REDUCTION THEORY IN ALGEBRAIC NUMBER FIELDS

BY HANS ZASSENHAUS

Communicated by Olga Taussky Todd, February 19, 1974

When is the half-group \( GL(n, \mathbb{Z}^{\geq 0}) \) of the unimodular matrices of degree \( n \) over the half-ring \( \mathbb{Z}^{\geq 0} \) of the nonnegative integers finitely generated?\(^1\) Precisely if \( n \leq 3 \).

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 \( \mathbb{Z}^{\geq 0} \) with a given irreducible characteristic polynomial over \( \mathbb{Z} \), the rational integer ring, and on the following generalization of a well-known Frobenius theorem (Theorem 2): Let the semi-simple commutative hypercomplex system \( A \) over \( \mathbb{R} \), 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 infinitely many \( \mathbb{R} \)-homomorphisms \( \theta_i \) (\( 1 \leq i \leq s \)) of \( A \) into the complex number field \( \mathbb{C} \) such that (1) \( \bigcap_{i=1}^s \ker \theta_i = \{0\} \), (2) \( \ker \theta_i + \ker \theta_k = A \) (\( 1 \leq i < k \leq s \)), (3) \( A\theta_i = \mathbb{R} \) (\( 1 \leq i \leq \rho \); \( 0 < \rho \leq s \)), \( \rho \) maximum, (4) for each \( \rho \)-tuple of nonnegative real numbers \( \alpha_1, \ldots, \alpha_\rho \) there is an element \( h \) of \( H \) for which \( h\theta_i = \alpha_i \) (\( 1 \leq i \leq \rho \)), and (5) the set \( C = \{ (h\theta_1, \ldots, h\theta_s) | h \in H \cap \{0\} \} \) of \( C^{1 \times s} \) containing 0 and closed under multiplication, and conversely. Note that \( |\lambda_i| \leq \max_{1 \leq i \leq \rho} |\lambda_j| \) (\( 1 \leq i \leq s \)) for \( (\lambda_1, \ldots, \lambda_s) \) of \( C \).

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

\[ S_{\alpha \beta}^s(\Omega) = T_{\alpha \beta}^{-1} \Omega T_{\alpha \beta}^s \]

\((\alpha \neq \beta, 1 \leq \alpha \leq n, 1 \leq \beta \leq n, e = \pm 1, S_{\alpha \beta}^s(\Omega) \in (\mathbb{Z}^{\geq 0})^{n \times n})\) defining an oriented finite graph \( \Gamma(\Omega) \) with a finitely presented fundamental group generated

---

\(^1\) 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 \( GL(n, \mathbb{Z}^{\geq 0}) \) which is generated by the permutation matrices and the transvection matrices \( T_{\alpha \beta} = I_n(\delta_{\alpha \beta} \delta_{\alpha \beta}) \) (\( \alpha \neq \beta, 1 \leq \alpha \leq n, 1 \leq \beta \leq n \)) which is proper precisely if \( n \geq 3 \).
by fundamental loops corresponding to finitely many integral matrices commuting with $\Omega$ and generating a subgroup $U_{\omega}$ of the image of the unit group, $U(\Lambda)$, of $\Lambda$ under $\Delta$. An estimate based on Theorem 2 and the geometry of numbers is given such that $U_{\omega}v(-I_n) = U(\Lambda)\Delta$ if $v \geq v_0$. A method for obtaining a representative set of the ideal classes of $\Lambda$ 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