ACTA ARITHMETICA
143.3 (2010)

Noether's problem for some groups of order $16n$

by

Ivo Michailov (Shoumen)

1. Introduction. Let K be a field and G be a finite group. Let G act on the rational function field $K(x_g : g \in G)$ by K-automorphisms defined by $g \cdot x_h = x_{gh}$ for any $g, h \in G$. Denote by $K(G)$ the fixed field

$$K(x_g : g \in G)^G = \{f \in K(x_g : g \in G) \mid \sigma \cdot f = f, \forall \sigma \in G\}.$$

Noether's problem then asks whether $K(G)$ is rational (= purely transcendental) over K. Noether's problem is closely related to the inverse Galois problem.

The main results about Noether's problem for abelian groups can be found in the survey article [Sw]. More recently, Noether's problem for non-abelian p-groups was investigated in [CHK, CHPK, HK2, Ka1, Ka2].

Let $n \geq 2$ be an arbitrary natural number. In this paper we will concentrate on certain meta-abelian groups of orders $8n$ and $16n$ with two or three generators over a field K which contains a primitive $4n$th or $2n$th root of unity.

Let G be a non-abelian group of order $8n$, having a cyclic subgroup of order $4n$. Then G is generated by two elements σ and τ such that $\sigma^{4n} = 1$, $\tau^2 = \sigma^a$ and $\tau\sigma = \sigma^r\tau$, where $a, r \in \mathbb{Z}$ are subject to some restrictions. For example, r must be a solution to the congruence

$$x^2 \equiv 1 \pmod{4n}. \tag{1.1}$$

Therefore, $r = -1, \pm 1 + 2s$, where

$$s(s \pm 1) \equiv 0 \pmod{n}. \tag{1.2}$$

One solution to (1.2) is clearly $s = n$. The solutions -1 and $\pm 1 + 2n$ of (1.1) give only four non-isomorphic groups, by imitating the argument of

2010 *Mathematics Subject Classification*: Primary 12F12; Secondary 13A50, 11R32, 14E08.
Key words and phrases: Noether's problem, rationality problem, inverse Galois problem, dihedral group, modular group.

DOI: 10.4064/aa143-3-7

Hall [Ha, Th. 12.5.1, p. 187] for 2-groups. Their representations are:

$$D_{8n} \cong \langle \sigma, \tau \mid \sigma^{4n} = \tau^2 = 1,\ \tau\sigma = \sigma^{-1}\tau \rangle, \text{ the dihedral group,}$$
$$SD_{8n} \cong \langle \sigma, \tau \mid \sigma^{4n} = \tau^2 = 1,\ \tau\sigma = \sigma^{2n-1}\tau \rangle, \text{ the semidihedral group,}$$
$$Q_{8n} \cong \langle \sigma, \tau \mid \sigma^{4n} = 1, \tau^2 = \sigma^{2n},\ \tau\sigma = \sigma^{-1}\tau \rangle, \text{ the quaternion group,}$$
$$M_{8n} \cong \langle \sigma, \tau \mid \sigma^{4n} = \tau^2 = 1,\ \tau\sigma = \sigma^{2n+1}\tau \rangle, \text{ the modular group.}$$

If n is a power of 2, the congruence (1.2) has no other solutions. If n is not a power of 2, however, (1.2) may have other solutions (e.g., $s = 2$ for $n = 6$).

Our first result is

Proposition 1.1. *Let G be a non-abelian group of order $8n$, having a cyclic subgroup of order $4n$ for any $n \geq 2$. Assume that K is a field which contains a primitive $4n$th root of unity. Then $K(G)$ is rational over K.*

The next result is the following

Theorem 1.2. *Let $1 \to \mu_2 \cong \{\pm 1\} \to G \to H \to 1$ be a group extension, where H is isomorphic to any of the groups D_{8n}, SD_{8n}, Q_{8n} and M_{8n}. Assume that K is a field which contains a primitive $4n$th root of unity. Then $K(G)$ is rational over K.*

In Section 5 we show that for some of the groups considered in Theorem 1.2 we need only a primitive $2n$th root of unity in K. To this end we apply a somewhat different approach described in Theorem 2.7. It involves calculations of the obstructions to some embedding problems, discussed recently in [Mi1, Mi2, Zi1, Zi2].

2. Generalities. We list several results which will be used in what follows.

Theorem 2.1 ([HK1, Theorem 1]). *Let G be a finite group acting on $L(x_1, \ldots, x_m)$, the rational function field of m variables over a field L such that*

(i) *$\sigma(L) \subset L$ for any $\sigma \in G$;*
(ii) *the restriction of the action of G to L is faithful;*
(iii) *for any $\sigma \in G$,*

$$\begin{pmatrix} \sigma(x_1) \\ \vdots \\ \sigma(x_m) \end{pmatrix} = A(\sigma) \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} + B(\sigma)$$

where $A(\sigma) \in \mathrm{GL}_m(L)$ and $B(\sigma)$ is an $m \times 1$ matrix over L.

Then there exist $z_1, \ldots, z_m \in L(x_1, \ldots, x_m)$ such that $L(x_1, \ldots, x_m)^G = L^G(z_1, \ldots, z_m)$ and $\sigma(z_i) = z_i$ for any $\sigma \in G$ and $1 \leq i \leq m$.

THEOREM 2.2 ([AHK, Theorem 3.1]). *Let G be a finite group acting on $L(x)$, the rational function field of one variable over a field L. Assume that, for any $\sigma \in G$, $\sigma(L) \subset L$ and $\sigma(x) = a_\sigma x + b_\sigma$ for some $a_\sigma, b_\sigma \in L$ with $a_\sigma \neq 0$. Then $L(x)^G = L^G(z)$ for some $z \in L[x]$.*

THEOREM 2.3 ([CHK, Theorem 2.3]). *Let K be any field, $K(x,y)$ the rational function field of two variables over K, and $a, b \in K \setminus \{0\}$. If σ is a K-automorphism on $K(x,y)$ defined by $\sigma(x) = a/x$, $\sigma(y) = b/y$, then $K(x,y)^{\langle\sigma\rangle} = K(u,v)$, where*

$$u = \frac{x - \frac{a}{x}}{xy - \frac{ab}{xy}}, \qquad v = \frac{y - \frac{b}{y}}{xy - \frac{ab}{xy}}.$$

Moreover, $x + a/x = (-bu^2 + av^2 + 1)/v$, $y + b/y = (bu^2 - av^2 + 1)/u$, $xy + ab/(xy) = (-bu^2 - av^2 + 1)/(uv)$.

In the theorem below, ζ_e denotes a primitive eth root of unity.

THEOREM 2.4 ([Ka3, Cor. 3.2]). *Let K be a field and G be a finite group. Assume that* (i) *G contains an abelian normal subgroup H such that G/H is cyclic of order n,* (ii) *$\mathbb{Z}[\zeta_n]$ is a unique factorization domain, and* (iii) *$\zeta_{e'} \in K$ where $e' = \operatorname{lcm}\{\operatorname{ord}(\tau), \exp(H)\}$ and τ is some element of G whose image generates G/H. If $G \to \mathrm{GL}(V)$ is any finite-dimensional linear representation of G over K, then $K(V)^G$ is rational over K.*

Let $\mathrm{Br}(K)$ denote the Brauer group of a field K, and $\mathrm{Br}_N(K)$ its N-torsion subgroup for any $N > 1$. Following Roquette [Ro], if $\gamma = [B] \in \mathrm{Br}(K)$ is the class of a K-central simple algebra B and $m \geq 1$ is a multiple of the index of B, then $F_m(\gamma)$ denotes the mth Brauer field of γ. Moreover, $F_m(\gamma)/K$ is a regular extension of transcendence degree $m-1$, which is rational if and only if γ is trivial. The following result was essentially obtained by Saltman [Sa, p. 541] and proved in detail by Plans [Pl, Prop. 7].

THEOREM 2.5. *Let $1 \to C \to H \to G \to 1$ be a central extension of finite groups, representing an element $\varepsilon \in H^2(G,C)$. Let K be an infinite field and let N denote the exponent of C. Assume that N is prime to the characteristic of K and that K contains μ_N, the group of Nth roots of unity. Let there be given a decomposition $C \cong \mu_{N_1} \times \cdots \times \mu_{N_r}$, and let the corresponding isomorphism $H^2(G,C) \cong \bigoplus_i H^2(G, \mu_{N_i})$ map ε to (ε_i). Let there also be given a faithful subrepresentation V of the regular representation of G over K, and let $\gamma_i \in \mathrm{Br}_N(K(V)^G) \subset \mathrm{Br}(K(V)^G)$ be the inflation of ε_i with respect to the isomorphism $G \cong \mathrm{Gal}(K(V)/K(V)^G)$. Then*

$K(H)$ is rational over the $K(V)^G$-free compositum $F_m(\gamma_1) \cdots F_m(\gamma_r)$,

where m denotes the order of G.

We are going to formulate an important corollary of the latter theorem, which involves some generalities for the embedding problem of fields. Let E/F be a Galois extension with Galois group Z and let

$$1 \to X \to Y \underset{\pi}{\to} Z \to 1 \tag{2.1}$$

be a group extension, i.e., a short exact sequence. The *embedding problem* related to E/F and (2.1) then consists in determining whether there exists a Galois algebra (also called a *weak* solution) or a Galois extension (called a *proper* solution) L such that E is contained in L, Y is isomorphic to $\mathrm{Gal}(L/F)$, and the homomorphism of restriction of automorphisms of L to E coincides with π. This embedding problem will be denoted by $(E/F, Y, X)$.

Let p be a prime, let F be a field with characteristic not p, and let F contain all pth roots of unity. Denote by μ_p the cyclic group of all pth roots of unity which is contained in $F^\times = F \setminus \{0\}$. We have the following well known

Theorem 2.6 ([Ki]). *Let L/F be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/F)$ and let $1 \to \mu_p \to Y \to G \to 1$ be a non-split central group extension with characteristic class $\gamma \in H^2(G, \mu_p)$. Also, let $i : H^2(G, \mu_p) \to H^2(G, L^\times)$ be a homomorphism induced by the inclusion $\mu_p \subset L^\times$. Then the embedding problem $(L/F, Y, \mu_p)$ is properly solvable iff $i(\gamma) = 1 \in H^2(G, L^\times)$.*

Let $\varepsilon \in Z^2(G, \mu_p)$ represent γ given in the statement of the latter theorem. Then from [Ja, Th. 8.11] it follows that $H^2(G, L^\times)$ is isomorphic to the relative Brauer group $\mathrm{Br}(L/F)$ by $i(\gamma) \mapsto [L, G, \varepsilon]$, where $[L, G, \varepsilon] \in \mathrm{Br}(L/F)$ is the equivalence class of the crossed product algebra (L, G, ε). We know that (L, G, ε) is an F-algebra generated by L and elements u_σ, $\sigma \in G$, with relations $u_1 = \varepsilon(1, 1) = 1$, $u_\sigma u_\tau = \varepsilon(\sigma, \tau) u_{\sigma\tau}$ and $u_\sigma x = \sigma x u_\sigma$ for all $\sigma, \tau \in G$ and $x \in L$. Notice also that $i(\gamma) \in \mathrm{Br}(L/F) \subset \mathrm{Br}_p(F)$ is in fact the inflation of ε with respect to the isomorphism $G \cong \mathrm{Gal}(L/F)$. The element $i(\gamma) \in \mathrm{Br}_p(F)$ is called the *obstruction* to the embedding problem.

Theorem 2.7. *Let p be a prime, let F be an infinite field with characteristic not p, and let F contain all pth roots of unity. Let $1 \to \mu_p \to H \to G \to 1$ be a non-split central extension of finite groups, representing an element $\varepsilon \in H^2(G, \mu_p)$. Let $L = K(x_g : g \in G)$ be the rational function field with a G-action given by the regular representation of G over K. Assume that the embedding problem given by $L/K(G)$ and the group extension $1 \to \mu_p \to H \to G \to 1$ is solvable. Then $K(H)$ is rational over $K(G)$.*

Proof. Note that the obstruction $i(\gamma) = \inf(\varepsilon) \in \mathrm{Br}_p(K(G))$ is isomorphic to the crossed product algebra $[L, G, \varepsilon]$, which is split in $\mathrm{Br}_p(K(V)^G)$, since the embedding problem is solvable. Hence $F_m(\gamma)$ is rational over $K(G)$, so Theorem 2.5 implies our result. ∎

3. Proof of Proposition 1.1. If $\mathrm{char}(K) = p > 2$ and p divides n we can apply [KP, Th. 1.6] to reduce the rationality problem to a similar one, where p is relatively prime to the order of the given groups. Now, let $\mathrm{char}(K) \neq 2$. We can then assume that $\mathrm{char}(K) = 0$ or $\mathrm{char}(K)$ is relatively prime to $2n$.

Let $\bigoplus_{g\in G} K \cdot x(g)$ be the representation space of the regular representation of G and let ζ be a primitive $4n$th root of unity in K. Define

$$v = \sum_{i=0}^{4n-1} \zeta^{-i} x(\sigma^i).$$

Then $\sigma(v) = \zeta v$.

Define $x_1 = v$, $x_2 = \tau v$. We find that

$$\sigma : x_1 \mapsto \zeta x_1,\ x_2 \mapsto \zeta^r x_2, \qquad \tau : x_1 \mapsto x_2 \mapsto \zeta^a x_1.$$

Applying Theorem 2.1 we find that if $K(x_1, x_2)^G$ is rational over K, then so is $K(G) = K(x(g) : g \in G)^G$.

Define $y_1 = x_1$, $y_2 = x_1 x_2^{-1}$. Then $K(x_1, x_2) = K(y_1, y_2)$ and

$$\sigma : y_1 \mapsto \zeta y_1,\ y_2 \mapsto \zeta^{1-r} y_2, \qquad \tau : y_1 \mapsto y_2^{-1} y_1,\ y_2 \mapsto \zeta^{-a} y_2^{-1}.$$

By Theorem 2.2, if $K(y_2)^G$ is rational over K, so is $K(y_1, y_2)^G$. Finally, $K(y_2)^G$ is rational over K by Luroth's Theorem.

If $\mathrm{char}(K) = 2$, we can apply [KP, Th. 1.3] to reduce the problem to the rationality problem for a group isomorphic to a semi-direct product of a cyclic group of odd order with the cyclic group of order 2. Let G be such a group. Then $G = \langle \sigma, \tau \mid \sigma^m = \tau^2 = 1,\ \tau\sigma = \sigma^b \tau \rangle$, where m is odd and $b^2 \equiv 1 \pmod{m}$. If $b = 1$, by [KP, Th. 1.3] and Fischer's Theorem [Sw, Theorem 6.1] it follows that $K(G)$ is rational over K. Otherwise, we can apply the same approach as in the case $\mathrm{char}(K) \neq 2$, since both Luroth's Theorem and Theorem 2.2 hold for any field K.

4. Proof of Theorem 1.2. First, assume that $\mathrm{char}(K) = 2$. Then by [KP, Th. 1.3] we can reduce the problem to the one considered in Proposition 1.1. If $\mathrm{char}(K) = p$ and p divides n we can apply [KP, Th. 1.6] to reduce the problem to a similar one, where p is relatively prime to the order of the given groups. This can be achieved by taking consecutively group extensions of the kind $1 \to \mu_p = \langle \sigma^{4n/p} \rangle \to G \to G_1 \to 1$. Therefore, we can assume that $\mathrm{char}(K) = 0$ or $\mathrm{char}(K)$ is relatively prime to $2n$. If the group extension in the statement is split, [KP, Th. 1.9] yields the rationality of $K(G)$ over K. Therefore, we can also assume that the group extension is non-split.

We divide the proof into several steps.

Step I. Let us first describe the cohomology groups $H^2(H,\mu_2)$ for H being isomorphic to any of the groups D_{8n}, SD_{8n}, Q_{8n} and M_{8n}.

I.1) Let $H \cong D_{8n}$. We have the non-equivalent exact sequences

$$1 \to \mu_2 \to G \underset{\substack{\sigma\mapsto\sigma\\ \tau\mapsto\tau}}{\longrightarrow} D_{8n} \to 1,$$

where the generators σ and τ of G satisfy the relations $\sigma^{4n}=\varepsilon_1$, $\tau^2=\varepsilon_2$, $\tau\sigma=\varepsilon_3\sigma^{-1}\tau$ for $\varepsilon_i=\pm1$. The existence of the group G for any choice of ε_i is easily verified. Therefore, $H^2(D_{8n},\mu_2)\cong\mu_2^3$ and all non-split sequences give us six non-isomorphic groups:

$$\begin{aligned}
&G_1\cong D_{16n},\quad G_2\cong SD_{16n},\quad G_3\cong Q_{16n},\\
&G_4=\langle\sigma,\tau,\rho\mid\sigma^{4n}=1,\ \tau^2=\rho \text{ central},\ \rho^2=1,\ \tau\sigma=\sigma^{-1}\tau\rangle,\\
&G_5=\langle\sigma,\tau,\rho\mid\sigma^{4n}=1,\ \tau^2=\rho \text{ central},\ \rho^2=1,\ \tau\sigma=\sigma^{-1}\tau\rho\rangle,\\
&G_6=\langle\sigma,\tau,\rho\mid\sigma^{4n}=1,\ \tau^2=1,\ \rho^2=1,\ \rho \text{ central},\ \tau\sigma=\sigma^{-1}\tau\rho\rangle.
\end{aligned}$$

I.2) Let $H\cong SD_{8n}$. We have the non-equivalent exact sequences

$$1 \to \mu_2 \to G \underset{\substack{\sigma\mapsto\sigma\\ \tau\mapsto\tau}}{\longrightarrow} SD_{8n} \to 1,$$

where the generators σ and τ of G satisfy the relations $\sigma^{4n}=1$, $\tau^2=\varepsilon_2$, $\tau\sigma=\varepsilon_3\sigma^{2n-1}\tau$ for $\varepsilon_i=\pm1$ $(2\le i\le 3)$. There is no group extension for $\varepsilon_1=-1$. Therefore, $H^2(SD_{8n},\mu_2)\cong\mu_2^2$ and all non-split sequences give us three non-isomorphic groups:

$$\begin{aligned}
&G_7=\langle\sigma,\tau,\rho\mid\sigma^{4n}=1,\ \tau^2=\rho \text{ central},\ \rho^2=1,\ \tau\sigma=\sigma^{2n-1}\tau\rangle,\\
&G_8=\langle\sigma,\tau,\rho\mid\sigma^{4n}=1,\ \tau^2=\rho \text{ central},\ \rho^2=1,\ \tau\sigma=\sigma^{2n-1}\tau\rho\rangle,\\
&G_9=\langle\sigma,\tau,\rho\mid\sigma^{4n}=1,\ \tau^2=1,\ \rho^2=1,\ \rho \text{ central},\ \tau\sigma=\sigma^{2n-1}\tau\rho\rangle.
\end{aligned}$$

I.3) Let $H\cong Q_{8n}$. We have the non-equivalent exact sequences

$$1 \to \mu_2 \to G \underset{\substack{\sigma\mapsto\sigma\\ \tau\mapsto\tau}}{\longrightarrow} Q_{8n} \to 1,$$

where the generators σ and τ of G satisfy the relations $\sigma^{4n}=1,\tau^2=\varepsilon_2\sigma^{2n},\tau\sigma=\varepsilon_3\sigma^{-1}\tau$ for $\varepsilon_i=\pm1$ $(2\le i\le3)$. Therefore, $H^2(Q_{8n},\mu_2)\cong\mu_2^2$ and all non-split sequences give us three non-isomorphic groups:

$$\begin{aligned}
&G_{10}=\langle\sigma,\tau,\rho\mid\sigma^{4n}=1,\ \tau^2=\sigma^{2n}\rho,\ \rho \text{ central},\ \rho^2=1,\ \tau\sigma=\sigma^{-1}\tau\rangle,\\
&G_{11}=\langle\sigma,\tau,\rho\mid\sigma^{4n}=1,\ \tau^2=\sigma^{2n}\rho,\ \rho \text{ central},\ \rho^2=1,\ \tau\sigma=\sigma^{-1}\tau\rho\rangle,\\
&G_{12}=\langle\sigma,\tau,\rho\mid\sigma^{4n}=1,\ \tau^2=\sigma^{2n},\ \rho^2=1,\ \rho \text{ central},\ \tau\sigma=\sigma^{-1}\tau\rho\rangle.
\end{aligned}$$

I.4) Let $H\cong M_{8n}$. We have the non-equivalent exact sequences

$$1 \to \mu_2 \to G \underset{\substack{\sigma\mapsto\sigma\\ \tau\mapsto\tau}}{\longrightarrow} M_{8n} \to 1,$$

where the generators σ and τ of G satisfy the relations $\sigma^{4n}=1$, $\tau^2=\varepsilon_2$, $\tau\sigma=\varepsilon_3\sigma^{2n+1}\tau$ for $\varepsilon_i=\pm1$ $(2\le i\le 3)$. Therefore, $H^2(M_{8n},\mu_2)\cong\mu_2^2$ and all non-split sequences give us three non-isomorphic groups:

$$G_{13}=\langle\sigma,\tau,\rho\mid\sigma^{4n}=1,\ \tau^2=\rho\text{ central},\ \rho^2=1,\ \tau\sigma=\sigma^{2n+1}\tau\rangle,$$
$$G_{14}=\langle\sigma,\tau,\rho\mid\sigma^{4n}=1,\ \tau^2=\rho\text{ central},\ \rho^2=1,\ \tau\sigma=\sigma^{2n+1}\tau\rho\rangle,$$
$$G_{15}=\langle\sigma,\tau,\rho\mid\sigma^{4n}=1,\ \tau^2=1,\ \rho^2=1,\ \rho\text{ central},\ \tau\sigma=\sigma^{2n+1}\tau\rho\rangle.$$

Notice we have several isomorphic pairs of groups: $G_8\cong G_{11}, G_4\cong G_{10}$ and $G_6\cong G_9$. This becomes obvious if we replace ρ with $\sigma^{2n}\rho$.

Step II. The rationality of $K(D_{16n})$, $K(SD_{16n})$ and $K(Q_{16n})$ over K can be shown in the same way as in the proofs of [HK2, Theorems 3.2 and 3.3]. One only has to replace everywhere the numbers $2^{n-2},2^{n-3}$ and 2^{n-4} with $4n,2n$ and n, respectively.

So, it remains to consider the nine groups G_i for $i=4,5,6,7,8,12,13,14,15$.

Step III. Let $\bigoplus_{g\in G}K\cdot x(g)$ be the representation space of the regular representation of G and let ζ be a primitive $4n$th root of unity in K. Define

$$v=\sum_{i=0}^{4n-1}\zeta^{-i}x(\sigma^i).$$

Then $\sigma v=\zeta v$.

Define $x_1=v$, $x_2=\tau v$, $x_3=\rho v$, $x_4=\rho\tau v$. Applying Theorem 2.1 we find that if $K(x_1,x_2,x_3,x_4)^G$ is rational over K, then $K(G)=K(x(g):g\in G)^G$ is also rational over K.

Define $y_1=x_1-x_3$, $y_2=x_2-x_4$, $y_3=x_1+x_3$, $y_4=x_2+x_4$. Clearly, $K(x_1,x_2,x_3,x_4)=K(y_1,y_2,y_3,y_4)$. Then for any of the groups under consideration we have

$$\rho: y_1\mapsto -y_1,\ y_2\mapsto -y_2,\ y_3\mapsto y_3,\ y_4\mapsto y_4.$$

Define $z_1=y_1^2$, $z_2=y_1y_2$, $z_3=y_3$, $z_4=y_4$. Then $K(y_1,y_2,y_3,y_4)^{\langle\rho\rangle}=K(z_1,z_2,z_3,z_4)$.

III.1) *The group* G_4. We find that

$$\sigma: x_1\mapsto\zeta x_1,\ x_2\mapsto\zeta^{-1}x_2,\ x_3\mapsto\zeta x_3,\ x_4\mapsto\zeta^{-1}x_4,$$
$$\tau: x_1\mapsto x_2\mapsto x_3\mapsto x_4\mapsto x_1,$$

whence

$$\sigma: y_1\mapsto\zeta y_1,\ y_2\mapsto\zeta^{-1}y_2,\ y_3\mapsto\zeta y_3,\ y_4\mapsto\zeta^{-1}y_4,$$
$$\tau: y_1\mapsto y_2\mapsto -y_1,\ y_3\mapsto y_4\mapsto y_3.$$

Therefore,

$$\sigma: z_1 \mapsto \zeta^2 z_1,\ z_2 \mapsto z_2,\ z_3 \mapsto \zeta z_3,\ z_4 \mapsto \zeta^{-1} z_4,$$
$$\tau: z_1 \mapsto z_2^2 z_1^{-1},\ z_2 \mapsto -z_2,\ z_3 \mapsto z_4,\ z_4 \mapsto z_3.$$

Define $t_1 = z_1^{2n}$, $t_2 = z_2$, $t_3 = z_3^2 z_1^{-1}$, $t_4 = z_3 z_4$. Since $[K(z_i) : K(t_i)] = 4n$, we have $K(z_1, z_2, z_3, z_4)^{\langle\sigma\rangle} = K(t_1, t_2, t_3, t_4)$. The action of τ is now given by

$$\tau: t_1 \mapsto t_2^{4n} t_1^{-1},\ t_2 \mapsto -t_2,\ t_3 \mapsto t_4^2 t_2^{-2} t_3^{-1},\ t_4 \mapsto t_4.$$

Define $s_1 = t_1 t_2^{-2n}$, $s_2 = t_2$, $s_3 = t_3 t_2$, $s_4 = t_4$. Then

$$\tau: s_1 \mapsto s_1^{-1},\ s_2 \mapsto -s_2,\ s_3 \mapsto -s_4^2 s_3^{-1},\ s_4 \mapsto s_4.$$

By Theorem 2.2, if $K(s_1, s_3, s_4)^{\langle\tau\rangle}$ is rational over K, so is $K(s_1, s_2, s_3, s_4)^{\langle\tau\rangle}$. The rationality of $K(s_1, s_3, s_4)^{\langle\tau\rangle}$ over K now follows from Theorem 2.3 for $x = s_1$, $y = s_3$, $a = 1$, $b = -s_4^2$.

The remaining groups can be considered in a similar manner; we leave the details to the interested reader.

5. The rationality of $K(G_i)$ for $4 \le i \le 9$ and $i = 13$. It is not hard to see that, for the groups G_i for $4 \le i \le 15$, Theorem 1.2 has a short proof by applying Theorem 2.4. Moreover, we have

THEOREM 5.1. *Let H be a non-abelian group of order $8n$, having a cyclic subgroup of order $4n$ for any $n \ge 2$, and let $1 \to \mu_2 \to G \to H \to 1$ be a group extension such that G does not have a cyclic subgroup of index 2. Assume that K is a field which contains a primitive $4n$th root of unity. Then $K(G)$ is rational over K.*

Proof. Let H be generated by two elements σ and τ such that $\sigma^{4n} = 1$, $\tau^2 = \sigma^a$ and $\tau\sigma = \sigma^r\tau$ for some $a, r \in \mathbb{Z}$. Then the pre-images $\tilde{\sigma}$ and $\tilde{\tau}$ of σ and τ in G are subject to the relations $\tilde{\sigma}^{4n} = 1$, $\tilde{\tau}^2 = \varepsilon_1\tilde{\sigma}^a$ and $\tilde{\tau}\tilde{\sigma} = \varepsilon_2\tilde{\sigma}^r\tilde{\tau}$ for some $\varepsilon_1, \varepsilon_2 \in \mu_2$. It is easy to see now that G is metacyclic or meta-abelian and satisfies the conditions of Theorem 2.4. ∎

We do not know the answer to the rationality problem for non-abelian groups of order $8n$ having a cyclic subgroup of index 2, which are not isomorphic to any of the groups D_{8n}, SD_{8n}, Q_{8n} or M_{8n}. We are able, however, to improve Theorem 1.2 regarding the groups G_i for $4 \le i \le 9$ and $i = 13$. Since the case $\mathrm{char}(K) = p > 2$ and $(p, n) \ne 1$ can be dealt with in a similar manner to Sections 3 and 4, we will assume henceforth that if $\mathrm{char}(K) = p > 2$ then $(p, n) = 1$.

Now, let H be isomorphic to D_{8n} or SD_{8n} and let L/F be an H-extension. Then L/F contains a biquadratic extension $K/F = F(\sqrt{a}, \sqrt{b})/F$

such that the generators σ and τ of H act in the following way:

$$\sigma : \sqrt{a} \mapsto -\sqrt{a},\ \sqrt{b} \mapsto \sqrt{b}, \qquad \tau : \sqrt{a} \mapsto \sqrt{a},\ \sqrt{b} \mapsto -\sqrt{b}.$$

In [Mi1] and [Zi1] the reader can find two different approaches to calculating the obstructions, displayed in the following three propositions.

PROPOSITION 5.2 ([Zi1, Th. 2.1]). *Let F be a field with* $\mathrm{char}(F) \neq 2$, *let H be isomorphic to D_{8n} or SD_{8n}, and let L/F be an H-extension containing a biquadratic extension $K/F = F(\sqrt{a}, \sqrt{b})/F$. Then the obstruction to the embedding problem given by L/F and the group extension*

$$1 \to \mu_2 \to G_i \to H \to 1$$

for $i = 4$ and $i = 7$ is $(b, -1) \in \mathrm{Br}(F)$.

PROPOSITION 5.3 ([Zi1, Th. 2.2]). *Let F be a field with* $\mathrm{char}(F) \neq 2$, *let H be isomorphic to D_{8n} or SD_{8n}, and let L/F be an H-extension containing a biquadratic extension $K/F = F(\sqrt{a}, \sqrt{b})/F$. Then the obstruction to the embedding problem given by L/F and the group extension*

$$1 \to \mu_2 \to G_i \to H \to 1$$

for $i = 6$ and $i = 9$ is $(a, -1) \in \mathrm{Br}(F)$.

PROPOSITION 5.4 ([Zi1, Th. 2.3]). *Let F be a field with* $\mathrm{char}(F) \neq 2$, *let H be isomorphic to D_{8n} or SD_{8n}, and let L/F be an H-extension containing a biquadratic extension $K/F = F(\sqrt{a}, \sqrt{b})/F$. Then the obstruction to the embedding problem given by L/F and the group extension*

$$1 \to \mu_2 \to G_i \to H \to 1$$

for $i = 5$ and $i = 8$ is $(ab, -1) \in \mathrm{Br}(F)$.

Next, we are going to prove the following

THEOREM 5.5. *Assume that K is an infinite field with* $\mathrm{char}(K) \neq 2$ *which contains a primitive $2n$th root of unity for some n even. Then $K(G_i)$ is rational over K for any $i = 4, 5, 6, 7, 8, 9$.*

Proof. Let H be isomorphic to D_{8n} or SD_{8n} and let $L/F = K(x_h : h \in H)/K(H)$ be the H-extension obtained by the rational function field $K(x_h : h \in H)$. From Propositions 5.2–5.4 it then follows that the obstruction to the embedding problem given by L/F and $1 \to \mu_2 \to G_i \to H \to 1$ is $(*, -1) \in \mathrm{Br}(K(H))$. Note that K has a fourth root of unity (n is even), so the obstruction $(*, -1)$ is always split. Then Theorem 2.7 implies the rationality of $K(G_i)$, since $K(H)$ is rational, as we have noticed in Section 4. ∎

We now turn our attention to the modular group.

THEOREM 5.6. *Let the modular group M_{8n} for $n \geq 2$ be generated by σ and τ such that $\sigma^{4n} = \tau^2 = 1$ and $\tau\sigma = \sigma^{2n+1}\tau$. Assume that K contains a primitive $2n$th root of unity. Then $K(M_{8n})$ is rational over K.*

Proof. If $\mathrm{char}(K) = 2$, then by [KP, Th. 1.3] we can reduce the problem to the rationality problem for the group $\mathbb{Z}/2n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, which has an affirmative answer by Fischer's Theorem [Sw, Theorem 6.1]. Now, assume that $\mathrm{char}(K) \neq 2$.

Let $\bigoplus_{g\in M_{8n}} K \cdot x(g)$ be the representation space of the regular representation of M_{8n} and let ζ be a primitive $2n$th root of unity in K. Define

$$v = \sum_{0\le i\le 2n-1} \zeta^{-i}(x(\sigma^{2i}) + x(\sigma^{2i}\tau)).$$

Then $\sigma^2(v) = \zeta v$ and $\tau(v) = v$. Define $x_0 = v$, $x_1 = \sigma(v)$. Then we have

$$\sigma : x_0 \mapsto x_1 \mapsto \zeta x_0, \qquad \tau : x_0 \mapsto x_0,\ x_1 \mapsto -x_1.$$

Applying Theorem 2.1 we find that if $K(x_0, x_1)^{M_{8n}}$ is rational over K, then so is $K(M_{8n})$.

Define $y_0 = x_0$, $y_1 = x_1/x_0$. We find that

$$\sigma : y_0 \mapsto y_1 y_0,\ y_1 \mapsto \zeta y_1^{-1}, \qquad \tau : y_0 \mapsto y_0,\ y_1 \mapsto -y_1.$$

From Theorem 2.2 it follows that if $K(y_1)^{M_{8n}}$ is rational over K, then so is $K(y_0, y_1)^{M_{8n}}$. The rationality of $K(y_1)^{M_{8n}}$ follows from Luroth's Theorem. ■

We can as well improve [HK2, Theorem 3.1] concerning the rationality of the modular 2-group. Our proof generalizes the proof of [CHK, Theorem 3.3], where it is shown that $K(M_{16})$ is rational over K for any K.

Theorem 5.7. *Let the modular group M_{2^n} for $n \ge 4$ be generated by σ and τ such that $\sigma^{2^{n-1}} = \tau^2 = 1$ and $\tau\sigma = \sigma^{2^{n-2}+1}\tau$. Assume that K contains a primitive 2^{n-3}th root of unity. Then $K(M_{2^n})$ is rational over K.*

Proof. If $\mathrm{char}(K) = 2$, Kuniyoshi's Theorem [CK, Theorem 1.7] implies the rationality of $K(M_{2^n})$ over K. Now, assume that $\mathrm{char}(K) \neq 2$.

Let $\bigoplus_{g\in M_{2^n}} K \cdot x(g)$ be the representation space of the regular representation of M_{2^n}. We claim that we can reduce the problem to the rationality problem for the fixed field of a function field $K(z_0, z_1, z_2, z_3)$, where M_{2^n} acts faithfully by

$$\sigma : z_0 \mapsto z_1 \mapsto z_2 \mapsto z_3 \mapsto -\zeta z_0,$$
$$\tau : z_0 \mapsto z_0,\ z_1 \mapsto -z_1,\ z_2 \mapsto z_2,\ z_3 \mapsto -z_3,$$

ζ being a primitive 2^{n-3}th root of unity.

Define

$$x_i = x(\sigma^i) + x(\sigma^i\tau), \quad 0 \le i \le 2^{n-1} - 1.$$

Then $\sigma(x_i) = x_{i+1}$ and $\tau(x_i) = x_{(2^{n-2}+1)i}$, where the indices are taken mod 2^{n-1}. Applying Theorem 2.1 we find that if $K(x_0, \ldots, x_{2^{n-1}-1})^{M_{2^n}}$ is rational over K, then so is $K(M_{2^n})$.

Define $y_i = x_i - x_{i+2^{n-2}}$, $y_{i+2^{n-2}} = x_i + x_{i+2^{n-2}}$ for $0 \le i \le 2^{n-2} - 1$. We find that

$$\begin{aligned}
\sigma &: y_0 \mapsto y_1 \mapsto \cdots \mapsto y_{2^{n-2}-1} \mapsto -y_0, \\
&\quad y_{2^{n-2}} \mapsto y_{2^{n-2}+1} \mapsto \cdots \mapsto y_{2^{n-1}-1} \mapsto y_{2^{n-2}}, \\
\tau &: y_0 \mapsto y_0,\ y_1 \mapsto -y_1,\ y_2 \mapsto y_2, \ldots, y_{2^{n-2}-1} \mapsto -y_{2^{n-2}-1}, \\
&\quad y_{2^{n-2}} \mapsto y_{2^{n-2}},\ y_{2^{n-2}+1} \mapsto y_{2^{n-2}+1}, \ldots, y_{2^{n-1}-1} \mapsto y_{2^{n-1}-1}.
\end{aligned}$$

Since M_{2^n} acts faithfully on $K(y_0, \ldots, y_{2^{n-2}-1})$ we again apply Theorem 2.1 so that we only have to show the rationality of $K(y_0, \ldots, y_{2^{n-2}-1})^{M_{2^n}}$ over K.

If $n \ge 5$, let ζ_4 be a primitive 4th root of unity and define $u_i = \zeta_4 y_i - y_{i+2^{n-3}}$, $u_{i+2^{n-3}} = \zeta_4 y_i + y_{i+2^{n-3}}$ for $0 \le i \le 2^{n-3} - 1$. Now we have

$$\begin{aligned}
\sigma &: u_0 \mapsto u_1 \mapsto \cdots \mapsto u_{2^{n-3}-1} \mapsto -\zeta_4 u_0, \\
&\quad u_{2^{n-3}} \mapsto u_{2^{n-3}+1} \mapsto \cdots \mapsto u_{2^{n-2}-1} \mapsto \zeta_4 u_{2^{n-3}}, \\
\tau &: u_0 \mapsto u_0,\ u_1 \mapsto -u_1,\ u_2 \mapsto u_2, \ldots, u_{2^{n-2}-1} \mapsto -u_{2^{n-2}-1}.
\end{aligned}$$

We again apply Theorem 2.1 so that we only have to show the rationality of $K(u_0, \ldots, u_{2^{n-3}-1})^{M_{2^n}}$ over K. If $n \ge 6$, let ζ_8 be a 8th root of unity such that $\zeta_8^2 = -\zeta_4$. Define $v_i = \zeta_8 u_i - u_{i+2^{n-4}}$, $v_{i+2^{n-4}} = \zeta_8 u_i + u_{i+2^{n-4}}$ for $0 \le i \le 2^{n-4} - 1$. Now we have

$$\begin{aligned}
\sigma &: v_0 \mapsto v_1 \mapsto \cdots \mapsto v_{2^{n-4}-1} \mapsto -\zeta_8 v_0, \\
&\quad v_{2^{n-4}} \mapsto v_{2^{n-4}+1} \mapsto \cdots \mapsto v_{2^{n-3}-1} \mapsto \zeta_8 v_{2^{n-4}}, \\
\tau &: v_0 \mapsto v_0,\ v_1 \mapsto -v_1,\ v_2 \mapsto v_2, \ldots, v_{2^{n-3}-1} \mapsto -v_{2^{n-3}-1}.
\end{aligned}$$

Analogously, we reduce the rationality problem for M_{2^n} to the rationality problem for $K(v_0, \ldots, v_{2^{n-4}-1})^{M_{2^n}}$ over K. Thus we can prove our claim, proceeding by induction.

Now, let $K(z_0, z_1, z_2, z_3)$ be a function field, where M_{2^n} acts by

$$\begin{aligned}
\sigma &: z_0 \mapsto z_1 \mapsto z_2 \mapsto z_3 \mapsto -\zeta z_0, \\
\tau &: z_0 \mapsto z_0,\ z_1 \mapsto -z_1,\ z_2 \mapsto z_2,\ z_3 \mapsto -z_3,
\end{aligned}$$

ζ being a primitive 2^{n-3}th root of unity. We have $\sigma^{2^{n-2}}(z_i) = -z_i$. Define $w_0 = z_0^2, w_1 = z_1/z_0, w_2 = z_2/z_1, w_3 = z_3/z_2$. Then $K(z_0, z_1, z_2, z_3)^{\langle \sigma^{2^{n-2}} \rangle} = K(w_0, w_1, w_2, w_3)$. We find that

$$\begin{aligned}
\sigma &: w_0 \mapsto w_0 w_1^2,\ w_1 \mapsto w_2 \mapsto w_3 \mapsto -\zeta/(w_1 w_2 w_3), \\
\tau &: w_0 \mapsto w_0,\ w_1 \mapsto -w_1,\ w_2 \mapsto -w_2,\ w_3 \mapsto -w_3.
\end{aligned}$$

Theorem 2.2 implies that the rationality problem for $K(z_0, z_1, z_2, z_3)^{M_{2^n}}$ can be reduced to the rationality problem for $K(w_1, w_2, w_3)^{M_{2^n}}$.

Define $t = w_1 w_3$, $x = w_1$, $y = w_2$. Then we have

$$\sigma : t \mapsto -\zeta/t,\ x \mapsto y \mapsto t/x,$$
$$\sigma^2 : t \mapsto t,\ x \mapsto t/x,\ y \mapsto -\zeta/(ty),$$
$$\tau : t \mapsto t,\ x \mapsto -x,\ y \mapsto -y.$$

From Theorem 2.3 it follows that $K(t,x,y)^{\langle\sigma^2\rangle} = K(t,u,v)$, where

$$u = \frac{x - \frac{t}{x}}{xy + \frac{\zeta}{xy}}, \qquad v = \frac{y + \frac{\zeta}{ty}}{xy + \frac{\zeta}{xy}}.$$

We have

$$\sigma(u) = \frac{y + \frac{\zeta}{ty}}{\frac{ty}{x} + \frac{\zeta x}{ty}}, \qquad \sigma(v) = \frac{\frac{t}{x} - x}{\frac{ty}{x} + \frac{\zeta x}{ty}}.$$

Define $w = u/v$. Then $\sigma(w) = -1/w$, $\tau(w) = w$.

Calculations show that

$$\frac{\frac{ty}{x} + \frac{\zeta x}{ty}}{y + \frac{\zeta}{ty}} = \frac{\zeta u^2 + t^2 v^2}{tv},$$

whence we find that

$$\sigma(u) = \frac{t}{u\big(\zeta w + \frac{t^2}{w}\big)}.$$

Define $z = u^2(\zeta w + t^2/w)/t$. Then $K(t,u,v)^{\langle\tau\rangle} = K(t,u^2,w) = K(t,z,w)$. We find that

$$\sigma : t \mapsto -\zeta/t,\ w \mapsto -1/w,\ z \mapsto 1/z.$$

Define $p = (1-z)/(1+z)$. Hence $K(t,w,z)^{\langle\sigma\rangle} = K(t,w,p)^{\langle\sigma\rangle}$ is rational over K if and only if $K(t,w)^{\langle\sigma\rangle}$ is. Finally, Theorem 2.2 yields the rationality of $K(t,w)^{\langle\sigma\rangle}$. ■

Finally, we will prove the following

THEOREM 5.8. *If K is an infinite field with* $\mathrm{char}(K) \neq 2$, *which contains a primitive $2n$th root of unity for some n even, then $K(G_{13})$ is rational over K. Moreover, if $n = 2^k$ for $k \geq 1$ and K contains only a primitive 2^kth root of unity, then $K(G_{13})$ is rational over K.*

Proof. Let H be isomorphic to M_{8n} and let $L/F = K(x_h : h \in H)/K(H)$ be the H-extension obtained by the rational function field $K(x_h : h \in H)$. From [Mi2, Prop. 4.4] or [Zi2, Th. 2.2] it follows that the obstruction to the embedding problem given by L/F and $1 \to \mu_2 \to G_{13} \to H \to 1$ is $(*, -1) \in \mathrm{Br}(K(H))$. Note that K has a fourth root of unity (n is even), so the obstruction $(*, -1)$ is always split.

Theorem 5.6 implies that $K(H)$ is rational over K. Therefore, Theorem 2.7 implies the rationality of $K(G_{13})$ over K. If $n = 2^k$ and K contains only a primitive 2^kth root of unity, then Theorem 5.7 yields the rationality of $K(G_{13})$ over K. ∎

Acknowledgments. This work was partially supported by project No. RD-07-1035/30.03.2010 of Shumen University.

References

[AHK] H. Ahmad, S. Hajja and M. Kang, *Rationality of some projective linear actions*, J. Algebra 228 (2000), 643–658.

[CK] H. Chu and M. Kang, *Rationality of p-group actions*, ibid. 237 (2001), 673–690.

[CHK] H. Chu, J. Hu and M. Kang, *Noether's problem for dihedral 2-groups*, Comment. Math. Helv. 79 (2004), 147–159.

[CHPK] H. Chu, J. Hu, Y. Prokhorov and M. Kang, *Noether's problem for groups of order 32*, J. Algebra 320 (2008), 3022–3035.

[HK1] S. Hajja and M. Kang, *Some actions of symmetric groups*, J. Algebra 177 (1995), 511–535.

[Ha] M. Hall, *The Theory of Groups*, Chelsea Publ., New York, 1976.

[HK2] S. Hu and M. Kang, *Noether's problem for some p-groups*, in: Rationality Problem, F. Bogomolov and Y. Tschinkel (eds.), Progr. Math., Birkhäuser, Boston, 2008 (available at http://arxiv.org/abs/0704.1701).

[Ja] N. Jacobson, *Basic Algebra II*, W. H. Freeman, New York, 1989.

[Ka1] M. Kang, *Noether's problem for dihedral 2-groups II*, Pacific J. Math. 222 (2005), 301–316.

[Ka2] —, *Noether's problem for metacyclic p-groups*, Adv. Math. 203 (2005), 554–567.

[Ka3] —, *Rationality problem for some meta-abelian groups*, J. Algebra 322 (2009), 1214–1219.

[KP] M. Kang and B. Plans, *Reduction theorems for Noether's problem*, Proc. Amer. Math. Soc. 137 (2009), 1867–1874.

[Ki] I. Kiming, *Explicit classifications of some 2-extensions of a field of characteristic different from 2*, Canad. J. Math. 42 (1990), 825–855.

[Mi1] I. Michailov, *On Galois cohomology and realizability of 2-groups as Galois groups*, preprint.

[Mi2] —, *Induced orthogonal representations of Galois groups*, J. Algebra 322 (2009), 3713–3732.

[Pl] B. Plans, *On Noether's problem for central extensions of symmetric and alternating groups*, ibid. 321 (2009), 3704–3713.

[Ro] P. Roquette, *On the Galois cohomology of the projective linear group and its applications to the construction of generic splitting fields of algebras*, Math. Ann. 150 (1963), 411–439.

[Sa] D. J. Saltman, *Twisted multiplicative field invariants, Noether's problem, and Galois extensions*, J. Algebra 131 (1990), 535–558.

[Sw] R. Swan, *Noether's problem in Galois theory*, in: Emmy Noether in Bryn Mawr, B. Srinivasan and J. Sally (eds.), Springer, Berlin, 1983, 21–40.

[Zi1] N. Ziapkov, *Some relatives of the dihedral group as Galois groups*, C. R. Acad. Bulgare Sci. 62 (2009), 1063–1066.

[Zi2] N. Ziapkov, *Some relatives of the modular group as Galois groups*, ibid. 62 (2009), 1203–1206.

Ivo Michailov
Faculty of Mathematics and Informatics
Constantin Preslavski University
Universitetska St. 115
9700 Shoumen, Bulgaria
E-mail: ivo_michailov@yahoo.com

Received on 14.3.2009
and in revised form on 27.7.2009 (5972)