ELSEVIER

Available online at www.sciencedirect.com

ScienceDirect

Journal of Number Theory 120 (2006) 229–233

JOURNAL OF
Number
Theory

www.elsevier.com/locate/jnt

Some remarks on Hilbertian fields (An appendix to the paper "Galois averages" by R. Massy) ☆

C.U. Jensen [a,*], Richard Massy [b]

[a] *Department of Mathematics, Copenhagen University, DK-2100 Copenhagen, Denmark*
[b] *Département de Mathématiques, Université de Valenciennes, Le Mont Houy, F-59313 Valenciennes, France*

Received 16 April 2005; revised 5 October 2005

Available online 3 February 2006

Communicated by David Goss

Abstract

The paper gives proofs of some results just claimed in [R. Massy, Galois averages, J. Number Theory 113 (2005) 244–275]. For instance, it is proved that for a finite non-trivial separable extension M/F, $M \neq F$, of Hilbertian fields finitely generated over their prime field, the quotient group $M^\times/F^\times$, for the corresponding multiplicative groups of non-zero elements, cannot be a torsion group of finite exponent.

This paper[1] gives proofs of some results announced in [M] which may be of some independent interest.

Let p be a prime number and throughout this paper F denotes a field of characteristic $\neq p$. Further let E be a finite Galois extension of F with Galois group $G := \mathrm{Gal}(E/F)$, containing the pth roots of unity μ_p. As proved in [M], there exists a cyclic extension M/E of degree p such that M is Galois over F if and only if there exist a homomorphism $f \in \mathrm{Hom}(G, \mathbb{F}_p^\times)$ and an element $x \in E^\times \setminus E^{\times p}$ for which $g(x) \in x^{f(g)} E^{\times p}$ for all $g \in G$.

☆ R. Massy, Galois averages, J. Number Theory 113 (2005) 244–275, doi:10.1016/j.jnt.2004.09.005.

* Corresponding author.
E-mail addresses: cujensen@math.ku.dk (C.U. Jensen), richard.massy@univ-valenciennes.fr (R. Massy).

[1] In [M, Ref. [11]] C.U. Jensen and R. Massy, Galois extensibility and Hilbertian fields.

0022-314X/$ – see front matter © 2006 Elsevier Inc. All rights reserved.
doi:10.1016/j.jnt.2005.12.003

This motivates us to introduce the subspace $\mathrm{Nor}^f(E/F)$ for a homomorphism $f \in \mathrm{Hom}(G, \mathbb{F}_p^\times)$ as

$$\mathrm{Nor}^f(E/F) := \{\bar{e} \in E^\times/E^{\times p} \mid \forall g \in G\ g(\bar{e}) = \bar{e}^{f(g)}\},$$

where $E^\times/E^{\times p}$ is considered as a vector space over $\mathbb{F}_p$.

The importance of $\mathrm{Nor}^f(E/F)$ is elaborated in [M].

In general, $\mathrm{Nor}^f(E/F)$ may be trivial for some or for all f.

Example 1. Let F be the smallest (infinite) algebraic extension over $\mathbb{Q}$ containing the pth cyclotomic field $\mathbb{Q}(\mu_p)$, which is closed under pth roots, i.e. $F^p = F$. Let E be a cyclic extension of F of degree q where q is a prime number $> p$. Then, there is no cyclic extension of E of degree p which is Galois over F. Indeed, otherwise the Galois group over F would contain a normal subgroup of index p so that there would exist a cyclic extension of F of degree p, contradicting the fact that $F = F^p$.

Example 2. Let F be a local field of characteristic 0 for which the residue field has characteristic $q \neq p$. Further, let E be a Galois extension of F containing μ_p and assume that the order of the Galois group G of E/F is not divisible by p. By well-known structure theorems for local fields, it is straightforward to check that:

(1) If $\mu_p \subseteq F$, there is exactly one homomorphism $f \in \mathrm{Hom}(G, \mathbb{F}_p^\times)$ such that $\mathrm{Nor}^f(E/F) \neq E^{\times p}$ (namely, the one sending every $g \in G$ into $\bar{1} \in \mathbb{F}_p^\times$).

(2) If $\mu_p \nsubseteq F$, there are at most two homomorphisms $f \in \mathrm{Hom}(G, \mathbb{F}_p^\times)$ for which $\mathrm{Nor}^f(E/F) \neq E^{\times p}$.

However, for Hilbertian fields, $\mathrm{Nor}^f(E/F)$ is always very big. Indeed, among other things, we shall here prove the following result announced without proof in [M, Theorem 1.3]:

Theorem 3. *Let F be a Hilbertian field. With the above notations,* $\mathrm{Nor}^f(E/F)$ *is an infinite-dimensional $\mathbb{F}_p$-vector space for every homomorphism f belonging to* $\mathrm{Hom}(G, \mathbb{F}_p^\times)$.

We shall prove this theorem in a more general setting. Let E/F be a Galois extension with Galois group G. If $s = \sum_{g \in G} h_g g$ is an element of the group ring $\mathbb{Z}[G]$ and α is an element in E, we define $s(\alpha)$ as the product $\prod_{g \in G} g(\alpha)^{h_g}$. In this way, E becomes a $\mathbb{Z}[G]$-module. Moreover, for any prime number p, we may view $E^\times/E^{\times p}$ both as a vector space over $\mathbb{F}_p$ and as a module over the group ring $\mathbb{F}_p[G]$.

Lemma 4. *Let E/F be a Galois extension with Galois group G. If F is Hilbertian, then for any non-trivial $s \in \mathbb{F}_p[G]$ the elements $s(\alpha)$, $\alpha \in E^\times$, modulo $E^{\times p}$, generate an infinite-dimensional subspace of the $\mathbb{F}_p$-space $E^\times/E^{\times p}$.*

Proof. Since F as a Hilbertian field is infinite, there exist infinitely many primitive elements for the extension E/F that are mutually non-conjugate. Consider the field $F(T)$ of rational functions in one variable T over F. For a rational integer h, let $\bar{h}$ denote the corresponding residue class modulo p. Let $s = \sum_{g \in G} \bar{h}_g g$, $h_g \in \mathbb{Z}$, be a non-trivial element in $\mathbb{F}_p[G]$, so that there is at least one g' for which $h_{g'} \not\equiv 0 \bmod p$. For a natural number n let b_i, $1 \leqslant i \leqslant n$, be integers such that $0 \leqslant b_i \leqslant p-1$ and there is at least one i' for which $b_{i'} \neq 0$. Further, let $\gamma_1, \dots, \gamma_n$ be primitive elements for E/F that are mutually non-conjugate. The element

$$\prod_{1 \leqslant i \leqslant n} s(T+\gamma_i)^{b_i} = \prod_{1 \leqslant i \leqslant n} \prod_{g \in G} \bigl(T + g(\gamma_i)\bigr)^{b_i h_g}$$

cannot be the pth power of an element in the rational function field $E(T)$. This follows from the fact that the $(T + g'(\gamma_{i'}))$-adic valuation of $E(T)$ has a value on the above product that it is not divisible by p. Consequently the $p^n - 1$ polynomials

$$X^p - \prod_{1 \leqslant i \leqslant n} s(T+\gamma_i)^{b_i}$$

are irreducible in $E[X,T]$. Since F is Hilbertian, there exists an element $k \in F$ such that the polynomials

$$X^p - \prod_{1 \leqslant i \leqslant n} s(k+\gamma_i)^{b_i}$$

are irreducible in $E[X]$ (cf. for instance [F-J, Lemma 11.6 and Corollary 11.7]). Hence none of the elements

$$\prod_{1 \leqslant i \leqslant n} s(k+\gamma_i)^{b_i}$$

are pth powers of elements in E. If we set $\alpha_i := k + \gamma_i$, the elements $s(\alpha_i)$ modulo $E^{\times p}$ $(i = 1, \dots, n)$ thus are independent elements in the $\mathbb{F}_p$-space $E^\times / E^{\times p}$. Since n was an arbitrary natural number, the statement in the lemma follows. □

We are now in a position to prove Theorem 3.

Proof of Theorem 3. Let $f \in \mathrm{Hom}(G, \mathbb{F}_p^\times)$ be a homomorphism and let $b \in \mathbb{F}_p^\times$ be a generator of the image $f(G)$. The order d of b is a divisor of $p-1$. Let σ be an element in G for which $f(\sigma) = b$ and let H be the kernel of f. Then we can write $G = H \cup \sigma H \cup \sigma^2 H \cup \cdots \cup \sigma^{d-1} H$. For an element $\alpha \in E$, $H(\alpha)$ stands for the product $\prod_{h \in H} h(\alpha)$. For any α in E, the element

$$\beta := \sigma^{d-1} H(\alpha) \bigl(\sigma^{d-2} H(\alpha)\bigr)^b \bigl(\sigma^{d-3} H(\alpha)\bigr)^{b^2} \cdots \bigl(\sigma H(\alpha)\bigr)^{b^{d-2}} \bigl(H(\alpha)\bigr)^{b^{d-1}}$$

satisfies $\sigma(\beta) \in \beta^b E^{\times p}$ and hence $g(\beta) \in \beta^{f(g)} E^{\times p}$ for every $g \in G$. Therefore β modulo $E^{\times p}$ is in $\mathrm{Nor}^f(E/F)$. It now follows from Lemma 4 that the above β's modulo $E^{\times p}$ generate an infinite-dimensional subspace of the $\mathbb{F}_p$-space $E^\times / E^{\times p}$. □

We give some more applications of Lemma 4.

Theorem 5. *Let E/F be a finite Galois extension with Galois group G. If p is a prime number that does not divide the order of G, the $\mathbb{F}_p[G]$-module $E^\times/E^{\times p}$ is a direct sum of simple $\mathbb{F}_p[G]$-modules. If F is Hilbertian, each of the simple $\mathbb{F}_p[G]$-modules appears infinitely many times in the above decomposition.*

Proof. The first assertion is clear since, by Maschke's theorem, the group ring $\mathbb{F}_p[G]$ is semi-simple. The second assertion follows from the fact that any (left) simple $\mathbb{F}_p[G]$-module is the (left) annihilator of some idempotent in the group ring. Lemma 4 applied to this idempotent yields the assertion. □

If the Galois group G is Abelian and the exponent divides $p-1$, the simple $\mathbb{F}_p[G]$-modules are one-dimensional $\mathbb{F}_p$-spaces. The preceding theorem yields the following:

Theorem 6. *Let E/F be an Abelian extension such that the exponent of the Galois group G divides $p-1$. Then $E^\times/E^{\times p}$ is the direct sum of* $\mathrm{Nor}^f(E/F)$, *f running through* $\mathrm{Hom}(G, \mathbb{F}_p^\times)$. *Furthermore, when F is Hilbertian, each* $\mathrm{Nor}^f(E/F)$ *is an infinite-dimensional $\mathbb{F}_p$-space.*

In connection with the study of "Galois averages" (for instance characterizing the maximal intermediate field M in an Abelian extension E/F for which $M^\times/M^{\times p}$ is the direct sum of $\mathrm{Nor}^\varphi(M/F)$, φ running through the group $\mathrm{Hom}(\mathrm{Gal}(M/F), \mathbb{F}_p^\times)$), the following question arises (see [M, 3.9 and 3.10]): Let M/F be a finite extension and d an integer > 1. If $M^\times = F^\times M^{\times d}$ holds for the multiplicative groups, does this imply $M = F$? In general, this implication does not hold, as examples with local fields show. However, in the next theorem we shall show that it holds for "most" Hilbertian fields, namely for the Hilbertian fields that are finitely generated field extension of their prime field. These fields comprise the following fields:

- If $\mathrm{char}(F) = 0$, any algebraic number field and every finite algebraic extension of a non-trivial purely transcendental extension of $\mathbb{Q}$ of finite transcendency degree.
- If $\mathrm{char}(F) > 0$, any field that is a finitely generated but not an algebraic extension of its prime field.

In particular, every global field belongs to the above class of Hilbertian fields.

Theorem 7. *Let M be a finite separable extension of a Hilbertian field F which is finitely generated over its prime field. If for some integer $d > 1$ the equality $M^\times = F^\times M^{\times d}$ holds for the multiplicative groups of the fields, then $M = F$.*

Remark 8. In [M, Theorem 3.9], it is assumed that d is prime and $\mu_d \subset M$. These hypotheses have been removed in the above Theorem 7.

Proof of Theorem 7. F is a finite algebraic extension of one of the following fields: $\mathbb{Q}$, a non-trivial purely transcendental extension of $\mathbb{Q}$ of finite transcendency degree, or a non-trivial purely transcendental extension of a finite field of finite transcendency degree. Each of these fields has a family $\mathcal{M}$ of absolute values satisfying a product formula with positive exponents ℓ_v, $v \in \mathcal{M}$.

More concretely, this means that for any non-zero element a in the field, $|a|_v = 1$ for almost all $v \in \mathcal{M}$ and

$$\prod_{v\in\mathcal{M}} |a|_v^{\ell_v} = 1.$$

The extension of these absolute values to absolute values in F will satisfy a product formula of the same form as the v in $\mathcal{M}$. (Cf. for instance [L].) Since M/F is a finite separable extension, we can write $M = F(\alpha)$ for a suitable $\alpha \in M$. As follows from [D],[2] there exists a non-Archimedian absolute value v' of F such that the minimal polynomial $f(x)$ of α splits completely into $[M:F]$ distinct linear factors in the completion of F with respect to v'. This implies that v' has $[M:F]$ distinct prolongations to M. In our situation, v' can be taken to be a discrete rank one valuation. We write v' additively as a valuation w normalized so that $w(\pi) = 1$ for a uniformizing element $\pi \in F$.

The theorem will be proved by indirect argument. Suppose that the equality $M^\times = F^\times M^{\times d}$ holds with $n := [M:F] > 1$. Let $w_1, \dots, w_n$ be the n distinct prolongations of w to M. These valuations have the same value group as w has. By the approximation theorem, there exists an element $\beta \in M$ such that $w_1(\beta) = 1$ and $w_i(\beta) = 0$ for $2 \leqslant i \leqslant n$. The equality $M^\times = F^\times M^{\times d}$ implies that β can be written $\beta = \gamma\delta^d$ for a suitable $\gamma \in F$ and a suitable $\delta \in M$. Since $1 = w_1(\beta) = w_1(\gamma) + dw_1(\delta)$ and $0 = w_i(\beta) = w_i(\gamma) + dw_i(\delta)$ for $2 \leqslant i \leqslant n$, we conclude that

$$w_1(\gamma) \equiv 1 \pmod d$$

and

$$w_i(\gamma) \equiv 0 \pmod d \quad \text{for } 2 \leqslant i \leqslant n.$$

Since γ lies in F and $w_1, \dots, w_n$ have the same restriction to F, we have $w_1(\gamma) = w_i(\gamma)$ for $2 \leqslant i \leqslant n$, and thus the above congruences yield the desired contradiction. □

References

[D] A. Dress, Zu einem Satz aus der algebraischen Zahlentheorie, J. Reine Angew. Math. 216 (1964) 218–219.

[F-J] M. Fried, M. Jarden, Field Arithmetic, Springer, Berlin, 1986.

[L] S. Lang, Diophantine Geometry, Interscience, New York, 1962.

[M] R. Massy, Galois averages, J. Number Theory 113 (2005) 244–275.

[2] The authors are grateful to W.-D. Geyer for turning our attention to this paper which gives a much shorter proof than our original one.