Theorem 28 (the fundamental theorem of finite fields)
The size of every finite field is a power $q = p^n$ of a prime number p, where $n \in \mathbb{N}$. Furthermore, for every prime power q there exists a finite field with q elements. This field with q elements is unique up to isomorphisms of fields, and it can be realized as $\mathbb{F}_p[t]/g$ for some irreducible polynomial $g \in \mathbb{F}_p[t]$ of degree n.

How would you find an irreducible of a given degree n? For example, for the AES we need $n = 8$.

A naive algorithm:
For a given polynomial $g \in \mathbb{F}_p[t]$ of degree n one could test if it is irreducible by a brute-force

check. Just iterate over all polynomials $f \in \mathbb{F}_p[t]$ with $1 \le \deg f < n$ and check if g is divisible by f. If g is not divisible by any f, then g is irreducible. Otherwise, g is reducible.

In this way, we do about p^n iterations.

This method can be optimized by replacing the condition $1 \le \deg f < n$ with the condition $1 \le \deg f \le \lfloor \frac{n}{2} \rfloor$. For, if g is a product $g = f \cdot h$ and $\deg g = n$, then f or h has the degree at most $n/2$.

One can also do something similar to the sieve of Eratosthenes

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32								

Can we reuse this idea for irreducible polynomials?

$p = 2$ in $\mathbb{Z}_2[t]$

irreducible of degree one: t, $t+1$

irreducible of degree two: t^2+t+1

irreducible of degree three: t^3+t+1, t^3+t^2+1

irreducible of degree four: t^4+t+1, t^4+t^3+1, $t^4+t^3+t^2+t+1$

How do we test if $g = t^8 + t^4 + t^3 + t + 1$ is irreducible? If g had a non-trivial factor, then it would have an irreducible factor of degree at most $d = \left\lfloor \frac{\deg g}{2} \right\rfloor$. We've listed all these factors above. & by calculating the remainders of division of g by these factors, we convince ourselves that g is irreducible.

Remark The (essentially) unique field with $q = p^a$ elements is usually denoted by $\mathbb{F}_q$ or $GF(q)$.

GF abbreviates Galois field.

2.2 Investing linear and affine maps

Let me recall that a map $T: V \to W$ on vector spaces V and W over a field F is called F-linear if $T(\alpha x + \beta y) = \alpha T(x) + \beta T(y)$ holds for all $\alpha, \beta \in F$ and all $x, y \in V$.

Def If $T: V \to W$ is a linear map, then the map $S: V \to W$ of the form $S(x) = T(x) + a$, where $a \in W$, is called affine.

We want to understand how to invert linear and affine maps $F^n \to F^n$.

Proposition 29. Let $T : F^n \to F^m$ $(m, n \in \mathbb{N})$ be an F-linear map, where F is a field. Then there exist values $a_{ij} \in F$ $(i = 1 \dots m$ and $j = 1 \dots n)$ such that for the input $x = (x_j)_{j=1\dots n} \in F^n$ the output $y = T(x)$ is the vector $y = (y_i)_{i=1\dots m}$ is given by

$$y_i = \sum_{j=1}^{n} a_{ij} x_j .$$

Proof: Let's consider vectors $e_1, \dots, e_n \in F^n$ such that the i-th component of e_i is 1, whereas all the other components are 0.

$$e_1 = (1, 0, \dots, 0),$$
$$e_2 = (0, 1, 0, \dots, 0),$$
$$\vdots$$
$$e_n = (0, \dots, 0, 1).$$

We decompose $x = (x_1, \dots, x_n) \in K^n$ as $x = x_1 e_1 + x_2 e_2 + \dots + x_n e_n$. Then

$$T(x) = T(x_1 e_1 + x_2 e_2 + \dots + x_n e_n)$$
$$= x_1 \underbrace{T(e_1)}_{\| a_1} + x_2 \underbrace{T(e_2)}_{\| a_2} + \dots + x_n \underbrace{T(e_n)}_{\| a_n}$$

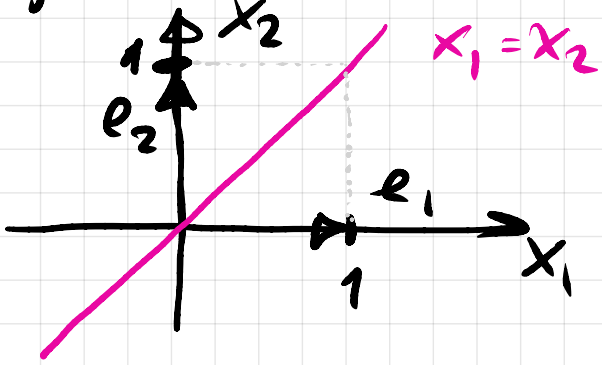
So, $y = T(x)$ satisfies $y = x_1 a_1 + \dots + x_n a_n$.

Let $a_j = (a_{ij})_{i=1,\dots,m} \in K^m$. Then, for $y = (y_i)_{i=1,\dots m}$, we have

$$y_i = x_1 a_{i1} + x_2 a_{i2} + \dots + x_n a_{in}$$

$$= \sum_{j=1}^{n} a_{ij} x_j \,. \qquad \square$$

Example for $F = \mathbb{R}$, let's consider the orthogonal projection onto the line given by $x_1 = x_2$.



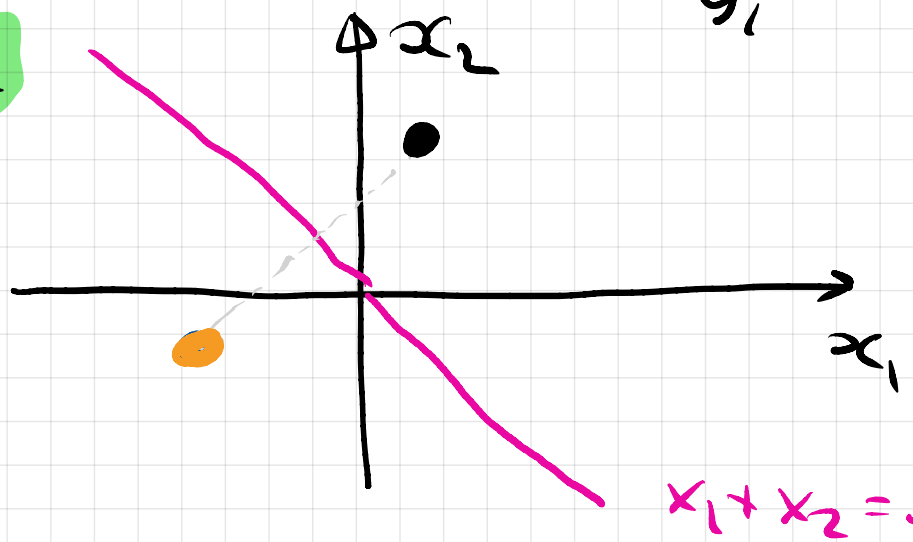
$T(x_1, x_2)$ is the orthogonal projection of (x_1, x_2) onto the line given by $x_1 = x_2$

$$T(x_1, x_2) = T(x) = T(x_1 e_1 + x_2 e_2)$$
$$= x_1 T(e_1) + x_2 T(e_2)$$

$$T(e_1) = (1/2, 1/2)$$
$$T(e_2) = (1/2, 1/2)$$

$$\Rightarrow T(x) = x_1 \cdot \left(\frac{1}{2}, \frac{1}{2}\right) + x_2 \cdot \left(\frac{1}{2}, \frac{1}{2}\right)$$
$$= \left(\underbrace{\frac{1}{2}x_1 + \frac{1}{2}x_2}_{y_1}, \underbrace{\frac{1}{2}x_1 + \frac{1}{2}x_2}_{y_2}\right).$$

Example



Reflection with respect to the line given by the equation $x_1 + x_2 = 0$ (the field is $\mathbb{R}$).

$$T: \mathbb{R}^2 \to \mathbb{R}^2$$

$$y = T(x) = x_1 T(e_1) + x_2 T(e_2) = x_1 (0,-1) + x_2 (-1,0)$$

$$T(e_1) = -e_2 = (0,-1)$$
$$T(e_2) = -e_1 = (-1,0)$$
$$= (-x_2, -x_1)$$

Remark A table of values $a_{ij} \in F$ in a field F with $i = 1, \dots m$ and $j = 1, \dots n$ is called a matrix of size $m \times n$ over F. The set of all such matrices ($m \times n$ with entries in F) is denoted as $F^{m \times n}$;

m is the number of rows and n is the

number of columns. For example,

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \end{bmatrix} \in \mathbb{Q}^{2\times 3}.$$

In linear algebra, one frequently prefers to interpret F^n as $F^{n\times 1}$, that is elements of F^n are viewed as columns.

So, instead of $(2,3,4)$ one could also write $\begin{bmatrix} 2 \\ 3 \\ 4 \end{bmatrix}$.

For a matrix $A = (a_{ij})_{\substack{i=1,\dots m \\ j=1,\dots n}} \in F^{m\times n}$

and a vector $x = (x_j)_{j=1,\dots n} \in F^n$

one defines a matrix-vector multiplication

es $y = A \cdot x$ with $y = (y_i)_{i=1 \dots m}$

such that $y_i = \sum_{j=1}^{n} a_{ij} x_j$.

So, every linear transformation

$T : F^n \to F^m$ can be defined

by $T(x) = A \cdot x$, where $A \in F^{m \times n}$.

Example

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 1 \cdot x_1 + 2 \cdot x_2 + 3 \cdot x_3 \\ 2 \cdot x_1 + 3 \cdot x_2 + 4 \cdot x_3 \end{bmatrix}$$

This matrix gives us a transformation from $\mathbb{Q}^3$ to $\mathbb{Q}^2$.

Definition Fo. two matrices

$$A = (a_{ij})_{\substack{i=1,\dots m \\ j=1,\dots n}} \in F^{m \times n}$$ and

$$B = (b_{jk})_{\substack{j=1,\dots n \\ k=1,\dots s}} \in F^{n \times s}$$

over a field F the product $A \cdot B$ is defined as the matrix

$$C = (c_{ik})_{\substack{i=1,\dots m \\ k=1,\dots s}} \in K^{m \times s}$$

with

$$c_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk}$$