# 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