A Book of Abstract Algebra | (2nd Edition)

Problem

Let *p* be a prime number, and *ω* a primitive *p*th root of unity in the field *F*.

Explain why $b^{sp} = a^{sm}$. Use this to show that $(b^s a^t)^p = a$.

Step-by-step solution

Step 1 of 4

Here, objective is to explain why $b^{sp} = a^{sm}$ and prove that $(b^s a^t)^p = a$.

Comment

Step 2 of 4

Consider the polynomial $x^p - a$.

$$x^p - a = 0$$
$$x = \sqrt[p]{a}\ \omega$$

Then, the root $d = \sqrt[p]{a}$, ω is the p^{th} root of unity

Comment

Step 3 of 4

Consider the polynomial $x^p - a \in F(x)$

P is a prime and $x^p - a$ is reducible in $F(x)$

Let, $d_1, d_2, \ldots\ldots\ldots\ldots d_p$ are the roots of $x^p - a$

$$x^p - a = (x - d_1)(x - d_2)\ldots\ldots(x - d_p)$$

$p(x) = (x - d_1)(x - d_2)\ldots\ldots.(x - d_m)$. $p(x)$ is the product of *m* number of these factors.

Since, degree $p(x) = m$

Let the Constant term of above equation is *b,*

$$b = (d_1 d_2 \ldots\ldots d_m)$$

$$b = \sqrt[p]{a} \ldots\ldots \sqrt[p]{a}$$

$$b = \omega^k (\sqrt[p]{a})^m$$

$$b = \omega^k d^m$$

$$b = \left(\sqrt[p]{a}\right)^m \qquad (\because \omega^k = 1)$$

$$b^p = a^m$$

$$b^{sp} = a^{sm}$$

Comment

Step 4 of 4

$$\begin{aligned} \text{Consider } (b^s a^t)^p &= (b^{sp} a^{tp}) \\ &= (a^{sm} a^{tp}) \\ &= a^{sm+tp} \\ &= a \qquad (\because sm + tp = 1) \end{aligned}$$

Then, $(b^s a^t)^p = a$

Hence, proved

Comment