MATH. SCAND. 4 (1956), 125–128

ON THE CLASS NUMBER OF NON-MAXIMAL ORDERS IN $\mathfrak{p}$-ADIC DIVISION ALGEBRAS

W. E. JENNER

In 1938 H. Zassenhaus [6] gave a proof that a finite group has only a finite number of unimodularly inequivalent rational integral representations of given finite degree. A crucial point in the proof consisted in showing that for a non-maximal order in a finite-dimensional division algebra over the rationals there are only a finite number of equivalence classes of right (left) ideals. This latter result is of considerable arithmetical interest even aside from its applications. In this paper it is shown that its analogue holds for $\mathfrak{p}$-adic division algebras. The proof uses the results of Hasse [1] on the arithmetic of $\mathfrak{p}$-adic division algebras. As an application, it is shown that a finite group has only a finite number of unimodularly inequivalent $\mathfrak{p}$-adic integral representations of given finite degree, a result which follows also from a theorem of Maranda [4]. For both rational and $\mathfrak{p}$-adic division algebras the right and left class numbers are equal. This was first shown for the case of semisimple algebras over the rationals by G. Shover [5] and the same methods work in the $\mathfrak{p}$-adic case. However, since the proof in [5] seems to be incomplete on some minor points, it has been thought advisable to outline a slightly different one incorporating appropriate modifications.

Let $\mathfrak{D}$ be a division algebra of finite dimension n over a $\mathfrak{p}$-adic field k and let $\mathfrak{o}$ be the ring of integers of k. Let $\mathfrak{O}$ be an arbitrary order of $\mathfrak{D}$, that is a subring of $\mathfrak{D}$ containing a k-basis and the unit element of $\mathfrak{D}$, and which is a finitely-generated $\mathfrak{o}$-module. Since $\mathfrak{o}$ is a principal ideal ring it follows that $\mathfrak{O}$ has a minimal basis. Now $\mathfrak{O}$ consists of elements which are integral over $\mathfrak{o}$ and so $\mathfrak{O}$ is contained in the unique maximal order $\mathfrak{J}$ of $\mathfrak{D}$ which consists of the set of all elements of $\mathfrak{D}$ which are integral over $\mathfrak{o}$ (cf. [1]). Consequently $\mathfrak{O}$ has a conductor $\mathfrak{f} \neq (0)$ with respect to $\mathfrak{J}$ (cf. [2]).

DEFINITION 1. A *right (left) ideal* $\mathfrak{a}$ of $\mathfrak{O}$ is an $\mathfrak{o}$-module contained in $\mathfrak{D}$ such that (1) $\mathfrak{a}\mathfrak{O} \subseteq \mathfrak{a}$ ($\mathfrak{O}\mathfrak{a} \subseteq \mathfrak{a}$), (2) there exists an element $c \neq 0$ in $\mathfrak{o}$ such that $c \cdot \mathfrak{O} \subseteq \mathfrak{a}$, and (3) there exists an element $d \neq 0$ in $\mathfrak{o}$ such that $d \cdot \mathfrak{a} \subseteq \mathfrak{O}$.

Received November 16, 1955.

DEFINITION 2. Two right (left) ideals $\mathfrak{a}$ and $\mathfrak{b}$ are said to be *equivalent* if there exists an element $\lambda \in \mathfrak{D}$ such that $\mathfrak{a} = \lambda \cdot \mathfrak{b}$ ($\mathfrak{a} = \mathfrak{b}\lambda$).

Let $e_1, \cdots, e_n$ be a minimal basis for $\mathfrak{O}$. Let $\mathfrak{x}$ be the row-vector $(e_1, \ldots, e_n)$ and set $\mathfrak{y} = {}^t\mathfrak{x}$. The regular representations $\alpha \to R_\alpha$ and $\alpha \to S_\alpha$ of $\mathfrak{D}$ are given by $\alpha \cdot \mathfrak{x} = \mathfrak{x} \cdot R_\alpha$ and $\mathfrak{y} \cdot \alpha = S_\alpha \cdot \mathfrak{y}$ respectively. Let $\mathfrak{a}$ be a finitely-generated $\mathfrak{o}$-module of rank n contained in $\mathfrak{D}$. Let $\alpha_1, \ldots, \alpha_n$ be a minimal basis of $\mathfrak{a}$ and let $\mathfrak{z}$ denote the transpose of the row-vector $(\alpha_1, \ldots, \alpha_n)$. With the module $\mathfrak{a}$ is associated a matrix M defined by $\mathfrak{z} = M \cdot \mathfrak{y}$. This matrix M is determined by $\mathfrak{a}$ to within unimodular equivalence. The following two theorems are due to MacDuffee and are proved in [3].

(I) A finitely-generated $\mathfrak{o}$-module $\mathfrak{a}$ contained in $\mathfrak{D}$ and of rank n is a right (left) ideal of $\mathfrak{O}$ if and only if there exist matrices C_α (D_α) with coefficients in $\mathfrak{o}$ such that $M \cdot S_\alpha = C_\alpha \cdot M$ ($M \cdot {}^tR_\alpha = D_\alpha \cdot M$) for all $\alpha \in \mathfrak{O}$ where M is the matrix corresponding to $\mathfrak{a}$.

(II) Let $\mathfrak{a}_1$ and $\mathfrak{a}_2$ be right (left) ideals with corresponding matrices M_1 and M_2 respectively, so that $M_i \cdot S_\alpha = C_\alpha^{(i)} \cdot M_i$ ($M_i \cdot {}^tR_\alpha = D_\alpha^{(i)} \cdot M_i$) for all $\alpha \in \mathfrak{O}$, $i = 1, 2$, and the matrices $C_\alpha^{(i)}$ ($D_\alpha^{(i)}$) have coefficents in $\mathfrak{o}$. Then $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are equivalent if and only if there exists a matrix E with coefficients in $\mathfrak{o}$ and whose determinant is a unit of $\mathfrak{o}$, such that

$$E \cdot C_\alpha^{(2)} = C_\alpha^{(1)} \cdot E \qquad (E \cdot D_\alpha^{(2)} = D_\alpha^{(1)} \cdot E)$$

for all $\alpha \in \mathfrak{O}$.

Now let $\mathfrak{a}$ be a left ideal of $\mathfrak{O}$ with corresponding matrix M. Then $M \cdot {}^tR_\alpha = D_\alpha \cdot M$ for all $\alpha \in \mathfrak{O}$ where the D_α have coefficients in $\mathfrak{o}$. Now $\mathfrak{D}$ is a separable algebra and so its discriminant matrix is non-singular and intertwines the right and left regular representations; thus there exists a non-singular matrix T with coefficients in k such that $S_\alpha \cdot T = T \cdot R_\alpha$ for all $\alpha \in \mathfrak{D}$. Then $M \cdot {}^tR_\alpha = M \cdot {}^tT \cdot {}^tS_\alpha \cdot ({}^tT)^{-1} = D_\alpha \cdot M$ and by a slight rearrangement, $({}^tM)^{-1} \cdot T^{-1} \cdot S_\alpha = {}^tD_\alpha \cdot ({}^tM)^{-1} \cdot T^{-1}$. Thus, setting

$$H = ({}^tM)^{-1} \cdot T^{-1}$$

and $C_\alpha = {}^tD_\alpha$, one obtains $H \cdot S_\alpha = C_\alpha \cdot H$ for all $\alpha \in \mathfrak{O}$. By (I), H corresponds to a right-ideal $\mathfrak{a}^*$ with minimal basis $H \cdot \mathfrak{y}$. It is easily verified that this mapping $\mathfrak{a} \to \mathfrak{a}^*$ is a one-to-one mapping of the set of all left-ideals of $\mathfrak{O}$ onto the set of all right-ideals of $\mathfrak{O}$. Since $C_\alpha = {}^tD_\alpha$ in this correspondence, it follows from (II) that there is induced a one-to-one mapping of the set of equivalence classes of left-ideals onto the set of equivalence classes of right-ideals. Thus these two sets have the same cardinal number which will be called the *class number* of $\mathfrak{O}$.

REMARK. The preceding proof works under more general circumstances, namely when $\mathfrak{D}$ is a finite-dimensional Frobenius algebra with unit element and $\mathfrak{o}$ is a principal ideal ring.

Let $\mathfrak{a}$ be any right-ideal of $\mathfrak{O}$. Since every one-sided ideal of $\mathfrak{J}$ is principal (cf. [1]) it follows that $\mathfrak{a}\cdot\mathfrak{J}=\lambda\cdot\mathfrak{J}$ for some $\lambda\in\mathfrak{D}$. Then $\lambda^{-1}\cdot\mathfrak{a}\cdot\mathfrak{J}=\mathfrak{J}$ and so $\mathfrak{O}\subseteq\lambda^{-1}\cdot\mathfrak{a}\cdot\mathfrak{J}$. Consequently,

$$\mathfrak{J} = \lambda^{-1}\cdot\mathfrak{a}\cdot\mathfrak{J}\cdot\mathfrak{J} = \lambda^{-1}\cdot\mathfrak{a}\cdot\mathfrak{J} \subseteq \lambda^{-1}\cdot\mathfrak{a} \subseteq \mathfrak{J}.$$

Thus $\mathfrak{a}$ is equivalent to a right-ideal $\lambda^{-1}\cdot\mathfrak{a}$ of $\mathfrak{O}$ with $\mathfrak{J}\subseteq\lambda^{-1}\cdot\mathfrak{a}\subseteq\mathfrak{J}$. Since the difference module $\mathfrak{J}\,(\mathrm{mod}\,\mathfrak{J})$ is finite (cf. [1]), it follows that the number of equivalence classes of right-ideals is finite. This completes the proof of

THEOREM 1. *Let $\mathfrak{O}$ be an arbitrary order in a finite-dimensional $\mathfrak{p}$-adic division algebra. Then the number of equivalence classes of right-ideals of $\mathfrak{O}$ is equal to the number of equivalence classes of left ideals of $\mathfrak{O}$ and this number is finite.*

This result is now applied to a situation considered by Zassenhaus in [6] for the case of the rational ground field. Let $\mathfrak{O}$ be an order in a finite-dimensional algebra with unit element over a $\mathfrak{p}$-adic ground field k and let $\mathfrak{o}$ denote the ring of integers of k. An integral representation of $\mathfrak{O}$ is an $\mathfrak{o}$-homomorphism of $\mathfrak{O}$ onto a ring of $\mathfrak{o}$-endomorphisms of a finitely-generated $\mathfrak{o}$-module. It will be assumed that the unit element of $\mathfrak{O}$ maps into the identity operator on the module. Since $\mathfrak{o}$ is a principal ideal ring, such a module has a minimal basis and so the representation can be realized by matrices with coefficients in $\mathfrak{o}$. Two such representations $\alpha\to\Gamma_\alpha$ and $\alpha\to\Lambda_\alpha$ are said to be unimodularly equivalent if there exists an $\mathfrak{o}$-isomorphism Φ of the corresponding representation modules such that $\Phi\cdot\Gamma_\alpha\cdot\Phi^{-1}=\Lambda_\alpha$ for all $\alpha\in\mathfrak{O}$.

THEOREM 2. *Let $\mathfrak{O}$ be an order in a finite-dimensional semisimple $\mathfrak{p}$-adic algebra. Then the number of equivalence classes, with respect to unimodular equivalence, of integral representations of $\mathfrak{O}$ of given finite degree is finite.*

This is proved as in [6] except that Theorem 1 is used in place of the corresponding result for division algebras over the field of rational numbers.

COROLLARY. *A finite group has only a finite number of unimodularly inequivalent integral $\mathfrak{p}$-adic representations of given finite degree.*

This follows from Theorem 2 by taking $\mathfrak{D}$ to be the group ring over $\mathfrak{o}$ and using the fact that the group algebra of a finite group over a $\mathfrak{p}$-adic field is semisimple.

REFERENCES

1. H. Hasse, *Über $\mathfrak{p}$-adische Schiefkörper und ihre Bedeutung für die Arithmetik hyperkomplexer Zahlsysteme*, Math. Ann. 104 (1931), 495–534.
2. W. E. Jenner, *Block ideals and arithmetics of algebras*, Compositio Math. 11 (1953), 187–203.
3. C. C. MacDuffee, *Modules and ideals in a Frobenius algebra*, Monatsh. Math. Phys. 48 (1939), 293–313.
4. J.-M. Maranda, *On $\mathfrak{P}$-adic representations of finite groups*, Canadian J. Math. 5 (1953), 344–355.
5. G. Shover, *Class number in a linear associative algebra*, Bull. Amer. Math. Soc. 39 (1933), 610–614.
6. H. Zassenhaus, *Neuer Beweis der Endlichkeit der Klassenzahl bei unimodularer Äquivalenz endlicher ganzzahliger Substitutionsgruppen*, Hamburger Math. Einzelschr. 12 (1938), 276–288.

NORTHWESTERN UNIVERSITY, EVANSTON, ILLINOIS, U.S.A.