A Book of Abstract Algebra | (2nd Edition)

Chapter 32, Problem 7EG

Bookmark

Show all steps: ON

Problem

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

Use part 5 to prove that $Gal(\mathbb{Q}(\omega):\mathbb{Q})$ is a cyclic group.

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 $G = Gal(\mathbb{Q}(\omega):\mathbb{Q})$ is a cyclic group.

Comment

Step 2 of 2

Show that $G = \mathbb{Z}_p^{\times}$, the multiplicative group of units of a finite field.

ω is algebraic over $\mathbb{Q}$ with minimal polynomial $f(x) = 1 + x + \ldots + x^{p-1}$ and that

$S = \{\omega, \omega^2, \ldots, \omega^{p-1}\}$ is the set of conjugates of ω in $\mathbb{Q}$.

If $\tau \in G$, then τ is determined by its action on ω and must take ω to an element of S.

Define $\Theta : G \to \mathbb{Z}_p^{\times}$ as follows:

$\Theta(\tau) = [k]$ provided $\tau(\omega) = \omega^k$.

If $\tau, \alpha \in G$ with $\tau(\omega) = w^k$ and $\alpha(\omega) = \omega^m$, where $1 \le k, m \le p-1$, then

$$\tau\alpha(\omega) = \tau(\omega^m)$$
$$= (\tau(\omega))^m$$
$$= w^{mk}$$

and hence

$$\begin{aligned}\Theta(\tau\alpha) &= [km] \\ &= [k][m] \\ &= \Theta(\tau)\Theta(\alpha),\end{aligned}$$

and it follows that Θ is a group homomorphism.

Clearly， Θ is onto.

Let $\tau(\omega) = \alpha(\omega)$.

Then $\omega^k = \omega^m$.

$\Rightarrow k = m$ ， $1 \le k, m \le p-1$

$$\Rightarrow [k] = [m]$$
$$\Rightarrow \Theta(\tau) = \Theta(\alpha)$$

Thus， Θ is one-one.

Hence， Θ is an isomorphism.

Since G is isomorphic to the multiplicative group of units of a finite field， G is a cyclic group as the multiplicative group of units of a finite field is cyclic.

Comment