DAVID J. MURAKI is a professor of mathematics at Simon Fraser University. His usual research concerns wave propagation and atmospheric fluid dynamics. When not collaborating with scientists at the National Center for Atmospheric Research (Boulder, CO), he is an enthusiast of the visual arts.
Department of Mathematics, Simon Fraser University, Burnaby BC, Canada V5A 1S6
muraki@math.sfu.ca

Cyclic Extensions Are Radical

The fact that finite Galois extensions with cyclic Galois group can be constructed by adjoining a root of a well-chosen element of the base field is a basic result of Galois theory and a key point in studying the problem of solvability by radicals. In textbooks on the subject, this result is usually obtained as a consequence of Hilbert's Theorem 90, which is itself deduced from Artin's theorem on the independence of characters. The very simple argument we present below sidesteps those requirements.

Theorem. *If E/K is a cyclic extension of degree n of a field K which contains a primitive nth root of unity ζ, then there exists an $x \in E$ with $x^n \in K$ and $E = K(x)$.*

Notice that the existence of a primitive nth root of unity in K implies that the characteristic of this field does not divide n.

Proof. Let σ be a generator of the Galois group G of the extension. Since $\sigma^n = \mathrm{id}_E$, the minimal polynomial of σ over K divides $X^n - 1$ in $K[X]$ and then, as this polynomial has all its roots in K and they are all simple, σ is diagonalizable and its eigenvalues are nth roots of unity.

Let Γ be the set of eigenvalues of σ. If $\lambda, \mu \in \Gamma$, so that there are $a, b \in E^\times$ such that $\sigma(a) = \lambda a$ and $\sigma(b) = \mu b$, then $\lambda\mu \in \Gamma$, as $\sigma(ab) = \lambda\mu ab$. Since Γ is contained in Ω_n, the finite group of nth roots of unity, this is enough to conclude that Γ is in fact a *subgroup* of Ω_n. If m is the order of Γ, then we have that $\lambda^m = 1$ for all $\lambda \in \Gamma$ and, as σ is diagonalizable with eigenvalues in Γ, that $\sigma^m = \mathrm{id}_E$. As the order of σ is n and $m \leq n$, it follows from this that $m = n$.

All nth roots of unity are therefore eigenvalues of σ and, in particular, there is an $x \in E^\times$ such that $\sigma(x) = \zeta x$. Then $\sigma(x^n) = \zeta^n x^n = x^n$, so x^n is in the fixed field $E^G = K$. We thus see that x is a root of the polynomial $X^n - x^n$ of $K[X]$, which is irreducible over K: indeed, it has simple roots $x, \zeta x, \ldots, \zeta^{n-1}x$ in E and these are permuted transitively by σ. The degree of the subextension $K(x)/K$ of E/K is then n and, of course, this means that $E = K(x)$. ■

—Submitted by Mariano Suárez-Álvarez

http://dx.doi.org/10.4169/amer.math.monthly.123.2.160
MSC: Primary 12F10, Secondary 00A05