ON CONJUGATES IN DIVISION RINGS

CARL C. FAITH

Let D be a non-commutative division ring with centre C, and let Δ be a proper division subring not contained in C. In **(4)** Cartan raised the question: is it ever possible for each inner automorphism of D to induce an automorphism of Δ? As is well-known, Cartan **(4**, Théorème 4**)** with the aid of his Galois Theory answered this negatively in case D is a finite dimensional division algebra. Later Brauer **(3)**, and Hua **(8)**, using elegant, elementary methods, extended Cartan's theorem to arbitrary division rings.

Let D^* denote the group of all non-zero elements of D, and let $H(\Delta)$ be the subgroup of all elements of D^* which effect inner automorphisms of D that map Δ onto Δ. In this note I prove the following extension of the Cartan-Brauer-Hua theorem: *$H(\Delta)$ cannot have finite index in D^*.* This theorem implies (and is implied by) the condition: *D always contains infinitely many subrings $x\Delta x^{-1}$ isomorphic (or conjugate) to Δ.*

Although this result implies that every finite division ring is commutative, its proof does not constitute a new proof of this old theorem **(17)** of Wedderburn's. As a matter of fact, the proof requires not only Wedderburn's theorem but also Jacobson's theorem **(9)** on algebraic division algebras over a finite field.

1. Conjugates in division rings. If S is any subset of a division ring D, the *centralizer of S in D* is the set $S' = \{x \in D | sx = xs \text{ for all } s \in S\}$. When S consists of the single element θ, θ' denotes this division subring. S'' is the division subring $(S')'$. If Δ is any division subring of D, Δ^* represents the multiplicative group of non-zero elements of Δ. C will always be the centre of D.

The group of all automorphisms of D which leave fixed each element of Δ is signified by $G(\Delta)$; $J(\Delta)$ is the subgroup of those inner automorphisms of D which belong to $G(\Delta)$. The group $G(\Delta)$ is *outer* when $J(\Delta)$ is the identity subgroup (e). Since $J(\Delta)$ is isomorphic to ∇^*/C^*, where $\nabla = \Delta'$, one deduces from the following proposition that if $J(\Delta)$ is a finite group $\neq (e)$, then Δ' is a finite field. Thus when C is not a finite field, $J(\Delta)$ is finite if and only if $G(\Delta)$ is outer.

PROPOSITION 1. *If ∇ is any proper division subring of a division ring D, then ∇^* has finite index in D^* if and only if D is a finite field.*

Proof. If D is a finite field there is nothing to prove. Conversely, if D is not a finite field, then D is not finite **(17)**. Suppose ∇^* has finite index in D^*. Then

Received April 22, 1957.

∇^* necessarily has infinitely many elements; for each $\theta \in D$, there exist elements δ_1, δ_2, and $\delta \in \nabla$, $\delta_1 \neq \delta_2$, such that $\theta + \delta_1 = \delta(\theta + \delta_2)$. But then $(1 - \delta)\theta \in \nabla$. Since $\delta_1 \neq \delta_2$, δ cannot be 1. Thus $(\delta - 1)^{-1} \in \nabla$, so that $\theta \in \nabla$. Hence $D = \nabla$, and ∇ is not a proper subring.

Proposition 1 actually implies that a non-central element θ of a non-commutative division ring D has infinitely many conjugates in D. This is Herstein's theorem **(7)**. As several authors **(15, 16)** have remarked, the Cartan-Brauer-Hua theorem is not needed in the proof.

If Δ is an arbitrary division subring of D, there is occasion to consider isomorphisms of $\Delta(\theta)$ which leave fixed the elements of Δ. Such an isomorphism, often called *an isomorphism of* $\Delta(\theta)$ *with respect to* Δ, when induced by an inner automorphism of D is effected by an element $x \in \Delta'$. If θ commutes with every element of Δ', that is, if $\theta \in \Delta''$, then no non-trivial isomorphism of the kind mentioned exists. If Δ' is finite, then the number of conjugates $x^{-1}\theta x$, with $x \in \Delta'$, is also finite. In all other cases, however, θ has infinitely many such conjugates, as can be deduced from the case $\nabla = \Delta'$ of the next theorem, which has been obtained also by Kasch **(11)**.

THEOREM 1. *Let D be a non-commutative division ring, and let ∇ be an infinite division subring not contained in the center of D. Then every element θ in D which is outside of ∇' possesses infinitely many conjugates $x^{-1}\theta x$ with $x \in \nabla$.*

Proof. If θ has only finitely many conjugates with $x \in \nabla$, then A^* has finite index in ∇^*, where $A = \nabla \cap \theta'$. Since ∇ is not finite, by Proposition 1, A must be all of ∇. But then $\nabla' = A'$. Since $\theta \in A'$ this implies that $\theta \in \nabla'$, contrary to its choice. Thus θ must have infinitely many conjugates $x^{-1}\theta x$, with $x \in \nabla$.

The following corollaries are all proved under the assumption of Theorem 1, that is, $\nabla = \Delta'$ is infinite. In case D is an algebraic division algebra, Jacobson's theorem **(9)** makes this assumption on Δ' superfluous.

COROLLARY. *Let $[\theta]$ denote the set of elements in D of the form $x\theta x^{-1}$, with $x \in \Delta'$. Then, if $[\theta]$ contains an element other than θ, then $[\theta]$ contains infinitely many elements.*

Proof. Since $[\theta] \neq \theta$, then $\theta \notin \Delta''$, so by Theorem 1, the set $[\theta]$ is infinite.

If $[\theta]$ is finite for every $\theta \in D$, then $D = \Delta''$. Thus $\Delta' = C$, that is, $G(\Delta)$ is outer. This yields the next corollary, which emphasizes the severity of Nobusawa's locally finite condition **(13)**.

COROLLARY. *If the set of conjugates of θ with respect to Δ is finite for each $\theta \in D$, then $G(\Delta)$ is outer.*

Let X be indeterminate over Δ, and let $\Delta[X]$ denote the polynomial ring consisting of all finite sums of elements of the form $aXbX \ldots cXd$, with $a, b, \ldots, c, d, \in \Delta$. If $\theta \in D$ is a zero of a polynomial in $\Delta[X]$, then so is every conjugate of θ with respect to Δ. Thus the next corollary is a consequence of Theorem 1. When $\Delta = C$ it specializes to a corollary of Herstein's **(7)**.

COROLLARY. *If at least one zero of a polynomial $p(X) \in \Delta[X]$ lies in D but outside of Δ'', then $p(X)$ has infinitely many zeros in D.*

The next theorem provides another generalization of Herstein's theorem.

THEOREM 2. *Let D be a non-commutative division ring with centre C, and let Δ be a proper division subring which contains C, and has finite dimension d over C. Then any element of D which lies outside of Δ possesses infinitely many conjugates with respect to Δ.*

Proof. H. Cartan **(4)** has shown under the hypotheses of the theorem that D has finite dimension over Δ' equal to d, and moreover, that $\Delta'' = \Delta$. Now Δ' cannot be finite. Otherwise D is an algebraic division algebra over a finite field, and hence, by Jacobson's theorem **(9**, Theorem 8**)**, D is commutative, contrary to hypothesis. Theorem 1 now applies.

2. Isomorphic division subrings. Let Δ be a division subring of a non-commutative division ring D, such that Δ is not contained in the centre C of D. Then the number of distinct isomorphisms of Δ of the form $x^{-1}\Delta x$ is equal to the index of ∇^* in D^*, where ∇ is the centralizer of Δ in D. That this index is always infinite can be obtained from the case $A = D$ of the next proposition, as well as from Proposition 1.

PROPOSITION 2. *Let D be a division ring, and let A be a division subring with infinitely many elements. Let Δ be a division subring of D not contained in the centralizer A' of A. Then there exist infinitely many isomorphisms of Δ of the form $x^{-1}\Delta x$, with $x \in A$.*

Proof. By Theorem 1, any θ in D not in A' is moved infinitely many times by the inner automorphisms of D effected by the elements of A. Since Δ is not contained in A', there must be infinitely many distinct isomorphisms of the form $x^{-1}\Delta x$, with $x \in A$.

Let Δ be a proper division subring not contained in the centre C of a non-commutative division ring D. Let

$$H(\Delta) = \{x \in D^* | x\Delta x^{-1} = \Delta\},$$

and consider the two conditions:

(1) *index of $H(\Delta)$ in D^** $= m < \infty$;
(2) *index of ∇^* in $H(\Delta)$* $= r < \infty$;

where ∇ is the centralizer of Δ in D. I wish to prove that (1) cannot hold. Since Proposition 1 asserts that (1) and (2) cannot hold simultaneously, it will be useful to note some conditions under which (2) holds. Equation (2) can

https://doi.org/10.4153/CJM-1958-036-7 Published online by Cambridge University Press

be interpreted as follows: *The inner automorphisms of D induce only finitely many distinct automorphisms in Δ.* This case certainly occurs when Δ is a field having finite degree over $\Delta \cap C$. More generally, since the centre Z of Δ is mapped onto Z by every automorphism of Δ, it is easily seen that $H(Z) \supseteq H(\Delta)$. Thus if Z is not contained in C, the case just mentioned for fields having finite degree produces the next lemma.

LEMMA 1. *Let Δ be a proper division subring of a non-commutative division ring D such that the centre Z of Δ has finite degree $n > 1$ over $Z \cap C$, where C denotes the centre of D. Then $H(\Delta)$ has infinite index in D^*.*

The proposition below is actually a result of Brauer's **(3)**. It asserts that in general h and $h + 1$ cannot both belong to $H(\Delta)$. I include the proof for the sake of completeness.

PROPOSITION 3. *Let h and $h + 1$ be non-zero elements of D. Then both h and $h + 1$ belong to $H(\Delta)$, where Δ is a division subring of D, if and only if h lies in Δ, or in the centralizer of Δ.*

Proof. The sufficiency is evident. Let $\delta \in \Delta$. Then following Brauer **(3)**;

(i) $h\delta = \delta_0 h$, where $\delta_0 = h\delta h^{-1} \in \Delta$;

(ii) $(h + 1)\delta = \delta_1(h + 1)$, where $\delta_1 = (h + 1)\delta(h + 1)^{-1} \in \Delta$.

From (ii), $h\delta + \delta = \delta_1 h + \delta_1$, so that by (i), $(\delta_0 - \delta_1)h = (\delta_1 - \delta)$. If for some choice of δ, $\delta_0 \neq \delta_1$, then $h = (\delta_0 - \delta_1)^{-1}(\delta_1 - \delta)$ lies in Δ. Otherwise, for all δ, $\delta_0 = \delta_1$. Then from (ii) $\delta = \delta_0$. This is true for all δ. Thus h lies in the centralizer of Δ. This completes the proof.

Now let h and h_0 both belong to $H(\Delta)$. Then if $h + h_0 \in H(\Delta)$, it is necessary that $hh_0^{-1} + 1 \in H(\Delta)$. By the preceding proposition hh_0^{-1} lies in Δ, or Δ'. If further $h_0 \in \Delta \cap \Delta'$, then h lies in Δ, or Δ'. This produces the

COROLLARY. *If h, h_0, and $h + h_0$ all belong to $H(\Delta)$, Δ as in the preceding proposition, then hh_0^{-1} lies in either Δ, or Δ'. If further h_0 lies in the centre of Δ, then h lies in Δ, or Δ'.*

Let D be a non-commutative division ring with centre C, and let Δ be a proper division subring not contained in C. Then there exist two elements v and d, v in D but outside of Δ, and d in Δ, such that $vd \neq dv$. Now Nagahara **(12**, Lemma 1**)** has shown that there is at most one c in $d' \cap \Delta$ such that $(v + c)d(v + c)^{-1}$ lies in Δ. Now let $(v + c)d(v + c)^{-1}$ be outside of Δ, $c \in d' \cap \Delta$. Then $v + c$ does not belong to $H(\Delta)$. It is natural to inquire whether there exist at most two c's in $d' \cap \Delta$, say c_1 and c_2, such that $v + c_1$ and $v + c_2$ belong to the same right coset of $H(\Delta)$ in D^*. This question is answered in the affirmative below.

PROPOSITION 4. *Let D be a non-commutative division ring with centre C, and let Δ be a proper division subring not contained in C. Choose v in D outside of*

Δ, and d in Δ, such that $vd \neq dv$. Let $\{c_k\}$ be a sequence of distinct elements of $d' \cap \Delta$. Then at most two elements of the sequence $\{v + c_k\}$ can belong to the right coset of $H(\Delta)$ in D^* determined by any one of them.

Proof. Suppose $v + c_k$, $k = 1, 2, 3$, all belong to the same right coset of $H(\Delta)$ in D^*, where the c_k, $k = 1, 2, 3$, are distinct elements of $d' \cap \Delta$. Then $(v + c_1)(v + c_2)^{-1} = h$, and $(v + c_3)(v + c_2)^{-1} = h_0$, where h and h_0 belong to $H(\Delta)$. This implies that $(1 - h)v = hc_2 - c_1$, and $(1 - h_0)v = h_0c_2 - c_3$. Thus,

$$(\alpha) \quad v = - c_2 + (1 - h)^{-1}(c_2 - c_1),$$

and,

$$(\beta) \quad v = - c_2 + (1 - h_0)^{-1}(c_2 - c_3).$$

Moreover, by equating v in (α) and (β), one obtains:

$$(1 - h)(1 - h_0)^{-1} = (c_2 - c_1)(c_2 - c_3)^{-1} = d_0 \in d' \cap \Delta.$$

Therefore,

$$(\gamma) \quad d_0h_0 = h + (d_0 - 1).$$

From the corollary to Proposition 3, it follows, since neither d_0 nor $d_0 - 1$ equals zero, that $h(d_0 - 1)^{-1} \in \Delta$, whence $h \in \Delta$, or else $h(d_0 - 1)^{-1} \in \Delta'$. Now h cannot belong to Δ, otherwise by (α), v must belong to Δ, contrary to its choice. Consequently $h(d_0 - 1)^{-1} \in \Delta'$, so that h belongs to the division ring A generated by Δ' and the elements c_1, c_2, and c_3. But then (α) shows that $v \in A$. Thus $v \in d'$, that is, $vd = dv$, contrary to its choice. This completes the proof.

Evidently from this proposition, $H(\Delta)$ has infinite index in D^* provided only that Δ is a proper subring of D not contained in the centre such that for some choice of d in Δ, $d \notin C$, the division ring $d' \cap \Delta$ is infinite. Otherwise every $d \in \Delta$ belongs to a finite division ring. Thus (directly, even without applying Wedderburn's theorem) Δ is an algebraic division algebra over the finite field $Z = \Delta \cap \Delta'$. Then Jacobson's theorem **(9**, Theorem 8**)** implies that $\Delta = Z$, that is, Δ is commutative, so that $d' \cap \Delta = \Delta$ for each $d \in \Delta$. Consequently Δ must be a finite field of necessarily finite degree $n > 1$ over the subfield $\Delta \cap C$. The first lemma now may be applied to complete the proof of the next theorem.

THEOREM 3. *Let D be a non-commutative division ring, and Δ a proper division subring not contained in the centre. Then there exist infinitely many distinct subrings $x\Delta x^{-1}$.*

3. Applications. Let D be a non-commutative division ring, and let Δ and A be division subrings such that the following conditions are satisfied:

(1) Δ does not contain A.
(2) A' does not contain Δ.

When A is infinite, (2) in conjunction with Proposition 2 implies that Δ has infinitely many isomorphisms of the form $a\Delta a^{-1}$ with $a \in A$. Then it is interesting to ask: Are there infinitely many different subrings $a\Delta a^{-1}$ with $a \in A$? Theorem 3 shows that the answer to this question is yes in case A contains Δ properly, inasmuch as (2) implies that Δ is not contained in the centre of A. This is a special case of (I) of the next corollary.

COROLLARY 1. *Let D be a non-commutative division ring, and let Δ and A be division subrings such that* (1) *and* (2) *above hold. Then D contains infinitely many different subrings of the form $a\Delta a^{-1}$ with $a \in A$, provided any one of the following conditions are satisfied:*

(I) *$\Delta \cap A$ is not contained in the centre of A.*
(II) *$Z \cap A$ is infinite, where Z is the centre of Δ.*
(III) *D has characteristic* 0.
(IV) *D is algebraic over the prime subfield.*

Proof. (I) Let $B = \Delta \cap A$, and let $H_B = H(B) \cap A^*$, $H_\Delta = H(\Delta) \cap A^*$. It is easily verified that $H_B \supseteq H_\Delta$. Since $B \lneq A$, and since B is not contained in the centre of A, H_B, and *a fortiori* H_Δ, has infinite index in A^*. This completes the proof of (I).

(II) Since $A' \cap \Delta \neq \Delta$, and since $\Delta \cap A \neq A$, one can choose $d \in \Delta$, $d \notin A'$, and $v \in A$, $v \notin \Delta$ such that $vd \neq dv$. Now $d' \cap \Delta \cap A$ contains $Z \cap A$. By Proposition 4 the sequence $\{(v + c)\Delta(v + c)^{-1}\}$ is infinite, $c \in Z \cap A$. This completes the proof of (II).

(III)-(IV). Let P denote the prime subfield of D. If D has characteristic 0, then P is infinite, and so is $Z \cap A$. Hence (II) applies. If D is algebraic over P, then Jacobson's theorem shows that P must be infinite.

COROLLARY 2. *Let D be a non-commutative division ring, and let F be a division subring whose centralizer F' is not a field. Let d be any element of F' not contained in its centre. Let R be any division subring of F, and let $\Delta = R(d)$ denote the division subring generated by R and d. Then there exist infinitely many different $x\Delta x^{-1}$ with $x \in F'$.*

Proof. Let $A = F'$. It is clear that (1) of Corollary 1 holds inasmuch as Δ is contained in the centralizer d' of d, whereas A is not. Moreover, since $d \in \Delta \cap A$, it follows that $\Delta \cap A$ is not contained in the centre of A. Thus (I) and (2) of Corollary 1 hold, so that its conclusion applies.

It is an interesting consequence of this result that the extension D/F of the corollary possesses infinitely many intermediate division rings $x\Delta x^{-1}$ in the case $R = F$. That the hypothesis on F' is necessary in some cases for this situation to arise can be seen as follows: Let F be a division subring of D containing C, and having finite dimension over C. It is known (**10**, p. 165) that there is a $1 - 1$ correspondence between intermediate division subrings of F/C and those of D/F', and that $F'' = F$. Now suppose that

F' is a field. Then, since $F \supseteq F'$, F' has finite degree over C. If further we assume that F'/C is separable, then this extension contains only finitely many intermediate fields. Then D/F contains only finitely many intermediate division rings.

The Cartan-Brauer-Hua theorem has been generalized extensively to simple and other rings **(1, 2, 6, 14)**. I have obtained an analogue of Theorem 3 for these rings, and this has been announced in **(5)**. The new results in **(5)** neither depend upon, nor contain, the results of the present paper.

References

1. S. A. Amitsur, *Invariant submodules of simple rings*, Proc. Amer. Math. Soc., *7* (1956), 987–989.

2. W. E. Baxter, *Lie simplicity of a special class of associative rings*, Proc. Amer. Math. Soc., *7* (1956), 855–863.

3. R. Brauer, *On a theorem of H. Cartan*, Bull. Amer. Math. Soc., *55* (1949), 619–620.

4. H. Cartan, *Théorie de Galois pour les corps non commutatif*, Ann. Ecole Norm. Sup., *64* (1947), 59–77.

5. C. C. Faith, *Concerning non-invariant submodules of simple, matrix, and local matrix rings*, Notices Amer. Math. Soc., *5* (1958), 372.

6. A. Hattori and G. Toyoda, *On the multiplicative group of simple algebras*, J. Math. Soc. Japan, *4* (1954), 262–265.

7. I. N. Herstein, *Conjugates in division rings*, Bull. Amer. Math. Soc., *7* (1956), 1021–1022.

8. L. K. Hua, *Some properties of a sfield*, Proc. Nat. Acad. Sci., *35* (1949), 533–537.

9. N. Jacobson, *Structure theory for algebraic algebras of bounded degrees*, Ann. Math., *46* (1945), 695–707.

10. ———, *Structure of rings*, Amer. Math. Soc. Colloquim Publications, *37* (New York, 1956).

11. F. Kasch, *Eine Bemerkung ueber innere Automorphismen*, Math. J. Okayama University, *6*, (1957), 131–133.

12. T. Nagahara, *On generating elements of Galois extensions of division rings*, Math. J. Okayama Univ., *6* (1957), 182.

13. N. Nobusawa, *On compact Galois groups of division rings*, Osaka Math. J., *8* (1956), 43–50.

14. A. Rosenberg, *The Cartan-Brauer-Hua theorem for matrix and local matrix rings*, Proc. Amer. Math. Soc., *7* (1956), 891–898.

15. W. R. Scott, *On the multiplicative group of a division ring*, Proc. Amer. Math. Soc., *8* (1957), 305.

16. H. Tominaga, *A note on conjugates*, Math. J. Okayama Univ., *7* (1957), 75–76.

17. J. H. M. Wedderburn, *A theorem on finite algebras*, Trans. Amer. Math. Soc., *6* (1905), 349–352.

The Pennsylvania State University