ON THE SEMIGROUP OF IDEAL CLASSES IN AN ORDER OF AN ALGEBRAIC NUMBER FIELD

BY E. C. DADE, O. TAUSSKY AND H. ZASSENHAUS

Communicated by N. Jacobson, December 30, 1960

There is a natural link between classes of ideals in orders of algebraic number fields and similarity classes of integral matrices defined by unimodular matrices.

Two fractional ideals in an order of an algebraic number field are called *arithmetically equivalent* if and only if they differ by a factor in the field. It is known that the number of classes obtained in this way is finite and that the classes form a finite abelian semigroup. In order to study and generalize these ideal classes orders in finite extensions of more general fields are considered.

In order to describe the results obtained several abstract concepts concerning semigroups are introduced:

An element a of a multiplicative semigroup S is called *invertible* if the equations

$$ax = ya = e, \qquad ea = ae = a$$

hold for some elements x, y, e of S.

It follows then that e is uniquely determined, as a function of a, that it is an idempotent and that a has a unique inverse with respect to e, namely ex. All invertible elements with the same identity e form a multiplicative group $G(e)$. A semigroup is called *pure* if every invertible element is an idempotent.

Two elements a, b of S are called *weakly equivalent* if the equations

$$ax = b, \qquad by = a$$

can be solved in S.

Consequently weak equivalence classes can be introduced. Every idempotent weak equivalence class contains exactly one idempotent.

These concepts are now applied to the abelian semigroup of classes of ideals in an algebraic extension E of a field F. Such an ideal is defined as an $\mathfrak{o}_F$-module, formed of elements in E, where $\mathfrak{o}_F$ is a Dedekind ring in F with F as quotient field. The ideals are assumed finitely generated over $\mathfrak{o}_F$ and to contain a basis of E over F.

This set of ideals $\mathfrak{a}$ is closed with respect to multiplication, addition, intersection, quotient $\mathfrak{a}:\mathfrak{b}$ (i.e. the set of elements x in E satisfying $x\mathfrak{b}\subseteq\mathfrak{a}$) and the adjoint operation $\mathfrak{a}^T$ (the set of elements x of E satisfying the condition that

$$\operatorname{tr} xy \in \mathfrak{o}_F$$

for all y of $\mathfrak{a}$). For every ideal $\mathfrak{a}$ we denote the order $\mathfrak{a}\colon\mathfrak{a}$ by $\mathfrak{o}_{\mathfrak{a}}$.

In the special case where F is the rational number field and $\mathfrak{o}_F$ the ring of rational integers the ideal classes form a finite commutative semigroup under arithmetical equivalence.

To study these ideals the following lemma of Krull is used:

Let $\mathfrak{a}$, $\mathfrak{b}$ *be two ideals which satisfy the relations*

$$\mathfrak{a}\mathfrak{b} = \mathfrak{b}, \qquad \mathfrak{a}\mathfrak{a} \subseteq \mathfrak{a}.$$

Then $\mathfrak{a}$ *is an order, i.e., an ideal which contains a unit element and is closed under multiplication.*

The lemma implies that every idempotent ideal is an order. It further implies that two ideals $\mathfrak{a}$, $\mathfrak{b}$ are weakly equivalent if and only if

$$1 \in (\mathfrak{b}\colon\mathfrak{a})(\mathfrak{a}\colon\mathfrak{b}).$$

If F is a finite extension of the rational field and $\mathfrak{o}_F$ the ring of algebraic integers then a power of every ideal of E is an invertible ideal. For this same special case we have:

Every idempotent weak equivalence class is represented by precisely one order. Conversely, for a given order $\mathfrak{o}$ of E over $\mathfrak{o}_F$ all $\mathfrak{o}$-ideals $\mathfrak{a}$ satisfying

$$\mathfrak{a}(\mathfrak{o}\colon\mathfrak{a}) = \mathfrak{o}$$

form a multiplicative group $G(\mathfrak{o})$ with $\mathfrak{o}$ as identity. This group is the idempotent weak equivalence class represented by $\mathfrak{o}$.

In the general case we have: All invertible ideals $\mathfrak{x}$ of E over $\mathfrak{o}_F$ with the same identity order $\mathfrak{o}_{\mathfrak{x}}$ form a multiplicative abelian group $G(\mathfrak{o})$.

For two orders $\mathfrak{o}$, $\mathfrak{o}'$ of E over $\mathfrak{o}_F$ satisfying $\mathfrak{o}\subseteq\mathfrak{o}'$ and $\mathfrak{o}\colon\mathfrak{o}' \neq (0)$ the mapping $\sigma(\mathfrak{o}, \mathfrak{o}')$ given by

$$\sigma(\mathfrak{o}, \mathfrak{o}')\mathfrak{x} = \mathfrak{x}\mathfrak{o}' \qquad (\mathfrak{x} \in G(\mathfrak{o}))$$

is a homomorphism of $G(\mathfrak{o})$ onto $G(\mathfrak{o}')$.

Take again the case when F is a finite extension of the rational field and $\mathfrak{o}_F$ the ring of integers in it. It is concluded that every ideal $\mathfrak{a}$ in E over $\mathfrak{o}_F$ is weakly equivalent to an ideal $\mathfrak{b}$ such that $\mathfrak{b}^{\rho}$ is an order $\mathfrak{o}_1$, for some integer ρ and such that

$$\mathfrak{b} \subseteq \mathfrak{o}_1,$$
$$\mathfrak{b}\mathfrak{o}_1 = \mathfrak{o}_1.$$

For the proof the fact that some power of $\mathfrak{a}$ is invertible is used. This follows by finiteness considerations.

It is shown next that for the general case the following fact holds:[1] *Let $E/F=n$ and let $\mathfrak{a}^\rho$ be the least positive invertible power of the ideal $\mathfrak{a}$ in E, then*

$$\rho \leqq n-1.$$

Further $n-1$ is best possible.

For the proof of this the following general lemma is proved:

Let H be a commutative hypercomplex system with unit element of dimension n over the field F. If for a linear subspace M of H there is a positive integer r such that

$$M^r = H$$

then also

$$M^{n-1} = H.$$

The following generalization can also be proved: *if H has a faithful representation by $\mu \times \mu$ matrices then*

$$M^{\mu-1} = H.$$

Finally, a "reduction" theorem is proved. First, observe that in any commutative ring R with unit element and a subring $\mathfrak{o}$ containing the unit element the $\mathfrak{o}$-modules contained in R form a system $I^*(R/\mathfrak{o})$ that is closed under addition, multiplication, intersection and quotient forming.

Furthermore let us introduce the relation of weak equivalence between two $\mathfrak{o}$-modules $\mathfrak{a}$, $\mathfrak{b}$ contained in R:

"$\mathfrak{a}$ is weakly equivalent to $\mathfrak{b}$" if and only if

$$\mathfrak{a}(\mathfrak{b}:\mathfrak{a}) = \mathfrak{b}, \qquad \mathfrak{b}(\mathfrak{a}:\mathfrak{b}) = \mathfrak{a}.$$

This relation is reflexive, symmetric, transitive and multiplicative so that the weak equivalence classes form an abelian semigroup $W^*(R/\mathfrak{o})$. Among these the classes containing a representative $\mathfrak{a}$ satisfying

$$\mathfrak{o}_{\mathfrak{a}} \supseteq \mathfrak{o}, \qquad \mathfrak{a}^q = \mathfrak{o}_{\mathfrak{a}^q}$$

for some exponent q, form a subsemigroup $U^*(R/\mathfrak{o})$.

[1] This was conjectured on the basis of an example of an order in the cubic field generated by $\alpha^3+2\alpha^2+2\alpha+1=0$, computed on the IBM 709 at the Western Data Processing Center by E. C. Dade and H. Zassenhaus. (An account of this computation which was sponsored in part by ONR will be published separately.) In the case of an order in a quadratic extension of the rational number field every ideal class has an inverse, for the semigroup of ideal classes is in this case a union of groups. This had already been discovered by Gauss in terms of quadratic forms.

THEOREM. *Let F be a finite extension of the rational field. Let $\mathfrak{o}_F$ be the subring of the algebraic integers of F. Let E be an extension of F of finite degree n. Let $\mathfrak{o}$, $\mathfrak{o}'$ be two orders of E over $\mathfrak{o}_F$ satisfying $\mathfrak{o}' \subseteq \mathfrak{o}$. Let*

$$\mathfrak{f} = \mathfrak{o}' : \mathfrak{o}.$$

The weak equivalence classes of ideals $\mathfrak{a}$ of E over $\mathfrak{o}_F$ satisfying

$$(1) \qquad \mathfrak{o}_{\mathfrak{a}} \supseteq \mathfrak{o}', \qquad\qquad (2) \qquad \mathfrak{o}_{\mathfrak{a}}^{n-1} \subseteq \mathfrak{o}$$

form an abelian semigroup $W(\mathfrak{o}, \mathfrak{o}'/\mathfrak{o}_F)$ that is isomorphic to $U^*(\mathfrak{o}/\mathfrak{f})/(\mathfrak{o}'/\mathfrak{f})$.

CALIFORNIA INSTITUTE OF TECHNOLOGY AND
UNIVERSITY OF NOTRE DAME