

Abstract Algebra

RADICALS WITH PRIME EXPONENTS:-

In order to obtain the radical extensions we may need only radicals with prime exponents.

we consider an equation

$$x^n - a = 0 \quad \text{--- (1)}$$

If $n = rs$, then we have

$$x^{rs} - a = 0 \quad \text{or} \quad (x^r)^s - a = 0 \quad \text{--- (2)}$$

Now a root α of $x^n - a = 0$ is a root of

$$x^r = \beta \quad \text{--- (3)}$$

where β is a root of $x^s - a = 0$ --- (4)

Thus, if F is a field such that

$$x^n - a \in F[x], \text{ then } F \subseteq F(\beta) \subseteq F(\alpha)$$

Proceeding in this manner, we can find a finite series of pure extensions such that each member of the series is obtained on adjoining to its predecessor a radical with a prime exponent.

Now we shall refer to solvability by radicals in above manner as follows:

Let $\alpha_1, \alpha_2, \dots, \alpha_n$ be the n distinct roots of an equation $x^n - a = 0$ over F , which are in its splitting field. Obviously, none of α_i is zero. Then we consider

as the n distinct roots of an equation $x^n - 1 = 0$.

$$1 = \frac{\alpha_1}{\alpha_1}, \frac{\alpha_1}{\alpha_2}, \dots, \frac{\alpha_1}{\alpha_n}$$

These roots are also in the splitting field of $x^n - a = 0$

Hence, we conclude that the splitting field of $x^n - 1 = 0$ may be regarded as an intermediate field between F and the splitting field of $x^n - a = 0$.

Roots of unity and cyclotomic polynomials :-

Definition :- Let F be a field. Then the roots of $x^n - 1 = 0$ over F are known as the primitive n th roots of unity in its splitting field if $\omega^n = 1$, but $\omega^m \neq 1$ for any positive integer $m < n$. There are exactly $\phi(n)$ primitive n th roots of unity, for every integer n .

Definition :- If we consider the equation $x^n - 1 = 0$ over the field of rational numbers, then the complex numbers satisfying $x^n - 1 = 0$ divide the circumference of a circle with centre at the origin and of unit radius into n equal parts. Thus the equation $x^n - 1 = 0$ is known as cyclotomic.

Notes :- (i) If F be field and n be a positive integer. Then there exists a primitive n th root of unity in some extension K of F if and only if either characteristic of F is zero or not a divisor of n .