The Galois field $GF(2^3)$

Consider the polynomial $p(x) = x^3 + x + 1$.

Let $x = \alpha$ is used to represent the root.

So $\alpha^3 + \alpha + 1 = 0$. —— (1).

The field $GF(2^3)$ can be generated by the newly defined element α given by eqn - 1.

All properties are satisfied with respect to addition and multiplication. We can show this.

$$\left.\begin{array}{l} \alpha + 0 = \alpha \\ \alpha 1 = \alpha \end{array}\right\}$$ 0 and 1 are additive and multiplicative identity elements respectively.

$\alpha + \alpha = 0$, $\alpha = -\alpha$ $\qquad \alpha^{-1} = \frac{1}{\alpha}$.

$\alpha^{-1} \cdot \alpha = 1$.

$$\alpha^3 = \alpha + 1.$$

$$\alpha^4 = \alpha \cdot \alpha^3 = \alpha(\alpha + 1) = \alpha^2 + \alpha.$$

$$\alpha^5 = \alpha\alpha^4 = \alpha(\alpha^2 + \alpha) = \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1$$

$$\alpha^6 = \alpha \cdot \alpha^5 = \alpha(\alpha^2 + \alpha + 1) = \alpha^3 + \alpha^2 + \alpha$$
$$= \alpha + 1 + \alpha^2 + \alpha = 1 + \alpha^2.$$

These are polynomial representation of the elements α^3, α^4, α^5 and α^6. These four elements are differ from each other and from the four elements 0, 1, α, and α^2.

$$\alpha^7 = \alpha\alpha^6 = \alpha(\alpha^2 + 1) = \alpha^3 + \alpha = \alpha + 1 + \alpha = 1.$$

Which is an existing element,

Then $\alpha^8 = \alpha \cdot \alpha^7 = \alpha.$

$\alpha^9 = \alpha \cdot \alpha^8 = \alpha \cdot \alpha = \alpha^2$

$\alpha^{10} = \alpha \cdot \alpha^9 = \alpha \cdot \alpha^2 = \alpha^3$

~~and so forth.~~ $\left(\underline{\text{OR}}\ \alpha^{10 \equiv 3 \bmod 7} \right)$

$\alpha^{12} = \alpha^7 \cdot \alpha^5 = \alpha^5 \quad (12 \equiv 5 \bmod 7)$

and so forth.

Taking into account 0 and 1

we see that we have constructed a set with the 8 elements $0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5$ and α^6.

Along with the operations addition and multiplication the set forms a field, namely $GF(2^3)$.

<u>Note</u>

finite fields are also referred to as <u>Galois fields</u>

The fields are usually expressed as $GF(p^m)$.

Where p is the number of elements in the base field, which is referred to as the field's characteristics and m is the degree of the polynomial whose root is used to construct the field.

The order of the field is given by $q = p^m$.

we can perform the following addition in the element

$$\alpha^3 + \alpha^3 = 1\cdot\alpha^3 + 1\cdot\alpha^3 = \alpha^3(1+1) = 0$$

$$\alpha^4 + \alpha^6 = (\alpha^2+\alpha) + (\alpha^2+1) = \alpha+1 = \alpha^3.$$

Primitive field elements

The non-zero field elements of the Galois fields are generated by taking successive multiples of a single element α.

Field elements that can generate all the non-zero field elements of a field are said to be **primitive elements**:

α is primitive in $GF(2^3)$, $GF(2^4)$ and $GF(2^5)$.

Note: Every Galois field has at least one primitive field element.

Example: In $GF(2^3)$, α^2 is primitive

Let $\beta = \alpha^2$

$$\beta^2 = (\alpha^2)^2 = \alpha^4$$

$$\beta^3 = (\alpha^2)^3 = \alpha^6$$

$$\beta^4 = (\alpha^2)^4 = \alpha^8 = \alpha \quad (\text{Since } \alpha^7 = 1 \text{ in } GF(2^3))$$

$$\beta^5 = (\alpha^2)^5 = \alpha^{10} = \alpha^3 \quad (10 \equiv 3 \bmod 7)$$

$$\beta^6 = (\alpha^2)^6 = \alpha^{12} = \alpha^5. \quad (12 \equiv 5 \bmod 7).$$

These are six different elements.

Next power $\beta^7 = (\alpha^2)^7 = \alpha^{14} = \alpha^7 = 1$

$\beta^8 = \beta = \alpha^2$

$\beta^9 = \beta^2 = \alpha^4$ and so forth.

Hence α^2 can generate the non-zero elements of $GF(2^3)$ and is therefore a primitive field element of $GF(2^3)$.

<u>Note</u>

All elements (other than 0 and 1) of $GF(2^3)$ are primitive and therefore capable of generating the other non-zero elements.

<u>Example</u>: Show that α^5 is a primitive element of $GF(2^3)$.

Let $\beta = \alpha^5$

$\beta^2 = (\alpha^5)^2 = \alpha^{10} = \alpha^3$

$\beta^3 = (\alpha^5)^3 = \alpha^{15} = \alpha$

$\beta^4 = (\alpha^5)^4 = \alpha^{20} = \alpha^6$

$\beta^5 = (\alpha^5)^5 = \alpha^{25} = \alpha^4$

$\beta^6 = (\alpha^5)^6 = \alpha^{30} = \alpha^2$

$\beta^7 = (\alpha^5)^7 = \alpha^{35}$

Irreducible and primitive polynomials

The polynomials x^3+x+1, x^4+x+1 and x^5+x^2+1 used to generate $GF(2^3)$, $GF(2^4)$ and $GF(2^5)$ respectively cannot be factorized. Each polynomial is divisible only by itself and 1, Such polynomials are referred to as irreducible polynomials.

Note: An irreducible polynomial having an primitive field element as a root is called primitive polynomial.

We have ~~[illegible]~~ x^3+x+1, x^4+x+1 and x^5+x^2+1 have primitive element α as a root and therefore the polynomial used to generate $GF(2^3)$, $GF(2^4)$ and $GF(2^5)$ are primitive. ~~polynomial~~.

Scanned with CamScanner