962-11-735 **Donald Mills*** (ad3943@usma.edu), Department of Mathematical Sciences, West Point, NY 10996, and **Gavin McNay** (gavin.mcnay@nomura.co.uk), 20 Siddons Road, Tottenham, N17 London, England. *Primitive Roots in Cubic and Higher Extensions of a Finite Field.*

In 1983 S.D. Cohen proved that for any finite field $GF(q)$ and for any element θ such that $GF(q)(\theta) = GF(q^2)$ there exist elements a, $b \in GF(q)$ such that $a\theta + b$ is a primitive root of $GF(q^2)$. We consider the same question, but for higher extensions, namely cubic, quartic, and quintic extensions. We prove that for any finite field $GF(q)$ and for any element θ such that $GF(q)(\theta) = GF(q^3)$ there exist elements a, $b \in GF(q)$ such that $a\theta + b$ is a primitive root of $GF(q^3)$. We give asymptotic results for the quartic and quintic cases as well. Additionally, we address the more difficult question of whether the above problem can be resolved in the affirmative when $a = 1$ and θ is a defining element of either $GF(q^3)$ or $GF(q^4)$. These primitive sums can be used as pseudo-random vector generators; we illustrate this application for $n = 3$. (Received September 24, 2000)