

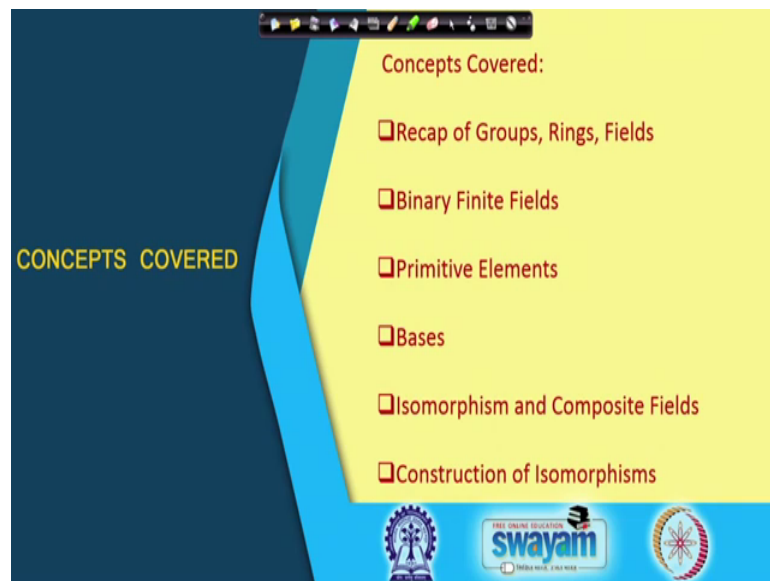
**Hardware Security**  
**Prof. Debdeep Mukhopadhyay**  
**Department of Computer Science and Engineering**  
**Indian Institute of Technology, Kharagpur**

**Lecture – 10**  
**Field Isomorphisms**

[noise]

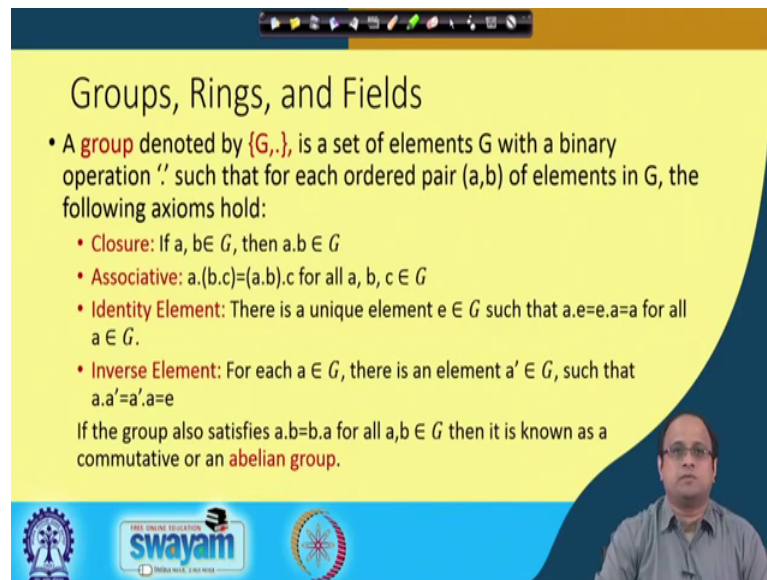
So, welcome to this class on Hardware Security, today we shall be discussing on the topic which is called as Field Isomorphisms, which is a very important mathematical tool to develop efficient architectures for finite fields which we can apply for realizing efficient architectures for a subsequently for AES kind of ciphers.

(Refer Slide Time: 00:35)



So, the concepts that I shall be trying to covered in today's class or I shall be starting to cover in today's class is we shall take a recap on groups rings and fields, we shall be discussing about binary finite fields we shall be discussing about the concept which is called as primitive elements. And then define what are called as basis of fields and then finally discuss about Isomorphisms and composite fields and try to construct Isomorphisms.

(Refer Slide Time: 01:01)



**Groups, Rings, and Fields**

- A **group** denoted by  $\{G, \cdot\}$ , is a set of elements  $G$  with a binary operation  $\cdot$  such that for each ordered pair  $(a, b)$  of elements in  $G$ , the following axioms hold:
  - **Closure:** If  $a, b \in G$ , then  $a \cdot b \in G$
  - **Associative:**  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$  for all  $a, b, c \in G$
  - **Identity Element:** There is a unique element  $e \in G$  such that  $a \cdot e = e \cdot a = a$  for all  $a \in G$ .
  - **Inverse Element:** For each  $a \in G$ , there is an element  $a' \in G$ , such that  $a \cdot a' = a' \cdot a = e$

If the group also satisfies  $a \cdot b = b \cdot a$  for all  $a, b \in G$  then it is known as a commutative or an **abelian group**.

So, to start with here is a quick recap on what are called as mathematical groups. So, as we know that mathematical groups are defined by an operator or a binary operator say it denoted it as dot, such that if I take any two ordered pairs  $a$  and  $b$  which belongs to  $G$  then the following axioms holds.

The first is closure that means, if I take two elements  $a$  and  $b$  in  $G$  apply the operator than the result is also in the group in associative, which means I can do either  $a \cdot b \cdot c$  there I can do either  $b \cdot c$  first or if I do  $a \cdot b$  first the results are same ok, so that is you can do it in anyway. The 2nd the 3rd properties identity element which means that there must be a unique element  $e$  which belongs also to the group, such that if I take  $a$  which is an another element in the group and then I apply the identity element either on the right or on the left I still get back the original element which is  $a$ .

That means  $a \cdot e$  is equal to  $e \cdot a$  which is equal to  $a$  for all  $a$  which belongs to  $G$ . Likewise you also need to have an inverse element which means that for any element  $a$  with belongs to  $G$  there must be an element  $a'$  which also belongs to  $G$ , such that  $a \cdot a'$  is equal to  $a' \cdot a$  which is equal to the identity element. If the group also satisfies commutativity which means that I can do  $a \cdot b$  or  $b \cdot a$  for all  $a, b$  which belongs to  $G$  then it is called as a commutative group or often called as a Abelian group.

(Refer Slide Time: 02:31)

The slide is titled "Groups, Rings, and Fields (contd.)" and contains the following text:

- A ring denoted by  $\{R, +, \cdot\}$ , is a set of elements  $R$  with **two** binary operations '+, ·' such that for all  $a, b, c \in R$  the following axioms hold
  - $R$  is an **abelian group** under **addition**.
  - The **closure property** of  $R$  is satisfied under **multiplication**.
  - The **associativity property** of  $R$  is satisfied under **multiplication**.
  - There exists a **multiplicative identity** element denoted by  $1$  such that for every  $a \in R$ ,  $a \cdot 1 = 1 \cdot a = a$ .
  - **Distributive Law**: For all  $a, b, c \in R$ ,  $a \cdot (b+c) = a \cdot b + a \cdot c$  and  $(a+b) \cdot c = a \cdot c + b \cdot c$
- The set of integers, real numbers, rational numbers, and complex numbers are all rings.
- A ring is said to be **commutative** if the commutative property under multiplication holds. That is, for all  $a, b \in R$ ,  $a \cdot b = b \cdot a$

The slide also features a video feed of a presenter in the bottom right corner and logos for "THE ONLINE EDUCATION swayam" and "INDIA WISE, LEAD WISE" at the bottom.

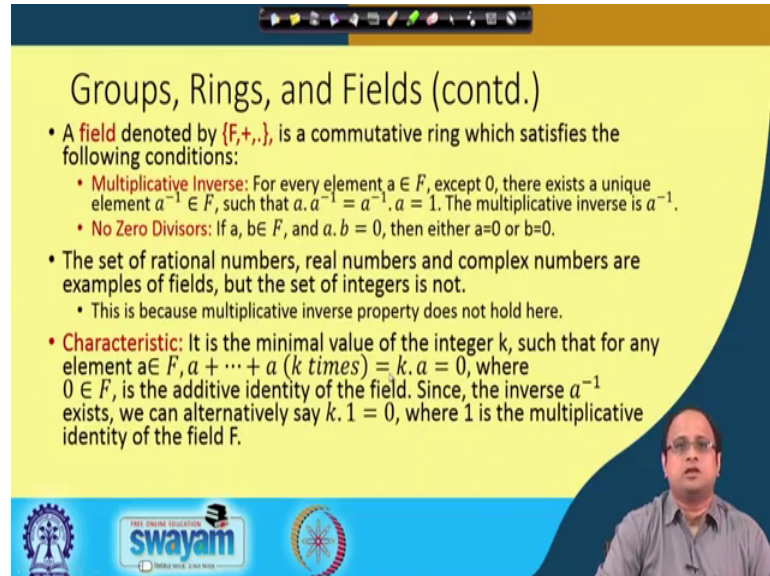
So, you can extend a group to agreeing by bringing another operator along with the so now you have got 2 operators say plus and dot often the 1st plus is called as the addition, where the 2nd one is called thought to be like something like a multiplication or product. So, such that the so again you know like few axioms has to have to hold.

For example for all  $a, b, c$  now which belongs to  $R$  that is the ring the following properties hold the first is that  $R$  has to be an Abelian group under addition. Then with respect to multiplication or the dot operator the closure property of  $R$  has to be satisfied. The associativity property of  $R$  is also satisfied under multiplication, there exist a multiplicative identity element denoted by  $1$  such that for all  $a$  which belongs to  $R$ , again I can do  $a \cdot 1$  or  $1 \cdot a$  I get back again I get back  $a$ . There is another law which also needs to be satisfied which is called as a distributive law, which means like now if I have got three elements which belongs to  $R$  then  $a \cdot (b + c)$  essential is equal to  $a \cdot b + a \cdot c$  which means multiplication distributes over addition.

Likewise you can also do  $a + b \cdot c$  and you will have  $a + c \cdot b + b \cdot c$ . So, therefore, you know in the several examples of rings for example, the set of integers real numbers, rational numbers, complex numbers are all examples of rings. So, ring is also again you know like a similar way like in the groups you said to be commutative, if the commutative property under multiplication holds; that means, for all  $a, b$  which belongs

to  $R$  we have got  $a \cdot b$  is equal to  $b \cdot a$ . So therefore, it is called it is a is an example of a commutative ring.

(Refer Slide Time: 04:23)



**Groups, Rings, and Fields (contd.)**

- A **field** denoted by  $(F, +, \cdot)$ , is a commutative ring which satisfies the following conditions:
  - **Multiplicative Inverse:** For every element  $a \in F$ , except 0, there exists a unique element  $a^{-1} \in F$ , such that  $a \cdot a^{-1} = a^{-1} \cdot a = 1$ . The multiplicative inverse is  $a^{-1}$ .
  - **No Zero Divisors:** If  $a, b \in F$ , and  $a \cdot b = 0$ , then either  $a=0$  or  $b=0$ .
- The set of rational numbers, real numbers and complex numbers are examples of fields, but the set of integers is not.
  - This is because multiplicative inverse property does not hold here.
- **Characteristic:** It is the minimal value of the integer  $k$ , such that for any element  $a \in F$ ,  $a + \dots + a$  ( $k$  times)  $= k \cdot a = 0$ , where  $0 \in F$ , is the additive identity of the field. Since, the inverse  $a^{-1}$  exists, we can alternatively say  $k \cdot 1 = 0$ , where 1 is the multiplicative identity of the field  $F$ .

Then we have got something which is called as field, so a field is denoted as  $F$  plus dot again you have got 2 operators and it so it is called a field. So, we extend the concept of groups to rings and then rings to fields. So, what is a field? So, field is a commutative ring with satisfies the following conditions. So, it of course, satisfies the properties of what are called as commutative ring as we have seen in the previous slide, but we extend it with some more some more conditions. For example, if you remember in the last definition we did not say that every element must have a multiplicative inverse.

So, now we bringing that notion where we say that for all elements  $a$  which belongs to  $F$  except 0; that means, for all non 0 elements of  $a$  of  $F$  there exist a unique element  $a$  inverse such that  $a$  into  $a$  inverse is equal to  $a$  inverse into  $a$  is equal to the multiplicative identity or 1. Now, the multiplicative inverse is denoted as  $a$  to the power minus 1, so essentially it says that all non 0 elements have multiplicative inverses. And it also has got no 0 devices, which means that if I have got elements  $a$  and  $b$  which belongs to  $F$  and if I have got the result  $a \cdot b$  equal to 0. Then either  $a$  is equal to 0 or  $b$  equal to 0; which means that 2 non zero elements in the field should not multiply to get 0 this is an important condition for it to be a field.

So, the set of rational numbers real numbers and complex numbers you can easily understand are now not examples of I mean not examples of fields, but the set of integers is not an example of field why? Because, multiplicative inverse property with now not hold you can easily see that suppose 5 is an integer and if I say like 1 by 5 is an is an inverse of it, for example but 1 by 5 is not an integer ok. So, therefore, it does not have any multiplicative inverse in the set of integers. There is another very important notion which we already have kind of discussed in the previous classes which is called as characteristic of a field.

Now, what is the characteristic? Now, it is a minimum value of the integer  $k$ , such that if I take an element  $a$  for example and I have  $a$  add  $a$  say  $k$  times I get  $k \cdot a$  which is equal to 0. So therefore, it is a minimum number of times I add an element  $a$  in the field to get 0 is called as the characteristic of the field. Now, you can easily understand there if it is a field and if  $a$  is a non zero element the  $a$  inverse also exists. And therefore you can also synonymously say that it is the minimum number of times I add one to get 0, that means  $k$  into 1 is equal to 0. So, there 1 is of course the multiplicative identity of the field  $F$ .

(Refer Slide Time: 07:19)

The slide is titled "GF(2): An Efficient Galois Field" and contains the following bullet points:

- Elements are  $\{0,1\}$ .
- Most computing systems are built on binary number systems.
- A single bit can be used to represent an element in  $GF(2)$ 
  - Compare it with that required for  $GF(3)$ .
- Addition in  $GF(2)$  can be realized by only XORs.
- Extension fields for  $GF(2)$  are denoted as  $GF(2^m)$  and also lead to efficient arithmetic operations.

The slide also features a video feed of a presenter in the bottom right corner and logos for "swayam" and "THE ONLINE EDUCATION" at the bottom.

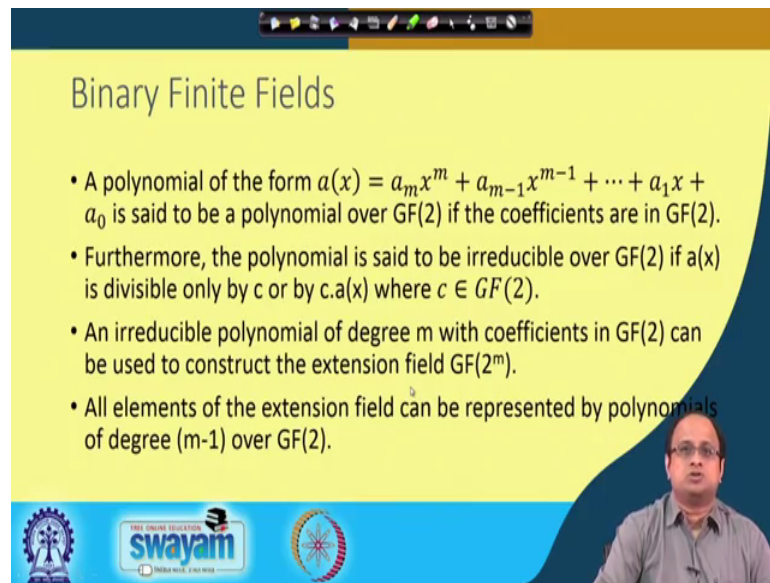
So, we have seen several examples of characteristic 3 fields characteristic 2 fields. So, in particular as we have discussed previously characteristic 2 fields are efficient, because of the you know lye a fact that it gives rise to you know like compact and efficient

architectures. So, in GF 2 which is essentially the smallest field in the you know like in 0 1 domain the elements are only 0 and 1. So, we have got either 0 and 1 as elements in this field and it actually gives rise to very compact systems because, you know most computing systems are built on binary number systems. So, it is very suited for our computing platforms.

In particular you can you know think about that a single bit can be used to represent an element in GF 2 and for example if you compare it with GF 3 you will see that GF 3 you will have elements 0 1 and 2, but is you can easily think of that for to realize these three elements you need 2 bits. So therefore, you are basically having provision for four elements but you are only using three elements. On the other hand write the utilization in GF 2 is very compact because, you have got a single bit to represent an element in GF 2 and you know that you can have two elements represented in GF 2 and you have exactly two elements in GF 2.

So therefore, you are not wasting any storage or wasting any space. So therefore, right GF 2 seems to be very efficient and indeed as we have discussed previously as well that their the operations. For example the addition is very easy in GF 2 there was no carry ok. So, the addition in GF 2 can be realize by only XOR or exclusive or and also like you can also extend GF 2 to something which is called as an extension field which is denoted as GF 2 power of m, which also leads to efficient arithmetic operations like as we have seen square rings and inverters and multiplications which we have pretty efficiently implemented.

(Refer Slide Time: 09:19)



**Binary Finite Fields**

- A polynomial of the form  $a(x) = a_mx^m + a_{m-1}x^{m-1} + \dots + a_1x + a_0$  is said to be a polynomial over  $GF(2)$  if the coefficients are in  $GF(2)$ .
- Furthermore, the polynomial is said to be irreducible over  $GF(2)$  if  $a(x)$  is divisible only by  $c$  or by  $c \cdot a(x)$  where  $c \in GF(2)$ .
- An irreducible polynomial of degree  $m$  with coefficients in  $GF(2)$  can be used to construct the extension field  $GF(2^m)$ .
- All elements of the extension field can be represented by polynomials of degree  $(m-1)$  over  $GF(2)$ .

THE ONLINE EDUCATION SWAYAM

So therefore, this brings us to this concept of binary finite fields. So, a binary finite field can be represented as a polynomial  $a(x)$ , where I have got say you know like the degree as  $x$  power of  $m$  the degree is  $m$  till say a constant term  $a_0$ , such that all the coefficients here are belonging to  $GF(2)$  which means they are either 0 or they are either 1. So, further more this polynomial is said to be irreducible over  $GF(2)$ , if  $a(x)$  is divisible by  $c$  or by  $c \cdot a(x)$ . That means, so where  $c$  is of course, like a constant which belongs to  $GF(2)$  so that means, you do not have any non trivial factors of the polynomial which belongs to this field.

So, an irreducible polynomial of degree  $m$  with coefficient in  $GF(2)$ , so now if you have got such an irreducible suppose this polynomial is irreducible which means like you cannot have such kind of trivial factors. So, you I mean you cannot have trivial factors for this polynomial  $a(x)$ , so then it qualifies as an irreducible polynomial. So, what do we do is you take the ring of polynomials, that means all polynomials possible in  $GF(2)[x]$  that means, all essentially it simply put it just means that I will take all possible polynomials whose coefficients are in  $GF(2)$  and then I will divide it or rather I will take the remainder after I divide that polynomial with this irreducible polynomial.

So, you can easily understand that if the degree of this polynomial is  $m$  then the degree of the remainder will be maximum  $m - 1$ . So, therefore, write any remainder with that I get or any modular that I get any modular polynomial that I get have got a

maximum degree of  $m$  minus 1. So therefore, the number of elements which I need to represent that module  $e$  is ranging from 0 to  $m$  minus 1. So, there are  $m$  bits and you essentially have got 2 to the power of  $m$  such possibilities, so that means like you can represent all elements in  $GF 2$  to the power of  $m$  using that representation.

So, essentially this is an this is this particular extension is what is called as an extension field or any means of the extension field therefore can be represented by a polynomial of degree  $m$  minus 1 over  $GF 2$  and this way we construct the extension field  $GF 2$  to the power of  $m$ .

(Refer Slide Time: 11:53)

Example  $GF(2^4)$

- Irreducible Polynomial:  $x^4+x+1$
- Generator:  $x$
- Elements:
  - 1:  $x$ , 2:  $x^2$ , 3:  $x^3$ , 4:  $x^4 = x + 1$ , 5:  $x^2 + x$ , 6:  $x^3 + x^2$ , 7:  $x^4 + x^3 = x + 1 + x^3$ , 8:  $x^2 + x + x^4 = x^2 + x + x + 1 = x^2 + 1$ , 9:  $x^3 + x$ , 10:  $x^4 + x^2 = x^2 + x + 1$ , 11:  $x^3 + x^2 + x$ , 12:  $x^4 + x^3 + x^2 = x + 1 + x^3 + x^2 = x^3 + x^2 + 1$ , 13:  $x^2 + x + x^4 + x^3 = x^2 + x + x + 1 + x^3 = x^3 + x^2 + 1$ , 14:  $x^4 + x^3 + x = x^3 + 1$ , 15:  $x^4 + x = 1$

So, now let us see an example so in particular I shall be constructing this field  $GF 2$  to the power of 4 which is an extension of  $GF 2$ . So, the irreducible polynomial that I used for this purpose is  $x$  to the power of 4 plus  $x$  plus 1, note that there can be more than 1 irreducible polynomial and I just choose one of them.

So, I choose some element which is called as a generator  $x$  which is also you know like you can think of the definition of a generator by being an element in the field, which if you raise to its powers it can actually generate all the non 0 elements in the field ok. So, note that it is not you cannot generate 0 out of this you can generate all the non 0 elements from  $x$ .



So, what I do is I calculate  $x$  x power of 1 x power of 2 x power of 3 and so on till x power of 15 to get back 1. So, after x power of fifteen I will again get x and the process and there pattern will repeat. So, basically what I have done is that in GF 2 to the power of 4 there are 15 nonzero elements there is one which element which is 0, but all this 15 nonzero elements can be now generated by only x and by reducing it by x power of 4 plus x plus one whenever the degree exceeds 4.

So, let us see the process suppose I start with x I then calculate x squared then I calculate x cube and then when I calculate x power of 4 as I said as I have to reduce this. So, how do I reduce it I substitute this x power of 4 plus x plus 1 as 0 which means x power of 4 is equivalent to x plus 1. So therefore, I replace x power of 4 by x plus 1, then I again multiply this with x square get x squared plus x and then I get x cube plus x squared then I get x power of 4 plus x squared x power of 4 is again replaced by x plus 1, so I get x squared plus x plus 1. And if I repeat this process in this fashion you will see that finally the 15 position I will get x to the power of 4 plus x which is nothing but 1. So therefore, write I will the process will repeat after this and again I will have x x squared x cube and so on ok.

So, therefore, I this x or this polynomial x serves as a generator and as we, we shall see subsequently this is also called as a primitive element in this field.

(Refer Slide Time: 14:15)

The slide is titled "Primitive Element of a Field" and contains the following text:

- Consider the field  $GF(2^n)$ .
- There is an element  $\alpha$  such that every non-zero element can be written in terms of the form of  $\alpha^k$ .
- This element is called the generator or **primitive element** of the group.
- A **primitive polynomial** is the monic polynomial of minimum degree such that the primitive element is a root.
- A primitive polynomial is always irreducible but not vice-versa.
- Over  $GF(2^n)$ , there are  $\phi(2^n - 1)/n$  primitive polynomials, where  $\phi$  is the Euler's Totient function.

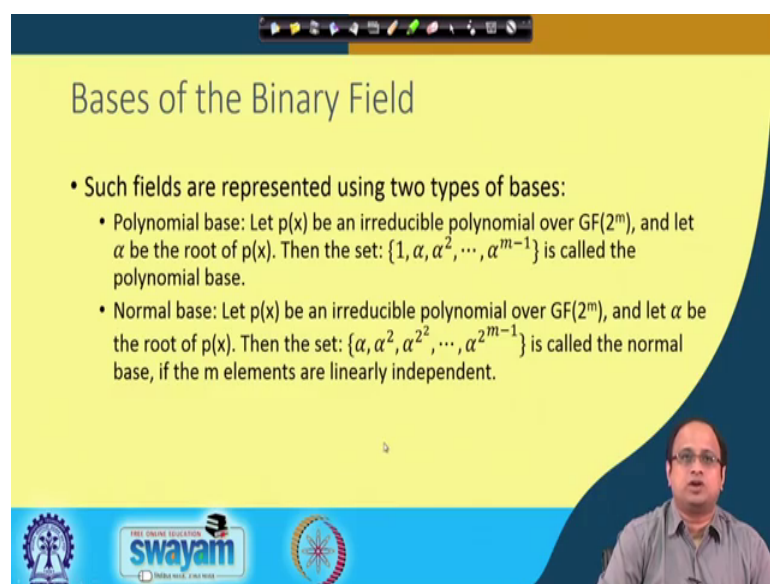
The slide also features a video inset of a man speaking in the bottom right corner and logos for "swayam" and "MHRD" at the bottom.

So, that essentially brings us to the primitive element of the field, so in general if in a more general setting if you considered the field  $GF(2^n)$  there is an element  $\alpha$ , such that for every nonzero element  $\beta$  there is a nonzero element  $k$  such that  $\beta = \alpha^k$ . This element is called the generator or the primitive element of the field.

Now, there is a concept of a special class of polynomial which is called as the primitive polynomial. So, what is a primitive polynomial? A primitive polynomial is a monic polynomial of minimum degree such that the primitive element is a root of the polynomial. This primitive element that we have been talking about is a root of this polynomial. So, it is the minimum degree monic polynomial where the primitive element is a root, interestingly a primitive element is always irreducible but not vice versa.

Over  $GF(2^n)$  there are  $\phi(2^n - 1)$  primitive polynomials possible, where  $\phi$  is the Euler Totient function. So, there are more than one primitive polynomials possible. If I take this polynomial and I equate to 0 then I will get elements which belong to the extension field and I roots of this polynomials. So, those elements which are roots are those roots essentially are primitive elements of this field ok.

(Refer Slide Time: 15:51)



The slide is titled "Bases of the Binary Field" and contains the following text:

- Such fields are represented using two types of bases:
  - Polynomial base: Let  $p(x)$  be an irreducible polynomial over  $GF(2^m)$ , and let  $\alpha$  be the root of  $p(x)$ . Then the set:  $\{1, \alpha, \alpha^2, \dots, \alpha^{m-1}\}$  is called the polynomial base.
  - Normal base: Let  $p(x)$  be an irreducible polynomial over  $GF(2^m)$ , and let  $\alpha$  be the root of  $p(x)$ . Then the set:  $\{\alpha, \alpha^2, \alpha^{2^2}, \dots, \alpha^{2^{m-1}}\}$  is called the normal base, if the  $m$  elements are linearly independent.

The slide also features a presenter in the bottom right corner and logos for Swamyam and other educational institutions at the bottom.

So, with this background right we essentially can start to look into the fields in much more you know like in much more details. So, how to explain how do we express the elements in the in the field, there are two important ways or two important ways in which you can do that actually; one is what is called as polynomial bases and the other one is what are called as normal bases.

So, in polynomial bases you again start with an irreducible polynomial again as we have been discussing that if I want to extend  $GF(2)$  to  $GF(2^n)$ , then I have to use an irreducible polynomial. So, I suppose you know like  $p(x)$  is an irreducible polynomial and let  $\alpha$  be the root of  $p(x)$  ok. So, in particular write what I will do is that I will then generate or rather I will write my polynomial base as  $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ . So, this becomes the you know like what is called as a polynomial bases, which means I can express any element in this field using linear combinations of these components.

Likewise there is also normal bases which is essentially again starting from  $p(x)$  which is an irreducible polynomial over  $GF(2)$  to the power of  $m$  and let again  $\alpha$  be the root of  $p(x)$  then the set  $\alpha, \alpha^2, \alpha^4, \dots, \alpha^{2^{m-1}}$ . Likewise  $\alpha^{2^0}, \alpha^{2^1}, \alpha^{2^2}, \dots, \alpha^{2^{m-1}}$  again you will see that you have the same number of elements in the bases ok. So, these particular this sequence is what is called as a normal bases if this  $m$  elements are linearly independent. So, if this there is a important criteria where the  $m$  elements have to be linearly independent.

So, again you can express any element in the field also by linear combinations of this with these bases ok. So, the important ramifications between them you know like between the polynomial bases which probably it is more simple to explain and the normal bases, through which you can actually have very interesting constructions very efficient constructions.

(Refer Slide Time: 17:55)

Polynomial Representation

- Any element in the field can be expressed in terms of its bases.
- For example in the field  $GF(2^m)$ , an element can be expressed wrt. its polynomial bases as:

$$a(\alpha) = a_{m-1}\alpha^{m-1} + \dots + a_1\alpha + a_0$$

swamyam

So, both are useful but let us try to look into the polynomial representation. So, in the polynomial representation any element in the field can be expressed in terms of his bases, the bases is as I said in the previous slide where I have got 1 alpha till alpha to the power of n minus 1.

So, if I want to you know like express say any elements say  $GF 2$  to the power  $m$ . So, this should be  $GF 2$  to the power of  $m$  an element can be expressed with respect to it is polynomial bases as a alpha. So, you can see that I am now having a general representation which is  $a\alpha$ , but I have now taken a specific instance of that ok. So, how I am generating this element I am taking linear combinations of my bases elements. So, the coefficients of my linear expansion essentially are denoted as  $a_0 a_1$  so until a minus 1 and these elements can be either in there in  $GF 2$ , that means they can be either 0 or they can be either 1.

So therefore, you can easily understand that this particular representation essentially can covered all the a I mean can covered the entire field  $GF 2$  to the power of  $m$ . So, it can very much represent any element in  $GF 2$  to the power of  $m$  and that is why this particular or this particular choices are essentially gives you the bases. Note that you cannot express you know like alpha power of  $m$  minus 1 by the other components ok, that that means these are the minimum number of elements we are required to express all elements in the field in the field.

(Refer Slide Time: 19:27)

The slide is titled "Isomorphism". It features a diagram on the left showing a mapping  $f$  from a set of elements  $x, y$  to a set of elements  $f(x), f(y)$ . A large arrow points from the left set to the right set. Below the diagram, a text box states: "An injective (one-to-one) homomorphism is called an isomorphism." To the right of the diagram, another text box defines a homomorphism: "For two groups  $G_1$  and  $G_2$ , a surjective function  $G_1$  to  $G_2$  is said to be a homomorphism iff  $f(x \circ y) = f(x) \dagger f(y)$ ." Below this, a note says: "Note, the operators on the left and right are not the same." At the bottom of the slide, a third text box explains: "The idea of isomorphism can be extended to rings and fields. In these extensions the only difference is that the latter two are defined wrt. Two operators, say  $(+, \cdot)$ . Thus, we say  $f: R_1 \rightarrow R_2$  is say a field isomorphism iff:  $f(a+b)=f(a)+f(b)$ , and  $f(a \cdot b)=f(a) \cdot f(b)$  for every  $a$  and  $b$  in  $R_1$ ." The slide also includes the Swamyam logo and other branding at the bottom.

So, now we are in a position to understand this concept of Isomorphisms ok. So, what is Isomorphisms? So, suppose you have got 2 groups  $G_1$  and  $G_2$  and I want to define a Surjective function  $G_1$  to  $G_2$ , that means from  $G_1$  to  $G_2$  such that in the following condition holds. So, what is the condition? So, I have got an operator here so suppose this operator is denoted as circle ok. So that means, I will do circle operation between elements in the group  $G_1$  and I do an operation which is define by a dagger symbol on the on the group  $G_2$ . So therefore, right if I want to do an operation between  $x$  and  $y$  and calculate  $x$  circle  $y$  I can also do this alternatively by mapping both  $x$  and  $y$  to this target group  $G_2$  by applying the mapping  $f$  for example.

So therefore, now I get  $f x$  and I get  $f y$  and then I apply the dagger operation will  $f x$  and  $f y$ , so I get  $f x$  dagger  $f y$ . So therefore, here we have we were like we took  $x$  we took  $y$  we applied the operator circle and got  $x$  circle  $y$ . So now, if I apply the function  $f$  to the result I get  $f x$  dagger  $f y$  and it turns out that  $f x$  dagger  $f y$  should be same as calculating  $f x$  of I mean  $f x$  dagger  $f y$  should be the same as  $f$  applied on  $x$  circle  $y$ . So, then this particular function is said to be a homomorphism ok. So, it is said to be homomorphism if and only if  $f x$  circle  $y$  is equal to  $f x$  dagger  $f y$ .

Note that the operators on the left and the right need not be the same they can be same they may not be same. So, when I further qualify this mapping as an injective function that means it is an one to one function. So, it is a one to one homomorphism then this is

what is called as isomorphism. Now, the idea of the isomorphism can be extended from groups to rings and fields, in this extension the only difference is that we have got further 2 operations rather than 1 operation.

So therefore, write they have got suppose you have operators are last end out then we say that the mapping from  $R_1$  to  $R_2$  is a field isomorphism if and only if  $f$  of  $a$  plus  $b$  is equal to  $f$  of  $a$  plus  $f$  of  $b$  and  $f$  of  $a$  dot  $b$  is equal to  $f$  of  $a$  dot  $f$  of  $b$  ok. So, I have just assume that the operators are same on both sides, but you can also generalized that. So therefore, this happens for every  $a$  and  $b$  which belongs to  $R_1$ .

(Refer Slide Time: 22:09)

**Example in  $GF(2^4)$**

0	$z^2$	$z^3$	$z^3 + z^2$
1	$z^2 + 1$	$z^3 + 1$	$z^3 + z^2 + 1$
$z$	$z^2 + z$	$z^3 + z$	$z^3 + z^2 + z$
$z + 1$	$z^2 + z + 1$	$z^3 + z + 1$	$z^3 + z^2 + z + 1$

There are 3 irreducible polynomials of degree 4, which can be used to construct the above field elements:  $f_1(z) = z^4 + z + 1, f_2(z) = z^4 + z^3 + 1, f_3(z) = z^4 + z^3 + z^2 + z + 1$ .  
 The fields are denoted as  $F_1, F_2,$  and  $F_3$  respectively.  
 The resulting fields all have 16 elements, as shown above.  
 However, the operations are different.  
 Like the same operation,  $z \cdot z^3$  would result in  $z^4 = z + 1, z^3 + 1, z^3 + z^2 + z + 1$  in the 3 fields.

So, this essentially write essentially gives as the definition of isomorphism, so let us try to see whether we can understand isomorphism in more details by take me an example. So, again I will take up my example of  $GF 2$  to the power of 4 and again I will represented all the elements in  $GF 2$  to the power of 4. So, note that now I have got also 0 which is over there, so I have got all the 16 elements. So, there is one which is 0 and then there are 15 non 0 elements in the field.

So, now as I said that there are 3 irreducible polynomials of degree 4 which can be which can be used to construct this above field elements. The 1st one as we have seen is  $z$  to the power of 4 plus  $z$  plus 1 you also have got another candidate  $f_2 z$  which is  $z$  to the power of 4 plus  $z$  cube plus 1 and then there is a 3rd one which is called as  $f_3 z$  which is actually a pentanomial. So, these are examples of trinomials, but now we have got

another polynomial which is a pentanomial which is  $z$  to the power of 4 plus  $z$  cube plus  $z$  square plus  $z$  plus 1, which is also an example of an irreducible polynomial for  $GF(2)$  to the power of 4.

So therefore, what I do is I extend using  $f_1(z)$  the field is what I called as say capital  $F_1$ , I extend again  $GF(2)$  to  $GF(2)$  to the power of 4 by using  $f_2(z)$  and that field I called as capital  $F_2$  likewise I have got capital  $F_3$ . So, now or you can easily understand that all the resulting fields will have sixteen elements interestingly the operations will be different. For example, like if I want to do say  $z$  into  $z$  cube in the 1st field I will get  $z$  to the power of 4 will result which is equal to  $z$  plus 1, in the 2nd field however that result will be  $z$  cube plus 1 and in the 3rd field it will be  $z$  cube plus  $z$  square plus  $z$  plus 1. So, you see I am doing the same operation but I am getting different results ok, because the fields are equivalent but they are not equal.

(Refer Slide Time: 24:07)

**Defining Isomorphism**

- The fields are isomorphic and one can establish a mapping between say  $F_1$  and  $F_2$ , by computing  $c \in F_2$ , st.  $f_1(c) \equiv 0 \pmod{f_2}$ .
- The mapping  $z \rightarrow c$  is thus used to construct the isomorphism, say  $T: F_1 \rightarrow F_2$
- An example for  $c$  could be  $c = z^2 + z$ . To verify compute:

$$f_1(z^2 + z) = (z^2 + z)^4 + (z^2 + z) + 1 = z^8 + z^4 + z^2 + z + 1 \pmod{f_2}$$

Now, note that for  $\text{mod } f_2$ , we substitute  $z^4 = z^3 + 1$ .

$$z^4 = z^3 + 1 \Rightarrow z^5 = z^4 + z = z^3 + z + 1 \Rightarrow z^6 = z^4 + z^2 + z = z^3 + z^2 + z + 1$$

$$\Rightarrow z^8 = z^6 + 1 = z^3 + z^2 + z.$$

Thus,  $f_1(c) = z^8 + z^4 + z^2 + z + 1 \equiv 0 \pmod{f_2}$

The slide also features a video feed of a presenter in the bottom right corner and logos for 'swayam' and 'THE INDIAN EDUCATION' at the bottom.

So, now I can actually you know like establish isomorphism between these fields I can say that you know like all these fields are actually equal, but they I mean an equivalent but they there we can actually you know the establish some kind of relationships between them. So, the fields are isomorphism are isomorphic and can establish and we can establish a mapping between say  $F_1$  and  $F_2$  and I will try to show you that how we can establish this mapping.

So, first I do is what I do is this I start computing an element  $c$  which belongs to  $F_2$ , such that if I take the you know like the irreducible polynomial  $F_1$  which is the irreducible polynomial of the first field and then substitute  $c$  in that ok. Then you can easily understand that what I will try to do is that I will try to calculate this modulo of  $F_2$  and if I calculate modulo  $F_2$  and then I get 0 then what I will say is that my  $z$  is mapped into  $c$  ok. So, what is  $z$  you can easily understand  $z$  will satisfy  $F_1$  in the 1st field but not  $c$ .

So, what I am trying to do now is that because  $c$  is an element in  $F_2$ . So, if they are equivalent then  $c$  should satisfy  $F_1$  but modulo of  $F_2$  and this street will work. So, let us see so how we can you know like develop 1 mapping using this observation. For example, suppose I take  $c$  is equal to  $z^2 + z$  ok, so to verify what I do is that I calculate  $f_1 z^2 + z$ .

So,  $F_1 z^2 + z$  is so if we remember what is  $F_1$  is  $z^4 + z + 1$  ok. So therefore, write if I substitute  $z$  as by  $z^2 + z$ , so I get the result as  $(z^2 + z)^4 + (z^2 + z) + 1$  and that if we expand I will get  $z^8 + z^4 + z^2 + z + 1$  module of  $F_2$  and what is  $F_2$   $F_2$  is  $z^4 + z^3 + 1$ . So, I can substitute  $z^4$  by  $z^3 + 1$ .

So, therefore,  $z^4$  is  $z^3 + 1$  and likewise  $z^5$  is  $z^4 + z$ , if I replace  $z^4$  with  $z^3 + 1$  then I get  $z^3 + z + 1$ . And likewise  $z^6$  is again if I multiply this by  $z$  I get  $z^4 + z^2 + z$  and again I will replace  $z^4$  I will get therefore  $z^3 + z^2 + z + 1$ . So, note that  $z^8$  again I can get  $z^8$  by directly squaring this, so I get that as equal to  $z^6 + 1$  and I replace  $z^6$  by this expansion, so I get  $z^3 + z^2 + z$ .

So, then  $f_1 c$  module of  $f_2$  is nothing but as we have seen  $z^8 + z^4 + z^2 + z + 1$  and that but that is that becomes equal to 0 ok. So, you can easily see this that if I you know like combine  $z^3 + z^2 + z$  with  $z^4$  which is  $z^3 + 1$  ok, then I will get an add  $z$  with it an add 1 with it an add  $z^2$  with it then the elements will get cancelled and I will get 0 module of  $F_2$ .



(Refer Slide Time: 27:35)

**Check on Homomorphism**

- Consider two elements  $e_1 = z^2 + z, e_2 = z^3 + z$ .
- Product in field  $F_1$ :  $(z^2 + z)(z^3 + z) = z^5 + z^4 + z^3 + z^2$
- In field  $F_1$ :  $z^4 = z + 1 \Rightarrow z^5 = z^2 + z$ .
  - Thus, the product is:  $z^2 + z + z^3 + z + 1 + z^2 = z^3 + 1$ .
- The same operation can also be performed in the field  $F_2$ .
- Compute,  $T(e_1) = (z^2 + z)^2 + (z^2 + z) \text{mod}(z^4 + z^3 + 1) = z^4 + z^2 + z^2 + z = z^3 + z + 1$ .
- Likewise,  $T(e_2) = (z^2 + z)^3 + (z^2 + z) \text{mod}(z^4 + z^3 + 1) = z + 1$

The slide also features the Swamyam logo and a video inset of a man speaking.

So, let us take on the homomorphism property ok, so in homomorphism property you consider 2 elements  $e_1$  and  $e_2$ . So, suppose  $e_1$  is equal to  $z^2 + z$  and  $e_2$  is equal to  $z^3 + z$  ok, so these are 2 elements in  $F_1$ . So therefore, if I want to trying you know do the product in the field  $F_1$  that is symbol I will take  $z^2 + z$  multiplied with  $z^3 + z$ , so I will get  $z^5 + z^4 + z^3 + z^2$ .

So, in the field  $F_1$  I know  $z^4 = z + 1$  as  $z^5 = z^2 + z$ . So, if I substitute this then the product right becomes  $z^2 + z + z^3 + z + 1 + z^2$  and that becomes equal to  $z^3 + 1$ . So, I get the result as  $z^3 + 1$ , so now let us see the you know like if I apply the homomorphism property I will get the same result.

Now, the same operation can also be performed in the field  $F_2$  what I do is I apply therefore, this mapping on  $e_1$ . So, what is the mapping I will replace  $z$  by  $z^2 + z$ . So, what is  $e_1$   $z^2 + z$  so therefore, I will replace this  $z$  by  $z^2 + z$ .

So, I get  $(z^2 + z)^2 + (z^2 + z) \text{mod}(z^4 + z^3 + 1)$  because, that is my field I mean polynomial in  $F_2$ . So therefore, if you expand this you will get  $z^4 + z^2 + z^2 + z$  which is and then I do a module of this I will get  $z^3 + z + 1$ . Likewise I do  $e_2$  which is again you know this element, so now again I replace  $z$  by  $z^2 + z$

z I do a similar manipulation and I get z plus 1. So, now if I take these two elements then they are elements in F2 now because I have mapped them to F2.

(Refer Slide Time: 29:25)

**Check on Homomorphism**

Multiplying in the field  $F_2$ :  $T(e_1)T(e_2) = (z+1)(z^3+z+1) \bmod (z^4+z^3+1) = z^2$ .

This can be seen as the mapped result from  $F_1$ :

$$\begin{aligned} T(z^3+1) &= (z^2+z)^3+1 = (z^6+z^5+z^4+C) \bmod (z^4+z^3+1) \\ &= (z^3+z^2+z+1)+(z^3+z+1)+(z^3+1)+(z^3+1) \\ &= z^2 \end{aligned}$$

I apply multiplication (Refer Time: 29:28) so I take z plus one multiplied with z cube plus z plus 1 do a mod of z to the power of 4 plus z cube plus 1 and this result is equal to z square. So, let us check this result whether in indeed satisfies the homomorphism requirements. So, if you remember like what we have got in the previous computation was we got the result essentially in the field F1 and the question is write we would like to see there when we you know like. So, the field the result in field F1 was z cube plus 1 and if we transform this result into the field F2, I should get the same result as that I get when I multiply the elements T1 and T2 ok.

So, in T 1 and T 2 I get the result is essentially z square. So therefore, now if I map z cube plus 1 I should get z square so let us verify that. So, if I want to map z cube plus 1 therefore, my processes I will again replace z by z square plus z. So, I will calculate z square plus z whole cube plus 1 and therefore if I expand this I will get z to the power of 6 plus z to the power of 5 plus z to the power of 4 plus z cube plus 1 and then remember in this field F2 I will do mod of z power of 4 plus z cube plus 1.

So therefore, if I replace this is the term by term you can verify that this result is indeed equal to z square ok, so therefore it indeed satisfies the property of homomorphism ok. So, let me stop here so we shall continue from this point in the next class, where we shall

try to understand how we can construct these transformations or homomorphisms or isomorphisms in a more algorithmic fashion ok.

Thank you.