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.

Let F be a finite field. If $a, b \in F$, let $p(x) = x^2 - a$ and $q(x) = x^2 - b$ be irreducible in $F[x]$, and let $\sqrt{a}$ and $\sqrt{b}$ denote roots of $p(x)$ and $q(x)$ in an extension of F. Explain why a/b is a square, say $a/b = c^2$ for some $c \in F$. Prove that $\sqrt{b}$ is a root of $p(cx)$.

Step-by-step solution

Step 1 of 3

Consider the finite field F and let $a, b \in F$. Assume that $p(x) = x^2 - a$, $q(x) = x^2 - b$ be irreducible in $F[x]$ and $\sqrt{a}, \sqrt{b}$ are the roots of these polynomials in some extension of F.

Objective is to prove that a/b is a square and $\sqrt{b}$ is a root of $p(cx)$ for some c in F.

Consider the following result:

The ca is a root of $p(x)$ if and only if a is a root of $p(cx)$.

Comment

Step 2 of 3

Let K is a extension field of F such that $\sqrt{a}, \sqrt{b} \in K$. Being an extension of F, $a, b \in K$. Since $a = \left(\sqrt{a}\right)^2, b = \left(\sqrt{b}\right)^2$, therefore

$$\begin{aligned}\frac{a}{b} &= \frac{\left(\sqrt{a}\right)^2}{\left(\sqrt{b}\right)^2} \\ &= \left(\sqrt{\frac{a}{b}}\right)^2.\end{aligned}$$

Let $c = \sqrt{\frac{a}{b}}$. Then $\frac{a}{b} = c^2$. This shows that a/b is a square in the field.

Comment

Step 3 of 3

Since $c = \sqrt{\frac{a}{b}}$, so $\sqrt{a} = c\sqrt{b}$.

This implies that $c\sqrt{b}$ is a root of polynomial $p(x) = x^2 - a$ in K.

Thus, $c\sqrt{b}$ is a root of polynomial $p(x)$ implies $\sqrt{b}$ is a root of $p(cx)$ (by the above result).

Comment