ISRAEL JOURNAL OF MATHEMATICS, Vol. 55, No. 2, 1986

SOME PROPERTIES OF THE ABSOLUTE GALOIS GROUP OF A HILBERTIAN FIELD

BY
ZOÉ CHATZIDAKIS
Department of Mathematics, Fine Hall, Princeton University, Princeton, NJ 08544, USA

ABSTRACT

Let K be a hilbertian field, $G(K)$ its absolute Galois group. If K is countable, then for a.a. $\bar{\sigma}$ in $G(K)^e$, $N(\langle\bar{\sigma}\rangle)=\langle\bar{\sigma}\rangle$, $C(\bar{\sigma})=\langle\bar{\sigma}\rangle$ if $e=1$, $=(1)$ if $e>1$ and there is no intermediate field $K\subseteq M\subsetneqq K_S(\bar{\sigma})$ with $[K_S(\bar{\sigma}):M]<\infty$. Let $\bar{\sigma}\in G(K)^e$. Then for a.a. $\bar{\tau}$ in $G(K)^f$, $\langle\bar{\sigma}\rangle\cap\langle\bar{\tau}\rangle=(1)$.

Introduction

We consider a hilbertian field K and denote by K_S its separable closure and by $G(K)$ its absolute Galois group, i.e. the Galois group of K in its separable closure. As a compact group, $G(K)$ has then a unique normalized Haar measure μ.

Jarden studied in [3], [4], [5] the general behaviour of elements in $G(K)$. We list here some of the results he obtained, K being a hilbertian field, e and f positive integers:

THEOREM [3]. *If K is countable, then for almost all $\bar{\sigma}$ in $G(K)^e$, $K_S(\bar{\sigma})$ is* PAC.

Here $K_S(\bar{\sigma})$ denotes the subfield of K_S fixed by the e-tuple $\bar{\sigma}$. A field F is PAC iff every absolutely irreducible variety defined over F has an F-rational point. Note that the hypothesis of countability cannot be removed, see [6].

THEOREM [4]. *For almost all $\bar{\sigma}$ in $G(K)^e$, for almost all $\bar{\tau}$ in $G(K)^f$:*

(1) $\langle\bar{\sigma}\rangle\cong\hat{F}_e$ *($\langle\bar{\sigma}\rangle$ denotes the closed subgroup generated by $\bar{\sigma}$; $\hat{F}_e$ is the free profinite group on e generators).*

(2) *The normalizer of $\langle\bar{\sigma}\rangle$ in $G(K)$, $N(\langle\bar{\sigma}\rangle)$, has measure* 0.

(3) *If K is a global field, then the centralizer of $\langle\bar{\sigma}\rangle$ in $G(K)$, $C(\bar{\sigma})$, is $\langle\sigma\rangle$ if $e=1$, trivial if $e\geqq 2$.*

Received March 5, 1985 and in revised form January 20, 1986

(4) $\langle\bar{\sigma}\rangle \cap \langle\bar{\tau}\rangle = (1)$.

(5) $(e = 1)$. *There does not exist an intermediate field* $K \subseteq L \subsetneq K_S(\sigma)$ *such that* $[K_S(\sigma): L] < \infty$.

In [4], Jarden asked several questions about the behaviour of $\bar{\sigma}$. Using a Galois group construction over hilbertian fields, we are able to answer them. Our results are the following, for K a hilbertian field:

THEOREM 2.2. *If K is countable and e is a positive integer, then for almost all* $\bar{\sigma}$ *in* $G(K)^e$, $N(\langle\bar{\sigma}\rangle) = \langle\bar{\sigma}\rangle$.

COROLLARY 2.3. *If K, e are as above, then for almost all* $\bar{\sigma}$ *in* $G(K)^e$,

$$C(\bar{\sigma}) = \langle\sigma\rangle \qquad \text{if } e = 1,$$
$$= (1) \qquad \text{if } e \geqq 2.$$

THEOREM 2.5. *If K is countable and e is a positive integer, then for almost all* $\bar{\sigma}$ *in* $G(K)^e$, *there is no intermediate field* $K \subseteq M \subsetneq K_S(\bar{\sigma})$ *with* $[K_S(\bar{\sigma}): M] < \infty$.

This result was obtained independently by Haran [2] for an arbitrary hilbertian field. As our proof uses a different method, we will give it in this paper.

We are also able to answer by the affirmative Problem 7 in [4]. This leads us to a generalization of one of Jarden's results:

THEOREM 2.8. *Let e, f be positive integers,* $\bar{\sigma}$ *in* $G(K)^e$. *Then for almost all* $\bar{\tau}$ *in* $G(K)^f$, $\langle\bar{\sigma}\rangle \cap \langle\bar{\tau}\rangle = (1)$.

I would like to thank Professor Macintyre for having called my attention to these problems, and Professor Jarden for his comments and for giving me a simple proof of Corollary 2.3. I would also like to thank the referee for his helpful suggestions.

I. Preliminaries

(1.1) Let K be a field. Then $G(K)$ is a profinite group and hence is compact. There is therefore a unique way to define a Haar measure μ on $G(K)$ so that $\mu(G(K)) = 1$. If L is a finite separable extension of K, then $\mu(G(L)) = [L : K]^{-1}$. We complete μ by adding to the measurable sets all the subsets of sets of measure 0 and denote this completion also by μ. For e a positive integer, we also denote by μ the power measure on $G(K)^e$.

We will often use the following generalization of Lemma 4.1 of [4]:

LEMMA. *Let K be a field, L a finite Galois extension of K. Suppose that $(M_i)_{i<\omega}$ is a sequence of finite Galois extensions of K, which contain L and are linearly disjoint over L. Let $e \geqq 1$, $\bar{\sigma}$ in* $\mathrm{Gal}(L/K)^e$ *and for each $i < \omega$, let $\bar{A}_i$ be a nonempty subset of* $\mathrm{Gal}(M_i/K)^e$ *consisting of extensions of $\bar{\sigma}$, and let $A_i = \{\bar{\tau} \in G(K)^e ; \bar{\tau}|_{M_i} \in \bar{A}_i\}$. If $\Sigma_{i\in\omega}[M_i : L]^{-e} = \infty$, then $\mu(\bigcup_{i\in\omega} A_i) = [L : K]^{-e}$.*

PROOF. W.l.o.g. we can suppose that $\bar{\sigma}$ is the identity element of $G(L/K)^e$, and thus that A_i is contained in $G(L)^e$. As $\mu(G(L)^e) = [L : K]^{-e}$, the result follows by Lemma 4.1 of [4].

(1.2) K is called hilbertian if it has the following property:

For every irreducible polynomial $f(T, X)$ in $K[T, X]$, one can find infinitely many elements a in K such that $f(a, X)$ is irreducible in $K[X]$.

Equivalently, one can replace T and X in the definition by sequences $T_1, \ldots, T_m$, $X_1, \ldots, X_n$ (see [7]). Examples of hilbertian fields are: $\mathbf{Q}$, $\mathbf{Q}^{ab}$, any function field $K(T)$. A finite extension of a hilbertian field is hilbertian.

(1.3) One of the well-known properties of hilbertian fields concerns solutions to embedding problems.

Let K be a hilbertian field, L a finite Galois extension of K and $p : G \to \mathrm{Gal}(L/K)$ an epimorphism of finite groups. Let $\bar{t}$ be a finite set of indeterminates; we then have a natural isomorphism between $\mathrm{Gal}(L/K)$ and $\mathrm{Gal}(L(\bar{t})/K(\bar{t}))$.

Suppose now that we can find a Galois extension M' of $K(\bar{t})$ which contains $L(\bar{t})$, and a group isomorphism $s : \mathrm{Gal}(M'/K(\bar{t})) \to G$ such that the following diagram commutes:

$$\begin{array}{ccc} & & \mathrm{Gal}(M'/K(\bar{t})) \\ & \swarrow^{s} & \downarrow \mathrm{res}_{L(\bar{t})} \\ G & \xrightarrow{p} & \mathrm{Gal}(L(\bar{t})/K(\bar{t})). \end{array}$$

Because K is hilbertian, we can then find a Galois extension M of K, which contains L, and a group isomorphism $s : \mathrm{Gal}(M/K) \to G$ such that the following diagram commutes:

$$\begin{array}{ccc} & & \mathrm{Gal}(M/K) \\ & \swarrow^{s} & \downarrow \mathrm{res}_{L} \\ G & \xrightarrow{p} & \mathrm{Gal}(L/K). \end{array}$$

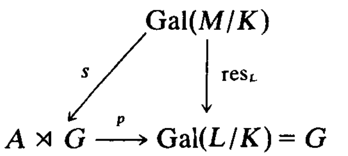
(1.4) Let m be a positive integer and let $\mathbf{Z}_m$ be the cyclic group of order m. Let G be a finite group. We can then view the group-ring $\mathbf{Z}_m[G]$ as a G-module, the action of G on it being multiplication on the right. 0 will denote the identity element of the additive group $\mathbf{Z}_m[G]$; 1 will denote the unit of the ring $\mathbf{Z}_m[G]$.

If A is a G-module, we can then form the semi-direct product $A \rtimes G$, where the universe is $A \times G$, and the group law is defined by:

$$(a, g)(b, h) = (a^h + b, gh)$$

for a, b in A, g, h in G (the group law in A is denoted additively; the group law in G is denoted multiplicatively; $(0, 1)$ is the identity element of $A \rtimes G$).

(1.5) Lemma [9, p. 91]. *Let K be a hilbertian field and let L be a finite Galois extension with Galois group G. Let A be a finite G-module. One can then find a Galois extension M of K containing L such that the following diagram commutes:*

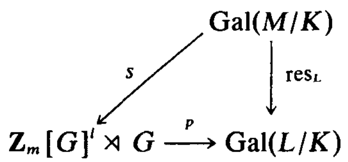


where s is a group isomorphism and p is the natural projection: $p(a, g) = g$.

(1.6) We will constantly use the following consequence of Lemma 1.5:

Corollary. *Let K be a hilbertian field, $L \subset L'$ two finite Galois extensions of K with $\mathrm{Gal}(L/K) = G$. Let m, l, n be integers.*

(1) *There is a Galois extension M of K which contains L and is linearly disjoint from L' over L, such that the following diagram commutes:*



for some group isomorphism s.

(2) *There is a Galois extension M of K which is linearly disjoint from L over K, with $\mathrm{Gal}(M/K) \cong S_n$ (the permutation group on n letters).*

Proof. (1) Let $H = \mathrm{Gal}(L'/K)$, $N = \mathrm{Gal}(L'/L)$. We then view $\mathbf{Z}_m[G]^l$ as an H-module, the action of H being induced by the epi $\mathrm{res}_L : H \to G$. Note that N acts trivially on $\mathbf{Z}_m[G]^l$. By Lemma (1.5), we can therefore obtain Galois extensions M' and M such that the following diagram commutes:

$$\begin{array}{ccc} \mathrm{Gal}(M'/K) = \mathbf{Z}_m[G]^l \rtimes H & \xrightarrow{\mathrm{res}_{L'}} & H = \mathrm{Gal}(L'/K) \\ \downarrow \mathrm{res}_M & & \downarrow \mathrm{res}_L \\ \mathrm{Gal}(M/K) = \mathbf{Z}_m[G]^l \rtimes G & \xrightarrow{\mathrm{res}_{L'}} & G = \mathrm{Gal}(L/K) \end{array}$$

M being the subfield of M' fixed by the subgroup $0 \rtimes N$ of $\mathbf{Z}_m[G]^l \rtimes H$; the horizontal maps are the natural projections on the second coordinate.

As $N = \mathrm{Gal}(L'/L)$ acts trivially on $\mathbf{Z}_m[G]^l$, $\mathrm{Gal}(M'/L) = \mathbf{Z}_m[G]^l \times N$, and thus L' and M are linearly disjoint over L.

(2) Let $t_1, \ldots, t_n$ be new indeterminates, let M' be the splitting field over $K(\bar{t})$ of the equation $X^n + t_1X^{n-1} + \cdots + t_n$. It is well known that $\mathrm{Gal}(M'/K(\bar{t})) \cong S_n$. M' and $L(\bar{t})$ are also linearly disjoint over $K(\bar{t})$. As K is hilbertian, we can therefore find an M satisfying the conclusion.

II. Proof of the theorems

(2.1) LEMMA. *Let m, e be integers, $m > 1$; let G be a finite group and take $g_1, \ldots, g_e$ in G. We then consider the group $\mathbf{Z}_m[G] \rtimes G$ and the natural projection $p : \mathbf{Z}_m[G] \rtimes G \to G$. Let H be the subgroup of G generated by $g_1, \ldots, g_e$, H' the subgroup of $\mathbf{Z}_m[G] \rtimes G$ generated by the elements $(1, g_1), \ldots, (1, g_e)$. Then*

$$p(N(H')) \subseteq H.$$

PROOF. As H is a subgroup of G, we can look at the subgroup $\mathbf{Z}_m[H] \rtimes H$ of $\mathbf{Z}_m[G] \rtimes G$. We first note that $H' \subseteq \mathbf{Z}_m[H] \rtimes H$ because $\mathbf{Z}_m[H] \rtimes H$ contains the elements $(1, g_1), \ldots, (1, g_e)$.

Suppose now that

$$(a, h)^{-1}(1, g_1)(a, h) = (b, g') \in H'.$$

We then get:

$$(b, g') = (-ah^{-1}g_1h + h + a, h^{-1}g_1h).$$

Hence $g' = h^{-1}g_1h$ and $b = -ag' + h + a$, i.e., $(h - b) = a(g' - 1)$.

Let n be the order of g'. Then

$$\begin{aligned} (h - b)(1 + g' + \cdots + g'^{n-1}) &= a(g'^n - 1) \\ &= 0 \end{aligned}$$

$$h(1 + g' + \cdots + g'^{n-1}) = b(1 + g' + \cdots + g'^{n-1}).$$

As $b \in \mathbf{Z}_m[H]$, $g' \in H$ and the left-hand side of the equation is non-zero, we must have: $h \in H$.

(2.2) THEOREM. *Let K be a countable hilbertian field, let $e \geqq 1$. Then for almost all $\sigma_1, \ldots, \sigma_e$ in $G(K)^e$ we have $N(\langle\sigma_1, \ldots, \sigma_e\rangle) = \langle\sigma_1, \ldots, \sigma_e\rangle$.*

PROOF. For each finite Galois extension L of K, let

$$T_L = \{\bar\sigma \in G(K)^e\,;\ \text{there is } M \supset L \text{ finite Galois over } K \text{ such that } \operatorname{res}_L(N(\langle\bar\sigma_{|M}\rangle)) \subseteq \langle\bar\sigma_{|L}\rangle\}.$$

We claim that $\mu(T_L) = 1$. Let $\bar\tau \in G(L/K)^e$. By (1.6) and Lemma 2.1, we can then find a finite Galois extension M_1 of K containing L, and $\bar\sigma_1$ in $\mathrm{Gal}(M_1/K)^e$ such that

(1) $\bar\sigma_1 \big|_L = \bar\tau$,

(2) $\operatorname{res}_L(N(\langle\bar\sigma_1\rangle)) \subseteq \langle\bar\tau\rangle$.

We now use repeatedly (1.6) and (2.1) to obtain a sequence M_i, $i < \omega$ of finite Galois extensions of K containing L and $\bar\sigma_i$ in $\mathrm{Gal}(M_i/K)^e$ such that:

(1) $\bar\sigma_i \big|_L = \bar\tau$.

(2) $\operatorname{res}_L(N(\langle\bar\sigma_i\rangle)) \subseteq \langle\bar\tau\rangle$.

(3) M_i is linearly independent of $M_1 \cdots M_{i-1}$ over L.

(4) $[M_i : L] = [M_1 : L]$.

The fields M_i are therefore linearly independent over L, and by Lemma 1.1, the set $\{\bar\sigma \in G(K)^e\,;\ \bar\sigma \big|_{M_i} = \bar\sigma_i$ for some $i < \omega\}$ has therefore measure $[L:K]^{-e}$. The union of all these sets for $\bar\tau$ ranging over $\mathrm{Gal}(L/K)^e$ has therefore measure 1; clearly it is contained in T_L and therefore $\mu(T_L) = 1$.

Let $T = \bigcap T_L$ where L ranges over all finite Galois extensions of K. As K is countable, $\mu(T) = 1$. If $\bar\sigma$ is an element of T, we claim that $N(\langle\bar\sigma\rangle) = \langle\bar\sigma\rangle$.

Otherwise, let $\tau \in N(\langle\bar\sigma\rangle)$, $\tau \notin \langle\bar\sigma\rangle$. Then for some finite Galois extension L of K, $\tau \big|_L \notin \langle\bar\sigma \big|_L\rangle$. As $\bar\sigma \in T_L$, we reach a contradiction.

(2.3) COROLLARY. *Let K be countable hilbertian, let $e \geqq 1$. Then for almost all $\bar\sigma$ in $G(K)^e$,*

$$C(\bar\sigma) = \langle\sigma\rangle \qquad \text{if } e = 1$$

$$= (1) \qquad \text{if } e > 1.$$

PROOF. By 2.2, we know that for almost all $\bar\sigma$ in $G(K)^e$, $N(\langle\bar\sigma\rangle) = \langle\bar\sigma\rangle$. As $C(\bar\sigma) \subseteq N(\langle\bar\sigma\rangle)$, we get $C(\bar\sigma) \subseteq \langle\bar\sigma\rangle$ for a.a. $\bar\sigma$ in $G(K)^e$.

If $e = 1$, then clearly $C(\sigma) = \langle\sigma\rangle$.

If $e > 1$, then by a result of Jarden, for a.a. $\bar\sigma$ in $G(K)^e$, $\langle\bar\sigma\rangle \cong \hat F_e$. But the center of $\hat{F}_e$ is trivial for $e \geqq 2$ (see [4]). Hence for almost all $\bar{\sigma}$ in $G(K)^e$, for $e \geqq 2$, $C(\langle\bar{\sigma}\rangle) = (1)$.

(2.4) LEMMA. *Let m, e be integers, $m > 1$, $e \geqq 1$; let G be a finite group and take $g_1, \ldots, g_e$ in G. We now consider the group $\mathbf{Z}_m[G] \rtimes G$. Let H be the subgroup of G generated by $g_1, \ldots, g_e$, H' the subgroup of $\mathbf{Z}_m[G] \rtimes G$ generated by $(1, g_1), \ldots, (1, g_e)$. Then for all g in $G \setminus H$, for all a in $\mathbf{Z}_m[G]$, $[\langle (a, g), H' \rangle : H'] > [\langle g, H \rangle : H]$.*

PROOF. As in Lemma 2.1, we can prove that H' is contained in the subgroup $\mathbf{Z}_m[H] \rtimes H$ of $\mathbf{Z}_m[G] \rtimes G$.

Let n be the order of g_1. Then

$$(1, g_1)^n = (1 + g_1 + \cdots + g_1^{n-1}, 1).$$

$$(a, g)^{-1}(1, g_1)^n (a, g) = ((1 + g_1 + \cdots + g_1^{n-1})g, 1).$$

Thus $(a, g)^{-1}(1, g_1)^n (a, g)$ is an element of $\langle (a, g), H' \rangle$ but does not belong to $\mathbf{Z}_m[H] \rtimes H$ because $g \notin H$. Pick elements (a_i, h_i), $i = 1, \ldots, r$ in $\langle (a, g), H' \rangle$ such that the elements h_i form a set of coset representatives of H in $\langle g, H \rangle$, $(a_1, h_1) = (0, 1)$. Then the cosets $(a_i, h_i)\mathbf{Z}_m[H] \rtimes H$, $i = 1, \ldots, r$ and $(a, g)^{-1}(1, g_1)^n (a, g)\mathbf{Z}_m[H] \rtimes H$ are distinct; as H' is contained in $\mathbf{Z}_m[H] \rtimes H$, this gives us $[\langle (a, g), H' \rangle : H'] > r = [\langle g, H \rangle : H]$.

(2.5) THEOREM. *Let K be countable hilbertian, let $e \geqq 1$. Then for almost all $\bar{\sigma}$ in $G(K)^e$, if M is a proper subfield of $K_S(\bar{\sigma})$ containing K, then $[K_S(\bar{\sigma}) : M]$ is infinite.*

PROOF. For each finite Galois extension L of K, let

$$T_L = \{\bar{\sigma} \in G(K)^e \,;\, \text{there is } M \supset L \text{ finite Galois over } K \text{ such that for all } \tau \text{ in } \mathrm{Gal}(M/K), \text{ either } \tau\restriction_L \in \langle \bar{\sigma}\restriction_L \rangle \text{ or } [\langle \bar{\sigma}\restriction_M, \tau\restriction_M \rangle : \langle \bar{\sigma}\restriction_M \rangle] > [\langle \bar{\sigma}\restriction_L, \tau\restriction_L \rangle : \langle \bar{\sigma}\restriction_L \rangle]\}.$$

Then $\mu(T_L) = 1$. The proof is similar to the one given in Theorem 2.2. It uses Lemma 2.4 instead of Lemma 2.1.

Let $T = \bigcap T_L$ where L ranges over all finite Galois extensions of K; $\mu(T) = 1$; let $\bar{\sigma}$ be an element of T and let $\tau \in G(K)$, $\tau \notin \langle \bar{\sigma} \rangle$. We can then find a finite Galois extension M of K such that $\tau\restriction_M \notin \langle \bar{\sigma}\restriction_M \rangle$. Using the fact that $\bar{\sigma} \in \bigcap T_L$, we can therefore find a sequence of finite Galois extensions of K, M_i, $i < \omega$ which contain M and satisfy:

(1) $M_i \subset M_{i+1}$.

(2) $[\langle \bar\sigma \restriction_{M_i}, \tau \restriction_{M_i} \rangle : \langle \bar\sigma \restriction_{M_i} \rangle] < [\langle \bar\sigma \restriction_{M_{i+1}}, \tau \restriction_{M_{i+1}} \rangle : \langle \bar\sigma \restriction_{M_{i+1}} \rangle]$.
Therefore $[\langle \bar\sigma, \tau \rangle : \langle \bar\sigma \rangle]$ is infinite.

(2.6) LEMMA. *Let G be a finite group, let f be a positive integer, $l \geqq f2^{|G|}$. Then for all $a_1, \ldots, a_f$ in $\mathbf{Z}_2[G]^l$, we can find G-submodules N_1, N_2 of $\mathbf{Z}_2[G]^l$, such that*
(1) $\mathbf{Z}_2[G]^l = N_1 \oplus N_2$,
(2) $a_1, \ldots, a_f \in N_1$,
(3) *N_2 is a free $\mathbf{Z}_2[G]$-module of rank $\geqq l - f2^{|G|}$.*

PROOF. We use induction on f. For $f = 1$ let $a = a_1$. Let $\{e_1, \ldots, e_l\}$ be a basis of $\mathbf{Z}_2[G]^l$, and write a as $(b_1, \ldots, b_l)$ with respect to the basis $\{e_1, \ldots, e_l\}$. For c in $\mathbf{Z}_2[G]$, define $I_c = \{i ; b_i = c\}$ and let N_c be the G-submodule of $\mathbf{Z}_2[G]^l$ generated by $\{e_i ; i \in I_c\}$. If I_c is non-empty, pick an element i_c in it. Then the elements $\Sigma_{i \in I_c} e_i$ and $e_j, j \neq i_c, j \in I_c$ form a basis for N_c.

Let N_1 be the G-submodule of $\mathbf{Z}_2[G]^l$ generated by the elements $\Sigma_{i \in I_c} e_i$ for c in $\mathbf{Z}_2[G]$, let N_2 be the G-submodule generated by the elements $\{e_j ; j \neq i_c$ for all c in $\mathbf{Z}_2[G]\}$. Then $\mathbf{Z}_2[G] = N_1 \oplus N_2$, $a \in N_1$, N_2 is free of rank $\geqq l - |\mathbf{Z}_2[G]| = l - 2^{|G|}$.

For $f > 1$, suppose that we have found G-submodules N_1', N_2' of $\mathbf{Z}_2[G]^l$ such that $\mathbf{Z}_2[G]^l = N_1' \oplus N_2'$, $a_1, \ldots, a_{f-1} \in N_1'$ and N_2' is a free $\mathbf{Z}_2[G]$-module of rank $\geqq l - (f-1)2^{|G|}$. Let $a_f = b_1 + b_2$ where $b_1 \in N_1'$, $b_2 \in N_2'$. By the case $f = 1$, we can then find G-submodules M_1, N_2 of N_2' such that $b_2 \in M_1$, $M_1 \oplus N_2 = N_2'$ and N_2 is a free $\mathbf{Z}_2[G]$-module of rank $\geqq l - (f-1)2^{|G|} - 2^{|G|} = l - f2^{|G|}$. Take $N_1 = N_1' \oplus M_1$.

(2.7) LEMMA. *Let G be a finite group, $g_1, \ldots, g_f$, $h_1, \ldots, h_e$ elements of G, $l = f + e2^{|G|}$. Then for all $a_1, \ldots, a_e$ in $\mathbf{Z}_2[G]^l$, we can find $b_1, \ldots, b_f$ in $\mathbf{Z}_2[G]^l$ such that in the group $\mathbf{Z}_2[G]^l \rtimes G$*

$$\langle (b_1, g_1), \ldots, (b_f, g_f) \rangle \cap \langle (a_1, h_1), \ldots, (a_e, h_e) \rangle = (1).$$

PROOF. Use Lemma 2.6 to find G-submodules N_1 and N_2 of $\mathbf{Z}_2[G]^l$ such that
(1) $\mathbf{Z}_2[G]^l = N_1 \oplus N_2$,
(2) $a_1, \ldots, a_e \in N_1$,
(3) N_2 is free of rank f.
Let $\{e_1, \ldots, e_f\}$ be a basis for N_2 and let b_i be the element $(0, e_i)$ of $N_1 \oplus N_2 \cong N_1 \times N_2$, for $i = 1, \ldots, f$. Let $w(X_1, \ldots, X_f)$ be a word in $X_1, \ldots, X_f$ and suppose that

$$w((0, e_1, g_1), \ldots, (0, e_f, g_f)) = (0, b, g) \in \langle (a_1, 0, h_1), \ldots, (a_e, 0, h_e) \rangle$$

in $\mathbf{Z}_2[G]^l \rtimes G \cong (N_1 \times N_2) \rtimes G$. Then $b = 0$.

Placing ourselves in the subgroup $N_2 \rtimes G$ of $(N_1 \times N_2) \rtimes G$ it therefore suffices to prove that if $w((e_1, g_1), \ldots, (e_f, g_f)) = (0, g)$ then $g = 1$. Because the order of each (e_i, g_i) is finite, we can assume that $w(X_1, \ldots, X_f)$ is of the form

$$X_1^{a_{1,1}} X_2^{a_{2,1}} \cdots X_f^{a_{f,1}} X_1^{a_{1,2}} X_2^{a_{2,2}} \cdots X_f^{a_{f,2}} \cdots X_1^{a_{1,r}} X_2^{a_{2,r}} \cdots X_f^{a_{f,r}}$$

where the $a_{i,j}$ are positive integers.

We now view $\mathbf{Z}_2[G]^f \rtimes G$ as $(\mathbf{Z}_2[G] \times \mathbf{Z}_2[G] \times \cdots \times \mathbf{Z}_2[G]) \rtimes G$, and we look at the ith coordinate of $w((e_1, g_1), \ldots, (e_f, g_f))$ for $1 \leqq i \leqq f$. We then get:

$$(1)\quad (1 + g_1 + \cdots + g_1^{a_{1,1}-1}) g_2^{a_{2,1}} \cdots g_f^{a_{f,r}} + \cdots + (1 + g_1 + \cdots + g_1^{a_{1,r}-1}) g_2^{a_{2,r}} \cdots g_f^{a_{f,r}} = 0,$$

$$(2)\quad (1 + g_2 + \cdots + g_2^{a_{2,1}-1}) g_3^{a_{3,1}} \cdots g_f^{a_{f,r}} + \cdots + (1 + g_2 + \cdots + g_2^{a_{2,r}-1}) g_3^{a_{3,r}} \cdots g_f^{a_{f,r}} = 0,$$

$\vdots$

$$(f)\quad (1 + g_f + \cdots + g_f^{a_{f,1}-1}) g_1^{a_{1,2}} \cdots g_f^{a_{f,r}} + \cdots + (1 + g_f + \cdots + g_f^{a_{f,r}-1}) = 0.$$

We now multiply the equation (i) on the left by $(1 - g_i)$ and get (we are in characteristic 2):

$$(1')\qquad (1 + g_1^{a_{1,1}}) g_2^{a_{2,1}} \cdots g_f^{a_{f,r}} + \cdots + (1 + g_1^{a_{1,r}}) g_2^{a_{2,r}} \cdots g_f^{a_{f,r}} = 0,$$

$$(2')\qquad (1 + g_2^{a_{2,1}}) g_3^{a_{3,1}} \cdots g_f^{a_{f,r}} + \cdots + (1 + g_2^{a_{2,r}}) g_3^{a_{3,r}} \cdots g_f^{a_{f,r}} = 0,$$

$\vdots$

$$(f')\qquad (1 + g_f^{a_{f,1}}) g_1^{a_{1,2}} \cdots g_f^{a_{f,r}} + \cdots + (1 + g_f^{a_{f,r}}) = 0.$$

For $1 < i \leqq f$, $1 \leqq j \leqq r$ the term $g_i^{a_{i,j}} \cdots g_f^{a_{f,r}}$ occurs exactly twice in this system: once in the summand $(1 + g_{i-1}^{a_{i-1,j}}) g_i^{a_{i,j}} \cdots g_f^{a_{f,r}}$ of equation $((i-1)')$, once in the summand $(1 + g_i^{a_{i,j}}) g_{i+1}^{a_{i+1,j}} \cdots g_f^{a_{f,r}}$ if $i < f$ or $(1 + g_i^{a_{i,j}}) g_1^{a_{1,j+1}} \cdots g_f^{a_{f,r}}$ if $i = f$, $j < r$ or $(1 + g_f^{a_{f,r}})$ if $i = 1$, $j = r$ of equation (i'). Also if $i = 1$, $1 < j \leqq r$ the term $g_1^{a_{1,j}} \cdots g_f^{a_{f,r}}$ occurs exactly twice in this system: once in the summand $(1 + g_1^{1,j}) g_2^{2,j} \cdots g_f^{f,r}$ of equation $(1')$, once in the summand $(1 + g_f^{f,j-1}) g_1^{1,j} \cdots g_f^{f,r}$ of equation (f').

Adding up the equations $(1')$ through (f'), we therefore get $1 + g_1^{a_{1,1}} \cdots g_f^{a_{f,r}} = 0$, i.e. $g = 1$.

Corollary. *Let K be a hilbertian field, L a finite Galois extension of K and $\sigma_1, \ldots, \sigma_e, \tau_1, \ldots, \tau_f$ in* $\mathrm{Gal}(L/K)$. *We can then find a finite Galois extension M of K which contains L, and extensions $\sigma_1', \ldots, \sigma_e', \tau_1', \ldots, \tau_f'$ of $\sigma_1, \ldots, \sigma_e, \tau_1, \ldots, \tau_f$ to M such that*

$$\langle \sigma_1', \ldots, \sigma_e' \rangle \cap \langle \tau_1', \ldots, \tau_f' \rangle = (1).$$

Proof. By (1.6), we can find a Galois extension M of K which contains L and such that the following diagram commutes:

$$\begin{array}{ccc} & & \mathrm{Gal}(M/K) \\ & \swarrow^{s} & \downarrow{\scriptstyle \mathrm{res}_L} \\ \mathbf{Z}_2[G]^e \rtimes G & \xrightarrow{\ p\ } & \mathrm{Gal}(L/K) = G \end{array}$$

where s is some group isomorphism and p is the natural projection. Extend $\tau_1, \ldots, \tau_f$ in such a way that $\langle \tau_1', \ldots, \tau_f' \rangle \subseteq 0 \rtimes G$. Let $\{e_1, \ldots, e_e\}$ be the natural basis of $\mathbf{Z}_2[G]^e$ and let $\sigma_i' = (e_i, \sigma_i)$. Then by the Lemma,

$$\langle \sigma_1', \ldots, \sigma_e' \rangle \cap \langle \tau_1', \ldots, \tau_f' \rangle = (1).$$

This corollary gives an affirmative answer to Problem 7 in [4] and can then be used to prove one of Jarden's results, that if K is hilbertian, then for a.a. $\bar{\sigma}$, $\bar{\tau}$ in $G(K)^{e+f}$, $\langle \bar{\sigma} \rangle \cap \langle \bar{\tau} \rangle = (1)$.

(2.8) THEOREM. *Let K be a hilbertian field, $\bar{\sigma}$ in $G(K)^e$, $f \geqq 1$. Then for almost all $\bar{\tau}$ in $G(K)^f$, $\langle \bar{\sigma} \rangle \cap \langle \bar{\tau} \rangle = (1)$.*

PROOF. Let $w_i(X_1, \ldots, X_f)$, $i < \omega$ be an enumeration of all the words in $X_1, \ldots, X_f$.

Let $T_i = \{\bar{\tau} \in G(K)^f;\ w_i(\bar{\tau}) \notin \langle \bar{\sigma} \rangle\}$. We claim that $\mu(T_i) = 1$. Pick n sufficiently large so that one can find in S_n elements $g_1, \ldots, g_f$ such that $w_i(g_1, \ldots, g_f) \neq 1$. By (1.6) we can now find finite Galois extensions $N_1 \subset M_1$ of K such that the following diagram commutes:

$$\begin{array}{ccc} \mathrm{Gal}(M_1/K) & \xrightarrow{\mathrm{res}_{N_1}} & \mathrm{Gal}(N_1/K) \\ \downarrow & & \downarrow \\ \mathbf{Z}_2[S_n]^l \rtimes S_n & \xrightarrow{\ p\ } & S_n \end{array}$$

where p is the natural projection, the vertical arrows are group isomorphisms and $l = f + e2^{|G|}$. By Lemma 2.8, we can therefore find $g_1', \ldots, g_f'$ in $\mathbf{Z}_2[S_n]^l \rtimes S_n$ such that $p(g_i') = g_i$ and $w_i(g_1', \ldots, g_f') \notin \langle \bar{\sigma} |_{M_1} \rangle$. We now iterate this construction to obtain a sequence M_j, $j < \omega$ of Galois extensions of K, elements $\bar{g}_j'$ in $\mathrm{Gal}(M_j/K)^f$ such that

(1) The M_j are linearly independent over K.

(2) $[M_j : K] = [M_1 : K]$.

(3) $w_i(\bar{g}_j') \notin \langle \bar{\sigma} |_{M_j} \rangle$.

By Lemma 1.1, $\mu(T_i) = 1$. Let $T = \bigcap_{i<\omega} T_i$. Then $\mu(T) = 1$ and any element $\bar{\tau}$ in T satisfies $\langle \bar{\sigma} \rangle \cap \langle \bar{\tau} \rangle = (1)$.

REFERENCES

1. M. Fried and M. Jarden, *Field Arithmetic*, to appear.

2. D. Haran, *The Bottom Theorem*, Israel J. Math., to appear.

3. M. Jarden, *Elementary statements over large algebraic fields*, Trans. Am. Math. Soc. **164** (1972), 67–91.

4. M. Jarden, *Algebraic extensions of finite corank of hilbertian fields*, Israel J. Math. **18** (1974), 279–307.

5. M. Jarden, *Intersections of conjugate fields of finite corank over hilbertian fields*, J. London Math. Soc. **17** (1978), 393–396.

6. M. Jarden and S. Shelah, *Pseudo algebraically closed fields over rational function fields*, Proc. Am. Math. Soc. **87** (1983), 223–228.

7. S. Lang, *Fundamentals of Diophantine Geometry*, Springer-Verlag, Berlin, 1983.

8. S. Lang, *Algebra*, Addison-Wesley, 1984.

9. K. Uchida, *Separably hilbertian fields*, Kodai Math. J. **3** (1980), 83–95.