RATIONAL VECTOR SPACES II

By C. J. Everett and H. J. Ryser

1. **Introduction.** The previous paper in this journal entitled Rational Vector Spaces I and designated subsequently by [4] is concerned with the development of the structure of vector spaces defined over the field of rational numbers. Our present paper is a continuation of [4] and studies algebraic number fields as an example of the rational space theory. A large class of normal algebraic fields admit the trace function $T(\alpha^*\beta)$, where α^* denotes the complex conjugate of α, as a rational-valued inner product. Those fields which have an orthonormal basis with respect to this inner product are called *I*-fields. A number of theorems are established concerning these *I*-fields. For example, we prove that there exists only one *I*-field of degree two. However, every normal cubic field is an *I*-field and for every integer $n > 2$, there exists an infinitude of *I*-fields of degree n. In closing the function $T^{\frac{1}{2}}(\alpha^*\alpha)$ is studied as a pseudovaluation of an algebraic field.

2. **Algebraic number fields as rational inner product spaces.** Let $p(x) = x^m + r_1x^{m-1} + \cdots + r_m = (x - \rho_1) \cdots (x - \rho_m) = 0$ be an equation with coefficients in the rational field R and suppose that $p(x) = 0$ is irreducible over R. The set of all rational functions of $\rho = \rho_1$ with coefficients in R constitutes the *algebraic number field* $R(\rho)$. Evidently the field $R(\rho)$ is a rational vector space and has a basis $1, \rho, \cdots, \rho^{m-1}$. The m roots of the equation $p(x) = 0$ determine the conjugate fields $R(\rho_1), \cdots, R(\rho_m)$. If each of the conjugate fields contains the same elements, $R(\rho)$ is called a *normal algebraic field*, and the irreducible equation $p(x) = 0$ is called a *normal equation*. Every algebraic field $R(\rho)$ is extendible to its root field $R(\rho_1, \cdots, \rho_m)$, and this is a normal algebraic field of the form $R(\eta)$.

Let $R(\eta)$ denote a normal algebraic field, where $\eta = \eta_1$ satisfies the irreducible equation $y(x) = (x - \eta_1) \cdots (x - \eta_n) = 0$ of degree n. An *R-automorphism* of $R(\eta)$ is a mapping $\alpha \leftrightarrow \theta\alpha$ from $R(\eta)$ to all of $R(\eta)$ such that $\theta(\alpha + \beta) = \theta\alpha + \theta\beta$, $\theta(\alpha\beta) = \theta\alpha\theta\beta$, and $\theta(a\alpha) = a\theta\alpha$ for $a \in R$. There are exactly n of these mappings, namely $\alpha = a_0 + a_1\eta + \cdots + a_{n-1}\eta^{n-1} \leftrightarrow \theta_i\alpha = a_0 + a_1\eta_i + \cdots + a_{n-1}\eta_i^{n-1}$. In the set $G = \{\theta_1, \cdots, \theta_n\}$ of all automorphisms, we define $\theta_j\theta_k$ by $\theta_j\theta_k(\alpha) = \theta_j(\theta_k\alpha)$, whereupon G becomes a group, the *Galois group* of $R(\eta)$.

Now the mapping $\alpha \leftrightarrow \alpha^*$, where α^* is the complex conjugate of α, is an R-automorphism σ which coincides with some θ_i of G. If $R(\eta)$ contains only real elements, then σ equals the identity automorphism θ_1. If $R(\eta)$ contains imaginary elements, then all the η_i are imaginary, since each η_i generates $R(\eta)$

Received November 4, 1948.