ABSTRAK

Untuk setiap bilangan prima p, terdapat medan berhingga berorder p, yaitu $\mathbf{Z}_p$. Galois menyatakan bahwa medan berhingga berorder pangkat bilangan prima dapat dikonstruksi jika dapat ditemukan polinomial takthereduksi berderajat positif atas $\mathbf{Z}_p$. Pada kenyataannya, dapat ditemukan polinomial takthereduksi berderajat positif atas $\mathbf{Z}_p$. Maka untuk setiap bilangan prima p dan setiap bilangan bulat positif n, selalu dapat dikonstruksi medan Galois berorder p^n, dinotasikan dengan GF(p^n). Lebih khusus, untuk suatu bilangan prima p dan suatu bilangan bulat positif n, terdapat satu dan hanya satu medan Galois berorder p^n. Dan banyaknya submedan dari medan Galois GF(p^n) adalah banyaknya bilangan bulat positif yang membagi n.

ABSTRACT

There exists a finite field of order p, namely $\mathbf{Z}_p$, for any prime p. According to Galois, a finite field of order a power of a prime could be constructed if an irreducible polynomial of positive degree over $\mathbf{Z}_p$ could be found. In fact, an irreducible polynomial of positive degree over $\mathbf{Z}_p$ can be found. Thus for any prime p and any positive integer n, a Galois field of order p^n, denoted by GF(p^n), can be constructed. In particular, for some prime p and some positive integer n, there is one and only one Galois field of order p^n. And the number of subfields of Galois field GF(p^n) is the number of positive integers that divide n.