \text{for } a \in K^* \quad \text{and} \quad z_i z_j = u_{ij} z_j z_i \tag{2.3.2}$$

where $u_{ij} = f(\beta_i, \beta_j) f(\beta_j, \beta_i)^{-1}$.

An iterated Laurent power series ring $K((z_1, \ldots, z_n))$ can be constructed by induction using these relations; namely,

$$K((z_1, \ldots, z_j)) = K((z_1, \ldots, z_{j-1}))((z_j)), \qquad j = 1, 2, \ldots, n$$

is a Laurent power series ring in the indeterminate z_j with coefficients in $K((z_1, \ldots, z_{j-1}))$, in which the commutation relations of z_j with the coefficients are derived from (2.3.2). By a proper identification, we actually have:

PROPOSITION. $\mathcal{D}(K, G, f, \varepsilon) = K((z_1, \ldots, z_n))$.

PROOF. One readily observes that the support of an element of $K((z_1, \ldots, z_n))$ is well-ordered, so that one can consider

$$K((z_1, \ldots, z_n)) \subseteq \mathcal{D}(K, G, f, \varepsilon).$$

The inclusion in the other direction follows from the fact that if $s = \Sigma a_\alpha z_\alpha \in \mathcal{D}(K, G, f, \varepsilon)$, then $s = \Sigma a_\alpha k_\alpha z_1^{\alpha_1} \cdots z_n^{\alpha_n}$ by (2.3.1) and since the support of s is well ordered:

$$s = \sum_{\alpha_n \geqq m_n} (\Sigma a_\alpha k_\alpha z_1^{\alpha_1} \cdots z_{n-1}^{\alpha_{n-1}}) z_n^{\alpha_n}$$

for some $m_n \in \mathbf{Z}$. A simple induction argument completes the proof.

2.4. To simplify notations, we denote $\mathcal{D}(K, G, f, \varepsilon) = \mathcal{D}_f$. We now determine the center $\mathcal{C}_f$ of $\mathcal{D}_f$ and the rank $[\mathcal{D}_f : \mathcal{C}_f]$.

With the aid of the cocycle f, we distinguish a subset $\Gamma_f \subset \mathbf{Z}^n$: it is the set of all $\gamma \in \mathbf{Z}^n$ with the following properties:

(a) $\gamma(a) = a$ for all $a \in K$,

(b) there exists $d_\gamma \in K^*$ such that for all $\beta \in \mathbf{Z}^n$ the following relation holds:

$$f(\beta, \gamma) f(\gamma, \beta)^{-1} = d_\gamma \beta(d_\gamma)^{-1}. \tag{2.4.1}$$

REMARKS. (1) If an element d_γ as in (b) exists, then it is uniquely determined up to multiplication by a non-zero element in the fixed field F. Indeed, if for

every $\beta \in \mathbf{Z}^n$, $d_\gamma \beta(d_\gamma)^{-1} = d'_\gamma \beta(d'_\gamma)^{-1}$, then $d'_\gamma d_\gamma^{-1} \in F^*$, whence $d'_\gamma = d_\gamma \cdot c$ for some $c \in F^*$.

(2) We have $\Gamma_f \supseteq \operatorname{Ker} \varepsilon$, since if $\gamma \in \operatorname{Ker} \varepsilon$, then (a) clearly holds (by definition of the action of $\mathbf{Z}^n$ on K), and we can choose $d_\gamma = 1$, since $f(\beta, \gamma) = f(\gamma, \beta) = 1$ for all $\beta \in \mathbf{Z}^n$.

The following proposition provides a description of the center $\mathscr{C}_f$ of $\mathscr{D}_f$:

PROPOSITION. *$\mathscr{C}_f$ is the set of all elements of $\mathscr{D}_f$ of the form*:

$$\sum_{\gamma \in \Gamma_f} c_\gamma (d_\gamma z_\gamma)$$

with arbitrary $c_\gamma \in F = K^G$.

PROOF. Let $s = \sum_{\alpha \in \mathbf{Z}^n} a_\alpha z^\alpha$. The relation $sa = as$ for all $a \in K$ is equivalent to: $\alpha(a) = a$ for all $\alpha \in \operatorname{supp}(s)$ and the condition that $sz_\beta = z_\beta s$ is equivalent to the requirement that $a_\alpha z_\alpha z_\beta = z_\beta a_\alpha z_\alpha$, which amounts to:

$$a_\alpha f(\alpha, \beta) = \beta(a_\alpha) f(\beta, \alpha).$$

Therefore, $s \in \mathscr{C}_f$ and only if $\operatorname{supp}(s) \subset \Gamma_f$ and for $\alpha \in \operatorname{supp}(s)$, the corresponding coefficient a_α satisfies (2.4.1). By Remark (1) above, a_α is then of the form: $a_\alpha = c_\alpha . d_\alpha$ for some $c_\alpha \in F^*$; whence $s \in \mathscr{C}_f$ if and only if

$$s = \sum_{\gamma \in \Gamma_f} c_\gamma (d_\gamma z_\gamma)$$

for some $c_\gamma \in F$.

2.5. THEOREM. *Γ_f is a subgroup of finite index in $\mathbf{Z}^n$ and*

$$[\mathscr{D}_f : \mathscr{C}_f] = (\mathbf{Z}^n : \Gamma_f) . [K : F].$$

PROOF. If $\gamma, \gamma' \in \Gamma_f$, then $d_\gamma z_\gamma$ and $d_{\gamma'} z_{\gamma'}$ are in $\mathscr{C}_f$, whence $(d_\gamma z_\gamma)(d_{\gamma'} z_{\gamma'})^{-1} \in \mathscr{C}_f$. since $(d_\gamma z_\gamma)(d_{\gamma'} z_{\gamma'})^{-1} = d_{\gamma - \gamma'} z_{\gamma - \gamma'}$ for some $d_{\gamma - \gamma'} \in K^*$, it follows from the preceding proposition that $\gamma - \gamma' \in \Gamma_f$, whence Γ_f is a subgroup of $\mathbf{Z}^n$. Since $\operatorname{Ker} \varepsilon \subseteq \Gamma_f$ by Remark (2) of (2.4) and since $(\mathbf{Z}^n : \operatorname{Ker} \varepsilon) = |G|$ is finite, the index of Γ_f in $\mathbf{Z}^n$ is finite. The rest of the theorem is an easy consequence of the description of $\mathscr{C}_f$ in Proposition 2.4: indeed, if $\{k_i\}$ is an F-basis of K and if $\{\alpha_j\}$ is a set of representatives of the cosets of Γ_f in $\mathbf{Z}^n$, then the set $\{k_i z_{\alpha_j}\}$ is a $\mathscr{C}_f$-basis of $\mathscr{D}_f$.

2.6. Recall that the *degree* of a finite-dimensional central division algebra is defined as the square root of its dimension. The previous theorem yields the following result on the degree of $\mathscr{D}_f$ (denoted by $\deg \mathscr{D}_f$):

COROLLARY. $\deg \mathscr{D}_f$ *divides* $|G|$.

PROOF. In (2.1), we already observed that $[K:F]$ divides $|G|$. Since on the other hand $(\mathbf{Z}^n:\Gamma_f)$ divides $(\mathbf{Z}^n:\operatorname{Ker}\varepsilon)=|G|$, Theorem 2.5 shows that $[\mathscr{D}_f:\mathscr{C}_f]$ divides $|G|^2$, whence $\deg \mathscr{D}_f$ divides $|G|$.

2.7. The most powerful tool for investigating the division ring $\mathscr{D}_f$ is the map

$$v:\mathscr{D}_f^*\to\mathbf{Z}^n$$

defined by:

$$v(s)=\min(\operatorname{supp}(s)),$$

i.e. $v(s)$ is the minimal α for which z_α has a non-zero coefficient. Clearly, v is a valuation on $\mathscr{D}_f$ with value group $\mathbf{Z}^n$ and residue field $\bar{\mathscr{D}}_f=K$; its restriction to $\mathscr{C}_f$ is a valuation with value group Γ_f and residue field $\bar{\mathscr{D}}_f=F$, by Proposition 2.4. The division ring $\mathscr{D}_f$ is *strongly maximal* with respect to v, in the terminology of [17, p. 54], i.e. every pseudo-convergent sequence in $\mathscr{D}_f$ has a pseudo-limit in $\mathscr{D}_f$. In [12, p. 103], this is shown for $f=1$ and with trivial action of G on K (i.e. for $\mathscr{D}_f$ commutative), but the proof carries over readily to our case. Similarly, $\mathscr{C}_f$ is strongly maximal, whence maximally complete by [17, Theorem 8, p. 51], whence also Henselian, which means that the valuation v on $\mathscr{C}_f$ has a unique prolongation to any algebraic extension of $\mathscr{C}_f$ [17, Theorem 10. p. 54]. If L is such an extension, we denote by $U_1(L)$ the multiplicative group of all 1-units in L, i.e. integral elements of L which are mapped onto 1 in the residue field $\bar{L}$. From the fact that L is Henselian, the following useful result is easily derived:

2.8. PROPOSITION. *If n is any integer which is not divisible by the characteristic of L, then the group $U_1(L)$ is uniquely divisible by n.*

PROOF. If $u\in U_1(L)$, then equation $X^n-u=0$ has a unique solution $x\in L$ such that $\bar{x}=1$ in $\bar{L}$, by [17, Lemma 1, p. 60], since the characteristic of $\bar{L}$ (which in this case is equal to the characteristic of L) does not divide n.

3. The Kummer subfields of $\mathscr{D}_f$

3.1. Our aim in this section is to determine the subfields of $\mathscr{D}_f$ which are Kummer extensions of $\mathscr{C}_f$. We shall obtain a complete description in the case where $\Gamma_f=\operatorname{Ker}\varepsilon$: this hypothesis holds, for instance, if G is the Galois group of K/F, i.e. if G acts faithfully on K.

Recall that a finite abelian Galois extension L/C is a *Kummer extension* if C contains a primitive m-th root of unity, where m is the exponent of the Galois

group $\mathrm{Gal}(L/C)$. Note that this requires that the characteristic of C does not divide the rank of L over C. We introduce the notations:

$$\mathrm{KUM}(L/C) = \{x \in L^* \mid x^m \in C\} \quad \text{and} \quad \mathrm{kum}(L/C) = \mathrm{KUM}(L/C)/C^*,$$

i.e. $\mathrm{kum}(L/C)$ is the factor group of $\mathrm{KUM}(L/C)$ modulo C^*.

The group $\mathrm{kum}(L/C)$ is dual to $\mathrm{Gal}(L/C)$ by the bilinear pairing:

$$\langle \sigma, \bar{a} \rangle = \sigma(a)a^{-1},$$

whence $\mathrm{kum}(L/C) \simeq \mathrm{Gal}(L/C)$ (not canonically). For details on Kummer theory, see e.g. [7, §8.9].

3.2. In a division algebra D with center C, any subfield which is a Kummer extension of C will be referred to as a *Kummer subfield* of D. These subfields can be constructed in the following way:

Assume C contains a primitive m-th root of unity for some $m \geqq 1$ and let A be a finite abelian subgroup of exponent m of the factor group D^*/C^*. For each $a \in A$, choose a representative $x_a \in D^*$ and consider the C-spaces

$$C(A) = \sum_{a \in A} Cx_a$$

which is clearly independent of the choice of representatives x_a. One easily verifies:

LEMMA. *If the elements x_a commute pairwise, then $C(A)$ is a Kummer subfield of D, and* $\mathrm{kum}(C(A)/C) = A$.

3.3. In our original division algebra $\mathscr{D}_f$, we consider the set $\mathscr{M}_f$ of all monomials, that is:

$$\mathscr{M}_f = \{az_\alpha \mid \alpha \in \mathbf{Z}^n, a \in K^*\}.$$

For any $s = \Sigma a_\alpha z_\alpha \in \mathscr{D}_f$, we denote by $\mu(s)$ the leading monomial, i.e.:

$$\mu(s) = a_{v(s)}z_{v(s)}.$$

A very simple and useful information is the fact that $\mu : \mathscr{D}_f^* \to \mathscr{M}_f$ is a homomorphism; hence if $s, t \in \mathscr{D}_f^*$ commute, then $\mu(s)$ and $\mu(t)$ also commute. This enables us to show:

3.4. PROPOSITION. *Every Kummer subfield L of $\mathscr{D}_f$ is conjugate to a Kummer subfield L' which has the property that* $\mathrm{kum}(L'/\mathscr{C}_f)$ *is represented by monomials of $\mathscr{M}_f$.*

PROOF. Let $\{a_i\}$ be a set of representatives in L of the elements of $\mathrm{kum}(L/\mathscr{C}_f)$, and let $L' = \Sigma C_f \mu(a_i)$. By (3.2), it follows that L' is a Kummer subfield of $\mathscr{D}_f$ and $\mathrm{kum}(L'/\mathscr{C}_f)$ has the monomials $\mu(a_i)$ as a set of representatives in L'^*.

Let m be the exponent of $\mathrm{Gal}(L/\mathscr{C}_f)$ and let $a_i^m = c_i \in \mathscr{C}_f^*$; then

$$L = \mathscr{C}_f(\{c_i^{1/m}\}) \quad \text{and} \quad L' = \mathscr{C}_f(\{\mu(c_i)^{1/m}\}).$$

As $\mu(c_i)c_i^{-1}$ is a 1-unit in $\mathscr{C}_f$, we have $\mu(c_i)c_i^{-1} \in \mathscr{C}_f^{*m}$ by Proposition 2.8, whence $\mu(c_i) \equiv c_i \bmod \mathscr{C}_f^{*m}$. It then follows from [7, p. 497] that L and L' are $\mathscr{C}_f$-isomorphic, whence also conjugate in $\mathscr{D}_f$, by the Skolem–Noether theorem.

3.5. Given a Kummer subfield L in $\mathscr{D}_f$, let $\bar{L}$ be its residue field and let $S_L = \varepsilon v(L)$ be the image of the value group $v(L)$ in G. We also note that $F \subseteq \bar{L} \subseteq K$ since $K = \bar{\mathscr{D}}_f$ and $F = \bar{\mathscr{C}}_f$.

LEMMA *The field $\bar{L}$ is a Kummer extension of F and S_L acts trivially on $\bar{L}$.*

PROOF. First, we show that S_L acts trivially on $\bar{L}$. Let $\sigma \in S_L = \varepsilon v(L)$ and $a \in \bar{L}$; then there exists two elements $s_a, x_\sigma \in L$ such that $\varepsilon v(x_\sigma) = \sigma$ and $\mu(s_a) = a$. Since multiplication in L is commutative and since μ is a homomorphism, we have

$$a \,.\, \mu(x_\sigma) = \mu(s_a) \,.\, \mu(x_\sigma) = \mu(x_\sigma) \,.\, \mu(s_a) = \mu(x_\sigma) \,.\, a.$$

On the other hand, since $\mu(x_\sigma) = b \,.\, z_{v(\sigma)}$ for some $b \in K^*$ and since $\varepsilon v(x_\sigma) = \sigma$, relation (2.1.1) (defining multiplication in $\mathscr{D}_f^*$) shows that

$$\mu(x_\sigma)a = \sigma(a)\mu(x_\sigma).$$

Therefore, $\sigma(a) = a$, as required.

Next, let L_T be the inertia subfield of $L/\mathscr{C}_f$, i.e. the maximal unramified extension of $\mathscr{C}_f$ contained in L. Since $L/\mathscr{C}_f$ is Galois, the residue field $\bar{L}$ is Galois over F and $\mathrm{Gal}(\bar{L}/F)$ is canonically isomorphic to $\mathrm{Gal}(L_T/\mathscr{C}_f)$: see, e.g. [17, Theorem 1, p. 62]. Therefore, $\bar{L}/F$ is an abelian Galois extension. Moreover, since $\mathscr{C}_f$ contains a primitive m-th root of unity, where $m = \exp(\mathrm{Gal}(L/\mathscr{C}_f))$, its residue field F also contains a primitive m-th root of unity, whence $\bar{L}/F$ is a Kummer extension.

3.6. *From now on, we assume* $\Gamma_f = \mathrm{Ker}\,\varepsilon$. Under this restriction, we prove:

PROPOSITION. *Let L be a Kummer subfield of $\mathscr{D}_f$ and S_L its corresponding subgroup of G. There is a short exact sequence*:

$$s_L : 1 \to \mathrm{kum}(\bar{L}/F) \to \mathrm{kum}(L/\mathscr{C}_f) \xrightarrow{\varepsilon v} S_L \to 1$$

and since $\mathrm{kum}(L/\mathscr{C}_f)$ *is an abelian group, we have* $s_L \in H^2(S_L, \mathrm{kum}(\bar{L}/F))_{\mathrm{sym}}$.

PROOF. Let L_T be the inertia subfield of $L/\mathscr{C}_f$ as before, and consider the short exact sequence:

$$1 \to \mathrm{Gal}(L/L_T) \to \mathrm{Gal}(L/\mathscr{C}_f) \to \mathrm{Gal}(L_T/\mathscr{C}_f) \to 1.$$

By duality between Galois groups and Kummer groups, we get:

$$1 \to \mathrm{kum}(L_T/\mathscr{C}_f) \to \mathrm{kum}(L/\mathscr{C}_f) \to \mathrm{kum}(L/L_T) \to 1. \tag{3.6.1}$$

In order to obtain the exact sequence s_L from the sequence above, we note first that the canonical isomorphism $\mathrm{Gal}(L_T/\mathscr{C}_f) \simeq \mathrm{Gal}(\bar{L}/F)$ for inertial extensions (see [17, Theorem 1, p. 62]) yields a canonical isomorphism: $\mathrm{kum}(L_T/\mathscr{C}_f) \simeq \mathrm{kum}(\bar{L}/F)$. On the other edge of (3.6.1), we have to show: $\mathrm{kum}(L/L_T) \simeq S_L$.

Since $\mathrm{kum}(L/L_T) \subset L^*/L_T^*$, we may consider the map induced by v:

$$v : \mathrm{kum}(L/L_T) \to v(L)/v(L_T). \tag{3.6.2}$$

Since $L_T/\mathscr{C}_f$ is unramified, we have $v(L_T) = \Gamma_f = \mathrm{Ker}\,\varepsilon$, whence we get a homomorphism:

$$\varepsilon v : \mathrm{kum}(L/L_T) \to S_L.$$

To complete the proof, we show that this map is an isomorphism or, equivalently, that the map v in (3.6.2) is 1–1.

Denote by $U(L)$ the group of all units in L and by $U_1(L)$ the group of 1-units. We have exact sequences of natural maps:

$$1 \to U(L) \to L^* \to v(L) \to 0, \tag{3.6.3}$$

$$1 \to U_1(L) \to U(L) \to \bar{L}^* \to 1. \tag{3.6.4}$$

Comparing the sequence (3.6.4) with a similar exact sequence with L_T instead of L, and taking into account the fact that $\bar{L}_T = \bar{L}$, we get an isomorphism:

$$U(L)/U(L_T) \simeq U_1(L)/U_1(L_T)$$

which shows, by Proposition 2.8, that the group $U(L)/U(L_T)$ is uniquely divisible by the exponent of $\mathrm{Gal}(L/L_T)$, which we denote by e.

Next, consider the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 1 & \to & U(L)/U(L_T) & \to & L^*/L_T^* & \to & v(L)/v(L_T) & \to & 0 \\ & & \downarrow e & & \downarrow e & & \downarrow e & & \\ 1 & \to & U(L)/U(L_T) & \to & L^*/L_T^* & \to & v(L)/v(L_T) & \to & 0 \end{array}$$

in which the vertical maps send each element onto its e-th power and the rows are obtained from (3.6.3). Since $v(L)/v(L_T)$ is killed by e, by [17, Theorem 5, p. 66] and since $U(L)/U(L_T)$ is uniquely divisible by e, the snake lemma shows that the e-torsion part of L^*/L_T^* is isomorphic to $v(L)/v(L_T)$ under an isomorphism induced by v. This shows that (3.6.2) is an isomorphism, since the e-torsion part of L^*/L_T^* is $\mathrm{kum}(L/L_T)$.

Now, the short exact sequence s_L is an element of $H^2(S_L, \mathrm{kum}(\bar{L}/F))$, as a group extension, with S_L acting trivially on $\mathrm{kum}(\bar{L}/F)$, by Lemma 3.5. Since $\mathrm{kum}(L/\mathscr{C}_f)$ is an abelian group, it follows easily that s_L is represented by symmetric cocycles, whence $s_L \in H^2(S_L, \mathrm{kum}(\bar{L}/F))_{\mathrm{sym}}$.

3.7. COROLLARY. *For any Kummer subfield L of $\mathscr{D}_f$,*

$$[L : \mathscr{C}_f] = |S_L| \cdot [\bar{L} : F].$$

3.8. Next we show that the field $\bar{L}$, the group S_L and the cocycle s_L which are associated to the Kummer subfield L are all invariant under conjugacy:

PROPOSITION. *If L and L' are two conjugate Kummer subfields of $\mathscr{D}_f$, then $\bar{L}' = \bar{L}$, $S_{L'} = S_L$ and every $\mathscr{C}_f$-isomorphism $\varphi : L \to L'$ induces an isomorphism $\varphi_* : \mathrm{kum}(L/\mathscr{C}_f) \to \mathrm{kum}(L'/\mathscr{C}_f)$ such that the following diagram is commutative:*

$$\begin{array}{ccccccccc} s_L : 1 & \to & \mathrm{kum}(\bar{L}/F) & \to & \mathrm{kum}(L/\mathscr{C}_f) & \to & S_L & \to & 1 \\ & & \| & & \downarrow \varphi^* & & \| & & \\ s_{L'} : 1 & \to & \mathrm{kum}(\bar{L}'/F) & \to & \mathrm{kum}(L'/\mathscr{C}_f) & \to & S_{L'} & \to & 1 \end{array}$$

which means that $s_L = s_{L'}$ in $H^2(S_L, \mathrm{kum}(\bar{L}/F))_{\mathrm{sym}}$.

PROOF. Let $\varphi : L \to L'$ be a $\mathscr{C}_f$-isomorphism. By the Skolem–Noether theorem, there exists $a \in \mathscr{D}_f^*$ such that $\varphi(x) = axa^{-1}$ for all $x \in L$, whence $v(\varphi(x)) = v(a) + v(x) - v(a)$, and

$$v(\varphi(x)) = v(x) \quad \text{for } x \in L. \tag{3.8.1}$$

This already proves $v(L) = v(L')$, whence $S_L = S_{L'}$.

Moreover, relation (3.8.1) also shows that φ induces an F-isomorphism $\bar{\varphi} : \bar{L} \to \bar{L}'$. Since $\bar{L}$ and $\bar{L}'$ are Galois over F and are both contained in K, we must have $\bar{L} = \bar{L}'$.

Finally, it is easy to see that the induced automorphism $\bar{\varphi}_*$ of $\mathrm{kum}(\bar{L}/F)$ is the identity, since if $x \in \mathrm{KUM}(\bar{L}/F)$, then $\bar{\varphi}(x) = \zeta x$ for some root of unity $\zeta \in F$. The rest of the proposition follows easily from this observation.

3.9. The results obtained so far are valid for the Kummer subfields of all the division rings $\mathcal{D}_f = \mathcal{D}(K, G, f, \varepsilon)$ which are defined with the same K, G and ε, since no reference to the cocycle f was made. In the rest of this section, we obtain necessary and sufficient conditions for the cocycle s_L to belong to a Kummer subfield of $\mathcal{D}_f$. To this end, we relate the cocycles f and s_L with the aid of the following diagram:

$$\begin{array}{ccc} Z^2(S_L, \mathrm{KUM}(\bar{L}/F))_{\mathrm{sym}} & \xrightarrow{i_*} & H^2(S_L, K^*) \\ \downarrow{\scriptstyle e_*} & & \uparrow{\scriptstyle \mathrm{res}^G_{S_L}} \\ H^2(S_L, \mathrm{kum}(\bar{L}/F))_{\mathrm{sym}} & & H^2(G, K^*) \end{array}$$

The horizontal map i_* is induced by the inclusion $i : \mathrm{KUM}(\bar{L}/F) \hookrightarrow K^*$, the left vertical map e_* is induced by the map $e : \mathrm{KUM}(\bar{L}/F) \to \mathrm{kum}(\bar{L}/F)$, which is the reduction modulo F^* and the right vertical map is the restriction from G to S_L.

The class of the cocycle f defining $\mathcal{D}_f$ lies in the lower right hand corner, i.e. in $H^2(G, K^*)$, while s_L appears in the lower left hand corner in $H^2(S_L, \mathrm{kum}(\bar{L}/F))_{\mathrm{sym}}$. Their relation is given in the following main result:

3.10. THEOREM. *If L is a Kummer subfield of $\mathcal{D}_f$, then there exists a cocycle $h \in Z^2(S_L, \mathrm{KUM}(\bar{L}/F))_{\mathrm{sym}}$ such that:*

(1) $i_*(h) = \mathrm{res}^G_{S_L}(f)$, *and*

(2) $e_*(h) = s_L$.

It is interesting that the converse also holds if F contains sufficiently many roots of unity (e.g. a primitive $|G|$-th root of unity: see 3.14 below). More precisely:

3.11. THEOREM. *Let $\bar{L}$ be a Kummer extension of F in K and let $S \subset G$ be a subgroup of G acting trivially on $\bar{L}$. If there exists a cocycle $h \in Z^2(S, \mathrm{KUM}(\bar{L}/F))_{\mathrm{sym}}$ such that $i_*(h) = \mathrm{res}^G_S(f)$, then there exists a Kummer subfield L in $\mathcal{D}_f$ such that:*

(1) *$\bar{L}$ is the residue field of L,*

(2) *$S = \varepsilon v(L)$ $(= S_L)$,*

(3) *The cohomology class s_L of* (3.6) *satisfies: $s_L = e_*(h)$, provided F contains sufficiently many roots of unity.*

We shall prove both theorems along similar lines and we start with the first theorem:

3.12. PROOF OF THEOREM 3.10. In this case the field L is given, but since our objects are invariant under conjugation, by Proposition 3.8, we may assume in view of Proposition 3.4 that $\mathrm{kum}(L/\mathscr{C}_f)$ is represented by monomials. Hence, for every $\sigma \in S_L$ we can choose a monomial $y_\sigma \in L$ whose class $\bar{y}_\sigma \in \mathrm{kum}(L/\mathscr{C}_f)$ satisfies:

$$\varepsilon v(\bar{y}_\sigma) = \sigma.$$

Let

$$y_\sigma = a_\sigma z_{\rho(\sigma)},$$

where $a_\sigma \in K^*$ and $\rho(\sigma) \in \mathbf{Z}^n$ is such that $\varepsilon\rho(\sigma) = \sigma$.

Computing $y_\sigma y_\tau$ we obtain:

$$\begin{aligned} y_\sigma y_\tau &= a_\sigma \sigma(a_\tau) z_{\rho(\sigma)} z_{\rho(\tau)} \\ &= a_\sigma \sigma(a_\tau) f(\sigma, \tau) z_{\rho(\sigma)+\rho(\tau)} \\ &= a_\sigma \sigma(a_\tau) a_{\sigma\tau}^{-1} f(\sigma, \tau) y_{\sigma\tau} [z_{\rho(\sigma\tau)}^{-1} z_{\rho(\sigma)+\rho(\tau)}]. \end{aligned}$$

To compute the last factor, we note that

$$z_{\rho(\sigma\tau)} \cdot z_{\rho(\sigma)-\rho(\sigma\tau)+\rho(\tau)} = f(\rho(\sigma\tau), \rho(\sigma) - \rho(\sigma\tau) + \rho(\tau)) z_{\rho(\sigma)+\rho(\tau)}.$$

Since $\rho(\sigma) - \rho(\sigma\tau) + \rho(\tau) \in \mathrm{Ker}\,\varepsilon$, and since f is normalized, it follows that

$$z_{\rho(\sigma\tau)}^{-1} \cdot z_{\rho(\sigma)+\rho(\tau)} = z_{\rho(\sigma)-\rho(\sigma\tau)+\rho(\tau)}.$$

From the fact that $\rho(\sigma) - \rho(\sigma\tau) + \rho(\tau) \in \mathrm{Ker}\,\varepsilon = \Gamma_f$, it also follows that $z_{\rho(\sigma)-\rho(\sigma\tau)+\rho(\tau)} \in \mathscr{C}_f^*$, by (2, 4). Denote:

$$c(\sigma, \tau) = z_{\rho(\sigma)-\rho(\sigma\tau)+\rho(\tau)} \in \mathscr{C}_f^*;$$

hence we obtain:

$$y_\sigma y_\tau = h(\sigma, \tau) c(\sigma, \tau) y_{\sigma\tau}, \tag{3.12.1}$$

where

$$h(\sigma, \tau) = a_\sigma \sigma(a_\tau) a_{\sigma\tau}^{-1} f(\sigma, \tau).$$

Our final step is to show that the cocycle h satisfies the conditions of (3.10).

First, since y_σ and y_τ commute (for they belong to L) and since clearly $c(\sigma, \tau) = c(\tau, \sigma)$, it follows from (3.12.1) that $h(\sigma, \tau) = h(\tau, \sigma)$, whence

$h \in Z^2(S, K^*)_{\mathrm{sym}}$. Also, by definition of h, it is clear that h is cohomologous to the restriction of f from G to S_L, which proves (1) of (3.10). To prove the rest, we consider relation (3.12.1) modulo $\mathscr{C}_f^*$:

$$\bar{y}_\sigma \bar{y}_\tau = e(h(\sigma, \tau))\bar{y}_{\sigma\tau},$$

where $e : K^* \to K^*/F^*$ is the canonical map. Since $\{\gamma_\sigma\}$ is a set of representatives of S_L in $\mathrm{kum}(L/\mathscr{C}_f)$, this relation shows that $e(h(\sigma, \tau)) \in \mathrm{kum}(\bar{L}/F)$ and that the cocyle $e_*(h)$ represents the group extension s_L of (3.6). Therefore, $h(\sigma, \tau) \in \mathrm{KUM}(\bar{L}/F)$ and $e_*(h) = s_L$, which concludes the proof.

3.13. Proof of Theorem 3.11. We start with a field $\bar{L} \subseteq K$, a group S acting trivially on $\bar{L}$ and a cocycle $h \in Z^2(S, \mathrm{KUM}(\bar{L}/F))_{\mathrm{sym}}$ such that $i_*(h) = \mathrm{res}_S^G(f)$. This last condition implies that there exists $\{a_\sigma\}_{\sigma \in G} \subset K^*$ such that for all $\sigma, \tau \in S$:

$$h(\sigma, \tau) = a_\sigma \sigma(a_\tau) a_{\sigma\tau}^{-1} f(\sigma, \tau).$$

For each $\sigma \in S$, we choose an element $\rho(\sigma) \in \mathbf{Z}^n$ such that $\varepsilon\rho(\sigma) = \sigma$ and we define:

$$y_\sigma = a_\sigma z_{\rho(\sigma)} \in \mathscr{M}_f \quad \text{and} \quad c(\sigma, \tau) = z_{\rho(\sigma)-\rho(\sigma\tau)+\rho(\tau)} \in \mathscr{C}_f^*.$$

As before, a straightforward computation yields:

$$y_\sigma y_\tau = h(\sigma, \tau) c(\sigma, \tau) y_{\sigma\tau}.$$

Since h and c are symmetric and since S is abelian, it follows immediately that $y_\sigma y_\tau = y_\tau y_\sigma$ for all $\sigma, \tau \in S$. Let $\bar{y}_\sigma = y_\sigma \mathscr{C}_f^* \in \mathscr{D}_f^*/\mathscr{C}_f^*$; since $c(\sigma, \tau) \in \mathscr{C}_f^*$, we obtain:

$$\bar{y}_\sigma . \bar{y}_\tau = e(h(\sigma, \tau))\bar{y}_{\sigma\tau},$$

where $e : K^* \to K^*/F^*$ is the canonical map. Hence, the subgroup $A \subset \mathscr{D}_f^*/\mathscr{C}_f^*$ generated by $\mathrm{kum}(\bar{L}/F)$ and the set $\{\bar{y}_\sigma\}$ is an extension of $\mathrm{kum}(\bar{L}/F)$ by S, with cocycle $e_*(h) \in Z^2(S, \mathrm{kum}(\bar{L}/F))$: The following sequence

$$1 \longrightarrow \mathrm{kum}(\bar{L}/F) \longrightarrow A \xrightarrow{\varepsilon v} S \longrightarrow 1$$

is exact.

At this stage we introduce the hypothesis that F contains a primitive m-th root of unity, where m is the exponent of A; then by Lemma 3.2 the algebra $L = \mathscr{C}_f(A)$ is a Kummer subfield of $\mathscr{D}_f$ such that $\mathrm{kum}(L/\mathscr{C}_f) = A$, whence $[L : \mathscr{C}_f] = |A| = |S| . [\bar{L} : F]$.

Since the residue field of L obviously contains $\bar{L}$ and since $\varepsilon v(L)$ clearly contains S, it follows from the last relations and from Corollary 3.7 that $\bar{L}$ is the residue field of L and that $\varepsilon v(L) = S$, which completes the proof.

3.14. REMARK. In the proof of the preceding theorem, we have constructed a finite abelian subgroup $A \subset \mathscr{D}_f^*/\mathscr{C}_f^*$ and we needed a primitive m-th root of unity, where m is the exponent of A. Since A turns out to be $\mathrm{kum}(L/\mathscr{C}_f)$, the integer m is also the exponent of the Kummer subfield constructed. This exponent obviously divides the rank $[L : \mathscr{C}_f]$ which divides the degree of $\mathscr{D}_f$; moreover, $\deg \mathscr{D}_f$ divides $|G|$, by Corollary 2.6. Hence, a primitive $|G|$-th root of unity in F is sufficient in all cases.

4. The case of trivial action

4.1. In this section, we consider the extreme case where the group G acts *trivially* on the field K. As in (1.2), we correspond to the cocycle $f \in Z^2(G, K^*)$ a skew-symmetric map $a_f : G \times G \to K^*$ by setting:

$$a_f(\sigma, \tau) = f(\sigma, \tau) f(\tau, \sigma)^{-1} \qquad \text{for all } \sigma, \tau \in G.$$

PROPOSITION. *Let m be the exponent of G. The cocycle f satisfies the condition that $\Gamma_f = \mathrm{Ker}\, \varepsilon$ if and only if a_f is regular, i.e. $a_f(\sigma, G) = 1$ implies $\sigma = 1$. This condition holds only if K contains a primitive m-th root of unity.*

PROOF. Since the action of G is trivial, Γ_f is the set of all $\gamma \in \mathbf{Z}^n$ such that

$$f(\beta, \gamma) f(\gamma, \beta)^{-1} = 1 \qquad \text{for all } \beta \in \mathbf{Z}^n;$$

in other words, $\Gamma_f = \varepsilon^{-1}(R)$, where $R = \{\sigma \in G \mid a_f(\sigma, G) = 1\}$. Therefore, $\Gamma_f = \mathrm{Ker}\, \varepsilon$ if and only if $R = \{1\}$, which proves the first part.

If $R = \{1\}$, then the exponent of the group $a_f(\sigma, G) \subset K^*$ is equal to the order of σ, for all $\sigma \in G$; if G has exponent m, then it contains an element σ of order m, whence K^* also contains an element of order m, which is a primitive m-th root of unity. This completes the proof.

If $\Gamma = \mathrm{Ker}\, \varepsilon_f$, then choosing a primitive m-th root of unity in K^* we may identify a_f with a regular skew-symmetric *form* on G. Henceforth, we assume that $\Gamma_f = \mathrm{Ker}\, \varepsilon$ and we denote simply by G the symplectic module (G, a_f).

Recall that an isotropic subgroup $H \subset G$ is a subgroup for which $a_f(H, H) = 1$. These subgroups completely determine the subfields of $\mathscr{D}_f$, as shown in the following theorem:

4.2. THEOREM. *Every extension L of $\mathscr{C}_f$ in $\mathscr{D}_f$ is a Kummer subfield of $\mathscr{D}_f$ and $\varepsilon v(L)$ is an isotropic subgroup of G. The map $L \to \varepsilon v(L)$ defines a one-to-one correspondence between the set of classes of conjugate subfields of $\mathscr{D}_f$ which contain $\mathscr{C}_f$ and the set of isotropic subgroups of G. This correspondence satisfies:*

(1) $[L : \mathscr{C}_f] = |\varepsilon v(L)|$ *and* $\varepsilon v : \mathrm{kum}(L/\mathscr{C}_f) \to \varepsilon v(L)$ *is an isomorphism.*

(2) *If $L_1 \subseteq L_2$, then $\varepsilon v(L_1) \subseteq \varepsilon v(L_2)$ and if S_1, S_2 are isotropic subgroups such that $S_1 \subseteq S_2$, then there exists subfields L_1, L_2 such that $L_1 \subseteq L_2$ and $\varepsilon v(L_i) = S_i$ for $i = 1, 2$.*

PROOF. The valuation v on $\mathscr{D}_f$ makes $\mathscr{D}_f$ a totally ramified extension of $\mathscr{C}_f$ since $\bar{\mathscr{C}}_f = F = K = \bar{\mathscr{D}}_f$. Hence, every extension of $\mathscr{C}_f$ in $\mathscr{D}_f$ is totally ramified, whence a Kummer extension of $\mathscr{C}_f$, since K contains a primitive m-th root of unity: see [17, Theorem 4, p. 66].

Let L be a (Kummer) subfield of $\mathscr{D}_f$ and let $S_L = \varepsilon v(L) \subseteq G$ as in §3. Since $\bar{L} = F = K$, we have $\mathrm{KUM}(\bar{L}/F) = K^*$ and $\mathrm{kum}(\bar{L}/F) = 1$; it then follows from Theorem 3.10 that $\mathrm{res}^G_{S_L}(f)$ is symmetric, hence $a_f(\sigma, \tau) = 1$ for $\sigma, \tau \in S_L$, which means that S_L is isotropic in G.

Conversely, let S be an isotropic subgroup of G; then $a_f(S, S) = 1$, which means that $\mathrm{res}^G_S(f) \in Z^2(S, K^*)_{\mathrm{sym}}$ and we can apply Theorem 3.11 with $h = \mathrm{res}^G_S(f)$ and $\bar{L} = K$ to obtain a Kummer subfield L of $\mathscr{D}_f$ such that $S = \varepsilon v(L)$ as required.

Before completing the proof that εv induces a one-to-one correspondence between classes of conjugate subfields and isotropic subgroups, we observe that (1) readily follows from Proposition 3.6 since $\mathrm{kum}(\bar{L}/F) = 1$ for every (Kummer) subfield L.

Next, we prove (2): let $S_1 \subseteq S_2$ for some isotropic subgroups of G and let L_1, L_2 be two Kummer subfields such that $\varepsilon v(L_i) = S_i$. By Proposition 3.4, we can find Kummer subfields L_1', L_2' which are conjugate to L_1 and L_2 respectively, and such that $\mathrm{kum}(L_i'/\mathscr{C}_f)$ is represented by monomials in $\mathscr{M}_f$ for $i = 1, 2$. In other words, $\mathrm{kum}(L_1'/\mathscr{C}_f)$ and $\mathrm{kum}(L_2'/\mathscr{C}_f)$ both lie in the factor group $(\mathscr{M}_f . \mathscr{C}_f^*)/\mathscr{C}_f^*$.

Clearly, $\mathscr{C}_f^* \subset \mathrm{Ker}\, \varepsilon v$ since $v(\mathscr{C}_f^*) = \Gamma_f = \mathrm{Ker}\, \varepsilon$; moreover it is easily seen, using Proposition 2.4, that $\mathscr{M}_f \cap \mathrm{Ker}\, \varepsilon v \subset \mathscr{C}_f^*$, so that the homomorphism $\varepsilon v : (\mathscr{M}_f . \mathscr{C}_f^*)/\mathscr{C}_f^* \to G$ is actually an isomorphism. Now, by (1) and by Proposition 3.8, we have $\varepsilon v\,(\mathrm{kum}(L_i'/\mathscr{C}_f)) = \varepsilon v(L_i') = S_i$ for $i = 1, 2$; but since $S_1 \subseteq S_2$, it follows that $\mathrm{kum}(L_1'/F) \subseteq \mathrm{kum}(L_2'/F)$ and hence $L_1' \subseteq L_2'$ since $\mathrm{KUM}(L_1'/F)$ and $\mathrm{KUM}(L_2'/F)$ generate L_1' and L_2' respectively; also $\varepsilon v(L_i') = S_i$. This proves (2).

Moreover, if $S_1 = S_2$ then obviously $L_1' = L_2'$; since L_i' is conjugate to L_i for $i = 1, 2$, this shows that if $\varepsilon v(L_1) = \varepsilon v(L_2)$, then L_1 and L_2 are conjugate. To

complete the proof, it now suffices to note that εv is well-defined on classes of conjugate subfields of $\mathcal{D}_f$ by Proposition 3.8.

4.3. COROLLARY. *The isomorphism classes of Galois groups of maximal subfields of $\mathcal{D}_f$ are identical to the isomorphism classes of Lagrangians of the symplectic module G.*

PROOF. Recall that a Lagrangian of G is by definition a maximal isotropic subgroup; they thus correspond to maximal subfields of $\mathcal{D}_f$. Since the Galois group of a Kummer extension is isomorphic to its Kummer group, the corollary readily follows from the preceding theorem.

4.4. If the field K is algebraically closed, then we can apply a recent result of the authors [19] to prove:

THEOREM. *If K is algebraically closed, then for every splitting field M of $\mathcal{D}_f$, Galois over $\mathcal{C}_f$, the Galois group* $\mathrm{Gal}(M/\mathcal{C}_f)$ *contains (an isomorphic image of) a Lagrangian of G.*

PROOF. By the main theorem of [19], the splitting field M contains (an isomorphic image of) a maximal subfield L of $\mathcal{D}_f$; hence $\mathrm{Gal}(L/\mathcal{C}_f)$, which is isomorphic to a Lagrangian S of G, is a homomorphic image of $\mathrm{Gal}(M/\mathcal{C}_f)$. Since the residue field K of $\mathcal{C}_f$ is algebraically closed, M is totally ramified over $\mathcal{C}_f$. It the characteristic of K does not divide $[M : \mathcal{C}_f]$, then it follows from [17, p. 66] that $\mathrm{Gal}(M/\mathcal{C}_f)$ is abelian; in this case, since S is a homomorphic image of $\mathrm{Gal}(M/\mathcal{C}_f)$, it is also isomorphic to a subgroup of $\mathrm{Gal}(M/\mathcal{C}_f)$ and the theorem is proved.

If the characteristic of K, which we denote by p, divides $[M : \mathcal{C}_f]$, then let P be a p-Sylow subgroup of $\mathrm{Gal}(M/\mathcal{C}_f)$ and let $N = M^P$ be its fixed field. Since p does not divide $[L : \mathcal{C}_f]$, we have $L \subset N$; but N is Galois over $\mathcal{C}_f$ with abelian Galois group, by [17, p. 66], whence S is isomorphic to a subgroup of $\mathrm{Gal}(N/\mathcal{C}_f)$. On the other hand, since N is Galois over $\mathcal{C}_f$, the corresponding subgroup P is normal in $\mathrm{Gal}(M/\mathcal{C}_f)$ and it follows from [5, Theorem 15.2.2] that $\mathrm{Gal}(M/\mathcal{C}_f)$ contains a subgroup isomorphic to $\mathrm{Gal}(N/\mathcal{C}_f)$. Therefore, $\mathrm{Gal}(M/\mathcal{C}_f)$ also contains a subgroup isomorphic to S and the proof is complete.

5. Laurent power series

5.1. The division algebras $\mathcal{D}_f$ with trivial action of G on K are closely related to some other known division algebras, which are constructed as follows:

Let $r_1, \ldots, r_n$ be n positive integers and let m be the least common multiple of

$r_1, \ldots, r_n$. Let also K be a field containing a primitive m-th root of unity ω; then $\omega_i = \omega^{mr_i^{-1}}$ is a primitive r_i-th root of unity for $i = 1, \ldots, n$.

Consider the iterated Laurent series ring in $2n$ non-commuting indeterminates:

$$D(K, r_1, \ldots, r_n) = K((x_1, y_1, \ldots, x_n, y_n))$$

with the multiplication table:

$$x_i a = a x_i, \qquad y_i a = a y_i \qquad \text{for } a \in K,$$

$$x_i x_j = x_j x_i, \qquad y_i y_j = y_j y_i,$$

$$x_i y_j = y_j x_i \quad \text{for } i \neq j,$$

$$x_i y_i = \omega_i y_i x_i.$$

These division rings were first considered in [3, §2] (see also [6, Chapter II, §5]) in order to construct non-crossed-product division algebras, and they are of the type described in the previous sections:

5.2. PROPOSITION. *$D(K, r_1, \ldots, r_n) \simeq \mathcal{D}(K, G, f, \varepsilon)$ for some abelian group G acting trivially on K, some map $\varepsilon : \mathbf{Z}^{2n} \to G$ and some cocycle $f \in Z^2(G, K^*)$ for which $\Gamma_f = \operatorname{Ker} \varepsilon$.*

PROOF. Let $G = (\mathbf{Z}/r_1\mathbf{Z})^2 \times \cdots \times (\mathbf{Z}/r_n\mathbf{Z})^2$ and let $\sigma_1, \tau_1, \ldots, \sigma_n, \tau_n$ be the standard basis of G, so that σ_i and τ_i have order r_i. Let $a : G \times G \to K^*$ be the skew-symmetric map defined by:

$$a(\sigma_i, \sigma_j) = a(\tau_i, \tau_j) = 1 \qquad \text{for all } i, j,$$

$$a(\sigma_i, \tau_j) = 1 \qquad \text{for } i \neq j,$$

$$a(\sigma_i, \tau_i) = \omega_i.$$

It follows from Proposition 1.3 that there exists a cocycle $f \in Z^2(G, K^*)$ such that $f(\sigma, \tau) f(\tau, \sigma)^{-1} = a(\alpha, \tau)$ for all $\sigma, \tau \in G$. Now let $\varepsilon : \mathbf{Z}^{2n} \to G$ be the canonical homomorphism, which maps the standard basis $\beta_1, \ldots, \beta_{2n}$ of $\mathbf{Z}^{2n}$ onto $\sigma_1, \tau_1, \ldots, \sigma_n, \tau_n$. From Proposition 2.3 we conclude that $\mathcal{D}(K, G, f, \varepsilon) \simeq D(K, r_1, \ldots, r_n)$ by mapping $z_{2i-1} \to x_i$ and $z_{2i} \to y_i$. Moreover, the skew-symmetric map $a = a_f$ is easily seen to be regular, whence $\Gamma_f = \operatorname{Ker} \varepsilon$ by Proposition 4.1.

5.3. The preceding proposition has also an "almost" converse result:

PROPOSITION. *Let G be an abelian group acting trivially an a field K and let $f \in Z^2(G, K^*)$. If the corresponding skew-symmetric map $a_f \in \operatorname{Skew}(G, K^*)$ is*

regular, then there exist integers $r_1, \ldots, r_n$ *and a homomorphism* $\varepsilon : \mathbf{Z}^{2n} \to G$ *such that* $\mathcal{D}(K, G, f, \varepsilon) \simeq D(K, r_1, \ldots, r_n)$.

PROOF. Let m be the exponent of G. Since a_f is regular, it follows from Proposition 4.1 that K contains a primitive m-th root of unity ω, which we use to identify a_f to a regular skew-symmetric form on G. Theorem 1.4 then shows that G has a basis $(\sigma_1, \tau_1, \ldots, \sigma_n, \tau_n)$ such that

$$a_f(\sigma_i, \sigma_j) = a_f(\tau_i, \tau_j) = 1, \qquad a_f(\sigma_i, \tau_j) = 1 \quad \text{for } i \neq j \quad \text{and} \quad a_f(\sigma_i, \tau_i) = \omega^{mr_i^{-1}},$$

where r_i denotes the order of σ_i, which is equal to the order of τ_i. If $\varepsilon : \mathbf{Z}^{2n} \to G$ maps the standard basis of $\mathbf{Z}^{2n}$ onto $\sigma_1, \tau_1, \ldots, \sigma_n, \tau_n$, it then follows from Proposition 2.3 that $\mathcal{D}(K, G, f, \varepsilon) \simeq D(K, r_1, \ldots, r_n)$.

5.4. The results of the preceding section yield a different proof of [3, Theorem 3] (see also [6, Theorem 1, p. 102]):

THEOREM. *Let p be a prime number and let K be a field containing a primitive p-th root of unity. Every maximal subfield of* $D(K, p, \ldots, p)$ *(with n times p) is Galois over the center with elementary abelian Galois group of rank n. Moreover, if K is algebraically closed, then the Galois group of every Galois splitting field of* $D(K, p, \ldots, p)$ *contains such a group.*

PROOF. From Proposition 5.2, it follows that $D(K, p, \ldots, p) \simeq \mathcal{D}(K, G, f, \varepsilon)$ with an elementary abelian group G of rank $2n$. By Theorem 4.2, every maximal subfield is Galois over the center and by Corollary 4.3, its Galois group is isomorphic to a Lagrangian of G, and is therefore elementary abelian of rank n, by Proposition 1.6. The rest follows from Theorem 4.4.

5.5. Similarly, we have:

THEOREM. *Let r be an integer and let K be a field containing a primitive r-th root of unity. Every maximal subfield of* $D(K, r)$ *is Galois over the center with a Galois group isomorphic to a direct product of two cyclic groups whose orders multiply to r. Moreover, if K is algebraically closed, then the Galois group of every Galois splitting field of* $D(K, r)$ *contains such a group.*

The proof is similar, using Proposition 1.7 instead of 1.6.

6. Simultaneous crossed products

6.1. DEFINITIONS. A group G is said to *split* a central simple algebra A over a field F if A is split by some Galois extension K of F whose Galois group $\mathrm{Gal}(K/F)$ is isomorphic to some *subgroup* of G.

If k is a field and if G, H are two groups, we say that H is *G-adequate* over k and we denote $G \Rightarrow_k H$ if every simple k-algebra split by G is also split by H. In other words, this means that for every extension $F \supset k$, every central simple algebra over F which is similar to a crossed product of some *subgroup* of G is also similar to a crossed product of some *subgroup* of H.

The aim of this section is to show how the results of the preceding sections can be applied to yield some information on adequacy of finite groups. We first note the following immediate consequences of the definitions:

PROPOSITION.

(a) *If $G \Rightarrow_k H$, then $G \Rightarrow_F H$ for every field $F \supset k$.*

(b) *If G is isomorphic to a subgroup of H, then $G \Rightarrow_k H$.*

(c) *If $G \Rightarrow_k G'$ and $G' \Rightarrow_k G''$, then $G \Rightarrow_k G''$.*

6.2. Next, we investigate how adequacy of direct products relate to adequacy of the factors. The following lemma is probably well-known, but we include a proof for the reader's convenience.

LEMMA. *Let G_1 and G_2 be finite groups and let $J \subset G_1 \times G_2$ be a subgroup of their direct product. If $|G_1|$ and $|G_2|$ are relatively prime, then $J = (J \cap G_1) \times (J \cap G_2)$.*

PROOF. Let J_1 be the image of J under the projection map $\pi_1 : G_1 \times G_2 \to G_1$. Since the kernel of π_1 is G_2 ($= 1 \times G_2$ in $G_1 \times G_2$), the map π_1 induces a canonical isomorphism: $J/J \cap G_2 \simeq J_1$.

Since $|J_1|$ and $|J \cap G_2|$ are relatively prime, it follows from theorem 15.2.2 of [5] that J contains a subgroup J_1' isomorphic to J_1. This subgroup clearly lies in the kernel of the projection map $\pi_2 : G_1 \times G_2 \to G_2$, i.e. in G_1, since its order is relatively prime to $|G_2|$. Theorefore, $J_1' \subset J \cap G_1$, whence

$$|(J \cap G_1) \times (J \cap G_2)| \geqq |J_1'| \cdot |J \cap G_2|.$$

As $J/J \cap G_2 \simeq J_1$, we also have $|J_1| \cdot |J \cap G_2| = |J|$, and the preceding inequality yields: $|(J \cap G_1) \times (J \cap G_2)| \geqq |J|$.

Since obviously $J \supset (J \cap G_1) \times (J \cap G_2)$, it follows that $J = (J \cap G_1) \times (J \cap G_2)$.

6.3. LEMMA. *Let G_1 and G_2 be two finite groups of relatively prime orders and let F be a field. If A is a central simple F-algebra split by $G_1 \times G_2$, then $A \simeq A_1 \otimes_F A_2$ for some algebras A_1, A_2 split by G_1 and G_2 respectively. Moreover, every splitting group of A splits A_1 and A_2.*

Conversely, if A_1 and A_2 are central simple F-algebras split by G_1 and G_2 respectively, then $A_1 \otimes_F A_2$ is split by $G_1 \times G_2$.

PROOF. Let K be a splitting field of A, Galois over F with Galois group $\mathrm{Gal}(K/F)$ isomorphic to a subgroup of $G_1 \times G_2$. By Lemma 6.2,

$$\mathrm{Gal}(K/F) = (\mathrm{Gal}(K/F) \cap G_1) \times (\mathrm{Gal}(K/F) \cap G_2),$$

whence $K = K_1 \otimes_F K_2$ for some subfields K_1, K_2 of K such that $\mathrm{Gal}(K_i/F) \simeq \mathrm{Gal}(K/F) \cap G_i$ (for $i = 1, 2$). This implies in particular that $[K_1 : F]$ and $[K_2 : F]$ are relatively prime.

Since the index of A divides $[K : F] = [K_1 : F][K_2 : F]$, it follows from [2, Theorem 5.18] that $A \sim A_1 \otimes_F A_2$, where the index of A_i divides $[K_i : F]$ for $i = 1, 2$.

The indices of A_1 and A_2 are thus relatively prime, whence A_1 and A_2 are both split by every splitting field of A, by [2, Theorem 4.10]: this already shows that every splitting group of A splits A_1 and A_2. In particular, K splits A_1 and A_2, whence K_1 splits A_1 and K_2 splits A_2, since the index of A_1 (resp. A_2) is relatively prime to $[K : K_1] = [K_2 : F]$ (resp. to $[K : K_2] = [K_1 : F]$). Since $\mathrm{Gal}(K_1/F)$ and $\mathrm{Gal}(K_2/F)$ are isomorphic to subgroups of G_1 and G_2 respectively, this proves that A_i is split by G_i, for $i = 1, 2$. The converse is clear, since if K_1, K_2 are splitting fiels of A_1 and A_2 respectively and if the ranks of K_1 and K_2 are relatively prime over F, then $K_1 \otimes_F K_2$ is a splitting field of $A_1 \otimes_F A_2$.

6.4. THEOREM. *Let G_1, G_2, H_1, H_2 be finite groups and let k be a field. If $|G_1|$ and $|H_1|$ are both relatively prime to $|G_2|$ and $|H_2|$, then $G_1 \times G_2 \Rightarrow_k H_1 \times H_2$ if and only if $G_1 \Rightarrow_k H_1$ and $G_2 \Rightarrow_k H_2$.*

PROOF. Assume first $G_1 \times G_2 \Rightarrow_k H_1 \times H_2$ and let A be a central simple algebra split by G_1. Since G_1 is isomorphic to a subgroup of $G_1 \times G_2$, we have $G_1 \Rightarrow_k H_1 \times H_2$ by transitivity of $\Rightarrow_k$, whence A is split by $H_1 \times H_2$. Since $|H_1|$ and $|H_2|$ are relatively prime, the previous lemma shows that $A \simeq A_1 \otimes_F A_2$, where A_i is an algebra split by H_i for $i = 1, 2$. Moreover, it also shows that A_1 and A_2 are both split by G_1, since A is split by G_1.

Now, the index of A_2 divides $|G_1|$ and $|H_2|$, since G_1 and H_2 split A_2, whence $A_2 \sim 1$ (i.e. A_2 is a matrix algebra) since $|G_1|$ and $|H_2|$ are relatively prime. Therefore, $A \sim A_1$, whence A is split by H_1: this proves $G_1 \Rightarrow_k H_1$ and we similarly have $G_2 \Rightarrow_k H_2$.

Conversely, assume $G_1 \Rightarrow_k H_1$ and $G_2 \Rightarrow_k H_2$, and let A be an algebra split by $G_1 \times G_2$. The previous lemma shows that $A \simeq A_1 \otimes_F A_2$ where A_i is split by G_i

for $i = 1, 2$. By hypothesis, it follows that A_i is split by H_i and then, by Lemma 6.3 again, that $A \simeq A_1 \otimes_F A_2$ is split by $H_1 \times H_2$. This completes the proof.

6.5. COROLLARY. *If G and H are finite nilpotent groups, then, denoting by $G(p)$ (resp. $H(p)$) a Sylow p-subgroup of G (resp. H), we have $G \Rightarrow_k H$ if and only if $G(p) \Rightarrow_k H(p)$ for all primes p.*

PROOF. This readily follows from the theorem, since finite nilpotent groups are direct products of their Sylow subgroups [5, Theorem 10.3.4].

6.6. When G is abelian, the results of the previous sections yield rather strong conditions on the groups which are G-adequate:

THEOREM. *Let G be an abelian group and let k be a field whose characteristic does not divide $|G|$. If $G \Rightarrow_k H$ for some group H, then H contains (an isomorphic image of) a Lagrangian of every symplectic module containing (an isomorphic image of) G as a Lagrangian. In particular, $|G|$ divides $|H|$.*

PROOF. Let K be an algebraic closure of k and let (G', a) be a symplectic module containing G as a Lagrangian. By Lemma 1.5, it follows that $|G'| = |G|^2$, hence the characteristic of K does not divide $|G'|$. Choosing a primitive $\exp(G')$-th root of unity in K, we may identify the form a to a regular skew-symmetric map $a \in \mathrm{Skew}(G', K^*)$. By Proposition 1.3, there is a cocycle of $f \in H^2(G', K^*)$ whose corresponding form a_f is a. Consider then the algebra $\mathcal{D}_f = \mathcal{D}(K, G', f, \varepsilon)$ (for some map $\varepsilon : \mathbf{Z}^n \to G'$): since G is a Lagrangian of (G', a_f), it splits $\mathcal{D}_f$, by Corollary 4.3. Now $G \Rightarrow_k H$ and $\mathcal{C}_f \supset k$, hence H also splits $\mathcal{D}_f$. By Theorem 4.4, it follows that H contains an isomorphic image of a Lagrangian of G'. Therefore, $|G|$ divides $|H|$, since the order of every Lagrangian of G' is equal to $|G|$, by Lemma 1.5. This completes the proof.

6.7. When H also is assumed to be abelian, then $G \Rightarrow_k H$ if and only if $G(p) \Rightarrow_k H(p)$ for all primes p, by Corollary 6.5. When dealing with adequacy of abelian groups, we may thus restrict to abelian p-groups.

In order to obtain explicit relations on the invariant factors of abelian groups G, H such that $G \Rightarrow_k H$, we quote the following result of [20]:

Let G and H be abelian p-groups (for some prime p); choose an integer n such that $2n \geqq \mathrm{rk}\, G, \mathrm{rk}\, H$, and let $(g_1, \ldots, g_{2n})$ and $(h_1, \ldots, h_{2n})$ with $g_1 \geqq \cdots \geqq g_{2n} \geqq 0$ and $h_1 \geqq \cdots \geqq h_{2n} \geqq 0$ be the exponents of p in the invariant factors of G and H respectively. We refer to these sequences as the *invariant exponents* of G and H respectively.

PROPOSITION. *G is a Lagrangian in a symplectic module M_1 with invariant exponents $(g_1+g_2, g_3+g_4, \ldots, g_{2n-1}+g_{2n})$ (each twice repeated) and also in a symplectic module M_2 with invariant exponents $(g_1, g_2, \ldots, g_{2n})$ (each twice). If H is isomorphic to some Lagrangian of M_1 and to some Lagrangian of M_2, then*

(6.7.1) $g_{2i-1}+g_{2i} = h_{2i-1}+h_{2i}$ *and* $g_{2i-1} \geqq h_{2i-1} \geqq h_{2i} \geqq g_{2i}$ *for* $i = 1, \ldots, n$.

6.8. This proposition has an immediate consequence for the adequacy of groups:

COROLLARY. *Let G be an abelian p-group and let H be a p-group such that $|G| = |H|$. If $G \Rightarrow_k H$ for some field k of characteristic different from p, then H is abelian and the invariant exponents of G and H are related by* (6.7.1).

PROOF. From Theorem 6.6, it readily follows that H is isomorphic to a Lagrangian of every symplectic module containing G as a Lagrangian, since $|G| = |H|$; therefore, H is abelian and the rest follows from the previous proposition.

6.9. COROLLARY. *If G and H are finite abelian groups such that $G \Rightarrow_k H$ and $H \Rightarrow_k G$ for some field k whose characteristic does not divide $|G|$ nor $|H|$, then $G \simeq H$.*

PROOF. If follows from Theorem 6.6 that $|G|$ divides $|H|$ since $G \Rightarrow_k H$, and that $|H|$ divides $|G|$ since $H \Rightarrow_k G$. Therefore, $|G| = |H|$. By Corollary 6.5, we also have $G(p) \Rightarrow_k H(p)$ and $H(p) \Rightarrow_k G(p)$ for all primes p, whence the invariant exponents of $G(p)$ and $H(p)$ are related by (6.7.1) and similar relations with g_i and h_i permuted. From these relations, it clearly follows that the invariant exponents of $G(p)$ and $H(p)$ are equal, whence $G(p) \simeq H(p)$ for all primes p. Therefore, $G \sim H$.

In other words, this corollary shows that if G and H are non-isomorphic finite abelian groups and if k is a field whose characteristic is relatively prime to $|G|$ and $|H|$, then either there is a simple k-algebra which is a crossed product of a subgroup of G but not of a subgroup of H, or there is a simple k-algebra which is a crossed product of a subgroup of H but not of a subgroup of G.

7. Splitting groups of universal division algebras

7.1. The results of the preceding section yield some information on the minimal Galois extensions which split the universal division algebra $\mathrm{UD}(k, n)$, thanks to the following theorem, due to the second author [4, p. 15]:

THEOREM. *Let k be an infinite field. If the universal division algebra* $\mathrm{UD}(k, n)$ *is split by a group H, then H splits every central simple algebra of degree n over any field $F \supset k$. Therefore, $G \Rightarrow_k H$ for every group G of order dividing n.*

The second assertion follows from the first, since every central simple algebra split by a group of order dividing n is similar to a central simple algebra of degree n, and is therefore split by H.

7.2. COROLLARY. *With the conditions of the previous theorem, and assuming moreover that the characteristic of k does not divide n, the group H must contain subgroups isomorphic to Lagrangians of every symplectic module of order dividing n^2.*

PROOF. As in Theorem 6.6, any symplectic module G' of order dividing n^2 yields a division algebra $\mathscr{D}_f$ of rank $[\mathscr{D}_f : \mathscr{C}_f] = |G'|$, which has the property that every splitting group of $\mathscr{D}_f$ contains (an isomorphic image of) a Lagrangian of G'. Since $\mathscr{D}_f$ is similar to a central simple algebra of degree n, it is split by H; therefore, H contains (an isomorphic image of) a Lagrangian of G'.

7.3. This last result yields a restriction on the minimal order of the groups which split $\mathrm{UD}(k, n)$:

THEOREM. *Let $n = p_1^{r_1} \cdots p_s^{r_s} p_{s+1} \cdots p_t$ where $r_i \geqq 2$ for $i = 1, \ldots, s$ and $\{p\}$ are different primes. If H is a splitting group of* $\mathrm{UD}(k, n)$, *where k is an infinite field whose characteristic does not divide n, then*

$$|H| \geqq n \cdot p_1^{r_1 - 2} \cdots p_s^{r_s - 2}.$$

REMARK. This includes the fact that if $r_i \geqq 3$ for some i, then $\mathrm{UD}(k, n)$ is not a crossed product (see e.g. [6, p. 110]).

PROOF. Let p^r be the highest power of a prime $p = p_i$ dividing n. Consider the two examples of symplectic modules of order p^{2r} of 1.6 and 1.7: namely, the elementary abelian group A_{2r} and B_{2r}, the direct product of two cyclic groups of order p^r. Since p^{2r} divides n^2, it follows from Corollary 7.2 that H contains a subgroup H_1 isomorphic to a Lagrangian of A_{2r} and a subgroup H_2 isomorphic to a Lagrangian of B_{2r}. Since all the Sylow p-subgroups of H are conjugate, we may assume that H_1 and H_2 are both contained in some Sylow p-subgroup $H(p)$.

Proposition 1.6 shows that H_1 is elementary abelian (of rank r) and Proposition 1.7 shows that H_2 is a direct sum $C_{p^s} \oplus C_{p^t}$ of two cyclic groups with $s + t = r$. Therefore, $H_1 \cap H_2$ is elementary abelian of rank at most 2, whence $|H_1 \cap H_2| \leqq p^2$.

Now, let $H_1H_2 = \{h_1h_2 \mid h_i \in H_i \text{ for } i = 1,2\} \subset H(p)$. By counting the classes $\{H_1h \mid h \in H_2\}$, we get $|H_1H_2| = |H_1|\,|H_2|\,|H_1 \cap H_2|^{-1}$, whence

$$|H(p)| \geqq |H_1|\,|H_2|\,|H_1 \cap H_2|^{-1} \geqq p^{2r} \cdot p^{-2}.$$

Consequently, $|H(p)| \geqq p^{2(r-1)}$. If $r = 1$, then H_1 and H_2 are cyclic of order p, whence $|H(p)| \geqq p$. This completes the proof that

$$|H| \geqq p_1^{2(r_1-1)} \cdots p_s^{2(r_s-1)} p_{s+1} \cdots p_t,$$

since $|H| = \Pi_p |H(p)|$.

7.4. The preceding proof shows that in order to get a better bound for $|H|$, we need a bound for the order of the groups satisfying the condition of Corollary 7.2. This seems to be a rather difficult problem, which will be dealt with elsewhere. Here we quote one result from [20]:

THEOREM. *Let $(e_1, \ldots, e_m)$ be the invariant exponents of an abelian p-group P, with $e_1 \geqq \cdots \geqq e_m \geqq 0$. If P contains (an isomorphic image of) a Lagrangian of every symplectic module of order p^{2r}, then*

$$e_\nu + e_{\nu+1} \geqq \left[\frac{r}{\nu}\right] \qquad \text{for } \nu = 1, \ldots, r. \tag{7.4.1}$$

(Here, $[r/\nu]$ denotes the greatest integer q such that $q \leqq (r/\nu)$.)

7.5. Now, suppose H is an *abelian* splitting group of UD(k, n), let p be a prime dividing n and let $H(p)$ be the Sylow p-subgroup of H. Let also p^r be the highest power of p dividing n. From Corollary 7.2, and from the fact that every p-subgroup of H is contained in $H(p)$, it follows that $H(p)$ contains an isomorphic image of a Lagrangian of every symplectic module of order p^{2r}, whence the invariant exponents $a_1, \ldots, a_m$ of $H(p)$ satisfy relation (7.4.1).

From this relation, it follows in particular that $e_1 + e_2 \geqq r$ and $e_\nu \geqq \frac{1}{2}[r/\nu]$ for $\nu = 1, \ldots, r$, since $e_\nu \geqq e_{\nu+1}$. Since e_ν is an integer, we even have:

$$e_\nu \geqq \left\{\frac{1}{2}\left[\frac{r}{\nu}\right]\right\} \qquad \text{for } \nu = 1, \ldots, r$$

where $\{\rho\}$ denotes, for any real number ρ, the smallest integer q such that $q \geqq \rho$. Therefore,

$$\sum_\nu e_\nu = e_1 + e_2 + \sum_{\nu \geqq 3} e_\nu \geqq r + \sum_{\nu \geqq 3} \left\{\frac{1}{2}\left[\frac{r}{\nu}\right]\right\}.$$

Since $|H(p)| = p^{\Sigma e_\nu}$ and $|H| = \Pi_p |H(p)|$, we have proved:

THEOREM. *Let $n = p_1^{r_1} \cdots p_t^{r_t}$, where $\{p_i\}$ are different primes, and let k be an infinite field whose characteristic does not divide n. If H is an abelian splitting group of* $\mathrm{UD}(k, n)$, *then $|H|$ is divisible by $p_1^{R_1} \cdots p_t^{R_t}$, where*

$$R_i = r_i + \sum_{\nu \geqq 3} \left\{ \frac{1}{2} \left[\frac{r_i}{\nu} \right] \right\} .$$

REMARK. As a function of r_i,

$$R_i = (r_i \log r_i)/2 + O(r_i).$$

8. A survey of previously known results

Some results on adequacy of groups are implicit in the recent literature. In this section, we collect those we are aware of and translate them in the notations of this paper.

The adequacy to cyclic groups has been particularly investigated:

THEOREM. *Let k be a field of characteristic $p \geqq 0$ and let C_n be a cyclic group of order n.*

(a) (Risman [13, Theorem 1]) *If $|H| = n$ and if n and p are relatively prime, then $C_n \Rightarrow_k H$ if and only if $H \simeq C_r \times C_s$ where s divides r and k contains a primitive s-th root of unity.*

(b) (Saltman [15]) *If $n = p^r$, then $C_n \Rightarrow_k H$ if and only if n divides $|H|$.*

In particular, part (a) shows that if k has no n-th root of unity except 1, then $C_n \Rightarrow_k H$ if and only if $H = C_n$. The same arguments as in [13] can be used to prove more generally:

PROPOSITION. *Let k be a field of characteristic $p \geqq 0$, let n be an integer not divisible by p and let G, H be two groups of order n. If G is abelian and if 1 is the only n-th root of unity in k, then $G \Rightarrow_k H$ if and only if $H \simeq G$.*

The case where n is a power of p was studied by Saltman, who proved [16, Theorem 3.2]:

THEOREM. *Let k be a field of characteristic $p \neq 0$ and let G, H be two p-groups of the same order. If G is abelian and not cyclic, then $G \Rightarrow_k H$ if only if $G \simeq H$.*

It was communicated to us by Saltman that the same holds if G, H are p-groups of the same order for some prime p and $\mathrm{char}(k) = 0$.

In the case where G is not abelian, much less is known. There is however one result for the case $G = D_{2n}$, the dihedral group of order $2n$:

THEOREM (Rowen and Saltman [14]). *If n is odd and if k contains a primitive n-th root of unity, then $D_{2n} \Rightarrow_k C_{2n}$.*

There is also an old result for the case $G = C_m \propto C_p$, a semi-direct product of cyclic groups:

THEOREM (Albert [1]). *If $\mathrm{char}(k) = p$ and if p does not divide m, then $C_m \propto C_p \Rightarrow_k C_{pm}$. In particular, if p is odd, $D_{2p} \Rightarrow_k C_{2p}$.*

Appendix. Symmetric cocycles and the inflation map

Let G be a finite abelian group and $\varepsilon : \mathbf{Z}^n \to G$ be a surjective homomorphism. Let also A be a G-module. Letting $\mathbf{Z}^n$ act on A through ε, we have an inflation map:

$$\inf : H^2(G, A) \to H^2(\mathbf{Z}^n, A).$$

The aim of this appendix is to provide a proof of the following result:

THEOREM. *The kernel of* $\inf : H^2(G, A) \to H^2(\mathbf{Z}^n, A)$ *is* $H^2(G, A)_{\mathrm{sym}}$.

We need two lemmas:

LEMMA 1. *Every symmetric cocycle is cohomologous (in $H^2(G, A)$) to a symmetric cocycle with values in A^G, the subgroup of A elementwise fixed under G.*

PROOF. Choose a basis $\mathfrak{b} = (\sigma_1, \ldots, \sigma_r)$ of G, so that $G = \langle\sigma_1\rangle \oplus \cdots \oplus \langle\sigma_r\rangle$, let $C^2_{\mathfrak{b}}(G, A)$ be the group of couples of families $((u_{ij})_{1 \le i,j \le r}, (b_i)_{1 \le i \le r})$ with $u_{ij}, b_i \in A$ for all i, j and $u_{ii} = 0$; $u_{ij} + u_{ji} = 0$ for all i, j.

Let $Z^2_{\mathfrak{b}}(G, A)$ be the subgroup of families for which the following relations hold:

$$(\sigma_i - 1)u_{jk} + (\sigma_j - 1)u_{ki} + (\sigma_k - 1)u_{ij} = 0, \tag{A.1}$$

$$(\sigma_i - 1)b_j = N_j u_{ij}, \tag{A.2}$$

where N_j is the sum of all the elements in the subgroup $G_j \subset G$ generated by σ_j. Let also $B^2_{\mathfrak{b}}(G, A)$ be the subgroup of families for which there exists a family $(c_i)_{1 \le i \le r}$ in A such that:

$$u_{ij} = (\sigma_i - 1)c_j - (\sigma_j - 1)c_i,$$

$$b_i = N_i c_i,$$

and let $H^2_{\mathfrak{b}}(G, A) = Z^2_{\mathfrak{b}}(G/A)/B^2_{\mathfrak{b}}(G, A)$. Then there is a canonical isomorphism:

$$\nu : H^2(G, A) \to H^2_{\mathfrak{b}}(G, A)$$

which maps a cocycle $f \in Z^2(G, A)$ onto the couple (u_{ij}, b_i) defined by:

$$u_{ij} = f(\sigma_i, \sigma_j) - f(\sigma_j, \sigma_i),$$

$$b_i = \sum_{\sigma \in G_i} f(\sigma, \sigma_i).$$

(See for instance [18, §1].)

If f is symmetric, then $u_{ij} = 0$ for all i, j, whence $b_i \in A^G$, by condition (A.2). Define then a cocycle $g \in Z^2(G, A)$ by:

$$g(\sigma_i^k, \sigma_i^m) = 0 \qquad \text{for } 0 \leqq k, \quad m \leqq n_i - 1 \quad \text{and} \quad k + m \leqq n_i - 1,$$

$$g(\sigma_i^k, \sigma_i^m) = b_i \qquad \text{for } 0 \leqq k, \quad m \leqq n_i - 1 \quad \text{and} \quad k + m \geqq n_i,$$

where n_i denotes the order of σ_i, and

$$g\left(\prod_i \sigma_i^{k_i}, \prod_j \sigma_j^{m_j}\right) = \sum_{i=1}^{r} g(\sigma_i^{k_i}, \sigma_i^{m_i}).$$

It is easy to check that g is a symmetric cocycle with values in A^G and that $\nu(f) = \nu(g)$, so that f and g are cohomologous.

LEMMA 2. *$H^2(G, A)_{\mathrm{sym}}$ lies in the kernel of* $\inf : H^2(G, A) \to H^2(\mathbf{Z}^n, A)$.

PROOF. Since $\mathbf{Z}^n$ acts trivially on A^G, the group $H^2(\mathbf{Z}^n, A^G)_{\mathrm{sym}}$ classifies the abelian group extensions of A^G by $\mathbf{Z}^n$; therefore,

$$H^2(\mathbf{Z}^n, A^G)_{\mathrm{sym}} = \mathrm{Exp}^1_{\mathbf{Z}}(\mathbf{Z}^n, A^G) = 0,$$

since $\mathbf{Z}^n$ is $\mathbf{Z}$-projective. Consider then the following commutative diagram:

$$\begin{array}{ccc} H^2(G, A^G)_{\mathrm{sym}} & \xrightarrow{\inf} & H^2(\mathbf{Z}^n, A^G)_{\mathrm{sym}} \\ {\scriptstyle i_*}\downarrow & & \downarrow{\scriptstyle i_*} \\ H^2(G, A)_{\mathrm{sym}} & \xrightarrow[\inf]{} & H^2(\mathbf{Z}^n, A) \end{array}$$

where i_* is induced by the inclusion map $i : A^G \to A$.

By Lemma 1, the left vertical map is surjective. From the fact that the right upper corner is zero, it then follows that $\inf(H^2(G, A)_{\mathrm{sym}}) = 0$.

PROOF OF THE THEOREM. By Lemma 2, it suffices to prove: $\mathrm{Ker}(\inf) \subset$

$H^2(G, A)_{\text{sym}}$. Let Γ be the kernel of $\varepsilon : \mathbf{Z}^n \to G$. The terms of low degree in the Lyndon–Hochschild–Serre spectral sequence associated to the extension

$$0 \to \Gamma \to \mathbf{Z}^n \to G \to 0$$

yield an exact sequence:

$$H^1(\Gamma, A)^G \xrightarrow{\text{tg}} H^2(G, A) \xrightarrow{\text{inf}} H^2(\mathbf{Z}^n, A)$$

where tg is the transgression map (see for instance [8, p. 354]). From the definition of the transgression map (see [8, ch. 11, §9]), it follows easily that the image of tg lies in $H^2(G, A)_{\text{sym}}$. Therefore, $\ker(\text{inf}) \subset H^2(G, A)_{\text{sym}}$, and the proof is complete.

References

1. A. A. Albert, *A note on normal division algebras of prime degree*, Bull. Am. Math. Soc. **44** (1938), 649–652.
2. A. A. Albert, *Structure of Algebras*, Am. Math. Soc. Coll. Pub. 24, Providence, R.I., 1961.
3. S. A. Amitsur, *On central division algebras*, Isr. J. Math. **12** (1972), 408–420.
4. S. A. Amitsur, *Divison Algebras, A Survey*, in *Algebraists' Homage: Papers in Ring Theory and Related Topics*, Contemp. Math. **13** (1982), 3–26.
5. M. Hall, *The Theory of Groups*, Macmillan, New York, 1959.
6. N. Jacobson, *PI-Algebras. An Introduction*, Lecture Notes in Math. **441**, Springer, Berlin, 1975.
7. N. Jacobson, *Basic Algebra II*, Freeman, San Francisco, 1980.
8. S. McLane, *Homology*, Springer, Berlin, 1963.
9. C. Miller, *The second homology group of a group, relations among commutators*, Proc. Am. Math. Soc. **3** (1952), 588–595.
10. B. H. Neumann, *On ordered division rings*, Trans. Am. Math. Soc. **66** (1949), 202–252.
11. G. de Rham, *Sur l'analysis situs des variétés à n dimensions*, J. Math. Pures Appl. **10** (1931), 115–200.
12. P. Ribenboim, *Théorie des valuations*, Presses Univ. Montréal, Montréal, 1968.
13. L. Risman, *Cyclic algebras, complete fields and crossed products*, Isr. J. Math. **28** (1977), 113–128.
14. L. Rowen and D. Saltman, *Dihedral algebras are cyclic*, Proc. Am. Math. Soc. **84** (1982), 162–164.
15. D. Saltman, *Splittings of cyclic p-algebras*, Proc. Am. Math. Soc. **62** (1977), 223–228.
16. D. Saltman, *Noncrossed product p-algebras and Galois p-extensions*, J. Algebra **52** (1978), 302–314.
17. O. F. G. Schilling, *The Theory of Valuations*, Math. Surveys 4, Am. Math. Soc., Providence, 1950.
18. J.-P. Tignol, *Produits croisés abéliens*, J. Algebra **70** (1981), 420–436.
19. J.-P. Tignol and S. A. Amitsur, *Totally ramified splitting fields of central simple algebras over Henselian fields*, J. Algebra, to appear.
20. J.-P. Tignol and S. A. Amitsur, *Symplectic modules*, in preparation.
21. C. T. C. Wall, *Quadratic forms on finite groups, and related topics*, Topology **2** (1963), 281–298.