IC/95/72

INTERNATIONAL CENTRE FOR THEORETICAL PHYSICS

ON DERIVED GROUPS OF DIVISION RINGS II

M. Mahdavi–Hezavehi

S. Akbari–Feyzaabaadi

M. Mehraabaadi

and

H. Hajie–Abolhassan

INTERNATIONAL ATOMIC ENERGY AGENCY

UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION

MIRAMARE-TRIESTE

IC/95/72

International Atomic Energy Agency
and
United Nations Educational Scientific and Cultural Organization
INTERNATIONAL CENTRE FOR THEORETICAL PHYSICS

ON DERIVED GROUPS OF DIVISION RINGS II

M. Mahdavi-Hezavehi [1]
International Centre for Theoretical Physics, Trieste, Italy,

S. Akbari–Feyzaabaadi, M. Mehraabaadi and H. Hajie–Abolhassan
Department of Mathematical Sciences, Sharif University of Technology,
P.O.Box 11365-9415, Tehran, Iran.

ABSTRACT

Let D be a division ring with centre F and denote by D' the derived group (commutator subgroup) of $D^* = D - \{0\}$. It is shown that if each element of D' is algebraic over F, then D is algebraic over F. It is also proved that each finite separable extension of F in D is of the form $F(c)$ for some element c in the derived group D'. Using these results, it is shown that if each element of the derived group D' is of bounded degree over F, then D is finite dimensional over F.

MIRAMARE -TRIESTE
May 1995

[1]On sabbatical leave from: Sharif University of Technology, P.O. Box 11365-9415, Tehran, Iran.

Recently one of the authors, in his investigation of algebraic properties of the derived group D'(cf. [5]), showed that any subfield K of D separable over F is generated over F by a commutative subgroup of D', and raised the following questions:

(a) *Given a division ring D with centre F, let K be a finite separable extension of F in D. Does there exist an element c in the derived group D' such that $K = F(c)$?*

(b) *If each element of D' is algebraic over F, is D algebraic over F?*

In this note we shall give a positive answer to questions (a) and (b), and produce an application of these results to generalize a basic theorem of [2, p. 181] which asserts that any division algebra of bounded degree over its centre F is finite dimensional over F. To prove (a), we need some preparations. Given a monoid K and S a subset of K, we shall say that K is *radical* over S if for each element $a \in K$ there exists a non-negative integer $n(a)$ such that $a^{n(a)} \in S$. We first recall a result due to Kaplansky (cf.[3, p.258]), which asserts that given a radical field extension $F \subset K$, then Char $K = p > 0$, and either K is purely inseparable over F or K is algebraic over its prime subfield. We shall use this result in conjunction with the following

Lemma. *Let K be an abelian group and $K_i, i = 1, 2, \cdots, n$, be subgroups of K such that $\cup_1^n K_i \subset K$ and K is radical over $\cup_1^n K_i$. Then there exists $1 \leq j \leq n$ such that K is radical over K_j.*

Proof. We tensor K with the rational numbers Q over the integers Z and consider the Q-vector space $K \otimes Q$ and Q-subspaces $K_i \otimes Q$. Since K is radical over $\cup_1^n K_i$, it is easily checked that $K \otimes Q = \cup_1^n K_i \otimes Q$. Thus the result follows from the fact that a vector space over an infinite field is not the union of finitely many proper subspaces.

To present some applications of the Lemma, we recall the following well-known

Remark. *Let $F \subsetneq K$ be a finite separable field extension. If $\{K_i\}$ is the collection of proper intermediate subfields of K/F, then for each element $a \in K \setminus \cup K_i$, one has $K = F(a)$.*

Now, it may be of interest to record the following result as the first application of the Lemma.

Corollary 1. *Let $F \subsetneq K$ be a finite separable field extension. Then there is an element $a \in K$ such that $K = F(a)$ with $N_{K/F}(a) = 1$. Furthermore, if K^* contains some torsion-free element, then there exists an element $a \in K$ with $N_{K/F}(a) = 1$ such that $K = F(a) = F(a^2) = F(a^3) = \cdots$.*

Proof. We shall consider two cases :

Case 1. F is finite. Put $| F |= q$, $dim_F K = n$ so that $| K |= q^n$. For each $x \in K$ we know that $N_{K/F}(x) = x^{\frac{q^n-1}{q-1}}$. Assume that b is a generator of the cyclic group K^*. Thus b has order $q^n - 1$ and we have $N_{K/F}(b^{q-1}) = (b^{q-1})^{\frac{q^n-1}{q-1}} = 1$. We claim that $K = F(b^{q-1})$. Since the order of b^{q-1} is $\frac{q^n-1}{q-1} > q^{n-1}$ we conclude that $| F(b^{q-1}) |> q^{n-1}$ and consequently $K = F(b^{q-1})$.

Case 2. F is infinite. Put $n = dim_F K$. By the Remark, there is a finite number of proper subfields $K_i, i = 1, 2, \cdots, m$, of K containing F such that for each element $a \in K \setminus \cup_1^m K_i$ we have $K = F(a)$. We shall now show that there is an element $b \in K$ such that for each natural number j, $b^j \in K \setminus \cup_1^m K_i$. Suppose on the contrary that for each $c \in K$ there is a natural number $n(c)$ such that $c^{n(c)} \in \cup_1^m K_i$. Thus, by the Lemma, there exists $1 \leq j \leq m$ such that K is radical over K_j. Now, by Kaplansky's Lemma, we obtain Char$K = p > 0$, and either K is purely inseparable over K_j or K is algebraic over its prime subfield P. But the first case does not occur and so K is algebraic over P. Put $K = F(b)$ and denote by F_o the field generated by P and the coefficients of the minimal polynomial of b over F. Now, put $K_o = F_o(b)$. Thus $dim_{F_o} K_o = n$ and, by the case 1, there is an element $a \in K_o$ with $N_{K_o/F_o}(a) = 1$ such that $K_o = F_o(a) = F_o(b)$. We now have $b \in F_o(a) \subseteq F(a)$, and consequently $K = F(a)$. Since the degree of the minimal polynomial of a over F_o is equal to the degree of the minimal polynomial of a over F we conclude that these polynomials are identical and so $N_{K/F}(a) = 1$. Thus we may assume that there is an element $b \in K$ such that for each natural number j, $b^j \in K \setminus \cup_1^m K_i$, and therefore $K = F(b^n)$. Now put $a = \frac{b^n}{N_{K/F}(b)}$ to obtain $K = F(b^n) = F(a)$ with $N_{K/F}(a) = 1$. Finally, assume K^* contains a torsion-free element. Keeping the notations of Case 2, if for each $b \in K \setminus \cup_1^m K_i$ there exists a natural number $r(b)$ such that $b^{r(b)} \in \cup_1^m K_i$, then, as above, we conclude K must be algebraic over the prime subfield of K. This implies that each element of K^* is torsion which contradicts our hypothesis. Thus there exists an element $b \in K \setminus \cup_1^m K_i$ such that $b, b^2, b^3, \cdots$, do not belong to $\cup_1^m K_i$. Now put $a = \frac{b^n}{N_{K/F}(b)}$ to obtain the result.

We note that in the characteristic zero Corollary 1 takes a modest form as

Corollary 2. *Let $F \subseteq K$ be a finite field extension with Char $K = 0$. Then there exists an element $a \in K$ with $N_{K/F}(a) = 1$ such that $K = F(a) = F(a^2) = F(a^3) = \cdots$.*

We note that there exist finite separable extensions of an infinite field whose elements are torsion. As an example, let Z_p denote the integers modulus a prime number p and take an infinite algebraic extension of Z_p that is not the full algebraic closure of Z_p, since every nonzero element of the algebraic closure of Z_p is torsion.

When the field extension lies in a division ring D, the conclusion of Corollary 1 takes a different form. To prove it, we need to invoke a result from [4] or also [5] as follows:

Lemma A. *Let D be a division ring with centre F. Then for each element $a \in D$ algebraic over F, there exists a positive integer $n(a)$, depending on a, and an element $c_a \in D' \cap F(a)$ such that $a^{n(a)} = N_{F(a)/F}(a)c_a$ with $N_{F(a)/F}(c_a) = 1$, where $N_{F(a)/F}$ is the norm of $F(a)$ to F.*

Theorem 1. *Let D be a division ring with centre F. Given a finite separable field extension $F \subseteq K$ in D, then we have:*
(i) There exists an element $c \in D'$ with $N_{K/F}(c) = 1$ such that $K = F(c)$.
(ii) If each multiplicative commutator is algebraic over F, then there exists $c \in D'$ with $N_{K/F}(c) = 1$ such that $K = F(c) = F(c^2) = F(c^3) = \cdots$.
(iii) If K has a non-trivial F-automorphism, then there is a multiplicative commutator a in D' with $N_{K/F}(a) = 1$ such that $K = F(a)$.

Proof. (i) Put $n = dim_F K$. By the Remark, there is a finite number of proper subfields $K_i, i = 1, 2, \cdots, m$, of K containing F such that for each element $a \in K \setminus \cup_1^m K_i$ we have $K = F(a)$. Now, by Lemma A, we obtain an element $c_a \in D'$ such that $a^{n(a)} = N_{K/F}(a)c_a$ with $N_{K/F}(c_a) = 1$. If for each $a \in K \setminus \cup_1^m K_i$, $c_a \in \cup_1^m K_i$, then K is radical over $\cup_1^m K_i$. Consequently, Char $K = p > 0$, and either K is algebraic over the prime subfield P or K is purely inseparable over K_j. The second case cannot occur, so let K be algebraic over P. We know, by Corollary 1, that there exists an element $a \in K$ with $N_{K/F}(a) = 1$ such that $K = F(a)$. Now, a is algebraic over P, and hence F. Also, K/F is a cyclic extension from the theorem of natural irrationalities and the theory of finite fields. So, using Hilbert's Satz 90 and the Skolem-Noether Theorem, we conclude that a is a multiplicative commutator and the result follows. Thus there is an element $a \in K \setminus \cup_1^m K_i$ such that $c_a \notin \cup_1^m K_i$ and so $K = F(c_a)$ and this completes the proof of (i).
(ii) Keeping the notations of part (i), if for each $a \in K \setminus \cup_1^m K_i$ there exists a natural number $r(a)$ such that $c_a^{r(a)} \in \cup_1^m K_i$, then K is radical over $\cup_1^m K_i$. Using the Lemma as above, we conclude that K is algebraic over the prime subfield P. Then F will be algebraic over P and consequently all multiplicative commutators are torsion. So, by Theorem 1 of [1], D is commutative and there is nothing to prove. Thus there exists an element $a \in K \setminus \cup_1^m K_i$ such that $c_a, c_a^2, c_a^3, \cdots$ do not belong to $\cup_1^m K_i$. Therefore, for each positive integer t we obtain $K = F(c^t)$, where $c = c_a$, and this completes the proof of (ii).
(iii). If F is finite, we saw that $K = F(a)$, where a is a multiplicative commutator. So assume that F is infinite. Using the notations of part (ii), let $\sigma \neq 1$ be the F-automorphism of K. If for each $x \in K \setminus \cup_1^m K_i$ we have $x^{-1}\sigma(x) \in \cup_1^m K_i$, then for $m + 1$ distinct elements $r_1, r_2, \cdots, r_{m+1}$ of F we obtain $(x + r_j)^{-1}\sigma(x + r_j) \in \cup_1^m K_i$, for all $1 \leq j \leq m + 1$. Thus there exist i, j with $i \neq j$ such that $(x + r_i)^{-1}\sigma(x + r_i) \in K_s$ and $(x + r_j)^{-1}\sigma(x + r_j) \in K_s$, for some s. So there exist elements $t_1, t_2 \in K_s$ such that

$\sigma(x+r_i) = t_1(x+r_i), \sigma(x+r_j) = t_2(x+r_j)$. Consequently, we obtain

$$r_i - r_j = (t_1 - t_2)x + t_1 r_i - t_2 r_j. \quad (1)$$

If $t_1 \neq t_2$, then $x = (t_1 - t_2)^{-1}(r_i - r_j - t_1 r_i + t_2 r_j)$. This gives the contradiction $x \in K_s$. Thus $t_1 = t_2$ and from (1) we obtain $t_1 = t_2 = 1$, consequently $\sigma(x) = x$, i.e., σ is trivial on K. This contradiction allows us to choose an element $x \in K \setminus \cup_1^m K_i$ such that $x^{-1}\sigma(x) \notin \cup_1^m K_i$. We know, by the Skolem-Noether Theorem, that $\sigma(x) = y^{-1}xy$ for some $y \in D^*$. Therefore, by the Remark, we obtain $K = F(a)$, where $a = x^{-1}y^{-1}xy$. It is easily proved that $N_{K/F}(a) = 1$, and this completes the proof of the theorem.

To prove our final result we need the following

Theorem 2. *Let D be a division ring with centre F. If each element of D' is algebraic over F, then D is algebraic over F. Equivalently, either D is algebraic over F or D' contains a transcendental element over F.*

Proof. We know by Cartan-Brauer-Hua's Theorem that the division ring generated by F and D' is D itself. So it is enough to prove that the sum and the product of any two algebraic elements of D over F are also algebraic over F. We first show that if $x, y \in D$ are algebraic over F, then xy is also algebraic over F. Consider the factor group D^*/F^*D'. Since x and y are algebraic over F, by Lemma A, their images $x(F^*D')$ and $y(F^*D')$ are torsion in D^*/F^*D'. Consequently, $xy(F^*D')$ is torsion which implies that xy is algebraic over F. From this we conclude that if $x, y \in D$ are algebraic over F, then $x + y = x(1 + x^{-1}y)$ is also algebraic over F and thus the result follows.

We are now in a position to prove an interesting consequence of the above results as follows:

Corollary 3. *Let D be a division ring with centre F. If there is an integer n such that $[F(c) : F] \leq n$ for each $c \in D'$, then D is of finite dimension over F.*

Proof. If D is commutative, there is nothing to prove. Otherwise, by Theorem 1(i) and the hypothesis, the degrees of finite separable extensions of F in D are bounded by some integer. Thus, there is a separable subfield K of D with $dim_F K$ maximal. Put $L = C_D(K)$, the centralizer of K in D. Since $dim_F K < \infty$, by the Double Centralizer Theorem, $Z(L) = K$. We claim that $L = K$. If L is commutative, then $L = Z(L) = K$ and we are through. Otherwise, by Corollary 4 of [5], there is an element $a \in L' \setminus K$ separable over K, where L' is the derived group of L^*. Thus $K(a)$ is a finite extension of K which is separable over F and $dim_F K(a) = (dim_K K(a))(dim_F K) > dim_F K$. This contradicts $L \neq K$. Thus K is a maximal subfield of D which is of finite dimension over

F and consequently $dim_F D < \infty$.

Finally, it is believed that the results of the Abstract remain true if one replaces the elements of D' with multiplicative commutators, but we have not been able to establish them.

Acknowledgments The authors would like to thank the referee for his constructive comments. The authors are also indebted to the Institute for Theoretical Physics and Mathematics, and the Research Council of the University for their support. M.M–H. would like to thank Professor Abdus Salam, the International Atomic Energy Agency and UNESCO for hospitality at the International Centre for Theoretical Physics, Trieste, where this work was revised.

References

[1] Herstein, I.N., Multiplicative Commutators in Division Rings, *Israel Journal of Mathematics*, Vol.31, No.2, 1978.

[2] Jacobson, N., Structure of Rings, Coll., Pub., Vol. 37, Amer. Math. Soc., Providence, R.I., 1956.

[3] Lam, T.Y., A First Course in Non-Commutative Rings, GTM, No. 131, Springer-Verlag, 1991.

[4] Mahdavi-Hezavehi, M., Extending Valuations to Algebraic Division Algebras, *Communications in Algebra*, Vol. 22(11), 1994, 4373-4378.

[5] Mahdavi-Hezavehi, M., On Derived Groups of Division Rings, *Communications in Algebra*, to appear.