

Title	On a theorem of Kaplansky
Author(s)	Ikeda, Masatoshi
Citation	Osaka Mathematical Journal. 1952, 4(2), p. 235-240
Version Type	VoR
URL	<a href="https://doi.org/10.18910/4708">https://doi.org/10.18910/4708</a>
rights	
Note	

*Osaka University Knowledge Archive : OUKA*

<https://ir.library.osaka-u.ac.jp/>

Osaka University

## *On a Theorem of Kaplansky*

By Masatoshi IKEDA

I. Kaplansky has proved an interesting theorem: any division ring is commutative if, for every element  $x$ , some power  $x^{n(x)}$  is in the centre.<sup>1)</sup> As special cases this theorem contains the well-known theorem of Wedderburn of finite division rings as well as its generalization due to Jacobson.<sup>2)</sup> On the other hand I. N. Herstein has proved that any ring in which  $x^n - x$  is in its centre for every element  $x$  and for a fixed integer  $n > 1$ , is commutative. Moreover he has conjectured that the rings in which  $x^{n(x)} - x$  is in the centre for every element  $x$  and for an integer  $n(x)$  (depending on  $x$  and larger than 1) may be commutative.<sup>3)</sup>

In this note we shall prove a generalization of Kaplansky's theorem and, as its applications, we shall generalize a result of Hua<sup>4)</sup> and show that Herstein's conjecture is valid for semi-simple rings in the sense of Jacobson.

**Theorem.** *Let  $D$  be a division ring with centre  $Z$  and let  $c_i (i = 0, 1, \dots, r)$  be  $r+1$  fixed non-zero elements in the prime subfield of  $D$ . If, for every element  $x$  in  $D$ , there are integers  $n_0(x) > n_1(x) > \dots > n_r(x) > 0$  such that i)  $\sum_{i=0}^r c_i x^{n_i(x)}$  is in  $Z$  and ii)  $n_1(x)$  is smaller than an integer  $M$  (not depending on  $x$ ), then  $D$  is commutative.*

Here, if we put  $r = 0$ , we have Kaplansky's theorem. Hence we prove only the case  $r > 0$ .

To prove our theorem, it is sufficient according to Kaplansky to prove the following<sup>5)</sup>

**Lemma.** *Let  $K$  be a field,  $L (\neq K)$  an extension of  $K$  and let  $c_i (i = 0, 1, \dots, r)$  be  $r+1$  fixed non-zero elements in the prime subfield of  $L$ . If, for every element  $x$  in  $L$ , there are integers  $n_0(x) > n_1(x) > \dots$*

---

1) Cf. Kaplansky [5].

2) Cf. Jacobson [4] Th. 8.

3) Cf. Herstein [1].

4) Cf. Hua [2] Th. 7.

5) Cf. Kaplansky [5].

$n_r(x) > 0$  such that (i)  $\sum_{i=0}^r c_i x^{n_i(x)}$  is in  $K$  and (ii)  $n_1(x)$  is smaller than a fixed integer  $M$ , then  $L$  has prime characteristic and is either purely inseparable over  $K$  or algebraic over its prime subfield.

Proof. For every element  $x$ ,  $m_0(x) > m_1(x) > \dots > m_r(x) > 0$  denote the system of  $r+1$  integers satisfying (i) such that  $m_1(x)$  is the minimum of  $n_1(x)$ . Hence  $m_1(x)$  is smaller than  $M$  by (ii).

(a) First we prove that  $L$  has prime characteristic.

Assume that  $L$  has characteristic zero. Then the prime subfield  $P$  of  $L$  is the field of rational numbers. Therefore, we may assume that  $c_i (i=0, \dots, r)$  are  $r+1$  fixed non-zero integers. Now let  $a$  be an element in  $L$  but not in  $K$ . Then  $a$  can be sent into an element  $b (\neq a)$  by a suitable isomorphism  $\theta$  which leaves  $K$  elementwise fixed. Here  $b$  need not be in  $L$ . By  $\theta$ ,  $a^{-1}$  and  $i(a+1)$ ,  $i$  an arbitrary integer, are sent into  $b^{-1}$  and  $i(b+1)$  respectively. Since  $\sum_{\kappa=0}^r c_\kappa (a^{-1})^{m_\kappa(a^{-1})}$  and  $\sum_{\kappa=0}^r c_\kappa (i(a+1))^{m_\kappa(i(a+1))}$  are in  $K$ , we have readily

$$(1) \quad \sum_{\kappa=0}^r c_\kappa (a^{-1})^{m_\kappa(a^{-1})} - \sum_{\kappa=0}^r c_\kappa (b^{-1})^{m_\kappa(a^{-1})} = 0$$

and

$$(2) \quad \sum_{\kappa=0}^r c_\kappa \left\{ (i(b+1))^{m_\kappa(i(a+1))} - (i(a+1))^{m_\kappa(i(a+1))} \right\} = 0.$$

Multiplying (1) by  $(ab)^{m_0(a^{-1})}$ , we have

$$(3) \quad \left( \sum_{\kappa=0}^r c_\kappa a^{m_0(a^{-1}) - m_\kappa(a^{-1})} \right) b^{m_0(a^{-1})} - \sum_{\kappa=0}^r c_\kappa a^{m_0(a^{-1})} b^{m_0(a^{-1}) - m_\kappa(a^{-1})} = 0.$$

Dividing (2) by  $i^{m_r(i(a+1))}$ , we have

$$(4) \quad \sum_{\kappa=0}^r c_\kappa i^{m_\kappa(i(a+1)) - m_r(i(a+1))} \left\{ (b+1)^{m_\kappa(i(a+1))} - (a+1)^{m_\kappa(i(a+1))} \right\} = 0.$$

Since  $b-a \neq 0$ , dividing (4) by  $(b+1) - (a+1)$ , we have

$$(5) \quad c_0 i^{m_0(i(a+1)) - m_r(i(a+1))} b^{m_0(i(a+1)) - 1} + \dots \text{ terms with powers of } b \\ \dots + \sum_{\kappa=0}^r c_\kappa i^{m_\kappa(i(a+1)) - m_r(i(a+1))} \left( \sum_{\lambda=0}^{m_\kappa(i(a+1)) - 1} (a+1)^\lambda \right) = 0.$$



wise fixed. By  $\theta$ ,  $a^{-1}$  and  $z(a+1)$  are set into  $b^{-1}$  and  $z(b+1)$  respectively. In the same way as in (a), we have

$$(6) \quad \left( \sum_{\kappa=0}^r c_{\kappa} a^{m_0(a^{-1})-m_{\kappa}(a^{-1})} \right) b^{m_0(a^{-1})} - \sum_{\kappa=0}^r c_{\kappa} a^{m_0(a^{-1})} b^{m_0(a^{-1})-m_{\kappa}(a^{-1})} = 0$$

and

$$(7) \quad c_0 z^{m_0(z(a+1))-m_r(z(a+1))} b^{m_0(z(a+1))-1} + \dots \text{ terms with powers of } b \\ \dots + \sum_{\kappa=0}^r c_{\kappa} z^{m_{\kappa}(z(a+1))-m_r(z(a+1))} \left( \sum_{\lambda=0}^{m_{\kappa}(z(a+1))-1} (a+1)^{\lambda} \right) = 0.$$

Eliminating  $b$  from (6) and (7), we have an equation  $F(X) = 0$  satisfied by  $a$ . It is easy to see that the coefficients of  $F(X)$  are in  $P[z]$  and the constant term of  $F(X)$  is a product of suitable powers of  $c_0$  and  $c(z) = \sum_{\kappa=0}^r c_{\kappa} m_{\kappa}(z(a+1)) z^{m_{\kappa}(z(a+1))-m_r(z(a+1))}$ . Here we may assume that  $m_0(x), m_1(x), \dots, m_r(x)$  are not all congruent to zero mod.  $p$  for every separable element  $x$  over  $K$ . For, if  $m_i(x) = p^{\mu} m_i'(x)$  for  $i = 0, \dots, r$ , then  $\sum_{i=0}^r c_i x^{m_i(x)} = (\sum_{i=0}^r c_i x^{m_i'(x)}) p^{\mu}$  is in  $K$ . Since  $x$  is separable over  $K$ ,  $\sum_{i=0}^r c_i x^{m_i'(x)}$  is separable over  $K$ , so  $\sum_{i=0}^r c_i x^{m_i'(x)}$  is in  $K$ . This contradicts the minimality of  $m_1(x)$ . Therefore  $c(z)$  is not zero, since  $z$  is transcendental over  $P$ . Therefore  $F(X) = 0$  is a non-trivial equation and consequently  $a$  is algebraic over  $P(z)$ . Furthermore the domain of integrity  $P[z]$  of  $P(z)$  is a unique factorization domain. Let  $g(X) \equiv \sum_{i=0}^N \alpha_i X^i$  be a primitive irreducible polynomial in  $P[z][X]$  satisfied by  $a$ . Now assume that  $\alpha_0$  is not in  $P$  and  $\pi$  is a prime divisor of  $\alpha_0$ . Since  $\pi(\pi^M a + 1)$  is sent into  $\pi(\pi^M b + 1)$  by  $\theta$ ,

$$\sum_{\kappa=0}^r c_{\kappa} \left\{ (\pi(\pi^M b + 1))^{m_{\kappa}(\pi(\pi^M a + 1))} - (\pi(\pi^M a + 1))^{m_{\kappa}(\pi(\pi^M a + 1))} \right\} = 0.$$

Dividing this by  $\pi^{m_r(\pi(\pi^M a + 1))} \{(\pi^M b + 1) - (\pi^M a + 1)\}$ , we have the relation :

$$c_0 \pi^{m_0(\pi(\pi^M a + 1)) - m_r(\pi(\pi^M a + 1))} (\pi^M b)^{m_0(\pi(\pi^M a + 1)) - 1} + \dots \text{ terms with powers of } b \\ \dots + \left\{ \dots \text{ terms with powers of } a \dots \right. \\ \left. + \sum_{\kappa=0}^r c_{\kappa} m_{\kappa}(\pi(\pi^M a + 1)) \pi^{m_{\kappa}(\pi(\pi^M a + 1)) - m_r(\pi(\pi^M a + 1))} \right\} = 0.$$

In this relation, terms with powers of  $b$  or  $a$  are divisible by  $\pi^M$ . Hence if  $m_i(\pi(\pi^M a + 1)) \equiv 0(p)$  for  $i > s$  and  $m_s(\pi(\pi^M a + 1)) \not\equiv 0(p)$  for an  $s \neq 0$ , we divide the above relation by  $\pi^{m_s(\pi(\pi^M a + 1)) - m_r(\pi(\pi^M a + 1))}$ . Now we eliminate  $b$  from the relation thus obtained and (6). Then we have an equation  $G(X) = 0$  satisfied by  $a$  where the constant term  $G(0)$  of  $G(X)$  is either a product of powers of  $c_0$  and  $\sum_{\kappa=0}^s c_{\kappa} m_{\kappa}(\pi(\pi^M a + 1)) \pi^{m_{\kappa}(\pi(\pi^M a + 1)) - m_s(\pi(\pi^M a + 1))}$  for some  $s \neq 0$  or a product of powers of  $c_0$

and  $c_0 m_0 (\pi (\pi^M a + 1)) \pi^{m_0 (\pi (\pi^M a + 1)) - m_r (\pi (\pi^M a + 1))}$ . It is easy to see that the coefficients of  $G(X)$  are in  $P[z]$ . Therefore,  $\alpha_0$  is a divisor of the constant term  $G(0)$  of  $G(X)$  and consequently  $\pi$  is a divisor of  $G(0)$ . If  $G(0)$  is a product of powers of  $c_0$  and  $\sum_{\kappa=0}^s c_\kappa m_\kappa (\pi (\pi^M a + 1)) \pi^{m_\kappa (\pi (\pi^M a + 1)) - m_s (\pi (\pi^M a + 1))}$  for an  $s \neq 0$ , then a product of powers of  $c_0 \neq 0$  and  $c_s m_s (\pi (\pi^M a + 1)) \neq 0$  is divisible by  $\pi$ . This is a contradiction. Therefore,  $G(0)$  is a product of a power of  $\pi$  and an element in  $P$ . Thus we see that the constant term of a primitive irreducible polynomial in  $P[z][X]$  satisfied by a separable element is either in  $P$  or a product of a power of an irreducible polynomial in  $P[z]$  and an element in  $P$ .

Now if we take  $a + H(z)$ ,  $H(z)$  an arbitrary polynomial in  $P[z]$ , in place of  $a$ , then the constant term of a primitive irreducible polynomial in  $P[z][X]$  satisfied by  $a + H(z)$  must be either in  $P$  or a product of a power of an irreducible polynomial in  $P[z]$  and an element in  $P$ . Now we take  $z^i$  as  $H(z)$ , where  $i$  is an integer larger than the degrees of  $\alpha_\kappa (\kappa = 0, \dots, N)$ . Then  $a + z^i$  satisfies  $g(X - z^i)$  which is a primitive irreducible polynomial in  $P[z][X]$ . Obviously the constant term  $g(-z^i)$  of  $g(X - z^i)$  is not in  $P$ . Hence  $g(-z^i) = \beta h(z)^i$ , where  $h(z)$  is an irreducible polynomial in  $P[z]$  and  $\beta$  is an element in  $P$ . Take  $z^i + h(z)^t$  as  $H(z)$ , where  $t$  is an integer larger than  $l$ . Then the constant term  $g(-(z^i + h(z)^t))$  of  $g(X - (z^i + h(z)^t))$  which is a primitive irreducible polynomial in  $P[z][X]$  satisfied by  $a + z^i + h(z)^t$ , is not in  $P$  and is divisible by  $h(z)$ . Therefore,  $g(-(z^i + h(z)^t))$  must be a product of a power of  $h(z)$  and an element in  $P$ . But this is impossible. Thus we have a contradiction. Therefore  $K$  is algebraic over  $P$  and  $L$  is algebraic over  $P$ .

**Corollary.** *Let  $D$  be a division ring with centre  $Z$  and let  $f(X)$  be a fixed polynomial of degree  $n$  whose coefficients are in the prime subfield of  $D$ . If  $x^{n(x)} + f(x)$  is in  $Z$  for every  $x$  in  $D$  and for an integer  $n(x)$  (depending on  $x$  and larger than  $n$ ), then  $D$  is commutative.*

**Remark.** It is probably true that we can drop the condition (ii) and take the assumption that  $c_i (i = 0, \dots, r)$  are in  $Z$ , in place of the assumption that  $c_i$  are in the prime subfield. But this is still an open question.

As the first application of our theorem, we shall generalize a result of Hua<sup>6)</sup> as follows:

**Theorem.** *Any non-commutative division ring  $D$  is generated by*

---

6) Cf. Hua [2] Th. 7.

elements of the form  $\sum_{i=0}^r c_i x^{n_i(x)}$ , where  $c_i (i=0, 1, \dots, r)$  are the fixed non-zero elements in the prime subfield of  $D$  and  $n_0(x) > n_1(x) > \dots > n_r(x) > 0$  are intergers such that  $n_i(x) = n_i(a^{-1}xa)$  for all  $a \neq 0$  in  $D$  and  $n_1(x)$  is smaller than a fixed integer  $M$ .

Proof. Let  $D'$  be the division ring generated by the elements  $\sum_{i=0}^r c_i x^{n_i(x)}$ , then  $D'$  is invariant under inner automorphisms of  $D$ . If  $D' \neq D$ , then  $D'$  is contained in the centre of  $D$ , by a result of Hua.<sup>7)</sup> Then  $D$  is commutative. This is a contradiction. Therefore  $D' = D$ .

As the second application of our theorem, we show that Herstein's conjecture is valid for semi-simple rings in the sense of Jacobson:

**Theorem.** *Let  $A$  be a semi-simple ring with centre  $Z$  and let  $c$  be an integer. If there is an integer  $n(x)$  larger than 1 for every element  $x$  and  $x^{n(x)} + cx \in Z$ , then  $A$  is commutative.*

Proof. Since  $A$  is semi-simple,  $A$  is a subdirect sum of primitive rings.<sup>8)</sup> Since our assumption is valid for residue class rings of  $A$ , it is sufficient to prove our assertion in the case where  $A$  is a primitive ring. Any primitive ring is isomorphic to a dense ring  $R$  of linear transformations in a vector space  $V$  over a division ring  $D$ .<sup>9)</sup> Let  $V$  be more than one-dimensional and let  $\alpha$  and  $\beta$  be two linear independent vectors. Since  $R$  is dense, there is an element  $a$  in  $R$  such that  $\alpha a = \beta$  and  $\beta a = 0$ . Then, for any integer  $n > 1$ ,  $\alpha(a^n + ca) = c\beta$  and  $\beta(a^n + ca) = 0$ . If  $c\beta = 0$ , then  $c\gamma = 0$  for all vectors in  $V$ . Hence  $cb = 0$  for all  $b$  in  $R$ , so  $cx = 0$  for all  $x$  in  $A$ . But this case was proved by Kaplansky.<sup>10)</sup> If  $c\beta \neq 0$ , then  $a^n + ca$  is not in the centre of  $R$ . For,  $a^n + ca$  does not commute with the linear transformation in  $R$  such that  $\alpha \rightarrow \beta$  and  $\beta \rightarrow \alpha$ . Hence  $V$  is one-dimensional, so  $R$  is a division ring. Then, by our theorem,  $R$  is commutative.

Putting  $c = -1$ , we see that Herstein's conjecture is valid for semi-simple rings.

(Received March, 15, 1952)

### References

- [1] I. N. Herstein: A generalization of a theorem of Jacobson, Amer. J. of Math. 73 (1951).
- [2] L. K. Hua: Some properties of a sfield, Proc. Nat. Acad. Sci. U. S. A., 35 (1949).
- [3] N. Jacobson: The radical and semi-simplicity for arbitrary rings, Amer. J. of Math. 67 (1945).
- [4] —: Structure theory for algebraic algebras of bounded degree, Ann. of Math. 46 (1945).
- [5] I. Kaplansky: A theorem on division rings, Canadian J. Math. 3 (1951).

7) Cf. Hua [2] Th. 1.

8) Cf. Jacobson [3].

9) Cf. Jacobson [3].

10) Cf. Kaplansky [5].