A Book of Abstract Algebra | (2nd Edition)

Problem

In the next three parts, let ω be a primitive pth root of unity, where p is a prime.

Prove: If $h \in Gal(\mathbb{Q}(\omega) : \mathbb{Q})$, then $h(\omega) = \omega k$ for some k where $1 \le k \le p - 1$.

Step-by-step solution

Step 1 of 2

Consider a primitive $p\text{th}$ root of unity ω ,where p is a prime. The objective is to prove that if $h \in Gal(\mathbb{Q}(\omega):\mathbb{Q})$,then $h(\omega) = \omega^k$ for $1 \le k \le p-1$.

Comment

Step 2 of 2

Consider $x^p - 1 = (x-1)\Phi_p(x)$ where $\Phi_p(x) = x^{p-1} + ... + x^3 + x^2 + x + 1$ is the irreducible cyclotomic polynomial having ω as a root.

Every automorphism of $K = \mathbb{Q}(\omega)$ over $\mathbb{Q}$ must map ω into one of the $p-1$ roots

$\omega, \omega^2, ..., \omega^{p-1}$ of this polynomial.

Thus , if $h \in Gal(\mathbb{Q}(\omega):\mathbb{Q})$,then $h(\omega) = \omega^k$ for $1 \le k \le p-1$.

Comment