GENERA AND DECOMPOSITIONS OF LATTICES OVER ORDERS

BY

H. JACOBINSKI

Göteborg, Sweden

Let k be an algebraic number field of finite degree, A/k a semi-simple finite-dimensional algebra over k and o a Dedekind ring with quotient field k. We consider o-orders R in A, that is, subrings with $kR=A$ and $1 \in R$, such that R is finitely generated as an o-module. An important example is the group ring oG of a finite group G, which is an order in kG. An R-lattice M is a finitely generated (unital) R-module, which is torsion-free as an o-module. The category of R-lattices we denote by $\mathcal{L}_R$. For every prime ideal p in o, let o_p be the p-adic completion and put $R_p = o_p \otimes R$, $M_p = o_p \otimes M$ etc. Then R_p is an o_p-order in A_p and M_p is an R_p-lattice.

Two R_p-lattices M and N belong to the same genus—notation $M \sim N$—if $M_p \cong N_p$ as R_p-modules for every p. By $\mathcal{G}_R$ we denote the category of genera of R-lattices. It is well-known, that $M \sim N$ does not in general imply $M \cong N$; but the number of isomorphism classes in a genus is finite. In the present paper, we first give a classification of these isomorphism classes by means of ideal classes in the integral closure over o of the center of A (Theorem 2.2). This generalizes results of an earlier paper (Jacobinski [9]). The proof makes use of the classical theory of maximal orders and here we need the assumption, that k is an algebraic number field and o Dedekind. For a very small exceptional class of R-lattices, the classification is not complete. This is due to the fact, that maximal orders in a totally definite skew-field of index 2 have rather irregular properties.

We then use our result on the isomorphism classes in a genus to study various properties of R-lattices. As an immediate consequence we obtain an upper bound—depending only on R—for the number of isomorphism classes in a genus (Prop. 2.7).

An R-lattice X is called a local direct factor of M, if for every p, X_p is isomorphic to a direct factor of M_p. We show (Theorem 3.3), that then M has a decomposition of the form $M = X' \oplus N$, with $X' \sim X$. In a very special case—$R = oG$ the group ring of a finite group and X a free oG-module—the existence of such a decomposition was shown by Bass ([2], Prop. 10.2), using results of Swan. Then we deduce a rather mild condition, referring only to the A-modules $k \otimes X$ and $k \otimes M$, in order that a local direct factor X of M be isomorphic to a (global) direct factor of M. (Theorem 3.6). Such a condition can be obtained from a theorem of Serre ([12], and [2], p. 24), which is valid for a wider class of modules than R-lattices but only if X is a free R-module. Our result holds for arbitrary R-lattices X and in case X is free it is somewhat stronger than the one deduced from Serre's theorem.

In section 4 we study cancellation, i.e. under what conditions does a relation $Y \oplus M \cong Y \oplus N$ imply $M \cong N$. In case Y is projective, such a condition follows from the well-known cancellation theorem of Bass (Bass [2], p. 28). Our result also holds for non-projective R-lattices Y and is somewhat stronger for projective Y. This makes it possible to give a rather complete answer to a question raised by Swan (Swan, [13], § 10) concerning cancellation in the category of projective modules over a group ring (see 5.3–5.5).

Let B be a category of R-lattices, which is closed under direct sums. We define a relative Grothendieck group $D(B)$ with relations for split exact sequences only. It turns out, that two R-lattices are in the same genus if and only if their images in $D(\mathfrak{L}_R)$ differ by a torsion element only. We then show that $D(B)$ is the direct sum of a free group and a finite group, which is isomorphic to a group of ideal classes of the same type as the one that occurred in connection with the isomorphism classes in a genus. In particular, if we consider the category $\mathfrak{P}_R$ of finitely generated projective R-modules, then $D(\mathfrak{P}_R)$ coincides with the ordinary Grothendieck group $K(\mathfrak{P}_R)$ and we obtain a rather explicit description of $K(\mathfrak{P}_R)$ from our result on $D(B)$.

In the last section we study decompositions into indecomposable R-lattices. We say that B has unique decomposition, if for every element of B the decomposition into indecomposable R-lattices is unique, up to an automorphism. It is well-known that $\mathfrak{L}_{R_p}$ has unique decomposition and that $\mathfrak{L}_R$ in general has not. We show, that the lack of unicity has two sources. The first comes from the fact that a genus may contain several different isomorphism classes. A survey of the various decompositions arising from this source can be given by means of our result on the isomorphism classes in a genus. The other source comes from the fact that the category $\mathcal{G}_R$—with addition defined in the natural way—does not in general have unique decomposition. We are thus led to study decompositions of genera instead of R-lattices, and we give a survey of the different decompositions of a genus. As a corollary we obtain that there are only finitely many indecomposable projective R-modules (up to isomorphism). If $\mathcal{G}_R$ has unique decomposition, then decompositions in $\mathfrak{L}_R$ are rather regular and easy to describe. We give a sufficient condition for $\mathcal{G}_R$

to have unique decomposition; it turns out that this is the case e.g. if $R = ZG$ where G is a finite p-group and $p \neq 2$.

Notations. By R-lattice we will in general mean left R-lattice. Every R-lattice M will be identified with its image in $k \otimes M$; then we can write kM instead of $k \otimes M$. For brevity we put

$$E(M) = \mathrm{Hom}_R\,(M, M)$$

and

$$E(kM) = \mathrm{Hom}_A\,(kM, kM).$$

It is easily seen that $E(M)$ is an o-order in $E(kM)$. We consider kM as a right $E(kM)$-module; this makes M a right $E(M)$-lattice.

1. Maximal orders

We consider first lattices over a maximal order $\mathfrak{O}$; for the arithmetic of maximal orders see Deuring [5] or Chevalley [3]. A (fractional) full $\mathfrak{O}$-ideal is an $\mathfrak{O}$-lattice $\mathfrak{A} \subset A$, such that $k\mathfrak{A} = A$. $\mathfrak{A}$ is integral if $\mathfrak{A} \subset \mathfrak{O}$. The right order of $\mathfrak{A}$ consists of all $x \in A$ such that $\mathfrak{A}x \subset \mathfrak{A}$. This is also a maximal order in A. When writing a product $\mathfrak{A}\mathfrak{B}$, we will always assume that the right order of $\mathfrak{A}$ equals the left order of $\mathfrak{B}$.—The following proposition was proved by Chevalley [3] for A a skew-field.

PROPOSITION 1.1. *Let $\mathfrak{O}$ be a maximal order in A and $M \in \mathfrak{L}_{\mathfrak{O}}$. Then*

1) $E(M)$ is a maximal order in $E(kM)$

2) if $N \in \mathfrak{L}_{\mathfrak{O}}$ and $kN = kM$, then there is a unique left $E(M)$-ideal $\mathfrak{a}$, such that

$$N = M\mathfrak{a}.$$

For a proof see [9], Satz 1 (or [1], p. 12), where only the unicity of $\mathfrak{a}$ is lacking. If $M\mathfrak{a} = M\mathfrak{b}$, then both $\mathfrak{a}\mathfrak{b}^{-1}$ and its inverse $\mathfrak{b}\mathfrak{a}^{-1}$ are in $E(M)$ and this implies $\mathfrak{a} = \mathfrak{b}$ ([5], p. 74). The proposition implies that $M \cong N$ if and only if $\mathfrak{a}$ is a principal ideal, $\mathfrak{a} = E(M)a$, $a \in E(kM)$. Passing to the p-adic completion, we obtain

COROLLARY 1.2. *Two $\mathfrak{O}$-lattices M and N are in the same genus if and only if $kM \cong kN$ as A-modules.*

If $kM \cong kN$, we may suppose $kM = kN$. Then $N = M\mathfrak{a}$ and $M_p = N_p\mathfrak{a}_p$. Now $E(M_p)$ is a maximal order and every $E(M_p)$-ideal is principal. Thus we obtain $M_p \cong N_p$ and the other direction follows from the Theorem of Deuring–Noether.

Let Γ be the genus that contains M. The corollary implies, that the isomorphism classes in Γ are in 1–1-correspondence with the left ideal classes in $E(M)$. Eichler [6] has shown that the ideal classes in a maximal order are in 1–1-correspondence with certain ideal classes in the center, the application being given by the reduced norm. This means that the isomorphism classes in Γ correspond to certain ideal classes in the center of $E(M)$. We are now going to explain this in more detail.

Let $A = \oplus \sum A_i$ be the decomposition of A into simple algebras and let e_i be the identity of A_i. For any R-lattice M put

$$e_M = \sum_{e_i M \neq 0} e_i.$$

Then $e_M M = M$ and $(1-e_M)M = 0$. If $M \sim N$, then $e_M = e_N$ and we can write e_Γ instead of e_M. Let K_i be the center of A_i and denote by C_i the integral closure of oe_i in K_i. Then $K = \oplus \sum K_i$ is the center of A, $C = \oplus \sum C_i$ the maximal o-order in K and $e_M K$ the center of $E(kM)$. A maximal order always contains the maximal order of its center. Thus, for $M \in \mathfrak{L}_{\mathfrak{D}}$, $e_M C$ is the center of $E(M)$.

Let $I(e_M)$ be the group of invertible fractional $e_M C$-ideals. We embed $I(e_M)$ in $I = I(1)$ by $x \to x \oplus (1-e_M)C$ and consider $I(e_M)$ as a subgroup of I. Denote by n_i the reduced norm of $E(e_i kM)$ over K_i and put $n = \sum n_i$. For $x \in E(kM)$ the reduced norm $n(x)$ is then an element of $e_M K$. The norm $n(\mathfrak{a})$ of an $E(M)$-ideal is the ideal in $e_M C$ generated by all $n(a)$, $a \in \mathfrak{a}$. It is well-known (see Deuring [5], VI, § 4) that

$$n(\mathfrak{a}\mathfrak{b}) = n(\mathfrak{a})n(\mathfrak{b})$$

provided that the right order of $\mathfrak{a}$ coincides with the left order of $\mathfrak{b}$. Now Proposition 1.1 permits us to define the reduced norm for a pair of $\mathfrak{D}$-lattices M and N, provided $kM = kN$. For then there is a unique left $E(M)$-ideal $\mathfrak{a}$ such that $N = M\mathfrak{a}$ and we define

$$n(M, N) = n(\mathfrak{a}) \quad \text{for } N = M\mathfrak{a}.$$

According to this definition, $n(M, N)$ is an ideal in $I(e_M)$. Since we have identified $I(e_M)$ with a subgroup of $I(1)$, we can as well consider $n(M, N)$ an ideal in $I(1)$.

Let $\bar{\Gamma}$ be the set of all $N \in \Gamma$ such that kN is a fixed A-module. Then $\bar{\Gamma}$ represents all isomorphism classes in Γ and the reduced norm defines a map

$$n : \bar{\Gamma} \times \bar{\Gamma} \to I(e_\Gamma).$$

This is an epimorphism because from the arithmetic of maximal orders it is well known, that every ideal in $I(e_\Gamma)$ is the norm of some left $E(M)$-ideal. We note some simple properties of the reduced norm. First we have

$$n(M, N) = n(M, U)\, n(U, N) \quad \text{if } M, N, U \in \bar{\Gamma}. \tag{1}$$

Put $U=M\mathfrak{b}$ and $N=U\mathfrak{c}$; then $N=M\mathfrak{b}\mathfrak{c}$. Since the right order of $\mathfrak{b}$ coincides with the left order of $\mathfrak{c}$, we have $n(\mathfrak{b}\mathfrak{c})=n(\mathfrak{b})n(\mathfrak{c})$ which is equivalent to (1).

Now suppose $M=X\oplus Y$ with $X, Y\in\mathcal{L}_{\mathfrak{O}}$ and let $N\in\overline{\Gamma}$ be of the form $N=X'\oplus Y'$ with $kX=kX'$ and $kY=kY'$. Since we consider $I(e_X)$ as a subgroup of I, $n(X, X')$ is in I and we have $n(X, X')=n(X\oplus Y, X'\oplus Y)$. Then from (1) we obtain

$$n(X\oplus Y, X'\oplus Y')=n(X, X')\, n(Y, Y') \tag{2}$$

It is well-known, that maximal orders in a totally definite skew field of index 2 have rather exceptional properties. As a consequence of this there is a—rather small—class of $\mathfrak{O}$-lattices which behave irregularly and which often must be excluded in the sequel. We are now going to define the class of well-behaved lattices; since the situation is similar for non-maximal orders, we do this at once for arbitrary orders R.

Recall that an infinite prime of K_i is an archimedian valuation of K_i and that the prime is said to be ramified in A_i if the corresponding algebra over the completion of K_i does not split, i.e. if it is a ring of matrices over the quaternions. Let $r(A_i, M)$ denote the number of irreducible A_i-modules in a decomposition of kM. Then if A_i is a ring of matrices over the skew-field Ω_i, $E(e_ikM)$ is a ring of matrices of degree $r(A_i, M)$ over Ω_i. Then we define

Definition 1.3. *$\mathcal{L}'_R$ consists of all R-lattices M such that $r(A_i, M)\neq 1$ whenever A_i is a ring of matrices over a skew-field of index 2 over K_i, in which every infinite prime of K_i is ramified.*

Note that this is a condition on kM only. Equivalently we could say that M is in $\mathcal{L}'_R$ if and only if none of the simple algebras in $E(kM)$ is a totally definite skew field of index 2.

Now let $S(e_M)$ be the subgroup of principal ideals (a) in $I(e_M)$, such that each e_ia is positive at every infinite prime of K_i, that is ramified in A_i. Then we have

Theorem 1.4. (Eichler) *For $M\in\mathcal{L}'_{\mathfrak{O}}$ a full left $E(M)$-ideal $\mathfrak{a}$ is principal, if and only if $n(\mathfrak{a})\in S(e_M)$.*

For a proof see [6]. Since we are concerned with isomorphism classes in a genus rather than with ideal classes in a maximal order we reformulate this in the following way. Denote by $\mathcal{G}'_{\mathfrak{O}}$ the genera in $\mathcal{L}'_{\mathfrak{O}}$ and suppose $\Gamma\in\mathcal{G}'_{\mathfrak{O}}$. Put $V_\Gamma=I(e_\Gamma)/S(e_\Gamma)$ and, for $M, N\in\overline{\Gamma}$, let $v(M, N)$ be the image of $n(M, N)$ in V_Γ. Now from (1) and the theorem it follows that $v(M, N)$ does not change if M and N are replaced by isomorphic lattices. Thus we can extend the definition of $v(M, N)$ to all M, N in Γ. Let M be fixed and consider the map $N\to v(M, N)$ for $N\in\Gamma$. Then the theorem says that this map is a bijection of the isomorphism classes in Γ onto V_Γ. In the next section we will derive a similar result for genera of R-lattices, where R is an arbitrary o-order in A.

2. Isomorphism classes in a genus

Let R be any o-order in A. We choose a maximal order $\mathfrak{O}$ which contains R and a two sided $\mathfrak{O}$-ideal $\mathfrak{F}$ contained in R; such ideals exist since both $\mathfrak{O}$ and R are finitely generated o-modules and $k\mathfrak{O}=kR=A$. We do not suppose that $\mathfrak{F}$ is the maximal two-sided $\mathfrak{O}$-ideal in R. Recall that we identify M with its image in $k\otimes M$. Then we have

$$\mathfrak{F}M\subset M\subset \mathfrak{O}M.$$

This relation can be used to give several different characterizations of the lattices that belong to the genus determined by M (see Jacobinski [9], Satz 2). We will now explain one of these.

A fractional $E(\mathfrak{O}M)$-ideal $\mathfrak{a}$ is said to be prime to $\mathfrak{F}$, if for every prime p in o, $\mathfrak{F}_p\neq(1)$ implies $\mathfrak{a}_p=(1)$. The same definition applies also to C-ideals or o-ideals. If $\mathfrak{a}$ is integral, then $\mathfrak{a}$ is prime to $\mathfrak{F}$ if and only if $n(\mathfrak{a})$, taken in $E(\mathfrak{O}M)$, is prime to $n(\mathfrak{F})$, taken in $\mathfrak{O}$.

Let $\mathfrak{a}$ be prime to $\mathfrak{F}$. Then $\mathfrak{a}=\alpha^{-1}\mathfrak{a}'$, with $\alpha\in e_M C$, $\mathfrak{a}'$ an integral $E(\mathfrak{O}M)$-ideal and both $\mathfrak{a}'$ and α prime to $\mathfrak{F}$. Then we define

$$M_{\mathfrak{a}}=\alpha^{-1}(M\cap \mathfrak{O}M\mathfrak{a}').$$

$M_{\mathfrak{a}}$ is an R-lattice and according to [9], Satz 2, we have:

PROPOSITION 2.1. *Two R-lattices M and N are in the same genus if and only if there is a left $E(\mathfrak{O}M)$-ideal $\mathfrak{a}$, which is prime to $\mathfrak{F}$, such that $N\cong M_{\mathfrak{a}}$.*

Now choose an arbitrary element X of Γ and let $\bar{\Gamma}$ be the set of all $X_{\mathfrak{a}}$ where $\mathfrak{a}$ runs through all left $E(\mathfrak{O}X)$-ideals, prime to $\mathfrak{F}$. Then every isomorphism class in Γ contains an element of $\bar{\Gamma}$ and in studying isomorphism classes, we can replace Γ by $\bar{\Gamma}$. We remark first that

$$\mathfrak{O}X_{\mathfrak{a}}=\mathfrak{O}X\mathfrak{a} \tag{3}$$

for we have $\mathfrak{O}X\mathfrak{a}\supset\mathfrak{O}(X_{\mathfrak{a}})\supset\mathfrak{F}X\mathfrak{a}$ and if $\mathfrak{F}_p=(1)$ this implies $(\mathfrak{O}X_{\mathfrak{a}})_p=(\mathfrak{O}X\mathfrak{a})_p$. But since $\mathfrak{a}$ is prime to $\mathfrak{F}$, $\mathfrak{F}_p\neq(1)$ implies $\mathfrak{a}_p=(1)$ and then $(\mathfrak{O}X_{\mathfrak{a}})_p=(\mathfrak{O}X)_p=(\mathfrak{O}X\mathfrak{a})_p$, which proves (3). From (3) it follows easily that every R-lattice M in $\bar{\Gamma}$ determines a unique left $E(\mathfrak{O}X)$-ideal $\mathfrak{a}$ such that $M=X_{\mathfrak{a}}$. For $X_{\mathfrak{a}}=X_{\mathfrak{b}}$ implies $\mathfrak{O}X\mathfrak{a}=\mathfrak{O}X\mathfrak{b}$ and this implies $\mathfrak{a}=\mathfrak{b}$ according to Proposition 1.1.

Now let M, N be a pair of R-lattices in $\bar{\Gamma}$. This pair uniquely determines the pair $\mathfrak{O}M$, $\mathfrak{O}N$ of $\mathfrak{O}$-lattices and for this pair we have defined $n(\mathfrak{O}M, \mathfrak{O}N)$ in the preceding section. Thus for $M, N\in\bar{\Gamma}$ we can define

$$n(M, N)=n(\mathfrak{O}M, \mathfrak{O}N).$$

According to this definition, $n(M, N)$ seems to depend on the choice of the maximal order $\mathfrak{O}$. This is, however, not the case, for $n(M, N)$ is already determined by the pair M, N considered as modules over the center of R (see Jacobinski [9], § 3).

Let $I_{\mathfrak{F}}(e_\Gamma)$ be the group of all invertible fractional $e_\Gamma C$-ideals that are prime to $\mathfrak{F}$. If we put $M = X_{\mathfrak{a}}$ and $N = X_{\mathfrak{b}}$, then from (3) we see that $\mathfrak{O}N = \mathfrak{O}M\mathfrak{a}^{-1}\mathfrak{b}$ and so $n(M, N) = n(\mathfrak{a}^{-1}\mathfrak{b})$ is prime to $\mathfrak{F}$ since $\mathfrak{a}$ and $\mathfrak{b}$ are prime to $\mathfrak{F}$. Thus $n(M, N)$ is in $I_{\mathfrak{F}}(e_\Gamma)$ for $M, N \in \overline{\Gamma}$.

Now let $M = X_{\mathfrak{a}}$ be fixed and let N vary in $\overline{\Gamma}$. Then $n(M, N)$ defines a map

$$n\colon \overline{\Gamma} \to I_{\mathfrak{F}}(e_\Gamma).$$

This map is an epimorphism. For every $c \in I_{\mathfrak{F}}(e_\Gamma)$ is the norm of some left $E(\mathfrak{O}M)$-ideal $\mathfrak{c}$, which is prime to $\mathfrak{F}$. Putting $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$ and $N = X_{\mathfrak{b}}$ we see from (3) that $n(M, N) = n(\mathfrak{c}) = c$ as desired.

Denote by H_M the subgroup of $I_{\mathfrak{F}}(e_\Gamma)$ generated by principal ideals of the form $(n(a))$ with $a \in E(M)$ and put

$$V_M = I_{\mathfrak{F}}(e_\Gamma)/H_M.$$

We will show later that $M \sim N$ implies $H_M = H_N$. Assuming this we can write H_Γ and V_Γ instead of H_M and V_M. Denote by $v(M, N)$ the image of $n(M, N)$ in V_Γ. Then v defines an epimorphism

$$v\colon \overline{\Gamma} \times \overline{\Gamma} \to V_\Gamma.$$

We now show

THEOREM 2.2. *Suppose $\Gamma \in \mathcal{G}'_R$ and let M be any fixed lattice in $\overline{\Gamma}$. Then for $N \in \overline{\Gamma}$, the map*

$$N \to v(M, N)$$

defines a bijection of the isomorphism classes in $\overline{\Gamma}$ onto V_Γ; in particular, $M \cong N$ if and only if $v(M, N) = 1$.

The proof will be divided into several lemmas. The first is

LEMMA 2.3. *If $\mathfrak{a}$ is integral, then $M \cong M_{\mathfrak{a}}$ is equivalent to $\mathfrak{a} = E(\mathfrak{O}M)a$ with $a \in E(M)$.*

Since $\mathfrak{a}$ is integral, $M_{\mathfrak{a}}$ is contained in M. Thus if $M_{\mathfrak{a}} \cong M$, then there is an $a \in E(M)$ such that $M_{\mathfrak{a}} = Ma$ and $\mathfrak{O}M_{\mathfrak{a}} = \mathfrak{O}M\mathfrak{a} = \mathfrak{O}Ma$ implies $\mathfrak{a} = E(\mathfrak{O}M)a$. On the other hand, suppose $\mathfrak{a} = E(\mathfrak{O}M)a$ with $a \in E(M)$ and a prime to $\mathfrak{F}$. Then Ma and $M_{\mathfrak{a}}$ coincide at every p. This means $Ma = M_{\mathfrak{a}}$ and so $M \cong M_{\mathfrak{a}}$.

LEMMA 2.4. (Eichler). *Suppose $M \in \mathfrak{L}'_R$ and define the two-sided $E(\mathfrak{O}M)$-ideal $\mathfrak{f}$ by $\mathfrak{F}M = \mathfrak{O}M\mathfrak{f}$. If $x \in E(\mathfrak{O}M)$ and*

$$n(x) \equiv \varepsilon \quad (\mathfrak{f})$$

with ε a unit in $e_M C$, then there is a unit $u \in E(\mathfrak{O}M)$, such that

$$x \equiv u \quad (\mathfrak{f}).$$

For a proof see Eichler [7], p. 239.

LEMMA 2.5. *If $M \in \mathfrak{L}'_R$, then $M \cong M_\mathfrak{a}$ if and only if $n(\mathfrak{a}) \in H_M$.*

Multiplying $\mathfrak{a}$ by an element of o, we can assume that $\mathfrak{a}$ is integral, i.e. $M_\mathfrak{a} \subset M$. Then clearly $M \cong M_\mathfrak{a}$ implies $n(\mathfrak{a}) \in H_M$. On the other hand, suppose $n(\mathfrak{a}) \in H_M$. Since $H_M \subset S(e_M)$, Theorem 1.5 implies that $\mathfrak{a} = E(\mathfrak{O}M)a$, with $a \in E(\mathfrak{O}M)$. Then $n(\mathfrak{a}) \in H_M$ means that there is $b \in E(M)$, such that $n(a) = n(b)\varepsilon$, with ε a unit in $e_M C$. Since both a and b are prime to $\mathfrak{F}$, we can find $\alpha \in e_M C$, $\alpha \equiv 1$ $(\mathfrak{f})$ such that $x = \alpha a b^{-1}$ is in $E(\mathfrak{O}M)$. Then $n(x) = n(\alpha)\varepsilon \equiv \varepsilon$ $(\mathfrak{f})$ and according to the preceding lemma, there is a unit u in $E(\mathfrak{O}M)$, such that $x = u(1+y)$ with $y \in \mathfrak{f}$. This implies $\alpha\mathfrak{a} = E(\mathfrak{O}M)(1+y)b$. Now $y \in \mathfrak{f}$ implies that $M(1+y) \subset M + M\mathfrak{f} = M$. Thus $(1+y)b$ is in $E(M)$ and Lemma 2.3 implies that $M_{\alpha\mathfrak{a}} \cong M$, which is equivalent to $M_\mathfrak{a} \cong M$.

LEMMA 2.6. *If $M \in \mathfrak{L}'_R$ and $M \sim N$, then $H_M = H_N$.*

Let $S_\mathfrak{F}(e_M)$ be the subgroup of $I_\mathfrak{F}(e_M)$ generated by all ideals (α) with $\alpha \equiv 1$ $(\mathfrak{F})$ and such that each $e_i\alpha$ is positive at those infinite primes of K_i that are ramified in A_i. We will first show that both H_M and H_N contain $S_\mathfrak{F}(e_M)$.

As before, define $\mathfrak{f}$ by $\mathfrak{O}M\mathfrak{f} = \mathfrak{F}M$. Then for $\alpha \in C$ the congruences $\alpha \equiv 1$ $(\mathfrak{F})$ and $\alpha \equiv 1$ $(\mathfrak{f})$ are equivalent. For $\mathfrak{F}$ is a two-sided integral $\mathfrak{O}$-ideal and so there is an integer $s > 0$, such that $\mathfrak{F}^s = g\mathfrak{O}$, with g an ideal in C. But then $\mathfrak{F}^s M = \mathfrak{O}M\mathfrak{f}^s = \mathfrak{O}Mg$ and this implies $\mathfrak{f}^s = E(\mathfrak{O}M)g$. Thus for $\alpha \in e_M C$, $\alpha \equiv 1$ $(\mathfrak{F})$ is equivalent to $(\alpha - 1)^s \equiv 0$ $(e_M g)$. Since the same is true for $\alpha \equiv 1$ $(\mathfrak{f})$, these congruences are in fact equivalent.

Now let (α) be an integral ideal in $S_\mathfrak{F}(e_M)$. Because of Theorem 1.4, (α) is the norm of a principal ideal $\mathfrak{a} = E(\mathfrak{O}M)a$, which can be supposed prime to $\mathfrak{F}$ and integral. Then $n(a) = \alpha\varepsilon \equiv \varepsilon$ $(\mathfrak{f})$ with ε a unit in $e_M C$. From Lemma 2.4 we see, that $\mathfrak{a}$ is generated by an element $1+y$, with $y \in \mathfrak{f}$. Since $1+y \in E(M)$, this shows that $S_\mathfrak{F}(e_M) \subset H_M$ for every $M \in \mathfrak{L}'_R$.

To prove the lemma, we now have to show, that H_M and H_N are equal modulo $S_\mathfrak{F}(e_M)$. If $N \cong N'$, then certainly $H_N = H_{N'}$. Thus we can suppose $N = M_\mathfrak{b}$, with $\mathfrak{b}$ integral and prime to $\mathfrak{F}$. Then we can find $\beta \in e_M C$, such that $\beta M \subset M_\mathfrak{b}$; since $\mathfrak{b}$ is prime to $\mathfrak{F}$, we can even choose $\beta \equiv 1$ $(\mathfrak{f})$. Then $a \in E(M)$ implies $\beta a \in E(N)$. Since $n(a) \equiv n(\beta a)$ $(\mathfrak{f})$, this means $H_M \subset H_N$. By symmetry we obtain $H_M = H_N$, which completes the proof of Lemma 2.6.

Combining Lemma 2.5 and 2.6, we have shown, that for M and N in $\bar{\Gamma}$, $M \cong N$ is equivalent to $n(M, N) \in H_\Gamma$, that is to $v(M, N)=1$. For N' in $\bar{\Gamma}$, we obtain from (1) that

$$v(M, N') = v(M, N)\, v(N, N').$$

Since $v(N, N')=1$ if and only if $N \cong N'$, the map $\bar{\Gamma} \to V_\Gamma$, defined by $N \to v(M, N)$ is an injection on the isomorphism classes of $\bar{\Gamma}$; it is also surjective, since every ideal in $I_{\mathfrak{F}}(e_\Gamma)$ is the norm of some $E(\mathfrak{O}M)$-ideal prime to $\mathfrak{F}$. This completes the proof of Theorem 2.2.

Remark 1. We have defined $v(M, N)$ only if N is in $\bar{\Gamma}$. Because of the theorem, $v(M, N)$ depends only on the isomorphism classes and we can extend the definition to arbitrary M, N in Γ: if $N \cong M_{\mathfrak{a}}$, we put $v(M, N) = v(M, M_{\mathfrak{a}})$.

Remark 2. We indicate briefly what happens if M does not belong to $\mathfrak{L}'_R$. Then H_M, V_M and the map $N \to v(M, N)$ are still well-defined. Since Lemma 2.3 is valid for every $M \in \mathfrak{L}_R$, the map $\bar{\Gamma} \to V_M$ is a map of the isomorphism classes in $\bar{\Gamma}$ and it is still an epimorphism. But it need no longer be injective; in particular, $v(M, N) = v(M, N')$ is necessary but not sufficient for $N \cong N'$.

We now derive some consequences of the theorem. Let $|\Gamma|$ denote the number of isomorphism classes in Γ. Then we have

PROPOSITION 2.7. *There is a number b, depending only on R, such that $|\Gamma| \leq b$ for every genus Γ in $\mathcal{G}_R$.*(1)

Suppose first that $\Gamma \in \mathcal{G}'_R$. Then according to the theorem, $|\Gamma|$ equals the order of V_Γ. Since $S_{\mathfrak{F}}(e_\Gamma) \subset H_\Gamma$, the group V_Γ is a homomorphic image of $I_{\mathfrak{F}}(e_\Gamma)/S_{\mathfrak{F}}(e_\Gamma)$. If b' is the order of the group $I_{\mathfrak{F}}(1)/S_{\mathfrak{F}}(1)$ we thus obtain that $|\Gamma| \leq b'$ for $\Gamma \in \mathcal{G}'_R$.

Now suppose $\Gamma \notin \mathcal{G}'_R$ and choose $M \in \Gamma$. Then for at least one i, $e_i kM$ is an irreducible A_i-module and A_i is a ring of matrices over a totally definite skew-field of index 2. Let ε be the sum of all these e_i and let $\varepsilon' = 1 - \varepsilon$. Put $S = \varepsilon kM \cap M$ and $S' = \varepsilon' M$; then $S' \in \mathfrak{L}'_R$ and we have an exact sequence

$$0 \to S \to M \to S' \to 0.$$

If $N \sim M$, we have a similar sequence

$$0 \to T \to N \to T' \to 0$$

and corresponding sequences for M_p and N_p. Since T and T' are defined by means of the central idempotents ε and ε' respectively, an isomorphism $M_p \to N_p$ gives rise to isomorphisms

(1) Another proof of this has recently been given by Roiter, (Roiter [13]) by means of other methods.

$S_p \to T_p$ and $S'_p \to T'_p$. Thus $M \sim N$ implies $S \sim T$ and $S' \sim T'$. In other words, the genera Λ and Λ' that contain S and S' respectively are uniquely determined by Γ. Moreover, $S \cong T$ and $S' \cong T'$ together with $M \sim N$ imply that $M \cong N$ (see [4], Theorem 72.25 and 75.27). From this we see that

$$|\Gamma| \leqslant |\Lambda||\Lambda'| \quad \text{for arbitrary } \Gamma \in \mathcal{G}_R.$$

Since $\Lambda' \in \mathcal{G}'_R$, we know already that $|\Lambda'| \leqslant b'$, where b' only depends on R. To find a similar bound for $|\Lambda|$, we observe that if $T \in \Lambda$, then each $e_i kT$ is either $=0$ or irreducible. Thus there is only a finite number of possibilities for the A-module kT. But then, according to the theorem of Jordan–Zassenhaus, there is only a finite number of possibilities for the genus Λ. If c is an upper bound for the number of isomorphism classes in these genera, we obtain that $|\Gamma| \leqslant cb' = b$, which completes the proof.

The following proposition gives a global characterization of the lattices belonging to the same genus (cf. Proposition 5.1). Let zM denote the direct sum of z copies of M.

PROPOSITION 2.8. *There is an integer z, depending only on R, such that for $M, N \in \mathfrak{L}_R$*

$$M \sim N \quad \textit{if and only if} \quad zM \cong zN.$$

Let t be the exponent of the group $I_{\mathfrak{F}}(1)/S_{\mathfrak{F}}(1)$ and choose $z > 1$ and divisible by t. If $M \sim N$ we obtain from (2) that

$$n(zM, zN) = n(M, N)^z \in S_{\mathfrak{F}}(e_M) \subset H_{zM}.$$

Since $z > 1$, $r(A_i, zM)$ is always $\neq 1$. Consequently, zM is in $\mathfrak{L}'_R$ and the theorem implies that $zM \cong zN$. On the other hand, $zM \cong zN$ implies $zM_p \cong zN_p$ for every p and this implies $M_p \cong N_p$ since $\mathfrak{L}_{R_p}$ has unique decomposition ([4], p. 540).

As in [9] we define restricted genera in the following way.

DEFINITION 2.9. *Two R-lattices M and N are in the same restricted genus if $M \sim N$ and $\mathfrak{O}M \cong \mathfrak{O}N$.*

According to this definition, the division $\Gamma = \bigcup \gamma_i$ of a genus Γ into restricted genera γ_i depends on the choice of $\mathfrak{O}$. However, if $\Gamma \in \mathcal{G}'_R$, the choice of $\mathfrak{O}$ does not matter (see [9], § 3). Suppose $\Gamma \in \mathcal{G}'_R$ and let $M, N \in \bar{\Gamma}$. Then, according to Theorem 1.4, $\mathfrak{O}M \cong \mathfrak{O}N$ if and only if $n(\mathfrak{O}M, \mathfrak{O}N) \in S(e_M)$. Now $n(\mathfrak{O}M, \mathfrak{O}N) = n(M, N)$; putting $\bar{\gamma} = \gamma \cap \bar{\Gamma}$, we see that for $M, N \in \bar{\gamma}$, the map

$$N \to v(M, N)$$

defines a bijection of the isomorphism classes in $\bar{\gamma}$ onto $S(e_\Gamma) \cap I_{\mathfrak{F}}(e_\Gamma) / H_\Gamma$. Since this group depends only on Γ, all the restricted genera in Γ have the same number of isomorphism classes (provided $\Gamma \in \mathcal{G}'_R$). Moreover, the number of restricted genera in Γ equals the order of $I_{\mathfrak{F}}(e_\Gamma) / S(e_\Gamma) \cap I_{\mathfrak{F}}(e_\Gamma)$; it depends only on e_Γ.

The following proposition generalizes an earlier result of the author (see Jacobinski [9], Corollary 2 of Theorem 5).

PROPOSITION 2.10. *There is an R-lattice T, such that for every $M, N \in \mathfrak{L}'_R$, M and N are in the same restricted genus, if and only if*

$$M \oplus T \cong N \oplus T.$$

Let T be an $\mathfrak{O}$-lattice in $\mathfrak{L}'_{\mathfrak{O}}$ such that $e_T = 1$. Then $T \in \mathfrak{L}'_R$ and, since $\mathfrak{O}$ is maximal, we have $H_T = S(1) \cap I_{\mathfrak{F}}(1)$. Now $H_{M\oplus T} \supset H_T$ and so we obtain $H_{M\oplus T} = S(1) \cap I_{\mathfrak{F}}(1)$. This means that the restricted genus γ determined by $M \oplus T$ contains only one isomorphism class. Thus if M and N are in the same restricted genus, then $M \oplus T$ and $N \oplus T$ are both in γ, i.e. $M \oplus T \cong N \oplus T$. Conversely, if $M \oplus T \cong N \oplus T$ then first $M \sim N$, since the Krull–Schmidt theorem is valid for R_p-lattices. Moreover, we have $\mathfrak{O}M \oplus \mathfrak{O}T \cong \mathfrak{O}N \oplus \mathfrak{O}T$ and according to (2) and Theorem 1.4 this implies $n(\mathfrak{O}M, \mathfrak{O}N) \in S(e_M)$. Since we have supposed $M, N \in \mathfrak{L}'_R$, we obtain $\mathfrak{O}M \cong \mathfrak{O}N$, which completes the proof.

3. Local and global decompositions

An R-lattice X is called a local direct factor of M if for every p, X_p is isomorphic to a direct factor of M_p. This is in fact a property of the genera $\Gamma(M)$ and $\Gamma(X)$ determined by M and X. We will study the relations between local and global direct factors of an R-lattice M. First we show that the genus $\Gamma(X)$ always contains a direct factor of M. In the special case $R = oG$, the group ring of a finite group and X a free oG-module, this was proved by Bass, using results of Swan ([2], Prop. 10.2). Then we give a rather mild condition, which assures that a local direct factor is isomorphic to a direct factor of M. As already pointed out in the introduction, if X is a projective R-module, such a condition follows from a theorem of Serre ([2], Theorem 9.3).

We have previously defined two R-lattices to belong to the same genus if $M_p \cong N_p$ for every p. It is easy to see that it is sufficient if p varies in a finite set U, determined by R (cf. Curtis–Reiner [4], p. 571, where U is the set of primes dividing the Higman ideal $i(R)$).

LEMMA 3.1. *Let $U \neq \emptyset$ be a finite set of prime ideals in o, which contains all primes p such that R_p is not a maximal order. Then $M \sim N$ is equivalent to*

$$M_p \cong N_p \quad \textit{for } p \in U.$$

Since $U \neq \emptyset$, $M_p \cong N_p$ for $p \in U$ implies $kM \cong kN$. But for $q \notin U$, R_q is a maximal order in A_q and then $k_q M_q \cong k_q N_q$ implies $M_q \cong N_q$ (cf. Corollary 1.2) and this completes the proof.

If R is a maximal order, we can choose $U \neq \emptyset$ arbitrarily. For R not maximal, we have already chosen a maximal order $\mathfrak{O}$ and a two-sided ideal $\mathfrak{F} \subset R$, and we can take U to be the set of all primes in o such that $\mathfrak{F}_p \neq (1)$. In the sequel, we will always suppose U to be chosen in this way.

Note also that in the definition of a local direct factor we need only claim that X_p is isomorphic to a direct factor of M_p for $p \in U$. For then we have $kM \cong kX \oplus S$. Let Y be an $\mathfrak{O}$-lattice such that $kY = S$. Then according to Corollary 1.2 we have

$$\mathfrak{O}M \sim \mathfrak{O}X \oplus Y.$$

But for $p \notin U$, $R_p = \mathfrak{O}_p$ and so $M_p = (\mathfrak{O}M)_p$ and $X_p = (\mathfrak{O}X)_p$. This shows, that X_p is isomorphic to a direct factor of M_p for every p.

The lemma implies that any genus Γ is completely determined by the set $\{M_p\}_{p \in U}$ for $M \in \Gamma$. On the other hand, suppose we are given R_p-lattices Y^p for $p \in U$. If these Y^p are chosen arbitrarily, there will not in general exist an R-lattice M such that $M_p \cong Y^p$ and then the set $\{Y^p\}$ will not define a genus.—The following lemma is a slight generalization of results of Heller (see [8], where o is a valuation ring).

LEMMA 3.2. *Suppose given for every $p \in U$ a R_p-lattice Y^p. Then there exists $M \in \mathfrak{L}_R$ such that*

$$M_p \cong Y^p \quad \textit{for all } p \in U$$

if and only if there is an A-module S, such that

$$k_p \otimes_k S \cong k_p \otimes_{o_p} Y^p \quad \textit{for all } p \in U.$$

The condition is clearly necessary. To show that it is sufficient, let N be an $\mathfrak{O}$-lattice with $kN = S$. Replacing every Y^p by an isomorphic lattice we can then suppose $Y^p \subset N_p$. We consider N as a submodule of each N_p and put

$$M = \bigcap_{p \in U} N \cap Y^p.$$

The annihilator of each $N / N \cap Y^p$ is a power of p and from this we see that $M_p \cong Y^p$ for $p \in U$ and $M_p \cong N_p$ otherwise. It remains to show that M is an R-lattice. Clearly M is a finitely generated o-module and $kM = S$. Let $R' = \{x \mid xM \subset M, x \in A\}$ be the left order of M. Then $M_p = Y^p$ implies $R_p \subset R'_p$ for $p \in U$. For $p \notin U$ we have $M_p = N_p$ and $R'_p = \mathfrak{O}_p = R_p$. Thus for every p the left order of M_p contains R_p and this implies $M \in \mathfrak{L}_R$.

THEOREM 3.3. *Let X and M be R-lattices and suppose that X is a local direct factor of M. Then there is a decomposition*

$$M = X' \oplus Y, \ \textit{with}\ X' \sim X \ \textit{and}\ Y \in \mathfrak{L}_R.\text{(1)}$$

Since X is a local direct factor of M, there are R_p-lattices Y^p such that

$$M_p \cong X_p \oplus Y^p, \quad p \in U.$$

Moreover, kX is isomorphic to a direct factor of kM; put $kM \cong kX \oplus S$. Then, according to Lemma 3.2 there is an R-lattice Y such that $Y_p \cong Y^p$ for every $p \in U$. This means $M \sim X \oplus Y$ and the theorem now follows from

LEMMA 3.4. *Let X and Y be R-lattices and suppose*

$$M \sim X \oplus Y.$$

Then there is a decomposition

$$M = X' \oplus Y' \ \textit{with}\ X' \sim X \ \textit{and}\ Y' \sim Y.$$

If X and Y are in $\mathfrak{L}'_R$. this follows easily from Theorem 2.2. To show it without this assumption put $N = X \oplus Y$. Replacing M by an isomorphic lattice, we can suppose $M = N_{\mathfrak{a}}$ with $\mathfrak{a}$ an integral left $E(\mathfrak{O}N)$-ideal prime to $\mathfrak{F}$. Then $\mathfrak{O}M = \mathfrak{O}N\mathfrak{a}$ is contained in $\mathfrak{O}N$. Put $\mathfrak{O}M \cap \mathfrak{O}X = \mathfrak{O}X\mathfrak{b}$ where $\mathfrak{b}$ is a left $E(\mathfrak{O}X)$-ideal prime to $\mathfrak{F}$. Then $\mathfrak{O}M/\mathfrak{O}X\mathfrak{b}$ is an $\mathfrak{O}$-lattice too. Since $\mathfrak{O}$ is hereditary, every $\mathfrak{O}$-lattice is a projective $\mathfrak{O}$-module and so every exact sequence of $\mathfrak{O}$-lattices splits. Thus we obtain

$$\mathfrak{O}M = \mathfrak{O}X\mathfrak{b} \oplus T \quad \text{with } T \in \mathfrak{L}_{\mathfrak{O}}.$$

Every element of $\mathfrak{O}M$ is of the form $x+y$ with $x \in \mathfrak{O}X$ and $y \in \mathfrak{O}Y$. Let $\mathfrak{O}X\mathfrak{b}'$ be the projection of $\mathfrak{O}M$ on $\mathfrak{O}X$. Then we have $\mathfrak{O}X \supset \mathfrak{O}X\mathfrak{b}' \supset \mathfrak{O}X\mathfrak{b}$ and so $\mathfrak{b}'$ is prime to $\mathfrak{F}$. Thus we can find $\delta \in o$, $\delta \equiv 1\ (\mathfrak{F})$, such that $\mathfrak{b}'\delta \subset \mathfrak{b}$. Put

$$\mathfrak{O}M\mathfrak{d} = \mathfrak{O}X\mathfrak{b} \oplus T\delta.$$

Then clearly $\mathfrak{O}M\mathfrak{d} = \mathfrak{O}X\mathfrak{b} \oplus \mathfrak{O}Y\mathfrak{c}$ with $\mathfrak{c}$ a left $E(\mathfrak{O}Y)$-ideal prime to $\mathfrak{F}$ and we have

$$M_{\mathfrak{d}} = X_{\mathfrak{b}} \oplus Y_{\mathfrak{c}}.$$

Since $X_{\mathfrak{b}} \sim X$ and $Y_{\mathfrak{c}} \sim Y$, the lemma will be proved if we show that $M_{\mathfrak{d}}$ and M are isomorphic. According to Lemma 2.3 this is the case if and only if $\mathfrak{d}$ is generated by an element of $E(M)$. Consider δ as an element of $E(T)$ and put $d = \mathrm{id}_{\mathfrak{O}X\mathfrak{b}} \oplus \delta$. Then d generates

(1) This theorem, as well as the following lemma can also be obtained from results of Reiner and Jones (see [4], § 81A).

$\mathfrak{b}$ and $\delta \equiv 1$ $(\mathfrak{F})$ implies $d \in E(M)$ and the proof is complete. — We note the following corollary of Theorem 3.3.

COROLLARY 3.5. *If a genus Γ contains one indecomposable lattice, then every lattice in Γ is indecomposable.*

Recall that for any R-lattice M we denote by $r(A_i, M)$ the number of irreducible A_i-modules in a decomposition of kM. We now show

THEOREM 3.6. *Let X be a local direct factor of M such that*

$$r(A_i, X) < r(A_i, M) \quad \textit{whenever } r(A_i, X) \neq 0.$$

Then X is isomorphic to a direct factor of M, i.e.

$$M \cong X \oplus Y \quad \textit{with } Y \in \mathfrak{L}_R.\text{(}^1\text{)}$$

We know already that there is a decomposition $M = X' \oplus Y'$, with $X \sim X'$. Put

$$\mathfrak{O}Y' = e_X \mathfrak{O} Y' \oplus (1 - e_X)\mathfrak{O} Y'.$$

Then our assumption on $r(A_i, X)$ implies, that $e_X \mathfrak{O} Y'$ affords a faithful representation of $e_X \mathfrak{O}$. Thus every element of $I_{\mathfrak{F}}(e_X)$ is the norm of a left $E(e_X \mathfrak{O} Y')$-ideal $\mathfrak{b}$, which is prime to $\mathfrak{F}$. If $X \cong X'_{\mathfrak{a}}$, we choose $\mathfrak{b}$ such that $n(\mathfrak{a}) n(\mathfrak{b}) \in S_{\mathfrak{F}}(e_X)$ and put

$$\mathfrak{O}X'\mathfrak{a} \oplus e_X \mathfrak{O} Y' \mathfrak{b} \oplus (1 - e_X)\mathfrak{O} Y' = \mathfrak{O} M \mathfrak{c}.$$

Then clearly, $M_{\mathfrak{c}} \cong X \oplus Y$, with $Y \sim Y'$ and the theorem is proved if we show that $M \cong M_{\mathfrak{c}}$. Our assumption on $r(A_i, X)$ implies that $T = \mathfrak{O}X' \oplus e_X \mathfrak{O} Y'$ is in $\mathfrak{L}'_{\mathfrak{O}}$. Applying Lemma 2.4 we see that $\mathfrak{O}X'\mathfrak{a} \oplus e_X \mathfrak{O} Y' \mathfrak{b} = T\alpha$, where α induces the identity on $T/\mathfrak{F}T$. But then the ideal $\mathfrak{c}$ is generated by $\beta = \alpha \oplus (1 - e_X)$ and β induces the identity on $\mathfrak{O}M/\mathfrak{F}M$. This means that β is in $E(M)$ and so $M_{\mathfrak{c}} \cong M$ according to Lemma 2.3, which completes the proof.

4. Cancellation

Let X, M and N be R-lattices, such that

$$X \oplus M \cong X \oplus N. \qquad (*)$$

Under what conditions can X be cancelled here, i.e. when does (*) imply $M \cong N$? If R is a maximal order, Theorem 1.4 and (2) imply that X can be cancelled if $M \in \mathfrak{L}'_{\mathfrak{O}}$, but

(1) After the completion of the present paper I found that a similar result has recently been obtained by Roiter (see [13], Prop. 5) by means of different methods. Roiter assumes, that kM/kX affords a faithful representation of A, which is a little more restrictive than our assumption on the $r(A_i, X)$.

for $M \notin \mathfrak{L}'_{\mathfrak{O}}$, this is no longer true. Other examples where cancellation is not possible can be constructed by means of Proposition 2.10. On the other hand, we already mentioned in the introduction, that if X is a projective R-module, the cancellation-theorem of Bass ([2], § 9) implies, that X can be cancelled if M possesses a local direct factor, which is free of rank $\geqslant 2$. For non-projective X however, no such condition seems to have been known.

We remark first, that (*) always implies $M \sim N$ since $\mathfrak{L}_{R_p}$ has unique decomposition. Now suppose X fixed and let Y vary in the genus $\Gamma(M)$ that contains M. Then

$$Y \to X \oplus Y$$

induces a map j of the isomorphism classes in $\Gamma(M)$ into those of $\Gamma(X \oplus M)$. If this map j is injective, then X can be cancelled in (*) even if M is replaced by some $M' \sim M$. Now suppose that both M and $X \oplus M$ belong to $\mathfrak{L}'_R$. Then from Theorem 2.2 and (2) we see that j is injective if and only if

$$H_M = I_{\mathfrak{F}}(e_M) \cap H_{X \oplus M}.$$

Using this condition we can show

THEOREM 4.1. *Suppose $M \in \mathfrak{L}'_R$ and let X be a local direct factor of zM for some $z > 0$. Then for $N \in \mathfrak{L}_R$*

$$X \oplus M \cong X \oplus N \quad \textit{implies} \quad M \cong N.$$

Since X is a local direct factor of zM, $r(A_i, X) > 0$ implies $r(A_i, M) > 0$. From this we see, that $e_M = e_{X \oplus M}$ and that $X \oplus M$ is in $\mathfrak{L}'_R$ too. According to the remark above, we must show that $H_M = I_{\mathfrak{F}}(e_M) \cap H_{X \oplus M}$. But $I_{\mathfrak{F}}(e_M) = I_{\mathfrak{F}}(e_{X \oplus M}) \supset H_{X \oplus M}$ and so the theorem is equivalent to

$$H_M = H_{X \oplus M}.$$

We need one more reduction. Since X is a local direct factor of zM, we obtain from Theorem 3.6 that there is a decomposition

$$(z+1)M \cong X \oplus T \quad \text{with } T \in \mathfrak{L}_R.$$

This implies $(z+2)M \cong (X \oplus M) \oplus T$ and so $H_{X \oplus M}$ is a subgroup of $H_{(z+2)M}$. Thus we have

$$H_M \subset H_{X \oplus M} \subset H_{(z+2)M}.$$

Now the theorem follows from

LEMMA 4.2. *For any $M \in \mathfrak{L}'_R$ and any integer $s > 0$, $H_M = H_{sM}$.*

We know already that $S_{\mathfrak{F}}(e_M)$ is contained in every H_{sM} (Lemma 2.6) and so we need only show that $H_{sM}/S_{\mathfrak{F}}(e_M)$ does not depend on s. As before, define $\mathfrak{f}$ by $\mathfrak{F}M = \mathfrak{O}M\mathfrak{f}$. Then for $x \in E(\mathfrak{O}M)$, $x \equiv 1$ ($\mathfrak{f}$) implies $n(x) \equiv 1$ ($\mathfrak{f}$). This is easily seen to be true if $\mathfrak{f}$ is generated by an ideal of the center; the general case follows from this by extending k to a splitting field of A. Put $Q = E(M)/\mathfrak{f}$ and let $E^*(M)$ be the subset of elements prime to $\mathfrak{F}$ in $E(M)$. Then the map $E(M) \to Q$ takes every $x \in E^*(M)$ into an invertible element of Q and so we have an epimorphism

$$\varphi_1\colon E^*(M) \to \mathrm{GL}(1, Q).$$

In the same way, if we define $\mathfrak{f}_s$ by $\mathfrak{F}(sM) = \mathfrak{O}(sM)\mathfrak{f}_s$, the map $E(sM) \to E(sM)/\mathfrak{f}_s$ induces an epimorphism

$$\varphi_s\colon E^*(sM) \to \mathrm{GL}(s, Q).$$

We embed $E^*(sM)$ in $E^*((s+1)M)$ by $a \to a \oplus \mathrm{id}_M$ and in the same way $\mathrm{GL}(s, Q)$ in $\mathrm{GL}(s+1, Q)$. Now Q is an Artin-ring and so $n=1$ defines a stable range over Q (see [2], p. 14). If $\varepsilon(s, Q)$ denotes the subgroup generated by the elementary matrices in $\mathrm{GL}(s, Q)$, we have ([2], Theorem 4.2)

$$\mathrm{GL}(s, Q) = \mathrm{GL}(1, Q)\varepsilon(s, Q).$$

Now $E(sM)$ is the ring of $s \times s$ matrices over $E(M)$. Every element of $\varepsilon(s, Q)$ lifts to an elementary matrix e in $E^*(sM)$ and $n(e) = 1$. Thus for every $g_s \in E^*(sM)$ we have $g_s = g_1 ex$ with $g_1 \in E^*(M)$ and $x \in \operatorname{Ker} \varphi_s$. But then $x \equiv 1$ ($\mathfrak{f}_s$) and $n(x) \equiv 1$ ($\mathfrak{F}$), which implies $n(g_s) \equiv n(g_1)$ ($\mathfrak{F}$). Consequently, $H_{sM}/S_{\mathfrak{F}}(e_M) = H_M/S_{\mathfrak{F}}(e_M)$ and this completes the proof of the lemma and of Theorem 4.1.

Remark 1. If $M \notin \mathcal{L}'_R$, then at any rate $sM \in \mathcal{L}'_R$ for $s > 1$ and from the lemma we see that $H_{sM} = H_{2M}$ for every $s > 1$.

Remark 2. If we apply the cancellation theorem of Bass ([2], Theorem 9.3) to R-lattices, we obtain: If X is projective and M has a local direct factor, which is R-free and of rank $\geqslant 2$, then $X \oplus M \cong X \oplus M'$ implies $M \cong M'$. This is a special case of our theorem, since the hypothesis implies that $M \in \mathcal{L}'_R$ and that X is a local direct factor of some zM.

As an application, we consider the following special situation. Let $M \in \Gamma \in \mathcal{G}_R$ and consider the genus $s\Gamma$, that contains sM for a fixed integer $s > 1$. Choose $s-1$ R-lattices M^i in Γ and let N denote their direct sum. Then N is a local direct factor of every $Y \in s\Gamma$, and we obtain from Theorem 3.6 that Y has a decomposition

$$Y \cong M^1 \oplus \ldots \oplus M^{s-1} \oplus X, \quad \text{with } X \sim M. \tag{4}$$

In particular we can choose $M^1 = \ldots = M^{s-1} = M$ and this yields

$$Y \cong (s-1)M \oplus X, \quad \text{with } X \sim M. \tag{4'}$$

From the cancellation theorem it follows immediately that in both these decompositions, Y determines X uniquely, up to an isomorphism, provided M is in $\mathfrak{L}'_R$. If this is not the case, then from $Y \cong Y'$ we can only infer that $M^i \oplus X \cong M^i \oplus X'$ for every i.

In some special cases the decompositions (4) or (4') are well-known. Let first A be a skew-field, $R = \mathfrak{D}$ a maximal order in A and take $M \cong \mathfrak{D}$. Then for every $Y \in \mathfrak{L}_{\mathfrak{D}}$, kY is isomorphic to the direct sum of s copies of A. According to Corollary 1.2, this implies that $Y \sim F_s$, where F_s is a free $\mathfrak{D}$-module of rank s. Thus every $Y \in \mathfrak{L}_{\mathfrak{D}}$ has a decomposition

$$Y \cong F_{s-1} \oplus \mathfrak{A},$$

where $\mathfrak{A}$ is a left $\mathfrak{D}$-ideal with $k\mathfrak{A} = A$. This was proved by Chevalley ([3], p. 12). If A is any simple algebra and $\mathfrak{D}$ a maximal order in A, we take M such that kM is an irreducible A-module. Then in the same way as above we see, that to every $Y \in \mathfrak{L}_{\mathfrak{D}}$ there is an integer s such that $Y \sim sM$ and Y has decompositions of the form (4) and (4') (Jacobinski [9]).

Another example is furnished by projective modules over a group ring oG if no prime dividing the order of G is a unit in o. Swan [13] has shown that such a module P is locally free everywhere. This means that $P \sim F_s$, where F_s is free of rank s. Then from (4') we see that

$$P \cong F_{s-1} \oplus I,$$

where I is a projective ideal with $kI = kG$ (Swan [13], Theorem 7.2). If none of the simple algebras in kG is a totally definite quaternion skew field, then F_1 is in $\mathfrak{L}'_{oG}$ and I is uniquely determined (up to an isomorphism) by P. From this we can obtain conditions for cancellation of projective oG-modules. We prefer however to discuss this later (see 5.3).

5. The group $D(B)$

We now define a kind of relative Grothendieck-groups with relations for split exact sequences only. Let $B \subset \mathfrak{L}_R$ be closed under direct sums and let $Y(B)$ be the free abelian group with a generator y_M for every $M \in B$. Denote by $Y'(B)$ the subgroup generated by all elements $y_M - y_N - y_S$ such that $M \cong N \oplus S$, for $N, S \in B$. Then we put

$$D(B) = Y(B)/Y'(B).$$

If we consider B as a category with only direct injections and direct projections as morphisms, $D(B)$ is the usual Grothendieck-group of B. To avoid confusion with the Grothendieck-group $K(B)$ of B as a subcategory of $\mathfrak{L}_R$, we prefer the notation $D(B)$. Of special interest is the case $B = \mathfrak{P}_R$ the category of finitely generated projective R-modules; then the two groups coincide.

If $R = oG$ is the group ring of a finite group G, one can define a ring structure on $D(\mathfrak{L}_{oG})$ by means of the tensor product. This ring has been studied in several papers by Reiner; see Reiner [11] and the literature cited there. In this paper, which was published after the completion of the present work, Reiner also gives a proof of a part of Theorem 5.6 in the special case that $B = \mathfrak{L}_R$.

The image of $M \in B$ in $D(B)$ we denote by $[M]_B$ or simply by $[M]$. Clearly, $[M]_B = [N]_B$ if and only if there is $X \in B$, such that $M \oplus X \cong N \oplus X$. Let e_B be the central idempotent in A such that

$$e_B M = M \quad \text{and} \quad (1 - e_B)M = 0 \quad \text{for all } M \in B,$$

and let H_B be the subgroup of $I_{\mathfrak{F}}(e_B)$ generated by all groups H_M for $M \in B$. H_B is generated by a finite number of groups H_{M_i}, $M_i \in B$ and then $T = \oplus \sum M_i$ is in B and $H_B = H_T$. Replacing if necessary T by $2T$ we see that

$$H_B = H_T \quad \text{with} \quad T \in B \cap \mathfrak{L}'_R. \tag{*}$$

As before we put
$$V_B = I_{\mathfrak{F}}(e_B)/H_B.$$

Then $v_B(M, N)$ is defined for $M \sim N$ and $M, N \in B$ (cf. Remark 1 after Lemma 2.6). We now show

PROPOSITION 5.1. *Let $B \subset \mathfrak{L}_R$ be closed under direct sums and denote by $[M]_B$ the image of $M \in B$ in $D(B)$. Then for $M, N \in B$ we have*

1) $[M]_B - [N]_B$ is torsion if and only if $M \sim N$

2) $[M]_B = [N]_B$ if and only if $M \sim N$ and $v_B(M, N) = 1$.

According to Proposition 2.8, $M \sim N$ implies $zM \cong zN$ and so $[M]_B - [N]_B$ is torsion. Conversely, if $[M]_B - [N]_B$ is torsion, we have

$$zM \oplus X \cong zN \oplus X, \quad X \in B \quad \text{and} \quad z > 0,$$

and this implies $M \sim N$, since the Krull–Schmidt theorem holds for R_p-lattices. To prove 2), suppose first $M \sim N$ and $v_B(M, N) = 1$ and choose T as in (*). Then also $v_B(M \oplus T, N \oplus T) = 1$ and since $H_B = H_T = H_{M \oplus T}$, this implies $M \oplus T \cong N \oplus T$ and so $[M]_B = [N]_B$. Conversely, if $[M]_B = [N]_B$ then there is $X \in B$ such that $N \oplus X \cong M \oplus X$. Replacing if necessary X by $X \oplus T$, we can assume $X \in \mathfrak{L}'_R$ and $H_X = H_B$. But then we obtain from Theorem 2.2 that $v_B(M \oplus X, N \oplus X) = 1$ and this implies $v_B(M, N) = 1$, which completes the proof.

Since H_B is generated by norms of principal ideals prime to $\mathfrak{F}$, we always have $H_B \subset S(e_B) \cap I_{\mathfrak{F}}(e_B)$. In particular, if $B = \mathfrak{L}_R$ we have $H_B = S(1) \cap I_{\mathfrak{F}}(1)$ and then, according to Theorem 1.4, $v_B(M, N) = 1$ is equivalent to $\mathfrak{O}M \cong \mathfrak{O}N$, provided $M \in \mathfrak{L}'_R$. Thus we obtain (cf. Definition 2.9 and Proposition 2.10)

COROLLARY 5.2. *Two R-lattices $M, N \in \mathfrak{L}'_R$ are in the same restricted genus if and only if they have the same image in $D(\mathfrak{L}_R)$.*

The second part of Proposition 5.1 can easily be rephrased as a condition for cancellation in the category B. We say that $M \in B$ is cancellative in B, if every relation

$$X \oplus M \cong X \oplus N, \quad \text{with } X, N \in B \tag{**}$$

implies $M \cong N$. If every element of B is cancellative, we say that B has cancellation.

PROPOSITION 5.3. *An element $M \in B \cap \mathfrak{L}'_R$ is cancellative in B if and only if*

$$H_M = H_B \cap I_{\mathfrak{F}}(e_M).$$

For a relation (**) is equivalent to $[M]_B = [N]_B$ and this in turn is equivalent to $M \sim N$ and $v_B(M, N) = 1$. But according to Theorem 2.2, M and N are isomorphic if and only if $v_M(M, N) = 1$. Thus M is cancellative in B if and only if for every N in B with $M \sim N$, $v_B(M, N) = 1$ implies $v_M(M, N) = 1$. From the definition of V_B and V_M it follows immediately that this is the case if and only if $H_M = H_B \cap I_{\mathfrak{F}}(e_M)$.

As an application of this proposition, let G be a finite group and consider the category $\mathfrak{P}$ of finitely generated projective oG-modules. Swan (see [15]) has raised the question whether $\mathfrak{P}$ has cancellation or not. He himself showed (Swan [16]) that this is not always the case by constructing—for a special group G—a non-cancellative projective oG-module.

From the proposition above we see, that there are two possibilities for a $P \in \mathfrak{P}$ to be non-cancellative. The first is that $P \notin \mathfrak{L}'_{oG}$ and this is actually the case in the counterexample given by Swan. The second possibility is that $H_P \neq H_{\mathfrak{P}} \cap I_{\mathfrak{F}}(e_P)$ and I do not know whether this can actually occur. If instead of $\mathfrak{P}$ we consider the subcategory $\mathfrak{P}^0$, consisting of all $P \in \mathfrak{P}$ such that kP is kG-free, we can show

COROLLARY 5.4. *Every element of $\mathfrak{P}^0 \cap \mathfrak{L}'_{oG}$ is cancellative in $\mathfrak{P}$.*

Let F_s denote a free oG-module of rank s. According to a theorem of Swan (Swan [15], Theorem 6.1), $P \in \mathfrak{P}^0$ implies $P \sim F_s$ for some $s > 0$. If none of the simple algebras in kG is a totally definite skew-field of index 2, such a P is automatically in $\mathfrak{L}'_{oG}$; otherwise this is the case only if $s > 1$. But then Lemma 4.2 and the remark after it implies that the group H_P is the same for all $P \in \mathfrak{P}^0 \cap \mathfrak{L}'_{oG}$. This means $H_P = H_{\mathfrak{P}^0}$ and this implies that P is cancellative in $\mathfrak{P}^0$. Since every $Q \in \mathfrak{P}$ is a direct factor of some F_s, we see that $H_{\mathfrak{P}} = H_{\mathfrak{P}^0}$ and consequently every $P \in \mathfrak{P}^0 \cap \mathfrak{L}'_{oG}$ is cancellative also in $\mathfrak{P}$.

COROLLARY 5.5. *Suppose that none of the rational primes dividing the order of G is a unit in o and that none of the simple algebras in a decomposition of kG is a totally definite* *skew-field of index 2. Then the category of finitely generated projective oG-modules has cancellation.*

For our assumptions imply that $\mathcal{P}=\mathcal{P}^0$ (Swan [15], Theorem 8.1) and that $\mathcal{P}^0\subset\mathcal{L}'_{oG}$.

We define the sum of two genera Γ_1 and Γ_2 to be the genus which contains $M_1\oplus M_2$ with $M_1\in\Gamma_1$ and $M_2\in\Gamma_2$. Clearly $\Gamma_1+\Gamma_2$ does not depend on the choice of M_1 and M_2. Moreover, Theorem 3.3 implies that every R-lattice X in $\Gamma_1+\Gamma_2$ has a decomposition $X=X_1\oplus X_2$ with $X_1\in\Gamma_1$ and $X_2\in\Gamma_2$. Thus we could equally well define

$$\Gamma_1+\Gamma_2=\{X_1\oplus X_2,\ X_1\in\Gamma_1,\ X_2\in\Gamma_2\}.$$

We denote by $\tilde{B}$ the set of genera, which contain elements of B. In the same way as for R-lattices we can define the group $D(\tilde{B})$ with relations corresponding to all sums $\Gamma=\Gamma_1+\Gamma_2$ in $\tilde{B}$. Since $\Gamma+\Gamma'=\Gamma+\Gamma''$ implies $\Gamma'=\Gamma''$, the map $\tilde{B}\to D(\tilde{B})$ is an injection. Moreover, if $D_t(B)$ denotes the torsion subgroup of $D(B)$, the first part of Proposition 5.1 implies that the sequence

$$0\to D_t(B)\to D(B)\to D(\tilde{B})\to 0$$

is exact. As we will see, $D(\tilde{B})$ is free and so this sequence splits. Moreover, we will show, that $D_t(B)$ is isomorphic to a subgroup of V_B. As already mentioned, a special case of this was shown by Reiner, who proves that $D(\mathcal{G}_R)$ is free and that $D_t(\mathcal{L}_R)$ is a finite group (see Reiner [11]).

THEOREM 5.6. *For any $B\subset\mathcal{L}_R$, which is closed under direct sums the group $D(\tilde{B})$ is free and*

$$D(B)\cong W_B\oplus D(\tilde{B}),$$

where $W_B=\{v_B(X,X'),\ X\sim X',\ X,X'\in B\}$ is a subgroup of V_B.

We show first that $D(\tilde{B})$ is free. If $M\in\Gamma$, then Γ is completely determined by the set $\{M_p\}_{p\in U}$ (Lemma 3.1). Thus $\Gamma\to\{M_p\}_{p\in U}$ induces an injection

$$\sigma\colon D(\tilde{B})\to\prod_{p\in U}D(\mathcal{L}_{R_p}).$$

Now every R_p-lattice has a unique decomposition into indecomposable lattices. This means that each $D(\mathcal{L}_{R_p})$ is free with the images of indecomposable R_p-lattices as generators and so $D(\tilde{B})$ is free too.

It remains to show that $D_t(B)$ is isomorphic to W_B. Choose m pairs S_i, S_i' in B with $S_i\sim S_i'$ such that W_B is the set of all $v_B(S_i,S_i')$, $i=1,\dots,m$ and put $S=S_1\oplus\dots\oplus S_m$. Then $S\in B$ and W_B consists of all $v_B(S,S')$ such that $S'\sim S$ and $S'\in B$. Now $v_B(S\oplus S,S'\oplus S'')$ is in W_B and equals $v_B(S,S')v_B(S,S'')$. This shows that W_B is a group.

Replacing if necessary S by $S\oplus T$, we can assume that moreover $V_S=V_B$. According to Proposition 5.1, every $\tau\in D_t(B)$ is of the form $[X]_B-[X']_B$ with $X\sim X'$. Then we have also

$$\tau=[S\oplus X]_B-[S\oplus X']_B.$$

We choose $S'\in B$ such that $v_B(X,X')=v_B(S,S')$. Since $V_B=V_S=V_{X\oplus S}$, we see from Theorem 2.2 that $S\oplus X'\cong S'\oplus X$. Thus we obtain that every $\tau\in D_t(B)$ is of the form

$$\tau=[S]_B-[S']_B,\quad \text{with } S'\sim S \text{ and } S'\in B.$$

But now it is easy to see that the map $\varphi:\tau\to v_B(S,S')$ defines a group homomorphism $D_t\to W_B$ which clearly is onto. Because of Proposition 5.1, φ is also injective and this completes the proof.

Remark. If the category B is also closed under direct factors in $\mathfrak{L}_R$, then $W_B=V_B$, for then every isomorphism class in the genus determined by S contains elements of B (cf. Prop. 2.8). But in general W_B and V_B will not be equal. For instance, if X is any fixed R-lattice and $B=\{sX,\ s>0\}$, then W_B is trivial.

The injection σ defined above identifies $D(\tilde{B})$ with a subgroup of $\prod_{p\in U}D(\mathfrak{L}_{R_p})$. It is not hard to describe this subgroup explicitly. For simplicity, we consider only the case $B=\mathfrak{L}_R$. Let k' be a splitting field of A and let $K(A')$ be the Grothendieck group of $A'=k'\otimes A$, or equivalently, the group of characters of finitely generated A'-modules. If k'' is any extension field of k and $A''=k''\otimes A$, then we can consider $K(A'')$ as a subgroup of $K(A')$; in particular, $K(A_p)$ is a subgroup of $K(A')$ for every p.

Let X be an R_p-lattice. Then the map $X\to k_pX$ induces a homomorphism

$$\chi_p:\ D(\mathfrak{L}_{R_p})\to K(A')$$

Let $a=\{a_p\}_{p\in U}$ be an element of $\prod D(\mathfrak{L}_{R_p})$. We extend χ_p to a homomorphism $\prod D(\mathfrak{L}_{R_p})\to K(A')$ in the obvious way. Then we have

PROPOSITION 5.7. *The map $D(\mathcal{G}_R)\to\prod_{p\in U}D(\mathfrak{L}_{R_p})$ induced by $\Gamma\to\{M_p\}_{p\in U}$ identifies $D(\mathcal{G}_R)$ with the subgroup of all $a\in\prod D(\mathfrak{L}_{R_p})$, such that*

1) $\chi_p(a)=\chi_q(a)$ for all p, q in U, and

2) $\chi_p(a)$ is already in $K(A)$.

These conditions are clearly necessary and from Lemma 3.2 it follows immediately that they also are sufficient.

With a view to applications in the next section, we now specialize B in the following way. For $M\in\mathfrak{L}_R$, we put

$$B_M=\{X,\ X\oplus X'\cong sM,\quad X,X'\in\mathfrak{L}_R,\ s>0\}.$$

Let Γ be the genus that contains M. Writing B_Γ instead of $\tilde{B}_M$ we have

$$B_\Gamma = \{\Lambda,\ \Lambda + \Lambda' = s\Gamma,\ \Lambda,\Lambda' \in \mathcal{G}_R,\ s>0\}.$$

Clearly, $B_M = B_{zM}$ for every $z>0$. Thus, replacing if necessary M by $2M$ we can assume that $M \in \mathfrak{L}'_R$.

PROPOSITION 5.8. *Suppose $M \in \mathfrak{L}'_R$ and let Γ be the genus which contains M. Then*

$$D(B_M) \cong V_M \oplus D(B_\Gamma)$$

and $D(B_\Gamma)$ is free and finitely generated.

B_M is clearly closed under direct sums and direct factors, so that $W_{B_M} = V_{B_M}$ and we obtain

$$D(B_M) \cong V_{B_M} \oplus D(B_\Gamma).$$

We show first that $V_{B_M} = V_M$ or equivalently, $H_{B_M} = H_M$. Since $M \in B_M$, this amounts to showing that $H_X \subset H_M$ for every $X \in B_M$. According to the definition of B_M we have $X \oplus X' \cong sM$ and this implies $H_X \subset H_{sM}$. But $H_{sM} = H_M$ (Lemma 4.2) so that in fact $H_X \subset H_M$. — It remains to show that $D(B_\Gamma)$ is finitely generated. As in the proof of the theorem, we have an injection

$$\sigma:\ D(B_\Gamma) \to \prod_{p \in U} D(\mathfrak{L}_{R_p})$$

and here $\operatorname{Im}\sigma$ is contained in $\prod_{p\in U} D(B_{M_p})$. Now each $D(B_{M_p})$ is finitely generated—namely by the images of those indecomposable R_p-lattices, that appear in a decomposition of M_p—and so $D(B_\Gamma)$ is finitely generated too.

We apply our results to the category $\mathfrak{P} = \mathfrak{P}_R$ of finitely generated projective R-modules. Let again F_s denote a free R-module of rank s. If none of the simple algebras A_i in A is a totally definite skew-field of index 2, then every F_s is in $\mathfrak{L}'_R$; otherwise we must suppose $s>1$. Depending on this we put $T = F_1$ or $T = F_2$. Then $\mathfrak{P}_R = B_T$ and the group $D(B_T)$ coincides with the usual Grothendieck-group $K(\mathfrak{P}_R)$. From Proposition 5.8 we obtain

$$K(\mathfrak{P}_R) \cong V_T \oplus D(\tilde{\mathfrak{P}}_R),$$

where $D(\tilde{\mathfrak{P}}_R) \cong Z^{(\sigma)}$ is a free abelian group of finite rank σ. In case $T = F_1$, V_T is simply the factor group of the group of ideals prime to $\mathfrak{F}$ in the integral closure of the center of A modulo the subgroup of ideals of the form $(n(x))$ with $x \in R$; if $T = F_2$ then x must vary in the ring of 2×2 matrices over R.

Let again $\mathfrak{P}^0_R$ be the subcategory of all $P \in \mathfrak{P}_R$, such that kP is a free A-module. $\mathfrak{P}^0_R$

satisfies the condition of Theorem 5.6. Moreover, $H_{\mathfrak{P}^0} = H_{\mathfrak{P}} = H_T$ and so we obtain

$$K(\mathfrak{P}_R^0) \cong V_T \oplus D(\tilde{\mathfrak{P}}_R^0),$$

where $D(\tilde{\mathfrak{P}}_R^0) \cong Z^{(\sigma_0)}$ is a free abelian group of rank σ_0.

The projective class group $C(R)$ is defined as the factor group of $K(\mathfrak{P}_R)$ modulo the subgroup generated by the image of F_1 (see Rim [12]). Let Γ be the genus that contains F_1. Then it may happen that $\Gamma = z\Lambda$ with $\Lambda \in \mathcal{G}_R$ and $z > 1$ and then Λ is in $\tilde{\mathfrak{P}}_R$ too. If a_R denotes the maximal value of such a z, we obtain from the expression for $K(\mathfrak{P}_R)$ that

$$C(R) \cong V_T \oplus Z / a_R Z \oplus Z^{(\sigma-1)}$$

Similarly the reduced projective class group $C^0(R)$ is defined as the factor group of $K(\mathfrak{P}_R^0)$ modulo the subgroup generated by the image of F_1. Since here a decomposition $\Gamma = z\Lambda$ with $z > 1$ and $\Lambda \in \tilde{\mathfrak{P}}_R^0$ is impossible, we obtain

$$C^0(R) \cong V_T \oplus Z^{(\sigma_0 - 1)}$$

Specializing once more, we consider the case $R = oG$, G a finite group. Then Swan ([15], Theorem 6.1) has shown that if $P, Q \in \mathfrak{P}_{oG}$ and $kP \cong kQ$ as kG-modules, then P and Q are in the same genus. This means that $D(\tilde{\mathfrak{P}}_{oG})$ is isomorphic to the additive group generated by the characters of projective oG-modules. This group has been determined explicitly by Swan ([17], Theorem 4). In particular we see that every genus in $\tilde{\mathfrak{P}}_{oG}^0$ contains some F_s. This means that $\sigma_0 = 1$. Moreover, $a_{oG} = 1$ since the trivial representation of G occurs only once in the regular representation. Thus we obtain

$$C(oG) \cong V_T \oplus Z^{(\sigma-1)}$$

and

$$C^0(oG) \cong V_T.$$

The second formula implies in particular that $C^0(oG)$ is a finite group for which fact different proofs have been given by Reiner, Rim and Swan, see for instance Swan [17]. Because of the importance of the reduced projective class group, we state our result explicitly.

COROLLARY 5.9. *Let G be a finite group and denote by f the product of all primes p in o such that o_pG is not a maximal order (this f divides the order of G). Let I_f denote the group of all invertible ideals prime to f in the integral closure over o of the center of kG. Let H denote the subgroup of I_f generated by ideals of the form $(n(x))$, where x varies in oG if none of the simple algebras in kG is a totally definite skew-field of index 2 and in the ring of 2×2 matrices over oG otherwise. Then*

$$C^0(oG) \cong I_f / H.$$

6. Decompositions into indecomposable lattices

We have repeatedly used the fact that $\mathfrak{L}_{R_p}$ has unique decomposition, i.e. that every R_p-lattice is uniquely decomposable into indecomposable R_p-lattices (up to an automorphism). It is well-known that this is not true for $\mathfrak{L}_R$ (Reiner [10]). Examples of R-lattices that have essentially different decompositions follow immediately from Proposition 2.8 and 2.10. In this section we will give a survey of the different possible decompositions of a given R-lattice into indecomposable R-lattices.

In the previous section we have already defined the sum of two genera Γ_1 and Γ_2 to be the genus generated by $X_1 \oplus X_2$ for $X_1 \in \Gamma_1$ and $X_2 \in \Gamma_2$. A genus Λ is indecomposable if $\Lambda = \Lambda_1 + \Lambda_2$ implies $\Lambda_1 = 0$ or $\Lambda_2 = 0$. From Theorem 3.3 and Corollary 3.5 we know, that Λ is indecomposable if it contains an indecomposable R-lattice and that then every element of Λ is indecomposable.

Now take $M \in \mathfrak{L}_R$ and let

$$M = M_1 \oplus \ldots \oplus M_t \tag{*}$$

be a decomposition of M into indecomposable R-lattices. Let Γ, Γ_i be the genera that contain M and M_i respectively. Then from (*) we obtain a decomposition

$$\Gamma = \Gamma_1 + \ldots + \Gamma_t. \tag{**}$$

Here the Γ_i are indecomposable genera since each of them contains an indecomposable R-lattice, viz. M_i. Now let us start with a decomposition (**) of the genus Γ into indecomposable genera. Then Theorem 3.3 implies, that there is at least one decomposition (*) with $M_i \in \Gamma_i$. Thus our problem of finding all decompositions of a given R-lattice M falls into two parts. First we have to determine all the different decompositions (**) of the corresponding genus and then to every such decomposition, we must find all different decompositions (*) with $M_i \in \Gamma_i$. The first problem, viz. decompositions in $\mathcal{G}_R$, we will discuss later in this section; the second one is easily solved by means of Theorem 2.2, provided $\Gamma_i \in \mathcal{G}_R'$ for all i.

Take a fixed decomposition (**) and suppose that we have already found one corresponding decomposition $M = M_1 \oplus \ldots \oplus M_t$ with $M_i \in \Gamma_i$. Let X_i vary in Γ_i; then we have to find all different decompositions $M \cong X_1 \oplus \ldots \oplus X_t$. In the same way as after Proposition 2.1, we denote by $\overline{\Gamma}_i$ the set of all R-lattices of the form $\mathfrak{O} M_i \mathfrak{a} \cap M_i$ with $\mathfrak{a}$ prime to $\mathfrak{F}$. Since $\overline{\Gamma}_i$ contains representatives of all isomorphism classes in Γ_i, it is sufficient to let X_i vary in $\overline{\Gamma}_i$. Then $n(M_i, X_i) = x_i$ is defined; this is an ideal in $I_{\mathfrak{F}}(e_{\Gamma_i})$. Recall that for every genus Λ we identify $I_{\mathfrak{F}}(e_\Lambda)$ with a subgroup of $I_{\mathfrak{F}}(1)$ by means of the injection $a \to a \oplus (1 - e_\Lambda) C$. Thus x_i becomes an element of $I_{\mathfrak{F}}(e_\Gamma)$ and the map $(x_1, \ldots, x_t) \to x_1 \ldots x_t$

defines an epimorphism

$$\prod I_{\mathfrak{F}}(e_{\Gamma_i}) \to I_{\mathfrak{F}}(e_{\Gamma}).$$

The image of $\prod H_{\Gamma_i}$ is clearly in H_Γ and so we obtain an epimorphism

$$\varphi\colon \prod V_{\Gamma_i} \to V_\Gamma.$$

Now suppose $\Gamma_i \in \mathcal{G}'_R$ for $i=1, \ldots, t$; then Γ is in $\mathcal{G}'_R$ too. The isomorphism classes in Γ_i and Γ are in 1–1-correspondence with the elements of V_{Γ_i} and V_Γ resp. Thus $X_1 \oplus \ldots \oplus X_t$ is isomorphic to M if and only if the corresponding element of $\prod V_{\Gamma_i}$ is in $\operatorname{Ker}\varphi$. This means, that every element of $\operatorname{Ker}\varphi$ corresponds to a class of equivalent decompositions of M. Some of these may differ only by the arrangement of the factors. Discarding these, we have solved the first problem mentioned above.

Before proceeding to the second problem, we deduce a necessary (but not sufficient) condition in order that $\mathcal{L}_R$ has a unique decomposition

PROPOSITION 6.1. *If $\mathcal{L}_R$ has unique decomposition then $|\Gamma| = 1$ for every $\Gamma \in \mathcal{G}_R$, that is $M \sim N$ implies $M \cong N$ for arbitrary $M, N \in \mathcal{L}_R$.*

If $M \sim N$, then for some integer z we have $zM \cong zN$ (Proposition 2.8) and, since $\mathcal{L}_R$ has unique decomposition, this implies $M \cong N$. — A consequence of this is

COROLLARY 6.2. *If $\mathcal{L}_R$ has unique decomposition, then the maximal order C of the center of A is a principal ideal ring.*

Let Γ be a genus in $\mathcal{G}'_{\mathfrak{D}}$ such that $e_\Gamma = 1$. Then Γ is also a genus of R-lattices, since $R \subset \mathfrak{D}$. If $\mathcal{L}_R$ has unique decomposition, we have $|\Gamma| = 1$. According to Theorem 1.4, this implies $I(1) = S(1)$, which is a little more than asserted.

We now turn to the question of finding all decompositions of a given genus Γ into indecomposable genera. Clearly, every such decomposition takes place in the category

$$B_\Gamma = \{\Lambda, \quad \Lambda + \Lambda' = z\Gamma, \quad \Lambda, \Lambda' \in \mathcal{G}_R, z > 0\}$$

which we introduced in the preceding section. Instead of only Γ, it is more convenient to study decompositions of all elements of B_Γ at the same time. We show

THEOREM 6.3. *For arbitrary $\Gamma \in \mathcal{G}_R$, the category B_Γ contains only a finite number of indecomposable genera.*

Let $[\Lambda]$ denote the image of Λ in $D(B_\Gamma)$. The map $\Lambda \to [\Lambda]$ is an injection and thus identifies B_Γ with a semigroup $D^+(B_\Gamma)$ contained in $D(B_\Gamma)$ and $D^+(B_\Gamma)$ generates $D(B_\Gamma)$. We first show

LEMMA 6.4. *There are a finite number of Z-homomorphisms*

$$f_j\colon\ D(B_\Gamma)\to Z,\quad j=1,\ldots,N$$

such that an element x of $D(B_\Gamma)$ is in $D^+(B_\Gamma)$ if and only if $f_j(x)\geqslant 0$ for $j=1,\ldots,N$.

For each $\Lambda\in B_\Gamma$, choose an R-lattice $X\in\Lambda$, and map Λ onto X_p. This induces a homomorphism

$$\sigma_p\colon\ D(B_\Gamma)\to D(B_{M_p}).$$

The group $D(B_{M_p})$ is free; a basis is formed by the images of the indecomposable R_p-lattices T_i, that occur in a decomposition of M_p. Thus we have

$$\sigma_p x = z_1[T_1]+\ldots+z_r[T_r]\quad\text{with } z_i\in Z.$$

Let $\{f_j\}_1^N$ be the set of all projections $x\to z_i$ for p varying in U. Then clearly $f_j(x)\geqslant 0$ is necessary for $x\in D^+(B_\Gamma)$. Conversely, suppose that $f_j(x)\geqslant 0$ for all j. This means that each $\sigma_p x$ is in $D^+(B_{M_p})$ for $p\in U$ and so there exist R_p-lattices Y^p, such that $\sigma_p x=[Y^p]$ for $p\in U$. Now it is easy to see, that there exists an A-module S, such that $k_p\otimes_k S\cong k_p\otimes_{o_p} Y^p$ for each $p\in U$ (cf. Proposition 5.7) and then Lemma 3.2 implies the existence of an R-lattice Y, such that $Y_p\cong Y^p$ for each $p\in Y$. Let Λ be the genus that contains Y and let y be the image of that genus in $D^+(B_\Gamma)$. Then we have $\sigma_p x=\sigma_p y$ for every $p\in U$. But we have seen earlier that the map

$$\sigma\colon\ D(B_\Gamma)\to\prod_{p\in U} D(B_{M_p})$$

induced by the σ_p is an injection. Consequently, we have $x=y$ and x is in $D^+(B_\Gamma)$.

Let m be the number of generators of $D(B_\Gamma)$. Then the rank of $\{f_j\}_1^N$ is m too; for otherwise $D^+(B_\Gamma)$ would contain a subgroup $\neq 0$ of $D(B_\Gamma)$. But if $x\in D^+(B_\Gamma)$ and $-x\in D^+(B_\Gamma)$ then $x=0$. We view $D(B_\Gamma)$ as an m-dimensional point-lattice. Then the inequalities $f_j\geqslant 0$ define a non-degenerate convex cone in $D(B_\Gamma)$. Such a cone is the union of a finite number of cones C_i, each of which has exactly m faces. Thus we have

$$D^+(B_\Gamma)=\bigcup C_i$$

and each C_i is defined by m independent inequalities $g_j\geqslant 0$ with $g_j\in\operatorname{Hom}(D(B_\Gamma),Z)$. Now take an indecomposable genus in B_Γ and let x be its image in $D^+(B_\Gamma)$. Then x lies in some C_i and is a fortiori indecomposable in C_i, that is $x=a+b$ with $a,b\in C_i$ implies $a=0$ or $b=0$. Thus we need only show that such a cone C only contains a finite number of indecomposable elements. But this is easy to see. Suppose C is defined by the inequalities $g_j\geqslant 0$, $j=1,\ldots,m$. Since the g_j are independent, we can find integers $a_j>0$, such that the system

$$g_j = a_j$$
$$g_i = 0 \quad \text{for } i \neq j$$

has a solution t_j. If x is an element of C such that $g_j(x) > a_j$ for some j, then $x - t_j$ is in C too and so x is decomposable. This means that the indecomposable elements of C satisfy the system

$$0 \leqslant g_j(x) \leqslant a_j, \quad j = 1, \ldots, m,$$

which has only a finite number of solutions. This completes the proof of Theorem 6.3.

Now let $\Lambda_1, \ldots, \Lambda_s$ be the indecomposable genera in B_Γ, and let $x_1, \ldots, x_s$ be their images in $D(B_\Gamma)$. Since every genus has at least one decomposition into indecomposable genera, these x_i generate $D(B_\Gamma)$ and so $s \geqslant m$. If s happens to be $= m$, then the x_i are a basis of $D(B_\Gamma)$ and every element of $D^+(B_\Gamma)$ is uniquely representable in the form $z_1 x_1 + \ldots + z_s x_s$ with $z_i \geqslant 0$. This means that B_Γ has unique decomposition.

If $s > m$, there is at least one non-trivial relation $z_1 x_1 + \ldots + z_s x_s = 0$. Separating positive and negative z_i, we obtain a non-trivial relation

$$\sum z_i' \Lambda_i = \sum z_i'' \Lambda_i.$$

Thus, for $s > m$, B_Γ does not have unique decomposition. But this does not imply, that every element of B_Γ has several different decompositions into indecomposable genera. In particular, the genus Γ with which we started, may or may not have a unique decomposition into indecomposable genera. The situation can be described in the following way. Let Y be the free abelian group with basis $y_1, \ldots, y_s$ and denote by Y^+ the elements of Y that have non-negative coefficients with respect to this basis. Then $y_i \to [\Lambda_i]$ induces an epimorphism $\varphi: Y \to D(B_\Gamma)$ and it is easily seen that the different decompositions of a genus Λ are in 1–1-correspondence with the elements of $\varphi^{-1}([\Lambda]) \cap Y^+$. Thus if $\varphi: Y \to D(B_\Gamma)$ is known, we can find all decompositions of a genus $\Lambda \in B_\Gamma$. — To describe those genera, which have more than one decomposition into indecomposable genera, let $a = z_1 y_1 + \ldots + z_s y_s$ be an element $\neq 0$ in $\operatorname{Ker} \varphi$. Separating positive and negative z_i, we can write $a = t - t'$, with $t, t' \in Y^+$. Let C be the subcategory of genera in B_Γ, whose image in $D(B_\Gamma)$ is of the form $\varphi(t)$. Then clearly, a genus Λ has more than one decomposition into indecomposable genera if and only if it has a decomposition $\Lambda = \Lambda' + \Lambda''$ with $\Lambda' \in C$. — We now mention a simple case where $\mathcal{G}_R$ has unique decomposition.

PROPOSITION 6.5. *Suppose that U contains only one element p (i.e. R_q is a maximal order for $q \neq p$) and that moreover $K(A) = K(k_p \otimes A)$. Then $\mathcal{G}_R$ has unique decomposition. In other words, if M_i and N_i are indecomposable R-lattices such that*

$$M_1 \oplus \ldots \oplus M_s \cong N_1 \oplus \ldots \oplus N_t$$

then $s = t$ and the N_i can be rearranged such that $M_i \sim N_i$ for $i = 1, \ldots, s$.

First from Proposition 5.7 we see that our conditions on R imply that $D(\mathcal{G}_R) \cong D(\mathcal{L}_{R_p})$. Then from the construction of the f_j in Lemma 6.4 we see that also $D^+(\mathcal{G}_R)$ and $D^+(\mathcal{L}_{R_p})$ are isomorphic. But $\mathcal{L}_{R_p}$ has unique decomposition and so $\mathcal{G}_R$ has unique decomposition too. — Clearly if moreover every genus in $\mathcal{G}_R$ has only one isomorphism class, then $\mathcal{L}_R$ has unique decomposition. (cf. Heller [8], who proved this if o is a valuation ring and $K(A) = K(k_p \otimes A)$)

Corollary 6.6. *Let G be a finite p-group with $p \neq 2$ and put $R = ZG$. Then $\mathcal{G}_R$ has unique decomposition.*

The discriminant of ZG, with respect to the trace of the regular representation is a power of p. This implies that $Z_q G$ is a maximal order for $q \neq p$. Let A_i be one of the simple algebras in QG and let K_i be its center. Since K_i is a subfield of the field of p^m-th roots of unity, p is completely ramified in K_i. Thus $Q_p \otimes K_i$ is a field and then $K(QG) = K(Q_p G)$ follows from the well-known fact that A_i is a complete ring of matrices over K_i.(1) We sketch a proof of this, following the method of Schilling, which is based on the fact that an algebra that does not split is ramified at two primes at least. Suppose that $H_i = G/G_1$ is represented faithfully by A_i. Since the center of H_i is not trivial, we see that K_i contains a p-th root of unity and because of our assumption $p \neq 2$, this implies that K_i is completely imaginary. Let $\mathfrak{p}$ be the (single) prime in K_i that divides p. Since the discriminant of ZG is a power of p, this $\mathfrak{p}$ is the only finite prime of K_i that could be ramified in A_i. Thus at most one prime of K_i is ramified in A_i and so A_i splits. — From Theorem 6.3 we obtain immediately

Theorem 6.7. *For an arbitrary R-lattice M, the category $B_M = \{X, X \oplus Y \cong zM, X, Y \in \mathcal{L}_R, z > 0\}$ contains only a finite number of indecomposable R-lattices (up to isomorphisms).*

This follows from the fact that indecomposable R-lattices determine indecomposable genera and that B_M is closed under direct factors in $\mathcal{L}_R$. Let $T_1, \ldots, T_s$ be representatives of the different indecomposable R-lattices in B_M. Then in a similar way as for genera, we can give a description of the different decompositions of a R-lattice $N \in B_M$; the only complication arises from the fact that the map $X \to [X] \in D(B_M)$ is not injective. Define Y, Y^+ and $\varphi: Y \to D(B_M)$ in the same way as for genera. Take a fixed $N \in B_M$ and suppose $z_1 y_1 + \ldots + z_s y_s \in \varphi^{-1}([N]) \cap Y^+$. Put $N' = z_1 T_1 + \ldots + z_s T_s$. Then we know, that $[N'] = [N]$, and this means that there is an R-lattice $X \in B_M$, such that

$$X \oplus N \cong X \oplus N'.$$

(1) See Schilling, *J. reine angew. Math.*, 174, 1936, p. 188 or Roquette, *Arch. Math.* (Basel), 9, 1958, 241–250.

According to Theorem 4.1, X can be cancelled here if $N \in \mathcal{L}'_R$ and if $X \in B_N$. Thus, for $N \in \mathcal{L}'_R$ and $B_N = B_M$, the different decompositions of N into indecomposable R-lattices are in 1-1-correspondence with the elements of $\varphi^{-1}([N]) \cap Y^+$.

Finally, we note a special case of the preceding theorem. If M is a free R-module, then B_M is the category of finitely generated projective R-modules and we have

COROLLARY 6.8. *The category $\mathfrak{P}_R$ of finitely generated projective R-modules contains only a finite number of indecomposable modules* (*apart from isomorphism*).

References

[1]. AUSLANDER, M. & GOLDMAN, O., Maximal orders. *Trans. Amer. Math. Soc.*, 97 (1960), 1–24.

[2]. BASS, H., K-theory and stable algebra. *Publications Inst. Hautes Etudes Sci.*, 22 (1964), 5–60.

[3]. CHEVALLEY, C., L'arithmétique dans les algèbres de matrices. *Actualités Sci. Ind.*, 323 (1936).

[4]. CURTIS, C. & REINER, I., *Representation theory of finite groups and associative algebras.* Interscience, 1962.

[5]. DEURING, M., *Algebren.* Ergebnisse der Mathematik 4, 1935.

[6]. EICHLER, M., Über die Idealklassenzahl hyperkomplexer Systeme. *Math. Z.*, 43 (1937), 481–494.

[7]. —— Allgemeine Kongruenzklasseneinteilungen der Ideale einfacher Algebren über algebraischen Zahlkörpern und ihre L-Reihen. *J. reine angew. Math.*, 179 (1938), 227–251.

[8]. HELLER, A., On group representations over a valuation ring. *Proc. Nat. Acad. Sci. U.S.A.*, 47 (1961), 1194–1197.

[9]. JACOBINSKI, H., Über die Geschlechter von Gittern über Ordnungen. *J. reine angew. Math.*, 230 (1968), 29–39.

[10]. REINER, I., Failure of the Krull–Schmidt theorem for integral representations. *Michigan Math. J.*, 9 (1962), 225–232.

[11]. —— Representation rings. To appear in *Michigan Math. J.*

[12]. RIM, D. S., On projective class groups. *Trans. Amer. Math. Soc.*, 98 (1961), 459–467.

[13]. ROITER, A. V., On integral representations belonging to an order (Russian). *Izv. Akad. Nauk SSSR Ser. Mat.*, 30 (1966), 1315–1324.

[14]. SERRE, J.-P., *Modules projectifs et espaces fibrés à fibre vectorielle.* Sém. Dubreil, 1957–58, n° 23.

[15]. SWAN, R. G., Induced representations and projective modules. *Ann. of Math.*, 71 (1960), 552–578.

[16]. —— Projective modules over group rings and maximal orders. *Ann. of Math.*, 76 (1962), 55–61.

[17]. —— The Grothendieck ring of a finite group. *Topology 2* (1963), 85–110.

Received September 11, 1967