A Book of Abstract Algebra | (2nd Edition)

Chapter 32, Problem 6EI

Bookmark

Show all steps: ON

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 **G** is a cyclic group, there exists exactly one intermediate field *I* of degree *k*, for each integer *k* dividing [*K* : *F*].

Step-by-step solution

Step 1 of 2

Consider a root field K over F, let $G = Gal(K:F)$. The objective is to prove that if G is a cyclic group then there exists exactly one intermediate field I of degree k, for each integer k dividing $[K:F]$.

Comment

Step 2 of 2

By Galois theory, there is a one-to-one correspondence between subgroups H of G and fields $I = K_H$ such that $F \le I \le K$.

Because G is cyclic, it contains precisely one subgroup of each order k that divides $|G| = [K:F]$.

Such a subgroup corresponds to a field I where $F \le I \le K$ and $[K:I] = k$, so that

$$[I:F] = \frac{[K:F]}{[K:I]} = \frac{n}{k}.$$

Now as d runs through all divisors of n, the quotients $\frac{n}{k}$ also run through all divisors of n, so this proves the result.

Comment