STABLE RATIONALITY OF CERTAIN INVARIANT FIELDS

Esther Beneish
Eastern Washington University
Department of Mathematics
Cheney, WA 99004
email: ebeneish@mail.ewu.edu

Abstract:

Let F be a field. For a finite group G, let F(G) be the purely transcendental extension of F with transcendency basis $\{x_g: g \in G\}$. Let $F(G)^G$ denote the fixed field of F(G) under the action of G. Let w be a primitive (p-1)st root of 1, and let I be the ideal (p, w-a) in Z[w] where a is a primitive (p-1)st root of 1 mod p. We show that if G be the semi-direct product of a cyclic group of order p by a cyclic group of order prime to p, if I is principal, and if F contains a primitive pth root of 1, then $F(G)^G$ is stably rational over F. It is not known whether the set of primes p for which I is principal is finite or infinite. We also show that if p is an odd prime and G is a non abelian group of order p^3, then $F(G)^G$ is stably rational over F provided that F contains a primitive p^2-th root of 1.[1]

[1] 1991 Mathematics Subject Classification. Primary 13A50, 20C10.

Introduction:

Let F be a field, let G be a finite group G, and let F(G) denote the purely transcendental extension of F with transcendency basis $\{x_g : g \quad G\}$. Let $F(G)^G$ denote the fixed field of F(G) under the action of G. The question asked by Emmy Noether was: For which F and G is $F(G)^G$ rational over F? This question has been answered in various cases. If G is abelian of exponent n and F contains a primitive nth root of 1, then Fischer, [F], showed that $F(G)^G$ is rational over F. In [SR], Swan constructed the first example for which $F(G)^G$ is not rational over F, namely when G is the cyclic group of order 47 and F is the field of rational numbers. Endo, Miyata, Lenstra and Voskresenskii have classified the abelian groups G and fields F for which $F(G)^G$ is rational over F, [EM1], [L], [V]. In [SD], Saltman constructs p-groups G, such that $F(G)^G$ is not rational over F, where F is an algebraically closed field of characteristic prime to p. In [H], Hajja has shown that if F is an algebraically closed field of characteristic 0, and if G has an abelian normal subgroup N such that G/N is cyclic of order n and the nth cyclotomic field has class number 0, then $F(G)^G$ is rational over F.

Let p be a prime, and let F be a field. Let G be the semi-direct product of a cyclic group of order p by a cyclic group of order prime to p. Let w be a primitive (p-1)st root of 1, and let I be the ideal (p, w-a) in Z[w] where a is a primitive (p-1)st root of 1 mod p. We show that if I is principal, and if F contains a primitive pth root of 1, then $F(G)^G$ is stably rational over F, Theorem 1.4. It is not known whether the set of primes p for which I is principal is finite or infinite, however it was proved in [L, Corollary 7.6] that it has Dirichlet density 0. We also show that if p is an odd prime and G is a non abelian group of order p^3, then $F(G)^G$ is stably rational over F, provided that F contains a primitive p^2-th root of 1, Theorem 2.3. Some of these groups arose in our study of the stable rationality of the center of the division ring of generic matrices.

Section 1:

Let G be a finite group and let M be a ZG-lattice. We will denote by F(M) the quotient field of the group algebra, F[M], of the abelian group M written multiplicatively. Under this notation F(G) is F(ZG).

Definition:

Let G be a finite group. A ZG-lattice M is said to be permutation if there exists a Z-basis for M which is permuted by G. A ZG-module is said to be invertible if it is a direct summand of a permutation module. A ZG-module M is said to be stably permutation, if there exist permutation modules P and P’ such that M P P’.

Definition:

Let L and K be fields on which a finite group G acts. We say that L and K are isomorphic (stably isomorphic) as G-fields if they are isomorphic (stably isomorphic) and the isomorphism respect their G-actions.

Notation:

Throughout this article we will use the following notation unless otherwise specified.

- F will be a field.
- w = primitive (p-1)st root of 1.
- a = primitive (p-1)st root of 1 mod p.
- I = ideal (p, w-a) in Z[w].
- S = set of primes p for which I is principal.
- For any finite group G and any ZG-lattice M, $\hat{M}$ will denote the p-adic completion of M, and for any prime q, M_q will denote the localization of M at q.
- H = cyclic group of order p.
- C = cyclic group of order prime to p.
- H will be generated by h and C by c.
- G = $H \rtimes C$ will be the semi-direct product of H by C.

The following lemma has been proved in the literature in different forms, we include it for the reader’s convenience.

Lemma 1.1:

Let G be a finite group, and let V be a finitely generated G-faithful FG-module. Let $F_+(V)$ denote the function field of the symmetric algebra of V. Then for any G-faithful ZG-permutation lattice P, $F_+(V)$ and F(P) are stably isomorphic as G-fields.

Proof:

Let V_1 be the vector space FP=F $_Z$P. Then F(P) $F_+(V_1)$. Set L = $F_+(V)$ and L_1= $F_+(V_1)$. Then $F_+(V \quad V_1)$ $L_+(LV_1)$ $L_{1+}(L_1V)$. By Speizer's Lemma, see e.g. [W], LV_1^G contains an L-basis for LV_1, say $\{y_1,\ldots, y_r\}$, and L_1V^G contains an L_1-basis for L_1V, say $\{z_1,\ldots, z_t\}$. Thus

$$F_+(V \quad V_1) \quad L(y_1,\ldots, y_r) \quad L_1(z_1,\ldots, z_t),$$

hence

$$F_+(V)(y_1,\ldots, y_r) \quad F(P)(z_1,\ldots, z_t)$$

and so F(P) and $F_+(V)$ are stably isomorphic.

Remark:

Let G = H≻◁C be as defined above, and assume that C=Aut(H) so its order is p-1. Since ZG/H ZC $Z[x]/(x^{p-1}-1)$ as ZG-lattices, the decomposition of $\hat{Z}$G/H into indecomposables is given by

$$\hat{Z}G/H \quad {}_{k=1,\ldots,p-1}Z[x]/(x-\theta^k) \quad {}_{k=1,\ldots,p-1}Z_k$$

where θ is a primitive (p-1)st root of 1 in $\hat{Z}$ which is congruent to a mod p, and Z_k is the trivial $\hat{Z}$G-module of $\hat{Z}$-rank 1 with trivial H action, and such that $c1=\theta^k$. We set $X_k=Z_k/pZ_k$, so X_{p-1}= X the trivial $\hat{Z}$G-module of p elements.

We also have ZG/C ZH where the H-action on ZH is the obvious one and the C-action is given by $ch = h^a$. We will denote by A and A' the ZG-lattices ZH(h-1) and $ZH(h-1)^2$ respectively.

Proposition 1.2:

Let $G = H \rtimes C$ be the semi-direct product of a group H of order p by a cyclic group C equal to Aut(H). The ZG-lattice A is ZC-free, and if p S, then the ZG-lattice A' is stably permutation as a ZC-lattice.

Proof:

As above we let h generate H and c generate C. A Z-basis for A = ZH(h-1) is $\{h^i - 1: i=1,\dots, p-1\}$, and we have $c(h^i-1) = h^{ai}-1$. Thus C permutes the basis elements, and there is a ZC-isomorphism from A to ZC given by $(h-1) \to c$. Now there exists a ZG-exact sequence

$$0 \to A' \to A \to X_1 \to 0$$

with the map $A = ZH(h-1) \to X_1$ given by $h^i(h-1) \to 1$.

Since X_1 is of order p, its localization of at any prime $q \neq p$ is 0, thus $A'_q \quad A_q$. Therefore A' is ZC-cohomologically trivial. By [BK, Theorem 8.10, Chapter VI], this implies that A' is ZC-projective.

Let I be the ideal (p, w-a) in Z[w], as defined. Since $Z[w] \quad Z[x]/(\varphi(x))$ where $\varphi(x)$ is the (p-1)st cyclotomic polynomial, there exist a ring map $ZC \to Z[w]$ given by $1_{ZC} \to 1_{Z[w]}$. Thus Z[w] is a ZC-module where c acts by multiplication by w. Futhermore the map of ZC-modules $Z[w] \to X_1$ has kernel I. We have the following commutative diagram of ZC-modules.

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \uparrow & & \uparrow & & \\
0 & \to & A' & \to & A & \to & X_1 & \to & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \to & A' & \to & M & \to & Z[w] & \to & 0 \\
 & & & & \uparrow & & \uparrow & & \\
 & & & & I & & I & & \\
 & & & & \uparrow & & \uparrow & & \\
 & & & & 0 & & 0 & &
\end{array}$$

where M is the pullback of the maps $A \to X_1$ and $Z[w] \to X_1$.

For a ZC-lattice E, let E* = $Hom_Z(E,Z)$ be its dual. Since A' is ZC-projective, so is A'*, therefore M* A'* Z[w]*, and we have

$$M \quad A' \quad Z[w] \quad A \quad I \quad ZC \quad I.$$

If p S, I is principal, and therefore it is isomorphic to Z[w] as a ZC-module. By [EM3, Theorem 4.2], this implies that A' is stably permutation as a ZC-lattice.

Theorem 1.3:
Let p be a prime in S. Let G = $H \succ\!\lhd C'$ be the semi-direct product of a group H of order p by a cyclic group C' contained in Aut(H). Then $F(G)^G$ is stably rational over F provided that F contains a primitive pth root of 1.

Proof:
Let C = Aut(H), so C is of order p-1. Consider the ZC-exact sequence of Proposition 1.2, namely

$$0 \to A' \to A \to X_1 \to 0.$$

Restricting to C, and using the fact that A ZC by Proposition 1.2, we get the ZC-sequence

$$0 \to A' \to ZC \to X_1 \to 0.$$

Let F* be the multiplicatice group of F, and let Y = $Hom(X_1, F^*)$ be the character group of X_1. By Galois theory there is a linear action of $Y \succ\!\lhd C$ on F(ZC) such that

$$F(ZC)^{Y \succ\!\lhd C} \quad F(A')^C$$

and for any subgroup K of C

$$F(ZC)^{Y \succ\!\lhd K} \quad F(A')^K.$$

In particular

$$F(ZC)^{Y \succ\!\lhd C'} \quad F(A')^{C'}$$

Now as a group $G \quad Y \rtimes C'$. Let V the FG-module with F-basis $\{x_1,\ldots,x_{p-1}\}$ where G acts on x_i as on c^i for i=1,…,p-1. Then V is G-faithful and $F(ZC) \quad F_+(V)$. By Lemma 1.1, F(G) is G-stably isomorphic to F(ZC), hence $F(G)^G$ is stably isomorphic to $F(A')^{C'}$. Since A' is ZC'-stably permutation by Proposition 1.2, F(A') is stably isomorphic to F(ZC) as a C'-field by [B, Lemma 2.1]. The result now follows by [F] since C' is abelian.

Theorem 1.4:

Let G be the semi-direct product of a group H of order p, by a group C of order prime to p. Let w be a primitive (p-1)st root of 1, and let I be the ideal (p, w-a) in Z[w], where a is a primitive (p-1)st root of 1 mod p. If I is principal then $F(G)^G$ is stably rational over F provided that F contains a primitive pth root of 1.

Proof:

Let $G = H \rtimes C$. Let $C' = Ker(C \rightarrow Aut(H))$, then C' is normal in G. By Lemma 1.1, F(G) is stably isomorphic as a G-field to $F_+(V)$ for any faithful FG-lattice V. Let

$$V = F \quad {}_{z}ZG/C \quad W$$

where W is a one dimensional faithful representation of C, with trivial H-action. Then

$$F_+(V)^G = ((F_+(V)^{C'})^{G/C'}.$$

It is immediate that $F_+(V)^{C'}$ is stably isomorphic to F(ZG/C) as a G/C'-field. Thus $F(G)^G$ is stably isomorphic to $F(ZG/C)^{G/C'}$. But $G/C' \quad H \rtimes K$, where K = C/C' is a subgroup of Aut(H). The result then follows by Theorem 1.3.

Section 2:

Let p be an odd prime. In this section we show that if G is a non-abelian group of order p^3, then $F(G)^G$ is stably rational over F. By [G, Theorem 5.1, Chapter 5] there exists, up to isomorphism, two groups satisfying these conditions. They are the semi-direct products of a group of order p^2 by a group of order p. The group of order p^2 is cyclic in one case and p-elementary in the other.

Proposition 2.1:

Let H be a cyclic group of order p, with generator h. There exists an exact sequence

$$0 \rightarrow ZH(h\text{-}1)^2 \quad Z \rightarrow ZH \rightarrow D \rightarrow 0$$

where D is a ZH-module of order p^2 and exponent p.

Proof:

Let X denote the trivial ZH-module Z/pZ. We have the following exact sequence of ZH-modules

$$0 \rightarrow ZH(h\text{-}1) \quad Z \rightarrow ZH \rightarrow X \rightarrow 0$$

where the map ZH(h-1)   Z → ZH is inclusion of ZH(h-1) and sends 1_Z to the norm of H, and

$$0 \rightarrow ZH(h\text{-}1)^2 \rightarrow ZH(h\text{-}1) \rightarrow X \rightarrow 0$$

where the map $ZH(h\text{-}1)^2 \rightarrow ZH(h\text{-}1)$ is inclusion.

Combining these 2 sequences we get

$$0 \rightarrow ZH(h\text{-}1)^2 \quad Z \rightarrow ZH \rightarrow D \rightarrow 0 \qquad (3)$$

where D is given by the extension

$$0 \rightarrow X \rightarrow D \rightarrow X \rightarrow 0.$$

So D is of order p^2. We will prove that D has exponent p.

The map $ZH(h\text{-}1)^2$ Z → ZH in sequence (3) is inclusion on $ZH(h\text{-}1)^2$ and sends 1_Z to the norm of H. The ZH-module D   ZH/($ZH(h\text{-}1)^2$ Z) is generated by the classes of $\overline{1}$ and $\overline{h}$ of 1 and h, with $\overline{h}^2 = 2\overline{h} - \overline{1}$. Let N be the norm of H. Then

$$\sum_{i=1}^{p-1} ih^i(h-1) + N = \sum_{i=1}^{p-1} ih^{i+1} - \sum_{i=1}^{p-1} ih^i + \sum_{i=1}^{p} h^i =$$

$$\sum_{j=2}^{p} (j-1)h^j - \sum_{j=1}^{p-1} jh^j + \sum_{j=1}^{p} h^j =$$

$$\sum_{j=2}^{p-1} [(j-1)h^j - jh^j + h^j] + (p-1)1_H - h + h + 1_H = p$$

and we have $p(h-1) = \sum_{i=1}^{p-1} ih_i(h-1)^2$. Therefore $p\overline{1} = p\overline{h}$, and since $\overline{N} = 0$, we get $p^2\overline{1} = p^2\overline{h} = 0$. So the exponent of D is either p or p^2. It follows directly from $\overline{h}^2 = 2\overline{h} - \overline{1}$, that for k=1,…,p-1, $\overline{h}^k = k\overline{h} - (k-1)\overline{1}$. Therefore we have

$$0 = \overline{N} = \sum_{k=1}^{p-1}(k\overline{h} - (k-1)\overline{1}) + \overline{1}$$

equivalently

$$(\sum_{k=1}^{p-1} k)\overline{h} = \sum_{k=1}^{p-1} k\overline{1} - (\sum_{k=1}^{p-1}\overline{1}) - \overline{1}$$

$$(1/2)p(p-1)\overline{h} = (1/2)p(p-1)\overline{1} - p\overline{1}$$

$$(1/2)p(p-1)\overline{h} = \_p(p-3)\overline{1}$$

Since $p\overline{1} = p\overline{h}$ and $p^2\overline{1} = p^2\overline{h} = 0$, we get $2p\overline{h} = 0$ thus $p\overline{h} = p\overline{1} = 0$. Thus D is generated by

$\overline{1}$ and $\overline{h}$ with $p\overline{1} = p\overline{h} = 0$, and hence it is of exponent p. Clearly the H-action on D is not trivial.

Notation:

For all n in Z, for any finite group G and ZG-module M, $H^n(G,M)$ will denote the nth Tate cohomology group of G with coefficients in M.

Proposition 2.2:

Let G be a group of order p^3 having a cyclic subgroup K' of index p. Let H=G/K', and let K=Hom(K',F*). Then there exists a ZH-exact sequence

$$0 \to ZH \to ZH \to K \to 0.$$

Proof:

By [G, Theorem 5.1, Chapter 5] there exists, up to isomorphism, a unique group of order p^3 having a cyclic subgroup of index p. It is the semi-direct product of this cyclic group of order p^2 by a group of order p. Therefore K   K' as ZH-modules, and G   K' $\rtimes$H. Let X be the trivial ZH-module with p elements. There is a ZH-exact sequence

$$0 \to ZH \to ZH(h-1) \quad Z \to X \to 0 \qquad (1)$$

where the map ZH $\to$ ZH(h-1)   Z sends 1 to (h-1) + 1_Z. It is easily checked that the the map is injective and that its cokernel is X.

Now consider the ZH-exact sequence

$$0 \to ZH(h-1) \quad Z \to ZH \to X \to 0 \qquad (2)$$

where the map ZH(h-1)   Z $\to$ ZH is inclusion on ZH(h-1) and sends 1_Z to the norm of H which we denote by N. Combining these two sequences we get

$$0 \to ZH \to ZH \to T \to 0 \qquad (3)$$

where T is given by the following ZH-exact sequence

$$0 \to X \to T \to X \to 0 \qquad (4)$$

We will show that T   K as ZH-modules.

We know that T is of order p^2, and that there is a map from H to Aut(T). Again, by [G, Theorem 5.1, Chapter 5], there exists, up to isomorphism, two non abelian groups of order p^3, one of which is of exponent p. Therefore there exists, up to isomorphism, two non-trivial ZH-modules of order p^2, one of which is the group D of Proposition 2.1. So it suffices to show that the map form H to Aut(T) is non trivial, and that T is not isomorphic to K.

We first show that $T^H \neq T$ which will imply that the map H$\to$Aut(T) is not trivial.

From the ZH-sequence

$$0 \longrightarrow Z \xrightarrow{\;p\;} Z \longrightarrow X \longrightarrow 0$$

we get that $H^1(H,X) = Z/pZ$. From sequence (4) we get

$$0 \to X \to T^H \to X \to H^1(H,X) \to H^1(H,T) \to \dots$$

Now T is cohomologically trivial by sequence (3), so $T^H = X \neq T$.

Consider the ZH-sequence of Proposition 2.1, namely

$$0 \to ZH(h-1)^2 \quad Z \to ZH \to D \to 0.$$

We have $H^{-1}(H,D) = H^0(ZH(h-1)^2 \quad Z) = Z/pZ$. Therefore D is not cohomologically trivial and hence cannot be isomorphic to K. Thus T   K, which proves the result.

Theorem 2.3:

Let p be an odd prime. Let G be an abelian group of order p^3, and let F be a field containing a primitive p^2-th root of 1. Then $F(G)^G$ is stably rational over F.

Proof:

Let H, K and D be as in Propositions 2.1 and 2.2. Let K' = Hom(K, F*) and D' = Hom(D, F*) be the character groups of S and D respectively. By [G, Theorem 5.1, Chapter 5] G is isomorphic to either $K' \succ\!\lhd H$ or to $D' \succ\!\lhd H$.

<u>Case 1:</u> G $K' \succ\!\lhd H$.

By Proposition 2.2, we have a ZH-exact sequence

$$0 \to ZH \to ZH \to K \to 0.$$

By Galois theory $F(ZH)^G$ $F(ZH)^H$, which is rational over F, by [F]. Therefore $F(ZH)^G$ is stably rational over F. By Lemma 1.1, $F(G)^G$ is stably isomorphic to $F(ZH)^G$ which proves the result.

<u>Case 2:</u> G $D' \succ\!\lhd H$.

By Proposition 2.1 there exists a ZH-exact sequence

$$0 \to ZH(h-1)^2 \quad Z \to ZH \to D \to 0.$$

By Galois theory $F(ZH(h-1)^2 \quad Z)^H$ $F(ZH)^G$. Now ZH(h-1) and $ZH(h-1)^2$ are isomorphic as ZH-modules and the isomorphism is given by

$$h^i(h-1) \to h^i(h-1)^2.$$

Thus $F(ZH(h-1)^2 \quad Z)^H$ $F(ZH(h-1) \quad Z)^H$. We have a ZH-exact sequence

$$0 \to ZH(h-1) \to ZH \to Z \to 0,$$

and by [B, Lemma 1.2] F(ZH(h-1)   Z) and F(ZH) are isomorphic as H-fields. Therefore $F(ZH)^G$ and $F(ZH)^H$ are stably isomorphic and the argument now is the same as in Case 1.

References

[B] E. Beneish, Induction theorems on the center of the ring of generic matrices, Trans. of the AMS, 350(1998), no. 9, 3571-3585.

[BK] K Brown, Cohomology of groups, Springer-Verlag, New York,1982.

[CR] Curtis and Reiner, Methods of Representation Theory, vol 1, Wiley, New York, 1981.

[EM1] S. Endo and T. Miyata, Invariants of finite abelian groups. J. Math. Soc. Japan 25, (1973), 7-26.

[EM2] S. Endo and T. Miyata, On the classification of the function fields of algebraic tori, Nagoya Math. J. 56 (1974), 85-104.

[EM3] S. Endo and T. Miyata, Quasi-permutation modules over finite groups II, J. Math. Soc. Japan 26, (1974), 698-713.

[F] E. Fischer, Die Isomorphie der Invariantenkorper der endlichen Abel'schen Gruppen linearen Transformationen. Nachr. Konigl. Ges. Wiss. Gottingen (1915), pp 77-80.

[G] D. Gorenstein, Finite Groups, Harper & Row, 1968.

[H] M. Hajja, Rational invariants of meta-abelian groups of linear automorphisms, J. of Algebra 80, (1983), 295-305.

[L] H. W. Lenstra, Rational functions invariant under a finite abelian group, Inventiones Mathematica 25 (1974), 299-325.

[SD] D. Saltman, Noether's problem over an algebraically closed field, Invent. Math. 77, (1984) 71-84.

[SR] R. Swan, Invariant rational functions and a problem of Steenrod, Invent. Math. 7 (1969), 148-158.

[V] V.E. Voskresensskii, Rationality of certain algebraic tori (Russian). Izv. Akad. Nauk SSSR Ser. Mat. 35, 1037-1046 (1971). English translation: Math USSR-Izv. 5, (1971), 1049-1056.

[W] D.J. Winter, The structure of fields, Springer-Verlag, 1974.