

Finite Fields

♣ **Constructing Finite Fields.** A polynomial $p(x) \in \mathbb{K}[x]$ is said to be *irreducible over $\mathbb{K}[x]$* , if 1 and $p(x)$ are the only divisor of divisors of $p(x)$ in $\mathbb{K}[x]$. An irreducible polynomial over \mathbb{K} of degree n , $n > 1$ is said to be *primitive*, if it is not a divisor of $1+x^m$ for $m < 2^n - 1$. For example, $1+x+x^3$ is primitive, since is not a factor of $1+x^m$ for $m < 2^3 - 1 = 7$. However $1+x+x^2+x^3+x^4$ is irreducible but not primitive since it divides $1+x^5$ and $5 < 2^4 - 1 = 15$.

Let $\mathbb{K}^n[x]$ denotes the set of all polynomials in $\mathbb{K}[x]$ having degree less than n . Of course each word in \mathbb{K}^n corresponds to a polynomial in $\mathbb{K}^n[x]$ so we can define addition and multiplication of words in \mathbb{K}^n . In a field F if $ab = 0$ then $a = 0$ or $b = 0$. So we need to define a multiplication in \mathbb{K}^n which makes it a field. Consider the reducible polynomial $p(x) = 1+x^4$. Now try using multiplication modulo $p(x)$ to define multiplication of words in \mathbb{K}^4 . Note that

$$\begin{aligned} (0101)(0101) &\Leftrightarrow (x+x^3)(x+x^3) = x^2+x^6 \\ &\equiv (x^2+x^2) \pmod{1+x^4} \equiv 0 \Leftrightarrow 0000. \end{aligned}$$

Thus \mathbb{K}^4 cannot be a field under this definition of multiplication.

Now define multiplication of words in \mathbb{K}^4 using multiplication modulo the irreducible polynomial $h(x) = 1+x+x^4$. For the product of the same words, we have

$$\begin{aligned} (0101)(0101) &\Leftrightarrow (x+x^3)(x+x^3) = x^2+x^6 \\ &\equiv (x^3) \pmod{1+x+x^4} \Leftrightarrow 0001. \end{aligned}$$

We state the following Theorem without a proof.

Theorem 1. Let $h(x) \in \mathbb{K}[x]$ be an irreducible polynomial of degree n , where r is a positive integer. The set of all polynomials modulo $h(x)$ is a finite field of order 2^n denoted by $GF(2^n)$ (Galois field).

Let us consider the construction of $GF(2^3)$ using the primitive polynomial $h(x) = 1+x+x^3$ to define the multiplication. We do this by computing $x^i \pmod{h(x)}$:

$x^i \pmod{h(x)}$	Word
1	100
x	010
x^2	001
$x^3 \equiv 1+x$	110
$x^4 \equiv x+x^2$	011
$x^5 \equiv 1+x+x^2$	111
$x^6 \equiv 1+x^2$	101

We will illustrate the above material by actually constructing some finite fields of characteristic 2.

Since $8 = 2^3$, the prime field is $GF(2^3)$ and we need to find an irreducible cubic polynomial over that field. Since the coefficients can only be 0 and 1, the list of irreducible candidates is easily obtained.

$$x^3 + 1, \quad x^3 + x + 1, \quad x^3 + x^2 + 1, \quad x^3 + x^2 + x + 1.$$

Now substituting 0 gives 1 in all cases, and substituting 1 will give 0 only if there are an odd number of x terms, so the irreducible cubics are just $x^3 + x + 1$ and $x^3 + x^2 + 1$. Now the multiplicative group of this field is a cyclic group of order 7 and so every nonidentity element is a generator. Letting β be a root of the first polynomial, we have $\beta^3 + \beta + 1 = 0$, or $\beta^3 = \beta + 1$, so the powers of β are: $\beta^1 = \beta$ $\beta^2 = \beta^2$ $\beta^3 = \beta + 1$ $\beta^4 = \beta^2 + \beta$ $\beta^5 = \beta^2 + \beta + 1$ $\beta^6 = \beta^2 + 1$ $\beta^7 = 1$