A THEOREM ON DIVISION RINGS

IRVING KAPLANSKY

THE object of this note is to prove the following theorem.

THEOREM. *Let A be a division ring with centre Z, and suppose that for every x in A, some power (depending on x) is in Z: $x^{n(x)} \in Z$. Then A is commutative.*

This theorem contains as special cases three previously known results.

1. It includes Wedderburn's theorem that any finite division ring is commutative, and the generalization by Jacobson [3, Theorem 8] asserting that any algebraic division algebra over a finite field is commutative; for in such an algebra every non-zero element has some power equal to 1.

2. It includes a theorem of Emmy Noether, as generalized by Jacobson [3, Lemma 2], stating that any non-commutative algebraic division algebra contains an element separable over the centre; for otherwise a suitable p^mth power of every element would lie in the centre.

3. Hua [1, Theorem 7] has proved the special case of the theorem where the power n is independent of x, and the characteristic is at least n.

Although our theorem generalizes the two cited theorems of Jacobson, we are not giving a new proof of these theorems. In fact, we shall prove a preliminary lemma on fields which reduces the problem precisely to these two theorems.

LEMMA. *Let K be a field and L an extension of K, $L \neq K$, with the property that for every x in L, some power (the power depending on x) lies in K. Then L has prime characteristic, and it is either purely inseparable over K, or algebraic over its prime subfield.*

Proof. If L is indeed purely inseparable over K, there is of course nothing to prove. So suppose L contains an element y, y non $\in K$, which is separable over K. By a suitable isomorphism leaving K elementwise fixed, y can be sent into an element $z \neq y$ (of course z need not be in L). We have, say, $y^r \in K$ and and so $z^r = y^r$, whence $z = \epsilon y$ with $\epsilon^r = 1$. Suppose $(1 + y)^s \in K$; then similarly $1 + z = \eta(1 + y)$ with $\eta^s = 1$. We cannot have $\epsilon = \eta$, for then $\epsilon = 1$, $z = y$. So we may solve for y:

$$y = (1 - \eta)(\eta - \epsilon)^{-1}. \tag{1}$$

We see that y is algebraic over the prime subfield P of K. If k is any element of K, we can repeat this argument with $k + y$ instead of y, and thus deduce

Received September 26, 1950.

that $k + y$, and hence k, is algebraic over P. In short, K is algebraic over P. If P has prime characteristic, we have reached the other possibility stated in the conclusion of the lemma, so it remains only to exclude the possibility that P has characteristic 0 (which means that it is the field of rational numbers). This we do as follows. For any integer i we have an expression like (1) for $y + i$:

$$y + i = (1 - \eta_i)(\eta_i - \epsilon_i)^{-1}. \tag{2}$$

Moreover, the definition of η_i and ϵ_i shows that they lie in the normal field, say Q, generated by y over P. But Q, being a finite-dimensional extension of P, contains only a finite number of roots of unity. This leaves us powerless to account for the infinite number of elements in (2).

Proof of the theorem. If $A \neq Z$, choose any element x not in Z, and let L be the field generated by Z and x. Then the hypothesis of the lemma is fulfilled (with Z playing the role of K). The possibility that Z has prime characteristic and is algebraic over its prime subfield is ruled out by the first theorem of Jacobson cited above. So it must be true that L is purely inseparable over Z. This is the case for every x, and we contradict the second theorem of Jacobson.

Theorem 7 of [1] actually states that a non-commutative division ring is generated by its nth powers. Our theorem can be given a corresponding extension as follows. For every x of a non-commutative division ring A, let there be given a positive integer $n(x)$ such that $n(x) = n(a^{-1}xa)$ for all $a \neq 0$; let B be the division subring generated by the elements $x^{n(x)}$; then $B = A$. For B is invariant under all inner automorphisms, and if $B \neq A$ then by the theorem of Cartan-Brauer-Hua [1, Theorem 2] B is contained in the centre of A, contradicting the above theorem.

In conclusion we discuss two possibilities of generalization. In the first place we might consider relaxing the requirement that A be a division ring. In fact, our theorem remains correct if we merely assume that A is semi-simple in the sense of Jacobson [2]. The manœuvre for proving this has become fairly standard since the appearance of Jacobson's paper. If P is a primitive ideal in A, our hypothesis is inherited by A/P; if we prove that each A/P is commutative we will know that A is commutative, and so we need only consider the case where A is primitive. We represent A as a dense ring of linear transformations in a vector space V over a division ring. We now in effect check our theorem for two-by-two matrices. In detail: if V is more than one-dimensional, let α and β be linearly independent vectors, and let x be an element of A sending α into itself and annihilating β. It is impossible for any power of x to be in the centre. So V is one-dimensional, and we are back to the division ring case of the theorem.

Another path along which to proceed is to have a polynomial more general than x^n. We shall not attempt more than the case where n is independent of

x, although it would be interesting to invent plausible "one-parameter families" generalizing $\{x^n\}$. We assume then that there exists a polynomial f with coefficients in Z (we can suppose it has no constant term) such that $f(x) \in Z$ for every x. Since A then satisfies the identity $f(x)y - yf(x) = 0$, it follows forthwith from [4, Theorem 1] that A is finite-dimensional over Z. But as a matter of fact it is again true that A is commutative. For suppose f has smallest possible degree among polynomials with $f(x) \in Z$. We can suppose there is an element u in Z no power of which is 1 (otherwise Z would be of prime characteristic and algebraic over its prime field, etc.). Consider the polynomial $g(x) = f(x) - u^n f(xu^{-1})$, n being the degree of f; the degree of g is less than n, and it again has the property $g(x) \in Z$ for every x. The only way out is for g to be identically zero, which means $f(x) = x^n$, and we are back to the old case.

One must step cautiously in attempting to generalize this last result beyond division rings: observe that the ring of two-by-two matrices over $GF(2)$ satisfies the identity $x^8 = x^2$.

References

[1] L. K. Hua, *Some properties of a sfield*, Proc. Nat. Acad. Sci. USA, vol. 35 (1949), 533-537.

[2] N. Jacobson, *The radical and semi-simplicity for arbitrary rings*, Amer. J. of Math., vol. 67 (1945), 300-320.

[3] ——— *Structure theory for algebraic algebras of bounded degree*, Ann. of Math., vol. 46 (1945), 695-707.

[4] I. Kaplansky, *Rings with a polynomial identity*, Bull. Amer. Math. Soc., vol. 54 (1948), 575-580.

University of Chicago

https://doi.org/10.4153/CJM-1951-033-7 Published online by Cambridge University Press