

# NORMAL DIVISION ALGEBRAS OVER A MODULAR FIELD\*

BY

A. ADRIAN ALBERT

1. **Introduction.** Let  $\phi(\omega) = 0$  have coefficients in a modular field  $F$  of characteristic  $p$  and be irreducible in  $F$ . Then  $\phi(\omega) = 0$  and the field  $F(x)$  generated by any one of its roots  $x$  are called separable or inseparable according as  $\phi(\omega) = 0$  has not or has multiple roots. It is well known<sup>†</sup> that if  $\phi(\omega) = 0$  is inseparable, then

$$\phi(\omega) \equiv \sum_i \alpha_i \omega^{p^i} \quad (\alpha_i \text{ in } F),$$

and that there exist inseparable extensions  $F(x)$  of  $F$  if and only if some quantity  $\alpha$  of  $F$  is not the  $p$ th power of any quantity of  $F$ .

An infinite field  $F$  is called perfect if either  $F$  is non-modular or every quantity of  $F$  has the form  $\beta^p$  where  $p$  is the characteristic of  $F$  and  $\beta$  is in  $F$ . In any consideration of normal division algebras  $D$  over  $F$  the property that  $F$  is perfect is used only when we consider quantities of  $D$  and the minimum equations of these quantities. But if the degree  $n$  of  $D$  is not divisible by the characteristic  $p$  of  $F$ , then the assumption that  $F$  is perfect evidently *has no value* and is a needless extremely strong restriction on  $F$ .

In most of the papers on the structure of normal division algebras written recently in Germany<sup>‡</sup>, the assumption has been that  $F$  is perfect. But I shall prove here that if  $F$  is perfect of characteristic  $p$ , then  $n$  is not divisible by  $p$ . Hence it is now necessary to consider algebras of degree  $p^e$  over  $F$  of characteristic  $p$ , where  $F$  is *not perfect*.

I shall give here a brief discussion of the validity of the major results on algebras over non-modular fields when  $F$  is assumed to be merely *any infinite field*. Moreover, I shall determine all normal division algebras of degree two over  $F$  of characteristic two, of degree three over  $F$  of characteristic three. §

2. **The existence of a maximal separable sub-field of  $A$ .** Let  $A$  be any normal division algebra of degree  $n$  over any field  $F$ , and let

$$(1) \quad \underline{\hspace{10em}} \quad u_1, \dots, u_m \quad (m = n^2)$$

\* Presented to the Society, December 1, 1933; received by the editors November 22, 1933.

† Cf. B. L. van der Waerden's *Moderne Algebra* for the theory of modular fields.

‡ In particular the papers by R. Brauer.

§ I have also completed a determination of all normal division algebras of degree four over  $F$  of characteristic two and have offered this more complicated determination for publication in the *American Journal of Mathematics*.

be a basis of  $F$ . Then it is known\* that if  $K$  is an algebraically closed extension of  $F$ , the algebra  $A_K$  over  $K$  is a total matrix algebra  $M$ . Let

$$(2) \quad e_{\alpha\beta} = v_j = \sum_{i=1}^m \mu_{ji} u_i, \quad u_i = \sum_{j=1}^m \lambda_{ij} v_j \quad (i, j = 1, \dots, m).$$

where  $\alpha, \beta = 1, \dots, n$  and  $j = (\alpha - 1)n + \beta$ . The quantities  $\lambda_{ij}, \mu_{ji}$  are then in  $K$  and  $e_{\alpha\beta}$  corresponds to an  $n$ -rowed matrix with unity in the  $\alpha$ th row and  $\beta$ th column and zero elsewhere.

The rank equation of  $A$  is the minimum equation of the quantity  $x = \sum_{i=1}^m \xi_i u_i$  where the  $\xi_i$  are independent variables. Then it is known that we have the result†

**THEOREM 1.** *The rank equation of  $A$  is the characteristic equation of the matrix*

$$(3) \quad \|\zeta_{\alpha\beta}\| \quad (\alpha, \beta = 1, \dots, n)$$

where

$$(4) \quad \zeta_{\alpha\beta} = \sum_{i=1}^m \mu_{ji} \xi_i, \quad j = (\alpha - 1)n + \beta.$$

*This equation has coefficients in  $L = F(\xi_1, \dots, \xi_m)$  and is irreducible in  $L$ .*

E. Noether and G. Köthe have given proofs‡ of

**THEOREM 2.** *Algebra  $A$  of degree  $n$  over an infinite field  $F$  has separable sub-fields  $F(x)$  of degree  $n$ .*

Their proofs are not at all elementary while my very much earlier simpler proof§ for the case where  $F$  is non-modular holds and uses only Theorem 1. We may in fact prove

**THEOREM 3.** *The sub-fields  $F(x)$  of Theorem 2 may be so chosen that  $x$  satisfies*

$$\omega^n + \lambda_1 \omega^{n-1} + \dots + \lambda_n = 0 \quad (\lambda_1 \neq 0, \lambda_i \text{ in } F).$$

For the rank equation  $R(\omega; \xi_1, \dots, \xi_m)$  is satisfied by any matrix (3) when the corresponding values of  $\xi_1, \dots, \xi_m$  are given. Let  $\beta_1, \dots, \beta_n$  be  $n$  quantities of the infinite field  $F$  so chosen that  $\beta_1, \dots, \beta_{n-1}$  are distinct

\* Cf. van der Waerden's *Algebra*, II, p. 176.

† For proof of Theorem 1, see L. E. Dickson's *Algebren und ihre Zahlentheorie*, pp. 259-262. Dickson's proof uses only (2) and is an immediate consequence of his Theorem 5 without the argument of the unnecessary section 132.

‡ *Journal für Mathematik*, vol. 166 (1932), pp. 182-184, for Köthe's proof, and *Mathematische Zeitschrift*, vol. 37 (1933), pp. 514-541, p. 535 for Noether's proof.

§ *Bulletin of the American Mathematical Society*, vol. 36 (1930), pp. 649-650.

and  $\beta_n \neq \beta_i, -(\beta_1 + \dots + \beta_{n-1})$  for  $i = 1, \dots, n-1$ . Then we solve (4) for the  $\xi_i$  and have proved the existence of  $\xi_{i0}$  in  $K$  for which  $R(\omega; \xi_{10}, \dots, \xi_{m0}) = 0$  has distinct roots and the coefficient  $\lambda_i(\xi_{10}, \dots, \xi_{m0})$  of  $\omega^{n-1}$  is not zero. Let  $D(\xi_1, \dots, \xi_n)$  be the discriminant of  $R(\omega; \xi_1, \dots, \xi_m)$ . Then

$$D(\xi_{10}, \dots, \xi_{m0})\lambda(\xi_{10}, \dots, \xi_{m0}) \neq 0,$$

so that  $D(\xi_1, \dots, \xi_m) \cdot \lambda(\xi_1, \dots, \xi_m) \neq 0$ . But then there exist values  $\xi_{i1}$  of  $\xi_1, \dots, \xi_m$  in  $F$  such that  $D(\xi_{11}, \dots, \xi_{m1}) \cdot \lambda(\xi_{11}, \dots, \xi_{m1}) \neq 0$  and hence such that the rank equation of  $A$  for  $x = \sum \xi_{i1} u_i$  has distinct roots and coefficient of  $\omega^{n-1}$  not zero.

The characteristic equation of the corresponding matrix (3) is an exact power of the minimum equation of  $x$  since  $x$  in the division algebra  $A$  has irreducible minimum equation. Since the characteristic equation has been shown to have distinct roots, it is the minimum equation of  $x$  and we have proved Theorems 2, 3.

**3. Known theorems.** In this section we shall state certain well known theorems on algebras over non-modular fields which hold for any infinite field. We first have

**THEOREM 4.** *Let  $D$  be a normal division algebra of degree  $n$  over  $F$ , and let  $Z$  be equivalent to any sub-field of  $D$  of degree  $n$ . Then  $D \times Z = D_Z$  is a total matric algebra.*

Wedderburn's proof\* of this theorem holds for an arbitrary field. As an immediate consequence of Theorem 2 we have

**THEOREM 5.** *There exist separable splitting fields of  $D$  of degree  $n$ .*

We of course say that  $Z$  is a splitting field of  $D$  if  $D_Z$  is a total matric algebra.

We also have Wedderburn's theorems:

**THEOREM† 6.** *Let  $A$  be a normal simple algebra of degree  $n^2$  over  $F$ . Then  $A = M \times D \sim D$ , where  $M$  is a total matric algebra and  $D$  is a normal division algebra whose degree is the index of  $A$ . Moreover  $D$  and  $M$  are uniquely determined apart from an interior automorphism of  $A$ .*

**THEOREM‡ 7.** *Let  $B$  be a normal simple algebra over  $F$  contained in any algebra  $A$  over  $F$  with the same modulus as  $B$ . Then  $A = B \times C$  where  $C$  also has the same modulus as  $A$ .*

\* For Theorems 10, 12, see Wedderburn's paper in these Transactions, vol. 22 (1921), pp. 129-135. The proof of Theorem 4 appears on p. 133 and the footnote to p. 134.

† Cf. L. E. Dickson's *Algebras*, p. 120.

‡ Proceedings of the Edinburgh Mathematical Society, vol. 25 (1906-07), pp. 1-3.

The proofs given by Wedderburn of the above Theorems 6, 7 also hold in view of Theorem 5. They may also be applied, as in the non-modular case, to give my

**INDEX REDUCTION THEOREM.\*** *Let  $D$  be a normal division algebra of degree (index)  $n$  over any infinite field  $F$ ,  $Z$  an algebraic field of degree  $r$  over  $F$ . Then the index of  $D_Z$  over  $Z$  is*

$$n' = n/s,$$

where the index reduction factor  $s$  divides  $r$ .

As a consequence we have the whole Brauer exponent theory as well as my

**THEOREM† 8.** *Let  $D$  be a normal division algebra of degree  $n$  over any infinite field  $F$ ,  $p$  a prime divisor of  $n$ . Then there exists a field  $Z$  of degree  $r$  over  $F$  such that*

$$D = M \times B \sim B \quad (M \text{ total matrix}),$$

where  $B$  is a cyclic division algebra of degree  $p$  over its centrum  $Z$ .

**THEOREM‡ 9.** *Let  $Z_0$  be in  $D$  so that the degree  $r$  of the field  $Z_0$  divides  $n$  and let  $Z$  be equivalent to  $Z_0$*

$$D_Z = M \times B,$$

as in the Index Reduction Theorem. Then the algebra  $B_0$  over  $Z_0$  of all quantities of  $D$  commutative with every quantity of  $Z_0$  is equivalent to  $B$  over  $Z$ .

We may indeed say that almost all of the recent general theory on normal division algebras holds when  $F$  is any infinite field. The determination theorems on algebras of degree 2, 3, 4 do not hold however. We shall give here a determination in the cases  $n=2, 3$ , and, in a later American Journal paper, the case  $n=4$ . We shall require

**THEOREM 10.** *Let  $D$  be a normal division algebra of degree  $n$  over  $F$ , and let  $x$  in  $D$  have  $\phi(\omega) = 0$  of degree  $v$  as its minimum equation. Then*

$$\phi(\omega) \equiv (\omega - x_r)(\omega - x_{r-1}) \cdots (\omega - x_2)(\omega - x),$$

where the  $v$  factors may be permuted cyclically.

**THEOREM§ 11.** *Every root  $y$  in  $D$  of  $\phi(\omega) = 0$  is a transform  $txt^{-1} = y$  of  $x$  by  $t$  in  $D$ .*

\* On direct products, these Transactions, vol. 33 (1931), pp. 690-711.

† For probably the best proof of Theorem 8 see (1), (2) on p. 725 of the joint paper by H. Hasse and myself in these Transactions, vol. 34 (1932), pp. 722-726.

‡ On normal simple algebras, these Transactions, vol. 34 (1932), pp. 620-625.

§ Cf. Annals of Mathematics, vol. 30 (1929), pp. 322-338, Theorem 12.

**THEOREM 12.** Let  $f(\omega) \equiv g(\omega) \cdot h(\omega)$  where  $f, g, h$  have coefficients in  $D$  and  $\omega$  is a scalar variable. Then if  $\omega - x$  is a right divisor of  $f(\omega)$ ,  $h(\omega) \equiv q(\omega) (\omega - x) + R$  where  $R \neq 0$  is in  $D$ , then  $\omega - RxR^{-1}$  is a right divisor of  $g(\omega)$ .

4. Algebras over perfect fields. We may now prove

**THEOREM 13.** Let  $D$  be a normal division algebra of degree  $n$  over a perfect modular field  $F$  of characteristic  $p$ . Then  $n$  is not divisible by  $p$ .

For by Theorem 8, if  $n$  is divisible by  $p$  then there exists an extension  $Z$  of finite degree over  $F$ , such that  $D \times Z = M \times B$  where  $B$  is a cyclic division algebra of degree  $p$  over  $F$ . But it is known\* that then  $Z$  is perfect. Moreover  $B = (X, S, \gamma)$  where  $X$  is cyclic of degree  $p$  over  $Z$  and with generating automorphism  $S$ ,  $\gamma$  in  $Z$  is not the norm  $N(f)$  of any  $f$  in  $X$ . But  $Z$  is perfect,  $\gamma = \delta^p = N(\delta)$ , a contradiction.

5. Algebras of degree two. Let  $D$  be a normal division algebra of degree two over an infinite field  $F$  of characteristic two. By Theorem 2, algebra  $D$  contains a separable quadratic field  $F(x)$ ,  $x^2 = \lambda x + \mu$  where  $\lambda \neq 0$ ,  $\mu \neq 0$  are in  $F$ . We let  $i = \lambda^{-1}x$  so that  $i^2 = \lambda^{-2}(\lambda x + \mu) = i + \alpha$  where  $\alpha = \mu\lambda^{-2} \neq 0$  is in  $F$ . The equation  $\omega^2 = \omega + \alpha$  is cyclic and in fact has the roots  $i, i+1$ . By Theorem 12 there exists a quantity  $j$  in  $D$  such that  $ji = (i+1)j$ . But then  $j^2i = ij^2$ . Since  $F(i)$  is a maximal sub-field of  $A$ , the quantity  $j^2$  is in  $F(i)$ . But  $F(j^2) < F(i)$  since  $jj^2 = j^2j$ , but  $ji \neq ij$ . Hence  $j^2 = \gamma$  in  $F$  and we have proved

**THEOREM 14.** Every normal division algebra  $D$  of degree two over  $F$  of characteristic 2 is a cyclic algebra

$$(1, i, j, ij), \quad i^2 = i + \alpha, \\ ii = (i + 1)j, \quad j^2 = \gamma,$$

with  $\alpha$  and  $\gamma$  in  $F$ .

6. Algebras of degree three. We now let *three* be the degree of  $D$  and the characteristic of  $F$ . By Theorem 2 there exists a separable cubic sub-field  $F(u)$  of  $F$  such that  $u$  has

$$\phi(\omega) \equiv \omega^3 + \alpha\omega^2 + \beta\omega + \gamma = 0,$$

with  $\alpha \neq 0$  by Theorem 3. By Theorem 10 we have

$$\phi(\omega) \equiv (\omega - u_3)(\omega - u_2)(\omega - u_1)$$

where  $u = u_1, u_2, u_3$  are evidently distinct and  $u_2, u_3$  are transforms of  $u$  by

\* Cf. E. Steinitz, *Algebraische Theorie der Körper*, p. 55.

quantities of  $F$ . If

$$x = u_2u_1 - u_1u_2$$

is zero then evidently  $\phi(\omega)$  is a cyclic equation,  $D$  is a cyclic algebra. For  $u_2u_1 = u_1u_2$  implies that  $u_2$  is in  $F(u_1)$ .

Hence let  $x \neq 0$ . By Wedderburn's proof for the case where the characteristic of  $F$  is not three, we have

$$xu_1 = u_2x, \quad xu_2 = u_3x, \quad xu_3 = u_1x,$$

so that  $x^3u_1 = u_1x^3$  and  $x^3$  is in  $F$ . Let then  $x^3 = \delta$  in  $F$ .

The minimum equation of  $x$  with respect to  $F$  is

$$\psi(\omega) \equiv \omega^3 - \delta \equiv (\omega - x)^3 = 0,$$

so that  $F(x)$  is inseparable and *Wedderburn's proof breaks down*. But let  $v = u_1x - xu_1 = (u_1 - u_2)x \neq 0$ . Write  $x = x_1$ . Then  $x_1 \neq u_1x_1u_1^{-1}$  since  $(x_1 - u_1x_1u_1^{-1})u_1 = xu_1 - u_1x = -v \neq 0$ . Hence  $\omega - u_1x_1u_1^{-1}$  is a right divisor of  $\psi(\omega)$  but not of  $\omega - x$ , and, by Theorem 12, with  $R = u_1x_1u_1^{-1} - x_1 = vu_1^{-1}$  we have  $\omega - vx_1v^{-1}$  a right divisor of  $(\omega - x_1)^2$ . We have obtained

$$(\omega - x_1)^2 \equiv (\omega^2 - 2x_1\omega + x_1^2) \equiv (\omega - x_3)(\omega - x_2), \quad x_2 = vx_1v^{-1}.$$

Now

$$x_2 = vx_1v^{-1} = (u_1 - u_2)x_1^2x_1^{-1}(u_1 - u_2)^{-1} = (u_1 - u_2)x_1(u_1 - u_2)^{-1}.$$

But

$$x_1(u_1 - u_2) = (u_2 - u_3)x_1, \quad (u_2 - u_3)^{-1}x_1 = x_1(u_1 - u_2)^{-1}$$

and

$$x_2 = (u_1 - u_2)(u_2 - u_3)^{-1}x_1.$$

If  $x_2 = x_1$  then  $u_1 - u_2 = u_2 - u_3$ . But  $3u_2 = 0, u_1 - 2u_2 + u_3 = u_1 + u_2 + u_3 = 0 = \alpha$ , a contradiction. Hence  $x_2 \neq x_1$ . Also  $x_3 + x_2 + x_1 = 0, x_3 + x_2 = 2x_1, x_3 - x_1 = x_1 - x_2 \neq 0, x_3 - x_2 = 2(x_1 - x_2) \neq 0$ . Thus  $x_3, x_2, x_1$  are all distinct and we have obtained a factorization in  $D$  of  $\psi(\omega)$  into distinct factors in spite of the fact that  $\psi(\omega) = 0$  is inseparable.

Moreover  $(\omega - x_1)^3 \equiv (\omega - x_2)^3 \equiv (\omega - x_3)^3 \equiv (\omega - x_1)(\omega - x_3)(\omega - x_2)$ , so that  $(\omega - x_2)^2 - (\omega - x_1)(\omega - x_3)$  and  $x_1x_3 = x_2^2$ .

If  $x_2x_1 - x_1x_2 = 0$ , then  $x_2 \neq x_1$  is in  $F(x_1), (x_2 - x_1)^3 = x_2^3 - x_1^3 = 0$ , a contradiction. Hence  $y = x_2x_1 - x_1x_2 \neq 0$ . By the Wedderburn proof\*

$$yx_1 = x_2y, \quad yx_2 = x_3y, \quad yx_3 = x_1y, \quad y^3 = \epsilon \text{ in } F.$$

---

\* These Transactions (loc. cit.), 1921.

We let  $z_1 = x_1y$ ,  $z_2 = yz_1y^{-1} = yx_1yy^{-1} = yx_1$ , a transform of  $z_1$  by  $y$ . Also  $yx_1 \neq x_1y$  so that  $z_2 \neq z_1$ . Thus  $z_2z_1 - z_1z_2 = yx_1^2y - x_1y^2x_1 = (x_2^2 - x_3x_1)y^2 = 0$ . Hence  $z_2$  is commutative with  $z_1$ ,  $z_2$  is in  $F(z_1)$ ,  $z_2 \neq z_1$  and  $F(z_1)$  is cyclic. We have proved

**THEOREM 15.** *Every normal division algebra of degree three over any infinite field  $F$  is cyclic.*

THE INSTITUTE FOR ADVANCED STUDY,  
PRINCETON, N. J.