

## A Book of Abstract Algebra | (2nd Edition)

Chapter 27, Problem 5EF

Bookmark

Show all steps: 

ON

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  $F$ .  
If  $a$  and  $b$  are nonsquares in  $\mathbb{R}$ ,  $a/b$  is a square (why?). Use the same argument as in part 4 to prove that any two simple extensions of  $\mathbb{R}$  are isomorphic (hence isomorphic to  $\mathbb{C}$ ).

>

Step-by-step solution

Step 1 of 2 ^

Objective is to prove that if  $a$  and  $b$  non-squares real numbers then  $a/b$  is a square.

Since  $a$  and  $b$  are some real numbers, then corresponding  $\sqrt{a}, \sqrt{b}$  will also be the members of  $R$ . Then

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

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

Comment

Step 2 of 2 ^

Note that, any simple extension of  $R$  will be quadratic. Also, polynomials of degree  $\leq 2$  are the only irreducibles in  $R$ .

Also from the result: if polynomials  $p(x)$  and  $q(x)$  are arbitrary irreducibles in  $F[x]$  of degree 2, then any two quadratic extensions of a field are isomorphic.

Thus, any two simple extensions of  $R$  are isomorphic. Since quadratic extension of  $R$  is the set of all complex numbers, therefore any two simple extensions of  $R$  are isomorphic to  $\mathbb{C}$ .

Comment

