J. Math. Soc. Japan
Vol. 13, No. 4, 1961

Quasi-equality in maximal orders

By Oscar GOLDMAN[1]

(Received May 1, 1961)

Introduction.

Let R be an integrally closed noetherian domain. Artin and van der Waerden [3] have defined the group of quasi-equality classes of ideals of R. In this paper we extend this notion to the case of a maximal order in a separable algebra over the quotient field K of R.

If Λ is a maximal order in such an algebra Σ, we consider the finitely generated R-submodules of Σ which span Σ over K and which have Λ as a left and right operator domain. Restricting our attention to those modules which are reflexive (Section 1) and defining multiplication suitably (Section 3), there is defined a group $G(\Lambda)$ which has the same relation to Λ as has the group of quasi-equality classes of ideals to R.

The group $G(\Lambda)$ is abelian and does not depend on Λ; if Γ is another maximal order, then $G(\Lambda)$ and $G(\Gamma)$ are naturally isomorphic. Finally, Theorem 3.4 shows that $G(\Lambda)$ is completely determined by the arithmetic of Σ in relation to the minimal prime ideals of R.

We use certain facts of the general theory of maximal orders over Dedekind rings; these may be found for example in Chapter VI of Deuring [2].

Section 1. Lattices.

Throughout this paper, R will denote an integrally closed noetherian domain with quotient field K and Σ will denote a (finite dimensional) separable algebra over K. By a *lattice* in Σ will be meant a finitely generated R-submodule of Σ which spans Σ over K.

If A is an R-module, we shall denote by A^* the dual, $\mathrm{Hom}_R(A, R)$ of A. There is an obvious natural homomorphism $A \to A^{**}$. We shall say that A is *reflexive* if that homomorphism is an isomorphism.

If A is a lattice in Σ every element of A^* has a unique extension to an element of $\mathrm{Hom}_K(\Sigma, K)$. Since Σ is a finite dimensional vector space over K

1) This work was done while the author held a fellowship from the National Science Foundation.

it is certainly reflexive, so that we may identify A^{**} with a submodule of Σ. Under that identification, A^{**} is again a lattice, and $A\subset A^{**}$. We may describe A^{**} explicitly as follows: an element $x\in\Sigma$ is in A^{**} if, and only if, $f(x)\in R$ for all those $f\in \mathrm{Hom}_K(\Sigma, K)$ for which $f(A)\subset R$.

PROPOSITION 1.1. *Let A and B be lattices in Σ, and let $C=\{x\in\Sigma \mid xA\subset B\}$. Then C is also a lattice. If B is reflexive, then C is also reflexive. The same statements hold for $D=\{x\in\Sigma \mid Ax\subset B\}$.*

PROOF. The assertion that C is a lattice is trivial to verify. To show that the reflexivity of B implies that of C, we proceed as follows. Let $f\in B^*$ and $a\in A$. Define, for $x\in\Sigma$, $g(x)=f(xa)$. If x is in C, then $xa\in B$ so that $g(x)=f(xa)\in R$. Thus, $g\in C^*$. Hence, if $y\in C^{**}$, we have $g(y)\in R$. But this shows that $f(yA)\subset R$, for every $f\in B^*$. Thus, $yA\subset B^{**}=B$, or $y\in C$. Hence $C^{**}=C$, or C is reflexive.

For later application we describe some of the relations between the formation of double duals and localization with respect to minimal prime ideals of R. If $\mathfrak{p}$ is a minimal prime ideal in R, we denote by $R_{\mathfrak{p}}$ the ring of quotients of R with respect to $\mathfrak{p}$. If A is a lattice in Σ, then $AR_{\mathfrak{p}}$ is a lattice over $R_{\mathfrak{p}}$.

PROPOSITION 1.2. *If A is a lattice in Σ and $\mathfrak{p}$ is a minimal prime ideal of R, then $AR_{\mathfrak{p}}=A^{**}R_{\mathfrak{p}}$.*

PROOF. It is clear that $A^*R_{\mathfrak{p}}=\mathrm{Hom}_{R_{\mathfrak{p}}}(AR_{\mathfrak{p}}, R_{\mathfrak{p}})$ and therefore that $A^{**}R_{\mathfrak{p}}=\mathrm{Hom}_{R_{\mathfrak{p}}}(A^*R_{\mathfrak{p}}, R_{\mathfrak{p}})=\mathrm{Hom}_{R_{\mathfrak{p}}}(\mathrm{Hom}_{R_{\mathfrak{p}}}(AR_{\mathfrak{p}}, R_{\mathfrak{p}}), R_{\mathfrak{p}})$. Since $R_{\mathfrak{p}}$ is a discrete valuation ring, we find $\mathrm{Hom}_{R_{\mathfrak{p}}}(\mathrm{Hom}_{R_{\mathfrak{p}}}(AR_{\mathfrak{p}}, R_{\mathfrak{p}}), R_{\mathfrak{p}})=AR_{\mathfrak{p}}$ and the result follows.

PROPOSITION 1.3. *If A and B are reflexive lattices such that the equality $AR_{\mathfrak{p}}=BR_{\mathfrak{p}}$ holds for every minimal prime ideal $\mathfrak{p}$ of R, then $A=B$.*

PROOF. Set $C=A+B$ and $\mathfrak{a}=\mathrm{ann}(C/A)$. Since A is reflexive, it follows from Proposition 1.4 of [1] that either $\mathfrak{a}=R$ (in which case $A=C$), or else $\mathfrak{a}$ is contained in some minimal prime ideal of R. If $\mathfrak{p}$ is any minimal prime ideal, the equality $AR_{\mathfrak{p}}=BR_{\mathfrak{p}}$ gives $AR_{\mathfrak{p}}=CR_{\mathfrak{p}}$ so that $\mathfrak{a}\not\subset\mathfrak{p}$. Thus, $\mathfrak{a}=R$ and therefore $A=C$. Since the situation is symmetric in A and B, it follows that $A=B$.

Section 2. Orders.

A lattice subring of Σ is called an *order*. An order is said to be *maximal* if it is not contained in a properly larger order.

The general discussion on orders in the first section of [1] is formulated for central simple algebras. Actually the proofs apply unchanged to the case of separable algebras. In particular, this is so for Theorem 1.5 of [1]: an order Λ is maximal if, and only if, Λ is reflexive and $\Lambda R_{\mathfrak{p}}$ is a maximal order over $R_{\mathfrak{p}}$, for every minimal prime ideal $\mathfrak{p}$ of R.

If A is a lattice, the set $\mathfrak{O}_l(A)$ of all $x\in\Sigma$ such that $xA\subset A$ is an order, called the *left order* of A. The *right order* $\mathfrak{O}_r(A)$ of A is defined in a similar fashion. The orders $\mathfrak{O}_l(A)$ and $\mathfrak{O}_r(A)$ are also referred to as the *associated orders* of A.

As an immediate application of Proposition 1.1 we have:

THEOREM 2.1. *The associated orders of a reflexive lattice are reflexive.*

PROOF. The assertion follows immediately from Proposition 1.1 by taking $A=B$ equal to the given lattice.

COROLLARY 2.2. *If A is a reflexive lattice and one of its associated orders is maximal, then the other one is also.*

PROOF. Suppose that $\mathfrak{O}_l(A)$ is maximal. By the proposition above we already known that $\mathfrak{O}_r(A)$ is reflexive. Hence, it is sufficient to show that $\mathfrak{O}_r(A)R_{\mathfrak{p}}$ is a maximal order over $R_{\mathfrak{p}}$, for every minimal prime ideal $\mathfrak{p}$ of R. It is clear that $\mathfrak{O}_l(AR_{\mathfrak{p}})=\mathfrak{O}_l(A)R_{\mathfrak{p}}$ and $\mathfrak{O}_r(AR_{\mathfrak{p}})=\mathfrak{O}(A)R_{\mathfrak{p}}$. The maximality of $\mathfrak{O}_l(A)$ over R implies the maximality of $\mathfrak{O}_l(A)R_{\mathfrak{p}}$ over $R_{\mathfrak{p}}$ which, because $R_{\mathfrak{p}}$ is a Dedekind ring, implies the maximality of $\mathfrak{O}_r(AR_{\mathfrak{p}})$ over $R_{\mathfrak{p}}$. Thus $\mathfrak{O}_r(A)R_{\mathfrak{p}}$ is maximal over $R_{\mathfrak{p}}$ and hence $\mathfrak{O}_r(A)$ is a maximal order.

If A is a lattice, the *inverse* A^{-1} of A is defined as the set of all $x\in\Sigma$ for which $AxA\subset A$. Equivalently, A^{-1} is the set of all $y\in\Sigma$ such that $yA\subset\mathfrak{O}_r(A)$ or the set of all $z\in\Sigma$ such that $Az\subset\mathfrak{O}_l(A)$.

If A is a lattice, set $\Lambda=\mathfrak{O}_l(A)$. Then A is naturally a left Λ-module. The inverse A^{-1} may be identified with $\mathrm{Hom}_\Lambda(A,\Lambda)$ as follows. If $z\in A^{-1}$ set $f(a)=az$ for $a\in A$. Then $f(a)\in\Lambda$ so that f defines a map from A into Λ, which is clearly Λ-linear on the left. On the other hand, let $f\in\mathrm{Hom}_\Lambda(A,\Lambda)$. Then, f extends uniquely to an element of $\mathrm{Hom}_\Sigma(\Sigma,\Sigma)$ (where Σ is considered as a left Σ-module). Such a homomorphism is given by right multiplication by some $z\in\Sigma$. Since $f(A)\subset\Lambda$, it follows that $z\in A^{-1}$.

THEOREM 2.3. *Let A be a lattice such that $\Lambda=\mathfrak{O}_l(A)$ is maximal. Then, A is reflexive as an R-module if, and only if, A is reflexive as a Λ-module.*

PROOF. Suppose first that A is reflexive as an R-module. Then by Proposition 1.1, A^{-1} is also a reflexive R-module. Furthermore, by Corollary 2.2, $\mathfrak{O}_r(A)$ is also maximal. Clearly, $\mathfrak{O}_l(A^{-1})=\mathfrak{O}_r(A)$ and $\mathfrak{O}_r(A^{-1})=\mathfrak{O}_l(A)$. Hence, $(A^{-1})^{-1}=\mathrm{Hom}_\Lambda(A^{-1},\Lambda)$. If $\mathfrak{p}$ is any minimal prime ideal of R, then $(A^{-1})R_{\mathfrak{p}}=(AR_{\mathfrak{p}})^{-1}$, with a similar statement for $(A^{-1})^{-1}$. However, $R_{\mathfrak{p}}$ is a Dedekind ring, so that $(A^{-1})^{-1}R_{\mathfrak{p}}=AR_{\mathfrak{p}}$. Applying Proposition 1.3 shows that $(A^{-1})^{-1}=A$, or that A is a reflexive Λ-module.

On the other hand, suppose that A is a reflexive Λ-module. Namely, $A=\{x\in\Sigma \mid A^{-1}x\subset\Lambda\}$. Since Λ is reflexive, because it is maximal, it follows from Proposition 1.1 that A is a reflexive R-module.

A lattice will be called *proper* if it is reflexive and its associated orders are maximal.

THEOREM 2.4. *Let A be a proper lattice. Then A^{-1} is also proper,* $(AA^{-1})^{**} = \mathfrak{O}_l(A)$ *and* $(A^{-1}A)^{**} = \mathfrak{O}_r(A)$. *Finally,* $(A^{-1})^{-1} = A$.

PROOF. The statement that A^{-1} is proper and that $(A^{-1})^{-1} = A$ is contained in Theorem 2.3. To see that $(AA^{-1})^{**} = \mathfrak{O}_l(A)$, let $\mathfrak{p}$ be a minimal prime ideal of R. Then, $A^{-1}R_\mathfrak{p} = (AR_\mathfrak{p})^{-1}$, and $(AR_\mathfrak{p})(AR_\mathfrak{p})^{-1} = \mathfrak{O}_l(AR_\mathfrak{p}) = \mathfrak{O}_l(A)R_\mathfrak{p}$ because $R_\mathfrak{p}$ is a Dedekind ring. Using Proposition 1.2 shows that $(AA^{-1})^{**}R_\mathfrak{p} = (AA^{-1})R_\mathfrak{p} = \mathfrak{O}_l(A)R_\mathfrak{p}$. Since this is so for every minimal prime ideal of R, it follows from Proposition 1.3 that $(AA^{-1})^{**} = \mathfrak{O}_l(A)$. In the same way we find $(AA^{-1})^{**} = \mathfrak{O}_r(A)$.

Section 3. The group of a maximal order.

If A and B are lattices, we define the *product* $A \circ B$ as $(AB)^{**}$. Clearly, $A \circ B$ is a reflexive lattice. It is also clear that $\mathfrak{O}_l(A \circ B) \supset \mathfrak{O}_l(A)$. Hence if A is a proper lattice, so that $\mathfrak{O}_l(A)$ is a maximal order, then $\mathfrak{O}_l(A \circ B)$ must coincide with $\mathfrak{O}_l(A)$ and therefore $A \circ B$ is also a proper lattice.

PROPOSITION 3.1. *If A, B and C are lattices, then* $(A \circ B) \circ C = A \circ (B \circ C) = (ABC)^{**}$.

PROOF. Let $\mathfrak{p}$ be a minimal prime ideal of R. Then, a repeated application of Proposition 1.2 shows that $(A \circ B) \circ CR_\mathfrak{p} = (ABC)^{**}R_\mathfrak{p} = A \circ (B \circ C)R_\mathfrak{p}$. Since the three lattices $A \circ (B \circ C)$, $(A \circ B) \circ C$ and $(ABC)^{**}$ are all reflexive, the assertion follows from Proposition 1.3.

Let Λ be a maximal order, and let $G(\Lambda)$ be the set of all proper lattices in Σ having Λ as both right and left associated orders. If A and B are in $G(\Lambda)$, then $A \circ B$ and A^{-1} are also in $G(\Lambda)$. Clearly $\Lambda \in G(\Lambda)$.

THEOREM 3.2. *$G(\Lambda)$ is an abelian group under the composition $A, B \to A \circ B$.*

PROOF. That $G(\Lambda)$ is a group follows from Theorem 2.4 and Proposition 3.1; the neutral element of $G(\Lambda)$ is clearly Λ. To see that $G(\Lambda)$ is abelian, let A and B be elements of $G(\Lambda)$ and let $\mathfrak{p}$ be any minimal prime ideal of R. Then, $(A \circ B)R_\mathfrak{p} = ABR_\mathfrak{p} = (AR_\mathfrak{p})(BR_\mathfrak{p})$. Since $R_\mathfrak{p}$ is a Dedekind ring, we have $(AR_\mathfrak{p})(BR_\mathfrak{p}) = (BR_\mathfrak{p})(AR_\mathfrak{p})$. Thus, $(A \circ B)R_\mathfrak{p} = (B \circ A)R_\mathfrak{p}$ and Proposition 1.3 then shows that $A \circ B = B \circ A$.

THEOREM 3.3. *If Λ and Γ are maximal orders in Σ, then $G(\Lambda)$ and $G(\Gamma)$ are naturally isomorphic.*

PROOF. Let $\mathfrak{F}$ be the *conductor* of Γ with respect to Λ, i. e., $\mathfrak{F} = \{x \in \Sigma \mid x\Gamma \subset \Lambda\}$. Then $\mathfrak{F}$ is a proper lattice whose associated left order is Λ and right order is Γ. If $B \in G(\Gamma)$, then $\mathfrak{F} \circ B \circ \mathfrak{F}^{-1} \in G(\Lambda)$ and the map $B \to \mathfrak{F} \circ B \circ \mathfrak{F}^{-1}$ is an isomorphism of $G(\Gamma)$ with $G(\Lambda)$.

Let Δ be a third order. Then, defining the isomorphisms by means of the appropriate conductors leads to the following diagram:

$$\begin{tikzcd} G(\Gamma) \arrow[rr] \arrow[dr] & & G(\Lambda) \arrow[dl] \\ & G(\Delta) & \end{tikzcd}$$

The naturality of the isomorphisms between these various groups will be proved when we show that the diagram is commutative.

Set $\mathfrak{F}_1=\{x \mid x\Lambda\subset\Delta\}$ and $\mathfrak{F}_2=\{x \mid x\Gamma\subset\Delta\}$. Then, if $A\in G(\Gamma)$ we must show that $\mathfrak{F}_1\circ\mathfrak{F}\circ A\circ\mathfrak{F}^{-1}\circ\mathfrak{F}_1^{-1}=\mathfrak{F}_2\circ A\circ\mathfrak{F}_2^{-1}$. Now, $\mathfrak{F}_2^{-1}\circ\mathfrak{F}_1\circ\mathfrak{F}\in G(\Gamma)$, so that because $G(\Gamma)$ is abelian, we have $\mathfrak{F}_2^{-1}\circ\mathfrak{F}_1\circ\mathfrak{F}\circ A\circ\mathfrak{F}^{-1}\circ\mathfrak{F}_1^{-1}\circ\mathfrak{F}_2=A$ from which the assertion follows.

Let Λ be a maximal order in Σ and let A be an element of $G(\Lambda)$ which is contained in Λ. Set $\mathfrak{a}=\mathrm{ann}(\Lambda/A)$. Then the ideal $\mathfrak{a}$ is contained in only a finite number of minimal prime ideals of R. If $\mathfrak{p}$ is a minimal prime ideal which does not contain $\mathfrak{a}$, then $AR_{\mathfrak{p}}=\Lambda R_{\mathfrak{p}}$. Thus $AR_{\mathfrak{p}}\neq\Lambda R_{\mathfrak{p}}$ for only finitely many $\mathfrak{p}$. Given any $C\in G(\Lambda)$, C can be expressed in the form $A\circ B^{-1}$ with both A and B in $G(\Lambda)$ and both contained in Λ. Hence, $CR_{\mathfrak{p}}\neq\Lambda R_{\mathfrak{p}}$ for only a finite set of $\mathfrak{p}$.

The map $A\to AR_{\mathfrak{p}}$ defines a homomorphism from $G(\Lambda)$ into $G(\Lambda R_{\mathfrak{p}})$. There is therefore defined a homomorphism from $G(\Lambda)$ into the direct product $\prod_{\mathfrak{p}} G(\Lambda R_{\mathfrak{p}})$. The preceding remarks show that the image is contained in the direct sum $\sum_{\mathfrak{p}} G(\Lambda R_{\mathfrak{p}})$ of the groups $G(\Lambda R_{\mathfrak{p}})$.

THEOREM 3.4. *The homomorphism $G(\Lambda)\to\sum_{\mathfrak{p}} G(\Lambda R_{\mathfrak{p}})$ is an isomorphism.*

PROOF. Proposition 1.3 shows immediately that the homomorphism is a monomorphism. We must prove that the mapping is onto.

Let $\mathfrak{p}$ be some minimal prime ideal, and let M be an element of $G(\Lambda R_{\mathfrak{p}})$ which is contained in $\Lambda R_{\mathfrak{p}}$. Then M contains some power of $\mathfrak{p}$. Set $A=M\cap\Lambda$. Then it is readily verified that A is a lattice and that both of the associated orders of A coincide with Λ. Furthermore, $AR_{\mathfrak{p}}=M$. Finally, let $\mathfrak{q}$ be a minimal prime ideal of R different from $\mathfrak{p}$. Then, the fact that A contains a power of $\mathfrak{p}$ shows that $AR_{\mathfrak{q}}=\Lambda R_{\mathfrak{q}}$. Now set $B=A^{**}$. Then, $B\in G(\Lambda)$ and $BR_{\mathfrak{p}}=M$ while $BR_{\mathfrak{q}}=\Lambda R_{\mathfrak{q}}$ for all $\mathfrak{q}\neq\mathfrak{p}$. (These last two statements follow from Proposition 1.2.) Every element of $G(\Lambda R_{\mathfrak{p}})$ has the form $M\circ N^{-1}$ with M and N contained in $\Lambda R_{\mathfrak{p}}$. Hence, given any element $M\in G(\Lambda R_{\mathfrak{p}})$, there exists an $A\in G(\Lambda)$ such that $AR_{\mathfrak{p}}=M$ and $AR_{\mathfrak{q}}=\Lambda R_{\mathfrak{q}}$, for all $\mathfrak{q}\neq\mathfrak{p}$. It follows immediately that the map $G(\Lambda)\to\sum G(\Lambda R_{\mathfrak{p}})$ is an epimorphism.

COROLLARY 3.5. *If Σ is a central simple algebra over K and Λ is a maximal order in Σ, then $G(\Lambda)$ is a free abelian group whose generators are in one-to-one correspondence with the minimal prime ideals of R.*

PROOF. In this case $G(\Lambda R_{\mathfrak{p}})$ is an infinite cyclic group, and the assertion follows from the theorem.

Institute for Advanced Study
Princeton, New Jersey

References

[1] M. Auslander and O. Goldman, Maximal orders, Trans. Amer. Math. Soc., 97 (1960), 1–24.
[2] M. Deuring, Algebren, Springer, Berlin, 1935.
[3] B. L. van der Waerden, Modern Algebra, vol. II, New York, 1950.