BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 80, Number 5, September 1974

REDUCTION THEORY IN ALGEBRAIC NUMBER FIELDS

BY HANS ZASSENHAUS

Communicated by Olga Taussky Todd, February 19, 1974

When is the half-group $\mathrm{GL}(n, \boldsymbol{Z}^{\geqq 0})$ of the unimodular matrices of degree n over the half-ring $\boldsymbol{Z}^{\geqq 0}$ of the nonnegative integers finitely generated?[1] Precisely if $n<3$.

Here the reduction of finite real extensions E of the rational number field is based on Theorem 1 stating the finiteness of the number of all matrices of degree n over $\boldsymbol{Z}^{\geqq 0}$ with a given irreducible characteristic polynomial over $\boldsymbol{Z}$, the rational integer ring, and on the following generalization of a well-known Frobenius theorem (Theorem 2): Let the semisimple commutative hypercomplex system A over $\boldsymbol{R}$, the real number field, contain a semiring H that is closed for the natural topology of A such that $A=H+(-H)$, $H\cap -H=\{0\}$ (pointed cone semiring). Then there are finitely many $\boldsymbol{R}$-homomorphisms θ_i $(1\leqq i\leqq s)$ of A into the complex number field $\boldsymbol{C}$ such that (1) $\bigcap_{i=1}^{s} \ker \theta_i=0$, (2) $\ker \theta_i+\ker \theta_k=A$ $(1\leqq i<k\leqq s)$, (3) $A\theta_i=\boldsymbol{R}$ $(1\leqq i\leqq \rho; 0<\rho\leqq s)$, ρ maximum, (4) for each ρ-tuple of nonnegative real numbers $\alpha_1, \cdots, \alpha_\rho$ there is an element h of H for which $h\theta_i=\alpha_i$ $(1\leqq i\leqq \rho)$, and (5) the set $C=\{(h\theta_1, \cdots, h\theta_s) | h\in H \& 0\leqq |h\theta_i|\leqq 1\ (1\leqq i\leqq s)\}$ is a closed convex subset of $\boldsymbol{C}^{1\times s}$ containing 0 and closed under multiplication, and conversely. Note that $|\lambda_i|\leqq \max_{1\leqq j\leqq \rho} |\lambda_j|$ $(1\leqq i\leqq s)$ for $(\lambda_1, \cdots, \lambda_s)$ of C.

Theorem 1 is applied to a dedekind module M of E that is invariant under the E-order Λ. Any basis of M over $\boldsymbol{Z}$ leading to an irreducible integral representation Δ of Λ representing a given primitive element ω of E contained in Λ by an integral matrix Ω of degree n over $\boldsymbol{Z}^{\geqq 0}$ permits the repeated formation of certain $\alpha\beta$-successors (predecessors) defined as

$$S^{\varepsilon}_{\alpha\beta}(\Omega) = T^{-\varepsilon}_{\alpha\beta}\Omega T^{\varepsilon}_{\alpha\beta}$$

$(\alpha\neq\beta,\ 1\leqq\alpha\leqq n,\ 1\leqq\beta\leqq n,\ \varepsilon=\pm 1,\ S^{\varepsilon}_{\alpha\beta}(\Omega)\in(\boldsymbol{Z}^{\geqq 0})^{n\times n})$ defining an oriented finite graph $\Gamma(\Omega)$ with a finitely presented fundamental group generated

AMS (MOS) subject classifications (1970). Primary 12A45, 12A50.

[1] This question was raised recently by G. Pall; it started the present exploration of a semigroup theoretic generalization of Lagrange's reduction theory. We utilize the subsemigroup S_n of $\mathrm{GL}(n, \boldsymbol{Z}^{\geqq 0})$ which is generated by the permutation matrices and the transvection matrices $T_{\alpha\beta}=I_n^{+}(\delta_{i\alpha}\delta_{k\beta})$ $(\alpha\neq\beta,\ 1\leqq\alpha\leqq n,\ 1\leqq\beta\leqq n)$ which is proper precisely if $n\geqq 3$.

by fundamental loops corresponding to finitely many integral matrices commuting with Ω and generating a subgroup U_Ω of the image of the unit group, $U(\Lambda)$, of Λ under Δ. An estimate based on Theorem 2 and the geometry of numbers is given such that $U_{\Omega^\nu}\langle -I_n\rangle = U(\Lambda)\Delta$ if $\nu \geqq \nu_0$. A method for obtaining a representative set of the ideal classes of Λ is developed in analogy to the method using continued fractions for real quadratic number field arithmetics.

A dualization method giving a new interpretation of the basic paper on 'matrix classes corresponding to an ideal and its inverse' (Illinois J. Math. **1** (1957), 108–113) by Olga Taussky is used in the course of the constructions.

DEPARTMENT OF MATHEMATICS, OHIO STATE UNIVERSITY, COLUMBUS, OHIO 43210