Fields
Field Axioms

- A field $\mathcal{F}$ consists of a set $S$ and two operations which we will call addition and multiplication, and denote them by $\oplus$ and $\otimes$.
- The set $S$ has two special elements, denoted by 0 and 1.
- The set $S$ and the addition operation $\oplus$ form an additive group denoted by $G_a = (S, \oplus)$ such that 0 is the neutral (identity) element of $G_a$.
- Also the set $S^* = S - \{0\}$ and the multiplication operation $\otimes$ form a multiplicative group denoted by $G_m = (S^*, \otimes)$ such that 1 is the neutral (identity) element of $G_m$.
- Furthermore, the distributivity of multiplication over addition holds:

$$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c) \quad \text{for} \quad a, b, c \in S$$
Size and Characteristic

- The number of elements in a field is the **size** of the field, which can be finite or infinite.

- The **characteristic** \( k \) of a field is the smallest number of times one must use 1 (the identity element of \( G_m \)) in a sum (using the addition operation \( \oplus \)) to obtain 0 (the identity element of \( G_a \))

\[
\underbrace{1 \oplus 1 \oplus \cdots \oplus 1}^{k \text{ 1s}} = 0
\]

- The characteristic is said to be zero, if the repeated sum never reaches the additive identity element 0.
Rings

- The set of integers $\mathbb{Z}$ and the integer addition $+$ and multiplication operation $\times$ does not form a field.
- We can easily verify that $(\mathbb{Z}, +)$ is an additive group with identity 0.
- However, $(\mathbb{Z} - \{0\}, \times)$ is not a multiplicative group; for example, the element $2 \in \mathbb{Z} - \{0\}$, however, it does not have an inverse: There is no such $x \in \mathbb{Z} - \{0\}$ that would give $2 \times x = 1$.
- In fact, $(\mathbb{Z}, +, \times)$ forms a **ring**, another mathematical structure similar to field, which does not require a multiplicative group.
- In a ring, the distributivity of multiplication over addition holds.
A rational number is defined to be a number of the form $\frac{a}{b}$ such that $b \neq 0$ and $a, b \in \mathbb{Z}$.

The set of rational numbers $\mathbb{Q}$ together with the usual addition $+$ and multiplication $\times$ operations, with additive and multiplicative identities $0$ and $1$, respectively, forms a field.

Indeed, $(\mathbb{Q}, +)$ is an additive group with identity $0$; the additive inverse of $\frac{a}{b}$ is found as $-\frac{a}{b}$.

Also, $(\mathbb{Q}, \times)$ is a multiplicative group with identity $1$; the multiplicative inverse of $\frac{a}{b}$ with $a \neq 0$ is found as $\frac{b}{a}$.

The size of the field $\mathbb{Q}$ is infinity; the characteristic of $\mathbb{Q}$ is zero since the sum $1 + 1 + \cdots + 1$ can never be equal to $0$. 
Infinite Fields

- Similarly, the set of real numbers \( \mathbb{R} \) together with the usual addition + and multiplication \( \times \) operations, with additive and multiplicative identities 0 and 1, respectively, form a field.
- Also, the set of complex numbers \( \mathbb{C} \) together with the usual addition + and multiplication \( \times \) operations, with additive and multiplicative identities 0 and 1, respectively, forms a field.
- Both of these fields have infinite size and zero characteristic.
- In cryptography, we deal with computable objects, and we have finite memory, therefore, infinite fields are not suitable.
- In cryptography, we deal with finite fields, a branch of mathematics where the name of Évariste Galois has a special place.
Évariste Galois

- Évariste Galois (1811-1832) was a French mathematician born in Bourg-la-Reine.
- While still in his teens, he was able to determine a necessary and sufficient condition for a polynomial to be solvable by radicals, thereby solving a long-standing problem.
- His work laid the foundations for Galois theory and group theory, two major branches of abstract algebra, and the subfield of Galois connections.
- He was the first person to use the word “group” (French: groupe) as a technical term in mathematics to represent a group of permutations.
- A radical Republican during the monarchy of Louis Philippe in France, he died from wounds suffered in a duel under questionable circumstances at the age of twenty.
Galois Field GF($p$)

- First we observe that for a prime $p$ the set $\mathbb{Z}_p$ together with the addition and multiplication mod $p$ operations forms a finite field of $p$ elements: we will denote this field by GF($p$), the Galois field of $p$ elements.

- The additive group $(\mathbb{Z}_p, +)$ has the elements $\mathbb{Z}_p = \{0, 1, 2, \ldots, p - 1\}$, the operation is addition mod $p$, and the additive identity element is $0$.

- The multiplicative group $(\mathbb{Z}_p^*, \times)$ has the elements $\mathbb{Z}_p^* = \{1, 2, \ldots, p - 1\}$, the operation is multiplication mod $p$, and the multiplicative identity element is $1$.

- The size of GF($p$) is $p$, while the characteristic is also $p$ since

\[
\underbrace{1 + 1 + 1 + \cdots + 1}_{p \text{ times}} = 0
\]
Since 2 is a prime, GF(2) is a Galois field of 2 elements

- The set is given as \{0, 1\}; the size is 2, and the characteristic is 2
- The additive identity is 0 while the multiplicative identity is 1
- The addition and multiplication operations are as follows:

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

In other words, the addition operation in GF(2) is equivalent to the Boolean exclusive OR operation, while the multiplication operation in GF(2) is the Boolean AND operation.
3 is also a prime, and thus, GF(3) is a Galois field of 3 elements

- The set is given as \{0, 1, 2\}; the size is 3, and the characteristic is 3
- The additive identity is 0 while the multiplicative identity is 1
- The additive group: \((\{0, 1, 2\}, +)\), the multiplicative group: \((\{1, 2\}, \times)\)
- The addition and multiplication operations in GF(3) are defined as mod 3 addition and mod 3 multiplication, respectively:

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>
Since the size $p$ of GF($p$) is a prime, a question one can pose is whether there are fields of size other than a prime.

For example, is there a field with 6 elements?

We can try to see if mod 6 arithmetic works, however, we already know that multiplicative inverse of certain elements mod 6 do not exist.

For example, 3 does not have a multiplicative inverse in mod 6, since there is no number $a$ that satisfies

$$3 \cdot a = a \cdot 3 = 1 \pmod{6}$$

So, our question remains: Is there a field with 6 elements?
Galois showed that the size of a finite field can only be a power of a prime number, in other words, $p^k$ for $k = 1, 2, 3, \ldots$

There is a particular construction of such fields, in fact, we already know how to construct $\text{GF}(p)$, it is simply mod $p$ arithmetic over $\mathbb{Z}_p$.

How does one construct $\text{GF}(p^2)$ or $\text{GF}(p^3)$, etc.

For example, what is the set and the arithmetic of $\text{GF}(7^3)$?
Construction of GF($2^k$)

- First we show how to construct the Galois field of GF($2^k$).
- In order to construct the Galois field of $2^k$ elements, we need to represent the elements of GF($2^k$), and we also need to show how we can perform the field operations: addition, subtraction, multiplication, and division (inversion) operations using this representation.
- It turns out there are more than one way to do that, for example, polynomial representation and normal representation.
- First we will show how to represent field elements using polynomials, and its associated arithmetic.
Representing the Elements of GF($2^k$)

- The polynomial representation of the Galois field of GF($2^k$) is based on the arithmetic of polynomials whose coefficients are from the base field GF(2) and whose degree is at most $k - 1$
- The elements of GF($2^k$) is polynomials whose degree is at most $k - 1$ and coefficients from GF(2), that is \{0, 1\}
- Let $a(x), b(x) \in$ GF($2^k$), then they are written as

\[
\begin{align*}
  a(x) &= a_{k-1}x^{k-1} + \cdots + a_1x + a_0 \\
  b(x) &= b_{k-1}x^{k-1} + \cdots + b_1x + b_0
\end{align*}
\]

such that $a_i, b_i \in \{0, 1\}$
Addition and Multiplication in $\text{GF}(2^k)$

- The field addition $c(x) = a(x) + b(x)$ is performed by polynomial addition, where the coefficients are added in $\text{GF}(2)$, therefore,

  $$c(x) = a(x) + b(x) = c_{k-1}x^{k-1} + \cdots + c_1x + c_0$$

  where $c_i = a_i + b_i \pmod{2}$

- On the other hand, the field multiplication is performed by first multiplying the polynomials, which would give a polynomial of degree at most $2k - 2$

- Then, we reduce the product polynomial modulo an **irreducible polynomial** of degree $k$
Therefore, in order to construct a Galois field $\text{GF}(2^k)$, we need an irreducible polynomial of degree $k$.

Irreducible polynomials of any degree exist, in fact, usually there are more than one for a given $k$.

We can use any one of these degree $k$ irreducible polynomials, and construct the field $\text{GF}(2^k)$.

It does not matter which one we choose — we just have to choose one and use that one only.

All such $\text{GF}(2^k)$ fields are isomorphic to one another.
Irreducible Polynomials over GF(2)

<table>
<thead>
<tr>
<th>$k$</th>
<th>irreducible polynomials</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$x$</td>
</tr>
<tr>
<td>2</td>
<td>$x^2 + x + 1$</td>
</tr>
<tr>
<td>3</td>
<td>$x^3 + x + 1$</td>
</tr>
<tr>
<td>4</td>
<td>$x^4 + x + 1$</td>
</tr>
<tr>
<td>5</td>
<td>$x^5 + x^2 + 1$</td>
</tr>
<tr>
<td></td>
<td>$x^5 + x^4 + x^3 + x + 1$</td>
</tr>
<tr>
<td>6</td>
<td>$x^6 + x + 1$</td>
</tr>
<tr>
<td></td>
<td>$x^6 + x^4 + x^2 + x + 1$</td>
</tr>
<tr>
<td></td>
<td>$x^6 + x^5 + x^3 + x^2 + 1$</td>
</tr>
<tr>
<td>7</td>
<td>$x^7 + x + 1$</td>
</tr>
<tr>
<td></td>
<td>$x^7 + x^6 + 1$</td>
</tr>
<tr>
<td></td>
<td>$x^7 + x^5 + x^3 + x + 1$</td>
</tr>
<tr>
<td></td>
<td>$x^7 + x^4 + x^3 + x^2 + 1$</td>
</tr>
<tr>
<td></td>
<td>$x^7 + x^5 + x^4 + x^3 + 1$</td>
</tr>
</tbody>
</table>
### Irreducible Polynomials over GF(2)

<table>
<thead>
<tr>
<th>$k$</th>
<th>irreducible polynomials</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>$x^8 + x^4 + x^3 + x + 1$</td>
</tr>
<tr>
<td></td>
<td>$x^8 + x^7 + x^2 + x + 1$</td>
</tr>
<tr>
<td></td>
<td>$x^8 + x^7 + x^6 + x + 1$</td>
</tr>
<tr>
<td></td>
<td>$x^8 + x^6 + x^3 + x^2 + 1$</td>
</tr>
<tr>
<td></td>
<td>$x^8 + x^5 + x^4 + x^3 + 1$</td>
</tr>
<tr>
<td></td>
<td>$x^8 + x^6 + x^5 + x^4 + 1$</td>
</tr>
<tr>
<td>257</td>
<td>$x^{257} + x^{12} + 1$</td>
</tr>
<tr>
<td></td>
<td>$x^{257} + x^{51} + 1$</td>
</tr>
<tr>
<td></td>
<td>$x^{257} + x^{206} + 1$</td>
</tr>
<tr>
<td></td>
<td>$x^{257} + x^{245} + 1$</td>
</tr>
</tbody>
</table>
Construction of $\text{GF}(2^2)$

- $\text{GF}(2^2)$ has $2^2 = 4$ elements: $\{0, 1, x, x + 1\}$
- The field addition is performed by adding the field elements, where the coefficients are added in $\text{GF}(2)$

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>$x$</th>
<th>$x + 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>$x$</td>
<td>$x + 1$</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>$x + 1$</td>
<td>$x$</td>
</tr>
<tr>
<td>$x$</td>
<td>$x$</td>
<td>$x + 1$</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$x + 1$</td>
<td>$x + 1$</td>
<td>$x$</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

- To perform field multiplication in $\text{GF}(2^2)$, we need an irreducible polynomial of degree 2
- There exists only one irreducible polynomial of degree 2 which is $p(x) = x^2 + x + 1$
Multiplication in $\mathbb{GF}(2^2)$

- Multiplication in $\mathbb{GF}(2^2)$ is performed by first multiplying the given input polynomials, where the coefficient arithmetic is performed in $\mathbb{GF}(2)$, and reducing the result mod $p(x) = x^2 + x + 1$
- For example, if $a(x) = x$ and $b(x) = x + 1$, then we have
  \[ c(x) = x \cdot (x + 1) = x^2 + x \]
- We now divide $c(x)$ by $p(x)$ and find the remainder $r(x)$ as
  \[
  \begin{array}{c}
  \phantom{00}x^2 + x \\
  x^2 + x + 1 \\
  \hline
  1
  \end{array}
  \]
  \[
  \begin{array}{c}
  \phantom{00}x^2 + x + 1 \\
  \hline
  1
  \end{array}
  \]

  Since $r(x) = 1$, the product of $x$ and $x + 1$ in $\mathbb{GF}(2^2)$ is equal to 1.
We only need perform reduction mod $p(x)$ if the degree of the resulting polynomial is more than 1.

Reduction mod $p(x)$ brings down the degree to $k$, and therefore, finding an element of $\text{GF}(2^k)$ which are polynomials whose coefficients are in $\text{GF}(2)$ and the degree at most $k - 1$.

If we continue with the construction of the multiplication table for $\text{GF}(2^2)$, we find the following:

<table>
<thead>
<tr>
<th>×</th>
<th>0</th>
<th>1</th>
<th>$x$</th>
<th>$x + 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>$x$</td>
<td>$x + 1$</td>
</tr>
<tr>
<td>$x$</td>
<td>0</td>
<td>$x$</td>
<td>$x + 1$</td>
<td>1</td>
</tr>
<tr>
<td>$x + 1$</td>
<td>0</td>
<td>$x + 1$</td>
<td>1</td>
<td>$x$</td>
</tr>
</tbody>
</table>
Representing the Elements of $\text{GF}(2^k)$

- An element $a(x)$ of $\text{GF}(2^k)$ is a polynomial of degree at most $k - 1$, with coefficients from $\text{GF}(2)$, as

$$a(x) = a_{k-1}x^{k-1} + \cdots + a_1x + a_0$$

- While the polynomial representation is the natural representation of the elements of $\text{GF}(2^k)$, we can also represent $a(x)$ using the coefficient vector as $(a_{k-1} \cdots a_1 a_0)$

- This is a binary vector, but it should not be confused with binary numbers

- Whenever we perform arithmetic with these vectors, we need to make sure that they are correctly operated on, for example, addition of $a(x)$ and $b(x)$ using their binary vector representation is performed by adding the individual vector bits mod 2.
Construction of $\text{GF}(2^3)$

- $\text{GF}(2^3)$ has $2^3 = 8$ elements:
  $$\{0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1\}$$

- We can represent the field elements more compactly using the binary vectors as $\{000, 001, 010, 011, 100, 101, 110, 111\}$, for example, $011$ represents $x + 1$, $100$ represents $x^2$, and so on.

- The field addition is performed by adding coefficients in $\text{GF}(2)$, which corresponds to bitwise XOR operation.

$$
\begin{array}{r@{}r@{}r@{}r}
011 & \oplus & 110 & = \\
& & & 101 \\
\end{array}
+ \\
\begin{array}{r@{}r@{}r@{}r}
x + 1 & \oplus & x^2 + x & = \\
& & & x^2 + 1 \\
\end{array}
$$
**Addition Table in $GF(2^3)$**

<table>
<thead>
<tr>
<th>+</th>
<th>000</th>
<th>001</th>
<th>010</th>
<th>011</th>
<th>100</th>
<th>101</th>
<th>110</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>000</td>
<td>001</td>
<td>010</td>
<td>011</td>
<td>100</td>
<td>101</td>
<td>110</td>
<td>111</td>
</tr>
<tr>
<td>001</td>
<td>001</td>
<td>000</td>
<td>011</td>
<td>010</td>
<td>101</td>
<td>100</td>
<td>111</td>
<td>110</td>
</tr>
<tr>
<td>010</td>
<td>010</td>
<td>011</td>
<td>000</td>
<td>001</td>
<td>110</td>
<td>111</td>
<td>100</td>
<td>101</td>
</tr>
<tr>
<td>011</td>
<td>011</td>
<td>010</td>
<td>001</td>
<td>000</td>
<td>111</td>
<td>110</td>
<td>101</td>
<td>100</td>
</tr>
<tr>
<td>100</td>
<td>100</td>
<td>101</td>
<td>110</td>
<td>111</td>
<td>000</td>
<td>001</td>
<td>010</td>
<td>011</td>
</tr>
<tr>
<td>101</td>
<td>101</td>
<td>100</td>
<td>111</td>
<td>110</td>
<td>001</td>
<td>000</td>
<td>011</td>
<td>010</td>
</tr>
<tr>
<td>110</td>
<td>110</td>
<td>111</td>
<td>100</td>
<td>101</td>
<td>010</td>
<td>011</td>
<td>000</td>
<td>001</td>
</tr>
<tr>
<td>111</td>
<td>111</td>
<td>110</td>
<td>101</td>
<td>100</td>
<td>011</td>
<td>010</td>
<td>001</td>
<td>000</td>
</tr>
</tbody>
</table>
To perform multiplication in \( \text{GF}(2^3) \), we need a polynomial of degree 3 over \( \text{GF}(2) \), which we select from the list as \( p(x) = x^3 + x + 1 \)

<table>
<thead>
<tr>
<th>( x \times )</th>
<th>000</th>
<th>001</th>
<th>010</th>
<th>011</th>
<th>100</th>
<th>101</th>
<th>110</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>000</td>
<td>000</td>
<td>000</td>
<td>000</td>
<td>000</td>
<td>000</td>
<td>000</td>
<td>000</td>
</tr>
<tr>
<td>001</td>
<td>000</td>
<td>001</td>
<td>010</td>
<td>011</td>
<td>100</td>
<td>101</td>
<td>110</td>
<td>111</td>
</tr>
<tr>
<td>010</td>
<td>000</td>
<td>010</td>
<td>100</td>
<td>110</td>
<td>011</td>
<td>001</td>
<td>111</td>
<td>101</td>
</tr>
<tr>
<td>011</td>
<td>000</td>
<td>011</td>
<td>110</td>
<td>101</td>
<td>111</td>
<td>100</td>
<td>001</td>
<td>010</td>
</tr>
<tr>
<td>100</td>
<td>000</td>
<td>100</td>
<td>011</td>
<td>111</td>
<td>110</td>
<td>010</td>
<td>101</td>
<td>001</td>
</tr>
<tr>
<td>101</td>
<td>000</td>
<td>101</td>
<td>001</td>
<td>100</td>
<td>010</td>
<td>111</td>
<td>011</td>
<td>110</td>
</tr>
<tr>
<td>110</td>
<td>000</td>
<td>110</td>
<td>111</td>
<td>001</td>
<td>101</td>
<td>011</td>
<td>001</td>
<td>100</td>
</tr>
<tr>
<td>111</td>
<td>000</td>
<td>111</td>
<td>101</td>
<td>010</td>
<td>001</td>
<td>110</td>
<td>100</td>
<td>011</td>
</tr>
</tbody>
</table>

An example: \( 101 \cdot 100 \rightarrow (x^2 + 1) \cdot x^2 = x^4 + x^2 \), then the reduction gives the product as \( x^4 + x^2 = x \pmod{x^3 + x + 1} \) which is 010
The Galois Field GF(3^2)

- We have seen that the elements of GF(3) are \{0, 1, 2\} while its arithmetic is addition and multiplication modulo 3.

- Similar to the GF(2^k) case, in order to construct the Galois field GF(3^k), we need polynomials degree at most \( k - 1 \) whose coefficients are in GF(3).

- For example, GF(3^2) has 9 elements and they are of the form \( a_1x + a_0 \), where \( a_1, a_0 \in \{0, 1, 2\} \), which is given as:

\[
\{0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2\}
\]

- The addition is performed by polynomial addition, where the coefficient arithmetic is mod 3, for example:

\[
(x + 1) + (x + 2) = 2x
\]
Multiplication in GF(3^2)

- In order to perform multiplication in GF(3^2), we need an irreducible polynomial of degree 2 over GF(3).
- This polynomial will be of the form \( x^2 + ax + b \) such that \( a, b \in \{0, 1, 2\} \).
- Note that \( b \neq 0 \) (otherwise, we would have \( x^2 + ax \) which is reducible).
- Therefore, all possible irreducible candidates are:
  - \( x^2 + 1 \), \( x^2 + 2 \), \( x^2 + x + 1 \), \( x^2 + x + 2 \), \( x^2 + 2x + 1 \), \( x^2 + 2x + 2 \).
- A quick check shows that \( x^2 + 1 \) is irreducible.
- The other two irreducible polynomials are \( x^2 + x + 2 \) and \( x^2 + 2x + 2 \).
Multiplication in $\text{GF}(3^2)$

- Multiplication of $a(x)$ and $b(x)$ in $\text{GF}(3^2)$ can be performed using

\[ c(x) = a(x) \cdot b(x) \pmod{x^2 + 1} \]

- For example, $a(x) = x + 1$ and $b = 2x + 1$ gives

\[
\begin{align*}
  c(x) &= (x + 1) \cdot (2x + 1) \pmod{x^2 + 1} \\
  &= 2x^2 + 3x + 1 \pmod{x^2 + 1} \\
  &= 2x^2 + 1 \pmod{x^2 + 1} \\
  &= 2
\end{align*}
\]

- Note in the construction of a Galois field, we select and use only one of the irreducible polynomials
Galois Field $GF(p^k)$

- $GF(p^k)$ consists of $p^k$ elements, which can be represented as polynomials of degree $k - 1$ with coefficients from $GF(p)$
- $GF(p)$ is called the ground field
- In order to perform multiplication, we need an irreducible monic polynomial of degree $k$ whose coefficients are in the ground field

$$p(x) = x^k + a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_1x + a_0$$

- As soon as we obtain such a polynomial, we can perform arithmetic in $GF(p^k)$, that is addition, multiplication, and inversion of the field elements