CONSTRUCTION OF SEMIABELIAN GALOIS EXTENSIONS

by MICHAEL STOLL

(Received 29 June, 1993)

1. Introduction. This paper shows how to construct Galois field extensions of Hilbertian fields with a given group out of some subclass (called 'semiabelian groups' by Matzat [**2**]) of all soluble groups as Galois group. This is done in a fairly explicit way by constructing polynomials whose Galois groups are universal in the sense that every group in the above subclass is obtained as a quotient of some of them.

The fact that groups of the type considered here can be obtained as Galois groups over Hilbertian fields is well known—it follows from the solubility of split embedding problems with abelian kernel (see [**2**] for an overview). The aim of this paper is to give an explicit construction of such extensions.

The paper consists of two sections. In the first one, the relevant class of groups is defined and studied to some extent, and some technical lemmas concerning wreath products are established. The definition of semiabelian groups given here differs from Matzat's, but it is easily seen that both notions agree. The second section gives the main result, applying the results of the first section to the Galois groups of certain polynomials.

R. W. K. Odoni [**4**] showed how to realise a multiple wreath product of cyclic groups as Galois group over a Hilbertian field containing "enough" roots of unity. The new idea in this paper is to overcome this restriction by adjoining the necessary roots of unity first.

I wish to thank R. W. K. Odoni for his work on the Galois theory of nested polynomials [**3, 4**], which prepared the ground for the present work, Cornelius Greither who drew my attention to it and told me to look at the quotient groups, and (last but not least) Fritz Grunewald with whom I had many pleasant and instructive discussions that eventually led to the present paper.

2. Semiabelian groups and wreath products.

Definition 1. A group G is called *semiabelian*, if there exist $n \in \mathbb{N}$ and abelian subgroups $A_1, \dots, A_n$ of G such that $G = A_1 \cdots A_n$, and such that A_i normalizes A_j whenever $i < j$. Such a sequence $A_1, \dots, A_n$ is called an *internal resolution* of G.

Clearly, every semiabelian group is soluble. The extra condition is that there exist a composition series whose factors can be obtained as images of abelian subgroups of G.

Lemma 1. *A finite group G is semiabelian if and only if G has a generating set $\{x_1, \dots, x_m\}$ such that the normal closure of x_i in $\langle x_1, \dots, x_i \rangle$ is abelian.*

Proof "$\Leftarrow$". Take $n = m$ and A_i = normal closure of x_i in $\langle x_1, \dots, x_i \rangle$. "$\Rightarrow$": Take generating sets $y_{i1}, \dots, y_{im_i}$ of A_i and set $m = \sum_i m_i$ and $(x_1, \dots, x_m) = (y_{11}, \dots, y_{1m_1}, \dots, y_{n1}, \dots, y_{nm_n})$.

https://doi.org/10.1017/S0017089500030433 Published online by Cambridge University Press

COROLLARY 1. (*a*) *Every finitely generated* 2-*step nilpotent group is semiabelian.*
(*b*) *Every abelian-by-cyclic group G is semiabelian.*

Proof.
(a) In a 2-step nilpotent group the normal closure of every element is abelian.
(b) Let A be an abelian normal subgroup of G with cyclic factor group generated by the image of $x \in G$. Then $\langle x \rangle, A$ is an internal resolution of G.

LEMMA 2. *Every quotient of a semiabelian group is semiabelian.*

Proof. Take the image of an internal resolution under the canonical epimorphism.

In order to treat wreath products concisely, we will consider triples (G, ϕ, U), where G is a finite group, U is a finite set, and $\phi: G \to S(U)$ is a (left) action of G on U ($S(U)$ denotes the group of permutations of U). In this context, G is an abbreviation of (G, λ, G), where λ is the left regular permutation representation of G. We will call (H, ψ, V) a *quotient* of (G, ϕ, U) if there is an epimorphism $\pi: G \to H$ and a map $\sigma: U \to V$ such that $\psi\pi(g)(\sigma(u)) = \sigma(\phi(g)(u))$ for all $g \in G$ and all $u \in U$. Then G' is a quotient of G in this sense whenever G' is a quotient of G as a group.

DEFINITION 2. The *wreath product* $(G, \phi, U) \wr (H, \psi, V)$ of (G, ϕ, U) and (H, ψ, V) is the triple $(G \ltimes H^U, \omega, U \times V)$, where G acts on the right of H^U by $f^g(u) = f(\phi(g)(u))$, and $\omega(g, f)(u, v) = (\phi(g)(u), \psi(f(u))(v))$. (Here, H^U denotes the set of all functions $U \to H$.)

The wreath product is associative in the sense that for $T_j = (G_j, \phi_j, U_j)$ $(j = 1, 2, 3)$, $(T_1 \wr T_2) \wr T_3$ and $T_1 \wr (T_2 \wr T_3)$ are isomorphic (as groups acting on the set, $U_1 \times U_2 \times U_3$).

LEMMA 3 (quotients of wreath products). (*a*) *If (H', ψ', V') is a quotient of (H, ψ, V), then $(G, \phi, U) \wr (H', \psi', V')$ is a quotient of $(G, \phi, U) \wr (H, \psi, V)$.*
(*b*) *If H is abelian and (G', ϕ', U') is a quotient of (G, ϕ, U), then the group component of $(G', \phi', U') \wr (H, \psi, V)$ is a quotient of the group component of $(G, \phi, U) \wr (H, \psi, V)$.*
(*c*) *If H is abelian, then $G \times H$ is a quotient of the group component of $G \wr H$.*
(*d*) *If $G_1, \ldots, G_n$ are abelian groups, and $G_1', \ldots, G_n'$ are quotients of $G_1, \ldots, G_n$, respectively, then the group component of $G_1' \wr \ldots \wr G_n'$ is a quotient of the group component of $G_1 \wr \ldots \wr G_n$.*

Proof. (a) Let π_H and σ_H be the given quotient maps. We take $\pi: G \ltimes H^U \to G \ltimes H'^U$, $(g, f) \mapsto (g, \pi_H \circ f)$ and $\sigma: U \times V \to U \times V'$, $(u, v) \mapsto (u, \sigma_H(v))$. π is clearly an epimorphism, and an easy calculation shows the compatibility of π and σ.
(b) Let π_G and σ_G be the given quotient maps. We take $\pi: G \ltimes H^U \to G' \ltimes H^{U'}$, $(g, f) \mapsto (\pi_G(g), f')$, where $f'(u') = \prod_{\sigma_G(u) = u'} f(u)$. π is a homomorphism because H is abelian, and clearly surjective.
(c) This follows from b) by taking a one-element set for U'.
(d) This follows from a) and b) by an easy induction.

LEMMA 4. (*a*) *Every split extension with abelian kernel of a semiabelian group is semiabelian.*

https://doi.org/10.1017/S0017089500030433 Published online by Cambridge University Press

(*b*) *The group component of a wreath product* $(G, \phi, U) \wr (H, \psi, V)$ *with* G *semiabelian and* H *abelian is semiabelian.*

Proof. (a) Let $1 \to A \to G \to H \to 1$ be split with A abelian and let $A_1, \ldots, A_m$ be an internal resolution of H. Then $G = A_1 \cdots A_m A$, and each A_i normalizes A, hence $A_1, \ldots, A_m, A$ is an internal resolution of G.

(b) H^U is abelian, hence $G \ltimes H^U$ is semiabelian by part a).

THEOREM 1 (characterising semiabelian groups). *A finite group* G *is semiabelian iff there are* $k, m \in \mathbb{N}$ *such that* G *is a quotient of* (*the group component of*) $C_m^{\wr k}$ (*where* C_m *is the cyclic group with* m *elements, and* $H^{\wr k}$ *means the* k*-fold wreath product* $H \wr \cdots \wr H$).

Proof. By the preceding lemma, every group that is the group component of some wreath power $C_m^{\wr k}$ is semiabelian. By Lemma 2, every quotient of such a group is again semiabelian.

Let G be a finite semiabelian group with internal resolution $A_1, \ldots, A_n$. We will show that G is a quotient of (the group component of) $A_1 \wr \cdots \wr A_n$. This will be done by induction on n. For $n = 1$, there is nothing to show. Let $n > 1$, and let $H = A_2 \cdots A_n$. Then H is a normal subgroup of G and has the internal resolution $A_2, \ldots, A_n$. By induction hypothesis, H is a quotient of $A_2 \wr \cdots \wr A_n$. If we can show that G is a quotient of $A_1 \wr H$, then by Lemma 3,a), G is a quotient of $A_1 \wr \cdots \wr A_n$. We define a map $\pi: A_1 \wr H \to G$ by letting $\pi(a, f) = a \prod_{\alpha \in A_1} (\alpha f(\alpha) \alpha^{-1})$. It is easily verified that π is an epimorphism, whence G is a quotient of $A_1 \wr \cdots \wr A_n$.

It remains to show that $A_1 \wr \cdots \wr A_n$ is obtainable as a quotient of some group $C_m^{\wr k}$. For this, let m be a common exponent of all the A_j, then there are numbers k_j such that A_j is a quotient of $C_m^{k_j}$. By lemma 3,c), $C_m^{k_j}$ and therefore A_j, too, are quotients of $C_m^{\wr k_j}$. Now, Lemma 3,d), shows that $A_1 \wr \cdots \wr A_n$ is a quotient of $C_m^{\wr k}$, where $k = \sum_j k_j$.

The preceding lemma and theorem also show that the class of finite internally soluble groups is the smallest nonempty class of finite groups closed with respect to split extensions with abelian kernel and quotients. This shows that our semiabelian groups coincide with those of Matzat [**2**]. This class of groups is also studied in [**1**].

We will end this section with a technical lemma that will be useful later.

LEMMA 5. *Let* $(G, \psi, G_1 \times U) = G_1 \wr (G_2, \phi, U)$, *and let* H *be a finite abelian group* (*which we will write additively*), *on which* G_1 *acts from the left. We let* P *be the group with underlying set* $G \times H^{G_1 \times U}$ *that acts on* $G_1 \times U \times H$ *by* $((g, f), h) \cdot (x, u, v) = (gx, \phi(f(x))(u), h(x, u) + g \cdot v)$. *Then* P *with this action is isomorphic with* $(G, \psi, G_1 \times U) \wr H$.

Proof. The group multiplication in P is given by

$$((g,f),h)((g',f'),h') = ((g,f)(g',f'),(x,u) \mapsto h(g'x, \phi(f'(x))(u)) + g \cdot h'(x,u))$$

(it is easily verified that this indeed defines a group law). $G \ltimes H^{G_1 \times U}$ is the group component of $(G, \psi, G_1 \times U) \wr H$. We define the isomorphism $\theta: P \to G \ltimes H^{G_1 \times U}$ by

$$\theta((g,f),h) = ((g,f),(x,u) \mapsto (gx)^{-1} \cdot h(x,u)).$$

https://doi.org/10.1017/S0017089500030433 Published online by Cambridge University Press

Obviously θ is a bijective map. We have to verify that it is a homomorphism:

$$\begin{aligned}
&\theta((g,f),h)\theta((g',f'),h')\\
&\quad=((g,f),(x,u)\mapsto(gx)^{-1}\cdot h(x,u))((g',f'),(x,u)\mapsto(g'x)^{-1}\cdot h'(x,u))\\
&\quad=((gg',x\mapsto f(g'x)f'(x)),(x,u)\mapsto(gg'x)^{-1}\cdot h(g'x,\phi(f'(x))(u))+(g'x)^{-1}\cdot h'(x,u))\\
&\quad=((g,f)(g',f'),(x,u)\mapsto(gg'x)^{-1}\cdot(h(g'x,\phi(f'(x))(u))+g\cdot h'(x,u)))\\
&\quad=\theta((g,f)(g',f'),(x,u)\mapsto h(g'x,\phi(f'(x))(u))+g\cdot h'(x,u))\\
&\quad=\theta(((g,f),h)((g',f'),h'))
\end{aligned}$$

In order to show that the two groups are isomorphic as groups acting on a set, we must produce a permutation ρ of $G_1\times U\times H$ such that

$$\rho(((g,f),h)(x,u,v))=\theta((g,f),h)\rho(x,u,v).$$

If we define $\rho(x,u,v)=(x,u,x^{-1}\cdot v)$, this equality holds, as a short computation shows:

$$\begin{aligned}
\rho(((g,f),h)(x,u,v))&=\rho(gx,\phi(f(x))(u),h(x,u)+g\cdot v)\\
&=(gx,\phi(f(x))(u),(gx)^{-1}\cdot h(x,u)+x^{-1}\cdot v)\\
&=\theta((g,f),h)(x,u,x^{-1}\cdot v)\\
&=\theta((g,f),h)\rho(x,u,v)
\end{aligned}$$

3. Realising semiabelian groups as Galois groups. Let K be some field, and let $t_1,t_2,\dots$ denote independent indeterminates over K. We take $m\in\mathbb{N}$ and assume m prime to the characteristic of K, unless the latter is zero. Let ζ be some primitive mth root of unity over K, f its irreducible polynomial, $K_0=K(\zeta)$, and G_0 the Galois group of K_0 over K. We define recursively

$$f_0(X)=f(X)\in K[X]\quad\text{and}\quad f_{k+1}(X)=f_k(X^m-t_{k+1})\in K[t_1,\dots,t_{k+1},X];$$

K_k will denote the splitting field of f_k over $K(t_1,\dots,t_k)$.

THEOREM 2. *The Galois group G_k of f_k over $K(t_1,\dots,t_k)$ is isomorphic with $G_0\wr C_m^{\wr k}$.*

Proof (*cf.* [**3**]). We proceed by induction on k, proving a little bit more, namely that we can label the zeros of f_k as $\alpha(i,j)$ with $i\in G_0$ and $j\in C_m^k$ such that the above wreath product acts on the indices according to its definition, and such that its action on ζ is given by the component in G_0. For $k=0$, we have only to remark that the action of G_0 on the zeros of f is isomorphic with the left regular permutation representation of G_0.

Suppose now the assertion true for some k and all fields with characteristic equal to that of K. Taking $K(t_{k+1})$ instead of K in the induction hypothesis, we see that the Galois group of f_k over $K(t_1,\dots,t_{k+1})$ is $G_0\wr C_m^{\wr k}$ (note that G_0 is also the Galois group of f over $K(t_{k+1})$) and that we can label the zeros of f_k in $K_k(t_{k+1})$ as $\alpha(i,j)$ with $i\in G_0$ and $j\in C_m^k$. Fixing the mth roots, the zeros of f_{k+1} in K_{k+1} are given as

$$\beta(i,j,l)=\zeta^l(\alpha(i,j)+t_{k+1})^{1/m}\quad\text{for}\quad i,j\quad\text{as above and}\quad l\in C_m.$$

https://doi.org/10.1017/S0017089500030433 Published online by Cambridge University Press

To every $\sigma \in G_{k+1}$ we associate $\bar{\sigma} = \sigma|_{K_k} \in G_k$ and $h_\sigma : G_0 \times C_m^k \to C_m$ defined by $\sigma(\beta(i,j,0)) = \beta(i',j',h_\sigma(i,j))$. Then we have

$$\sigma(\beta(i,j,l)) = \beta(\bar{\sigma}(i,j), h_\sigma(i,j) + g_\sigma l),$$

where g_σ denotes the G_0-component of $\bar{\sigma}$. Using Lemma 5, we see that we can embed G_{k+1} into $G_k \wr C_m$ as a subgroup with the right type of action on the roots of f_{k+1}.

To show that G_{k+1} is indeed the full wreath product, we use Kummer theory: $K_{k+1}/K_k(t_{k+1})$ is an m-Kummer extension obtained by taking the mth roots of $\# G_0 \cdot m^k$ elements. We will show that these are all independent, therefore the degree $[K_{k+1} : K_k(t_{k+1})] = m^{\# G_0 \cdot m^k} = \#(G_k \wr C_m)/\# G_k$, from which the claim follows.

The independence of the mth roots means that in every product

$$\prod_{i,j} (\alpha(i,j) + t_{k+1})^{c_{ij}}, \qquad c_{ij} \in \mathbb{N},$$

that is an mth power in $K_k(t_{k+1})$, all the exponents c_{ij} must be divisible by m. Now, the ring of polynomials $R = K_k[t_{k+1}]$ is a UFD, therefore integrally closed in $K_k(t_{k+1})$, hence the product has to be an mth power in R. Since all the $(\alpha(i,j) + t_{k+1})$ are distinct prime elements in R, the assertion follows.

Corollary 2. *Every finite semiabelian group G can be realized as a Galois group over every Hilbertian field K of characteristic zero or prime to the order of the group.*

Proof. The preceding theorem, together with the Hilbert irreducibility theorem (which holds for Hilbertian fields by definition), implies that for all m (prime to the characteristic of K if the latter is not zero) and all k, $G_0 \wr C_m^{\wr k}$ is realisable as a Galois group over K, where G_0 is some abelian group. By Lemma 3,d), $C_m^{\wr k}$ is a quotient of $G_0 \wr C_m^{*k}$, and by Theorem 1, every finite semiabelian group G is a quotient of some $C_m^{\wr k}$ (where m can be assumed prime to char(K) if $\# G$ is). Using Galois theory, we see that all these groups occur as Galois groups of some intermediate field of one of the above field extensions.

This result is quite well known, of course, see e.g. [**2**] and the references given there. However, our method of construction gives a new and more direct proof of this.

Remarks. 1) Examples of Hilbertian fields are finitely generated field extensions of $\mathbb{Q}$ and of $\mathbb{F}_p(t)$ (for any prime p) (see for example [**3**] and the references given there).
2) It is fairly obvious that the above results can be extended to groups whose order is not necessarily prime to the characteristic p (at least to those that have an internal resolution all of whose groups have p-elementary p-part) by using Artin-Schreier equations instead of Kummer equations.
3) It is easy to give polynomials with Galois groups of the form $G_0 \wr A_1 \wr \ldots \wr A_n$, where the A_j are given finite abelian groups: Just take for m the l.c.m. of the exponents of the A_j, define f_0 and G_0 as above, and let $f_{k+1} = \prod_{j=1}^{r_{k+1}} f_k(X^{d_j} - t_{k+1,j})$, assuming that $A_{k+1} = C_{d_1} \times \ldots \times C_{d_{r_{k+1}}}$. Then f_n has $G_0 \wr A_1 \wr \ldots \wr A_n$ as its Galois group over $K(t_{k_j} \mid 1 \le k \le n, 1 \le j \le d_k)$.
4) For some explicit examples how to get $C_2^{\wr n}$ as a Galois group over $\mathbb{Q}$, see [**5**].

REFERENCES

1. Ralf Dentzer, On split embedding problems with abelian kernel, Preprint 91-10, Interdisziplinäres Zentrum für wissenschaftliches Rechnen, Universität Heidelberg (1991).

2. B. Heinrich Matzat, Der Kenntnisstand in der konstruktiven Galoisschen Theorie, Preprint 90-18, Interdisziplinäres Zentrum für wissenschaftliches Rechnen, Universität Heidelberg (1990), or: PM **95** (1991), 65–98, Birkhäuser-Verlag.

3. R. W. K. Odoni, The Galois theory of iterates and composites of polynomials, *Proc. London Math. Soc.* (3), **51** (1985), 385–414.

4. R. W. K. Odoni, Realising wreath products of cyclic groups as Galois groups, *Mathematatika* **35** (1988), 101–113.

5. Michael Stoll, Galois groups over $\mathbb{Q}$ of some iterated polynomials, *Arch. Math.* **59** (1992), 239–244.

Mathematisches Institut der Universität
Beringstr. 4
D-53115 Bonn
⟨stoll@rhein.iam.uni-bonn.de⟩

https://doi.org/10.1017/S0017089500030433 Published online by Cambridge University Press