

FACTORIZING ALGEBRAIC NUMBERS

ROGER WIEGAND

University of Nebraska–Lincoln

An *algebraic number field* is a field obtained from the rational numbers \mathbb{Q} by adjoining a finite number of algebraic numbers. Equivalently, it is a field extension of \mathbb{Q} that is finite-dimensional as a vector space over \mathbb{Q} . For example, $\mathbb{Q}(\sqrt{2}, i)$ is four-dimensional, with basis $\{1, \sqrt{2}, i, i\sqrt{2}\}$. Every element of $\mathbb{Q}(\sqrt{2}, i)$ has degree 1, 2 or 4 over \mathbb{Q} . (The degree of an algebraic number is by definition the degree of its minimal polynomial.) For example, the minimal polynomial of $\alpha := i + \sqrt{2}$ is $x^4 - 2x^2 + 9$, so it has degree 4. Observe that $\alpha = (1 - i\sqrt{2}) \cdot i$, and each of the factors has degree 2. One can show, however, that $\beta := 1 + i + \sqrt{2}$ *cannot* be factored as a product of two (or more) elements of degree 2. On the other hand, β^2 *can* be so factored: $\beta^2 = (2 + 2\sqrt{2}) \cdot (1 + i)$. In fact, it turns out that the square of *every* element of $\mathbb{Q}(\sqrt{2}, i)$ is a product of elements of degree 2. This raises three questions: (1) For an algebraic number field K of dimension d over \mathbb{Q} , when can every element of K be factored as a product of elements of degree strictly smaller than d ? (2) When can some power of each element be factored as a product of elements of degree strictly smaller than d ? (3) When the answer to (2) is “yes”, is there a fixed power that takes care of *every* element of K ? These questions were answered in a 1992 paper *Galois groups and the multiplicative structure of field extensions*, Trans. Amer. Math. Soc **331** (1992), 563–584, by R. Wiegand and R. Guralnick. The answer to (1) is disagreeably technical, and I won’t discuss it in this talk. The answers to (2) and (3) can be stated rather easily (in fact, the answer to (3) is a three-letter word), but the proofs require some sophisticated group theory. Rather surprisingly, the 2×2 matrices of determinant 1 over fields of order p , where p is a Fermat prime, play a special role.