A Book of Abstract Algebra | (2nd Edition)

Problem

Throughout this set of questions, let K be a root field over F, let **G** = $Gal(K : F)$, and let I be any intermediate field. Prove the following:

If H is a subgroup of **G** and $H^\circ = \{a \in K : \pi(a) = a \text{ for every } \pi \in H\}$, then H° is a subfield of K, and $F \subseteq H^\circ$.

Step-by-step solution

Step 1 of 3

Consider a root field K over F, let $G = Gal(K:F)$, and let I be any intermediate field. The objective is to prove that if H is a subgroup of G then H^o is a subfield of K, where $H^o = \{a \in K : \pi(a) = a \text{ for every } \pi \in H\}$, and $F \subseteq H^o$.

Comment

Step 2 of 3

Let $x, y \in H^o$.

Show that $x - y \in H^o$ and if $y \neq 0$, then $xy^{-1} \in H^o$.

Since $\pi(y) = y$ for every $\pi \in H$, $\pi(-y) = -y$ because π is a group homomorphism under addition and $\pi(y^{-1}) = y^{-1}$ because π is a group homomorphism under multiplication for every $\pi \in H$.

Thus, $\pi(x-y) = \pi(x) + \pi(-y) = x - y$ and $\pi(xy^{-1}) = \pi(x)\pi(y^{-1}) = xy^{-1}$ for every $\pi \in H$.

Thus, $x - y \in H^o$ and if $y \neq 0$, then $xy^{-1} \in H^o$.

Comment

Step 3 of 3

Suppose that $F = H^o$.

$K = F(\alpha)$ for some $\alpha \in K$.

Define a polynomial $f(X) \in K[X]$ by $f(X) = \prod_{\sigma \in H}(X - \sigma(\alpha))$.

If τ is any automorphism in H, then apply τ to f. The result is

$(\tau f)(X) = \prod_{\sigma \in H}(X - (\tau\sigma)\alpha)$.

But as σ ranges over all of H, so does $\tau\sigma$, and consequently $\tau f = f$.

Thus each coefficient of f is fixed by H, so $f \in F[X]$.

Now, α is a root of f, since $X - \sigma(\alpha)$ is 0 when $X = \alpha$ and σ is the identity.

There are two things about the degree of f:

(1) By the definition of f, $\deg f = |H| < |G| = |K : F|$, and since f is a multiple of the minimal polynomial of α over F.

(2) $\deg f \geq [F(\alpha) : F] = [K : F]$, which is a contradiction.

Therefore, $F \subseteq H^o$.

Comment