TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 351, Number 8, Pages 3229–3241
S 0002-9947(99)02135-2
Article electronically published on February 10, 1999

DEFORMATIONS OF DIHEDRAL 2-GROUP EXTENSIONS OF FIELDS

ELENA V. BLACK

ABSTRACT. Given a G-Galois extension of number fields L/K we ask whether it is a specialization of a regular G-Galois cover of $\mathbb{P}^1_K$. This is the "inverse" of the usual use of the Hilbert Irreducibility Theorem in the Inverse Galois problem. We show that for many groups such arithmetic liftings exist by observing that the existence of generic extensions implies the arithmetic lifting property. We explicitly construct generic extensions for dihedral 2-groups under certain assumptions on the base field k. We also show that dihedral groups of order 8 and 16 have generic extensions over any base field k with characteristic different from 2.

INTRODUCTION

One of the central questions of Galois theory is whether all finite groups appear as Galois groups over a field K. If the field in question is the field of rationals or more generally a number field, this becomes the famous Inverse Galois problem. When asking this question with $K = \mathbb{Q}(t)$ one ordinarily considers only "geometric" extensions of $\mathbb{Q}(t)$, *i.e.* those that arise from an absolutely irreducible Galois branched covering of $\mathbb{P}^1_{\mathbb{Q}}$ (rather than, say, from an extension of $\mathbb{Q}$). If one can show that a finite group G appears as a Galois group over $\mathbb{Q}(t)$, one can then invoke Hilbert's Irreducibity Theorem to get G as a Galois group over the rationals. Thus Hilbert's Irreducibility Theorem provides a bridge from the inverse Galois problem for $\mathbb{Q}(t)$ to the same problem for $\mathbb{Q}$. What about the bridge in the other direction? Is it true that every Galois extension of the rationals arises as a specialization of some absolutely irreducible Galois branched covering of the projective line defined over $\mathbb{Q}$ and with the same group? We call such cover an *arithmetic lifting* of the given Galois extension.

In section 1 of this paper we discuss the connections between the Noether Problem for a finite group G, generic extensions for G over some base field k and the arithmetic lifting of G-Galois extensions of k. We show by a simple argument that the existence of a generic extension for G over k implies the arithmetic lifting property.

In section 2 we construct generic extensions for dihedral group D_{2^d} with the assumption that the 2^d-th roots of unity are contained in the base field k. In section 3, we relax this condition on the base field and just assume that $\zeta_{2^d} + \zeta_{2^d}^{-1}$ lies in k. Finally, in section 4, we show that D_8, the dihedral group of order 16, has

Received by the editors May 15, 1996 and, in revised form, September 18, 1996 and April 18, 1997.

1991 *Mathematics Subject Classification.* Primary 11R32, 11R58, 14E20, 14D10; Secondary 12F12, 12F10, 13B05.

a generic extension over k (and thus satisfies an arithmetic lifting property) without any assumptions on the base field k. The constructions in sections 2 and 3 employ the method used in [Sa] based on working over a field with all appropriate roots of unity and descending to k via the interplay between the action of D_{2^d} and the cyclotomic Galois group. In section 4, we use a different method based on resolving an obstruction in the Brauer group of K to the problem of embedding D_4-Galois extensions into D_8-Galois extensions.

I would like to thank Kevin Coombes and David Harbater for helpful conversations concerning material presented in this paper. My thanks also go to the referee who pointed out that the proofs in sections 2, 3 and 4 could be modified to imply an existence of generic extensions rather than just the weaker arithmetic lifting property.

0. Notation, definitions and background

Throughout this paper a ground field k has characteristic different from 2. A cyclic group of order n is denoted by C_n, and D_n denotes the dihedral group of order $2n$. By ζ_n we denote a primitive n-th root of unity and μ_n is a group of n-th roots of 1.

Let κ be an algebraically closed field. Let G be a finite group. 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 $X \to \mathbb{P}^1_\kappa$ is a *branched covering*. Let G be a finite group. A *G-Galois branched 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 $X \xrightarrow{G} \mathbb{P}^1_\kappa$ has a *model* $X_K \xrightarrow{G} \mathbb{P}^1_K$ over K if the following hold:

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-Galois branched 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 an 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 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 the 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.

Finally, 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.

1. Noether's problem, generic extensions and lifting property $\mathcal{L}Gal_{K(t)}$

We say that a finite group G has the lifting property $\mathcal{L}Gal_{K(t)}$ if every G-Galois extension of K arises from a specialization of a G-Galois regular branched covering of $\mathbb{P}^1_K$ defined over K. Thus the question discussed in the introduction becomes the question of whether for a given number field K, every finite group G has the property $\mathcal{L}Gal_{K(t)}$. This question is connected with Noether's problem and with the question of generic extensions [Sa].

Noether's problem arose from Noether's original idea for building Galois groups over the rationals. Any finite group G can be embedded as a transitive subgroup of S_n for some n. So, G acts on affine n-space $\mathbb{A}^n$ by permuting coordinates. The quotient scheme will give a G-cover $\mathbb{A}^n \to X = \mathbb{A}^n/G$. Then Noether's problem is whether X is a rational variety, *i.e.*, whether X is birationally isomorphic to an affine space $\mathbb{A}^n$. For example, Noether's problem is true for the symmetric group S_n for any n and for the alternating groups A_n for $n < 6$.

Saltman [Sa] introduced a related notion of a generic extension for a group G. 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.

Remark. Saltman's original definition of a generic extension for G over k was given in terms of Galois extension of rings ([Sa], p. 255). A G-Galois extension of commutative k-algebras S/R is defined to be a generic extension for G over k, if R is a localized polynomial ring over k, and for any G-Galois extension L/K of k-algebras with K a field, there is a k-algebra map $f : R \to K$ such that $L \cong S \otimes_f K$, the isomorphism preserving the respective G actions. The map f is called specialization.

Theorem 1.1. *Let G be a finite group and let k be a field. If G satisfies Noether's problem over k, then there is a generic extension for G over k.*

Proof. See [Sa], Theorem 5.1. □

Remark. It has been brought to our attention by B. H. Matzat that if G satisfies *generalized* Noether's problem over k, then there is a generic extension for G over k. As mentioned above in a classical version, Noether's problem poses the question whether the invaraiant field of a *permutation* group G acting on the rational function field is purely transcendental over the ground field. Let $G \leq GL_m(k)$ be a finite *linear* group. Then G acts on the indeterminates by linear transformations. The affirmative answer to Noether's problem in this case implies an existence of a generic extension for G over k. (See for example [Ke] (Th. 1.9).) The referee pointed out that this result first appeared in [Sa2].

The converse of Theorem 1.1 is not true. In [Sa] Saltman constructed explicitly generic extensions for all abelian groups of odd order n over fields of characteristic prime to n. But Swan [Sw] has shown the cyclic group C_{47} to be a counterexample to the Noether's problem over $\mathbb{Q}$.

Proposition 1.2. *Let G be a finite group and let k be a field. If there exists a generic extension for G over k, then G satisfies property $\mathcal{L}Gal_{K(t)}$ for any field K containing k.*

Proof. Note that if a group G has a generic extension over some base field k, then it also has a generic extension over any field K containing k (obtained by a base change). Thus, it suffices to show that if G has a generic extension over K, then G satisfies the property $\mathcal{L}Gal_{K(t)}$.

Assume that $Spec(S) \to U$ is a generic extension for G over K. Let L/K be a G-Galois extension. Then by the versal specialization property there is a K-rational point on U, say x, such that specialization at this point yields L/K. Now, consider a G-Galois extension of K-algebras M/K with M corresponding to a product of m copies of K, where m is the order of the group G, and where G acts on M by permuting the factors. Again, by the versal specialization property there is a K-rational point on U, say $y \in U$, such that specialization at y gives M/K. Recall that $U \subset \mathbb{A}^n$ is a basic affine set. Then the intersection X of U and a line in $\mathbb{A}^n$ through points x and y is isomorphic to Zariski open subset of $\mathbb{P}^1$. We have an embedding $X \xrightarrow{i} U$. The pullback of $Spec(S) \to U$ along this embedding i gives us an étale G-Galois covering of X defined over K, which we close to obtain G-Galois branched covering $Y \to \mathbb{P}^1$ defined over K. Recall that at the point $x \in U$ the specialization of $Spec(S) \to U$ is L/K. Since x also lies on $X \subset \mathbb{P}^1_K$ by design, the specialization at x of $Y \to \mathbb{P}^1$ is also L/K. We only need to show now that the constructed cover $Y \to \mathbb{P}^1_K$ is regular. This cover specializes to M/K at the point $y \in X \subset \mathbb{P}^1_K$. So points on Y above y are K-rational and this implies that the covering $Y \to \mathbb{P}^1_K$ is regular. □

Remark. It has been pointed out by the referee that Proposition 1.2 easily follows from Theorem 5.3 in [Sa]. In this theorem it is shown that if G has a generic Galois extension, then G has a so-called lifting property; that is, for any semilocal k-algebra T with Jacobson radical $J(T)$, and all G-Galois extensions L'/K' with $K' = T/J(T)$, there is a Galois extension T'/T such that $T' \otimes_T T/J(T) \cong L'$. Let $K(t)$ denote a function field of $\mathbb{P}^1_K$. There is a semilocal ring $R \subset K(t)$ with two primes such that localizations of R are local rings associated to $t = 0$ and $t = 1$, and $R/J(R) = K \oplus K$. If L/K is our given G-Galois extension, let L_1/K be the trivial G-Galois extension, and therefore $L \oplus L_1$ is G-Galois extension over $K \oplus K$. The lifting property says that this lifts to a G-Galois extension T/R, and we set $\mathcal{L} = T \otimes_R K(t)$. Then $\mathcal{L}/K(t)$ is a G-Galois extension of fields (since L is a field), and it is a regular extension since it specializes to L_1/K as well.

The converse of the Proposition 1.2 is not true. There is no generic extension over $\mathbb{Q}$ for a cyclic group of order 8 [Sa]. However, Beckmann [Be] constructed an arithmetic lifting of any A-Galois extension L/K, where K is any number field and A is any abelian group. In particular, C_8 satisfies property $\mathcal{L}Gal_{K(t)}$ for any number field K.

It follows from the work of Saltman and Proposition 1.2, that dihedral groups D_n with n odd satisfy the property $\mathcal{L}Gal_{K(t)}$ for any number field K. (For this case arithmetic liftings for D_n-Galois extensions of fields L/K were explicitly constructed in [Bl].) When n is divisible by $q = 2^d$ and $d \geqslant 3$ it was not known if there are generic extensions for D_n over the ground field k. In sections 2 and 3 we show that if the ground field k with $Char(k) \neq 2$ contains $\zeta_q + \zeta_q^{-1}$ or ζ_q, then there is a generic extension for D_q over k. Finally in section 4 we treat the case when $q = 8$ and k is *any* field of characteristic different from 2. We show there is a generic extension for D_8 in this case as well.

Remark. It may appear that there is a redundancy in sections 2 and 3. A general fact mentioned earlier is that if a finite group G has a generic extension over a field k, then it has a generic extension over any overfield k' of k. Thus it appears that if D_q has a generic extension over k, such that $\zeta_q + \zeta_q^{-1} \in k$ (as shown in section 3), then this group has a generic extension over k' containing ζ_q (as shown in section 2). (Throughout $q = 2^d$ for some d.) However, the argument in section 3 uses the results of section 2. There are two cases depending on whether there exists an automorphism of $k(\zeta_q)$ sending ζ_q to ζ_q^{-1} or not. Certainly if the characteristic of k is zero, such an automorphism exists and in this case the methods of section 3 are sufficient. However, if the base field k has positive characteristic, this is not always the case. For some $p = Char(k)$ such automorphism does not exist. That situation occurs if p is not congruent to $-1 \pmod q$. But in this case if $\zeta_q + \zeta_q^{-1} \in k$, then $\zeta_q \in k$, so one can apply an argument in section 2. Thus, the methods of section 2 handle the case when $Char(k) = p$ such that $\zeta_q + \zeta_q^{-1} \in k$ implies $\zeta_q \in k$, and the methods of section 3 deal with the situation when $k(\zeta_q)$ has an automorphism which sends ζ_q to ζ_q^{-1}.

2. Dihedral group D_{2^d} for $d \geq 2$ and k containing roots of unity

We let $q = 2^d$ and k be a field with $Char(k) \neq 2$. For this section we impose the condition that the base field k contains the q-th roots of unity. We prove here that dihedral group D_q has a generic extension over k.

Proposition 2.1. *Let $q = 2^d$ with $d \geq 2$. Let k be a field with $Char(k) \neq 2$, such that $\zeta_q \in k$. Then there is a generic extension for D_q over k.*

Proof. First we investigate extensions of k-algebras L/K with K a field, which are Galois with Galois group D_q. Let L/K be a Galois extension of k-algebras with Galois group D_q. Let E/K denote the quadratic subextension of L/K, obtained by taking the fixed ring of $C_q \lhd D_q$. Let σ denote a generator of $Gal(E/K)$ and let τ denote a generator of $Gal(L/E)$. By Kummer theory there is an element $\alpha \in E^\times$ such that L is obtained by adjoining the q-th root of α to E. We claim that α is of the form $\frac{\nu}{\sigma(\nu)}\beta^{q/2}$, for some $\nu \in E^\times$ and $\beta \in K^\times$. To see this, let y be a canonical primitive element of L/E; *i.e.*, $\tau(y) = y\zeta_q$ and $y^q = \alpha$. Since $\tau^{-1}\sigma = \sigma\tau$, it easily follows that $\sigma(y)y = \beta$ is invariant under both τ^{-1} and σ. For,

$$\tau^{-1}\sigma(y) = \sigma\tau(y) = \sigma(y\zeta_q) = \sigma(y)\zeta_q.$$

So then

$$\tau^{-1}(\sigma(y)y) = \tau^{-1}\sigma(y)\tau^{-1}(y) = \sigma(y)\zeta_q y\zeta_q^{-1} = \sigma(y)y.$$

Then $\sigma(y) = \beta/y$, and $\sigma(\alpha) = \beta^q/\alpha$ for some $\beta \in K$.

Next we have $\sigma(\alpha)\alpha = \beta^{q/2}\sigma(\beta^{q/2})$ or $\sigma(\alpha/\beta^{q/2}) = \beta^{q/2}/\alpha$. By Hilbert's Theorem 90, there is a $\nu \in E$ such that $\frac{\alpha}{\beta^{q/2}} = \frac{\nu}{\sigma(\nu)}$. So we can write $\alpha = \frac{\nu}{\sigma(\nu)}\beta^{q/2}$.

We are now ready to construct a generic extension for D_q over k. We form a localized polynomial ring $S = k[x_0, x_1, y](1/x_0x_1y)$. Let C_2 with generator ρ act on S by having $\rho(x_i) = x_{1-i}$ and acting trivially on y and k. Set $T = S[z]/(z^q - (x_0/x_1)y^{q/2})$. Let z be a canonical generator of T/S; thus $\tau(z) = \zeta_q z$ where τ generates the cyclic group $Gal(T/S)$ ([Sa], Prop. 0.6a). Extend the action of ρ to T by setting $\rho(z) = \frac{1}{z}y$. It is clear that $\rho\tau = \tau^{-1}\rho$ and T/R is a Galois extension with Galois group D_q. To show that in fact it is a generic extension for D_q over k, we first observe that $R = k[t_0, t_1, y](1/t_1y)$, where $t_0 = x_0 + x_1$ and

$t_1 = x_0x_1$, and therefore R is a localized polynomial ring. It remains to show that T/R has the versal specialization property. Let L/K be D_q-Galois extension of k-algebras, with K a field. Then $L = E[z]/(z^q - \alpha)$, where E/K is the quadratic subextension of L/K, $\alpha = \frac{\nu}{\sigma(\nu)}\beta^{q/2}$ with $\nu \in E$ and $\beta \in K$. We define a function $\phi : R \to K$ by sending $t_0 \to \nu + \sigma(\nu) \in K$, $t_1 \to \nu\sigma(\nu) \in K$ and $y \to \beta$. It is clear that $T \otimes_\phi K = L$ and hence extension T/R does indeed specialize to L/K, as desired. □

3. Dihedral group of order D_{2^d} when $\zeta_{2^d} + \zeta_{2^d}^{-1}$ lie in k

In this section we turn our attention to the group D_q, $q = 2^d, d \geq 2$ with the assumption that $\zeta_q + \zeta_q^{-1}$ lies in the ground field k, with $Char(k) \neq 2$. In this section we show that there exists a generic extension for D_q over k.

Throughout this section we let L/K be a Galois extension of k-algebras, with K a field, with its Galois group isomorphic to the dihedral group $D_q \cong C_q \rtimes C_2$. Let E/K be the quadratic subextension of L/K fixed by C_q. Let $K' = K \otimes_k k(\mu_q)$, $E' = E \otimes_k k(\mu_q)$ and $L' = L \otimes_k k(\mu_q)$. We fix notation for the generators of the various Galois groups. We denote by ϕ a generator of $Gal(k(\mu_q)/k) = \Phi_q$, by σ a generator of $Gal(E/K)$ and by τ a generator of $Gal(L/E)$. We extend the action of ϕ to K', E' and L' by letting it act on $k(\mu_q)$ in its usual Galois way and trivially on K, E and L respectively. Similarly we extend the action of σ to $E' = E \otimes_K K'$ and L'. We have $L' = L \otimes_E E'$. Define an extension of τ to $Aut(L')$ by making it act as the identity on E' and by the Galois action on L. By slight abuse of notation we still write ϕ, τ and σ for all these extension automorphisms. Note that actions of σ and ϕ on E' commute. Let K'' denote a fixed ring of E' under an automorphism $\sigma\phi$.

Lemma 3.1. *Let k be a field of characteristic different from 2. Assume that $\zeta_q + \zeta_q^{-1} \in k$ but ζ_q does not lie in k. Let K, E, L, K', E', L' be as above. Then $L' = E'[z]/(z^q - \alpha)$ where α lies in $(E')^{\sigma\phi} = K''$ and there are elements $a \in K^\times$ and $\nu \in (K'')^\times$ such that*

$$\alpha = \frac{\nu}{\sigma(\nu)}a^{q/2}.$$

Proof. Note that with our assumptions on k an automorphism ϕ is an involution which sends ζ_q to ζ_q^{-1}. We have σ, ϕ and τ in $Aut(L')$ and the following identities hold: $\phi\sigma = \sigma\phi$, $\tau\phi = \phi\tau$ and $\sigma\tau = \tau^{-1}\sigma$. Of course, σ and ϕ are involutions, while τ is an element of order q. We also note that the extension L'/K'' is a dihedral extension with the Galois group D_q generated by τ and $\phi\sigma$. The fixed field of τ in this extension is E'. Since $\mu_q \in E'$ and E' is a direct sum of fields, by Kummer theory $L' = E'[z]/(z^q - \alpha)$ for some $\alpha \in (E')^\times$. We claim that α can actually be chosen to lie in K''. Let z be a canonical primitive element of L'/E' so that $\tau(z) = z\zeta_q$. We have a relation $(\sigma\phi)\tau = \tau^{-1}(\sigma\phi)$. It easily follows from this relation that the element $\sigma\phi(z)/z$ is invariant under τ^{-1} (and hence under τ).

To see this, write

$$\tau^{-1}\left(\frac{\sigma\phi(z)}{z}\right) = \frac{\tau^{-1}\sigma\phi(z)}{\tau^{-1}(z)} = \frac{\sigma\phi\tau(z)}{z\zeta_q^{-1}} = \frac{\sigma\phi(z)\zeta_q^{-1}}{z\zeta_q^{-1}} = \frac{\sigma\phi(z)}{z}.$$

So there is an element $\gamma \in E'$ such that $\sigma\phi(z) = z\gamma$. Since $(\sigma\phi)^2 = id$, we have

$$z = (\sigma\phi)^2(z) = \sigma\phi(z\gamma) = z\gamma\sigma\phi(\gamma),$$

and so $\gamma\sigma\phi(\gamma) = 1$. By Hilbert's Theorem 90, there is an element $u \in E'$, such that $\gamma = u/\sigma\phi(u)$, which implies that αu^q is invariant under $\sigma\phi$. That shows that α can be chosen to lie in K''. Moreover, we can pick a canonical generator z of L'/E' so that $\sigma\phi(z) = z$.

Since τ and ϕ commute, one easily checks that the element $\phi(z)z$ is invariant under the action of τ. For,

$$\tau\phi(z) = \phi\tau(z) = \phi(z\zeta_q) = \phi(z)\zeta_q^{-1}.$$

We then have

$$\tau(\phi(z)z) = \tau(\phi(z))\tau(z) = \phi(z)\zeta_q^{-1}z\zeta_q = \phi(z)z.$$

It is also clearly invariant under the action of ϕ. So, $\phi(z) = \beta/z$, for some $\beta \in E$. Further, because of the anticommutativity of σ and τ, one easily checks that the element $\sigma(z)z$ is fixed both under τ and σ; hence, we can write $\sigma(z) = \gamma/z$ for some γ in K'. Recall that $\alpha = z^q$, so we get $\sigma(\alpha) = \gamma^q/\alpha$, and $\phi(\alpha) = \beta^q/\alpha$, for $\gamma \in K'$ and $\beta \in E$. We can also conclude that $\beta = \gamma$ because of commutativity of σ and ϕ and the fact that $\sigma\phi(z) = z$. Therefore $\beta = \gamma = a$ is an element of $K^\times$, being fixed by ϕ, σ and τ. Now, $\sigma(\alpha) = \phi(\alpha) = a^q/\alpha$, and hence

$$N_{K''/K}(\alpha/a^{q/2}) = 1.$$

By Hilbert's Theorem 90, there are $\nu \in (K'')^\times$ such that $\alpha = \frac{\nu}{\sigma(\nu)}a^{q/2}$, as claimed. □

Before turning our attention to a generic extension for D_q over k, we need a general lemma in the spirit of Saltman's results [Sa, Thm. 2.4(a, b)]. Let R, S be k-algebras, and let $R' = R \otimes_k k(\mu_q)$ and $S' = S \otimes_k k(\mu_q)$. For this lemma we let S/R be a C_2-Galois extension of k-algebras. Let the generator of this Galois group be denoted by ρ. Let the generator of $Gal(S'/S)$ be denoted by ϕ. Assume that S and $k(\mu_q)$ are disjoint over k.

Lemma 3.2. *Let elements $\lambda, \nu \in S'$, $\beta \in S$ and $\gamma \in R'$ be such that*

$$\frac{\lambda}{\phi(\lambda)}\beta^{q/2} = \frac{\nu}{\rho(\nu)}\gamma^{q/2}$$

and $\beta\rho(\beta) = \gamma\phi(\gamma)$. Let $\alpha = \frac{\lambda}{\phi(\lambda)}\beta^{q/2}$. Let $T' = S'[z]/(z^q - \alpha)$. Then $T' = T \otimes_R R'$ for some D_q- Galois extension T/R.

Proof. Let τ denote a generator of $Gal(T'/S')$, and let z be a canonical generator of T' over S', *i.e.* $\tau(z) = z\zeta_q$ and $z^q = \alpha$. Extend ϕ to $Aut(T')$ by defining $\phi(z) = \frac{1}{z}\beta$. Since $\alpha = \lambda/\phi(\lambda)\beta^{q/2}$ for $\beta \in S$, by Saltman [Sa, Thm. 2.4(a)] there is a C_q-Galois extension of T/S such that $T' = T \otimes_S S'$. In fact, T is just the fixed field of $\langle\phi\rangle$. Extend ρ to $\rho \in Aut(T')$ by defining $\rho(z) = \frac{1}{z}\gamma$. One easily checks the identities $\phi\tau = \tau\phi$, $\rho\tau = \tau^{-1}\rho$, $\rho^2 = id$ and $\phi^2 = id$. Finally, because $\beta\sigma(\beta) = \gamma\phi(\gamma)$, we have $\phi\rho = \rho\phi$. The last identity ensures that ρ restricted to T gives an element of $Gal(T/R)$ and that ρ restricted to S is equal to $\rho \in Gal(S/R)$. It is clear then that $Gal(T/R) = D_q$. □

We are now in the position to prove

Theorem 3.3. *Let $q = 2^d$ where $d \geq 2$. Let k be a field with $Char(k) \neq 2$ and such that $\zeta_q + \zeta_q^{-1} \in k$. Then there is a generic extension for D_q over k.*

Proof. We start by noting that if $\zeta_q \in k$, the statement of the theorem has been proved in Proposition 2.1. Thus for the rest of the proof, we assume that ζ_q is not in k and ϕ is an involution which sends ζ_q to ζ_q^{-1}.

Form the k-algebra $S' = k(\mu_q)[x_0, x_1, y](\frac{1}{x_0 x_1 y})$. Extend the action of the generator ϕ of $Gal(k(\mu_q)/k)$ to S' by letting ϕ act trivially on y and setting $\phi(x_i) = x_{1-i}$. Define $\rho \in Aut(S')$ by letting ρ act trivially on $k(\mu_q)$ and y and setting $\rho(x_i) = x_{1-i}$. Note that the actions of ϕ and ρ commute and therefore we have defined the action of $G = C_2 \oplus C_2$ on S'. We now let $R = S'^G$ and $S = S'^\phi$. It is clear that S/R is a C_2-Galois extension of k-algebras with its Galois group generated by ρ (that is, ρ restricted to S). Set $T' = S'[z]/(z^q - \frac{x_0}{x_1} y^{q/2})$. By Lemma 3.2, there exists a k-algebra T, such that T/R is a Galois extension with Galois group D_q and $T' = T \otimes_R R'$ (here $\lambda = \nu = x_0$ and $\beta = \gamma = y$). Recall from the proof of Lemma 3.2 that we extended the action of ϕ to T' by setting $\phi(z) = \frac{1}{z} y$ and $T = (T')^\phi$.

We claim that T/R is a generic extension for D_q over k. We first note that it is clear that R is a localized polynomial ring over k, since it is of the form $k[t_0, t_1, y](\frac{1}{t_1 y})$ with $t_0 = x_0 + x_1$ and $t_1 = x_0 x_1$. It remains to show that any D_q-Galois extension of k-algebras L/K with K a field is a specialization of T/R. Let L/K be a D_q-Galois extension of k-algebras, with K a field. As before, let E/K denote the quadratic subextension of L/K. By Lemma 3.1, there exist $a \in K'$ and $\nu \in K''$ such that $L' = E'[z]/(z^q - \alpha)$ with $\alpha = \frac{\nu}{\sigma(\nu)} a^{q/2}$. Define a k-algebra homomorphism $f'' : S' \to E'$ by setting $x_0 = \nu$, $x_1 = \sigma(\nu)$ and $y = a$. Note that f'' preserves the action of ρ on S' and σ on E' and so induces k-algebra homomorphism $f' : R' \to K'$. It is clear that $L' = T' \otimes_{f'} K'$ as Galois extensions of K'. Since f'' preserves the action of ϕ, so does f'. Therefore, f' induces a map $f : R \to K$. Taking ϕ-fixed subrings, we have that f realizes L/K. This concudes the proof of the Theorem 3.3. □

Corollary 3.4. *With q and k as above, let K be an overfield of k. Then D_q satisfies property $\mathcal{L}Gal_{K(t)}$.*

Proof. Use Theorem 3.3 and Proposition 1.2. □

Remark. We can now improve the result on arithmetic lifting of the dihedral groups D_n, where n is odd [Bl]. Let L/K be a Galois extension of number fields with the Galois group D_n. Let $q = 2^d$ be the highest power of 2 dividing n. Assume that $\zeta_q + \zeta_q^{-1}$ lies in K. Then there exists a regular D_n-Galois branched covering $X_K \to \mathbb{P}^1_K$ defined over K which specializes to L/K at $t = 0$. (See [Bl] on how, via use of fibered products, one passes from D_q for q a prime power to D_n for composite n.)

4. Dihedral group of order 16

In this section we retain the notation from above. Thus, D_8 denotes the dihedral group of order 16, $D_8 \cong C_8 \rtimes C_2$. Throughout this section let k be a field with $Char(k) \neq 2$ and let K be an overfield of k. Let R be a Noetherian regular local k-algebra with the maximal ideal M and the field of fractions $\mathcal{K}$. Note in particular that since R is regular local it is a domain.

For any field K, we denote the Brauer group of K and its two-torsion part by $Br(K)$ and $Br_2(K)$, respectively. An element in $Br_2(K)$ corresponding to a quaternion algebra generated by $a, b \in K^\times$ is denoted by (a, b).

Let $f : \Gamma \to G$ be an epimorphism of finite groups. We have an exact sequence of groups

$$1 \to N \to \Gamma \to G \to 1$$

where N is the kernel of f. The embedding problem for G-Galois extension of k-algebras S/R asks if there is a Galois extension T/R containing S with Galois group Γ so that the surjection $f : \Gamma \to G$ is a natural projection of Galois groups. If the answer to this question is affirmative for G-Galois extension S/R we say that S/R has a solvable embedding problem for Γ. We call an embedding problem a *central embedding problem* if N lies in the center of Γ. An embedding problem is called *Frattini* if N lies in the Frattini subgroup of Γ.

Lemma 4.1. *Let G be a finite group and S/R be a G-Galois extension of k-algebras. Let $1 \to N \to \Gamma \to G \to 1$ be a central embedding problem. Then any two solutions of the embedding problem for S/R differ by an element in $H^1_{et}(R, N)$. Conversely, given a solution of the embedding problem and an element α of $H^1_{et}(R, N)$ there is another solution which differs from a given one by α. Moreover, if $N = C_n$ cyclic of order n and $\zeta_n \in R$, then any two solutions of the embedding problem differ by a choice of $q \in R^\times$.*

Proof. Let ρ_1, ρ_2 be two homomorphisms from the fundamental group $\pi_1(Spec\, R)$ to Γ corresponding to two solutions of the embedding problem. Thus $f(\rho_1(\sigma)) = f(\rho_2(\sigma))$ for all $\sigma \in \pi_1(Spec\, R)$. Define a map from $\pi_1(Spec\, R)$ to N by sending $\sigma \to a_\sigma = \rho_1(\sigma)\rho_2(\sigma)^{-1}$ for all $\sigma \in \pi_1(Spec\, R)$. Note that $a_\sigma \in N$ since $f(a_\sigma) = 1$. We claim that the map defined above is a group homomorphism from $\pi_1(Spec\, R) \to N$, and so is an element of $H^1_{et}(R, N)$. Let σ, τ be elements of $\pi_1(Spec\, R)$, then

$$\begin{aligned} a_{\sigma\tau} &= \rho_1(\sigma\tau)\rho_2(\sigma\tau)^{-1} = \rho_1(\sigma)\rho_1(\tau)\rho_2(\tau)^{-1}\rho_2(\sigma)^{-1} \\ &= \rho_1(\sigma)a_\tau\rho_2(\sigma)^{-1} = \rho_1(\sigma)\rho_2(\sigma)^{-1}a_\tau = a_\sigma a_\tau. \end{aligned}$$

We used, of course, the fact that a_τ is in the center of Γ and commutes with $\rho_2(\sigma)^{-1}$.

To see the converse, let ρ_1 correspond to a given solution of the embedding problem. Let $\alpha \in H^1_{et}(R, N)$ be a group homomorphism and $a_\sigma = \alpha(\sigma) \in N$ for all $\sigma \in \pi_1(Spec\, R)$. Define $\rho_2(\sigma) = \rho_1(\sigma)a_\sigma^{-1}$ for all $\sigma \in \pi_1(Spec\, R)$. It is easy to see that ρ_2 is a homomorphism corresponding to another solution of the embedding problem. It is also clear that ρ_1 and ρ_2 differ by α.

Now, if $N \cong C_n$ and $\zeta_n \in R$, then $H^1_{et}(R, N) \cong R^\times/R^{\times n}$ by Kummer theory, and the statement of the lemma follows. If $R = K$ is a field, $H^1_{et}(R, -)$ is $H^1(K, -)$, and $\pi_1(Spec\, R)$ is replaced by Gal_K, the absolute Galois group of K. □

Lemma 4.2. *Let R be a Noetherian regular local k-algebra as above. Let $1 \to C_2 \to \Gamma \to G \to 1$ be a central Frattini embedding problem with cyclic kernel of order 2. Let S/R be a G-Galois extension of local k-algebras (so S is also a regular local domain). Let $\mathcal{L}/\mathcal{K}$ be the G-Galois extension of quotient fields of S/R. Assume that the extension $\mathcal{L}/\mathcal{K}$ has a solvable embedding problem for Γ. Then S/R also embeds into Γ-Galois extension T/R, i.e., S/R has a solvable embedding problem for Γ as well.*

Proof. By assumption $\mathcal{L}/\mathcal{K}$ embeds into a Γ-Galois extension $\mathcal{F}/\mathcal{K}$.

1. If $\mathcal{F}/\mathcal{K}$ is unramified at M we let T be an integral closure of R in $\mathcal{F}$. It is clear then that T/R is a required Γ-Galois extension, and S/R has a solvable embedding problem for Γ.

2. Suppose now that $\mathcal{F}/\mathcal{K}$ is ramified at M. Then since S/R is a G-Galois extension of *local* rings, $\mathcal{F}/\mathcal{L}$ is ramified at M (here M is considered an ideal in S). Let $\mathcal{F} = \mathcal{L}(\sqrt{\alpha})$ for some $\alpha \in \mathcal{L}^{\times}$. Let T' be an integral closure of R in $\mathcal{F}$. By the purity of the branch locus ([AlKl], p. 125) applied to (ramified) covering $Spec\, T'/Spec\, R$, the branch locus in $Spec\, R$ has pure codimension 1, which corresponds to an ideal of height 1. Thus there exist $0 \neq s \in M$ such that the ideal (s) contains the discriminant ideal. Since $Char\, k \neq 2$ the ramification is tame. By Abhyankar's Lemma ([SGA1], Exp. X, Lemma 3.6) there exist a nonsquare element $r \in (s) \subset \mathcal{K}$ such that $\mathcal{F} \otimes_{\mathcal{K}} \mathcal{K}(\sqrt{r})$ is unramified at an ideal of the integral closure of R in $\mathcal{K}(\sqrt{r})$ lying above M. Since $\mathcal{L}/\mathcal{K}$ is unramified at M we conclude that $\mathcal{L}$ and $\mathcal{K}(\sqrt{r})$ are disjoint over $\mathcal{K}$, and thus $\mathcal{L} \otimes_{\mathcal{K}} \mathcal{K}(\sqrt{r}) = \mathcal{L}(\sqrt{r})$. Now, $\mathcal{F}$ and $\mathcal{L}(\sqrt{r})$ are disjoint over $\mathcal{L}$ because the embedding problem is Frattini. Thus $\mathcal{F} \otimes_{\mathcal{K}} \mathcal{K}(\sqrt{r}) = \mathcal{F}(\sqrt{r})$. Then the extension $\mathcal{F}(\sqrt{r})/\mathcal{L}$ is biquadratic. Its Galois group is isomorphic to Klein 4-group which has exactly three subgroups of order 2. The inertia group of M (again M here is considered an ideal of S) is a cyclic group of order 2. Since $\mathcal{F}/\mathcal{L}$ and $\mathcal{L}(\sqrt{r})/\mathcal{L}$ are ramified, we have $\mathcal{F}(\sqrt{r})/\mathcal{F}$ and $\mathcal{F}(\sqrt{r})/\mathcal{L}(\sqrt{r})$ are unramified. Thus $\mathcal{F}(\sqrt{r})/\mathcal{F}(\sqrt{\alpha r})$ must be ramified since it corresponds to the only subgroup of order 2 remaining for the role of the inertia group. Therefore $\mathcal{F}(\sqrt{\alpha r})/\mathcal{L}$ is unramified.

By Lemma 4.1, the extension $\mathcal{L}(\sqrt{\alpha r})/\mathcal{K}$ is a solution of the embedding problem for $\mathcal{L}/\mathcal{K}$ and it is unramified at M. We are then reduced to case 1. □

In this section we show that the dihedral group of order 16 has a generic extension over k. In order to do this we use the following tool. As mentioned before it was shown in [Sa] that a finite group G has a generic extension over k if and only if the same pair has a so-called lifting property ([Sa], Thm. 5.3). Recall that G has a lifting property if for any semilocal k-algebra T with Jacobson radical $J(T)$, and all G-Galois extensions L/K with $K = T/J(T)$, there is a Galois extension T'/T such that $T' \otimes_T T/J(T) \cong L$. However, closer examination of the proof of the Theorem 5.3 in [Sa] reveals that in order to show that G has a generic extension over k it sufficies to show the lifting property for the case when $T = R$ is a Noetherian regular local k-algebra and L/K is a G-Galois extension of *fields*.

We return now to our case of dihedral groups. Let q be a power of 2. We have an exact sequence of groups:

$$1 \to C_2 \to D_{2q} \to D_q \to 1.$$

Given any D_q-Galois extension of k-algebras L/K we have a central and Frattini embedding problem. The obstruction to solving this problem is resolved by determining an element of $Br_2(K)$. By computing obstructions, Kiming [Ki] gives an explicit classification of all Galois extensions of fields with Galois groups D_4 and D_8 of any field K with characteristic different from 2. Here we use his results.

As discussed earlier we only need to show that given a D_8-Galois extension of fields L/K and Noetherian regular local k-algebra R with the residue field K, we can lift L/K to a D_8-Galois extension of local rings T/R. Let F/K be a D_4-Galois subextension of L/K. In order to construct a lifting of D_8-Galois extension L/K we first construct the lifting of D_4-Galois subextension F/K. We use Kiming's work and Lemma 4.2 to produce a D_4-Galois extension of k-algebras S/R with the following properties:

($B1$) $S/M = F$, *i.e.,* S/R specializes to F/K,

($B2$) S/R has a solvable embedding problem for D_8.

By Lemma 4.1 it follows that if D_4-Galois extension S/R satisfies $(B1)$ and $(B2)$, then there exists a D_8-Galois extension T/R such that $T/M = L$. Thus in order to show that there exists a lifting of D_8-Galois extension L/K, we only need to construct a lifting for D_4-Galois extension F/K with a solvable embedding problem for D_8.

Any D_2-Galois extension of K is of the form $K(\sqrt{a}, \sqrt{b})$ for some $a, b \in K^\times$, and such an extension embeds into a D_4-Galois extension of K if and only if $(a, -b) = 1 \in Br_2(K)$, *i.e.,* there exist $x, y \in K$ such that $b = ay^2 - x^2$. In general a D_4-Galois extension of a field K has the form

$$K(\sqrt{b}, \sqrt{a}, \sqrt{2q\theta}), \tag{1}$$

where $a, q \in K^\times$, $0 \neq b = ay^2 - x^2$ for some $x, y \in K$, and $\theta = ay + x\sqrt{a}$ ([Ki], Thm. 5). If $y \neq 0$ this D_4-Galois extension embeds in a D_8-Galois extension if and only if

$$(a, 2)(\frac{q}{y}, -b) = 1 \in Br_2(K) \tag{2}$$

([Ki], Thm. 6). If $y = 0$, the embedding problem is solvable if and only if $(a, 2) = 1$. In this case, $q \in K^\times$ is an arbitrary element.

Lemma 4.3. *Let $a \in K^\times$, $0 \neq b = ay^2 - x^2$ for some $x, y \in K$. Assume that $y \neq 0$. Then $K(\sqrt{a}, \sqrt{b})/K$ embeds into a D_8-Galois extension (with $K(\sqrt{b})/K$ as a unique quadratic subextension) if and only if for some $u, v, w \in K$*

$$x^2 - 2v^2 = a(u^2 + y^2 - 2w^2). \tag{3}$$

Moreover, the elements u, v, w can be chosen such that $x^2 - 2v^2 \neq 0$.

Proof. By Theorem 5 of [Ki] D_2-Galois extension $K(\sqrt{a}, \sqrt{b})/K$ embeds in a D_4-Galois extension of the form (1) for some q. It embeds into a D_8-Galois extension if and only if for some q, equation (2) holds. This equation holds for some q if and only if $K(\sqrt{-b})$ splits $(a, 2)$ if and only if there is $\nu \in (a, 2)$ noncentral such that $\nu^2 = -b$ ([Ja], p. 596). Now, suppose $(a, 2)$ is generated by α, β such that $\alpha^2 = a$, $\beta^2 = 2$ and $\alpha\beta = -\beta\alpha$. Any element z of quaternion algebra satisfies $z^2 - T(z)z + N(z) = 0$, where $T(z), N(z)$ are trace and norm of z. Any noncentral element whose square is central must have trace zero and thus live in the span of $\alpha, \beta, \alpha\beta$. So $\nu = u\alpha + v\beta + w\alpha\beta$, for some $u, v, w \in K$. Since $-b = \nu^2 = -N(\nu)$, we obtain $-b = au^2 + 2v^2 - 2aw^2$. On the other hand, we have $x, y \in K$ such that $-b = x^2 - ay^2$. Equating right-hand sides of these equalities gives us equation (3).

We now show that u, v, w can be chosen so that $x^2 - 2v^2 \neq 0$. Recall that $-b = \nu^2$, for $\nu = u\alpha + v\beta + w\alpha\beta$. The choices for such ν are precisely elements of the form $\gamma\nu\gamma^{-1}$ for $\gamma \in (a, b)$ a nonsingular element. So if $v^2 = (1/2)x^2$, we need to show that it is possible to find a nonsigular element γ of (a, b) such that $\gamma\nu\gamma^{-1} = u'\alpha + v'\beta + w'\alpha\beta$, and $v'^2 \neq (1/2)x^2$. Note that $\text{trace}((u\alpha + v\beta + w\alpha\beta)\beta^{-1}) = 2v$. We define a polynomial map $\phi : (a, 2)^\times \to K$ by setting $\phi(\gamma) = \text{trace}(\gamma\nu\gamma^{-1}\beta^{-1})$. It is enough to show

Proposition 4.4. *The image $\phi((a, 2)^\times)$ is dense in K in the Zariski topology.*

Let $\bar{K}$ be the algebraic closure of K. Let $\bar{\phi} : GL_2(\bar{K}) \to \bar{K}$ be the map induced from ϕ by extension of scalars. Since $(a, 2)^\times \subset ((a, 2) \otimes_K \bar{K})^\times = GL_2(\bar{K})$ is dense, it suffices to show that $\bar{\phi}(GL_2(\bar{K}))$ is dense in $\bar{K}$. Since $GL_2(\bar{K})$ is connected, it suffices to show that $\bar{\phi}(GL_2(\bar{K}))$ has at least two elements. Choose $c \in \bar{K}^\times$ such

that $\nu^2 = (c\beta)^2$. By Skolem-Noether ([Ja], p. 222) there is $\gamma_1 \in GL_2(\bar{K})$ such that $\gamma_1\nu\gamma_1^{-1} = c\beta$ and $\bar{\phi}(\gamma_1) = 2c \neq 0$. If $d \in \bar{K}$ is such that $\nu^2 = (d\alpha)^2$, then there is a γ_2 such that $\gamma_2\nu\gamma_2^{-1} = d\alpha$ and thus $\bar{\phi}(\gamma_2) = 0$.

This concludes the proof of Lemma 4.3. □

Lemma 4.5. *Suppose $K(\sqrt{-b})$ splits $(a, 2)$ and $-b = u^2+2v^2-2aw^2$ as in Lemma 4.3. Assume $y \neq 0$. Let $q \in K^\times$ and let $q_1 = \frac{q}{y}$. Then $(a, 2) = (-b, q_1)$ if and only if q is of the form $q = y(ac^2 + 2d^2 - 2ae^2) \neq 0$ for some $c, d, e \in K$, such that $cua + vd2 - ew2a = 0$.*

Proof. As in Lemma 4.3, let $-b = \nu^2$ and $\nu = u\alpha+v\beta+w\alpha\beta$. We need all elements δ of trace zero and such that $\nu\delta = -\delta\nu$. Our quaternion algebra has a unique simplectic involution $\gamma \to \bar{\gamma}$ such that $\bar{\alpha} = -\alpha$, $\bar{\beta} = -\beta$ and $\text{trace}(\gamma) = \gamma + \bar{\gamma}$, for any $\gamma \in (a, 2)$. Thus we have that $\text{trace}(\delta) = 0$ and $\text{trace}(\nu\delta) = 0$. Write $\delta = c\alpha + d\beta + e\alpha\beta$ for some $c, d, e \in K$, and the second condition implies that $cua + vd2 - ew2a = 0$. Since $q_1 = \delta^2$, we have that $q = y(c^2a + d^2 2 - e^2 2a)$. □

Theorem 4.6. *Let k be a field of characteristic different from 2. Then there exists a generic extension for the dihedral group of order 16 over k.*

Proof. Let L/K be a D_8-Galois extension of k-algebras which are overfields of k. Let R be a Noetherian regular local k-algebra with the maximal ideal M and the residue field K. We need to show that there exists a D_8-Galois extension of local k-algebras T/R such that $T/M = L$. By Theorem 5.3 of [Sa] this implies that D_8 has a generic extension over k.

Let F/K be a D_4-Galois subextension of L/K. Then necessarily F is of the form (1). There exist $x, y \in K$ such that $b = ay^2 - x^2$.

Case 1. First we assume that $y \neq 0$. There exist $u, v, w \in K$ such that (3) holds for a (Lemma 4.3). We may assume that $x^2 - 2v^2 \neq 0$ (Lemma 4.3). Also by Lemma 4.5, $-b = u^2a + v^2 2 - w^2 2a$ and $q = y(c^2a + d^2 2 - e^2 2a) \neq 0$ for some $c, d, e \in K$ such that $cua + vda - we2a = 0$.

Since $x^2 - 2v^2 \neq 0$, we have that $(u^2 + y^2 - 2w^2) \neq 0$. Let $x', y', u', v', w' \in R$ be preimages of $x, y, u, v, w \in K$. Then both $(x'^2 - 2v'^2)$ and $(u'^2 + y'^2 - 2w'^2)$ lie outside the maximal ideal M and are therefore units of R. Also $y' \in R^\times$. Set

$$a' = (x'^2 - 2v'^2)(u'^2 + y'^2 - 2w'^2)^{-1}$$

and $b' = y'^2a' - x'^2$, both of which are units in R. Since $b \neq 0$, one of $ua, 2v$ or $2aw$ is not zero and therefore we can lift c, d, e to $c', d', e' \in R$ such that $c'u'a' + d'v'2 - e'w'2a = 0$. Let $q' = y'(c'^2a' + d'^2 2 - e'^2 2a')$. Finally, let $\theta' = a'y' + x'\sqrt{a'}$. We claim that

$$S = R(\sqrt{a'}, \sqrt{b'}, \sqrt{2q'\theta'})$$

satisfies properties $(B1)$ and $(B2)$. Let $\mathcal{K}$ be a fraction field of R and let

$$\mathcal{L} = \mathcal{K}(\sqrt{a'}, \sqrt{b'}, \sqrt{2q'\theta'}).$$

Then $\mathcal{L}/\mathcal{K}$ is a D_4-Galois field extension with solvable D_8 embedding problem. The extension S/R is unramified at M since a', b', q', y' are units in R. The ring S is normal since R is normal and S is étale over R. Thus the integral closure of R in $\mathcal{L}$ is precisely S. Thus S/R is a D_4-Galois extension. It has a solvable embedding

problem for D_8 by Lemma 4.2. Finally the specialization to F/K is clear from our choice of a', b' and q'.

Case 2. We now assume that $y = 0$. Then by [Ki, Thm. 6] we have

$$F = K(\sqrt{-1}, \sqrt{a}, \sqrt{2q\sqrt{a}})$$

for $a, -a$ not squares in K. The obstruction in $Br_2(K)$ for such an extension to be embedded in a D_8-Galois extension of K is precisely $(a, 2)$. Therefore, $(a, 2) = 1 \in Br_2(K)$. Therefore, there exist elements $u, v \in K$ such that $a = u^2 - 2v^2$. Since a is not a square we know that $v \neq 0$. Let u', v' be preimages in R of u, v. Let q' be a preimage in $R^\times$ of $0 \neq q \in K$ and let m be a nonzero element of M. We now let $a' = q'^2(u'^2 - 2v'^2) \in R^\times$, $b' = m^4a' - 1 \in R^\times$ and $\tilde{q} = 1$. Let

$$S = R(\sqrt{a'}, \sqrt{b'}, \sqrt{2\tilde{q}(m^2a' + \sqrt{a'})}).$$

It is clear that D_4-Galois extension S/R specializes to F/K. To see that it also has a solvable embedding problem for D_8 note that

$$(a', 2)(-b', \frac{\tilde{q}}{m^2}) = 1 \in Br_2(\mathcal{K}).$$

Now apply Lemma 4.2. This concludes the proof of Theorem 4.6. □

References

[AlKl] A. Altman, S. Kleiman, *Introduction to Grothendieck duality theory*, Springer-Verlag, Heidelberg, 1970. MR **43:**224

[Be] S. Beckmann, *Is every extension of $\mathbb{Q}$ the specialization of a branched covering?*, J. of Algebra **164** (1994), 430–451. MR **95d:**12007

[Bl] E. Black, *Arithmetic lifting of dihedral extensions*, J. of Algebra **203** (1998), 12–29. CMP 98:12

[SGA1] A. Grothendieck, *Séminaire de la Géométrie Algébrique: Revêtements Etales et Groupe Fondamental*, Springer-Verlag, Heidelberg, 1971.

[Ja] N. Jacobson, *Basic Algebra II*, W. H. Freeman and Company, 1980. MR **81g:**00001

[Ke] G. Kemper, *Generic Polynomials and Noether's Problem for Linear Groups*, IWR preprint 95-19, Heidelberg (1995).

[Ki] I. Kiming, *Explict classification of some 2-extensions of a field of characteristic different from 2*, Can. J. Math **42** (1990), 825–855. MR **92c:**11115

[Sa] D. Saltman, *Generic Galois extensions and problems in field theory*, Advances in Math **43** (1982), 250–283. MR **84a:**13007

[Sa2] D. Saltman, *Groups acting on fields: Noether's Problem*, (AMS) Cont. Math **43** (1985), 267–277. MR **87a:**12008

[Sw] R. Swan, *Invariant rational functions and a problem of Steenrod*, Invent. Math. **7** (1969), 148–158. MR **39:**5532

Department of Mathematics, University of Pennsylvania, 209 South 33rd Street, Philadelphia, Pennsylvania 19104-6395

Current address: Department of Mathematics, University of Oklahoma, 601 Elm Avenue, Room 423, Norman, Oklahoma 73019

E-mail address: eblack@math.ou.edu