ABELIAN GALOIS GROUPS

CARL C. FAITH

The question of the existence of noninner, nonouter Abelian Galois groups of noncommutative rings seems not to have been considered previously. Amitsur [1] may have come closest when he constructed noninner, nonouter cyclic division ring extensions. Although these extensions are finite dimensional division ring extensions of Galois subrings corresponding to cyclic groups of automorphisms, nevertheless, as will be shown below, their Galois groups need not be Abelian.

The question is made more critical by results obtained below which imply for any finite dimensional division algebra, and, furthermore, for any full matrix ring over it having center $\neq GF(4)$, that any Abelian Galois group is inner or outer. Curiously enough Galois groups of the required kind do exist for some matrix rings over $GF(4)$. Affirmative results are obtained also for certain infinite dimensional division algebras first constructed by Köthe [3], and their associated matrix rings. For these rings a general procedure for obtaining noninner, nonouter Abelian Galois groups is discussed.

1. **Abelian inner groups.** Let K be a ring with identity 1. For any subring S of K with $1\in S$, S^* denotes the group of units in S. For any $x\in K^*$, I_x is the inner automorphism of K effected by x. If F is a Galois subring of K, then $I(G)$ is the subgroup of inner automorphisms of the Galois group $G=G(K/F)$ of the extension of K/F. Clearly $I(G)$ is isomorphic to A^*/C^*, where A and C denote the centralizers in K of F and K respectively. In this section some conditions on A are found under which the commutativity of A^*/C^* implies that of A.

LEMMA 1. *Let K be a central algebra, with identity* 1, *over a field C, and let A be a subalgebra of K, with $1\in A$, and with radical $R\neq\{0\}$. Then any automorphism σ of K mapping A onto itself and commuting with all inner automorphisms of K effected by elements of A^* leaves invariant the elements of A^*, and the elements of R as well.*

PROOF. Let $x=1+r$, $r\in R$, $r\neq 0$. Since $I_x\sigma=\sigma I_{x\sigma}$, σ commutes with I_x if and only if $x\sigma=\alpha x$ with α in the center C of K. Thus $1+r\sigma=\alpha+\alpha r$, $\alpha-1=\alpha r-r\sigma\in R$, whence $\alpha=1$, $r\sigma=r$. Now let $y\in A^*$, and $r\in R$, $r\neq 0$. Then $y\sigma=\beta y$, $(y+r)\sigma=\gamma(y+r)$ with $\beta,\gamma\in C$, so that $(\beta-\gamma)y=(\gamma-1)r\in R$. Thus $\beta=\gamma=1$; $y\sigma=y$ as desired.

Presented to the Society, August 27, 1958; received by the editors February 20, 1958 and, in revised form, October 13, 1958 and January 12, 1959.

(I) DEFINITION. *Throughout the remainder of this article A will always denote an algebra over a field C, having identity* 1, *with radical R such that $\overline{A}=A-R$ is a ring with minimum condition.*

It is easily seen, if A is simple, that A^* is Abelian whenever A^*/C^* is. This is the known case of the next result.

PROPOSITION 1. *A^*/C^* is Abelian if and only if A^* is.*

PROOF. By Lemma 1, if $\sigma=I_y$, $y\in A^*$, and if $R\neq\{0\}$, then $x\sigma=y^{-1}xy=x$ for all x, $y\in A^*$, that is, A^* is Abelian in this case. Now let $R=\{0\}$ so that A is a direct sum of simple ideals A_i, $i=1, 2, \cdots, t$, which are total matrix rings over division rings. In order to prove the proposition it suffices to show, in case A^* is noncommutative, that there exist x, $y\in A^*$ such that $xyx^{-1}y^{-1}\notin C^*$. Let e_i be the unity, and Z_i the center of A_i, $i=1, 2, \cdots, t$. If A is noncommutative then $Z_i\neq A_i$ for some i, say $Z_1\neq A_1$. Since the group of units of A_1 modulo the group of units in Z_1 is noncommutative, this being the well known case of the proposition, then there exist regular elements x_1, y_1 of A_1 such that $x_1y_1x_1^*y_1^*\notin Z_1$, where x_1^*, $y_1^*\in A_1$, and $x_1x_1^*=y_1y_1^*=e_1$. Then $xyx^{-1}y^{-1}\notin C^*$ where $x=x_1+e_2+\cdots+e_t$ and $y=y_1+e_2+\cdots+e_t$.

The proof of Proposition 1 reveals that the commutativity of A^*/C^* implies that of A when $R=\{0\}$. Proposition 1 shows that this implication also holds when $R\neq\{0\}$ if only A^* generates A (in the ring sense, or in the additive group sense). Sufficient conditions for this have been developed by Shoda [4]. For example, $\overline{A}$ simple, or $C\neq GF(2)$. This produces the next lemma.

LEMMA 2. *Commutativity of A^*/C^* and that of A are equivalent conditions provided any of the following conditions hold:*

(1) *$\overline{A}=A-R$ is simple,*

(2) *$C\neq GF(2)$,*

(3) *$R=\{0\}$.*

The following example shows that in a sense Lemma 2 is the best possible result in this direction. Let A be the algebra of 6 elements over $C=GF(2)$ having a basis consisting of the three elements e_1, e_2, r, and having the table:

	e_1	e_2	r
e_1	e_1	0	r
e_2	0	e_2	0
r	0	r	0

Clearly A is noncommutative, with $1=e_1+e_2$, and with radical

$R=\{0, r\}$. Furthermore $\overline{A}\cong C\oplus C$ is nonsimple, but $A^*=\{1, 1+r\}$ is Abelian.

2. **Abelian groups which are inner or outer.** In this section conditions on a ring K will be noted which imply that any Abelian Galois group of K must be inner or outer.

(II) DEFINITION. *Throughout this section K will denote a ring whose center C is a field, and F will be a Galois subring whose centralizer in K is A (cf. Definition* I), *and whose Galois group $G(K/F)$ is Abelian but not outer.*

Now let σ be an automorphism of K, and let I_x be any nontrivial inner automorphism which commutes with σ, and moreover, assume $x-1$ is regular too. Then, as in the proof of Lemma 1, $x\sigma=\alpha x$, $(x-1)\sigma=\beta(x-1)$, $\alpha, \beta\in C$, so that $(\alpha-\beta)x=\beta-1\in C$, that is, $\alpha=\beta=1$. Thus $x\sigma=x$. This computation establishes the next lemma.

LEMMA 3. *Let Q be a Galois subring of K with Abelian Galois group. Let x and $x-1$ be regular elements of the centralizer of Q in K. Then $x\notin C$ implies that $x\in Q$.*

PROPOSITION 2. *If $\overline{A}$ is simple, or if $C\neq GF(2)$ when A is nonsemisimple and $\overline{A}$ is nonsimple, or if $C\neq GF(k)$, $k=2, 3, 4$, when A is semisimple and nonsimple, then $A\subseteq F$.*

PROOF. Assume $\overline{A}$ is simple. If $R=\{0\}$ then A is a commutative simple algebra, that is, A is a field. Consequently A is generated by $\{x\in A^* \mid x\notin C,\ x-1\in A^*\}$. By Lemma 3, $A\subseteq F$ in this case. If $R\neq\{0\}$, then $A^*\subseteq F$ by Lemma 1. By Shoda's [4, Hilfssatz 5] A^* generates A, so that $A\subseteq F$. The same argument shows, when $R\neq\{0\}$ that $A\subseteq F$ whenever A^* generates A, e.g., when $C\neq GF(2)$.

We have reached the point in the proof of Proposition 2 where one may assume that $C\neq GF(k)$, $k=2, 3, 4$, and, moreover, that A is semisimple but not simple. Then, as was seen in the preceding section, A is commutative as well. Thus one may write A as a direct sum of fields A_i, with identities e_i, $i=1, \cdots, t$, $t\geqq 2$. Any automorphism σ of K/F induces an automorphism in A, and this simply permutes the e_i, $i=1, \cdots, t$. For any $a\in A$ set $a'=a\sigma$. We first show that $e_i=e_i'$, $i=1, \cdots, t$. Let $\alpha\in C$, $\alpha\notin\{0, 1\}$. Since C contains at least 5 elements, one can choose $\beta\in C$, $\beta\notin\{0, 1, \alpha, \alpha'\}$. Suppose $e_1'\neq e_1$, say $e_1'=e_2$, and let

$$x = \alpha e_1 + \beta e_2 + \cdots + \beta e_t.$$

Then

$$x' = \beta' e_1 + \alpha' e_2 + \cdots + \beta' e_t' \neq x,$$

contrary to Lemma 3 which states, since x and $x-1$ are both regular, and $x \notin C$, that $x \in F$. Hence $e_i' = e_i$ so that σ maps each A_i onto itself, $(ae_i)' = a'e_i \in A_i$, $i=1, \cdots, t$, for all $a \in A$. I wish to show that $a' = a$ for all $a \in A$. If $a \neq a'$, then $a'e_i \neq ae_i$ for some i, say $a'e_1 \neq ae_1$. Then $ae_1 \notin \{0, e_1\}$. Choose $b \in A$ such that $be_i \notin \{0, e_i\}$, $i=2, \cdots, t$, and such that $be_1 \neq ae_1$. Then as before, if $x = ae_1 + be_2 + \cdots + be_t$, then $x' \neq x$, even though x and $x-1$ are both regular, and $x \notin C$. This contradiction to Lemma 3 completes the proof.

THEOREM 1. *An Abelian Galois group of a finite dimensional simple central algebra over a field* $\neq GF(4)$ *is either inner or outer.*

PROOF. Let $G(K/Q)$ be an Abelian Galois group of K which is not outer. Clearly the centralizer of Q in K is a ring with minimum condition. Denote this ring by A. When $C = GF(2)$, or $C = GF(3)$, then $C \subseteq Q$. For all other possibilities for C, since $C = GF(4)$ is ruled out by hypothesis, Proposition 2 provides the stronger inclusion $A \subseteq Q$. Thus in all cases $G(K/Q) \subseteq G(K/C)$ which is known to be inner. Q.E.D.

If K is a division algebra, then the centralizer A of Q in K is also. Then $A \subseteq Q$ follows from Proposition 2, and, hence, the proof above yields the

COROLLARY. *An Abelian Galois group of a finite dimensional division algebra is either inner or outer.*

3. **A noninner, nonouter Abelian Galois group.** Let K be the ring of all $n \times n$ matrices, $n > 1$, over the field C. Then $K = P_n \otimes_P C$, where P denotes the prime subfield of C. Every automorphism σ of K has the form $\sigma = \rho I_\lambda$, where $\rho \in G(K/P_n)$ and $I_\lambda \in G(K/C)$, and $G(K/P_n)$ is outer, $G(K/C) \cong G(P_n/P)$. Now let $C = GF(4) = \{0, 1, \alpha, \beta\}$, and let $n=2$. Assume σ is not inner. Then $\alpha\rho = \beta$, and the group G generated by ρ and I_g is Abelian, and is a Galois group, where

$$g = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

The Galois subring $F = F(G)$ consists of all matrices of the form

$$\left\{ \begin{pmatrix} (u+v) & u \\ u & v \end{pmatrix} u, v \quad \in P \right\},$$

and the centralizer A of F in K consists of all matrices of the same form only with coefficients ranging over C, that is $A = F \otimes_P C$. Now A is a commutative, semisimple algebra over C with a two-element basis $e_1 = \alpha + g$, $e_2 = \beta + g$, and $e_i^2 = e_i$, $e_i e_j = 0$, $i \neq j$, $i = 1, 2$. Since

$G(K/F)$ is neither inner nor outer, it remains to show that this group is Abelian. To do this it suffices to show that ρ commutes with every I_λ, $\lambda \in A^*$. Let $\lambda = ae_1 + be_2$, with a, $b \in C$, $ab \neq 0$. Clearly $e_i\rho = e_j$, $i \neq j$, $i = 1$, 2, so that $\lambda\rho = (b\rho)e_1 + (a\rho)e_2 = b^2e_1 + a^2e_2$. If $a = b$, then $\lambda\rho = a\lambda$, and if $a \neq b$, then $\lambda\rho = \lambda$. Thus in all cases ρ commutes with I_λ, and $G(K/F)$ is a noninner, nonouter Abelian Galois group.

Perhaps it is worth remarking that if $G(K/F)$ is a noninner, nonouter Abelian Galois group of a finite dimensional simple central algebra K, then as Theorem 1 shows, the center C is $GF(4)$, and, moreover, by Proposition 2 and Lemma 2, the centralizer A of F is semisimple, nonsimple, and commutative. These facts are all included in the example of this section.

4. Construction of noninner, nonouter Abelian Galois groups. The example of §3 still leaves open the question of the existence of noninner, nonouter Abelian Galois groups of division rings. The results of §2 show, barring exceptional cases of the kind in §3, when K is simple, and in all cases when K is a division ring, that in order to construct Galois groups of the required kind for a central simple algebra K the following two conditions are necessary:

(1) K is infinite dimensional.

(2) $G(K/C)$ is not inner.

The existence of certain simple algebras (with minimum condition) satisfying both (1) and (2) is assured by the results of Köthe [**3**]. In this section the construction of noninner, nonouter Abelian Galois groups for certain K is reduced to that of nontrivial finite Abelian outer subgroups of $G(K/C)$.

If H is any group of automorphisms of K, then $T(H)$ will signify the subring generated by the set $\{\lambda \in K^* \mid I_\lambda \in H\}$. Clearly $T(H)$ is always a subalgebra of K. If S is any subring of K containing the identity of K, then $J(S)$ is the group consisting of all I_λ such that $\lambda \in S^*$. In case S is a subalgebra generated by S^*, for example, when S is a finite dimensional simple subalgebra, then $T(J(S)) = S$. Finally we recall that $I(H) = \{I_\lambda \in H\}$.

Now let G be an Abelian outer subgroup of $G(K/C)$, and let T be any subfield of K satisfying $\Delta = F(G) \supseteq T \supseteq C$, where $F(G)$ denotes the Galois subring of K corresponding to G. Setting $J = J(T)$, it is clear that $H = GJ$ is Abelian. In fact $H = G \otimes J$. When $G \neq (e)$ and $T \neq C$, then H is noninner and nonouter as well. Conditions of Nakayama [**4**] which imply that H is indeed a Galois group are now recalled.

PROPOSITION A. *Let K be a simple central algebra with mininum condition and identity, and let G be an Abelian outer subgroup of $G(K/C)$ of*

finite order $n>1$. Let T be any subfield of Δ, the Galois subring corresponding to G, such that T contains C, and has finite degree $d>1$ over C. Set $J=J(T)$. Then $H=GJ$ is a noninner, nonouter Abelian Galois group.

PROOF. Since $I(G)=(e)$, it is clear that $I(H)=J$, so that (a) $(H: I(H))=(G:(e))=n<\infty$. Furthermore, (b) $T(H)=T$ is a simple subalgebra of finite dimensions; (c) $J(T(H))=J\subseteq H$, so that H is *complete* in the sense of Nakayama. A group H satisfying (a)-(c), a *regular* group in Nakayama's sense, is a Galois group according to [**4**, Theorem 1]. This completes the proof.

PROPOSITION B. *Let K be as in the first sentence of Proposition* A. *Then K possesses a noninner, nonouter Abelian Galois group provided only that Δ, the Galois subring corresponding to G, is an algebraic subalgebra, or not a division algebra.*

PROOF. By Nakayama's Galois theory, Δ is a simple ring with minimum condition, and $[K:\Delta]=n$. Since $G(K/C)$ is not inner, evidently $\Delta\neq C$. Now Δ is the Kronecker product $\Delta=D\otimes_C C_q$, where C_q is a matrix ring of order q over C, and D is a division ring satisfying $\Delta\supseteq D\supseteq C$. If $q>1$, or if D is algebraic over C, one can always choose a subfield T of Δ having finite degree $d>1$ over C in accordance with the proposition above. This completes the proof.

In [**3**] (quoted in [**2**, p. 4]) Köthe constructed for a certain algebraic division algebra an outer automorphism S, of period 2, having the identity action on the center. In view of Proposition B one now knows that there exists an (infinite dimensional) division algebra K with a noninner, nonouter Abelian Galois group H. By considering the ring of matrices $Q=K_q$, $q>1$, and extending the group H of K to $Q=K\otimes_C C_q$ in the usual way (H having the identity action on C_q), one can make a similar statement about (infinite dimensional) simple algebras which are not division algebras.

THEOREM 2. *There exist division algebras, and also simple algebras which are not division algebras, possessing noninner, nonouter Abelian Galois groups.*

5. **Conclusion.** Theorem 2 establishes a starting point for the study of nonouter Abelian extensions. It would be interesting to know just which Abelian groups can play the rôle of an nonouter Abelian Galois group H. Consider the torsion case. If H is an arbitrary nonouter torsion Galois group of a division ring K, a theorem of Kaplansky (Canad. J. Math. vol. 3 (1951) pp. 290–292) implies that $T=T(H)$ is

a field which is either (i) purely inseparable over C, or (ii) algebraic over a finite field. As $I(H)$ is isomorphic to T^*/C^*, this indicates the complex structure nonouter torsion groups have. In passing note that, if T were chosen in accordance with (i), or (ii), then a regular group $H=G\otimes J$, where $I(H)=J=J(T)$, would be a torsion group.

Next let $H=G(K/F)$ be a regular Galois group generated by two regular subgroups $G_1=G(K/K_1)$ and $G_2=G(K/K_2)$ such that $G_1\cap G_2=(e)$. It follows easily that $F=F(G_1G_2)=F(G_1)\cap F(G_2)=K_1\cap K_2$, and, since $G(K/K_1K_2)\subseteq G_1\cap G_2=(e)$, that $K=K_1K_2$. Thus any direct decomposition of $H=G(K/F)$ into a product of regular subgroups will have some, if weak, effect on the structure of K,F.

A further observation can be made in case $T=T(H)$ is commutative: any factorization $T=T_1\otimes T_2$ over C, where T_i are subfields, will induce a direct decomposition of $J=J_1\otimes J_2$, where $J_i=J(T_i)$ are regular subgroups, $i=1$, 2. However, a direct decomposition of $J=T^*/C^*$ can be made into subgroups which are not regular. This fact no doubt will weaken any part the theory of Abelian groups might play in connection with structure the nonouter Abelian extensions.

6. **Appendix.** Let K be a ring whose center C is a field, and let F be a Galois subring whose Galois group is Abelian but not outer. It is interesting to note some conditions on the centralizer Q of F in K, other than those of Proposition 2, for which $Q\subseteq F$.

PROPOSITION 2′. *Then $Q\subseteq F$ provided both* (i) *Q is generated by a subset S of elements algebraic over C, and* (ii) *$C\cap F$ is infinite.*

PROOF. To each $a\in S$, $a\notin C$, there corresponds different $u, v\in F\cap C$ such that $a+u$, $a+v\in Q^*$. Then in the same way as the proof of Lemma 3 one concludes that $a\in F$. Since the elements of S are commutative, so is Q (even if Q is generated by S only in the ring sense.) This makes Q itself algebraic so that every $q\in Q$ not in C must lie in F. By considering elements aq of Q with $a\in C$, $q\notin C$, one sees that indeed $Q\subseteq F$.

REMARK. Another possibility is to require that $F\cap C$ contain at least $N+2$ elements when S is algebraic of bounded degree N.

Under the assumption that Q modulo its radical R has minimum condition, one may show by relentless computation, as the referee did, that Q has a module basis consisting of elements x with x, $x-1\in Q^*$, $x\notin C$, whenever C contains at least 5 elements. Theorem 1 follows almost immediately from this result and Lemma 3. In the case $Q-R$ is simple such a basis always exists, and Theorem 1 in an

earlier manuscript was in this setting. Credit is due the referee for its present form. However, in the present article, I have capitalized on the fact, illustrated above and also by Lemma 2, that under the axioms at our command Q must be commutative.

References

1. A. S. Amitsur, *Noncommutative cyclic fields*, Duke Math. J. vol. 21 (1954) pp. 87–106.

2. N. Jacobson, *The fundamental theorem of the Galois theory for quasi-fields*, Ann. of Math. vol. 41 (1940) pp. 1–7.

3. G. Köthe, *Schiefkörper unendlichen Ranges über dem Zentrum*, Math. Ann. vol. 105 (1931) pp. 15–39.

4. T. Nakayama, *Galois theory of simple rings*, Trans. Amer. Math. Soc. vol. 73 (1952) pp. 276–292.

5. K. Shoda, *Über die Galoissche Theorie die halbeinfachen hyperkomplexen Systeme*, Math. Ann. vol. 107 (1932–1933) pp. 252–258.

The Pennsylvania State University