PACIFIC JOURNAL OF MATHEMATICS
Vol. 139, No. 1, 1989

NONRATIONAL FIXED FIELDS

JAMES K. DEVENEY AND JOE YANIK

We present an example of a flag of rational extensions, stabilized by the action of the group of order 2 such that the fixed field under the group action is not retract rational and hence not rational. This fixed field is shown to be a genus 0 extension of a pure transcendental extension.

Let $L \supset K \supset F$ be fields finitely generated over F. If $K = F(X_1, \dots, X_n)$ where $\{X_1, \dots, X_n\}$ is algebraically independent over F then K is a rational extension of F. Saltman defined K to be a *retract rational extension of* F if K is the quotient field of an F-algebra A and there are maps $f\colon F[X_1, \dots, X_n](1/w) \to A$ and $g\colon A \to F[X_1, \dots, X_n](1/w)$ such that $f \circ g = \mathrm{id}$, where $\{X_1, \dots, X_n\}$ is algebraically independent over F and $w \in F[X_1, \dots, X_n]$. If rational extensions are considered free objects then retract rational extensions could in some sense be considered as projective objects.

Let G be a finite group of k-automorphisms of a rational function field $k(X_1, \dots, X_n)$. Assume that the "flag" of subfields $\{k[X_1, \dots, X_i)/1 \le i \le n\}$ is stablized by G. Then in many situations, for example if $|G|$ is odd, the fixed field of G will be rational over k [**10**, Lemma 4, p. 322]. We present an example of G as above, where $|G| = 2$ and the fixed field of G is not even retract rational. We also describe this field as a genus 0 extension of a pure transcendental extension of the rational members.

Let α be the automorphism of $Q(X_1, X_2, X_3, X_4, Z_1, \dots, Z_8)$ defined by

$$\begin{aligned} \alpha(X_i) &= X_{i+1} \quad \text{for } 1 \le i \le 3, \\ &\, -X_1 \quad \text{for } i = 4, \\ \alpha(Z_i) &= Z_{i+1} \quad \text{for } 1 \le i \le 7, \\ &\, Z_1 \quad \text{for } i = 8. \end{aligned}$$

Then α is a k-automorphism of order 8 and induces a G-action on $Q(X_1, X_2, X_3, X_4, Z_1, \dots, Z_8)$ where $G = C_8$. Furthermore, the restriction of α induces a faithful G-action on each of $Q(X_1, X_2, X_3, X_4)$ and $Q(Z_1, \dots, Z_8)$. By [**2**, Propositioon 1.4, p. 303] this implies that $Q(X_1, X_2, X_3, X_4, Z_1, \dots, Z_8)^\alpha$ is a rational extension of both

$Q(X_1, X_2, X_3, X_4)^\alpha$ and $Q(Z_1, \dots, Z_8)^\alpha$. But $Q(Z_1, \dots, Z_8)^\alpha$ is not retract rational [**6**, Theorem 5.11, p. 281] and stable isomorphism preserves retract rationality [**4**, Proposition 3.6, p. 183], so $Q(X_1, X_2, X_3, X_4)^\alpha$ is not retract rational.

Consider $Q(X_1, X_2, X_3, X_4)^{\alpha^2}$. We claim that

$$Q(X_1, X_2, X_3, X_4)^{\alpha^2} = Q\left(\frac{X_3^2 - X_1^2}{X_1X_3}, X_1^2 + X_3^2, X_1X_2 + X_3X_4, X_2X_3 - X_1X_4\right) \equiv L.$$

Clearly L is fixed by α^2 and

$$L \subseteq L\left(X_1X_3, \frac{X_3}{X_1}\right) \subseteq Q(X_1, X_2, X_3, X_4).$$

Since X_3/X_1 is a root of

$$Z^2 - \left(\frac{X_3^2 - X_1^2}{X_1X_3}\right)Z - 1 = 0$$

and, $X_1X_3 = (X_1^2 + X_3^2)/(X_1/X_3 + X_3/X_1)$,

$$\left[L\left(X_1X_3, \frac{X_3}{X_1}\right) : L\right] = 2.$$

Since X_3 is a root of $(X_1/X_3)Z^2 - X_1X_3 = 0$,

$$\left[Z(X_1, X_2, X_3, X_4) : L\left(X_1X_3, \frac{X_3}{X_1}\right)\right] = 2.$$

Thus L is of codimension 4 and the claim is established.

Let $U = (X_3^2 - X_1^2)/X_1X_3$, $V = X_1^2 + X_3^2$, $W = X_1X_2 + X_3X_4$ and $Y = X_2X_3 - X_1X_4$. Then α has order 2 on $Q(U, V, W, Y)$ and $Q(U, V, W, Y)^\alpha = Q(X_1, X_2, X_3, X_4)^\alpha$.

One can check that $\alpha(W) = Y$, $\alpha(Y) = W$,

$$\alpha(V) = \frac{W^2 + Y^2}{V} \quad \text{and} \quad \alpha(U) = \frac{(W^2 - Y^2)U + WY}{-4WYU + W^2 - Y^2}.$$

Thus α stabilizes the flag of subfields

$$Q(W + Y) \subseteq Q(W, Y) \subseteq Q(W, Y, U) \subseteq Q(W, Y, V, U),$$

α has order 2, and its fixed field is not retract rational.

It is interesting that the fixed field of α has a rather simpler description:

$$\begin{tikzcd}[column sep=small]
 & & Q(W,Y,V,U) \arrow[dll, dash] \arrow[d, dash] \arrow[drr, dash] & & \\
Q(W,Y,V) \arrow[dr, dash] & & L_1L_2 \arrow[dl, dash] \arrow[dr, dash] & & Q(W,Y,U) \arrow[dl, dash] \\
 & L_1 \arrow[dr, dash] & & L_2 \arrow[dl, dash] & \\
 & & Q(WY, W+Y) & &
\end{tikzcd}$$

where L_1 and L_2 are the fixed fields of the restrictions of α to $Q(W,Y,V)$ and $Q(W,Y,U)$, respectively, and $Q(W,Y,V,U)^\alpha = L_1L_2$. $L_1/Q(WY, W+Y)$ and $L_2/Q(WY, W+Y)$ are both genus 0 because they became rational after a change of base to $Q(W,Y)$. So the fixed field of α is just the free join of two genus 0 function fields over a pure transcendental extension of Q. Actually, it is possible to get an even simpler description, but first we need a few preliminaries.

Let L/K be a Galois extension with group G and let Z be transcendental over L. It has been noted (for example in **[11]**) that an extension of G to $L(Z)$ corresponds to a "crossed homomorphism" from G to $\mathrm{PGL}_2(L)$, (i.e. to an element of $H^1(G, \mathrm{PGL}_2(L))$) in the following manner: Given an extension we define

$$G \to \mathrm{PGL}_2(L)$$

by $\sigma \mapsto \overline{M}_\sigma$ where,

$$\text{if } \sigma(Z) = \frac{aZ+b}{cZ+d} \quad \text{then } M_\sigma = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \in \mathrm{GL}_2(L)$$

(note the transposition of the b and the c) and $\overline{M}_\sigma$ is the image of M_σ in $\mathrm{PGL}_2(L)$. Then one can check that $\sigma\tau \mapsto \overline{M}_\sigma \overline{M_\tau^\sigma}$ where

$$\text{if } M = \begin{bmatrix} a & c \\ b & d \end{bmatrix}, \quad M^\sigma = \begin{bmatrix} \sigma(a) & \sigma(c) \\ \sigma(b) & \sigma(d) \end{bmatrix}.$$

In the case where $G = \{e, \sigma\}$ is a group of order 2 the above can be summarized by saying that there is a one-to-one correspondence between extensions of G to $L(Z)$ and equivalence classes of matrices M_σ such that $M_\sigma M_\sigma^\sigma$ is a diagonal matrix. The correspondence is given by

$$\begin{aligned} \sigma(Z) = \frac{aZ+b}{cZ+d} &\mapsto \overline{M}_\sigma \\ &= \overline{\begin{bmatrix} a & c \\ b & d \end{bmatrix}} \quad \text{where } \overline{M}_\sigma = \overline{N}_\sigma \Leftrightarrow M_\sigma = \lambda N_\sigma \text{ for some } \lambda \in L. \end{aligned}$$

The fixed field of the extension of M_σ, $L(Z)^{M_\sigma}$ is actually a generic splitting field for a quaternion algebra over K (see **[1]**, **[3]**). The associated algebra has $\{1, \theta\}$ as an L-basis with multiplication defined by $\theta^2 = a\sigma(a) + c\sigma(b)$ and the requirement $\theta f = \sigma(f)\theta$ for $f \in L$.

THEOREM 2. *Let L be a Galois extension of K with group $G = \{e, \sigma\}$ of order 2 and let Z be transcendental over L. Let M_σ and N_σ be extensions of G to L. Then $L(Z)^{M_\sigma}$ is K-isomorphic to $L(Z)^{N_\sigma}$ if and only if $M_\sigma M_\sigma^\sigma = \eta N_\sigma N_\sigma^\sigma$ where η is the norm of an element of L. In particular, $L(Z)^{M_\sigma}$ is rational over K if and only if $M_\sigma M_\sigma^\sigma$ is the norm of an element of L (identifying L^* with the diagonal matrices in* $\mathrm{GL}_2(L)$.

Proof. The above theorem can be seen as a relatively straightforward application of the fact that the map $H^1(G, \mathrm{PGL}_2(L)) \to H^2(G, L^*)$ is one-to-one [7, Theorem 1]. However, we choose to present a more constructive proof which avoids the cohomology.

Assume we have an isomorphism $f: L(Z)^{M_\sigma} \to L(Z)^{N_\sigma}$. Note that $L(Z)^{M_\sigma} \otimes_K L \cong L(Z)^{M_\sigma}[L] = L(Z)$ and that if we extend the action of σ on L to $1 \otimes \sigma$ on $L(Z)^{M_\sigma} \otimes_K L$ we get M_σ under the above identification with $L(Z)$. Extend f to $\overline{f}: L(Z)^{M_\sigma} \otimes_K L \to L(Z)^{N_\sigma} \otimes_K L$ by $\overline{f} = f \otimes 1$. Then $\overline{f}$ is an L-automorphism of $L(Z)$ over L, so $\overline{f}(Z) = (aZ + b)/(cZ + d)$ for some $a, b, c, d \in L$.

Let $B = \left[\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right]$. Then by the above discussion we must have $\overline{M_\sigma} = \overline{B^{-1} N_\sigma B^\sigma}$ in $\mathrm{PGL}_2(L)$.

Therefore, there is a $\lambda \in L$ such that $M_\sigma = \lambda B^{-1} N_\sigma B^\sigma$. Thus

$$\begin{aligned} M_\sigma M_\sigma^\sigma &= \lambda B^{-1} N_\sigma B^\sigma \sigma(\lambda)(B^\sigma)^{-1} N_\sigma^\sigma B \\ &= \lambda\sigma(\lambda) N_\sigma N_\sigma^\sigma \text{(using the fact that } N_\sigma N_\sigma^\sigma \text{ is a scalar matrix).} \end{aligned}$$

Now let $\eta = \lambda\sigma(\lambda)$.

Suppose that M_σ and N_σ correspond to extensions of σ and that

$$M_\sigma M_\sigma^\sigma = \eta N_\sigma N_\sigma^\sigma \quad \text{where } \eta = \lambda\sigma(\lambda).$$

By replacintg N_σ with λN_σ we can assume that $\eta = 1$. Suppose that we can choose a matrix A in $M_2(L)$ so that

$$B = AM_\sigma^\sigma + N_\sigma A^\sigma \text{ is invertible.}$$

Then we claim that $M_\sigma = B^{-1} N_\sigma B^\sigma$. In fact

$$\begin{aligned} N_\sigma B^\sigma &= N_\sigma A^\sigma M_\sigma + N_\sigma N_\sigma^\sigma A \\ &= N_\sigma A^\sigma M_\sigma + A N_\sigma N_\sigma^\sigma \quad \text{(because } N_\sigma N_\sigma^\sigma \in L^*) \end{aligned}$$

But $N_\sigma N_\sigma^\sigma = M_\sigma M_\sigma^\sigma$.

Note that

$$\begin{aligned}(M_\sigma M_\sigma^\sigma)(M_\sigma^\sigma M_\sigma)^{-1} &= M_\sigma M_\sigma^\sigma M_\sigma^{-1}(M_\sigma^\sigma)^{-1} \\ &= M_\sigma^{-1} M_\sigma M_\sigma^\sigma (M_\sigma^\sigma)^{-1} \quad (\text{because } M_\sigma M_\sigma^\sigma \in L^*) \\ &= I.\end{aligned}$$

Hence $M_\sigma M_\sigma^\sigma = M_\sigma^\sigma M_\sigma$.

Therefore

$$N_\sigma B^\sigma = N_\sigma A^\sigma M_\sigma + AM_\sigma^\sigma M_\sigma = (N_\sigma A^\sigma + AM_\sigma^\sigma)M_\sigma = BM_\sigma$$

and the claim is established.

But, as before, if $\overline{f}$ is the L-automorphism of $L(Z)$ corresponding to B then $M_\sigma = B^{-1}N_\sigma B^\sigma$ means that $M_\sigma = \overline{f}^{-1} \circ N_\sigma \circ \overline{f}$ and $L(Z)^{M_\sigma} \cong L(Z)^{N_\sigma}$. Therefore, it only remains to prove the following.

Lemma 1. *With M_σ, N_σ as in the theorem, there is always an A such that $B = AM_\sigma^\sigma + N_\sigma A^\sigma$ is invertible.*

Proof. We will show that, in fact, we can choose A to be of the form $A = \left[\begin{smallmatrix} x & 0 \\ 0 & y \end{smallmatrix}\right]$.

Let $M_\sigma = \left[\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right]$, $N_\sigma = \left[\begin{smallmatrix} a' & c' \\ b' & d' \end{smallmatrix}\right]$. Then

$$B = \begin{bmatrix} x\sigma(a) + a'\sigma(x) & x\sigma(c) + c'\sigma(y) \\ y\sigma(b) + b'\sigma(x) & y\sigma(d) + d'\sigma(y) \end{bmatrix}$$

$$\begin{aligned}\det B = {}& [(\det M_\sigma^\sigma)y + d'\sigma(a)\sigma(y)]x + [a'\sigma(d)y + \det N_\sigma \sigma(y)]\sigma(x) \\ & - b'\sigma(c)x\sigma(x) - c'\sigma(b)y\sigma(y).\end{aligned}$$

By the algebraic independence of 1 and σ we can choose y so that $\det M_\sigma^\sigma y + d'\sigma(a)\sigma(y) \neq 0$.

With this choice of y we get

$$\det B = \alpha x + \beta\sigma(x) + \gamma x\sigma(x) + \delta \quad \text{with } \alpha \neq 0.$$

Now choose x so that $\det B \neq 0$.

Finally, $L(Z)^{M_\sigma}$ is rational over K if and only if $L(Z)^{M_\sigma}$ is isomorphic to $L(Z)^I$ where I is the identity matrix. Thus $L(Z)^\sigma$ is rational over K if and only if $M_\sigma M_\sigma^\sigma$ is a norm.

Returning to the example, with $L = Q(W, Y)$, $K = Q(W, Y)^\alpha$ and $Z = U$, α on $Q(W, Y, U)$ corresponds to the matrix

$$N_\alpha = \begin{bmatrix} W^2 - Y^2 & -4WY \\ WY & W^2 - Y^2 \end{bmatrix} \quad \text{and}$$

$$N_\alpha N_\alpha^\alpha = \begin{bmatrix} -(W^2 + Y^2)^2 & 0 \\ 0 & -(W^2 + Y^2)^2 \end{bmatrix}.$$

Since $(W^2+Y^2)^2$ is a norm, Theorem 2.1 says that we can find a new variable Z such that $\alpha(Z) = -1/Z$.

In fact, referring to the proof of the theorem, with $N'_\alpha = N_\alpha/(W^2+Y^2)$, $M_\alpha = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$, and $A = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$ we get $M_\alpha = B^{-1}N'_\alpha B$ where

$$B = AM_\alpha^\alpha + N'_\alpha A^\alpha = \begin{bmatrix} \dfrac{W^2-Y^2}{W^2+Y^2} & \dfrac{-4WY}{W^2+Y^2}+1 \\ \dfrac{WY}{W^2+Y^2}-1 & \dfrac{W^2-Y^2}{W^2+Y^2} \end{bmatrix}$$

i.e. if

$$\begin{aligned} Z &= \frac{\left(\dfrac{W^2-Y^2}{W^2+Y^2}\right)U + \dfrac{WY}{W^2+Y^2} - 1}{\left(1 - \dfrac{4WY}{W^2+Y^2}\right)U + \dfrac{W^2-Y^2}{W^2+Y^2}} \\ &= \frac{(W^2-Y^2)U + WY - (W^2+Y^2)}{(W^2+Y^2-4WY)U + W^2 - Y^2)} \end{aligned}$$

then $\alpha(Z) = -1/Z$.

So $Q(W,Y,U)^\alpha = Q(W,Y,Z)^\alpha$ is not rational over $Q(W,Y)^\alpha$, but it is rational over Q, as can be seen by applying [**4**, Proposition 1.4] to $Q(W,Y,Z)^\alpha$. One generating transcendence basis is

$$\left\{\frac{Z^2-1}{Z}, W+Y, \frac{Z^2+1}{Z}(W-Y)\right\}.$$

Applying the theorem again to $Q(W,Y,V)^\alpha/Q(W,Y)^\alpha$ we see that $Q(W,Y,V)^\alpha$ is not a rational extension of $Q(W,Y)^\alpha$ (because W^2+Y^2 is not a norm). Thus the fixed field of α is a genus 0 extension of a pure transcendental extension in three variables over Q.

References

[1] S. A. Amitsur, *Generic splitting fields of central simple algebras*, Ann. of Math., **62** (1955), 8–43.

[2] H. W. Lenstra, *Rational functions invariant under a finite abelian group*, Invent. Math., **25** (1974), 299–325.

[3] 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.

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

[5] ———, *Multiplicative field invariants*, J. Algebra, **106** (1987), 221–238.

[6] ———, *Generic Galois extension and problems in field theory*, Advances in Math., **43** (1982), 250–283.

[7] D. D. Triantaphyllou, *Invariants of finite groups acting non-linearly on rational function fields*, J. Pure Applied Algebra, **18** (1980), 315–331.
[8] B. L. Van der Waerden, *Algebra*, Vol. 2, Frederic Unger Co., New York, 1970.

Received September 4, 1987 and in revised form, May 25,1988.

VIRGINIA COMMONWEALTH UNIVERSITY
RICHMOND, VA 23284