JOURNAL OF NUMBER THEORY 34, 21–32 (1990)

On Two Classical Theorems in the Theory of Orders*

J. BRZEZINSKI

Department of Mathematics, Chalmers University of Technology and University of Göteborg, S-412 96 Göteborg, Sweden

Communicated by O. Taussky Todd

Received August 15, 1988; revised January 13, 1989

The paper contains generalizations of the Latimer–MacDuffee theorem and the Chevalley–Hasse–Noether theorem. It shows that the two theorems are closely related to each other by means of a duality, which depends on simultaneous actions of the idèle groups on maximal orders in central simple algebras and on embeddings of maximal commutative subrings into such orders.

INTRODUCTION

The purpose of the paper is to generalize two well-known theorems about orders and to point out very close connections between them.

The first theorem was published by C. G. Latimer and C. C. MacDuffee in 1933 (see [6, 9]):

(0.1) THEOREM. *Let $\Lambda = M_n(\mathbb{Z})$ and let $S = \mathbb{Z}[\theta]$, where $f(\theta) = 0$ for a monic separable polynomial $f \in \mathbb{Z}[X]$ of degree n. Then there is a one-to-one correspondence between the $\Lambda^* = GL_n(\mathbb{Z})$-orbits on the (ring-)embeddings of S into Λ and the ideal classes of S.*

Notice that if $\varphi: S \to \Lambda$ is an embedding, then the action of Λ^* is defined by conjugation, that is, $(\varphi \circ \lambda)(X) = \lambda^{-1}\varphi(x)\lambda$ for $x \in S$ and $\lambda \in \Lambda^*$. Of course, there is a bijection between the embeddings and the solutions to $f(X) = 0$ in Λ.

The second theorem was published independently by C. Chevalley, H. Hasse, and E. Noether in 1934 (see [3, 5, 7]). It gives a characterization of a class of ideals in maximal orders of finitely dimensional central simple algebras over global fields, which are extended from ideals in maximal commutative suborders. E. Noether defined in her paper a bouquet of orders (in German "Gebiet" but a better non-reserved English term seems

* This work was partially supported by the Swedish Natural Science Research Council.

0022-314X/90 $3.00

to be difficult to find) as a family of all maximal orders in such an algebra A having the same intersection S with a given maximal commutative subfield L of A and such that the completions of the orders in that family are equal at all ramification points of A. In terms of bouquets the Chevalley–Hasse–Noether theorem can be formulated in the following way (see [7, Sect. II, Satz 2; Sect. III, Satz 1]):

(0.2) THEOREM. *Let A be a finitely dimensional central simple algebra over a global field K and let S be the maximal order in a maximal commutative subfield of A. If Λ and Λ' are two orders belonging to a bouquet of S, then there is an S-ideal $\mathfrak{a}$ in L such that $\Lambda'\mathfrak{a} = \mathfrak{a}\Lambda$.*

Note that one can write $\Lambda' = \mathfrak{a}\Lambda\mathfrak{a}^{-1}$, and then the theorem says that Λ and Λ' belong to the same orbit of the group of S-ideals acting by conjugation on the maximal orders containing S.

The first theorem can be easily generalized by means of a result proved by Chevalley and used by him and Hasse in their proofs of the second theorem (see (2.2)). The Latimer–MacDuffee theorem is valid when $\mathbb{Z}$ is replaced by any principal ideal domain R, and S by any R-order in a commutative semisimple algebra of dimension n over the quotient field K of R (see (2.3)).

The second theorem also has a far-going generalization. Replacing K by the quotient field of any Dedekind ring R, L by any maximal commutative semisimple subalgebra of A, and modifying the notion of bouquet to consist of maximal orders whose completions are equal at each point where the algebra is not split, we get that the Chevalley–Hasse–Noether theorem is valid for every Gorenstein order S in L (see (2.6)).

Still the most interesting point is that the two theorems are essentially dual in a suitable sense, so each of them is an easy consequence of the other one. The duality follows from the fact that the idèle group of A acts by conjugation both on maximal orders in A and on the embeddings of S into A. This makes it possible to apply a purely combinatorial class number formula for transitive actions of groups on pairs of sets proved in [2]. The two theorems can be translated to some quantitative statements related to the actions of the idèle group and then connected by the class formula (see (2.9)).

In Section 1 we introduce the basic notions and the terminology. In Section 2 we prove the general versions of the two theorems and explain relations between them. In Section 3 we extend the Latimer–MacDuffee theorem still further, obtaining a generalization to the case of arbitrary global fields.

1. Preliminaries

First, following [2], we recall some necessary facts concerning actions of groups on pairs of sets.

Let $X\times G\to X$ and $G\times Y\to Y$ be actions of a group G on two sets X and Y, that is, $x(g_1g_2)=(xg_1)g_2$ and $xe=x$ when $x\in X$, $g_1, g_2\in G$ and e is the neutral element of G. Similarly for the action of G on Y. We assume that both actions are transitive.

Let $\mathscr{R}\subseteq X\times Y$ be a relation such that $(xg, y)\in\mathscr{R}$ if and only if $(x, gy)\in\mathscr{R}$. We shall say that $\mathscr{R}$-(X, G, Y) is a G-relation. If $x\in X$, denote $G(x)=\{g\in G:xg=x\}$ and $\mathscr{R}(x)=\{y\in Y:(x,y)\in\mathscr{R}\}$. Define similarly $G(y)$ and $\mathscr{R}(y)$ when $y\in Y$. Let $E(x, y)=\{g\in G:(xg, y)\in\mathscr{R}\}$ (we shall also write $E_G(x, y)$ when necessary). If E is a subset of G consisting of whole double cosets AgB, where A, B are subgroups of G and $g\in E$, then $A\backslash E/B$ denotes the set of all such double cosets in E, and $|A\backslash E/B|$ its cardinality.

Let $(x, y)\in\mathscr{R}$ and let N be a subgroup of $G(x)$. It is easy to see that N acts on $\mathscr{R}(x)$. The orbits of N on $\mathscr{R}(x)$ are in a one-to-one correspondence with the elements of the set $N\backslash E(x, y)/G(y)$, whose cardinality will be denoted by $e_N(x, y)$. Similarly, if N is a subgroup of $G(y)$, $e_N(x, y)$ will denote the cardinality of the set $G(x)\backslash E(x, y)/N$, whose elements are in a one-to-one correspondence with the orbits of N on $\mathscr{R}(y)$. These remarks imply the following "duality":

(1.1) Proposition. *Let $(x, y)\in\mathscr{R}$. Then the orbits of $G(x)$ on $\mathscr{R}(x)$ and $G(y)$ on $\mathscr{R}(y)$ are in one-to-one correspondences with the elements of $G(x)\backslash E(x, y)/G(y)$, that is, $e_{G(x)}(x, y)=e_{G(y)}(x, y)$.*

We shall work with actions of groups related to algebras over quotient fields of Dedekind rings. Recall some relevant notions. Let R be a Dedekind ring with quotient field K, and let A be a finitely dimensional separable K-algebra. If M is an R-module, then $M_\mathfrak{p}$ will denote the completion of M with respect to the topology defined by the non-zero prime ideal $\mathfrak{p}$ of R. Let Λ be an R-order in A, that is, a subring of A containing R, finitely generated and projective as an R-module and such that $K\Lambda=A$. Let $\mathscr{J}(A)$ be the idèle group of A, that is, $\mathscr{J}(A)$ consists of $\alpha=(a_\mathfrak{p})$ such that $a_\mathfrak{p}$ belongs to the group of units $A_\mathfrak{p}^*$ for non-zero $\mathfrak{p}\in\operatorname{Spec} R$ and $a_\mathfrak{p}\in\Lambda_\mathfrak{p}^*$ for almost all such $\mathfrak{p}$. The idèle group acts on the R-orders in A: If $\alpha=(a_\mathfrak{p})\in\mathscr{J}(A)$, then $\alpha\Lambda\alpha^{-1}$ denotes the R-order such that $(\alpha\Lambda\alpha^{-1})_\mathfrak{p}=a_\mathfrak{p}\Lambda_\mathfrak{p}a_\mathfrak{p}^{-1}$ for each $\mathfrak{p}\in\operatorname{Spec} R$. The existence and uniqueness of $\alpha\Lambda\alpha^{-1}$ follow from the "local–global principle": For each R-order Λ there is a unique R-order Λ' such that $\Lambda'_\mathfrak{p}=\Lambda_\mathfrak{p}$ for almost all $\mathfrak{p}\in\operatorname{Spec} R$ and $\Lambda'_\mathfrak{p}$ is equal to an arbitrarily chosen $R_\mathfrak{p}$-order for the remaining $\mathfrak{p}$ (see [4, (4.21)]). Two R-orders Λ and Λ' such that $\Lambda'=\alpha\Lambda\alpha^{-1}$, $\alpha\in\mathscr{J}(A)$, are said to belong to the same genus of orders. It is well known that the maximal R-orders form one genus (see [4, (26 .23)]).

Let S be an R-order in a commutative K-algebra L. An R-embedding $\varphi: S \rightarrow \Lambda$ is called optimal (pure) if $\Lambda/\varphi(S)$ is R-projective. It is easy to see that φ is optimal if and only if $K\varphi(S) \cap \Lambda = \varphi(S)$. This condition is clearly satisfied if $\varphi(S)$ is a maximal commutative subring of Λ. If φ is optimal, we shall say that Λ contains $\varphi(S)$ optimally.

The general situation described at the beginning of this section appears later in two special cases.

(1.2) EXAMPLES. (a) Let S be a maximal commutative subring of a maximal R-order Λ in A, and let $L = KS$. Let $G = \mathscr{J}(A)$, $X =$ the set of $\varphi = (\varphi_\mathfrak{p})$ such that $\varphi_\mathfrak{p}: S_\mathfrak{p} \rightarrow \Lambda_\mathfrak{p}$ is given by $\varphi_\mathfrak{p}(x) = a_\mathfrak{p}^{-1} x a_\mathfrak{p}$, where $\alpha = (a_\mathfrak{p}) \in \mathscr{J}(A)$, $Y =$ the set of the orders $\Lambda' = \alpha\Lambda\alpha^{-1}$, $\alpha \in \mathscr{J}(A)$, that is, the set of all maximal R-orders in A. The actions $X \times G \rightarrow X$ and $G \times Y \rightarrow Y$ are defined by

$$(\varphi \circ \alpha)_\mathfrak{p}(x) = a_\mathfrak{p}^{-1} \varphi_\mathfrak{p}(x)\, a_\mathfrak{p} \qquad \text{and} \qquad \alpha \circ \Lambda' = \alpha\Lambda'\alpha^{-1}.$$

Let

$$\mathscr{R} = \{(\varphi, \Lambda'): \varphi_\mathfrak{p}: S_\mathfrak{p} \rightarrow \Lambda'_\mathfrak{p} \text{ and } \varphi_\mathfrak{p} \text{ is optimal}\}.$$

It is easy to check that $\mathscr{R}$-(X, G, Y) is a G-relation. Let $x = (id_{S_\mathfrak{p}})$ and $y = \Lambda$. We shall write $x = S$ for simplicity. Then $G(S) = \mathscr{J}(L)$ the ideal group of L, $\mathscr{R}(S) =$ the set of maximal orders optimally containing S, $G(\Lambda) = \{\alpha \in \mathscr{J}(A) : \alpha\Lambda\alpha^{-1} = \Lambda\} =: \mathscr{N}(\Lambda)$, and $\mathscr{R}(\Lambda) =$ the set of optimal embeddings $\varphi = (\varphi_\mathfrak{p})$ such that $\varphi_\mathfrak{p}: S_\mathfrak{p} \rightarrow \Lambda_\mathfrak{p}$. Only the first equality needs an explanation. We have

$$\begin{aligned} G(S) &= \{\alpha \in \mathscr{J}(A) : \forall_\mathfrak{p} a_\mathfrak{p} x = x a_\mathfrak{p} \text{ for } x \in S_\mathfrak{p}\} \\ &= \mathscr{J}(A) \cap \Pi_\mathfrak{p} L_\mathfrak{p}^* = \mathscr{J}(L), \end{aligned}$$

since $a_\mathfrak{p}$ commuting with each element of the maximal commutative subring $L_\mathfrak{p} = K_\mathfrak{p} S_\mathfrak{p}$ of $A_\mathfrak{p}$ must belong to $L_\mathfrak{p}$. Moreover, $a_\mathfrak{p} \in L_\mathfrak{p} \cap \Lambda_\mathfrak{p}^* = S_\mathfrak{p}^*$ for almost all $\mathfrak{p} \in \operatorname{Spec} R$.

We shall apply (1.1) when $\Lambda = M_n(R)$. Let $\mathscr{U}(\Lambda) = \Pi_\mathfrak{p} \Lambda_\mathfrak{p}^*$, $\mathfrak{p} \in \operatorname{Spec} R$. Then $e_{\mathscr{N}(\Lambda)}(S, \Lambda) = e_{\mathscr{U}(\Lambda)}(S, \Lambda)$, since $N(\Lambda_\mathfrak{p}) = \{a \in A_\mathfrak{p}^* : a\Lambda_\mathfrak{p} a^{-1} = \Lambda_\mathfrak{p}\} = K_\mathfrak{p}^* \Lambda_\mathfrak{p}^*$ implies that the orbits of $\mathscr{N}(\Lambda)$ and $\mathscr{U}(\Lambda)$ are the same. Thus

$$(1.3) \qquad e_{\mathscr{U}(\Lambda)}(S, \Lambda) = e_{\mathscr{N}(\Lambda)}(S, \Lambda) = e_{\mathscr{J}(L)}(S, \Lambda)$$

according to (1.1).

(b) Keeping the notations as above, let $\Lambda = M_n(R)$. Let $G = \Lambda^*$, $X =$ the set of all embeddings $\varphi\colon S \to \Lambda$ such that $\varphi(x) = a^{-1}xa$, where $a \in \Lambda^*$, $Y =$ the set of all orders $\Lambda' = a\Lambda a^{-1}$, $a \in \Lambda^*$. Define the actions of G on the two sets and $\mathcal{R}$ similarly as in (a) (removing $\mathfrak{p}$). Of course, $\mathcal{R}$-(X, G, Y) is a G-relation. Now $G(S) = L^*$ and $G(\Lambda) = N(\Lambda) = \{a \in \Lambda^* : a\Lambda a^{-1} = \Lambda\} = K^*\Lambda^*$. Noting that the orbits of $N(\Lambda)$ and Λ^* on $\mathcal{R}(\Lambda)$ are the same and using (1.1), we now get

$$(1.4) \qquad e_{\Lambda^*}(S, \Lambda) = e_{N(\Lambda)}(S, \Lambda) = e_{L^*}(S, \Lambda).$$

Finally, recall that there is a general relation between the numbers of orbits on optimal embeddings and the class numbers

$$(1.5) \qquad \sum_{k=1}^{t} H(\Lambda_k)\, e_{\Lambda_k^*}(S, \Lambda_k) = h^{(f)}(S)\, e_{\mathcal{U}(\Lambda)}(S, \Lambda),$$

when all the components are finite. Λ_k represent the isomorphism classes of maximal orders in A. $H(\Lambda_k)$ is the two-sided class number of Λ_k, that is, the order of the group of the two-sided Λ_k-ideals modulo principal two-sided Λ_k-ideals. $e_{\Lambda_k^*}(S, \Lambda_k)$ is the number of optimal embeddings of S into Λ_k modulo the action of Λ_k^*. $h^{(f)}(S)$ is the locally free class group of S, that is, the order of the group of locally free S-ideals in L modulo the principal S-ideals. $e_{\mathcal{U}(\Lambda)}(S, \Lambda)$ is the number of local optimal embeddings $\varphi = (\varphi_{\mathfrak{p}})$, $\varphi_{\mathfrak{p}}\colon S_{\mathfrak{p}} \to \Lambda_{\mathfrak{p}}$ modulo the action of $\mathcal{U}(\Lambda) = \Pi_{\mathfrak{p}} \Lambda_{\mathfrak{p}}^*$, $\mathfrak{p} \in \operatorname{Spec} R$ (see [2, (2.2)]).

2. The Latimer–MacDuffee Theorem and the Chevalley–Hasse–Noether Theorem

Let R be a Dedekind ring with quotient field K, and let S be an R-order in a semisimple commutative K-algebra L. By an S-ideal we shall always mean an S-ideal I in L such that $KI = L$. Two S-ideals I and I' are in the same class if there is $a \in L^*$ such that $I' = aI$. I is locally free if there is $\alpha \in \mathcal{J}(L)$ such that $I = S\alpha$. The cardinality of the multiplicative group formed by the classes of locally free S-ideals will be denoted by $h^{(f)}(S)$ (compare (1.5)). An S-ideal I belongs to S if $O(I) = \{a \in L : aI \subseteq I\} = S$. Denote by $h(S)$ the cardinality of the set of classes formed by the S-ideals belonging to S. The classes of all S-ideals form a set whose cardinality is $\sum_{S'} h(S')$, where S' are all R-orders in L containing S. Occasionally, we call this sum the wide class number of S and denote it by $h^{(w)}(S)$. Recall that S is called a Gorenstein order if $\operatorname{Hom}_R(S, R)$ is S-projective (see [4, p. 776]).

(2.1) PROPOSITION. (a) *$h^{(f)}(S)=h(S)$ if and only if S is Gorenstein.*

(b) *If R is a discrete valuation ring, then $h(S)=1$ if and only if S is Gorenstein.*

(c) *$h(S)=h^{(f)}(S)\,\Pi_{\mathfrak{p}}h(S_{\mathfrak{p}})$, where the product is over all non-zero* $\mathfrak{p}\in\operatorname{Spec} R$

Proof. For (a) and (b) see [1, (2.3) and (2.7)]. For (c), let $X=\{\mathfrak{p}\in\operatorname{Spec} R:\mathfrak{p}\neq(0)$ and $S_{\mathfrak{p}}$ is not Gorenstein$\}$. X is finite (possibly empty) since $S_{\mathfrak{p}}$ is maximal in $L_{\mathfrak{p}}$ for almost all $\mathfrak{p}\in\operatorname{Spec} R$. Let I_k represent all classes of locally free S-ideals and let $I_{\mathfrak{p},l}$ represent all classes of $S_{\mathfrak{p}}$-ideals belonging to $S_{\mathfrak{p}}$ for $\mathfrak{p}\in X$. Consider S-ideals equal to the product of I_k for some k by an S-ideal I such that $I_{\mathfrak{p}}=S_{\mathfrak{p}}$ for $\mathfrak{p}\notin X$ and $I_{\mathfrak{p}}=I_{\mathfrak{p},l}$ for $\mathfrak{p}\in X$ and some l. The existence and uniqueness of so defined S-ideals follow from the "local–global principle" for lattices over Dedekind rings (see [4, (4.21)]). The set of them has cardinality $h^{(f)}(S)\,\Pi_{\mathfrak{p}}h(S_{\mathfrak{p}})$ and it is easy to check that they represent all $h(S)$ classes of the S-ideals belonging to S.

The following lemma was used by Chevalley and Hasse in their proofs of (0.2) (see [3, p. 87; 5, p. 14]). The result is similar to the Skolem–Noether theorem and it can be proved in a similar way (see [4, (3.62)]). We give a short proof for completeness.

(2.2) LEMMA. *Let $A=M_n(K)$ and let L be an n-dimensional commutative semisimple K-algebra. Then any two K-embeddings $\varphi_i\colon L\to A$, $i=1,2$, are A^*-equivalent, that is, there is $a\in A^*$ such that $\varphi_2(x)=a\varphi_1(x)\,a^{-1}$ for $x\in L$.*

Proof. Fix an isomorphism $A\cong\operatorname{End}_K(K^n)$ and let $K^n_{\varphi_i}$ be K^n considered as an L-module via φ_i. The two L-modules are L-isomorphic (to L) since each simple L-module must be represented in the decomposition of $K^n_{\varphi_i}$ exactly once (dimension over K!). Choose as a the matrix of the isomorphism between the two L-module structures on K^n.

We are now ready to prove the Latimer–MacDuffee theorem:

(2.3) THEOREM. *Let $\Lambda=M_n(R)$, where R is a principal ideal domain and let S be an R-order in an n-dimensional commutative semisimple K-algebra L. Then there is a bijection between the classes of S-ideals in L and the orbits of Λ^* on the R-embeddings of S into Λ such that a Λ^*-orbit consists of optimal embeddings if and only if the corresponding ideal class consists of ideals belonging to S.*

Proof. Let $\varphi\colon S\to\Lambda$ be an R-embedding. According to (2.2), there is a basis $U=(u_1,\ldots,u_n)$ for L over K such that $lU=U\varphi(l)$ when $l\in L$. Hence $I_U=Ru_1+\cdots+Ru_n$ is an S-ideal. If U' is another basis satisfying

$lU' = U'\varphi(l)$, then $U' = aU$ for some $a \in L^*$, so $I_{U'}$ and I_U are in the same class. In fact, there is $X \in GL_n(K)$ such that $U' = UX$, so $lU' = U\varphi(l)\, X = U'\varphi(l) = UX\varphi(l)$. Hence $\varphi(l)\, X = X\varphi(l)$ for $l \in L$. But $\varphi(L)$ is a maximal commutative subring of A, so $X \in \varphi(L)$. If $X = \varphi(a)$, $a \in L^*$, then $U' = U\varphi(a) = aU$. Define the class of I_U as the class of S-ideals corresponding to φ. If $\varphi'\colon S \to \Lambda$ is another embedding Λ^*-equivalent to φ, that is, $\varphi'(l) = M^{-1}\varphi(l)\, M$ for some $M \in \Lambda^*$ and all $l \in S$, then $lUM = U\varphi(l)\, M = UM\varphi'(l)$. But $I_{UM} = I_U$, so φ' and φ define the same class of S-ideals. Thus, we have a mapping from Λ^*-classes of embeddings to L^*-classes of S-ideals.

It is clear that for each S-ideal $I = Ru_1 + \cdots + Ru_n$, the equality $lU = U\varphi(l)$ defines an R-embedding $\varphi\colon S \to \Lambda$. If U is replaced by another basis $U' = UE$, $E \in \Lambda^*$, then φ is replaced by φ', which is Λ^*-equivalent to φ. If $I' = aI$, $a \in L^*$, then aU defines the same φ, since $l(aU) = (aU)\,\varphi(l)$. Thus each class of S-ideals defines a Λ^*-class of embeddings.

Clearly the two functions between the sets of Λ^*-classes of embeddings and L^*-classes of S-ideals are inverse to each other. It remains to prove the last statement concerning optimal embeddings and ideals belonging to S.

Let φ be an optimal embedding and let U be a corresponding basis. If $lI_U \subseteq I_U$, then $lU = U\varphi(l)$ gives $\varphi(l) \in \Lambda \cap \varphi(L) = \varphi(S)$, so $l \in S$, that is, I_U belongs to S. Conversely, let I belong to S and let U be an R-basis of I. If $\varphi(l) \in \Lambda$, then $lU = U\varphi(l)$ gives $lI \subseteq I$, so $l \in S$, that is, $\Lambda \cap \varphi(L) = \varphi(S)$.

(2.4) *Remarks.* (a) Using the notations of (1.2) (b), the last part of Theorem (2.3) says that $e_{\Lambda^*}(S, \Lambda) = h(S)$. This statement will be called the strong Latimer–MacDuffee theorem. If S' denotes an R-order in L containing S, then the set of Λ^*-orbits of all embeddings $S \to \Lambda$ has the cardinality $\sum_{S'} e_{\Lambda^*}(S', \Lambda)$, and the set of classes of all S-ideals has the cardinality $\sum_{S'} h(S') = h^{(w)}(S)$. The Latimer–MacDuffee theorem, that is, the first part of (2.3), establishes the equality of the last two sums, which follows immediately from the strong version.

(b) If $R = \mathbb{Z}$ and $S = \mathbb{Z}[\theta]$, where $f(\theta) = 0$ for a monic separable polynomial $f \in \mathbb{Z}[X]$ of degree n, then the first part of (2.3) is the original version of the Latimer–MacDuffee theorem, since the embeddings $\mathbb{Z}[\theta] \to M_n(\mathbb{Z})$ are in a one-to-one correspondence with the solutions to $f(X) = 0$ in $M_n(\mathbb{Z})$. Note that $\mathbb{Z}[\theta]$ is a Gorenstein order, since $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[\theta], \mathbb{Z}) \cong \mathbb{Z}[\theta]^\# = (1/f'(\theta))\, \mathbb{Z}[\theta]$, where $\mathbb{Z}[\theta]^\# = \{x \in \mathbb{Q}[\theta] : \mathrm{Tr}(x\mathbb{Z}[\theta] \subseteq \mathbb{Z}\}$ and $\mathrm{Tr}\colon \mathbb{Q}[\theta] \to \mathbb{Q}$ is the trace function. Therefore, according to (2.1) (a), $h(S) = h^{(f)}(S)$.

The dual of the Latimer–MacDuffee theorem is the following result:

(2.5) THEOREM. *Keeping the notations of* (2.3) *let $L \subseteq \Lambda$ and $S = L \cap \Lambda$. Then there is a bijection between the classes of S-ideals in L and the orbits* *of L^* on the maximal orders containing S such that an L^*-orbit consists or orders optimally containing S if and only if the corresponding ideal class consists of ideals belonging to S.*

Proof. According to (1.4) and (2.4) (a), $e_{L^*}(S, \Lambda) = e_{\Lambda^*}(S, \Lambda) = h(S)$, so there is a bijection between the L^*-orbits on maximal orders optimally containing S and the ideal classes of S-ideals belonging to S. Let S' denote an R-order in L containing S. The set of all maximal orders containing S is the disjoint union of the sets of maximal orders optimally containing S'. Therefore, the set of orbits of L^* on the maximal orders containing S has the cardinality $\sum_{S'} e_{L^*}(S', \Lambda) = \sum_{S'} h(S') = h^{(w)}(S)$.

Of course, it is possible to prove (2.5) directly and then deduce the Latimer–MacDuffee theorem (2.3) by using (1.4).

We now turn to the Chevalley–Hasse–Noether theorem. Let A be a central simple K-algebra, and let S be an R-order in a maximal commutative semisimple subalgebra L of A. Recall that two maximal orders Λ and Λ' belong to the same S-bouquet if $\Lambda \cap L = \Lambda' \cap L = S$ and $\Lambda_{\mathfrak{p}} = \Lambda'_{\mathfrak{p}}$ for each $\mathfrak{p} \in \operatorname{Spec} R$ such that $A_{\mathfrak{p}}$ is not split over $K_{\mathfrak{p}}$.

(2.6) THEOREM. *Let R be a Dedekind ring with quotient field K, and let A be a finitely dimensional central simple K-algebra. Let S be an R-order in a maximal commutative semisimple K-subalgebra L of A. Then all maximal orders in the same S-bouquet belong to the same $\mathscr{J}(L)$-orbit if and only if $S_{\mathfrak{p}}$ is a Gorenstein order for each $\mathfrak{p} \in \operatorname{Spec} R$ such that $A_{\mathfrak{p}}$ is split over $K_{\mathfrak{p}}$.*

Proof. Let Λ and Λ' be maximal orders belonging to a bouquet of S. We want to find $\alpha = (a_{\mathfrak{p}}) \in \mathscr{J}(L)$ such that $\Lambda' = \alpha \Lambda \alpha^{-1}$. For almost all $\mathfrak{p}$, $\Lambda_{\mathfrak{p}} = \Lambda'_{\mathfrak{p}}$, and then one can take $a_{\mathfrak{p}} = 1$. For a finite number of remaining $\mathfrak{p}$, $A_{\mathfrak{p}}$ is split and $\Lambda'_{\mathfrak{p}} = \Lambda_{\mathfrak{p}}$. If $S_{\mathfrak{p}}$ is Gorenstein, then according to (2.5) and (2.1) (b), $e_{L_{\mathfrak{p}}^*}(S_{\mathfrak{p}}, \Lambda_{\mathfrak{p}}) = h(S_{\mathfrak{p}}) = 1$, so $L_{\mathfrak{p}}^*$ acts transively on the bouquet of $S_{\mathfrak{p}}$. Therefore, one can find $a_{\mathfrak{p}} \in L_{\mathfrak{p}}^*$ such that $\Lambda'_{\mathfrak{p}} = a_{\mathfrak{p}} \Lambda_{\mathfrak{p}} a_{\mathfrak{p}}^{-1}$. If $S_{\mathfrak{p}}$ is not Gorenstein, then $h(S_{\mathfrak{p}}) \neq 1$ by (2.1) (b), so there are at least two orbits for the action of $L_{\mathfrak{p}}^*$ on the bouquet of $S_{\mathfrak{p}}$. If Λ' is such that $\Lambda'_{\mathfrak{p}}$ and $\Lambda_{\mathfrak{p}}$ belong to different $L_{\mathfrak{p}}^*$-orbits, then $\Lambda' \neq \alpha \Lambda \alpha^{-1}$ for all $\alpha \in \mathscr{J}(L)$, that is, Λ' and Λ are in different orbits of $\mathscr{J}(L)$. The existence of Λ' with the above property follows from the "local–global principle" (see Section 1).

(2.7) *Remark.* Note that $\mathscr{J}(L)$ acts on the set of all maximal orders optimally containing S. The action of $\mathscr{J}(L)$ can be replaced by an action of the group $I(S)$ of locally free S-ideals. In fact, mapping an idèle $\alpha \in \mathscr{J}(L)$ onto a locally free S-ideal $S\alpha$, one gets a surjective homomorphism with kernel $\Pi_{\mathfrak{p}} S_{\mathfrak{p}}^* = \mathscr{U}(S)$. Since $\mathscr{U}(S)$ acts trivially on any (maximal) order containing S, there is a natural action of $I(S)$ on these orders. Thus the statement of (2.6) may be formulated in the language of ideals as in (0.2).

If Λ is a matrix algebra, then the Chevalley–Hasse–Noether theorem can be extended by a more specific quantitative result.

(2.8) THEOREM. *Keeping the assumptions of* (2.6), *let* $\Lambda = M_n(R)$. *Then the cardinality of the set of* $\mathscr{J}(L)$*-orbits on the maximal orders optimally containing* S, *or equivalently, the cardinality of the set of* $\mathscr{U}(\Lambda)$*-orbits on the optimal embeddings* $S_\mathfrak{p} \to \Lambda_\mathfrak{p}$, $\mathfrak{p} \in \operatorname{Spec} R$, *is equal to* $\Pi_\mathfrak{p} h(S_\mathfrak{p})$.

Proof. Let us show that $e_{\mathscr{J}(L)}(S, \Lambda) = \Pi_\mathfrak{p} h(S_\mathfrak{p})$. $S_\mathfrak{p}$ is the maximal order in $L_\mathfrak{p}$ for almost all $\mathfrak{p} \in \operatorname{Spec} R$, and then $h(S_\mathfrak{p}) = 1$. For each of the finitely many $\mathfrak{p}$ such that $h(S_\mathfrak{p}) \neq 1$ choose $h(S_\mathfrak{p})$ orders representing all $L_\mathfrak{p}^*$-orbits on the $S_\mathfrak{p}$-bouquet (see (2.5)). Consider $\Pi_\mathfrak{p} h(S_\mathfrak{p})$ orders Λ' such that $\Lambda'_\mathfrak{p}$ is equal to one of the chosen $R_\mathfrak{p}$-orders when $h(S_\mathfrak{p}) \neq 1$ and $\Lambda'_\mathfrak{p} = \Lambda_\mathfrak{p}$ when $h(S_\mathfrak{p}) = 1$. The existence and uniqueness of such orders Λ' follow from the "local–global principle" (see Section 1). It is easy to see that the orders Λ' represent all orbits of $\mathscr{J}(L)$ on the S-bouquet.

(2.9) *Remark.* If $\Lambda = M_n(R)$, where R is a principal ideal domain, then the Latimer–MacDuffee theorem and the Chevalley–Hasse–Noether theorem are closely related by the duality of (1.1). In this case (1.5) reduces to

$$e_{\Lambda^*}(S, \Lambda) = h^{(f)}(S)\, e_{\mathscr{U}(\Lambda)}(S, \Lambda),$$

since $t = 1$ and $H(\Lambda) = 1$. The strong Latimer–MacDuffee theorem says that $e_{\Lambda^*}(S, \Lambda) = h(S)$. The Chevalley–Hasse–Noether theorem, as in (2.8), says that $e_{\mathscr{J}(L)}(S, \Lambda) = \Pi_\mathfrak{p} h(S_\mathfrak{p})$, $\mathfrak{p} \in \operatorname{Spec} R$. If the first of the theorems holds, then using (1.3) and (2.1)(c), we get

$$e_{\mathscr{J}(L)}(S, \Lambda) = e_{\mathscr{N}(\Lambda)}(S, \Lambda) = e_{\mathscr{U}(\Lambda)}(S, \Lambda) = h(S) : h^{(f)}(S) = \Pi_\mathfrak{p} h(S_\mathfrak{p}).$$

Similarly, the second of the theorems implies the first.

3. A FURTHER GENERALIZATION

What can be said about $e_{\Lambda^*}(S, \Lambda)$ when in the Latimer–MacDuffee theorem (2.3) the principal ideal ring R is replaced by a Dedekind ring? In this section, we give an answer to this question assuming, for simplicity of formulations, that K is a global field. But, in fact, all results and proofs which follow are valid for arbitrary Dedekind rings, when the cardinalities involved in (1.5) are finite.

Keeping the notations of (2.3), let $\mathrm{Nr}\colon L \to K$ be the norm map and $\mathrm{Nr}\colon \Lambda \to K$ the reduced norm map (see [4, Sect. D] and observe that

$\mathrm{Nr}(a) = \det(a)$ for $a \in A = M_n(K)$). If I is an S-ideal in L or a Λ-ideal in A, denote by $\mathrm{Nr}(I)$ the R-ideal generated by $\mathrm{Nr}(x)$, $x \in I$. Let $\mathrm{Cl}(R)$ denote the class group of R, and let $h_n(R) = |\mathrm{Cl}(R)^n| (h_1(R) = h(R))$. If $\mathfrak{a}$ is an R-ideal, its class in $\mathrm{Cl}(R)$ will be denoted by $[\mathfrak{a}]$. Let $\mathrm{Cl}_S(R)$ be the subgroup of $\mathrm{Cl}(R)$ generated by the classes $[\mathrm{Nr}(I)]$, where I is an S-ideal belonging to S. Note that if $\mathfrak{a}$ is an R-ideal, then $\mathrm{Nr}(\mathfrak{a}S) = \mathfrak{a}^n$, so $\mathrm{Cl}(R)^n$ is a subgroup of $\mathrm{Cl}_S(R)$. If P is a finitely generated projective R-module, let $[P]$ denote the Steinitz class of P in $\mathrm{Cl}(R)$, that is, if $P \cong \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n$, where $\mathfrak{a}_k$ are R-ideals, then $[P] = [\mathfrak{a}_1 \cdots \mathfrak{a}_n]$ (see [4, (4.13)]). Note that if $\alpha \in \mathscr{J}(L)$, then $[S\alpha] = [S][\mathrm{Nr}(S\alpha)]$ (see [4, Sect. D]).

The main result of this section is the following:

(3.1) THEOREM. *Let S be a Gorenstein R-order in L. Then there are $h_S(R)/h_n(R)$ isomorphism classes of maximal orders Λ in $A = M_n(K)$ such that $e_{\Lambda^*}(S, \Lambda) \neq 0$, and for them $e_{\Lambda^*}(S, \Lambda) = h(S)/h_S(R)$.*

Proof. First of all observe that by (2.1)(a) and (2.8), $h^{(\mathscr{I})}(S) = h(S)$ and $e_{\mathscr{U}(\Lambda)}(S, \Lambda) = 1$, so the right hand side of (1.5) is $h(S)$. In order to simplify the left hand side, note first that $H(\Lambda_k) = h_n(R)$ for $k = 1, ..., t$. In fact, the two-sided Λ-ideals in any maximal R-order Λ are $\Lambda\mathfrak{a}$, where $\mathfrak{a}$ is an R-ideal (see [4, (26.23)]). It is well known that $\Lambda\mathfrak{a}$ is principal if and only if $\mathrm{Nr}(\Lambda\mathfrak{a}) = \mathfrak{a}^n$ is principal (see [8, p. 386] where K need not be global). Therefore, the mapping $\Lambda\mathfrak{a} \mapsto [\mathfrak{a}^n]$ induces an isomorphism of the two-sided class group of Λ with $\mathrm{Cl}(R)^n$.

In order to simplify further the left hand side of (1.5) and to finish the proof of (3.1), we only need the following result, which we prove as Propositions (3.2) and (3.4): $e_{\Lambda_k^*}(S, \Lambda_k)$ is the same for all k for which it is different from 0 and it happens for exactly $h_S(R)/h_n(R)$ values of k.

(3.2) PROPOSITION. *$e_{\Lambda_k^*}(S, \Lambda_k) \neq 0$ for $h_S(R)/h_n(R)$ values of k.*

Proof. First of all, let us note that if I is an S-ideal in L such that $KI = L$, then the natural R-homomorphism $S \to \mathrm{End}_R(I)$ is an optimal embedding if and only if I belongs to S. It follows easily from the proof of (2.3) using localizations at $\mathfrak{p} \in \mathrm{Spec}\, R$.

Next observe that if $S \to \mathrm{End}_R(P)$ is an embedding, where P is a projective R-module of rank n, then P as an S-module is isomorphic to an S-ideal I in L. In fact, $K \otimes_R P$ is an L-module whose annihilator is trivial, so $K \otimes_R P \cong L$ as L-modules, since the dimensions of both modules over K are equal. Thus P considered as an S-submodule of $K \otimes_R P$ is isomorphic to some S-ideal I in L.

We also need the following result:

(3.3) LEMMA. *If P is a projective R-module of* rank n, *then there is an optimal embedding $S \to \operatorname{End}_R(P)$ if and only if $[P] = [S][\operatorname{Nr}(I)]$ for some S-ideal I in L belonging to S.*

Proof. Let $S \to \operatorname{End}_R(P)$ be an optimal embedding. Then according to the observations above, $P \cong I$, where I is an S-ideal in L belonging to S. Since S is Gorenstein, I is locally free, that is, there is $\alpha \in \mathscr{J}(L)$ such that $I = S\alpha$. Thus $[P] = [S\alpha] = [S][\operatorname{Nr}(S\alpha)]$. Conversely, if the last equalities hold, then $P \cong S\alpha$ as R-modules. Hence P has a structure of an S-module, and as such, it is isomorphic with an S-ideal belonging to S. Thus the embedding $S \to \operatorname{End}_R(P)$ corresponding to this structure is optimal.

We are now ready to finish the proof of (3.2). It is well known that $\Lambda_k \cong \operatorname{End}_R(P_k)$, where P_k are projective R-modules of rank n such that $[P_k]$ represent all cosets of $\operatorname{Cl}(R)^n$ in $\operatorname{Cl}(R)$ (see [4, (26.25; 8, Satz 3, p. 386]). As we have seen in (3.3), there is an optimal embedding $S \to \Lambda_k$ if and only if there is an S-ideal I_k belonging to S such that $[P_k] = [S][\operatorname{Nr}(I_k)]$. Let $[S]_n$ denote the image of $[S]$ in $\operatorname{Cl}(R)/\operatorname{Cl}(R)^n$. Then the elements of $\operatorname{Cl}(R)/\operatorname{Cl}(R)^n$ corresponding to k for which there is an optimal embedding $S \to \Lambda_k$ are exactly the elements of the coset $[S]_n(\operatorname{Cl}_S(R)/\operatorname{Cl}(R)^n)$ in $\operatorname{Cl}(R)/\operatorname{Cl}(R)^n$.

(3.4) PROPOSITION. *If $e_{\Lambda_k^*}(S, \Lambda_k) \neq 0$, then its value does not depend on k.*

Proof. Let Λ be a maximal order such that $e_{\Lambda^*}(S, \Lambda) \neq 0$ and $S \subset \Lambda$. Then using (1.2)(b), $e_{\Lambda^*}(S, \Lambda) = |L^* \backslash E_{\Lambda^*}(S, \Lambda)/\Lambda^*|$. Let in the notations of (1.2)(a), $E'_{\mathscr{J}(\Lambda)}(S, \Lambda) = \{\alpha \in \mathscr{J}(\Lambda) : (S, \alpha \circ \Lambda) \in \mathscr{R}$ and $\alpha\Lambda$ is principal$\}$. It is easy to check that the mapping

$$L^* \backslash E_{\Lambda^*}(S, \Lambda)/\Lambda^* \to L^* \backslash E'_{\mathscr{J}(\Lambda)}(S, \Lambda)/\mathscr{U}(\Lambda)$$

given by $L^* a \Lambda^* \mapsto L^* \alpha \mathscr{U}(\Lambda)$, where $\alpha = (a)$, is well defined and injective. But it is also surjective. Indeed, if $\alpha \in E'_{\mathscr{J}(\Lambda)}(S, \Lambda)$, then $\alpha\Lambda = a\Lambda$ for some $a \in \Lambda^*$. It is easy to check that $a \in E_{\Lambda^*}(S, \Lambda)$, so $L^* \alpha \mathscr{U}(\Lambda) = L^*(a)\,\mathscr{U}(\Lambda)$ is the image of $L^* a \Lambda^*$.

Now let $\Lambda_k = \alpha_k \Lambda \alpha_k^{-1}$ be such that $\varphi\colon S \to \Lambda_k$, where $\varphi(x) = a_k^{-1} x a_k$, $a_k \in A^*$, is an optimal embedding. As for Λ, $e_{\Lambda_k^*}(S, \Lambda_k) = |L_k^* \backslash E'_{\mathscr{J}(\Lambda)}(S_k, \Lambda_k)/\mathscr{U}(\Lambda_k)|$, where $L_k = \varphi(L)$ and $S_k = \varphi(S)$. It is easy to see that mapping $L^* \alpha \mathscr{U}(\Lambda)$ onto $L_k^*(a_k^{-1} \alpha \alpha_k^{-1})\,\mathscr{U}(\Lambda_k)$, one gets a bijection between $L^* \backslash E'_{\mathscr{J}(\Lambda)}(S, \Lambda)/\mathscr{U}(\Lambda)$ and $L_k^* \backslash E'_{\mathscr{J}(\Lambda)}(S_k, \Lambda_k)/\mathscr{U}(\Lambda_k)$, so $e_{\Lambda_k^*}(S, \Lambda_k) = e_{\Lambda^*}(S, \Lambda)$.

REFERENCES

1. J. BRZEZINSKI, Riemann–Roch theorem for locally principal orders, *Math. Ann.* **276** (1987), 529–536.
2. J. BRZEZINSKI, A combinatorial class number formula, *J. Reine Angew. Math.*, to appear.
3. C. CHEVALLEY, Sur certains idéaux d'une algèbre simple, *Abh. Math. Sem. Hamburger Univ.* **10** (1934), 83–105.
4. C. W. CURTIS AND I. REINER, "Methods of Representation Theory," Vol I, Wiley, New York, 1981.
5. H. HASSE, Über gewisse Ideale in einer einfachen Algebra, *Act. Sci. Ind. Paris* **109** (1934), 12–16.
6. C. G. LATIMER AND C. C. MACDUFFEE, A correspondence between classes of ideals and classes of matrices, *Ann. of Math.* **34** (1933), 313–316.
7. E. NOETHER, Zerfallende verschränkte Produkte und ihre Maximalordnungen, *Act. Sci. Ind. Paris* **148** (1934), 5–15.
8. O. SCHILLING, Über gewisse Beziehungen zwischen der Arithmetik hyperkomplexer Zahlsysteme und algebraischer Zahlkörper, *Math. Ann.* **111** (1935), 372–398.
9. O. TAUSSKY, On a theorem of Latimer and MacDuffee, *Canad. J. Math.* **1** (1949), 300–302.