1014-12-13 **Hendrik W. Lenstra Jr.***, Universiteit Leiden. *Entangled radicals, Part I.*

Let K be a field of characteristic zero, and let Ω be an algebraically closed field containing K; one may think of K and Ω as being the fields $\mathbf{Q}$ and $\mathbf{C}$ of rational and complex numbers, respectively. Write K^* for the multiplicative group of non-zero elements of K, and $\sqrt{K^*}$ for the group of *radicals* over K, i.e., the subgroup $\{a \in \Omega^* : a^n \in K^*$ for some positive integer $n\}$ of Ω^*. The structure of the extension field $K(\sqrt{K^*})$ of K is independent of the choice of Ω, and the question poses itself to "understand" this structure solely in terms of the base field K. One of the difficulties one faces, is the doubtful validity of a "rule" like $\sqrt{a} \cdot \sqrt{b} = \sqrt{ab}$. Another complication arises from "additive" entanglement of radicals, which manifests itself in enigmatic results from elementary number theory such as the following: if n is a positive integer for which $n^4 + 4^n$ is a prime number, then $n = 1$; and if p is a prime number with $p \equiv 1 \bmod 4$, then $(p^p - 1)/(p - 1)$ is composite. The lecture presents a novel approach to describing the structure of $K(\sqrt{K^*})$ that is based on ring theory. It is both of theoretical interest and potentially useful in computer algebra. At least in the case $K = \mathbf{Q}$, the answers are as complete and explicit as one might reasonably desire. (Received April 05, 2005)