LIFTING WREATH PRODUCT EXTENSIONS

ELENA V. BLACK

(Communicated by Michael Stillman)

ABSTRACT. Let G and H be finite groups and let K be a hilbertian field. We show that if G has a generic extension over K and H satisfies the arithmetic lifting property over K, then the wreath product $G \wr H$ of G and H also satisfies the arithmetic lifting property over K. Moreover, if the orders of H and G are relatively prime and G is abelian, then any extension of G by H (which is necessarily a semidirect product) has the arithmetic lifting property.

INTRODUCTION

The purpose of this note is to strengthen the main result of [Bl2], at the same time providing a much shorter proof which is more geometric and intuitive. The result concerns the arithmetic lifting property, which in some sense can be viewed as an "inverse" of the regular use of the Hilbert Irreducibility Theorem.

The question of arithmetic lifting of Galois extensions of a field K, pursued by the author for some time, arises naturally when one considers the standard approach to the Inverse Galois problem for K through algebraic geometry. The idea of this approach is to first construct a G-Galois branched covering of the projective line over a base field K and then invoke the Hilbert Irreducibility Theorem ([Se]) to obtain a G-Galois extension of K. It is natural to ask if one can obtain *every* G-extension of K in this way, *i.e.,* if every G-Galois extension of K is the specialization of a geometric G-Galois branched covering of $\mathbb{P}^1_K$ defined over K. If the answer to this question is affirmative for a finite group G over a field K, we say that G has the arithmetic lifting property over K. This question is closely related [Bl1] to the so-called Noether's problem and generic Galois extensions introduced by Saltman [Sa]. Many groups have been shown to have the arithmetic lifting property (see [Bl1]). In [Bl2] we consider certain semidirect products. The purpose of this note is to remove some hypotheses on the building blocks of these semidirect products thus strengthening the main result of [Bl2]. Let G and H be finite groups and let K be a hilbertian field. The main result of this note is to show that if G has a generic extension over K and H satisfies the arithmetic lifting property over K, then the wreath product $G \wr H$ also satisfies the arithmetic lifting property. In [Bl2] a similar result is obtained but only for $G = A$ an abelian group. As a consequence of our main result here, we show that if $G = A$ is abelian and the orders of G and H are relatively prime, then any semidirect product $G \rtimes H$ has the arithmetic

lifting property. This also strengthens similar results on semidirect products in [Bl2], where $G = A$ must be cyclic.

As we already mentioned the proof in this note not only strengthens the previous result but is also shorter, more geometric and intuitive. One should note however, that the proof in [Bl2] is constructive, and the arithmetic liftings of Galois extensions are explicitly described. The proof in this note is existential. We present this proof in section 1 after a brief section 0 containing relevant definitions.

0. Notation and definitions

Let G be a finite group and let K be a field. We denote a function field of $\mathbb{P}^1_K$ by $K(t)$ where t is an indeterminate. For the convenience of the reader we recall a few relevant definitions here. All of those can be found in [Bl1] and [Bl2].

Let κ be an algebraically closed field. Let X be an irreducible, smooth, projective algebraic curve over κ. Let $X \to \mathbb{P}^1_\kappa$ be a dominant morphism; $i.e.$, a non-constant rational map. We say that $X \to \mathbb{P}^1_\kappa$ is a *branched covering*. A *G-Galois branched covering* (often called a G-covering) is a branched covering $X \to \mathbb{P}^1_\kappa$ together with an isomorphism of G with $Gal(\kappa(X)/\kappa(t))$, where the corresponding function field extension is Galois. Let K be a subfield of κ. We say that $X \xrightarrow{G} \mathbb{P}^1_\kappa$ has a *model* $X_K \xrightarrow{G} \mathbb{P}^1_K$ over K if the following holds:

i) X_K is a connected, complete, smooth curve over K, such that $X_K \times_{Spec\ K} Spec\ \kappa \simeq X$;

ii) the maps $X_K \to \mathbb{P}^1_K$ and $X \to \mathbb{P}^1_\kappa$ are compatible;

iii) the function field extension $K(X_K)/K(t)$ is Galois with group G.

iv) the G-action on $\kappa(X) = K(X_K) \otimes_K \kappa$ is compatible with the G-action on $K(X_K)$.

We will also say in this case that $X_K \xrightarrow{G} \mathbb{P}^1_K$ is a regular G-covering defined over K.

A field extension $\mathcal{L}/K(t)$ is called *regular* if $\bar{K} \cap \mathcal{L} = K$, where $\bar{K}$ is a separable algebraic closure of K; in other words K is algebraically closed in $\mathcal{L}$. Note, in particular, that an extension $\mathcal{L}/K(t)$ corresponds to the function field extension of some branched covering $X_K \to \mathbb{P}^1_K$ defined over K if and only if it is regular. If $X_K \to \mathbb{P}^1_K$ is a regular G-Galois branched covering and y is a K-rational point on $\mathbb{P}^1_K$, the fiber of $X_K \to \mathbb{P}^1_K$ over y corresponds to an extension of K-algebras A/K. We call this extension A/K a *specialization* of $X_K \to \mathbb{P}^1_K$ at the point y. If y is inert, $i.e.$ the inverse image of y (in the scheme sense) is one closed point, then the corresponding extension of K-algebras is a G-Galois field extension.

By an *arithmetic lifting* of a field extension L/K we mean a G-Galois regular branched covering $X_K \to \mathbb{P}^1_K$ together with a K-rational point $y \in P^1_K$, such that this covering specializes to L/K at the point y. We say that a finite group G has *the arithmetic lifting property* over a field K if *every* G-Galois field extension of K has an arithmetic lifting.

A *generic* extension for a finite group G over the base field k is an étale G-Galois covering of a basic open set $U \subset \mathbb{A}^n_k$ for some n, such that the versal specialization property holds. Namely, for any G-Galois extension L/K of k-algebras with K a field, there is a K-rational point in U, such that specialization of the above-named G-extension at this point yields L/K. This notion of generic extension has been introduced by Saltman [Sa]. His original definition of a generic extension for G over

k was given in terms of Galois extension of rings [Sa, p.255]. (For the definitions of the Galois extensions of rings see [CHR].)

Two branched coverings $X_1 \to Y$ and $X_2 \to Y$ are called *disjoint* over Y if whenever there is a commutative diagram

$$
\begin{array}{ccc}
X_1 & & X_2 \\
& \searrow \quad \swarrow & \\
& Z & \\
& \downarrow & \\
& Y &
\end{array}
$$

then $Z \to Y$ is an isomorphism. On the function field level, this corresponds to linear disjointness of $\bar{K}(X_1)$ and $\bar{K}(X_2)$ over $\bar{K}(Y)$ where $\bar{K}$ is a separable algebraic closure of K.

1. Generalized arithmetic lifting property of wreath product extensions

Throughout this section K is a hilbertian field, G and H are finite groups, such that G has a generic extension over K and H has the arithmetic lifting property over K. We let the wreath product of G and H be denoted by Γ, *i.e.,* $\Gamma = G \wr H$. The main result of this paper is the following theorem.

Theorem 1.1. *Let K be a hilbertian field. Let G and H be finite groups such that G has a generic extension over K and H has the arithmetic lifting property over K. Let $\Gamma = G \wr H$ and let L/K be the Γ-Galois extension of K-algebras. Let E/K be the H-Galois subextension of L/K and assume that E/K is a* field *extension. Then there exist a regular Γ-Galois branched covering $Y_K \xrightarrow{\Gamma} \mathbb{P}^1_K$ defined over K, such that it specializes to L/K at $t = 0$.*

Corollary 1.2. *With G, H, Γ and K as in Theorem 1.1, Γ has the arithmetic lifting property over K.*

Corollary 1.3. *With the set-up of Theorem 1.1, assume in addition that G is abelian and the orders of G and H are relatively prime. Then any extension of G by H, which is necessarily a semidirect product $G \rtimes H$, has the arithmetic lifting property.*

Proof of Theorem 1.1. Let L/K be a given Γ-Galois extension of K-algebras. Let $N = \bigoplus_{h \in H} G_h$, where each G_h is a copy of G. Then $\Gamma = G \wr H = N \rtimes H$, where H acts on N by permuting the direct summands in the usual way. Let E be the fixed ring of N. By hypothesis E is a field. Let U denote the maximal field in L, so L is a direct sum of fields isomorphic to U and $E \subset U$.

• *Step* 1. Since L/K is a Γ-Galois extension of K-algebras, by Lemma 3.4 of [Sa] there exists a K-subalgebra $T \subset L$ containing E, such that T/E is Galois with group G, and such that the multiplication map defines an isomorphism $L \cong \bigotimes_{h \in H} h(T)$. Here the tensor product is over E.

• *Step* 2. Next we use the arithmetic lifting property for H to obtain a regular branched covering $X_K \xrightarrow{H} \mathbb{P}^1_K$ defined over K and specializing to E/K at $t = 0$. (The fact that E/K is a *field* extension is important here.)

On the function field level $X_K \to \mathbb{P}^1_K$ corresponds to a regular H-Galois extension of fields $K(X)/K(t)$. We may pick a primitive element x of this extension with $f(x,t) \in K[t]$ its minimal polynomial over $K(t)$. We arrange our choice of $f(x,t)$, so that the polynomial in one variable $f(x,0)$ is the minimal polynomial for a primitive element of E/K which we will denote by $\lambda \in E$.

Since K is hilbertian, there exist infinitely many pairwise linearly disjoint over K H-Galois field extensions of K corresponding to different specializations of $X_K \to \mathbb{P}^1_K$. Since U/K has only finitely many intermediate subfields, we can pick one of the specializations of $X_K \to \mathbb{P}^1_K$, say at $t = a \in K$, to satisfy the following two properties. First, this specialization is the H-Galois extension of fields (denoted F/K) such that F is linearly disjoint from U over K. Second, $f(x,a)$ is the minimal polynomial for a primitive element of F/K which we will denote by $\alpha \in F$. For future reference we denote the point of X lying above $t = a$ in the covering $X \overset{H}{\to} \mathbb{P}^1$ by P_a. Similarly, we denote by P_0 the point of X above $t = 0$.

• *Step* 3. Recall that G is assumed to have a generic extension over K, which implies in particular that there exists a regular G-Galois extension of $K(u)$ where u is an indeterminate. This fact allows us to use Theorem 2.2 from [MaMa, IV] which states that any H-Galois extension of K can be embedded *parametrically* into a $G \wr H$-Galois extension assuming that G is a Galois group of some regular extension of $K(u)$. This means that there exists a Γ-Galois extension $\mathcal{F}/K(\mathbf{u})$ with H-Galois subextension $F(\mathbf{u})/K(\mathbf{u})$ such that F is algebraically closed in $\mathcal{F}$. Here $\mathbf{u} = (u_1, u_2, ..., u_n)$ with u_i indeterminates. Thus there are infinitely many Γ-Galois field extensions of K, pairwise linearly disjoint over F, with fixed field of N equal to F. We pick one which is linearly disjoint over F with $U \otimes_K F$ and denote it $\tilde{F}/K$. Note that $U \otimes_K F/K$ is a field extension because U and F are linearly disjoint over K and it has only finitely many intermediate subfields, so such choice is possible. We use Saltman's lemma ([Sa], Lemma 3.4) again to obtain M/F which is a G-Galois extension of F such that $\tilde{F} \cong \bigotimes_{h \in H, F} h(M)$.

• *Step* 4. In Theorem 5.3 of [Sa] it is shown that if G has a generic extension, then G satisfies the following lifting property introduced by Saltman: for any semilocal K-algebra S with Jacobson radical $J(S)$, and all G-Galois extensions B'/K' with $K' = S/J(S)$, there is a Galois extension S'/S such that $S' \otimes_S (S/J(S)) \cong B'$. Let $K(u)$ denote a function field of $\mathbb{P}^1_K$. Let $\wp_1$ be a prime ideal of $K[u]$ generated by the irreducible polynomial $f(u,0)$ and $\wp_2$ be a prime ideal of $K[u]$ generated by the irreducible polynomial $f(u,a)$. (Recall that $f(u,0) \in K[u]$ is the minimal polynomial for $\lambda \in E$ and $f(u,a) \in K[u]$ is the minimal polynomial for $\alpha \in F$ from Step 2.) There is a semilocal ring $R \subset K(u)$ with two primes such that localizations of R are local rings associated to $\wp_1$ and $\wp_2$, and $R/J(R) = E \oplus F$. Note that $T \oplus M$ is naturally a G-Galois extension of $E \oplus F$. The lifting property says that this extension lifts to a G-Galois extension of K-algebras R'/R, and we set $\mathcal{L} = R' \otimes_R K(u)$. Then $\mathcal{L}/K(u)$ is a G-Galois extension of fields since M/F is a specialization and M is a field. It is a regular extension since M is linearly disjoint over K from any field contained in T and T/E is also a specialization. Thus it corresponds to a regular G-Galois branched covering of $\mathbb{P}^1$ defined over K and specializing at E-rational point (corresponding to $\wp_1$) to T/E and at F-rational point (corresponding to $\wp_2$) to M/F. We denote this covering $Z \overset{G}{\to} \mathbb{P}^1$.

• *Step* 5. Let us return to the H-Galois covering $X \to \mathbb{P}^1$ (from Step 2). On function field level it corresponds to a regular H-Galois extension of fields $K(X)/K(t)$.

Recall that $x \in K(X)$ is a primitive element of this extension and $f(x,t)$ is a minimal polynomial of x over $K(t)$. Since any nonconstant rational function on X defines a map from X to a projective line, we have that x defines a map from X to $\mathbb{P}^1$, which we denote $X \xrightarrow{\phi} \mathbb{P}^1$. Let $Z_x \to X$ be a pull-back of $Z \xrightarrow{G} \mathbb{P}^1$ along this map $X \xrightarrow{\phi} \mathbb{P}^1$, *i.e.,* we have the following commutative diagram:

$$
\begin{array}{ccc}
Z & \longleftarrow & Z_x \\
G\downarrow & & \downarrow \\
\mathbb{P}^1_K & \xleftarrow{\phi} & X
\end{array}
$$

We observe that $Z_x \to X$ is Galois with a group G and is defined over K. It is clear that Z_x is irreducible since at the point P_a of X (see Step 2) $Z_x \to X$ specializes to the field extension M/F. Similarly for any $h \in H$ the element $h(x) \in K(X)$ defines a map $X \xrightarrow{\phi_h} \mathbb{P}^1$. As above we can obtain regular G-Galois covers $Z_{h(x)} \to X$ as pullbacks of $Z \xrightarrow{G} \mathbb{P}^1$ along these maps $X \xrightarrow{\phi_h} \mathbb{P}^1$. Note that all $Z_{h(x)}$ are irreducible because of the specialization at the point P_a of X.

We claim that, for $h_1 \neq h_2 \in H$, $Z_{h_1(x)} \to X$ and $Z_{h_2(x)} \to X$ are disjoint over X. One can see that from the fact that they specialize to linearly disjoint field extensions over F at F-rational point P_a of X lying above $t = a$ in the covering $X \xrightarrow{H} \mathbb{P}$. ($h_1(M)$ and $h_2(M)$ are linearly disjoint over F, since the tensor product $\bigotimes_{h \in H, F} h(M) = \tilde{F}$ is a *field.*)

• *Step* 6. Let $Y = \bigtimes_{h \in H, X} Z_{h(x)} \to X$ be the fibered product of all $Z_{h(x)} \to X$ over X. This is clearly an irreducible Galois covering of X with Galois group $\bigoplus_{h \in H} G_h$ where each G_h is a copy of G. Consider the covering $Y \to \mathbb{P}^1$ obtained by composing $Y \to X \xrightarrow{H} \mathbb{P}^1$. It is clear that this covering $Y \to \mathbb{P}^1$ is the Γ-Galois branched covering which is defined over K. Finally, it specializes at $t = 0$ to L/K and at $t = a$ to $\tilde{F}/K$ which are disjoint over K, and thus these two specializations force this covering to be regular. $\square$

Proof of Corollary 1.2. It follows immediately from Theorem 1.1. If L/K is any Γ-Galois extension of *fields*, from Theorem 1.1 we obtain a regular Γ-Galois branched covering $Y \to \mathbb{P}^1$ defined over K which specializes to L/K at $t = 0$. This corresponds precisely to Γ having the arithmetic lifting property, according to the definition of this property. $\square$

Proof of Corollary 1.3. Let $G = A$ be an abelian group, which has a generic extension over K. Suppose the orders of A and H are relatively prime. We consider any extension of H by A which is necessarily a semidirect product $A \rtimes H$. Let L'/K be an $A \rtimes H$-Galois extension of fields. We need to show that it lifts to a regular $A \rtimes H$-Galois covering defined over K. As in [Bl2] we use Saltman's idea to reduce to considering wreath product instead [Sa]. We present it here for the convenience of the reader. Let $N = \bigoplus_{h \in H} A_h$, where each A_h is a copy of A. The group H acts on N by permuting the direct summands in the usual way. The semidirect product $N \rtimes H$ is the wreath product of A with H. Suppose now, that $\tilde{G} = A \rtimes H$ is any semidirect product of A and H. Then $\tilde{G}$ is a homomorphic image of the wreath product $\Gamma = A \wr H$. If the orders of A and H are relatively prime then the surjection $A \wr H \to A \rtimes H$ splits.

Since the surjection $f : \Gamma \to \tilde{G}$ splits, there exists a subgroup G' of Γ, isomorphic to $\tilde{G}$, and such that $\ker(f) \cap G' = (1)$ and $\Gamma = \ker(f)G'$. Thus we can identify the Galois group of L'/K with G'. Let $L = Ind_{G'}^{\Gamma}(L')$ [Sa, Prop.0.3]. Then the extension of K-algebras L/K is Galois with the group Γ. (Here L need not be a field, but it is of course the direct sum of fields.) Note that if E denotes the fixed field of A in L', then E is also a fixed field of N in L. By Theorem 1.1 there exists a Γ-Galois regular branched covering $Y \to \mathbb{P}^1$ defined over K which specializes to L/K at some K-rational point y. It is clear that $Y/\ker(f) = Y' \to \mathbb{P}^1_K$ is a $\tilde{G}$-Galois regular covering specializing to L'/K at the point y. (Recall that f here is a homomorphism $\Gamma \to \tilde{G}$.) □

Remark. We assume that K is a hilbertian field. In our proof this assumption is used in steps 2 and 3 to obtain "good" specializations of Galois extensions of purely transcendental extensions of K. If K is any field, then $\mathcal{K} = K(s)$ with s inderterminate is hilbertian. It has been observed by P. Dèbes that if a finite group G has the arithmetic lifting property over $K(s)$, then it has this property over K. The converse of this is unknown.

Note also that if a group G has a generic extension over K, then it has it over any overfield of K, in particular over $K(s)$. Thus, in the results of this note one may remove the hypothesis on the base field being hilbertian at the expense of assuming that H must satisfy the arithmetic lifting property over $K(s)$ instead of just over K.

Acknowledgement

References

[Bl1]   E. Black, *Deformation of dihedral 2-group extensions of fields*, Trans. Amer. Math. Soc. **351** (1999), 3229–3241. MR **99m:**12004

[Bl2]   E. Black, *On semidirect products and the arithmetic lifting property*, J. London Math. Soc. (2) **60** (1999), 677–688. CMP 2000:11

[CHR]   S.U. Chase, D.K. Harrison and A. Rosenberg, *Galois theory and Galois cohomology of communitive rings*, Mem. Amer. Math. Soc. **52** (1965), 15–33. MR **33:**4118

[MaMa] G. Malle and B.H. Matzat, *Inverse Galois theory*, Springer-Verlag, Berlin-Heidelberg-New York-Tokyo, 1999. CMP 2000:02

[Sa]   D. Saltman, *Generic Galois Extensions and Problems in Field Theory*, Advances in Math **43** (1982), 250–283. MR **84a:**13007

[Se]   J-P. Serre, *Topics in Galois theory*, Notes written by Henri Darmon, Jones and Bartlett Publ., Boston, 1992. MR **94d:**12006

Department of Mathematics, University of Oklahoma, Norman, Oklahoma 73019
E-mail address: eblack@math.ou.edu