

X Lecture two

sub-groups

A subset of G say H is said to be a sub-group of the Group G if it is a group under the group operation (of Group G).

1) First of all H has to be closed under the operation $*$.

2) Secondly, any element of H should have an inverse with respect to $*$ that is in H .

There is no need for checking other two properties since for $a \in H$ we have its inverse $a' \in H$ and therefore $a * a' = e \in H$ (due to H being closed under $*$).

Also since elements of H are also elements of G , associative property holds automatically.

So we have

Theorem 3: Let G be a group under $*$ and let $H \subseteq G$. The H is a subgroup of G iff:

i) H is closed under $*$

ii) For any $a \in H$, $a' \in H$ where a' is the inverse of a .

Example: The set of integers \mathbb{Z} is a group under $+$ (real addition).

a) set of even numbers is a subgroup of \mathbb{Z} .

b) The set of odd numbers is not a subgroup of \mathbb{Z} .

Definition: Let H be a subgroup of the Group G . Let a be an element of G .

- The set of elements $a * H = \{a * h : h \in H\}$ is called the left Coset of H .

- The set of elements $H * a = \{h * a : h \in H\}$ is the right Coset of H .

If the Group G is commutative (Abelian), then ~~if~~ every left Coset $a * H$ is identical to the right Coset $H * a$. We refer to them as just Cosets.

The importance of the notion of coset is that cosets of a subgroup partition the elements of the original group. That is they divide the elements of the original group into non-overlapping sets. The following theorems show this.

Theorem 4: Let H be a subgroup of a group G with operation $*$. No two elements of a coset of H are identical.

Proof: Consider the coset $a * H = \{a * h : h \in H\}$. Assume that two elements of $a * H$ say $a * h_1$ and $a * h_2$ are identical, where $h_1 \neq h_2$. Let a^{-1} be the inverse of a .

Then:

$$a^{-1} * (a * h_1) = a^{-1} * (a * h_2)$$

or

$$(a^{-1} * a) * h_1 = (a^{-1} * a) * h_2$$

$$e * h_1 = e * h_2 \Rightarrow h_1 = h_2$$

\Rightarrow Contradiction.

Theorem 5: Two different Cosets are disjoint.

That is no two elements in two different Cosets of a subgroup H of the group G are identical.

Proof:

Let $a * H$ and $b * H$ be two different Cosets of H with $a \in G$ and $b \in G$.

Let $a * h_1$ and $b * h_2$ be two elements in $a * H$ and $b * H$, respectively.

Assume that $a * h_1 = b * h_2$.

Denote the inverse of h_1 by h_1^{-1} . Then

$$(a * h_1) * h_1^{-1} = (b * h_2) * h_1^{-1}$$

$$\Rightarrow a * (h_1 * h_1^{-1}) = b * (h_2 * h_1^{-1})$$

$$\Rightarrow a * e = b * h$$

$$\Rightarrow a = b * h_3 \quad \text{where } h_3 = h_2 * h_1^{-1}$$

Now

$$\begin{aligned} a \neq b * h_3 &\Rightarrow a * H = (b * h_3) * H \\ &= \{(b * h_3) * h_4 : h_4 \in H\} \end{aligned}$$

$$= \{b * (h_3 * h_4) : h_3 * h_4 \in H\} = \{b * h_4 : h_4 \in H\}$$

$$= b * H \Rightarrow \text{Contradiction}$$

Theorem 6 (Lagrange's Theorem)

Let G be a finite group of order n and let H be a subgroup of order m .

Then m divides n and the partition G/H consists of $\frac{n}{m}$ Cosets of H .

Proof: Due to Theorem 4, every coset of H consists of m elements of G . Let i be the number of cosets of H . Then we have $n = i \cdot m$.

Therefore m divides n and $i = \frac{n}{m}$.

Fields: A field is a set with two operations. These two operations can be called addition and multiplication. However, they do not need necessarily be identical to real addition and real multiplication as is the case in real field (set of real numbers under normal addition and multiplication).

A field is roughly speaking a set of elements with two operations ~~an~~ such that performing these two operations and their inverse we

do not leave the set. In another word, the set is closed under two operations and their inverse.

Example: the set of real numbers \mathbb{R} under addition (and its inverse subtraction) and multiplication (also division) form a field.

Definition of a field:

Let F be a set of elements. Let two operation "addition" $+$ and "multiplication" \cdot be defined on elements of F .

The set F together with $+$ and \cdot is a field if:

i) F is a commutative (Abelian) group under $+$.

The identity element under $+$ is called "zero element" or "additive identity".

ii) The set of non-zero elements of F form a commutative group under multiplication.

The identity element with respect to \cdot is called "unit element" or "multiplicative element". It is denoted by 1 .

iii) Multiplication is distributive with respect to addition. That is:

for $a, b, c \in F$, we have:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

Properties of fields

Property I:

For every element $a \in F$, we have

$$a \cdot 0 = 0 \cdot a = 0$$

Proof: $a = a \cdot 1 = a \cdot (1 + 0) = a + a \cdot 0$ (add $-a$)
 $-a + a = -a + a + a \cdot 0$ to both sides

$$\Rightarrow 0 = 0 + a \cdot 0$$

$$\Rightarrow a \cdot 0 = 0$$

Property II: for $a \neq 0$ and $b \neq 0$, $a, b \in F$ we have $a \cdot b \neq 0$

Proof: Since ^{the set of} non-zero elements of F is closed under multiplication $a \cdot b \neq 0$.

Property III: $a \cdot b = 0$ and $a \neq 0 \Rightarrow b = 0$

Proof: Direct consequence of II. Since if $b \neq 0$ then $a \cdot b \neq 0$

Property IV: For any two element a and b of F , we have:

$$-(a \cdot b) = (-a) \cdot b = a \cdot (-b)$$

Proof:

$$0 = 0 \cdot b = (a + (-a)) \cdot b = a \cdot b + (-a) \cdot b$$

So $(-a) \cdot b$ is the additive inverse of $a \cdot b$, i.e.,

$$-(a \cdot b) = (-a) \cdot b$$

Similarly, we can show $-(a \cdot b) = a \cdot (-b)$.

Property V:

For $a \neq 0$, $a \cdot b = a \cdot c \Rightarrow b = c$

let multiplication inverse of a be a^{-1} .

Multiply both sides of $a \cdot b = a \cdot c$ by a^{-1}

$$a^{-1} \cdot (a \cdot b) = a^{-1} \cdot (a \cdot c)$$

$$\Rightarrow (a^{-1} \cdot a) \cdot b = (a^{-1} \cdot a) \cdot c$$

$$\Rightarrow 1 \cdot b = 1 \cdot c \Rightarrow b = c$$

Example: Consider the set $\{0, 1\}$ with modulo-2 addition and modulo-2 multiplication

+	0	1
0	0	1
1	1	0

mod-2 +

·	0	1
0	0	0
1	0	1

mod-2 multiplication

This is called the Galois field and is denoted by $GF(2)$.

Example: Let p be a prime. The set $\{0, 1, 2, \dots, p-1\}$ is a commutative group under modulo- p addition.

We also showed that non-zero elements $\{1, 2, \dots, p-1\}$ form a commutative group under multiplication modulo- p .

Using the fact that real multiplication is distributive over real addition, we can easily show that modulo- p multiplication is distributive over modulo- p addition.

So, the set $\{0, 1, \dots, p-1\}$ is a field of order p

under modulo- p multiplication and addition.

It is called a prime field since p is a prime. $GF(2)$ is a special case of prime field for $p=2$.

Some properties of finite fields:

Take the finite field with q elements, say $GF(q)$.

let's add 1 to itself to get the following

sums:

$$\sum_{i=1}^1 1 = 1, \quad \sum_{i=1}^2 1 = 1+1, \quad \sum_{i=1}^3 1 = 1+1+1, \dots$$

$$\sum_{i=1}^k 1 = 1+1+\dots+1 \quad k \text{ times}$$

Since the field is finite, all these sums cannot belong to it and be different. Since the field is closed under $+$, these sums have to belong to $GF(q)$. So, they cannot be all different. So, for

some $m < n$, we should have

$$\sum_{i=1}^m 1 = \sum_{i=1}^n 1 \Rightarrow \sum_{i=1}^{n-m} 1 = 0. \text{ So, there is a}$$

Smallest number λ :

$$\lambda, \text{ so that } \sum_{i=1}^{\lambda} 1 = 0$$

λ is called the characteristic of $GF(q)$.

Theorem 7: The characteristic λ of a finite field is prime.

Proof: assume that λ is not a prime.

So $\lambda = km$ for integers k and m which are smaller than λ .

Since the field is closed under multiplication

$$\left(\sum_{i=1}^k 1\right) \cdot \left(\sum_{i=1}^m 1\right) \in GF(q).$$

From the distributive law, we have

$$\left(\sum_{i=1}^k 1\right) \cdot \left(\sum_{i=1}^m 1\right) = \sum_{i=1}^{km} 1.$$

But since $\sum_{i=1}^{km} 1 = \sum_{i=1}^{\lambda} 1 = 0$

either $\sum_{i=1}^k 1$ or $\sum_{i=1}^m 1$ should be equal to 0.

It contradicts the fact that λ is the smallest number such that $\sum_{i=1}^{\lambda} 1 = 0$.

For any two integers k and $m < \lambda$ we have

$$\sum_{i=1}^k 1 \neq \sum_{i=1}^m 1.$$

This is true since if $\sum_{i=1}^k 1 = \sum_{i=1}^m 1$ then $\sum_{i=1}^{m-k} 1 = 0$

But $m - k < \lambda$ and this contradicts the fact that λ is the characteristic of the field.

So the sums

$$1 = \sum_{i=1}^1 1, \quad \sum_{i=1}^2 1, \quad \sum_{i=1}^3 1, \quad \dots, \quad \sum_{i=1}^{\lambda} 1 = 0$$

are λ distinct elements of $GF(q)$. This set of sums a subset of $GF(q)$ is itself a field under $+$ and \cdot and is denoted by $GF(\lambda)$.

It is a subfield of $GF(q)$.

Therefore, any ^{finite} field of q elements with characteristic λ has a subfield of λ elements. It can be proved that if $q \neq \lambda$ then q is a power of λ .

Now let's see how multiplication works when applied repeatedly.

Take an element of the field say a .

$$a^1 = 1, \quad a^2 = a \cdot a, \quad a^3 = a \cdot a \cdot a, \quad \dots$$

Since $GF(q)$ has a finite number of elements

and also it is closed under multiplication.

These products have to belong to $GF(q)$ and therefore cannot be distinct.

So, there must be some $k < m$ such that

$$a^k = a^m \Rightarrow a^{m-k} = 1$$

So, there must be a smallest number n such that $a^n = 1$. This number, n , is called the order of the field element a .

Now, the products $a^1, a^2, \dots, a^{n-1}, a^n = 1$ are all distinct. They form a field with n elements.

Firstly, it has the unit element 1.

Secondly considering $a^i \cdot a^j = a^{i+j}$ if $i+j < n$

and $i+j = n+r$ if $i+j > n$ for some $r < n$

so $a^i \cdot a^j = a^{n+r} = a^n \cdot a^r = 1 \cdot a^r = a^r \in$ field of n elements.

Also $a^i \cdot a^{n-i} = a^n = 1$ so a^{n-i} is the inverse

of a^i . The properties of associativity and commutativity are inherited from $GF(q)$.

So $a^n = 1$, a^1, a^2, \dots, a^{n-1} form a commutative group under multiplication. A group such as this, i.e., one that has one element whose powers constitute the whole group is called cyclic.

Theorem 8

Let a be a non-zero element of a finite field $GF(q)$ then $a^{q-1} = 1$.

Proof:

Let b_1, b_2, \dots, b_{q-1} be the $q-1$ non-zero elements of $GF(q)$. Multiply each by a

$$a \cdot b_1, a \cdot b_2, \dots, a \cdot b_{q-1}$$

These are non-zero and distinct.

Multiply them to get

$$(a \cdot b_1) \cdot (a \cdot b_2) \cdot \dots \cdot (a \cdot b_{q-1}) = b_1 \cdot b_2 \cdot \dots \cdot b_{q-1}$$

$$\text{or } a^{q-1} \cdot (b_1 \cdot b_2 \cdot \dots \cdot b_{q-1}) = b_1 \cdot b_2 \cdot \dots \cdot b_{q-1}$$

$$\Rightarrow a^{q-1} = 1$$

Theorem 9: Let a be a non-zero element of $GF(q)$. The order of a , say n , divides $q-1$.

Proof: Suppose n does not divide $q-1$.

Then

$$q-1 = k \cdot n + r \quad \text{for some } 0 < r < n$$

$$\text{Then } a^{q-1} = a^{kn+r} = a^{kn} \cdot a^r = (a^n)^k \cdot a^r$$

$$\text{But } a^{q-1} = 1 \text{ and } a^n = 1$$

$$\text{therefore } a^r = 1.$$

This contradicts the assumption that n is the order of a since $r < n$.

~~~~~  
In a finite field  $GF(q)$ , a non-zero element is called primitive if its order is  $q-1$ .

It is clear that powers of a primitive element generates all the non-zero elements of  $GF(q)$ .

Every finite field has a primitive element.

Example : Take  $GF(7)$  with modulo-7 operations :

| + | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 0 |
| 2 | 2 | 3 | 4 | 5 | 6 | 0 | 1 |
| 3 | 3 | 4 | 5 | 6 | 0 | 1 | 2 |
| 4 | 4 | 5 | 6 | 0 | 1 | 2 | 3 |
| 5 | 5 | 6 | 0 | 1 | 2 | 3 | 4 |
| 6 | 6 | 0 | 1 | 2 | 3 | 4 | 5 |

modulo-7  
addition

and

| • | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 0 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 0 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 0 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 0 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 0 | 6 | 5 | 4 | 3 | 2 | 1 |

Take element 3

$$3^1 = 3, \quad 3^2 = 3 \cdot 3 = 2, \quad 3^3 = 6, \quad 3^4 = 4$$

$$3^5 = 5, \quad 3^6 = 1$$

So 3 is a primitive element of  $GF(7)$ .

But take 4

$$4^1 = 4, \quad 4^2 = 4 \cdot 4 = 2, \quad 4^3 = 4 \cdot 4^2 = 1$$

So order of 4 is 3.



## Binary Field:

Recall that we said (showed) that a finite field with  $q$  elements only exists when  $q$  is a prime or it is a power of a prime. So, we have  $GF(q)$  or  $GF(q^m)$

The smallest prime is 2 and we saw that  $GF(2)$  with respect to modulo-2 addition (in digital electronic and logic you may have seen it as exclusive OR; XOR) and modulo-2 multiplication (AND in digital logic) form a field. In fact this is the field that we will be most interested in (also its extended field  $GF(2^m)$ ) in this course.

$GF(2)$  has elements 0 and 1.

Addition is performed modulo-2 that is  $0+1=1$ ,  $1+1=0$  and  $1+1+1=1$  etc.

Any equation relating variables in this field has coefficients 0 or 1. For example

$$X + Y + Z = 1$$

We do not have terms such as  $2X$ ,  $3Y$  etc.

$$\text{since } 2X = X + X = 0$$

$$\text{and } 3Y = Y + Y + Y = Y.$$

### Polynomials over $GF(2)$

Assume that you have a <sup>binary</sup> number  $f = f_n f_{n-1} \dots f_0$

written in a shift register. To find the value of  $f$  in decimal you add  $f_0$  to  $2f_1$ ,  $4f_2$ ,

That is

$$f = f_0 + f_1 \cdot 2 + f_2 \cdot 2^2 + f_3 \cdot 2^3 + \dots + f_n \cdot 2^n.$$

$2$  in fact is the shift operation in shift register.

Replacing  $2$  by a generic variable  $X$ , we get a polynomial in  $X$  with binary coefficients

$$f(X) = f_0 + f_1 X + f_2 X^2 + f_3 X^3 + \dots + f_n X^n$$

The largest power of  $X$  with non-zero coefficient is the degree of the polynomial.

In  $f(X)$  above if  $f_n \neq 0$  then  $f(X)$  has degree  $n$ . If we have  $f_i = 0$ ,  $i \geq 1$  then  $f(X) = f_0$ , i.e., it is a constant <sup>a function</sup> with degree zero.



If  $f_1 \neq 0$ , but  $f_i = 0$  for  $i \geq 2$  then we have a polynomial of degree one:

$$f(x) = f_0 + f_1 x$$

So we have two functions  $x$  and  $1+x$  for 2 we have four functions:

$$x^2, 1+x^2, x+x^2 \text{ and } 1+x+x^2$$

in general we have  $2^n$  functions of degree  $n$  over  $GF(2)$ .

Addition and multiplication of functions:

$$f(x) = f_0 + f_1 x + \dots + f_n x^n$$

can be added to

$$g(x) = g_0 + g_1 x + \dots + g_m x^m \quad m \leq n$$

to get:

$$f(x) + g(x) = (f_0 + g_0) + (f_1 + g_1)x + \dots + (f_m + g_m)x^m + \dots + f_n x^n$$

for example if  $f(x) = 1 + x + x^3 + x^5$  and

$$g(x) = 1 + x^2 + x^3 + x^4 + x^7.$$

Then

$$f(x) + g(x) = x + x^2 + x^4 + x^5 + x^7$$

multiplying  $f(x)$  by  $g(x)$  we get

$$\begin{aligned} f(x) \cdot g(x) &= [f_0 + f_1x + \dots + f_nx^n] \cdot [g_0 + g_1x + \dots + g_mx^m] \\ &= f_0g_0 + (f_1g_0 + g_1f_0)x + (f_2g_0 + f_1g_1 + f_0g_2) + \\ &\quad + \dots + (f_0g_i + f_1g_{i-1} + \dots + f_ig_0)x^i + \dots \\ &\quad + f_ng_nx^{n+m}. \end{aligned}$$

### Properties of polynomial operations over GF(2)

i) Commutativity:

and  $a(x) + b(x) = b(x) + a(x)$

$$a(x) \cdot b(x) = b(x) \cdot a(x)$$

ii) Associativity

$$a(x) + [b(x) + c(x)] = [a(x) + b(x)] + c(x).$$

and

$$a(x) \cdot [b(x) \cdot c(x)] = [a(x) \cdot b(x)] \cdot c(x)$$

iii) Distributivity of  $\cdot$  over  $+$ :

$$a(x) [b(x) + c(x)] = a(x) \cdot b(x) + a(x) \cdot c(x).$$

### Division of polynomials

Dividing  $f(x)$  by  $g(x)$  we either get a remainder zero and say  $g(x)$  divides  $f(x)$  or we get a function  $r(x)$  with degree less than



that of  $g(x)$ . That is

$$f(x) = q(x) \cdot g(x) + r(x)$$

$q(x)$  is called  
the quotient

Let's divide

$$f(x) = 1 + x + x^4 + x^5 + x^6$$

by

$$g(x) = 1 + x + x^3$$

$$\begin{array}{r} x^3 + x^2 \leftarrow q(x) \\ x^3 + x + 1 \overline{) x^6 + x^5 + x^4 + x + 1} \\ \underline{x^6 + x^4 + x^3} \phantom{+ 1} \\ x^5 + x^3 + x + 1 \\ \underline{x^5 + x^3 + x^2} \\ x^2 + x + 1 \leftarrow r(x) \end{array}$$

So

$$x^6 + x^5 + x^4 + x + 1 = (x^3 + x^2)(x^3 + x + 1) + x^2 + x + 1.$$

Now let's divide  $f(x) = x^4 + x^3 + x^2 + 1$

by  $x+1$ .

What do you expect to get as remainder?

Let's see:

$$\begin{array}{r} x^3 + x + 1 \\ x+1 \overline{) x^4 + x^3 + x^2 + 1} \\ \underline{x^4 + x^3} \phantom{+ 1} \\ x^2 + 1 \\ \underline{x^2 + x} \\ x + 1 \\ \underline{x + 1} \\ 2 - 2 \end{array}$$

Could we have found out that  $f(x)$  is divisible by  $x+1$  without doing the division?

Note that  $x+1=0 \Rightarrow x=-1$

Now let  $x=-1$  in  $f(x)$

$$f(-1) = 1 + 1^2 + 1^3 + 1^4 = 1 + 1 + 1 + 1 = 0$$

So  $x=-1$  is a root of  $f(x)$  so it is divisible by  $x+1$ .

### Definition

A polynomial is called irreducible if it is not divisible by any polynomial.

If the degree of  $f(x)$  is  $n$ , we only need to check those <sup>with degrees</sup>  $x^k$  in the range of 1 to  $n-1$ , i.e.,  $0 < k < n$ .

Take the polynomials of degree 2, i.e.,

$$x^2, x^2+1, x^2+x \text{ and } x^2+x+1$$

Only the last function  $x^2+x+1$  is irreducible.

The others have roots 1 or 0 and, therefore, are divisible by  $x$  or  $1+x$ .

For  $f(x) = x^2+x+1$ ,  $f(0) = f(1) = 1$  so it is not divisible by  $x$  and  $1+x$ .

Theorem 10: Any irreducible polynomial of degree  $m$  divides  $X^{2^m-1} + 1$ .

Example: The polynomial  $f(X) = X^3 + X + 1$  is irreducible since

$f(0) = f(1) = 1$  so it is not divisible by  $X$  and  $1+X$ . Note that we do not check for polynomials of degree 2 (why?).

According to theorem 10,  $X^3 + X + 1$  should divide  $X^{2^3-1} + 1 = X^7 + 1$ . Let's verify:

$$\begin{array}{r} X^4 + X^2 + X + 1 \\ X^3 + X + 1 \overline{) X^7 + 1} \\ \underline{X^4 + X^5 + X^4} \phantom{+ 1} \\ X^3 + X^4 + 1 \\ \underline{X^5 + X^3 + X^2} \phantom{+ 1} \\ X^4 + X^3 + X^2 + 1 \\ \underline{X^4 + X^2 + X} \phantom{+ 1} \\ X^3 + X + 1 \\ \underline{X^3 + X + 1} \\ 0 \end{array} \quad \checkmark$$



Definition: An irreducible polynomial  $p(x)$  of degree  $m$  is called primitive if the smallest positive integer  $n$  for which  $p(x)$  divides  $x^n + 1$  is  $n = 2^m - 1$ .

Example: Recall the example of  $f(x) = x^2 + x + 1$  degree 2. We showed that it is irreducible. We can see that the smallest  $n$  for which  $f(x)$  divides  $x^n + 1$  is  $n = 2^m - 1 = 2^2 - 1 = 3$ .

So  $f(x) = x^2 + x + 1$  is a primitive polynomial.

$GF(4)$  or  $GF(2^2)$  field.

We said that if  $q$  is a prime or power of a prime, then we can have a field  $GF(q)$ .

It is obvious that we cannot form a field over integers  $0, 1, 2, 3$  with modulo-4 addition and multiplication due to the fact that 4 is not a prime and  $1, 2, 3$  cannot form a group under modulo-4 multiplication.

So, we choose elements of  $GF(4)$  as polynomials. Since the field will have only 3 non-zero elements, if we take an element  $\alpha$  of it and form:

$$\alpha^0 = 1, \alpha^1 = \alpha, \alpha^2 = \alpha \cdot \alpha, \alpha^3 = \alpha \cdot \alpha^2, \dots$$

So all these powers of  $\alpha$  have to collapse into 3. This means that  $\alpha^3 = \alpha \cdot \alpha^2$  has to be one of the non-zero elements  $1, \alpha, \alpha^2$ .

Letting  $\alpha^3 = \alpha \cdot \alpha^2 = \alpha \Rightarrow \alpha^2 = 1 \Rightarrow$  not even 3 distinct elements  
and  
 $\alpha^3 = \alpha \cdot \alpha^2 = \alpha^2 \Rightarrow \alpha = 1 \Rightarrow$  not a solution either

$$\text{Letting } \alpha^3 = \alpha \cdot \alpha^2 = 1 \Rightarrow \alpha^2 = \alpha^{-1}$$

So, we have the Field:

$$GF(2^2) = \{0, 1, \alpha, \alpha^{-1}\} = \{0, 1, \alpha, \alpha^2\}$$

$\alpha^2 = \alpha^{-1}$  needs to be the sum (modulo addition) of two other members  $0+0=0, 0+1=1, 0+\alpha=\alpha$   
 $1+1=0, 1+\alpha$ . Among these only  $1+\alpha$  is different from the first three elements of  $0, 1, \alpha$ . So we

$$\text{write } GF(2^2) = \{0, 1, \alpha, 1+\alpha\}$$



That is  $\alpha^2 = \alpha + 1$  or  $\alpha^2 + \alpha + 1 = 0$

Important observation:

Recall that  $p(x) = x^2 + x + 1$  is a primitive polynomial. In fact we have used this polynomial to generate  $GF(4)$ . The procedure is as follows:

write  $p(\alpha) = \alpha^2 + \alpha + 1 = 0$

and get  $\boxed{\alpha^2 = \alpha + 1}$ .

Use this to generate:

$$\alpha^0 = 1$$

$$\alpha^1 = \alpha$$

$$\alpha^2 = 1 + \alpha$$

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

etc.

---

$GF(4)$  is very important in Quantum Physics and Quantum Coding as they represent four Pauli Matrices  $\sigma_0, \sigma_1, \sigma_2, \sigma_3$  or  $I, X, Y, Z$ .



| $m$ |                              | $m$ |                                 |
|-----|------------------------------|-----|---------------------------------|
| 3   | $1 + X + X^3$                | 14  | $1 + X + X^6 + X^{10} + X^{14}$ |
| 4   | $1 + X + X^4$                | 15  | $1 + X + X^{15}$                |
| 5   | $1 + X^2 + X^5$              | 16  | $1 + X + X^3 + X^{12} + X^{16}$ |
| 6   | $1 + X + X^6$                | 17  | $1 + X^3 + X^{17}$              |
| 7   | $1 + X^3 + X^7$              | 18  | $1 + X^7 + X^{18}$              |
| 8   | $1 + X^2 + X^3 + X^4 + X^8$  | 19  | $1 + X + X^2 + X^5 + X^{19}$    |
| 9   | $1 + X^4 + X^9$              | 20  | $1 + X^3 + X^{20}$              |
| 10  | $1 + X^3 + X^{10}$           | 21  | $1 + X^2 + X^{21}$              |
| 11  | $1 + X^2 + X^{11}$           | 22  | $1 + X + X^{22}$                |
| 12  | $1 + X + X^4 + X^6 + X^{12}$ | 23  | $1 + X^5 + X^{23}$              |
| 13  | $1 + X + X^3 + X^4 + X^{13}$ | 24  | $1 + X + X^2 + X^7 + X^{24}$    |

List of some primitive polynomials

A useful property of polynomials over  $GF(2)$

$$f^2(x) = f(x^2)$$

That is if  $f(x) = f_0 + f_1x + f_2x^2 + \dots + f_nx^n$

then

$$f^2(x) = f_0 + f_1x^2 + f_2x^4 + \dots + f_nx^{2n}$$

Proof:

$$\text{for } n=0 \Rightarrow f(x) = f_0 \Rightarrow f^2(x) = f_0 \cdot f_0 = f_0$$

$$\text{and } f(x^2) = f_0 \Rightarrow f^2(x) = f(x^2)$$

induction step: if

$$f^2(x) = f(x^2) \text{ for}$$

$$f(x) = f_0 + f_1x + \dots + f_kx^k$$

then it is

$$\text{true for } g(x) = f_0 + f_1x + \dots + f_kx^k + f_{k+1}x^{k+1}$$

$$g^2(x) = [f(x) + f_{k+1}x^{k+1}]^2$$

$$\begin{aligned}
 g^2(x) &= f^2(x) + f(x)f_{k+1}x^{k+1} + f(x)f_{k+1}x^{k+1} \\
 &\quad + f_{k+1}^2 x^{2(k+1)} \\
 &= f^2(x) + f_{k+1} \cdot x^{2(k+1)} \\
 &= g(x^2).
 \end{aligned}$$

So, since the property is true for  $n=0$  it is true for  $n=1$  and since it is true for  $n=1$ , it is true for  $n=2$  and so on.

### Constructing $GF(2^m)$

We saw earlier how to form  $GF(4) = GF(2^2)$ .

We start with an element  $\alpha$  and form

$$\alpha^0 = 1, \alpha^1 = \alpha, \alpha^2 = \alpha \cdot \alpha, \alpha^3 = \alpha \cdot \alpha^2, \dots$$

So, we will have the set

$$F = \{0, 1, \alpha, \alpha^2, \dots, \alpha^j, \dots\}$$

However, we need to collapse the set somehow to have only  $2^m$  distinct elements.

Take a primitive polynomial  $p(x)$  and let  $p(\alpha) = 0$ . That is let  $\alpha$  be a root of  $p(x)$ . We know that  $p(x)$  divides  $X^{2^m-1} + 1$ . So:

$$X^{2^m-1} + 1 = q(x)p(x)$$

Let  $x = \alpha$  to get  $\alpha^{2^m - 1} + 1 = q(\alpha)p(\alpha)$

Since  $p(\alpha) = 0$  we have  $\alpha^{2^m - 1} + 1 = 0$

or  $\alpha^{2^m - 1} = 1$

So, the field will have elements

$$0, 1, \alpha, \alpha^2, \dots, \alpha^{2^m - 2}.$$

So  $GF(2^m) = \{0, 1, \alpha, \alpha^2, \dots, \alpha^{2^m - 2}\}$

Example:  $GF(2^4)$

We use the primitive polynomial

$$p(x) = 1 + x + x^4$$

letting  $p(\alpha) = 1 + \alpha + \alpha^4 = 0$  we get  $\alpha^4 = \alpha + 1$ .

Three representations for the elements of  $GF(2^4)$  generated by  $p(X) = 1 + X + X^4$ .

| Power representation | Polynomial representation          | 4-Tuple representation |
|----------------------|------------------------------------|------------------------|
| 0                    | 0                                  | (0000)                 |
| 1                    | 1                                  | (1000)                 |
| $\alpha$             | $\alpha$                           | (0100)                 |
| $\alpha^2$           | $\alpha^2$                         | (0010)                 |
| $\alpha^3$           | $\alpha^3$                         | (0001)                 |
| $\alpha^4$           | $1 + \alpha$                       | (1100)                 |
| $\alpha^5$           | $\alpha + \alpha^2$                | (0110)                 |
| $\alpha^6$           | $\alpha^2 + \alpha^3$              | (0011)                 |
| $\alpha^7$           | $1 + \alpha + \alpha^3$            | (1101)                 |
| $\alpha^8$           | $1 + \alpha^2$                     | (1010)                 |
| $\alpha^9$           | $\alpha + \alpha^3$                | (0101)                 |
| $\alpha^{10}$        | $1 + \alpha + \alpha^2$            | (1110)                 |
| $\alpha^{11}$        | $\alpha + \alpha^2 + \alpha^3$     | (0111)                 |
| $\alpha^{12}$        | $1 + \alpha + \alpha^2 + \alpha^3$ | (1111)                 |
| $\alpha^{13}$        | $1 + \alpha^2 + \alpha^3$          | (1011)                 |
| $\alpha^{14}$        | $1 + \alpha^3$                     | (1001)                 |



The usefulness of having both polynomial and power representation is that we can use polynomial representation to do modulo-2 addition of bits of a symbol and the power representation performing multiplication using a log and an anti-log table to get the result.