156. A Note on Galois Theory of Division Rings of Infinite Degree

By Takasi NAGAHARA and Hisao TOMINAGA
Department of Mathematics, Okayama University, Japan

(Comm. by Z. SUETUNA, M.J.A., Dec. 12, 1955)

Although several generalizations of the theory of Galois for fields have been undertaken for non-commutative fields and rings under some finiteness assumptions,[1] there are few papers concerning non-commutative Galois theory for infinite cases among which one could only mention a work of G. Köthe[2] as a representative one. Recently, N. Nobusawa[3] constructed his Galois theory for division rings of infinite degree: Let $\mathfrak{G}$ be the maximal group of D/L, where D is a division ring and L is a division subring of D. If $\mathfrak{G}$ satisfies the following condition

(*) for each $a \in D$ the set $\{aG;\ G \in \mathfrak{G}\}$ is finite,

then, introducing the same topology as in the theory of Krull for fields,[4] $\mathfrak{G}$ becomes a compact group and there exists the one-to-one correspondence between division subrings of D containing L and closed regular subgroups of $\mathfrak{G}$.

The purpose of the present note is to prove the following

Theorem. *Let D be a division ring, L be a division subring and $\mathfrak{G}$ be the maximal group of D/L. If $\mathfrak{G}$ satisfies the following condition*

(*) *for each $a \in D$ the set $\{aG;\ G \in \mathfrak{G}\}$ is finite,*

then there hold the next propositions:

(i) *If C, the center of D, is infinite then $V_D(L)=C$.*[5]

(ii) *If $V_D(L) \supsetneqq C$ then $V_D(L)$ is finite.*

To prove this theorem, we shall require a chain of lemmas, which will be stated in the form rather general.

Throughout the paper, R will be a simple ring (i.e. a primitive ring with minimum condition), R' be a simple subring of R (with

1) G. Azumaya: Galois theory for uniserial rings, J. Math. Soc. Japan, **1** (1949). H. Cartan: Théorie de Galois pour les corps non commutatifs, Ann. Ecole Norm. Sup., **64** (1947). J. Dieudonné: La théorie de Galois des anneaux simples et semi-simples, Comm. Math. Helv., **21** (1948). N. Jacobson: A notè on division ring, Amer. J. Math., **69** (1947). T. Nakayama: Galois theory of simple rings, Trans. Amer. Soc., **73** (1952).

2) G. Köthe: Schiefkörper unendlichen Ranges über dem Zentrum, Math. Ann., **105** (1931).

3) N. Nobusawa: An extension of Krull's Galois theory to division rings, Osaka Math. J., **7** (1955).

4) W. Krull: Galoissche Theorie der unendlichen algebraischen Erweiterungen, Math. Ann., **100** (1928).

5) $V_D(L)$ denotes the centralizer of L in D.

the same identity element) and Z, Z' be centers of R and R' respectively.

Lemma 1. *Let a be in $V_R(R')\backslash Z$.*[6] *If $Z(a)$, the subring generated by Z and a, is contained in a division subring then, for two different elements c_1, c_2 in Z, $1+c_1a$ and $1+c_2a$ determine different R'-inner automorphisms of R. In particular, if Z is infinite then $Z(a)$ determines an infinite number of R'-inner automorphisms of R.*

Proof. If $(1+c_1a)x(1+c_1a)^{-1}=(1+c_2a)x(1+c_2a)^{-1}$ for every x in R then $(1+c_1a)^{-1}(1+c_2a)=c \in Z$. Thus we obtain $(1-c)+(c_1-c_2c)a=0$. As 1 and a are linearly independent over Z, we have $c=1$, $c_1=c_2c$, whence $c_1=c_2$.

Lemma 2. *Let $V_R(R')$ be simple and algebraic over Z, and let $\mathfrak{G}$ be the group of R'-automorphisms of R. If Z is infinite and $\mathfrak{G}$ satisfies the following condition*

(*) *for each $a \in R$ the set $\{aG;\ G \in \mathfrak{G}\}$ is finite,*

then $V_R(R')=Z$.

Proof. Let $V_R(R')=D_n$, where D_n means the ring of $n\times n$ matrices over a division ring $D \supseteq Z$. At first, we assume $D \supsetneqq Z$. Then we can select an element $a \in D\backslash Z$. As a is algebraic over Z, $Z(a)$ is a subfield of D, and finite over Z. Hence, by the fundamental theorem of simple rings, $V_R(Z(a))$ is simple and R is finite over $V_R(Z(a))$. And so we set $R=\sum_{i=1}^{k} b_iV_R(Z(a))$, where b_i in R. Since, by Lemma 1, $Z(a)$ determines an infinite number of R'-inner automorphisms, some of b_i's, say b_1, has infinite images by these inner automorphisms. This contradiction implies that $V_R(R')=Z_n$. Next, we suppose $n>1$. Let e_{ij} be the matric units of Z_n, then $1+ce_{12}$ is regular and its inverse is $1-ce_{12}$, where c in Z. Thus there holds that $(1+ce_{12})e_{22}(1+ce_{12})^{-1}=e_{22}+ce_{12}$. As Z is infinite, this is contrary to (*). Hence we obtain $V_R(R')=Z$.

Lemma 3. *Let the group $\mathfrak{G}$ of R'-automorphisms of R leave fix exactly R'. If $V_R(R')$ properly contains Z and if*

(*) *for each $a \in R$ the set $\{aG;\ G \in \mathfrak{G}\}$ is finite, and*

(**) *each subring of R which is finitely generated over R' is contained in some simple subring which is finite and Galois over R',*[7] *then $V_R(R')$ is algebraic over Z.*

Proof. Let $a \in V_R(R')\backslash Z$, then there exists an element b in R such that $ab \neq ba$. Now let R_1 be a simple subring containing R', a and b which is finite and Galois over R', and let $\mathfrak{G}_1$ be its Galois

6) $V_R(R')\backslash Z$ signifies the complement of Z in $V_R(R')$.

7) Let S be a simple subring of a simple ring R over which R is finite. R will be said to be *Galois* over S if (1) S is the invariant subring of some group $\mathfrak{G}$ of automorphisms of R, (2) $V_R(S)$ is simple and finite over Z, and (3) $[\mathfrak{G}:\mathfrak{J}]<\infty$, where $\mathfrak{J}$ is the totality of inner automorphisms in $\mathfrak{G}$.

group. Then we obtain $[R_1:R']=[\mathfrak{G}_1:\mathfrak{J}_1]\cdot[V_{R_1}(R'):Z_1]$,[8] where Z_1 is the center of R_1 and $\mathfrak{J}_1$ is the totality of inner automorphisms in $\mathfrak{G}_1$. Clearly $a\in V_{R_1}(R')\backslash Z_1$. Now we set $V_{R_1}(R')=D_n$, where D is a division ring, and distinguish two cases. I. $n>1$. Z_1 has to be finite. For, if not, making use of the same notation as at the latter part of the proof of Lemma 2, e_{22} has an infinite number of images by R'-inner automorphisms of R. II. $n=1$. Since R_1 is finite over R', by making use of Lemma 1, we also obtain that Z_1 is finite. (Recall here that each R'-inner automorphism of R_1 may be considered as that of R.) Hence, in either case, Z_1 is finite. Accordingly, $V_{R_1}(R')$ is finite,[9] and so it is absolutely algebraic. Hence a is algebraic over Z.

Before the proof of our theorem, we note here that, in Lemma 3, if R is a division ring then the condition (*) implies (**). Let $a_1,\dots,a_n$ be a finite number of elements of R, R^* be the subring generated by R' and all images of a_i's by $\mathfrak{G}$, $\mathfrak{G}^*$ be the restriction of $\mathfrak{G}$ on R^*. Then, to be easily verified, $\mathfrak{G}^*$ is a finite regular group of R^* over R'. Hence $[R^*:R']$ is finite,[10] accordingly R^* is finite and Galois over R'.

In the following, $K(a_1,\dots,a_n)$ will mean the division subring of D generated by a subring K and elements $a_1,\dots,a_n$.

Proof of Theorem

(i) If $V_D(L)\supsetneqq C$ then, by Lemma 3, $V_D(L)$ is algebraic over C. A contradiction will be given by Lemma 2.

(ii) By (i) of this theorem, C has to be finite and, by Lemma 3, $V=V_D(L)$ is algebraic over C. Hence V is a field[11] and locally finite over C.

Now we select an element $a\in V\backslash C$, then there exists an element $b\in D$ such that $ab\neq ba$. And let $\{a_iba_i^{-1};\ a_1\in V,\ i=1,2,\dots,k\}$ be the set of all images of b by the inner automorphisms in $\mathfrak{G}$, which is finite by (*). We shall prove first that $V=V'(a_1,\dots,a_k)$, where $V'=V_D(L(b))=V_V(b)$. For any x in V, there holds that $a_i^{-1}x\in V'$ for some i. Hence $x\in V'(a_i)\subseteqq V'(a_1,\dots,a_k)$, whence we shall obtain that $V=V'(a_1,\dots,a_k)=C(V',a_1,\dots,a_k)$. Since V is locally finite over C, our proof will be completed if we can prove the finiteness of V'. To this end, we suppose, in contrary, that V' is infinite. Now we consider the division subring $W=V'(a,b)$ and let C'' be its center. Clearly $a\in V_W(V'(a))\backslash C''$ and C'' contains the infinite field

8) T. Nakayama: Ibid., Theorem 1.

9) As an easy consequence, the center of R' is finite too.

10) N. Jacobson: Ibid., Theorem 2.

11) N. Jacobson: Structure theory for algebraic algebras of bounded degree, Ann. Math., **46** (1945), Theorem 11.

$V'(\subseteq V)$. Hence, by Lemma 1, the set $\{1+ca;\ c\in V'\}$ determines an infinite number of $V'(a)$-inner automorphisms of $W=V'(a, b)$, whence b has an infinite number of images by these inner automorphisms, being contrary to $(*)$.

Remark 1. Our theorem can be generalized as follows: Let the group $\mathfrak{G}$ of R'-automorphisms of R leave fix exactly R'. If $V_R(R')$ is simple and if

$(*)$ for each $a\in R$ the set $\{aG;\ G\in\mathfrak{G}\}$ is finite, and

$(**)$ each subring of R which is finitely generated over R' is contained in some simple subring which is finite and Galois over R', then there hold the next propositions:

(i) If Z is infinite then $V_R(R')=Z$.

(ii) If $V_R(R')\subsetneqq Z$ then $V_R(R')$ is finite.

Remark 2. Let D be not commutative and C be infinite. Then, for any $a\in D\backslash C$, there exists an element b such that $ab\neq ba$. Now we set $M=C(b)$ and $N=C(a, b)=M(a)$, and let C' be the center of N. Clearly $b\in V_N(M)\backslash C'$, and as $C'\supseteq C$, by Lemma 1, the set $[1+c'b;\ c'\in C']$ determines an infinite number of M-inner automorphisms of $N=M(a)$, whence a has an infinite number of images by these inner automorphisms of N (or of D). This fact shows that the theory of Nobusawa is not applicable for that of Köthe.

Remark 3. A group $\mathfrak{G}$ of D/L is said to be *almost outer* if G contains only a finite number of inner automorphisms. Mr. N. Nobusawa has kindly directed our attention to his new result that, in case D is locally finite over L, the condition that $\mathfrak{G}$ is almost outer implies the condition $(*)$.[12] Combining this fact with our theorem, we obtain that the condition $(*)$ is equivalent to the condition that D is locally finite over L and $\mathfrak{G}$ is almost outer.

Recently, we got a letter from N. Nobusawa in which he said that D. Zelinsky had obtained independently the same result with ours.

12) N. Nobusawa: On compact Galois groups of division rings, Osaka Math. J. (to appear).