

TP4

TP4

```
pretty_print_default()
```

```
p = 3
A = PolynomialRing(GF(p), 'X')
X = A.gen()
A
```

$\mathbf{F}_3[X]$

```
P = X^5+X^4+X^2+1
P
```

$X^5 + X^4 + X^2 + 1$

```
m = P.degree()
m
```

5

```
K = GF(p^m, name='alpha', modulus=P)
alpha = K.gen()
K
```

$\mathbf{F}_{3^5}$

```
K.cardinality()
```

243

```
n = alpha.multiplicative_order()
n
```

242

```
T = [alpha^i for i in range(0,n)]
```

```
def LD(x):
    if x not in K:
        print 'erreur: x non dans K'
        return None
    if x == 0:
        print 'erreur: x=0'
        return None
    return T.index(x)
```

```
F = lambda i: mod(p*i,n)
```

```
def Orb(i):
    if i not in IntegerRange(0,n):
        print 'erreur: i non compris entre 0 et n-1'
        return None
    Omega = []
```

```

j = i
while True:
    Omega.append(j)
    j = F(j)
    if j in Omega:
        break
return Omega

```

```
Orb(6)
```

```
[6, 18, 54, 162, 2]
```

```
delta = 8
delta
```

```
8
```

```
L = [Orb(i) for i in range(1,delta)]
L
```

```
[[1, 3, 9, 27, 81], [2, 6, 18, 54, 162], [3, 9, 27, 81, 1], [4, 12, 36, 108, 82], [5, 15, 45, 135, 163], [6, 18, 54,
```

```
J = list(Set(flatten(L)))
J
```

```
[1, 2, 3, 4, 5, 6, 135, 9, 12, 15, 81, 18, 83, 21, 27, 162, 163, 36, 7, 108, 45, 82, 54, 189, 63]
```

```
rac = [T[i] for i in J]
rac
```

```
 $[\alpha, \alpha^2, \alpha^3, \alpha^4, 2\alpha^4 + 2\alpha^2 + 2, \alpha^4 + 2\alpha^3 + \alpha^2 + 2\alpha + 1, \alpha^4 + \alpha, \alpha^4 + 2\alpha^2 + 2\alpha, \alpha^4 + \alpha^3 + 2\alpha^2 -$ 
```

```
g = prod([X-r for r in rac])
g
```

```
 $X^{25} + X^{24} + X^{22} + X^{21} + X^{20} + 2X^{18} + 2X^{17} + 2X^{16} + 2X^{15} + X^{13} + 2X^{12} + X^{10} + 2X^8 +$ 
```

```
k = n - g.degree()
k
```

```
217
```

```
p^k
```

```
343014338185106544799976221490560728408063812407121477134594544147051677470701808
```