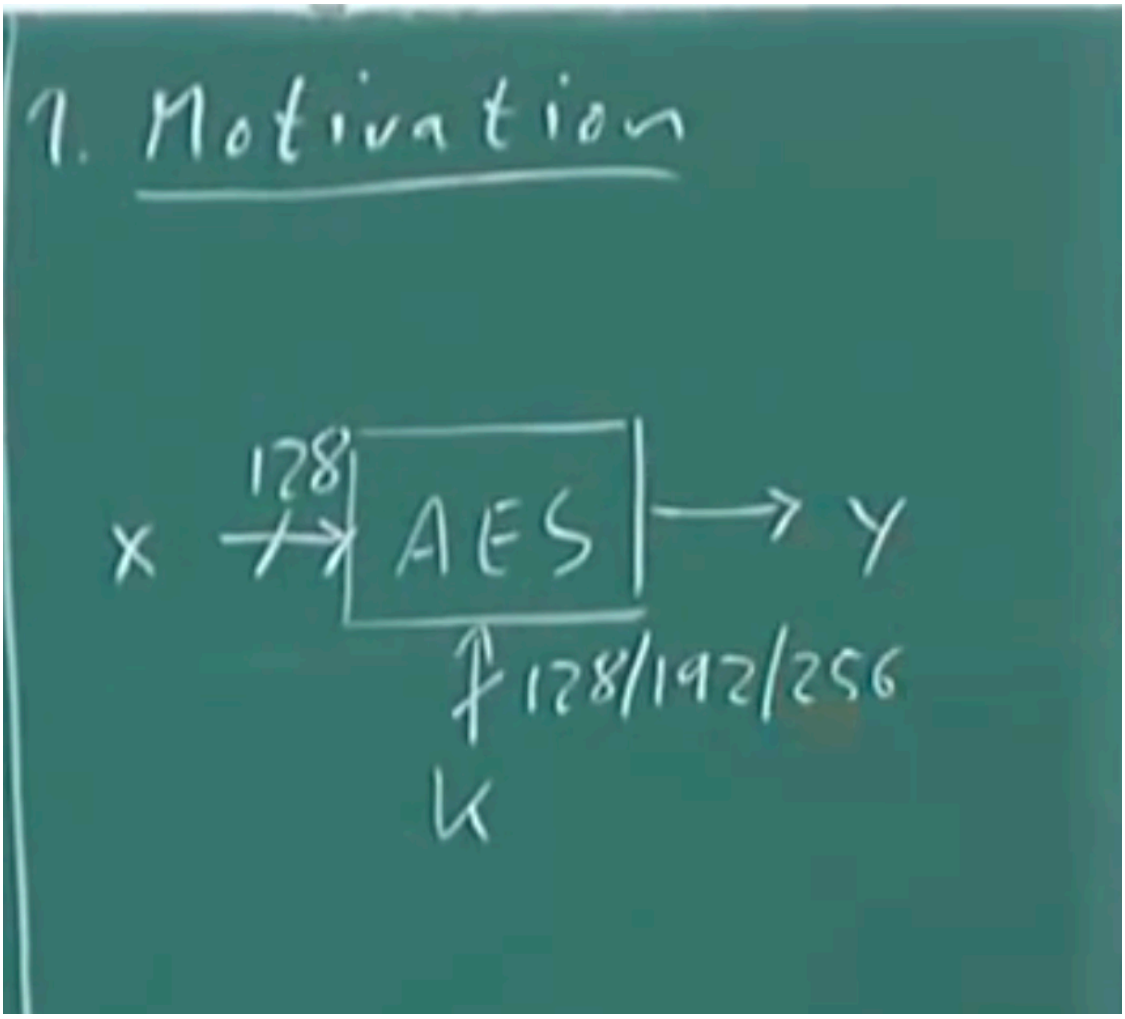
Lecture 7 Galois Fields for AES:

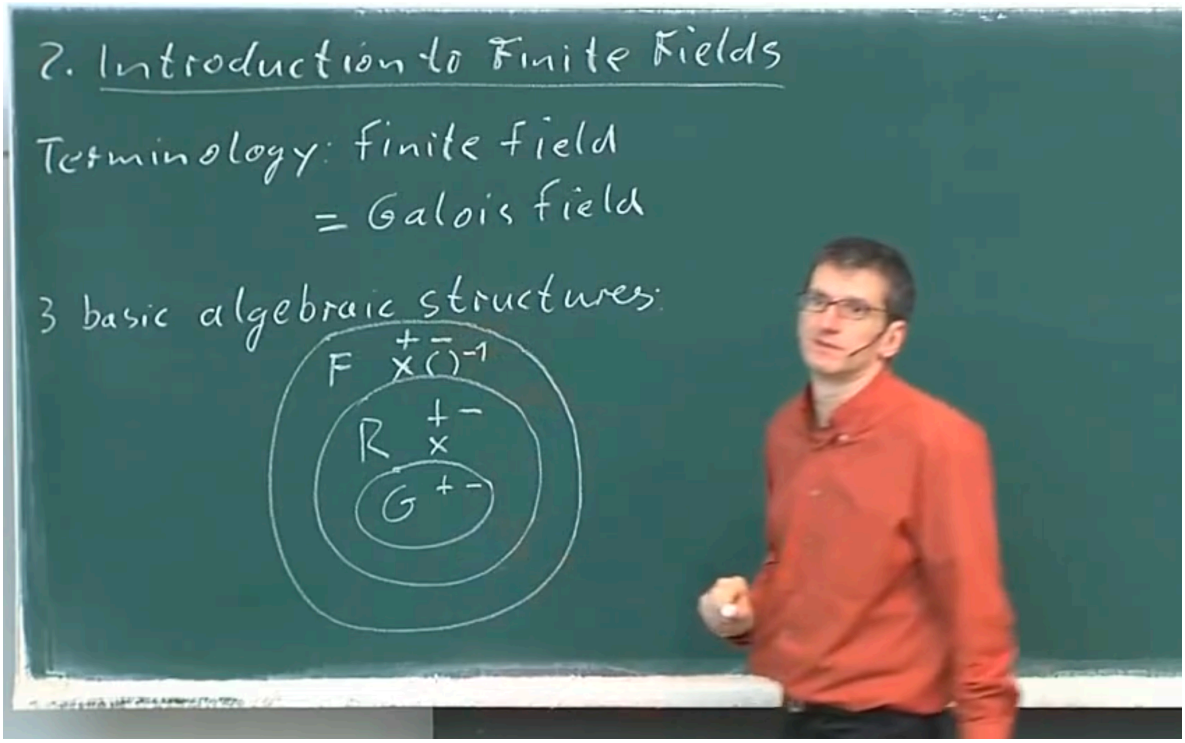
AES is very different from DES, we need to introduce a new Number System.
Main Topics :-

1. Motivation for AES
2. Intro of Finite Fields
3. Prime Fields
4. Extension Fields



Block size is 128 bits and Key Size can be 128/192/256 which is much more longer than DES.
For AES, all internal operations are based on Finite Fields. So we need to learn Finite Fields.

Intro Finite Fields :-
Finite Fields are also called Galois Field (Read about Galois Field)



G is group, R is Ring, F is Fields.

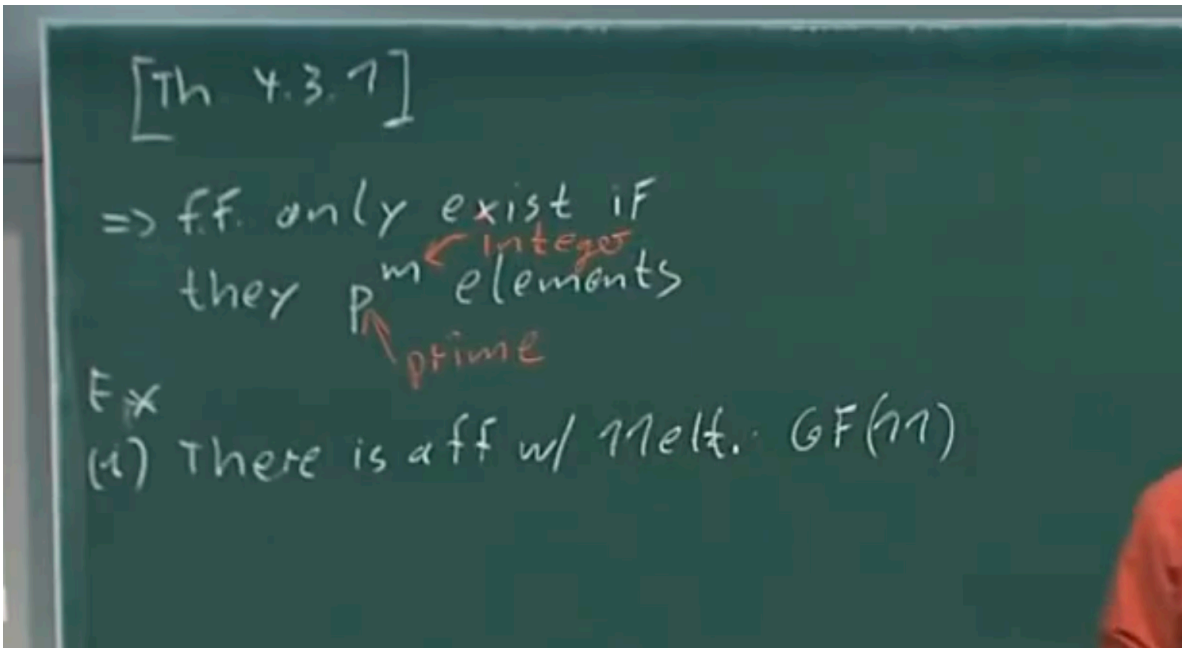
Definition of Group :- Set of elements with 2 operations ie plus and minus (modulo). Other rules are like associative, also order of operation doesn't matter.

Definition of Ring :- it has 3 operations +, -, and multiply. Also not all the ring elements have Multiplicative inverse.

Field has all the 4 operations. Ex of Field :- Real numbers, Complex numbers, Rational numbers but natural numbers is not a field as most numbers don't have multiplicative inverse.

In crypto we almost always deal with **Finite Fields.**
In AES we will do mathematics in a set of 256 elements.

Conditions to construct Finite Fields [4.3.1] :-
Finite fields only exists if we have P power M elements. (Where P is prime and M is natural number).

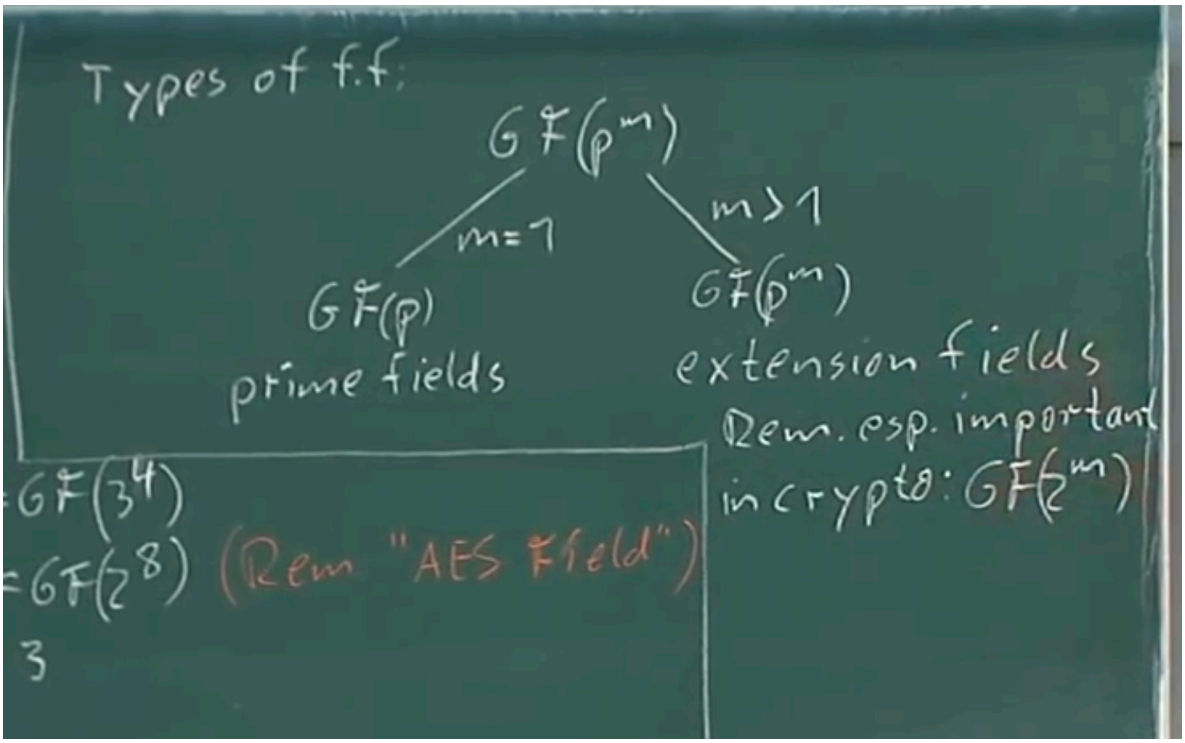


Galois Field (11) is an example of Finite Fields.
GF(81) => GF(3 power 4) => is also an example of Finite Fields.
GF(256) => GF(2 power 8) => is also an example of FF. => **AES Finite Field.**

GF(2) is super important field in practise which is the smallest FF.
12 is not an example of Finite Field as it is not represented as theory **4.3.1**

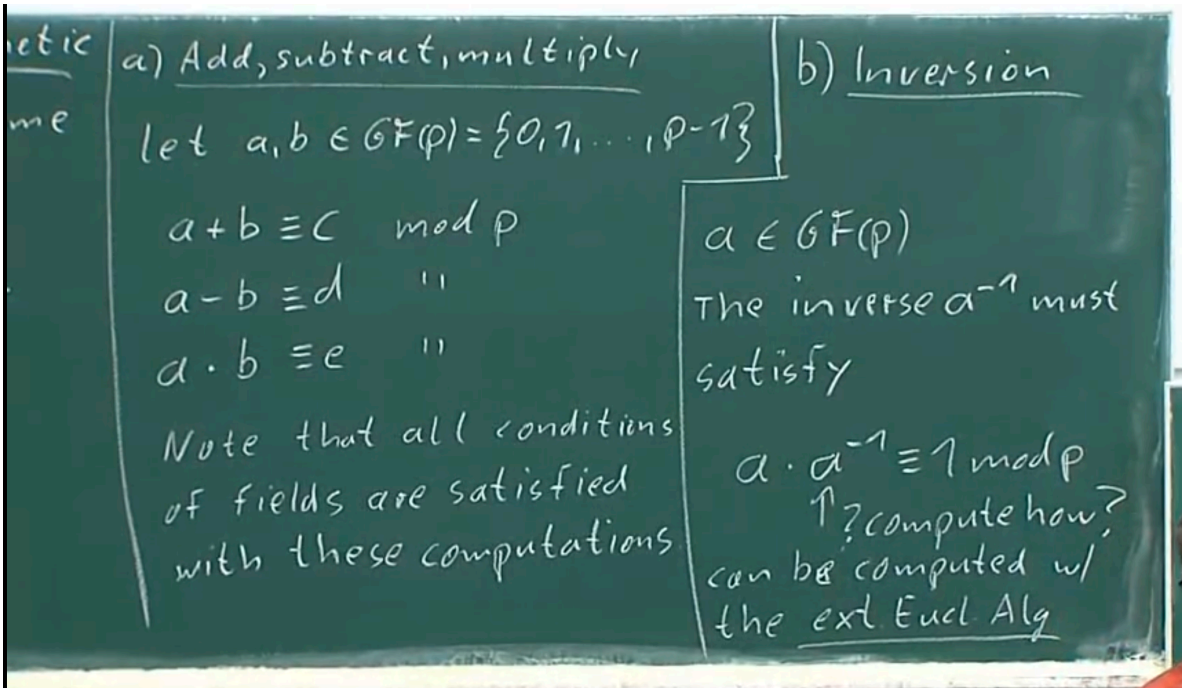
Distinguish between 2 types of Finite Fields :-

1. **M = 1 (we are talking about GF(P))** => Which are called Prime Fields
2. **M > 1 (we are talking about GF(P power M))** => Extension Fields.



PHD thesis of Cristof Paar is on Finite Fields.

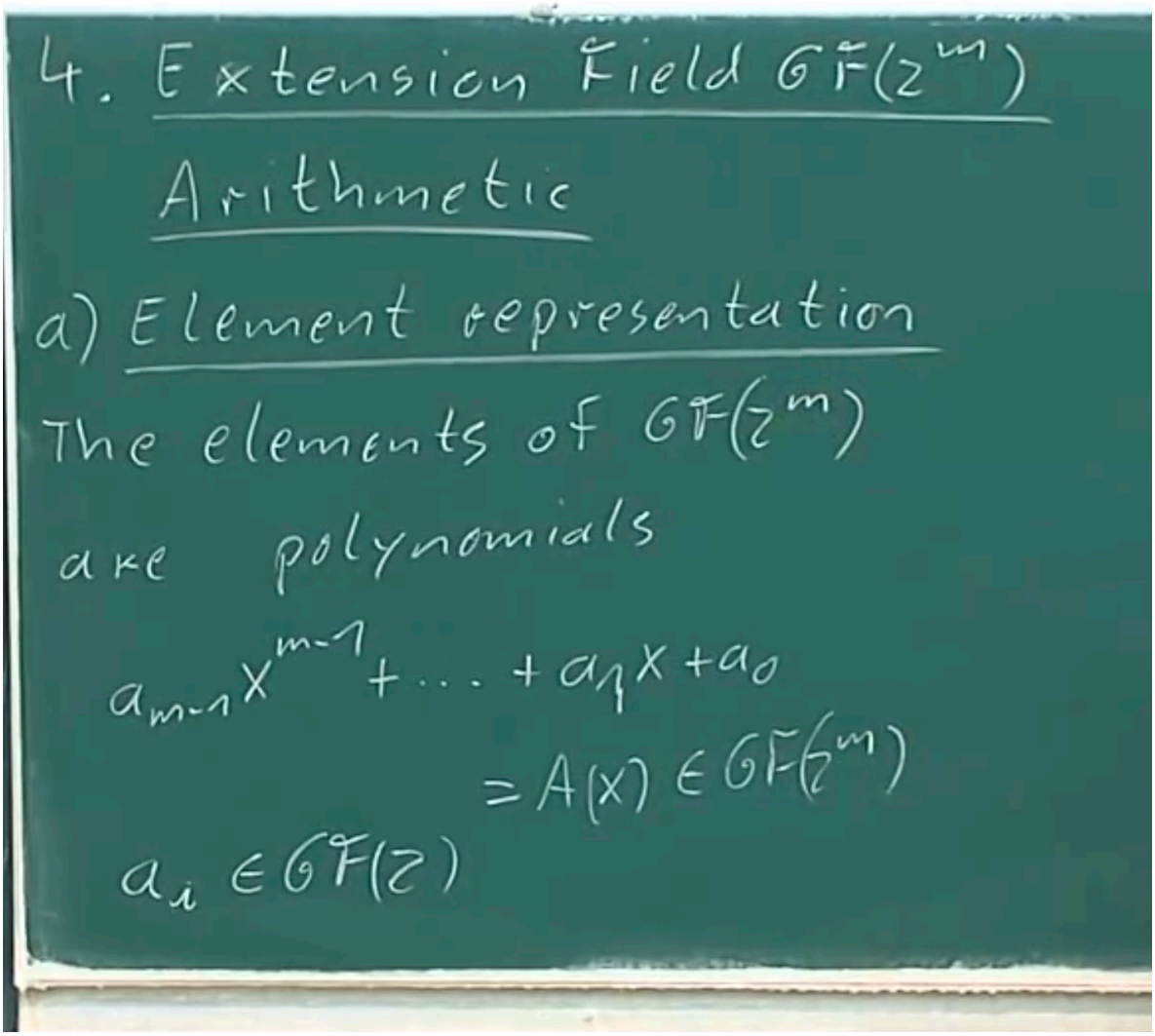
Prime Field Arithmetic :-
The Elements of a Prime Field GF(P) are the integers from 0 to P-1.



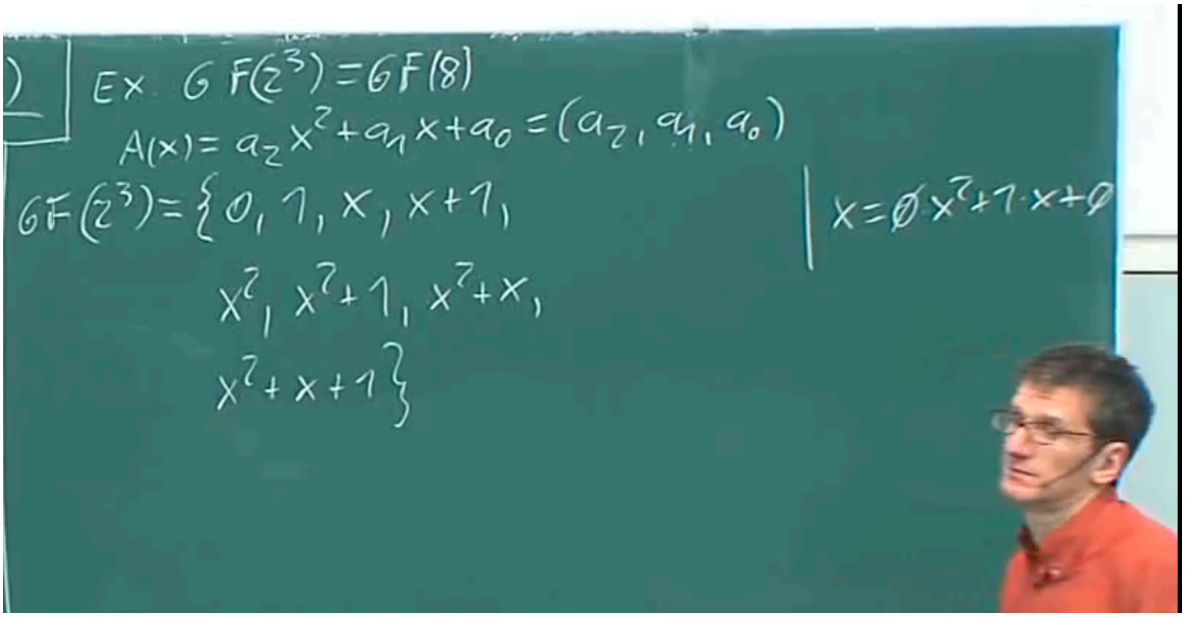
For finding multiplicative inverse there is an algorithm called **Extended Euclidian Algorithm.**

Multiplicative group except 0 element but entire additive group.

Extension Field GF(2 power m) Arithmetic :-
a) Element Representation :-
The elements of GF(2 power m) are polynomials.



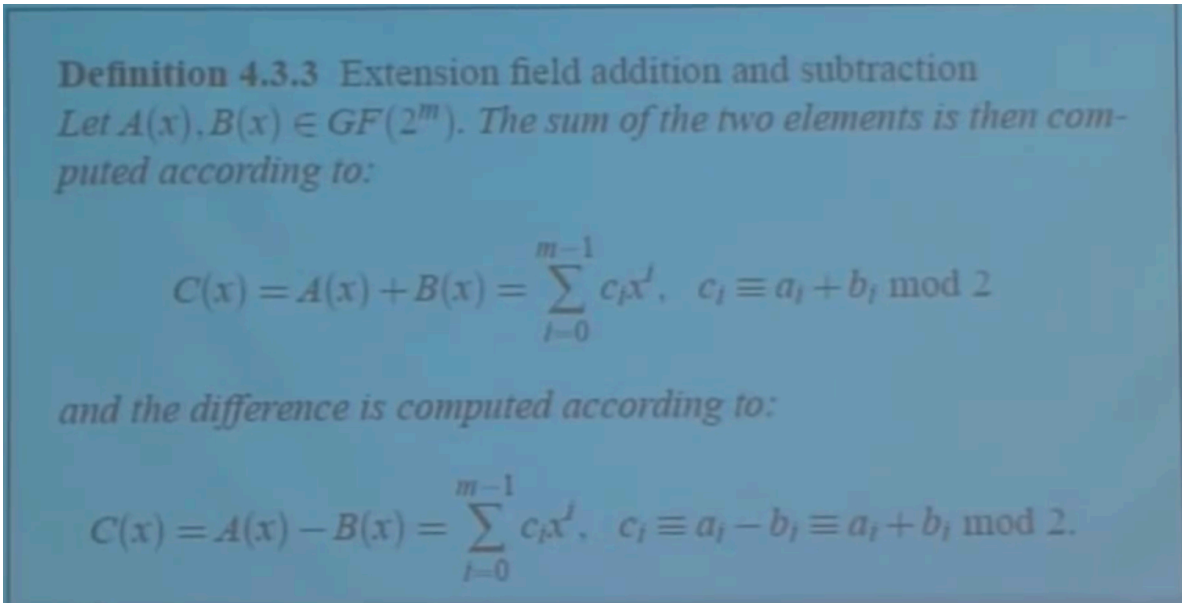
GF(2) is prime field. Example say we have a Extension Field GF(2 power 3) ==> GF(8) then the polynomial representation will be a2*x2 + a1*x1 + a0 and we know coefficients a1, a2, a0 all belongs to GF(2) ie {0 and 1} so
We can represent this in 3 bits (a2, a1, a0).



Question :- how to do arithmetic with these polynomials ?

Addition and Subtraction in 2 power m:-

Use regular polynomial and do modulo 2 addition.



Definition 4.3.3 Extension field addition and subtraction

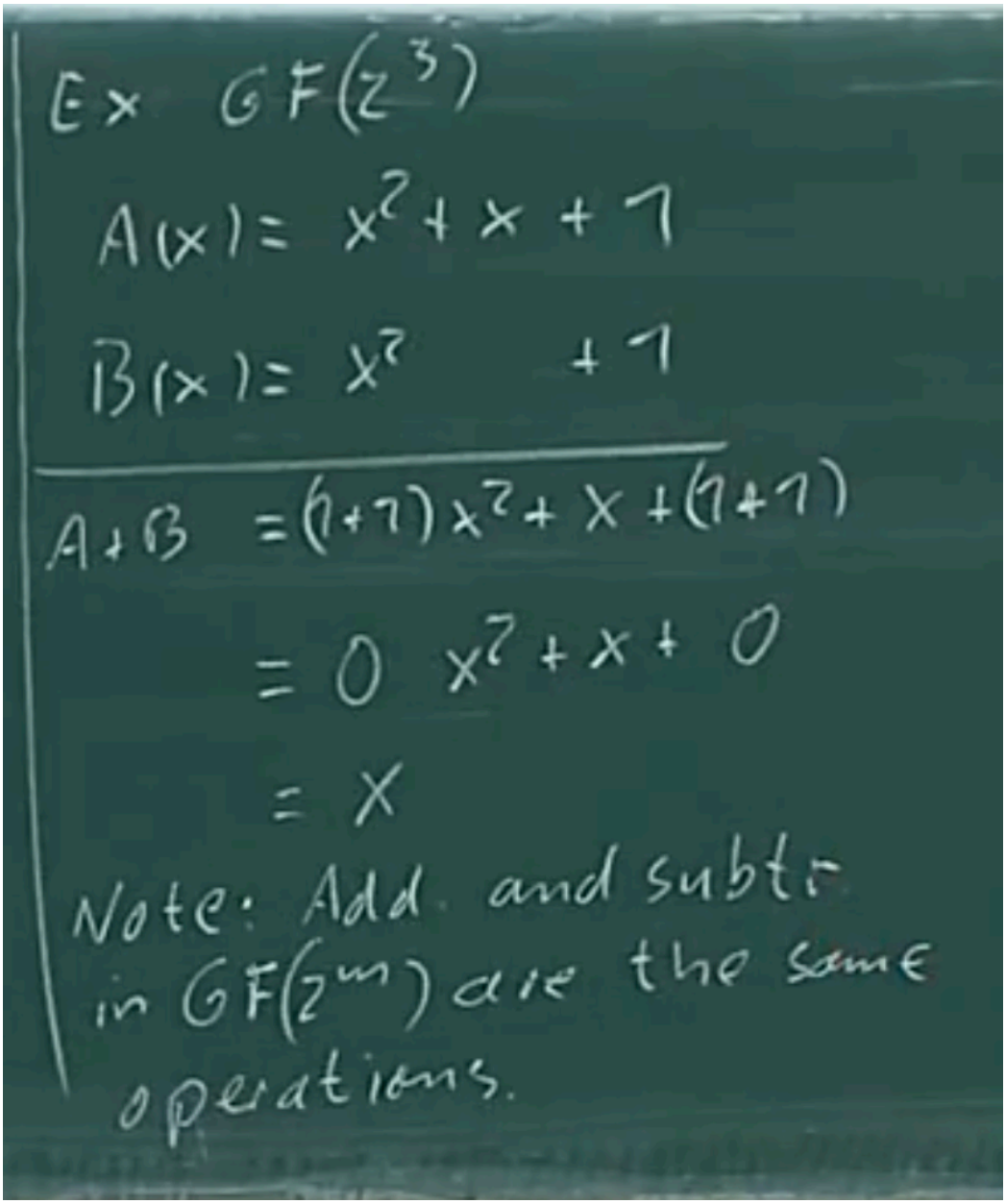
Let $A(x), B(x) \in GF(2^m)$. The sum of the two elements is then computed according to:

$$C(x) = A(x) + B(x) = \sum_{i=0}^{m-1} c_i x^i, \quad c_i \equiv a_i + b_i \bmod 2$$

and the difference is computed according to:

$$C(x) = A(x) - B(x) = \sum_{i=0}^{m-1} c_i x^i, \quad c_i \equiv a_i - b_i \equiv a_i + b_i \bmod 2.$$

Major thing is arithmetic is also in GF(2).



Multiplication in GF(2 power m) :-

Intuition :- Just do simple multiplication.
Ex GF(2 power 3) => we multiple A.B and say polynomials are x^2 + x + 1 and x^2 + 1

So multiplication will be x^4 + x^3 + 2x^2 + x + 1 => which results in x^4 + x^3 + x + 1
Incase of polynomial.

What is the problem ? It is not in the field as X^4 and X^3 are not in field.

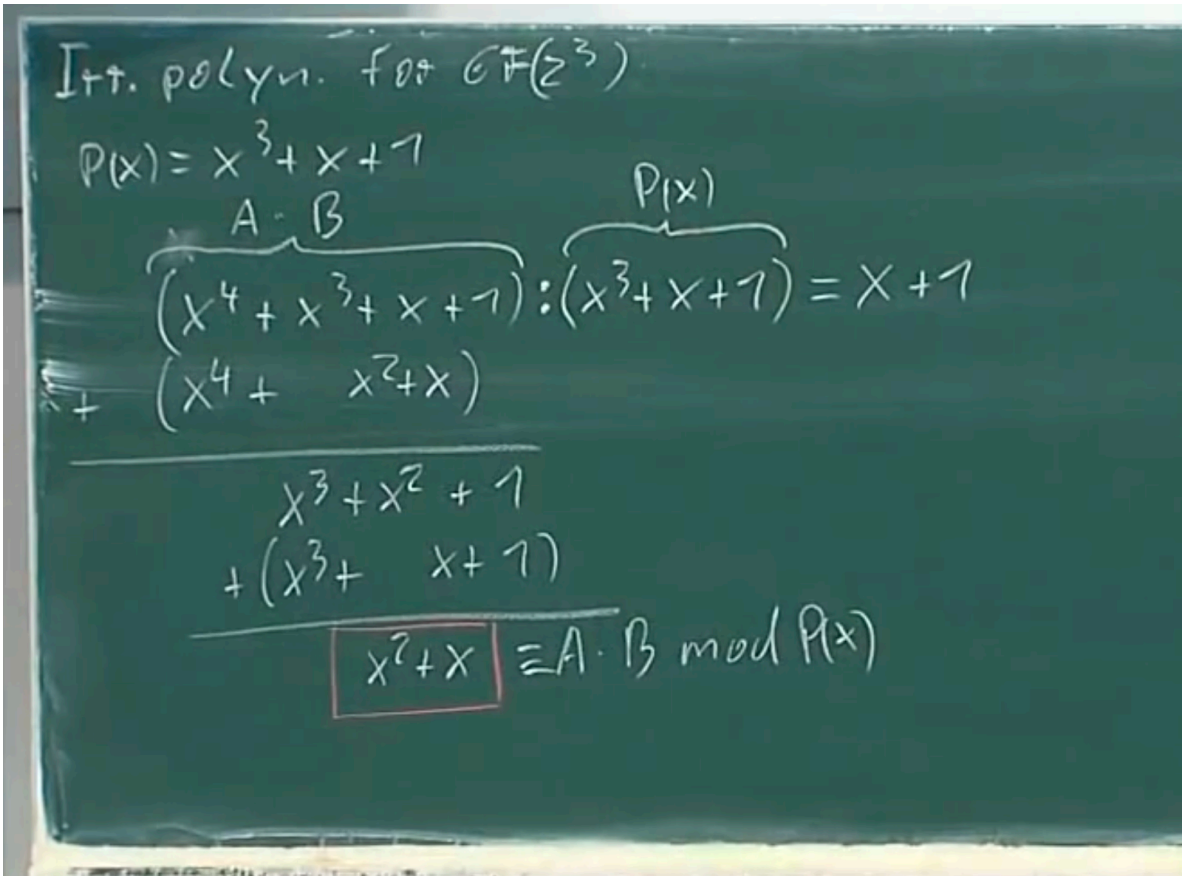
So how can we handle this issue ? In prime fields we have done modulo reduction. So we need to do the same here. We need to reduce the polynomial.

eg :- GF(7) => {0,1,2,3,4,5,6} so say A = 3 and B = 4 so C will be 12 equivalent to 12 mod 7 which is 5. Now question is what is 7 ?
7 is a prime as this is a prime field so in case extension fields we need to find a prime polynomial ie which are irreducible, cannot be factored.

So irreducible polynomial for GF(2 power 3) is **x^3 + x + 1** so final computation :-

Question :- Why Galois Field extension field module reduction (irreducible polynomial) is starting with max power of m ie for 2 power 3 , irreducible polynomial is X3 + X + 1 ? Why it starts with X3 not X2 ?
Answer :- May be because smaller than this polynomial will be maximum possible field polynomial. Ie in case 7 is divisor then max 6 is reminder so in our case max X2 + X + 1 can be the reminder.

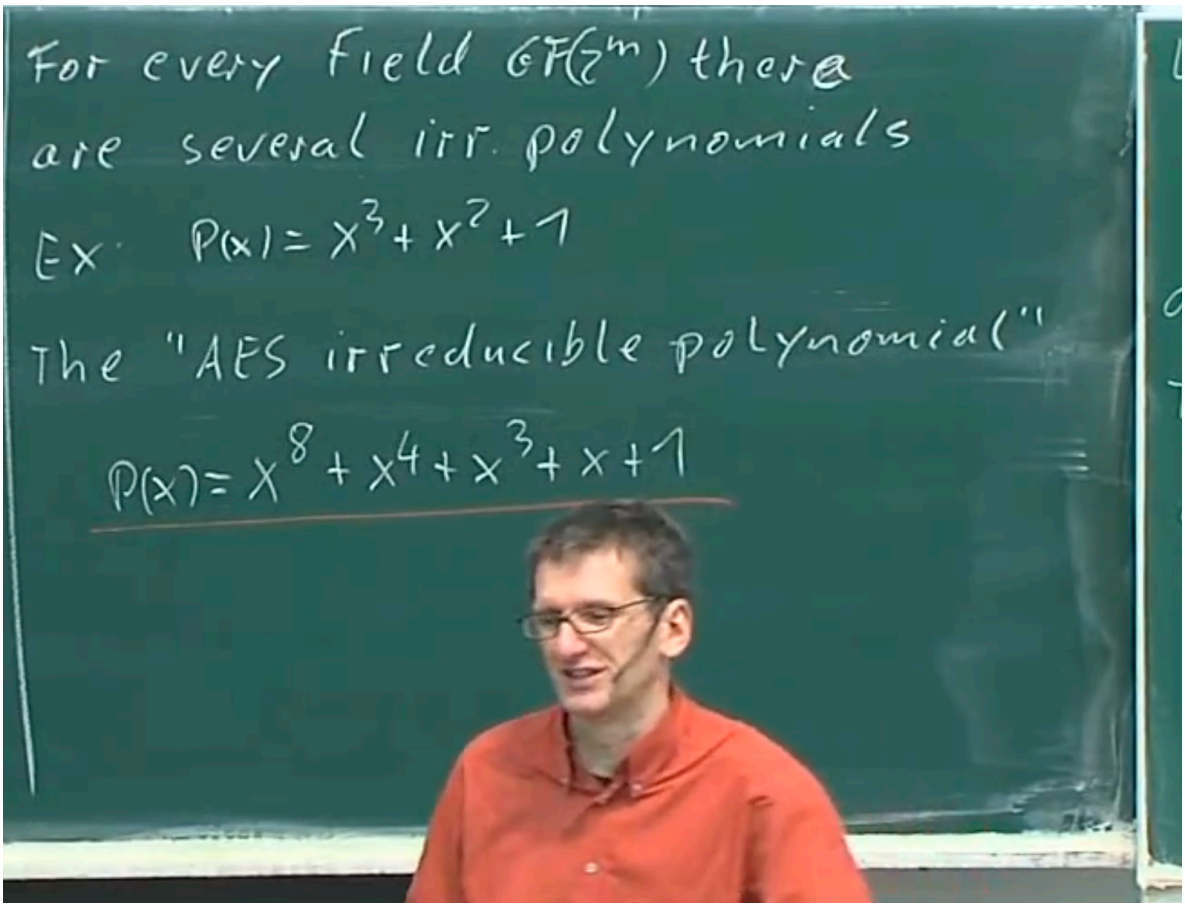
one more point is $x4 + x3 + x + 1 = (x2 + x + 1)(x2 + 1)$ is a reducible polynomial ie if you look closely you will find the Mod 2 removing “x2”.



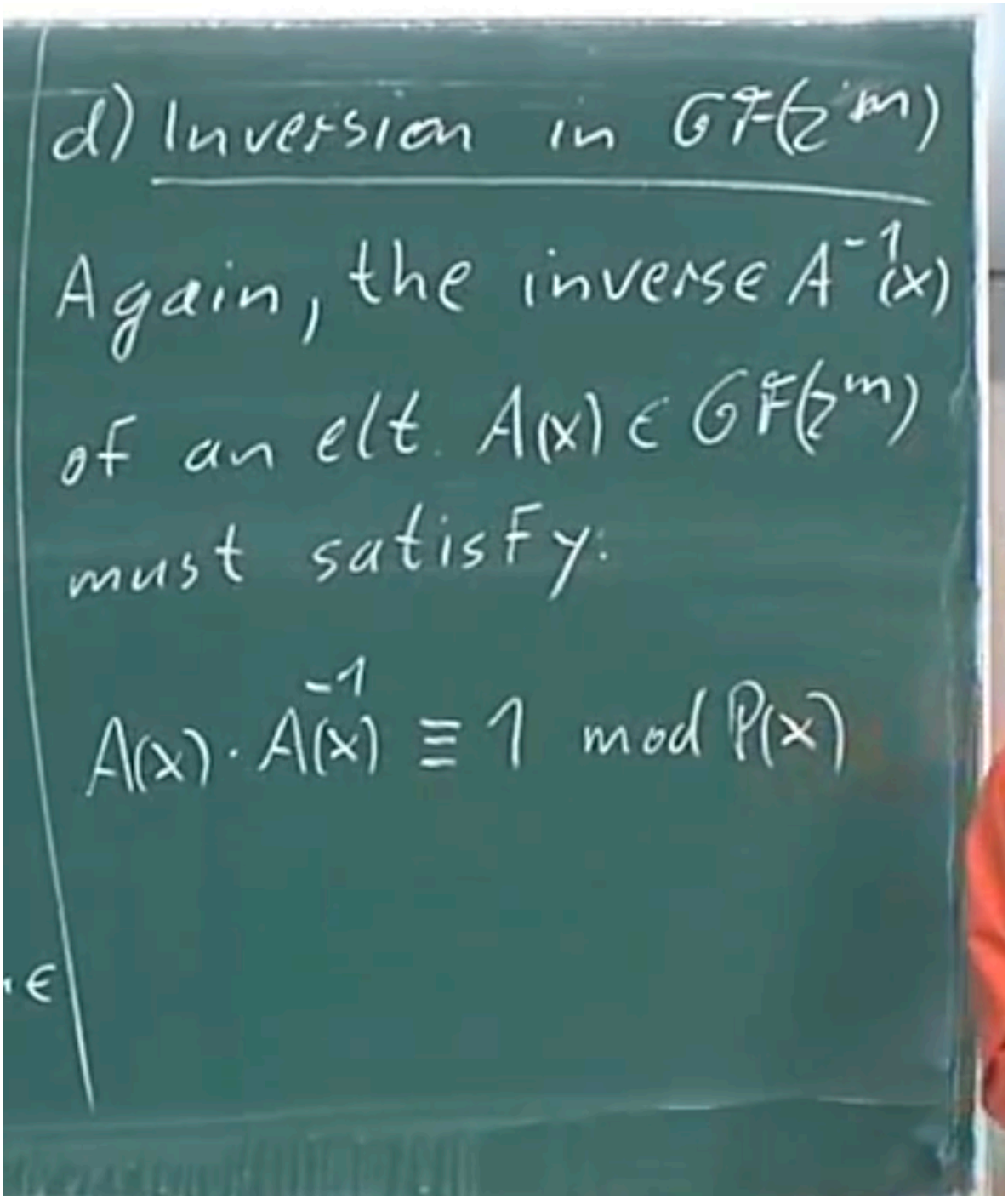
Question :- Where do I get this polynomial ?
For Ever field GF(2 ^ m) there are multiple/several irreducible polynomials, which is very different that prime GF.

If given GF(2 ^ m) you get a different result based on P(X) ie irreducible polynomial sp every Extension field result can be different based on irreducible polynomial.

AES irreducible polynomial is P(X) is X^8 + X^4 + X^3 + X + 1.



d) inversion of extension field GF (2 ^ m) :-



For finding inverse of A(X) ie A(X)^-1 , we need extended euclidian algorithm. This will be taught in 6th chapter.