A Book of Abstract Algebra | (2nd Edition)

Problem

Let F be a finite field, and F^* the multiplicative group of nonzero elements of F. Obviously $H = \{x^2 : x \in F^*\}$ is a subgroup of F^*; since every square x^2 in F^* is the square of only two different elements, namely $\pm x$, exactly half the elements of F^* are in H. Thus, H has exactly two cosets: H itself, containing all the squares, and aH (where $a \notin H$), containing all the nonsquares. If a and b are nonsquares, then by Chapter 15, Theorem 5(i),

$$ab^{-1} = \frac{a}{b} \in H$$

Thus: if a and b are nonsquares, a/b is a square. Use these remarks in the following:

If the minimum polynomial of a over F has degree 2, we call $F(a)$ a quadratic extension of F.

Use part 3 to prove: Any two quadratic extensions of a finite field are isomorphic.

Step-by-step solution

Step 1 of 3

Objective is to prove that any two quadratic extensions of a finite field are isomorphic.

Consider the finite field F and let $a, b \in F$. Assume that $p(x)$, $q(x)$ are arbitrary quadratic irreducible polynomials in $F[x]$ and $\sqrt{a}, \sqrt{b}$ are the roots of these polynomials in some extension of F.

Then a/b is a square and $\sqrt{b}$ will be a root of $p(cx)$ for some c in F.

Since $p(x) \in F[x]$ is an irreducible polynomial and $\sqrt{b}$ is a root of $p(cx)$. Therefore, it follows, from the above result, that

$$\frac{F[x]}{\langle p(cx)\rangle} \cong F(\sqrt{b}).$$

Comment

Step 2 of 3

Next, objective is to prove that $F(\sqrt{a}) \cong F(\sqrt{b})$. It is known that $\sqrt{a}$ is a root of $p(x)$ and $\sqrt{b}$ is a root of $p(cx)$. Thus,

$$\frac{F[x]}{\langle p(x)\rangle} \cong F(\sqrt{a}),\ \frac{F[x]}{\langle p(cx)\rangle} \cong F(\sqrt{b}).$$

Since $F[x]/\langle p(cx)\rangle \cong F[x]/\langle p(x)\rangle$, therefore

$$F(\sqrt{a}) \cong F(\sqrt{b}).$$

Comment

Step 3 of 3

Since polynomials $p(x)$ and $q(x)$ are arbitrary irreducibles in $F[x]$ of degree 2, therefore it can conclude that any two quadratic extensions of a finite field are isomorphic.

Comment