JOURNAL OF ALGEBRA 150, 321–323 (1992)

# Galois-Theoretical Groups

TUVAL FOGUEL

*Department of Mathematics, University of Illinois, Urbana, Illinois 61801*

*Communicated by Walter Feit*

Received December 7, 1990

A group $G$ is called Galois-theoretical if $C_G C_A(H) = H$ for any subgroup $H$ of $G$ and $C_A C_G(B) = B$ for any subgroup $B$ of $A = \mathrm{Aut}(G)$. This paper shows that a group $G$ is Galois-theoretical if and only if $G$ is isomorphic to the trivial group, to the cyclic group of order 3, or to the symmetric group of degree 3. © 1992 Academic Press, Inc.

## 1. INTRODUCTION

Let $A$ be a group acting on a group $G$. We say that $(A, G)$ satisfies the double centralizer property (or DCP) if $C_G C_A(H) = H$ for any subgroup $H$ of $G$ and $C_A C_G(B) = B$ for any subgroup $B$ of $A$. We see by [2] that the subgroup lattices of $A$ and $G$ are dual (anti-isomorphic).

The Galois theory of field extensions establishes a one-to-one correspondence between the lattice of intermediate fields of an extension and the subgroup lattice of its Galois group. This paper looks at a similar relation between a group $G$ and $\mathrm{Aut}(G)$. A group $G$ is called Galois-theoretical if $(\mathrm{Aut}(G), G)$ satisfies DCP. This paper classifies all such groups, by proving that:

THEOREM 1.1. *A group $G$ is Galois-theoretical if and only if $G$ is isomorphic to the trivial group, to the cyclic group of order* 3, *or to the symmetric group of degree* 3.

Theorem 1.1 proves an unpublished conjecture of Nigel Boston.

## 2. PRELIMINARIES

LEMMA 2.1. *If $G$ is a Galois-theoretical group, then $G$ is finite.*

*Proof.* Since $G$-has a dual, by [3, 4] we get that $G$ is the direct product (non-Cartesian) of finite subgroups $G_i$ for $i$ in $I$, where each $G_i$ is coprime



0021-8693/92 $5.00

to $G_j$ for all $j \neq i$, and each $G_i$ is a $P$-group or an $M$-group of prime power order (for definitions of $P$-group and $M$-group see [1]).

Assume that $G$ is not finite. For each $G_i$, we have that $|G_i| = p_i^{n_i} q_i$ where $q_i$ divides $(p_i - 1)$ and $q_i$ is 1 or a prime. Without loss of generality we may assume $I$ is the natural numbers and $p_i < p_{i+1}$ for all $i$. For each $G_i$ choose a $\beta_i$ in $\mathrm{Aut}(G_i)$ with order $(\beta_i) = p_i$, or $p_i - 1$. Define $\beta$ for all $g = g_{i1} \cdots g_{ik}$ in $G$ where $g_{ij}$ is in $G_{ij}$ by $\beta(g) = \beta_{i1}(g_{i1}) \cdots \beta_{ik}(g_{ik})$. We see that $\beta$ is in $\mathrm{Aut}(G) = A$ and order $(\beta) = \infty$. Therefore $A$ is not a torsion group, but $A$ has a dual contradicting Proposition 4.1 of [1]. ∎

LEMMA 2.2. *If G is a nontrivial Galois-theoretical group and coprime indecomposable, then G and* Aut(*G*) *are P-groups. And we have* $|G| = 3^{n+1}2 = |\mathrm{Aut}(G)|$ *or* $|G| = 3^{n+1}$ *and* $|\mathrm{Aut}(G)| = 3^n 2$ *where* $n \geq 0$.

*Proof.* Since $G$ is a finite group, and $(\mathrm{Aut}(G), G)$ satisfies DCP, we see by Theorem 2 of [2] that $G$ and $A = \mathrm{Aut}(G)$ are $P$-groups. And we also see that $|A| = q$, $|G| = p$, or $|A| = p^n q$, $|G| = p^n r$, or $|A| = p^n q$, $|G| = p^{n+1}$, where $n > 0$, $p$, $r$, and $q$ are primes, $q$ and $r$ divide $p - 1$. In each case we see that $(p-1)$ divides $|A|$. Therefore we get that $p = 3$, and $q = r = 2$. ∎

LEMMA 2.3. *If G is a nontrivial Galois-theoretical group, then G is Coprime indecomposable.*

*Proof.* Assume that $G = G_1 \times \cdots \times G_n$ where each $G_1$ is nontrivial, $n > 1$, and $(|G_i|, |G_j|) = 1$ whenever $i \neq j$. Then $A = \mathrm{Aut}(G) = A_1 \times \cdots \times A_n$ where each $A_i = \mathrm{Aut}(G_i)$. By Theorem 5 of [2] we get that $(A_i, G_i)$ satisfy DCP for all $i$. Therefore each $G_i$ is a nontrivial Galois-theoretical group. So by Lemma 2.2 we get that for each $G_i$, 3 divides $|G_i|$, contradicting that $(|G_i|, |G_j|) = 1$ whenever $i \neq j$. ∎

## 3. PROOF OF THEOREM 1.1

*Proof of* 1.1. By Theorem 3 of [2] we get that the trivial group, the cyclic group of order 3, and the symmetric group of degree 3 are Galois-theoretical groups.

If $G$ is a nontrivial Galois-theoretical group by Lemma 2.2, $G$ is a $P$-group. Suppose that $|G| = 3^n 2$ or $3^n$, $n > 1$, then $GL_n(3)$ is isomorphic to a subgroup of $\mathrm{Aut}(G)$. In the case that $n > 3$ we get that $3^{n+1}$ divides $|\mathrm{Aut}(G)|$ contradicting Lemma 2.2. For $n = 3$ or 2 we have $|GL_n(3)|$ does not divide $3^n 2$ again contradicting Lemma 2.2. Therefore $|G| = 3$ or 6 and $G$ is isomorphic to the cyclic group of order 3, or the symmetric group of degree 3. ∎

## REFERENCES

1. M. SUZUKI, Structure of a group and the structure of its lattice of subgroups, *in* "Ergeb. Math. Grenzgeb.," Vol. 10, Springer-Verlag, Berlin/Gottingen/Heidelberg, 1956.
2. R. A. CALCATERRA, Group action with inverting centralizers, *Arch. Math.* **49** (1987), 465–469.
3. G. ZACHER, I gruppi risolubili con duale, *Rend. Sem. Mat. Univ. Padova* **31** (1961), 104–113.
4. G. ZACHER, Caratterizzazione dei gruppi immagini omomorphe duali di un gruppo finito, *Rend. Sem. Mat. Univ. Padova* **31** (1961), 412–422.