Extension d'un corps fini

Comme pour $\mathbb{C} = \mathbb{R}(i)$ avec i racine de $x^2+1=0$
x^2+1 n'a pas de racine dans $\mathbb{R}$.

On part d'un corps de base $\mathbb{F}_2 = (\{0,1\}, +, \cdot)$
Un corps a des éléments de base $\{0,1\}$ et 2 opérations $+, \cdot$ et vérifie que tout élément a un opposé pour $+$ et un inverse pour $\cdot$.
et d'un polynôme irréductible comme x^3+x+1
Un polynôme est irréductible s'il n'a pas d'autres diviseurs que 1 et lui même dans $\mathbb{F}_2[x]$. Ni 0 ni 1 ne sont racine
On construit alors une extension de $\mathbb{F}_2[x]/_{x^3+x+1} \simeq \mathbb{F}_8$ corps à 8 éléments

0	1	x	$1+x$	x^2	x^2+1	x^2+x	x^2+x+1	← polynome
000	001	010	011	100	101	110	111	← vect. binaire

Le polynôme $x^3+x+1=0$ définit une relation de récurrence grâce à laquelle on peut définir les opérations de $\mathbb{F}_8$

$$x^3 = x+1$$

	0	1	x	$1+x$	x^2	$1+x^2$	x^2+x	$1+x+x^2$
0	0	1	x	$1+x$	x^2	$1+x^2$	x^2+x	$1+x+x^2$
1	1	0	$1+x$	x	$1+x^2$	x^2	$1+x+x^2$	$x+x^2$
x	x	$1+x$	0					
$1+x$								
x^2								
$1+x^2$								
$x+x^2$								
$1+x+x^2$								

	0	1	x	$1+x$	x^2	$1+x^2$	x^2+x	$1+x+x^2$
0	0	0	0	0	0	0	0	0
1	0	1	x	$1+x$	x^2	$1+x^2$	x^2+x	$1+x+x^2$
x	0	x	x^2	$x+x^2$				
$1+x$	0	$1+x$	$x+x^2$					
x^2	0	x^2						
$1+x^2$	0	$1+x^2$						
$x+x^2$	0	$x+x^2$						
$1+x+x^2$	0	$1+x+x^2$						

On a défini un corps à 8 éléments vus comme des polynômes de degré <3 ou des mots binaires de longueur 3 en utilisant

0	1	x	$1+x$	x^2	x^2+1	x^2+x	x^2+x+1	← polynôme
000	001	010	011	100	101	110	111	← vect. binaire

C'est ce que vous ferez en TD avec un polynôme de degré 2 (donc pour construire un corps à 2^2 éléments)

Il faudrait aussi vérifier que x^3+x+1 est irréductible
- ni 0 ni 1 ne sont racine
- aucun des polynôme de degré inférieur ne le divise

Calculons par exemple $x^3+x+1 \div x^2+x$

x^3+x+1 | x^2+x

x^3+x^2 | $x+1$

x^2+x+1

x^2+x

1 ← le reste n'est pas nul

le reste est 1 donc

x^2+x inverse de $x+1$ mod x^3+x+1

$x^3+x+1 = 1+(x^2+x)(x+1)$ ↘ mod x^3+x+1

$1 = (x^2+x)(x+1)$

$x^3+\cancel{x^2}+\cancel{x^2}+x$

↓ ↓

$\cancel{x}+1 \quad + \quad \cancel{x} = 1$