Math Ann 216, 99—104 (1975)

Abelian Extensions of Arbitrary Fields

W. Kuyk and H. W. Lenstra, Jr.

0. Introduction and Summary

Let k be an Hilbertian field, i.e. a field for which Hilbert's irreducibility theorem holds (cf. [1, 5]). It is obvious that the degree of the algebraic closure $\bar{k}$ of k is infinite with respect to k. It is not obvious that the same is true for the maximal p-extension of k, p a prime number. Let A be a finite abelian group. The question whether there exists a Galoisian extension l/k with Galois group A is, classically, known to be solvable if there exists a finite group G, and a surjective homomorphism $G \to A$, such that the following condition is satisfied. Suppose M is a faithful $k[G]$-module, and let $S_k(M)$ denote its symmetric algebra over k. The group G acts upon $S_k(M)$ and on its field of quotients $k(M)$ in a natural way. Then the condition is that the subfield $k(M)^G$ of $k(M)$ of all G-invariants is a purely transcendental field extension of k (cf. [6, 5]). This applies in particular to the case $G=A$, and M is the group ring $k[A]$. In that case we denote $k(M)^G$ by k_A.

Let k be an arbitrary field. Recently, the second named author [4] gave necessary and sufficient conditions in order that, for given k and A, the extension k_A/k is purely transcendental, as follows. To check the pure transcendency of k_A one has to look at a finite set of Dedekind domains $D_{q(A)} = \mathbf{Z}[\zeta_{q(A)}]$, where the positive integer $q(A)$ runs through a finite subset of $\mathbf{Z}$ and $\zeta_{q(A)}$ is a primitive $q(A)$-th root of unity. Then one can determine in every $D_{q(A)}$ an ideal $I_{q(A)}$ with the property: k_A is purely transcendental over k if and only if the two following conditions are satisfied:

(i) every ideal $I_{q(A)}$ is a principal ideal,

(ii) if 2^r is the highest power of 2 dividing the exponent of A and if the characteristic of k is not equal to 2, then the extension $k(\zeta_{2^r})/k$ has cyclic Galois group.

This leads to

Theorem 1 ([4], Corollary (7.5)). *Let A be a finite abelian group. Let k be any field satisfying the condition (ii) above. There exists a natural number n such that the field of invariants k_{A^n} of the group $A^n = A \oplus \ldots \oplus A$ is a purely transcendental extension of k.*

A quadruple (G, ϕ, A, k), with $\phi: G \to A$ a surjective continuous homomorphism of (not necessarily abelian) (pro-)finite groups and k a field, is called a *Galoisian extension problem*. Such an extension problem is said to be solvable if for every Galoisian extension field l/k with $\mathrm{Gal}(l/k) \cong A$, there exists a Galoisian extension m/k, $m \supset l$, such that $\mathrm{Gal}(m/k) \cong G$ and the Galois map $\mathrm{Gal}(m/k) \to \mathrm{Gal}(l/k)$ coincides with ϕ.

For $G=\mathbf{Z}/p^m\mathbf{Z}, A=\mathbf{Z}/p^n\mathbf{Z}$, p a prime number, n and m positive integers satisfying $m\geqq n\geqq 1$, we denote the natural surjective homomorphism $G\to A$ by ϕ_{mn}, if $G=\mathbf{Z}_p$, the additive group of p-adic integers, then we write $\phi_{\infty n}$ instead of ϕ_{mn} It is clear that the problem $P(m, n, k)=(\mathbf{Z}/p^m\mathbf{Z}, \phi_{mn}, \mathbf{Z}/p^n\mathbf{Z}, k)$ is solvable for all m and n, if and only if the problem $P(\infty, n, k)=(\mathbf{Z}_p, \phi_{\infty n}, \mathbf{Z}/p^n\mathbf{Z}, k)$ is solvable for all $n\geqq 1$ With these notations we prove

Theorem 2. *Let k be any field If $p=\mathrm{char}(k)$, then the extension problem $P(\infty, n, k)$ is solvable for all positive integers $n\geqq 1$ If $p\neq\mathrm{char}(k)$, let E_p denote the set $\{x \mid x^{p^m}=1\in K$ for some $m\in\mathbf{Z}, m\geqq 0\}$ of all p^m-th roots of unity, and put $K=k(E_p)$ Furthermore, suppose that the degree $[K\ k]$ of K/k is finite If $p\neq 2$ then the extension problem $P(\infty, n, k)$ is solvable for all $n\geqq 1$ If $p=2$, then let l/k be Galois with $\mathrm{Gal}(l/k)=\mathbf{Z}/2^n\mathbf{Z}, n>1$ Then k admits a $\mathbf{Z}_2$-extension If, on the contrary, $[K\ k]$ is infinite, then there exists at least one Galois extension of k with Galois group isomorphic to $\mathbf{Z}_p$*

Corollary 1. *Let k be a field, and let p be a prime number $\neq 2$ The following conditions (i) and (ii) are equivalent*

(i) *there exists a Galois extension l/k with $\mathrm{Gal}(l/k)\cong\mathbf{Z}/p\mathbf{Z}$,*

(ii) *there exists a Galois extension l/k with $\mathrm{Gal}(l/k)\cong\mathbf{Z}_p$*

For $p=2$ there is equivalence between

(iii) *there exists a Galois extension l/k with $\mathrm{Gal}(l/k)\cong\mathbf{Z}/4\mathbf{Z}$,*

(iv) *there exists a Galois extension l/k with $\mathrm{Gal}(l/k)\cong\mathbf{Z}_2$*

Putting Theorems 1 and 2 together we get

Corollary 2. *Let k be an Hilbertian field and let A be a finite abelian group satisfying the condition (ii) above*

There exists a Galois extension l/k with $\mathrm{Gal}(l/k)\cong\hat{\mathbf{Z}}\times A$, where $\hat{\mathbf{Z}}=\Pi\mathbf{Z}_p$ is the pro-cyclic group on one generator

Proof Corollary 1 is immediately clear from Theorem 2 For Corollary 2 one applies Corollary 1, taking into account that for $G=\mathbf{Z}/4\mathbf{Z}$ the field $k(M)^G$ is purely transcendental over k, whence the existence of a k-extension with Galois group $\mathbf{Z}_2$ The existence of a $\mathbf{Z}_p$-extension of $k, p\neq 2$, follows from Theorem 1 and Corollary 1 The factor A does not give any difficulty, because k being Hilbertian, there exists for every m an extension l of k with $\mathrm{Gal}(l/k)\cong A^m$ (Theorem 1, applying Galois theory)

Remark 1 Note that the Hilbertian field $\mathbf{Q}$ admits only one $\mathbf{Z}_p$-extension for every p, and infinitely many (linearly disjoint) extensions with group A (well-known), where A is an arbitrary finite abelian group However, the pair $(\mathbf{Q}, A)$ does not generally satisfy condition (ii)

Remark 2 Corollary 2 substantiates a claim made in [2] (p 401) and [3] (p 113) stating that for Hilbertian k, the maximal p-extension $k(p)$ has infinite degree over k Mr Jarden drew attention to the incompleteness of the proof in [2]

1. Proof of Theorem 2

Preserving the notations of the previous paragraph and Theorem 2, let $p=\mathrm{char}(k)$ It is well-known that the extension problem $P(n+1, n, k)$ is solvable for all $n \geqq 1$, e.g. using Witt vectors or by induction. This means however, that the extension problem $P(m, n, k)$ is solvable for all $m \geqq n \geqq 1$. Next, let $p \neq \mathrm{char}(k)$.

First we consider the case when $[K:k]$ is infinite. It is clear from infinite Galois theory, that $\mathrm{Gal}(K/k)$ is a closed subgroup of $\boldsymbol{Z}_p^*$. The latter group is of the form $\boldsymbol{Z}_p^* \cong \boldsymbol{Z}/(p-1)\boldsymbol{Z} \oplus \boldsymbol{Z}_p$ if $p \neq 2$, while $\boldsymbol{Z}_2^* \cong \boldsymbol{Z}/2\boldsymbol{Z} \oplus \boldsymbol{Z}_2$ if $p=2$. In both cases $\mathrm{Gal}(K/k) \cong F \oplus \boldsymbol{Z}_p$, where F is a finite group; Galois theory finishes this case.

We are left with the case when $[K:k] < \infty$. Again, there are two possibilities, viz. $K=k$ and $K \neq k$. First, if $K=k$, then let l/k be an extension with $\mathrm{Gal}(l/k) \cong \boldsymbol{Z}/q\boldsymbol{Z}$, and $q=p^m$. We have $l=k\left(\sqrt[q]{a}\right)$ for some $a \in k^*$, $a \notin k^{*p}$. The field $L=\bigcup_{n \geqq 1} k\left(\sqrt[p^n]{a}\right)$ is a Galois extension of $k=K$ with Galois group $\boldsymbol{Z}_p$, satisfying our desire. Let, alternatively, $K \neq k$, $\mathrm{Gal}(K/k)=\pi$. The group π is cyclic of order dividing $p-1$ if $p \neq 2$, and of order 2 if $p=2$. Let now $K(p)$ denote the maximal abelian Galois p-extension of K. The fact that $K(p)$ is a *Galois* extension of k gives the existence of an exact sequence of groups

$$0 \to A_p \to G \to \pi \to 0\,,$$

where $A_p = \mathrm{Gal}(K(p)/K)$ and $G = \mathrm{Gal}(K(p)/k)$.

The fact that over K the extension problem $P(\infty, m, K)$ is solvable, translates in terms of group theory as follows:

Lemma 1. *For every continuous surjective group homomorphism* $\alpha: A_p \to \boldsymbol{Z}/q\boldsymbol{Z}$, $q=p^m, m \geqq 1$, *there exists a continuous surjective homomorphism* $f_0: A_p \to \boldsymbol{Z}_p$ *such that the diagram*

$$\begin{tikzcd}
A_p \arrow[rr, "f_0"] \arrow[dr, "\alpha"'] & & \boldsymbol{Z}_p \arrow[dl, "\phi"] \\
& \boldsymbol{Z}/q\boldsymbol{Z} &
\end{tikzcd}$$

is commutative; here ϕ *denotes the natural homomorphism with kernel* $p^m \cdot \boldsymbol{Z}_p$.

Now the proof goes as follows. We are given an extension l/k with $\mathrm{Gal}(l/k) \cong \boldsymbol{Z}/p^n\boldsymbol{Z}$, where $n \geqq 1$ if $p \neq 2$ and $n \geqq 2$ if $p=2$. We wish to construct an extension M/k with $\mathrm{Gal}(M/k) \cong \boldsymbol{Z}_p$. We have $\mathrm{Gal}(l \cdot K/K) \cong \boldsymbol{Z}/q\boldsymbol{Z}$, where $q=2^{n-1}$ if $p=2$, $K \subset l$, and $q=p^n$ otherwise; so $q>1$ in all cases. The natural surjective map

$$A_p \to \mathrm{Gal}(l \cdot K/K) \cong \boldsymbol{Z}/q\boldsymbol{Z}$$

is denoted by α, and we let f_0, ϕ be as in Lemma 1. We are going to change f_0 in such a way that the kernel of the new map $A_p \to \boldsymbol{Z}_p$ defines a $\boldsymbol{Z}_p$-extension of K which is *Galois* and *abelian* over k. Then the construction of M will be immediate.

In order to carry out this programme we need to know how the statement "L is Galois and abelian over k" [for an intermediate field $K \subset L \subset K(p)$] translates in terms of group theory.

The group π acts on A_p via $a^\tau = \tau^* a \tau^{*-1}$ where $a \in A_p$, $\tau \in \pi$, and $\tau^* \in G$ a preimage of τ. Putting $A_p^I = \{a^i | a \in A_p, i \in I\}$, where I is the augmentation ideal of $\boldsymbol{Z}[\pi]$, the cyclicity of π entails $A_p^I=[G, G]$, the commutator group of G. This follows by direct verification, taking into account that $a^{\tau-1}=\tau^* a \tau^{*-1} a^{-1}$. The next lemma follows immediately from this consideration.

Lemma 2. *Let L be an intermediate field $K \subset L \subset K(p)$. The following conditions are equivalent*

(i) *L/k is Galois with abelian Galois group,*

(ii) *the subgroup $\operatorname{Gal}(K(p)/L)$ of A_p is invariant in G with abelian factor group,*

(iii) *the natural map ψ: $A_p \to \operatorname{Gal}(L/K)$ has the property $A_p^I \subset \operatorname{Ker}(\psi)$.*

It follows, in particular, that $A_p^I \subset \operatorname{Ker}(\alpha)$. We define s: $A_p \to A_p$ by $s(a)=a^S$ where $S=\sum_{\tau \in \pi} \tau \in \boldsymbol{Z}[\pi]$. Note that $A_p^I \subset \operatorname{Ker}(s)$, since $I \cdot S$ is the zero ideal of $\boldsymbol{Z}[\pi]$.

Proposition 1. *Assume $p \neq 2$, and let the notation be as above. The diagram*

$$\begin{tikzcd}
A_p \arrow[r, "s"] \arrow[d, "\alpha"'] & A_p \arrow[r, "f_0"] & \boldsymbol{Z}_p \arrow[r, "|\pi|^{-1}"] \arrow[d, "\phi"] & \boldsymbol{Z}_p \arrow[d, "\phi"] \\
\boldsymbol{Z}/q\boldsymbol{Z} \arrow[rr, "|\pi|"] & & \boldsymbol{Z}/q\boldsymbol{Z} \arrow[r, "|\pi|^{-1}"] & \boldsymbol{Z}/q\boldsymbol{Z}
\end{tikzcd}$$

where the map $|\pi|$ denotes the (continuous) automorphism "multiplication by $|\pi|$" on $\boldsymbol{Z}_p$ and $\boldsymbol{Z}/q\boldsymbol{Z}$, is commutative. Moreover, the surjective map $f_1=|\pi|^{-1} f_0 \circ s$ is such that $A_p^I \subset \operatorname{Ker}(f_1)$.

Proof. The commutativity of the diagram is easily verified by a straight-forward calculation, for the surjectivity of $|\pi|$ and $|\pi|^{-1}$ one has to note that $(|\pi|, p)=1$. The inclusion $A_p^I \subset \operatorname{Ker}(f_1)$ follows from $A_p^I \subset \operatorname{Ker}(s)$. Finally, the diagram tells us that the image of f_1 is a closed subgroup of $\boldsymbol{Z}_p$ mapping *onto* $\boldsymbol{Z}/q\boldsymbol{Z}$, so the procyclic structure of $\boldsymbol{Z}_p$ implies that f_1 is surjective. This proves Proposition 1.

Theorem 2 is now easily settled for $p \neq 2$. Let l, α be as before, let f_1 be as in Proposition 1, and let $L \subset K(p)$ be the invariant field of $\operatorname{Ker}(f_1)$. Then $l \subset L$, $\operatorname{Gal}(L/K) \cong \boldsymbol{Z}_p$, and L/k is Galois and abelian by Lemma 2. Further, Galois theory gives us an exact sequence of abelian groups

$$0 \to \boldsymbol{Z}_p \to \operatorname{Gal}(L/k) \to \pi \to 0$$

The sequence splits by $(|\pi|, p)=1$, so $L=M \cdot K$ where $\operatorname{Gal}(M/k) \cong \boldsymbol{Z}_p$. Finally, $l \subset M$ again follows from $(|\pi|, p)=1$. We conclude that M is the required extension of k and that the problem $P(\infty, n, k)$ is solvable for all $n \geqq 1$.

Proposition 2. *Assume $p=2$, and let the notation be as before. The diagram*

$$\begin{tikzcd}
A_2 \arrow[r, "s"] \arrow[d, "\alpha"'] & A_2 \arrow[r, "f_0"] & \boldsymbol{Z}_2 \arrow[d, "\phi"] \\
\boldsymbol{Z}/q\boldsymbol{Z} \arrow[rr, "2X"] & & \boldsymbol{Z}/q\boldsymbol{Z}
\end{tikzcd}$$

is commutative, but the homomorphism $f_1=f_0 \circ s$ not surjective. One has $A_2^I \subset \operatorname{Ker}(f_1)$, $\operatorname{Im}(f_1)=2\boldsymbol{Z}_2$, and, if $f_2=\frac{1}{2} f_1$, then f_2 is a continuous surjective homomorphism satisfying $A_2^I \subset \operatorname{Ker}(f_2)$.

Proof The commutativity of the diagram and the inclusion $A_2^I \subset \mathrm{Ker}(f_1)$ go as before Further, the diagram implies that $\mathrm{Im}(f_1)$ is a closed subgroup of $\boldsymbol{Z}_2$ mapping onto $2\boldsymbol{Z}/q\boldsymbol{Z}$ If $q>2$ this implies $\mathrm{Im}(f_1)=2\boldsymbol{Z}_2$ by the procyclic structure of $\boldsymbol{Z}_2$ In the case $q=2$ we arrive at the same conclusion by an explicit computation $q=2$ implies $\mathrm{Gal}(l/k)\cong \boldsymbol{Z}/4\boldsymbol{Z}$ and $K\subset l$, let $\sigma^* \in \mathrm{Gal}(K(p)/k)$ be such that $\sigma=\sigma^*|K$ generates π, then $\sigma^*|l$ generates $\mathrm{Gal}(l/k)$ so the element $\tau=(\sigma^*)^2$ of A_2 is not the identity when restricted to l, this means $\alpha(\tau)\neq 0 \in \boldsymbol{Z}/2\boldsymbol{Z}$ so $f_0(\tau)\in \boldsymbol{Z}_2\setminus 2\boldsymbol{Z}_2$, also $\tau^\sigma=\tau$ so $f_1(\tau)=f_0(\tau^2)\in 2\boldsymbol{Z}_2\setminus 4\boldsymbol{Z}_2$, therefore $2\boldsymbol{Z}_2\subset \mathrm{Im}(f_1)$, and since the opposite inclusion follows from the diagram we conclude $\mathrm{Im}(f_1)=2\boldsymbol{Z}_2$, as required The assertions about f_2 follow immediately This concludes the proof of Proposition 2

To finish the proof of Theorem 2, let l, α be as before and let f_2 be as in Proposition 2 Then the invariant field $L\subset K(2)$ of $\mathrm{Ker}(f_2)$ has Galois group $\cong \boldsymbol{Z}_2$ over K, and L is Galois and abelian over k There is an exact sequence

$$0\to \boldsymbol{Z}_2\to \mathrm{Gal}(L/k)\to \pi\to 0$$

If this extension splits then $\mathrm{Gal}(L/k)\cong \boldsymbol{Z}_2\oplus\pi$, and if it does not split then $\mathrm{Gal}(L/k)\cong \boldsymbol{Z}_2$ In both cases there exists an extension M of k with Galois group isomorphic to $\boldsymbol{Z}_2$

This concludes the proof of Theorem 2

Remark A closer look at the construction reveals that in the case $p=2$ the field M can be chosen such that the intersection $M\cap l$ has degree 2^{n-1} or 2^n over k

2. Supplementary Remarks

It is not true that any field k, admitting a field extension l with $\mathrm{Gal}(l/k)=V_4$ (cf Theorem 2) admits a $\boldsymbol{Z}/4\boldsymbol{Z}$-extension (and, by consequence, a $\boldsymbol{Z}_2$-extension) The field of all totally-real algebraic numbers, for instance, admits V_4-extensions and no $\boldsymbol{Z}/4\boldsymbol{Z}$-extensions The following is an example of a field admitting for an arbitrary cardinal number m an extension with Galois group $(\boldsymbol{Z}/2\boldsymbol{Z})^m$, and no $\boldsymbol{Z}/4\boldsymbol{Z}$-extension Let I be a set with $|I|=m$ and let $F=\boldsymbol{Q}(\{t_i|i\in I\})$ be a purely transcendental extension of $\boldsymbol{Q}$ with transcendental degree m Choose for every $i\in I$ an ordering $<_i$ of F, in such a manner that $t_i<_i 0$ and $0<_i t_j$, for $j\neq i$ Let R_i, $F\subset R_i\subset \bar{F}$, be a real-closed field the ordering of which is an extension of $<_i$ Then $k=\bigcap_{i\in I} R_i$ has the required property one sees easily that $\mathrm{Gal}(\bar{k}/k)$ is topologically generated by elements of order 2 It is also possible to give a proof of Theorem 2 $(p\neq 2)$ more directly by using Kummer theory However, this method does not seem to be readily extendible to the case $p=2$

References

1 Hilbert, D Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten J Reine Angew Math **110**, 104—129 (1892)

2 Kuyk, W Generic approach to the Galois embedding and extension problem J Algebra **9** (4), 393–407 (1968)

3 Kuyk, W Extensions de corps hilbertiens J Algebra **14** (1), 112—124 (1970)

4 Lenstra, Jr ,H W Rational functions invariant under a finite Abelian group Invent Math **25**, 299—325 (1974)
5 Lang, S Diophantine geometry Interscience Tracts 11 New York-London 1962
6 Noether, E Gleichungen mit vorgeschriebener Gruppe Math Ann **78**, 221—229 (1918)

W Kuyk
Department of Mathematics
Antwerp University
B-2020 Antwerp, Belgium

H W Lenstra, Jr
Mathematisch Instituut
Universiteit van Amsterdam
Roetersstraat 15
Amsterdam
The Netherlands

(Received October 30, 1974)