ON AUTOMORPHISM GROUPS OF FINITE ORDER IN DIVISION RINGS

By

Hisao TOMINAGA

It is a well-known theorem of E. Artin that if F is an algebraically closed (commutative) field of characteristic 0 then any automorphism of F of finite order is of order at most 2. Recently, in [1], H. Lenz drew out the essence of Artin's proof [1, Satz 3], and obtained several results concerned with automorphism groups of finite order. In the present note, we shall prove an extension of [1, Satz 3] to division rings and that of [1, Satz 5], whose proof is notably easy.

Let K be a division ring with the center Z, and $\mathfrak{G}$ an automorphism group of K. Then, $\mathfrak{G}$ induces an automorphism group $\overline{\mathfrak{G}}$ of the group K^*/Z^*, where K^* is the multiplicative group consisting of all non-zero elements of K. Particularly, if $\overline{\mathfrak{G}}$ coincides with the identity group then $\mathfrak{G}$ will be called an *M-group*. In case K is commutative, the notion of M-group is trivial of course. Now let p be a prime number, and k an element of K. If there exists a division subring K' of K such that $k^p \in K'$ and $k \notin K'$, then k will be called a *p-th root of* K. We consider here the following property of K:

(P) *For each p-th root k of K, the equation $x^p - k = 0$ has a solution in K.*

At first, we shall prove the following fundamental lemma.

Lemma 1. *Let K be strictly Galois*[1] *with respect to an M-group* $\mathfrak{P} = \{\sigma^i\}$ *of order p, and possess the property* (P). *If Z contains a primitive* p^2*-th root* η *of* 1, *then* η *is not contained in* $L = J(\mathfrak{P}, K)$ (*=the fix-subring of* $\mathfrak{P}$).

Proof. Evidently, $\zeta = \eta^p$ is a primitive p-th root of 1, and $[\Phi(\zeta):\Phi] < p$, where Φ is the prime subfield of K. If $\zeta\sigma \neq \zeta$, then $\Phi(\zeta)$ being $\mathfrak{P}$-normal, we have $[\Phi(\zeta):\Phi] \geq p$. We see therefore ζ is contained in L. Accordingly, by [2, Corollary 2], there exists a non-zero element $x \in K$ such that $x\sigma = x\zeta$. As $x^p \in L$ and $K = L[x]$ consequently, the property (P)

1) Cf. [3].

secures the existence of $y\in K$ with $y^p=x$. Recalling here $\mathfrak{P}$ is an M-group, we have $y\sigma=yz$ for some $z\in Z$. $(y\sigma)^p=y^p\sigma=x\zeta=(y\eta)^p$ yields therefore $\{(y\sigma)y^{-1}\eta^{-1}\}^p=(z\eta^{-1})^p=1$, whence we have $y\sigma=y\eta\zeta^\lambda$ where $0\leq\lambda\leq p-1$. If $\eta\in L$, then $y\sigma^p=y\eta^p\zeta^{p\lambda}=y\zeta\neq y$. But this contradicts $\sigma^p=1$.

The following lemma will be almost evident from the proof of [3, Lemma 5].

Lemma 2. *Let K be strictly Galois with respect to $\mathfrak{G}$. Then, for an arbitrary subgroup $\mathfrak{H}$ of $\mathfrak{G}$, K is strictly Galois with respect to $\mathfrak{H}$.*

Now we can extend [1, Satz 3] to division rings.

Theorem 1. *Let K be a division ring of characteristic 0 which is strictly Galois with respect to an M-group $\mathfrak{G}$ of order n. If K and Z possess the property* (P), *and Z contains a primitive $2p$-th root of* 1, *then p does not divide n if $p>2$, 4 does not divide n if $p=2$.*

Proof. (I) $p=2$. If 4 diveds n, then $\mathfrak{G}$ contains a subgroup $\mathfrak{H}$ of order 4, and K is strictly Galois with respect to $\mathfrak{H}$ (Lemma 2). Let $\mathfrak{P}_1$ be a subgroup of $\mathfrak{H}$ of order 2, and set $L_1=J(\mathfrak{P}_1, K)$. Then, $K=L_1[i]$ by Lemma 1, where i is an element of Z with $i^2=-1$. (i is a primitive $4(=2p=p^2)$-th root of 1.) And so, $i\notin L=J(\mathfrak{H}, K)$. If we set $L_2=L[i]$, then $[L_2:L]=2$ and $\mathfrak{H}(L_2)\neq 1$.[2)] For, if not, every σ in $\mathfrak{H}$ different from 1 moves i into $-i$. But this is impossible. This proves that K/L_2 is strictiy Galois with ressect to $\mathfrak{H}(L_2)$ of order 2. Hence, again by Lemma 1, $K=L_2[i]=L_2$. This contradiction shows that $4\nmid n$.

(II) $p>2$. If p divides n, then $\mathfrak{G}$ contains a subgroup $\mathfrak{P}=\{\sigma^i\}$ of order p, and K is strictly Galois with respect to $\mathfrak{P}$. Since Z possesses the property (P), it contains primitive p^j-th roots of 1 for all j. Since $E_{p,\infty}$, the subfield (of Z) generated by all the p^j-th roots of 1 ($j=1, 2, \cdots$), is $\mathfrak{P}$-normal, Lemma 1 shows that σ induces an automorphism of $E_{p,\infty}$ which leaves invariant every primitive p-th root of 1 and moves really primitive p^2-th roots of 1. But this contradicts [1, Satz 1].

Let L be a division subring of K. If, for every $k\in K$, there exists a finite number of division subrings $K_1, \cdots, K_m$ such that $L(k)=K_1\supseteq\cdots\supseteq K_m=L$ and $[K_i:K_{i+1}]_l\leq n$ (fixed) for $i=1, \cdots, m-1$, then we say that K/L is *n-accessible*. Further if, for every intermediate divisiôn subring L' of K/L, K/L' is n-accessible, then K/L will be said to be *completely n-accessible.* To be easily seen, in case K is commutative, the notion of n-accessibility coincides with that of complete n-accessibility. Now, let K/L be completely n-accessible and strictly Galois with respect to $\mathfrak{G}$ of

2) $\mathfrak{H}(L_2)=\{\sigma\in\mathfrak{H}\mid x\sigma=x \text{ for all } x\in L_2\}$.

prime order p, where $\mathfrak{G}$ is an automorphism group of K which leaves invariant every element of L. Then, $[K:L']=p$ where $L'=J(\mathfrak{G}, K)$, whence $K=L'[k]$ for some k. On the other hand, there exists a finite number of division subrings $K_1, \cdots, K_m$ such that $K=K_1 \supseteq \cdots \supseteq K_m = L'$ and $[K_i : K_{i+1}]_l = n_i \leq n$. And so, $p=[K:L']=\prod_{i=1}^{m-1} n_i$. Thus, we have proved the following which contains [1, Satz 5].

Theorem 2. *Let K be a division ring, and completely n-accessible over a division subring L. If K is strictly Galois with respect to $\mathfrak{G}$ of prime order p and $J(\mathfrak{G}, K)\supseteq L$, then $p \leq n$.*

References

[1] H. LENZ: Über endliche Automorphismengruppe unendlicher Körpererweiterungen, Archiv der Math., 4 (1953) 100–106.
[2] N. NOBUSAWA and H. TOMINAGA: Some remarks on strictly Galois extensions of simple rings, Math. J. Okayama Univ., 9 (1959) 13–17.
[3] H. TOMINAGA: A note on Galois theory of primary rings, Math. J. Okayama Univ., 8 (1958) 117–123.

Hokkaido University

(Received September 16, 1960)