Comment. Math. Helv. 79 (2004) 147–159
0010-2571/04/010147-13
DOI 10.1007/s00014-003-0783-8

Commentarii Mathematici Helvetici

Noether's problem for dihedral 2-groups

Huah Chu, Shou-Jen Hu and Ming-chang Kang

Abstract. Let K be any 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 $K(x_g : g \in G)^G$. Noether's problem asks whether $K(G)$ is rational (= purely transcendental) over K. We shall prove that $K(G)$ is rational over K if G is the dihedral group (resp. quasi-dihedral group, modular group) of order 16. Our result will imply the existence of the generic Galois extension and the existence of the generic polynomial of the corresponding group.

Mathematics Subject Classification (2000). Primary 12F12, 13A50, 11R32, 14E08.

Keywords. Rationality, Noether's problem, generic Galois extension, generic polynomials, dihedral groups.

§1. Introduction

Let K be any field and G be a finite group. Let G act on the rational function field $K(x_g : g \in G)$ by K-automorphisms such that $g \cdot x_h = x_{gh}$ for any $g, h \in G$. Denote by $K(G)$ the fixed field $K(x_g : g \in G)^G = \{f \in K(x_g : g \in G) : \sigma \cdot f = f \text{ for any } \sigma \in G\}$. Noether's problem asks whether $K(G)$ is rational (=purely transcendental) over K.

Noether's problem is related to the inverse Galois problem, which asks whether there is a Galois extension L over K such that $\mathrm{Gal}(L/K) \simeq G$ if the field K and the finite group G are prescribed. In fact, if K is an infinite field and $K(G)$ is rational over K, then there exists a generic Galois G-extension over the field K [Sa1, Theorem 5.1]; see Proposition 2.2 for a generalization. A generic Galois G-extension is some universal object of G-extensions such that we can apply Hilbert irreducibility theorem; see [Sa1; Me] for more details. When K is a Hilbertian field, i.e. Hilbert irreducibility theorem is valid for irreducible polynomials $f \in K[x_1, \cdots, x_n]$, the existence of a generic Galois G-extension over K will guarantee the existence of

All the authors are partially supported by the National Science Council, Republic of China.

a Galois extension field L over K with $\mathrm{Gal}(L/K) \simeq G$. In particular, if K is an algebraic number field, then the validity of Noether's problem for the pair (K, G) will imply the validity of the inverse Galois problem for the pair (K, G). However, the converse is not true in general: there is a generic Galois G-extension over $\mathbb{Q}$ if G is a cyclic group of odd order [Sa1, Theorem 2.1], while $\mathbb{Q}(G)$ is not rational over $\mathbb{Q}$ when G is a cyclic group of order 47 or 113 [Sw]. On the other hand, Saltman shows that, if G is the cyclic group of order 8, then there cannot be a generic Galois G-extension over $\mathbb{Q}$ [Sa1, Theorem 5.11] while the answer of the inverse Galois problem for $(\mathbb{Q}, G)$ is affirmative, e.g. the subfield L in $\mathbb{Q}(e^{2\pi\sqrt{-1}/32})$ such that L is a cyclic extension of degree 8 over $\mathbb{Q}$.

Yet another notion due to DeMeyer, Smith, Ledet and Kemper: a generic polynomial for G-extensions over K. It is known that the existence of a generic Galois G-extension over K is equivalent to that of a generic polynomial for G-extensions over K [Me; Sm; Le2; Ke]. Thus Noether's problem plays the same role in this situation.

Now we consider the case $G = D_n$, the dihedral group of order $2n$. Saltman shows that if K is an infinite field, $\mathrm{char} K \nmid n$ and n is odd, then there exists a generic Galois D_n-extension over K [Sa1, Theorem 3.5]; unfortunately the answer to Noether's problem in this case is rather incomplete, see [Ka]. Not much is known about the existence of a generic Galois D_n-extension over K if $\mathrm{char}\, K \neq 2$ and n is a power of 2. Black obtained several results in this direction [Bl]. She showed that a generic Galois D_8-extension (resp. D_4-extension) over K did exist if K was an infinite field with $\mathrm{char}\, K \neq 2$. On the other hand, Ledet exhibited the generic polynomial for G-extensions over K if K is an infinite field with $\mathrm{char}\, K \neq 2$ and G is the dihedral group (resp. the quasi-dihedral group, the modular group) of order 16 [Le1]. (The definitions of all these groups will be explained at the beginning of Section 3.) What we will prove in this paper is that $K(G)$ is rational over K when K is any field and G is any one of the above groups. See Theorems 3.1, 3.2 and 3.3. In some sense our results help to show why the constructions of Black and Ledet have to exist. It is amusing to compare these results with [Sa1, Theorem 5.11] which shows that $\mathbb{Q}(G)$ is never rational if G is any abelian group whose exponent is divisible by 8, while our results show that this phenomenon is not true for non-abelian groups. A final remark: Gröbner proves that $K(G)$ is rational if G is the quaternion group [Gr]. We will present a proof of Gröbner's result, which may be easier than Gröbner's original proof and will prelude the idea of the proof of Theorem 3.1.

We shall organize this paper as follows. We will recall some preliminaries and discuss the general situation of the rationality problem of $K(D_n)$ in Section 2; the rationality problem of $K(D_4)$ together with Gröbner's Theorem will be proved also. Section 3 contains the main results of this paper; we shall solve the rationality problem of three certain groups of order 16. The rationality problem of other groups of order 16 will be discussed in a separate paper.

Notations and terminologies. A field extension L over K is rational if L is purely transcendental over K; L is called stably rational over K if there exist elements $y_1, \cdots, y_N$ which are algebraically independent over L such that $L(y_1, \cdots, y_N)$ is rational over K. The dihedral group of order $2n$ is defined as $\langle \sigma, \tau : \sigma^n = \tau^2 = 1, \tau\sigma\tau^{-1} = \sigma^{-1} \rangle$, which is denoted by D_n. The quaternion group of order 8 is defined as $\langle \sigma, \tau : \sigma^4 = \tau^4 = 1, \sigma^2 = \tau^2, \tau\sigma\tau^{-1} = \sigma^{-1} \rangle$. Recall the definition $K(G)$ at the beginning of this section: $K(G) = K(x_g : g \in G)^G$. The representation space of the regular representation of G over K is denoted by $W = \oplus_{g \in G} K \cdot x(g)$ where G acts on W by $g \cdot x(h) = x(gh)$ for any $g, h \in G$. Finally, if L_1 and L_2 are extension fields of a field K such that G acts on L_1 and L_2 by K-automorphisms, we will say that L_1 is G-isomorphic to L_2 over$K$ if there is an isomorphism $\varphi : L_1 \longrightarrow L_2$ from L_1 onto L_2 over K with $\varphi(\sigma \cdot u) = \sigma \cdot \varphi(u)$ for any $\sigma \in G$, any $u \in L_1$.

§2. Generalities

We recall a variant of Hilbertsatz 90 which has been used by many people under different disguises.

Theorem 2.1 ([HK2, Theorem 1]). *Let L be a field and G be a finite group acting on $L(x_1, \cdots, x_m)$, the rational function field of m variables over L. Suppose that*
(i) *for any $\sigma \in G$, $\sigma(L) \subset L$;*
(ii) *the restriction of the action of G to L is faithful;*
(iii) *for any $\sigma \in G$,*

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

where $A(\sigma) \in \mathrm{GL}_m(L)$ and $B(\sigma)$ is an $m \times 1$ matrix over L. Then $L(x_1, \cdots, x_m)$ is G-isomorphic to $L(z_1, \cdots, z_m)$ with $\sigma(z_i) = z_i$ for any $\sigma \in G$, any $1 \leq i \leq m$. In particular, $L(x_1, \cdots, x_m)^G \simeq L^G(z_1, \cdots, z_m)$, i.e. $L(x_1, \cdots, x_m)^G$ is rational over L^G.

Proposition 2.2. *Let K be any infinite field and G be a finite group. Let $\rho : G \longrightarrow GL(V)$ be a faithful representation of G where V is some finite-dimensional vector space over K. If the fixed field $K(V)^G$ is stably rational over K, then there exists a generic Galois G-extension over K.*

Remark. Proposition 2.2 is a "cheap" special case of Saltman's Theorem about retract rational extensions [Sa2; Sa3, Theorem 2; Bl, Remark of Theorem 1.1]; it is weaker than Saltman's Theorem, but its proof is easier.

Proof. Let W be the representation space of the regular representation of G. Thus $K(G) = K(W)^G$. Consider the action of G on $K(V \oplus W)$. By Theorem 2.1 $K(V \oplus W)^G$ is rational over $K(V)^G$ and $K(W)^G$. Since $K(V)^G$ is stably rational, it follows that $K(G) = K(W)^G$ is also stably rational. Hence there exists a positive integer m such that $K(W)^G(w_1, \cdots, w_N)$ is rational over K where $N = (m-1)n$. (Remember that $n = |G|$.)

Consider the diagonal action of G on $W^m = W \oplus W \oplus \cdots \oplus W$ (m copies of W). By Theorem 2.1 $K(W^m)^G = K(W)^G(y_1, \cdots, y_N)$ is rational over K.

Now we can identify $K(W^m) = K(x_g^{(i)} : 1 \le i \le m, g \in G)$ and remember that $K(W^m)^G$ is rational over K. Imitate Saltman's proof of [Sa1, Theorem 5.1]. All we need to do is to define a G-equivariant map $\varphi : K[x_\sigma^{(i)} : 1 \le i \le m, \sigma \in G] \longrightarrow L$ (in the notations of [Sa1, Theorem 5.1]), i.e. we should find elements $\alpha_1, \cdots, \alpha_m \in L$ and define $\varphi(x_\sigma^{(i)}) = \sigma \cdot \alpha_i$ under the condition that t evaluated at the $\varphi(x_\sigma^{(i)})$'s is a unit. Note that we should prove a "multi-variable" version of [Sa1, Lemma 5.2]. But this is not difficult and is omitted. □

Theorem 2.3 ([HK1, (2.7) Lemma])**.** *Let K be any field, $a, b \in K - \{0\}$ and $\sigma : K(x, y) \longrightarrow K(x, y)$ be a K-automorphism defined by $\sigma(x) = a/x$, $\sigma(y) = b/y$. Then $K(x, y)^{<\sigma>} = K(u, v)$ where*

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

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

Theorem 2.4 ([AHK, Theorem 3.1])**.** *Let G be any group whose order may be finite or infinite. Suppose that G acts 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 $\sigma(x) = a_\sigma \cdot x + b_\sigma$ for some a_σ, $b_\sigma \in L$ with $a_\sigma \neq 0$. Then $L(x)^G = L^G$ or $L^G(f(x))$ where $f(x) \in L[x]$ is of positive degree.*

Theorem 2.5 (Kuniyoshi [Ku;Mi])**.** *Let K be a field with char $K = p > 0$ and G be a p-group. Then $K(V)^G$ is rational over K for any representation $\rho : G \longrightarrow GL(V)$ where V is a finite-dimension vector space over K.*

Proof. Since char $K = p > 0$ and $|G| = p^m$, any representation of G can be triangulated. Apply [HK1, (2.2) Theorem]. □

Let $G = D_n = \langle \sigma, \tau : \sigma^n = \tau^2 = 1, \tau\sigma\tau^{-1} = \sigma^{-1} \rangle$.

Proposition 2.6. *Let* char $K = 0$ *or* char $K \nmid n$ *and let ζ be a primitive n-th root*

of unity. If $\zeta + \zeta^{-1} \in K$, then $K(D_n)$ is rational over K. In particular, $K(D_4)$ is rational over K.

Remark. Compare with [Bl, Proposition 2.1 and Theorem 3.3].

Proof. Define $V = \oplus_{i=1}^{n} K \cdot x_i$ and let D_n act on V by

$$\begin{aligned} &\sigma : x_1 \mapsto x_2 \mapsto \cdots \mapsto x_n \mapsto x_1, \\ &\tau : x_i \mapsto x_{n-i} \quad \text{for } 1 \le i \le n-1, \\ &\quad x_n \mapsto x_n. \end{aligned}$$

Let $W = \oplus_{g \in D_n} K \cdot x(g)$ be the space of regular representation of D_n. Note that V is a subrepresentation of W, because we may define $W_0 = \oplus_{i=1}^{n} K \cdot x_i'$ where $x_i' = x(\sigma^i) + x(\sigma^i\tau)$. Then $x_i \mapsto x_i'$ for $1 \le i \le n$ provides an equivariant map from V onto W_0.

By Theorem 2.1 $K(W)$ is D_n-isomorphic to $K(V)(\widetilde{x}_1, \widetilde{x}_2, \cdots, \widetilde{x}_n)$ with $\lambda(\widetilde{x}_i) = \widetilde{x}_i$ for any $\lambda \in D_n$. Hence $K(D_n) = K(W)^{D_n} = K(V)^{D_n}(\widetilde{x}_1, \widetilde{x}_2, \cdots, \widetilde{x}_n)$. Thus it suffices to show that $K(V)^{D_n}$ is rational over K.

Define $y_i = \sum_{j=1}^{n} \zeta^{i(j-1)} x_j$ for $0 \le i \le n-1$.

Since $\zeta + \zeta^{-1} \in K$, it follows that $[K(\zeta) : K] \le 2$.

Case 1. $\zeta \in K$.

Note that $K(x_1, \cdots, x_n) = K(y_0, y_1, \cdots, y_{n-1})$ and $\sigma(y_i) = \zeta^{-i} y_i$, $\tau(y_i) = \zeta^{-2i} y_{n-i}$ for $0 \le i \le n-1$.

Apply Theorem 2.1. We get

$$K(y_0, y_1, \cdots, y_{n-1})^{D_n} = K(y_1, y_{n-1})^{D_n}(z_1, \cdots, z_{n-2})$$

with $\sigma(z_i) = \tau(z_i) = z_i$. Now $K(y_1, y_{n-1})^{D_n} = K(t, y_1)^{D_n}$ where $t = y_{n-1}/y_1$ and $\sigma(y_1) = \zeta^{-1} y_1$, $\sigma(t) = \zeta^2 t$, $\tau(y_1) = \zeta^{-2} t y_1$, $\tau(t) = \zeta^4/t$. Apply Theorem 2.4. It suffices to show that $K(t)^{D_n}$ is rational over K. However, it is clear that $K(t)^{D_n}$ is rational by Lüroth's Theorem.

Case 2. $\zeta \notin K$ and $\mathrm{Gal}(K(\zeta)/K) = \{id, \rho\}$ where $\rho(\zeta) = \zeta^{-1}$.

Extend the actions of σ, τ, ρ to $K(\zeta)(x_1, \cdots, x_n)$ by $\sigma(\zeta) = \tau(\zeta) = \zeta$, $\rho(x_i) = x_i$ for $1 \le i \le n$.

Note that

$$\begin{aligned} K(x_1, \cdots, x_n)^{<\sigma,\tau>} &= \{K(\zeta)(x_1, \cdots, x_n)^{<\rho>}\}^{<\sigma,\tau>} \\ &= K(\zeta)(x_1, \cdots, x_n)^{<\sigma,\tau,\rho>} \\ &= K(\zeta)(y_0, \cdots, y_{n-1})^{<\sigma,\tau,\rho>} \end{aligned}$$

where $\sigma(y_i) = \zeta^{-i} y_i$, $\tau(y_i) = \zeta^{-2i} y_{n-i}$, $\rho(y_i) = y_{n-i}$. Since $\langle \sigma, \tau, \rho \rangle \simeq D_n \times \mathbb{Z}_2$ acts on $K(\zeta)(y_1, y_{n-1})$ faithfully, we may apply Theorem 2.1. Thus it suffices to show that $K(\zeta)(y_1, y_{n-1})^{<\sigma,\tau,\rho>}$ is rational over K.

Define $t = y_{n-1}/y_1$. Then $\sigma(t) = \zeta^2 t$, $\sigma(y_1) = \zeta^{-1}y_1$, $\tau(t) = \zeta^4/t$, $\tau(y_1) = \zeta^{-2}ty_1$, $\rho(t) = 1/t$, $\rho(y_1) = ty_1$. By Theorem 2.4, if $K(\zeta)(t)^{<\sigma,\tau,\rho>}$ is rational over K, so is $K(\zeta)(t, y_1)^{<\sigma,\tau,\rho>}$ over K.

Define $m = n$, if n is an odd integer; $m = n/2$ if n is an even integer. Then the restriction of σ to $K(\zeta)(t)$ is of order m. Define $u = t^m$. It follows that $K(\zeta)(t)^{<\sigma>} = K(\zeta)(u)$ and $\tau(u) = 1/u$, $\rho(u) = 1/u$. Now $K(\zeta)(u)^{<\tau,\rho>} = K(\zeta)(u)^{<\tau\rho,\rho>} = \{K(\zeta)(u)^{<\tau\rho>}\}^{<\rho>} = K(u)^{<\rho>} = K(u+(1/u))$ is rational over K. □

Theorem 2.7 (Gröbner [Gr])**.** *Let G be the quaternion group. Then $K(G)$ is rational over K for any field K.*

Proof. Because of Theorem 2.5, we may assume that char $K \neq 2$. Recall the notations at the end of Section 1. We write $G = \langle \sigma, \tau : \sigma^4 = \tau^4 = 1, \sigma^2 = \tau^2, \tau\sigma\tau^{-1} = \sigma^3 \rangle$.

Define $V = \oplus_{i=1}^4 K \cdot x_i$ with $\sigma : x_1 \mapsto x_2$, $x_2 \mapsto -x_1$, $x_3 \mapsto -x_4$, $x_4 \mapsto x_3$, $\tau : x_1 \mapsto x_3$, $x_2 \mapsto x_4$, $x_3 \mapsto -x_1$, $x_4 \mapsto -x_2$.

Note that V is a faithful subrepresentation of the regular representation $W = \oplus_{g\in G} K \cdot x(g)$. In fact, we may take $x_1 = x(1) - x(\sigma^2)$, $x_2 = \sigma \cdot x_1$, $x_3 = \tau \cdot x_1$, $x_4 = \tau\sigma \cdot x_1$. Now apply Theorem 2.1. Thus it remains to prove that $K(x_1, x_2, x_3, x_4)^G$ is rational over K.

Define $y_1 = x_1/x_4$, $y_2 = x_2/x_4$, $y_3 = x_3/x_4$, $y_4 = x_4$.

It is straightforward to check that

$$\sigma : y_1 \mapsto y_2/y_3,\ y_2 \mapsto -y_1/y_3,\ y_3 \mapsto -1/y_3,\ y_4 \mapsto y_3y_4,$$
$$\tau : y_1 \mapsto -y_3/y_2,\ y_2 \mapsto -1/y_2,\ y_3 \mapsto y_1/y_2,\ y_4 \mapsto -y_2y_4.$$

If $K(y_1, y_2, y_3)^{<\sigma,\tau>}$ is rational over K, so is $K(y_1, y_2, y_3, y_4)^{<\sigma,\tau>}$ over K by Theorem 2.4.

Define $z_1 = y_1$, $z_2 = y_2/y_1$, $z_3 = y_3$. Then

$$\sigma : z_1 \mapsto z_1z_2/z_3,\ z_2 \mapsto -1/z_2,\ z_3 \mapsto -1/z_3,$$
$$\tau : z_1 \mapsto -z_3/z_1z_2,\ z_2 \mapsto 1/z_3,\ z_3 \mapsto 1/z_2.$$

Define $z = z_1(1 + (z_2/z_3))$. Then $K(y_1, y_2, y_3)^{<\sigma>} = K(z_1, z_2, z_3)^{<\sigma>} = K(z, z_2, z_3)^{<\sigma>}$. Now apply Theorem 2.3 with $a = b = -1$, i.e. define

$$u = \frac{z_2 - \dfrac{a}{z_2}}{z_2z_3 - \dfrac{ab}{z_2z_3}}, \qquad v = \frac{z_3 - \dfrac{b}{z_3}}{z_2z_3 - \dfrac{ab}{z_2z_3}}.$$

It follows that $K(z, z_2, z_3)^{<\sigma>} = K(z, u, v)$.

Now it is easy to check that

$$\tau : u \mapsto -v,\ v \mapsto -u,\ z \mapsto \lambda/z$$

where $\lambda = -2 - (z_2/z_3) - (z_3/z_2)$.

Since

$$\begin{aligned} -(z_2/z_3)-(z_3/z_2) &= (z_2 + (-1/z_2))(z_3 + (-1/z_3)) - (z_2z_3 + 1/(z_2z_3)) \\ &= \{(-bu^2+av^2+1)(bu^2-av^2+1)-(-bu^2-av^2+1)\}/(uv) \\ &= \{bu^2 + av^2 - (bu^2 - av^2)^2\}/(uv) \end{aligned}$$

by the last statement of Theorem 2.3 (here $a = b = -1$ in the present situation), we find that

$$\begin{aligned} \lambda &= -2 - \{u^2 + v^2 + (u^2 - v^2)^2\}/(uv) \\ &= -(u+v)^2\{(u-v)^2 + 1\}/(uv). \end{aligned}$$

Define $p = u + v$, $x = u - v$, $y = 2zuv/(u + v)$. We can check that

$$\tau : p \mapsto -p,\ x \mapsto x,\ y \mapsto A/y$$

where $A = -(x^2 + 1)(x^2 - p^2)$.

Define $t = p^2$, $q_1 = y + (A/y)$, $q_2 = p\{y - (A/y)\}$. We find that

$$K(z, u, v)^{<\tau>} = K(p, x, y)^{<\tau>} = K(t, x, q_1, q_2)$$

with the relation

$$q_1^2 - (q_2/p)^2 = 4A, \tag{1}$$

because $[K(t, x, q_1, q_2, p) : K(t, x, q_1, q_2)] \leq 2$, and $K(t, x, q_1, q_2, p) = K(x, q_1, y - (A/y), p) = K(p, x, y)$. (Note that the last equality holds because we can solve y within the field $K(x, q_1, y - (A/y), p)$.)

Now we will simplify the relation (1). It becomes

$$tq_1^2 - q_2^2 = -4(x^2 + 1)(x^2 - t)t.$$

Dividing by t^2 on both sides, we get

$$(1/t)q_1^2 - (q_2/t)^2 = -4(x^2 + 1)\{(1/t)x^2 - 1\}. \tag{2}$$

From (2), it is obvious that $t \in K(x, q_1, q_2/t)$. Thus

$$K(t, x, q_1, q_2) = K(t, x, q_1, q_2/t) = K(x, q_1, q_2/t)$$

is rational over K. □

§3. Main results

Without loss of generality we will assume that K is any field with char$K \neq 2$ throughout this section, because Theorem 2.5 will take care of the case char $K = 2$.

Let $G = \langle \sigma, \tau : \sigma^8 = \tau^2 = 1, \tau\sigma\tau^{-1} = \sigma^a \rangle$. If $a = -1$, then G is the dihedral group; if $a = 3$, then G is the quasi-dihedral group; if $a = 5$, G is the modular group [Le1]. In the quasi-dihedral group G, let $u = \sigma$, $v = \sigma\tau$, then G can be defined as $\langle u, v : u^4 = v^2, vuv^{-1} = u^3 \rangle$, which is the definition of this group given in [Le1].

We will find a faithful subrepresentation of $W = \oplus_{g\in G} K \cdot x(g)$, the regular representation of G. Define

$$x_i = x(\sigma^i) + x(\sigma^i\tau) \qquad \text{for } 0 \leq i \leq 7.$$

Then $\oplus_{i=0}^{7} K \cdot x_i$ is a G-subspace of W and $\sigma(x_i) = x_{i+1}$ and $\tau(x_i) = x_{ai}$ for $0 \leq i \leq 7$ where the index $i + 1$ or ai is understood to be taken modulo 8. By Theorem 2.1, in order to prove the rationality problem of $K(G)$, it suffices to consider the case of $K(x_0, x_1, \cdots, x_7)^G$.

Theorem 3.1. *If G is the dihedral group, then $K(G)$ is rational over K.*

Proof. Define $y_i = x_i - x_{i+4}$, $y_{i+4} = x_i + x_{i+4}$ for $0 \leq i \leq 3$. Because of Theorem 2.1, it suffices to show that $K(y_0, y_1, y_3, y_4)^{<\sigma,\tau>}$ is rational over K. Note that $\sigma : y_0 \mapsto y_1 \mapsto y_2 \mapsto y_3 \mapsto -y_0$, $\tau : y_0 \mapsto y_0$, $y_1 \mapsto -y_3$, $y_2 \mapsto -y_2$, $y_3 \mapsto -y_1$.

Let $\pi = \mathrm{Gal}(K(\sqrt{-1})/K)$. If $\sqrt{-1} \in K$, then π is the trivial group; if $\sqrt{-1} \notin K$, then $\pi = \langle \rho \rangle$ where $\rho(\sqrt{-1}) = -\sqrt{-1}$. In the sequel, we shall take the following convention: if we write the action of ρ, it is understood that $\sqrt{-1} \notin K$; however, if $\sqrt{-1} \in K$, the reader can just forget ρ even when we write the action of it.

We will extend the actions of σ, τ, ρ to $K(\sqrt{-1})(y_0, y_1, y_2, y_3)$ by requiring $\sigma(\sqrt{-1}) = \tau(\sqrt{-1}) = \sqrt{-1}$ and $\rho(y_i) = y_i$ for $0 \leq i \leq 3$. Note that

$$\begin{aligned} K(y_0, \cdots, y_3)^{<\sigma,\tau>} &= \{K(\sqrt{-1})(y_0, \cdots, y_3)^{<\rho>}\}^{<\sigma,\tau>} \\ &= K(\sqrt{-1})(y_0, \cdots, y_3)^{<\sigma,\tau,\rho>}. \end{aligned}$$

Define $z_1 = \sqrt{-1}y_1 + y_3$, $z_2 = \sqrt{-1}y_2 - y_0$, $z_3 = -\sqrt{-1}y_1 + y_3$, $z_4 = -\sqrt{-1}y_2 - y_0$. Then

$$\begin{aligned} &\sigma : z_1 \mapsto z_2 \mapsto \sqrt{-1}z_1,\ z_3 \mapsto z_4 \mapsto -\sqrt{-1}z_3, \\ &\tau : z_1 \mapsto -\sqrt{-1}z_3,\ z_2 \mapsto z_4,\ z_3 \mapsto \sqrt{-1}z_1,\ z_4 \mapsto z_2, \\ &\rho : z_1 \mapsto z_3,\ z_2 \mapsto z_4,\ z_3 \mapsto z_1,\ z_4 \mapsto z_2. \end{aligned}$$

Define $u_1 = z_2/z_1$, $u_2 = z_4/z_3$, $u_3 = z_2z_4$, $u_4 = z_1^4$. We get that

$$K(\sqrt{-1})(z_1, z_2, z_3, z_4)^{<\sigma^2>} = K(\sqrt{-1})(u_1, u_2, u_3, u_4)$$

and the actions of σ, τ, ρ are given by

$$\sigma : u_1 \mapsto \sqrt{-1}/u_1,\ u_2 \mapsto -\sqrt{-1}/u_2,\ u_3 \mapsto u_3/(u_1u_2),\ u_4 \mapsto u_1^4u_4,$$
$$\tau : u_1 \mapsto \sqrt{-1}u_2,\ u_2 \mapsto -\sqrt{-1}u_1,\ u_3 \mapsto u_3,\ u_4 \mapsto u_3^4/(u_1^4u_2^4u_4),$$
$$\rho : u_1 \mapsto u_2 \mapsto u_1,\ u_3 \mapsto u_3,\ u_4 \mapsto u_3^4/(u_1^4u_2^4u_4).$$

Define $w_1 = u_3+(u_3/(u_1u_2))$, $w_2 = u_1u_2$, $w_3 = u_1+(1/u_2)$, $w_4 = u_1^3u_2u_3^{-2}u_4$. Then

$$\sigma : w_1 \mapsto w_1,\ w_2 \mapsto 1/w_2,\ w_3 \mapsto \sqrt{-1}(w_2 + (1/w_2) + 2)/w_3,\ w_4 \mapsto -w_4,$$
$$\tau : w_1 \mapsto w_1,\ w_2 \mapsto w_2,\ w_3 \mapsto \sqrt{-1}(w_2 + (1/w_2) + 2)/w_3,\ w_4 \mapsto -1/w_4,$$
$$\rho : w_1 \mapsto w_1,\ w_2 \mapsto w_2,\ w_3 \mapsto (w_2 + (1/w_2) + 2)/w_3,\ w_4 \mapsto 1/w_4$$

Thus the action of $\sigma\tau$ is given by

$$\sigma\tau : w_1 \mapsto w_1,\ w_2 \mapsto 1/w_2,\ w_3 \mapsto w_3,\ w_4 \mapsto 1/w_4.$$

Define $w_5 = (w_2 - (1/w_2))(1 - w_4)/(1 + w_4)$. Then $K(\sqrt{-1})(w_1, w_2, w_3, w_4) = K(\sqrt{-1})(w_1, w_2, w_3, w_5)$ and $\sigma(w_5) = -(w_2-(1/w_2))^2/w_5$, $\sigma\tau(w_5) = w_5$, $\rho(w_5) = -w_5$.

Now $K(\sqrt{-1})(w_1, w_2, w_3, w_5)^{<\sigma,\tau>} = K(\sqrt{-1})(w_1, w_2, w_3, w_5)^{<\sigma,\sigma\tau>}$. Moreover, $K(\sqrt{-1})\ (w_1, w_2, w_3, w_5)^{<\sigma\tau>} = K(\sqrt{-1})(w_1, w_3, w_5, w_2 + (1/w_2))$.

Define $s = w_1, t = w_2 + (1/w_2), x = w_3, y = \sqrt{-1}w_5$. Then

$$\sigma : s \mapsto s,\ t \mapsto t,\ x \mapsto \sqrt{-1}(t + 2)/x,\ y \mapsto (t^2 - 4)/y,$$
$$\rho : s \mapsto s,\ t \mapsto t,\ x \mapsto (t + 2)/x,\ y \mapsto y.$$

By Theorem 2.3, define

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

where $a = \sqrt{-1}(t + 2)$, $b = t^2 - 4$, and we find that $K(\sqrt{-1})(w_1, w_3, w_5, w_2 + (1/w_2))^{<\sigma>} = K(\sqrt{-1})(s, t, x, y)^{<\sigma>} = K(\sqrt{-1})(s, t, u, v)$.

If $\sqrt{-1} \in K$, then $K(\sqrt{-1})(s, t, u, v) = K(s, t, u, v)$ is rational as we expect.

From now on, assume $\sqrt{-1} \notin K$ and ρ actually exists. We shall find the action of ρ on u and v. Remember $\rho(\sqrt{-1}) = -\sqrt{-1}$ and $\rho(a) = -a$, $\rho(b) = b$. Now

$$\rho(u) = \frac{\dfrac{t+2}{x} + \dfrac{ax}{t+2}}{\dfrac{t+2}{x}y + \dfrac{abx}{(t+2)y}} = \frac{x - \dfrac{a}{x}}{\dfrac{bx}{y} - \dfrac{ay}{x}},$$

$$\rho(v) = \frac{y - \dfrac{b}{y}}{\dfrac{t+2}{x}y + \dfrac{abx}{(t+2)y}} = -\sqrt{-1}\frac{y - \dfrac{b}{y}}{\dfrac{bx}{y} - \dfrac{ay}{x}}.$$

Define $w = (1+\sqrt{-1})u/v$. Then $\rho(w) = w$.

It is laborious, but not difficult, to verify that

$$\rho(u) = \frac{x - \dfrac{a}{x}}{\dfrac{bx}{y} - \dfrac{ay}{x}} = \frac{u}{bu^2 - av^2}. \tag{3}$$

Here is a cheating way to demonstrate the above identity. By Theorem 2.3, the right-hand side of Identity (3) is equal to $(y+(b/y)-(1/u))^{-1}$. It is really routine to check that the left-hand side of Identity (3) is equal to $(y+(b/y)-(1/u))^{-1}$.

In conclusion, we find $\rho(u) = c/u$ where $c = w^2/\{(t^2-4)w^2 + 2(t+2)\}$.

Define $p = \lambda u/w$ where $\lambda = (t^2-4)w^2 + 2(t+2)$. Then $\rho(p) = \lambda/p$.

Now $K(\sqrt{-1})(s,t,u,v)^{<\rho>} = K(\sqrt{-1})(s,t,w,p)^{<\rho>}$. We may show that $K(\sqrt{-1})(s,t,w,p)^{<\sigma>}$ is rational over $K(s,w)$ by applying [HK1, (2.4) Theorem]. Here we provide a direct proof of it. Note that $K(\sqrt{-1})(s,t,w,p)^{<\sigma>} = K(s,t,w,p_1,p_2)$ where $p_1 = p + (\lambda/p)$, $p_2 = \sqrt{-1}(p - (\lambda/p))$. Note that

$$p_1^2 + p_2^2 = 4\lambda = 4(t^2-4)w^2 + 8(t+2).$$

Define $r = t+2$. Then $t^2 - 4 = r(r-4)$ and we get

$$p_1^2 + p_2^2 = 4r(r-4)w^2 + 8r.$$

Dividing by r^2 on both sides, it turns out that

$$\begin{aligned}(p_1/r)^2 + (p_2/r)^2 &= 4w^2 - 16(1/r)w^2 + 8(1/r).\\ 8(1/r)(1-2w^2) &= (p_1/r)^2 + (p_2/r)^2 - 4w^2.\end{aligned}$$

Thus $r \in K(w, p_1/r, p_2/r)$.

It follows that

$$\begin{aligned}K(\sqrt{-1})(s,t,u,v)^{<\rho>} &= K(s,t,w,p_1,p_2) = K(r,s,w,p_1/r,p_2/r)\\ &= K(s,w,p_1/r,p_2/r)\end{aligned}$$

is rational over K. □

Theorem 3.2. *If G is the quasi-dihedral group, then $K(G)$ is rational over K.*

Proof. We shall show that $K(x_0,\cdots,x_7)^G$ is rational over K where $\sigma : x_0 \mapsto x_1 \mapsto \cdots \mapsto x_7 \mapsto x_0$, $\tau : x_0 \mapsto x_0$, $x_1 \leftrightarrow x_3$, $x_2 \leftrightarrow x_6$, $x_4 \mapsto x_4$, $x_5 \leftrightarrow x_7$.

The proof is almost the same as that in Theorem 3.1. We shall make the same change of variables, but the action may not be the same as in the proof of Theorem 3.1. We shall indicate the main modifications.

We shall define y_i, z_i, u_i, v_i, w_i by the same way as in Theorem 3.1. The actions of σ and ρ are the same. But we shall be careful about the action of τ. Note that

$$\begin{aligned}\tau :&y_0 \mapsto y_0,\ y_1 \mapsto y_3,\ y_2 \mapsto -y_2,\ y_3 \mapsto y_1,\\ &z_1 \mapsto \sqrt{-1}z_3,\ z_2 \mapsto z_4,\ z_3 \mapsto -\sqrt{-1}z_1,\ z_4 \mapsto z_2,\\ &u_1 \mapsto -\sqrt{-1}u_2,\ u_2 \mapsto \sqrt{-1}u_1,\ u_3 \mapsto u_3,\ u_4 \mapsto u_3^4/(u_1^4u_2^4u_4),\\ &v_1 \mapsto v_1, v_2 \mapsto v_2,\ v_3 \mapsto -\sqrt{-1}v_2/v_3,\ v_4 \mapsto -v_1^4/(v_2^2v_4),\\ &w_1 \mapsto w_1,\ w_2 \mapsto w_2,\ w_3 \mapsto -\sqrt{-1}(w_2 + (1/w_2) + 2)/w_3,\ w_4 \mapsto -1/w_4.\end{aligned}$$

Thus the action of $\sigma\tau$ is given by:

$$\sigma\tau : w_1 \mapsto w_1,\ w_2 \mapsto 1/w_2,\ w_3 \mapsto -w_3,\ w_4 \mapsto 1/w_4.$$

Define $w_3' = (w_2 - (1/w_2))w_3$; and we should redefine $x = w_3'$ in the present situation. Note that $\sigma(x) = -\sqrt{-1}(t^2-4)(t+2)/x$, $\rho(x) = (t^2-4)(t+2)/x$. All the others remain the same.

Thus we define u, v, w by the same way. But $a = -\sqrt{-1}(t^2-4)(t+2)$ in the present situation. Note that

$$\rho(u) = \frac{x - \dfrac{a}{x}}{\dfrac{bx}{y} - \dfrac{ay}{x}}, \qquad \rho(v) = \sqrt{-1}\ \frac{y - \dfrac{b}{y}}{\dfrac{bx}{y} - \dfrac{ay}{x}}.$$

Define $w = (1 - \sqrt{-1})u/v$. Then $\rho(w) = w$ as before.

Now $\rho(u) = c/u$ where $c = w^2/\{(t^2-4)w^2 + 2(t^2-4)(t+2)\}$. Define $p = \lambda u/w$ as before, but with $\lambda = (t^2-4)w^2 + 2(t^2-4)(t+2)$.

It follows that the fixed field is $K(s,t,w,p_1,p_2) = K(r,s,w,p_1,p_2)$ where $r = t-2$ and the relation becomes

$$p_1^2 + p_2^2 = 4r(r+4)w^2 + 8r(r+4)^2.$$

We change the above relation as

$$\left(\frac{p_1}{r(r+4)}\right)^2 + \left(\frac{p_2}{r(r+4)}\right)^2 = 4\left(\frac{w}{r+4}\right)^2 + 16\frac{1}{r}\left(\frac{w}{r+4}\right)^2 + \frac{8}{r}.$$

Thus $r \in K(w/(r+4), p_1/\{r(r+4)\}, p_2/\{r(r+4)\})$. □

Theorem 3.3. *If G is the modular group, then $K(G)$ is rational over K.*

Proof. We shall prove that $K(x_0, \cdots, x_7)^G$ is rational over K where $\sigma : x_0 \mapsto x_1 \mapsto \cdots \mapsto x_7 \mapsto x_0$, $\tau : x_0 \mapsto x_0$, $x_1 \leftrightarrow x_5$, $x_2 \mapsto x_2$, $x_3 \leftrightarrow x_7$, $x_4 \mapsto x_4$, $x_6 \mapsto x_6$.

Note that $\tau : y_0 \mapsto y_0,\ y_1 \mapsto -y_1,\ y_2 \mapsto y_2,\ y_3 \mapsto -y_3$. The situation is different from the previous two cases, and we cannot copy the proof of them. Fortunately the present situation turns out to be easier.

Define $z_0 = y_0^2,\ z_1 = y_1/y_0,\ z_2 = y_2/y_1,\ z_3 = y_3/y_2$. Then $K(y_0, \cdots, y_3)^{<\sigma^4>} = K(z_0, \cdots, z_3)$. Note that

$$\sigma : z_0 \mapsto z_0 z_1^2,\ z_1 \mapsto z_2 \mapsto z_3 \mapsto -1/(z_1 z_2 z_3),$$
$$\tau : z_0 \mapsto z_0,\ z_1 \mapsto -z_1,\ z_2 \mapsto -z_2,\ z_3 \mapsto -z_3.$$

By Theorem 2.1 it suffices to prove that $K(z_1, z_2, z_3)^{<\sigma,\tau>}$ is rational over K.

Define $t = z_1 z_3,\ x = z_1,\ y = z_2$. Then we get

$$\sigma : t \mapsto -1/t,\ x \mapsto y \mapsto t/x,$$
$$\tau : t \mapsto t,\ x \mapsto -x,\ y \mapsto -y.$$

Note that $\sigma^2(t) = t,\ \sigma^2(x) = t/x,\ \sigma^2(y) = -1/ty$. Hence define

$$u = \frac{x - \dfrac{a}{x}}{xy - \dfrac{ab}{xy}} = \frac{x - \dfrac{t}{x}}{xy + \dfrac{1}{xy}}, \qquad v = \frac{y - \dfrac{b}{y}}{xy - \dfrac{ab}{xy}} = \frac{y + \dfrac{1}{ty}}{xy + \dfrac{1}{xy}}$$

where $a = t,\ b = -1/t$. By Theorem 2.3, $K(t, x, y)^{<\sigma^2>} = K(t, u, v)$.

We find that $\tau(t) = t,\ \tau(u) = -u,\ \tau(v) = -v$. The action of σ is given by

$$\sigma(u) = \frac{y + \dfrac{1}{ty}}{\dfrac{ty}{x} + \dfrac{x}{ty}}, \qquad \sigma(v) = \frac{\dfrac{t}{x} - x}{\dfrac{ty}{x} + \dfrac{x}{ty}}.$$

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

It is not difficult to check that

$$\frac{y + \dfrac{1}{ty}}{\dfrac{ty}{x} + \dfrac{x}{ty}} = \frac{tv}{u^2 + t^2 v^2}.$$

Hence we find that $\sigma(u) = t/\{u(w + (t^2/w))\}$.

Note that $K(t, u, w)^{<\tau>} = K(t, u^2, w)$.

Define $z = u^2(w + (t^2/w))/t$. Then $\sigma(z) = 1/z$.

In summary, we will consider $K(t, u^2, w)^{<\sigma>} = K(t, w, z)^{<\sigma>}$ with $\sigma(t) = -1/t,\ \sigma(w) = -1/w,\ \sigma(z) = 1/z$.

Define $p = (1 - z)/(1 + z)$. Then $\sigma(p) = -p$. By Theorem 2.1, $K(t, w, z)^{<\sigma>} = K(t, w, p)^{<\sigma>}$ is rational provided that $K(t, w)^{<\sigma>}$ is rational. However the rationality of $K(t, w)^{<\sigma>}$ follows from Theorem 2.3. □

References

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

[Bl] E. V. Black, Deformations of dihedral 2-group extensions of fields, *Trans. Amer. Math. Soc.* **35** (1999), 3229–3241.

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

[Gr] W. Gröbner, Minimalbasis der Quaternionengruppe, *Monatshefte für Math. und Physik* **41** (1934), 78–84.

[HK1] M. Hajja and M. Kang, Three-dimensional purely monomial group actions, *J. Algebra* **170** (1994), 805–860.

[HK2] M. Hajja and M. Kang Some actions of symmetric groups, *J. Algebra* **177** (1995), 511–535.

[Ka] M. Kang, *Noether's problem for dihedral groups*, preprint.

[Ke] G. Kemper, Generic polynomials are descent-generic, *manuscripta math.* **105** (2001), 139–141.

[Ku] H. Kuniyoshi, On a problem of Chevalley, *Nagoya Math. J.* **8** (1955), 65–67.

[Le1] A. Ledet, Generic polynomials for quasi-dihedral, dihedral and modular extensions of order 16, *Proc. Amer. Math. Soc.* **128** (1999), 2213–2222.

[Le2] A. Ledet, Generic extensions and generic polynomials, *J. Symbolic Compt.* **30** (2000), 867–872.

[Me] F. R. DeMeyer, Generic polynomials, *J. Algebra* **84** (1983), 441–448.

[Mi] T. Miyata, Invariants of certain groups I, *Nagoya Math. J.* **41** (1971), 69–73.

[Sa1] D. J. Saltman, Generic Galois extensions and problems in field theory, *Advances in Math.* **43** (1982), 250–283.

[Sa2] D. J. Saltman, Retract rational fields and cyclic Galois extensions, *Israel J. Math.* **47** (1984), 165–215.

[Sa3] D. J. Saltman, Groups acting on fields: Noether's problem, *Contemporary Math.* **43** (1985), 267–277.

[Sm] G. W. Smith, Generic cyclic polynomials of odd degrees, *Communications in Algebra* **19** (1991), 3367–3391.

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

Huah Chu and Ming-chang Kang
Department of Mathematics
National Taiwan University
Taipei
Taiwan
e-mail: kang@math.ntu.edu.tw

Shou-Jen Hu
Department of Mathematics
Tamkang University
Taipei
Taiwan

(Received: September 16, 2002)