# Problème d'Algèbre de l'Agrégation 2007 et traduction pour Xcas

Renée De Graeve
Bernard Parisse

1er juin 2007

Les 4 premières parties sont largement indépendantes

## 1 Partie I

*Soit G un groupe multiplicatif de cardinal fini $N \in \mathbb{N}^*$.*

1. *Justifier le fait que $a^{N-1}$ est l'inverse de a dans G.*
   Si $a = 1$ c'est évident.
   Soit $a \neq 1$.
   Les $N+1$ éléments $1, a, a^2 ... a^{N-1}, a^N$ sont dans $G$, donc il existe $p$ et $q$ vérifiant $0 \leq p < q \leq N$ tel que $a^p = a^q$ c'est à dire, il existe $0 < h = q - p \leq N$ tel que $a^h = 1$.
   Le sous groupe engendré par $a$ est donc d'ordre $h$. On sait que l'ordre d'un sous groupe divise l'ordre d'un groupe donc $h$ divise $N$ c'est à dire $N = k * h$ avec $k \in \mathbb{N}^*$ donc $a^N = (a^h)^k = 1$. On montre ainsi que $a^{N-1}$ est l'inverse de $a$ dans $G$.
2. *On écrit la décomposition de $N-1$ en base 2 sous la forme :*

$$N - 1 = \sum_{i=0}^{k} x_i 2^i, \quad k \in \mathbb{N}, x_i \in \{0,1\} \text{ pour } i \in [0,k], x_k \neq 0.$$

*On considère les suites finies $(a_i)_{0 \leq i \leq k+1}$ et $(b_i)_{0 \leq i \leq k+1}$ définies par :*

$$a_0 = 1, b_0 = a, \quad \text{pour } i \in [0,k],\ a_{i+1} = a_i b_i^{x_i},\ b_{i+1} = b_i^2.$$

   (a) *Démontrer que $a_{k+1}$ est l'inverse de a dans G.*
   On a :

$$\begin{aligned} a_{k+1} &= a_k {b_k}^{x_k} \\ a_k &= a_{k-1} {b_{k-1}}^{x_{k-1}} \\ .... & \\ a_2 &= a_1 b_1^{x_1} \\ a_1 &= a_0 b_0^{x_0} \end{aligned}$$

   Donc puisque $a_0 = 1,\ b_0 = a$ et $b_{i+1} = b_i^2$ on a :

$$a_1 = a^{x_0} \text{ et } b_1 = a^2, \quad a_2 = a^{x_0} b_1^{x_1} = a^{x_0} (a^2)^{x_1} = a^{x_0 + 2x_1} \text{ et } b_2 = a^4 = a^{(2^2)}$$

Supposons $a_p = a^{x_0+2x_1+\ldots 2^{p-1}x_{p-1}}$ et $b_p = a^{(2^p)}$, alors :

$$a_{p+1} = a_p b_p{}^{x_p} = a^{x_0+2x_1+\ldots 2^{p-1}x_{p-1}} a^{(2^p)x_p} = a^{x_0+2x_1+\ldots 2^p x_p}$$

On a donc montré par récurrence que :

$$a_{k+1} = a^{x_0+2x_1+\ldots 2^k x_k} = a^{N-1}$$

(b) *En déduire un algorithme de calcul de $a^{-1}$ et préciser son coût dans le pire des cas.*
On écrit tout d'abord `inversG` une fonction `Xcas` qui traduit l'algorithme :

```
//calcul l'inverse de a dans un groupe mult de cardinal N
inversG(a,N):={
 local b,x,N1;
 N1:=N-1;
 b:=a;
 a:=1;
 while (N1!=0) {
  x:=irem(N1,2);
  N1:=iquo(N1,2);
  a:=a*b^x;
  b:=b^2;
 }
 return a;
}
```

Dans ce programme, le problème est que l'on utilise une fonction puissance lorsque l'exposant est 0,1 ou 2. Il est donc préférable de ne faire que des multiplications et d'écrire `inverseG` :

```
//calcul l'inverse de a dans un groupe mult de cardinal N
inverseG(a,N):={
 local b,N1;
 N1:=N-1;
 b:=a;
 a:=1;
 while (N1!=0) {
  if (irem(N1,2)) a:=a*b;
  b:=b*b;
  N1:=iquo(N1,2);
 }
 return a;
}
```

`inverseG(a,n)` est en fait le calcul dans un groupe $G$ multiplicatif de $a^{n-1}$. On peut écrire plus généralement, lorsque $G$ est le groupe des éléments inversibles de $\mathbb{Z}/p\mathbb{Z}$ ayant $n = \text{euler}(p)$ éléments, la fonction `puissmod(a,k,p)` qui calcule $a^k$ mod $p$ (c'est la fonction interne `powmod` de `Xcas`) :

```
puissmod(a,k,p):={
 local b;
 b:=a;
```

```
 a:=1;
 k:=irem(k,euler(p));
 while (k!=0) {
  if (irem(k,2)) a:=irem(a*b,p);
  b:=irem(b*b,p);
  k:=iquo(k,2);
 }
 return a;
}
```

Si on ne tient pas compte du calcul de `irem(N,2)` et de `iquo(N,2)` et, si on fait $k$ fois la boucle, on fait $2*k$ multiplications dans le pire des cas lorsque $N-1=2^{k+1}-1$ i.e. lorsque $k=\log_2(N)-1$, donc

**On fait** $2*\log_2(N)-2$ **multiplications.**

Pour ne pas avoir dans la suite du problème à réécrire une fonction `puissance` pour chaque groupe $G$, on va écrire une fonction `puissrapide` qui calcule $a^k$ avec comme paramètres un élément $a$ du groupe $G$, $k$ un entier, `mult` le nom de la loi multiplicative utilisée dans $G$, `unit` l'unité de $G$, et `ordre` le cardinal de $G$ s'il est connu ou 0 s'il ne l'est pas (en effet dans `Xcas`, `irem(n,0)=n`).

```
puissrapide(a,k,mult,unit,ordre):={
 local b;
 b:=a;
 a:=unit;
 k:=irem(k,ordre);
 while (k!=0) {
  if (irem(k,2)) a:=mult(a,b);
  b:=mult(b,b);
  k:=iquo(k,2);
 }
 return a;
}
```

Ainsi, pour chaque valeur de $p$, par exemple $p=71$, on définit la loi de multiplication dans $\mathbb{Z}/p\mathbb{Z}$ :

```
multmod71(a,b) :=irem(a*b,71);
```

On tape pour calculer, par exemple, $47^{750}$ dans $\mathbb{Z}/71$
*mathbbZ* :

```
puissrapide(47,750,multmod71,1,0)
```

Ou on tape puisque l'ordre du groupe multiplicatif de $\mathbb{Z}/71$
*mathbbZ* est 70 :

```
puissrapide(47,750,multmod71,1,70)
```

Ou on tape :

```
puismod(47,750,71)
```

ou encore avec la fonction interne de `Xcas` :

```
powmod(47,760,71)
```

On obtient :

```
32
```

On tape pour calculer, par exemple, $5^{71}$ dans $\mathbb{Z}/148\,\mathbb{Z}$ :

```
multmod148(a,b) :=irem(a*b,148);
puissrapide(5,71,multmod148,1,0)
```

Ou on tape :

```
puismod(5,71,148)
```

On obtient :

```
89
```

3. *Exemple avec G le groupe des éléments inversibles de* $\mathbb{Z}/148\,\mathbb{Z}$

   (a) *Déterminer le cardinal N de G.*
   $a \in G$ est inversible si $a$ est premier avec $148 = 4 * 37$.
   $G$ est donc l'ensemble des éléments impairs de 1 à 147 auxquels on enleve 37 et 3*37=111.
   $N$ vaut donc 74-2=72.
   On vérifie avec la commande `euler` de Xcas (`euler(148)` renvoie 72).

   (b) *Démontrer que 5 est un élément de G et déterminer son inverse par la méthode de la question I.2.*
   5 est premier avec 148 donc 5 est inversible.
   On tape pour calculer $5^{72-1}$ :

```
puissmod(5,71,148)
```

   Ou on tape :

```
puissrapide(5,71,multmod148,1,72)
```

   On obtient :

```
89
```

   On vérifie :

```
89*5=445=4*148+1
```

   (c) *Donner une autre méthode pour calculer cet inverse.*
   Puisque 5 et 148 sont premiers entre eux, on sait, d'après l'identité de Bézout, qu'il existe des entiers relatifs $u$ et $v$ tels que $5 * u + 148 * v = 1$.
   On tape :

```
iegcd(5,148)
```

   On obtient :

```
[-59,2,1]
```

   On a donc $-59 * 5 + 2 * 148 = 1$ et comme $-59 + 148 = 89$ on a :

$$89 * 5 - 3 * 148 = 1$$

   ainsi l'inverse de 5 est 89 dans $\mathbb{Z}/148\,\mathbb{Z}$.

## 2 Partie II

*Soient $\pi$ un élément d'un groupe multiplicatif G, e un entier relatif et $\alpha = \pi^e$. On considère l'application $f_\alpha$ de $\mathbb{Z} \times G$ dans $G^2$ définie par $f_\alpha(k,\tau) = (\pi^k, \tau\alpha^k)$.*

1. (a) *Exhiber une fonction $\phi_e$ de $G^2$ dans G, ne dépendant que de e et vérifiant :*

$$\forall (k,\tau) \in Z \times G \quad \tau = \phi_e o f_\alpha(k,\tau)$$

On a :

$$(\pi^k, \tau\alpha^k) = (\pi^k, \tau(\pi^e)^k) = (\pi^k, \tau(\pi^k)^e)$$

Pour $(a,b) \in G^2$, on pose :

$$\phi_e(a,b) = b * (a^e)^{-1}$$

où $(a^e)^{-1}$ désigne l'inverse de $a^e$ dans $G$. On a ainsi :

$$\phi_e o f_\alpha(k,\tau) = \phi_e(\pi^k, \tau(\pi^k)^e) = \tau$$

(b) *On suppose G et $\pi$ connu de tous. La personne* **A** *garde secret e et rend public $\alpha = \pi^e$ et $f_\alpha$.*
*On cherche une procédure permettant à chacun d'envoyer à* **A** *un message crypté sous la forme d'éléments $\tau$ de G telle que la connaissance de e suffise à retrouver le message initial.*
*Justifier le fait que si* **A** *recoit la suite $(\lambda_n, \mu_n) = f_\alpha(k_n, \tau_n)$ avec $(k_n, \tau_n) \in (Z, G)$ alors* **A** *peut décrypter cette suite grâce à $\phi_e$.*
Pour coder le message $\tau$ il suffit de connaitre $\alpha$ et $\pi$ : on calcule et on envoie $f_\alpha(k,\tau)$ pour un $k$ que l'on choisit arbitrairement. La personne qui reçoit le message connait $e$ donc connait $\phi_e$. Elle est donc capable de calculer $\phi_e o f_\alpha(k,\tau) = \tau$ donc de connaitre le message $\tau$.

2. *Dans cette question G est le groupe $\mathbb{F}_{29}^*$ du corps à 29 éléments et les nombres $\pi = 2$ et $\alpha = 18$ sont supposés public.*
*Chaque associé sait que les entiers (1,2...26,27,28) modulo 29 représentent les caractères (A,B..Z, ' ',',.') (27 représente l'espace et 28 représente le point de fin de phrase.)*

(a) *Sachant que* **A** *décrypte son message en calculant $a^{17}$ mod 29 lorsque $a \in (1,2...26,27,28)$, conjecturer la valeur de e et la contrôler grâce à $\alpha$.*
Pour décrypter le message, il faut savoir calculer l'inverse de $a^e$ dans $\mathbb{F}_{29}^*$ lorsque $a$ appartient à (1,2...26,27,28).
$G$ a 28 élements donc $a^{28} = 1$ mod 29 donc puisque $a^{28} = a^{17+11} = a^{17} * a^{11} = 1$ mod 29 on peut penser que $e = 11$
On vérifie, pour cela on calcule $\pi^e = 2^{11}$ mod 29 et on tape :

```
puissmod(2,11,29)
```

On obtient :

```
18
```

ce qui donne bien la valeur de $\alpha$.

(b) *Décrypter le message suivant (on donne la suite des couples $(\lambda_u, \mu_i)$) :*
*(16,17),(18,24),(28,22),(17,21),(23,23),(24,8).*
Pour décrypter un message on écrit les fonctions servant au décodage :

– `decod28(p)` qui a un nombre $p$ entre 1 et 28 retourne le caractère correspondant.
– `decode(a,b)` qui est la fonction $\phi_e$ ou encore $b * a^{17}$ dans $\mathbb{F}_{29}^*$.
– `decodel(L)` qui décode une liste de couples, représentés par une liste de 2 éléments, autrement dit une matrice à 2 colonnes.

```
decod28(p):={
 local r;
 r:=irem(p,29);
 if (r==0) return "erreur";
 if (r<27) return char(p+64);
 if (r==27) return char(32);
 return char(46);
}:;

decode(a,b):={
 return irem(b*powmod(a,17,29),29);
}:;

decodel(L):={
 local s,M;
 s:=size(L);
 M:=NULL;
 for (k:=0;k<s;k++) {
  M:= M,decod28(decode(op(L[k])));
 }
 return M;
}:;
```

Puis on tape :

```
L :=[[16,17],[18,24],[28,22],[17,21],[23,23],[24,8]]
                    decodel(L)
```

On obtient :

```
["C","O","G","I","T","O"]
```

# 3 Partie III

*Dans cette partie le corps de base est le corps fini $\mathbb{F}_{16}$ à 16 éléments, unique à un isomorphisme près.*

1. (a) *Comment peut-on construire $\mathbb{F}_{16}$ ?*

   Pour construire $\mathbb{F}_{16}$, on considère les polynômes à coefficients dans $\mathbb{Z}/2\mathbb{Z}$ modulo un polynôme irreductible à coefficients dans $\mathbb{Z}/2\mathbb{Z}$ de degré 4. $\mathbb{F}_{16}$ est donc composé de quadruplets de nombres valant 0 ou 1 et représentant un polynôme de degré 3 à coefficients dans $\mathbb{Z}/2\mathbb{Z}$.

   On choisit donc un polynôme $P[X]$ de degré 4 et irréductible dans $\mathbb{Z}/2\mathbb{Z}$ et on identifie $\mathbb{F}_{16}$ à $(\mathbb{Z}/2\mathbb{Z})[X]/P[X]$

   Avec `Xcas`, on tape :

   ```
   F16 :=GF(2,4,['t','F16'])
   ```

ce qui définit le corps `F16`, la variable $t$ sert à représenter les polynômes à coefficients dans $\mathbb{Z}/2\mathbb{Z}$. On obtient :

```
GF(2,t^4+t^3+1,[t,F16],undef)
```

ce qui signifie que Xcas utilise comme polynôme irréductible $t^4+t^3+1$ (c'est le même que celui du sujet, sinon il aurait fallu spécifier le polynôme irréductible choisi lors de la construction du corps par l'instruction `GF`). Ainsi `F16(t^4)` renvoie `F16(t^3+1)`, et `F16(t^5)` renvoie `F16(t^3+t+1)` obtenus par division euclidienne dans $\mathbb{Z}/2\mathbb{Z}$ de $t^4$ ou $t^5$ par $t^4+t^3+1$

(b) *Démontrer que le groupe multiplicatif $\mathbb{F}_{16}^*$ est formé des puissances successives d'un élément $\omega$ vérifiant $\omega^4+\omega^3+1=0$.*

On cherche l'ordre du groupe engendré par $\omega=\mathbb{F}_{16}(t)$ c'est-à-dire des restes de $t^k$ par $t^4+t^3+1$. Comme on sait que l'ordre du groupe multiplicatif $\mathbb{F}_{16}^*$ est 15, cet ordre est un diviseur de 15, donc 5 ou 15 (visiblement ce n'est pas 1 ni 3 !). On calcule donc le reste de $t^5$ par $t^4+t^3+1$, ce n'est pas 1 donc $\omega$ est bien d'ordre maximal 15.

Remarques :

- l'instruction `GF` de Xcas renvoie toujours un polynôme irréductible primitif, c'est-à-dire que l'ordre du groupe engendré par $t$ est l'ordre du groupe multiplicatif.
- Pour former `F16`, on rajoute à ces 15 èléments, l'élément `F16(0)` qui est le zéro de $\mathbb{F}_{16}$.

(c) *Démontrer que $\omega,\omega^2,\omega^4,\omega^8$ sont les racines du polynôme $X^4+X^3+1$ dans $\mathbb{F}_{16}$.*

En caractéristique 2, l'application $\phi(x)=x^2$ vérifie $\phi(x+y)=\phi(x)+\phi(y)$, donc :

$$\phi(P(X))=\phi(X^4+X^3+1)=\phi(X^4)+\phi(X^3)+1=\phi(X)^4+\phi(X)^3+1=P(\phi(X))$$

Donc, comme $\omega$ est racine de $P=X^4+X^3+1$, il en est de même de $\phi(\omega)=\omega^2,\phi(\omega^2)=\omega^4,\phi(\omega^4)=\omega^8$.

Avec `Xcas` on tape :

```
w :=F16(t)
P(x) :=x^4+x^3+1
seq(P(w^(2^k)),k,0,3)
```

On obtient :

```
[F16(0),F16(0),F16(0),F16(0)]
```

(d) *Démontrer que la famille $(\omega,\omega^2,\omega^4,\omega^8)$ est une base de $\mathbb{F}_{16}$ sur $\mathbb{F}_2$.*

On a $\omega^4=\omega^3+1$ et comme la somme des racines de $X^4+X^3+1$ vaut 1, on en déduit que $\omega^8=1+\omega+\omega^2+\omega^4=\omega+\omega^2+\omega^3$. On écrit en ligne les coordonnées de cette famille dans la base canonique $1,\omega,\omega^2,\omega^3$, on trouve

$$\begin{pmatrix} 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 1 & 0 & 0 & 1\\ 0 & 1 & 1 & 1 \end{pmatrix}$$

On échange la ligne 3 et la ligne 1, puis on ajoute à la ligne 4 les lignes 2 et 3 à la ligne 4 pour obtenir une matrice triangulaire.

Avec Xcas, on peut utiliser l'instruction `rref(M%2)` où `M` désigne la matrice ci-dessus.

On peut aussi faire un raisonnement un peu plus général : la famille a le bon nombre d'éléments, il suffit de montrer que c'est une famille libre. Soit

$$a\omega + b\omega^2 + c\omega^4 + d\omega^8 = 0$$

une relation linéaire où $a,b,c,d \in \mathbb{Z}/2$ est non identiquement nul. On applique à cette relation $\phi$ qui est linéaire sur le $\mathbb{Z}/2$-espace vectoriel $\mathbb{F}_{16}$, puis à nouveau $\phi$ et $\phi$. On obtient un système linéaire de 4 équations où $a,b,c,d$ subissent une rotation, en faisant la somme des 4 équations, on montre que $a+b+c+d$ est nul. Donc le nombre de 1 est pair. Il ne peut valoir 4 (la somme des racines est 1), ni 2 (les racines sont distinctes 2 à 2), donc vaut 0.

2. (a) *Soit $a \in \mathbb{F}_{16}$. Résoudre dans $\mathbb{F}_{16}$ l'équation $x^5 = a$, en discutant selon les valeurs de a.*
On sait que pour tout $x \in \mathbb{F}_{16}^*$, on a $x^{15} = 1$ donc si $x^5 = a$ admet une solution, alors $a^3 = 1$ dont les solutions sont les $\omega^{5k}$ pour $k = 0,1,2$. Les racines de l'équation $x^5 = \omega^{5k}$ sont $\omega^{k+3l}$ pour $l = 0,1,2,3,4$.

   (b) *Démontrer qu'il existe quatre éléments $\gamma \in \mathbb{F}_{16}$ tels que $\gamma, \gamma^2, \gamma^4, \gamma^8$ est une base de $\mathbb{F}_{16}$ sur $\mathbb{F}_2$ telle que le produit de 2 de ses éléments appartient à la base ou est égal à 1.*
*Expliquer rapidement pourquoi les calculs dans $\mathbb{F}_{16}$ sont plus faciles dans une telle base.*
On choisit l'une des 4 solutions différentes de 1 de $x^5 = 1$ comme valeur de $\gamma$, en effet si $\gamma^5 = 1$ avec $\gamma \neq 1$ on a $\gamma^4 + \gamma^3 + \gamma^2 + \gamma + 1 = 0$. On a alors :

$$\begin{aligned}
\gamma\gamma^2 = \gamma^3 &= \gamma^8 \\
\gamma\gamma^4 = \gamma^5 &= 1 \\
\gamma\gamma^8 = \gamma^9 &= \gamma^4 \\
\gamma^2\gamma^4 = \gamma^6 &= \gamma \\
\gamma^2\gamma^8 = \gamma^{10} &= 1 \\
\gamma^4\gamma^8 = \gamma^{12} &= \gamma^2
\end{aligned}$$

Si $\gamma \neq 1$ est solution de $x^5 = 1$, $\gamma^2, \gamma^4, \gamma^8$ sont les 3 autres solutions de $x^5 = 1$ différentes de 1 puisque $(\gamma^n)^5 = 1$ quelque soit $n$. On peut démontrer comme ci-dessus qu'ils forment une famille libre. On peut aussi faire le calcul, par exemple si $\gamma = \omega^3$ on a :

$$\gamma = t^3, \quad \gamma^2 = t^3 + t^2 + t + 1, \quad \gamma^4 = t + 1, \quad \gamma^8 = t^2 + 1$$

sont les solutions de $x^5 = 1$ différentes de 1. On montre facilement que $[t^3, t^3 + t^2 + t + 1, t^2 + 1, t + 1]$ forment une base de $\mathbb{F}_{16}$ puisque ils sont indépendants et au nombre de 4.
La multiplication est plus rapide dans la base $\gamma, \gamma^2, \gamma^3 = \gamma^8, \gamma^4$ car

$$1 = \gamma^4 + \gamma^3 + \gamma^2 + \gamma$$

on peut donc faire la multiplication avec un algorithme semblable à celui utilisé avec les entiers écrits en base 10.
On écrit le programme `multi(a,b)` qui renvoie les coefficients du produit $a * b$ dans la base $\gamma, \gamma^2, \gamma^3, \gamma^4$ lorsque $a$ et $b$ sont des éléments de $\mathbb{F}_{16}$ donnés par tous leurs coefficients dans cette base :

```
multi(a,b):={
 local c,ci,k,j,p,u;
 c:=[];
```

```
 for (j:=3;j>=0;j--){
  ci:=[0];
  for (k:=3;k>=0;k--){
   ci:=prepend(ci,(a[k] and b[j]));
  }
  for (p:=0;p<=3-j;p++){
   ci:=append(tail(ci),head(ci));
  }
  u:=ci[4];
  for (p:=0;p<4;p++){
    ci[p]:=ci[p] xor u;
  }
  ci[4]:=0;
  c:=append(c,mid(ci,0,4));
 }
 for (j:=3;j>0;j--){
  for (k:=3;k>=0;k--){
   c[j-1,k]:=c[j,k] xor c[j-1,k];
  }
 }
return c[0];
}
```

On tape par exemple :

```
multi([1,0,1,1],[0,1,1,1])
```

On obtient :

```
[0,0,0,1]
```

ce qui veut dire que :

$$(\gamma^4+\gamma^2+\gamma)*(\gamma^3+\gamma^2+\gamma)=\gamma$$

On vérifie en tapant (`c :=w^3` représente $\gamma$) :

```
c :=w^3;
(c^4+c^2+c)*(c^3+c^2+c)
```

On obtient :

```
F16(t^3)
```

**Remarque** : le plus efficace (pour des corps de cardinal petit), c'est de coder les éléments du corps par l'exposant de $\omega$ ou par 15 pour $0_{\mathbb{F}_{16}}$ (représentation dite multiplicative). La multiplication est alors triviale : si l'un des arguments vaut 15, on renvoie 15, sinon on renvoie la somme des exposants modulo 15. Pour l'addition, il faut d'abord passer en représentation additive, où l'élément du corps est codé sur un entier de 4 bits, chaque bit représentant une coordonnée dans la base $\omega^3,\omega^2,\omega,1$. En effet, en représentation additive, l'addition se code par un ou exclusif. Le passage entre les deux représentations se fait par l'intermédiaire d'une table calculée une fois pour toutes (la table se calcule uniquement avec des opérations de décalage et de ou exclusif avec un entier sur 5 bits représentant le polynôme minimal de $\omega$, dans notre cas `0b11001`).

Par exemple, en représentation multiplicative, $\omega^5$ et $\omega^4$ sont représentés respectivement par 5 et 4. Leur produit est $\omega^9$ représenté par $9=5+4 \pmod 1 5$. Pour trouver leur

somme, il faut passer en représentation additive, dans la base $\omega^3, \omega^2, \omega, 1$, l'élément $\omega^5$ est $(1,0,1,1)$, soit `0b1011` en base 2, l'élément $\omega^4$ est $(1,0,0,1)$, soit `0b1001` en base 2, donc la somme de $\omega^5$ et $\omega^4$ est `bitxor(0b1011,0b1001) = 0b0010`, c'est donc $\omega$, reprśenté par 1 en représentation multiplicative.

Ceci se généralise en caractéristique 2, on utilise d'ailleurs souvent $\mathbb{F}_{256}$ car l'élément du corps est alors représenté par un octet.

# 4 Partie IV

*Une cubique sur un corps $\mathbb{K}$ est l'ensemble des points $M=(x,y)\in\mathbb{K}^2$ annulant un polynôme $P$ non nul du 3ième degré en $X$ et $Y$ à coefficients dans $\mathbb{K}$.*
*Cette partie étudie quelques cubiques particulières sur $\mathbb{R}$.*

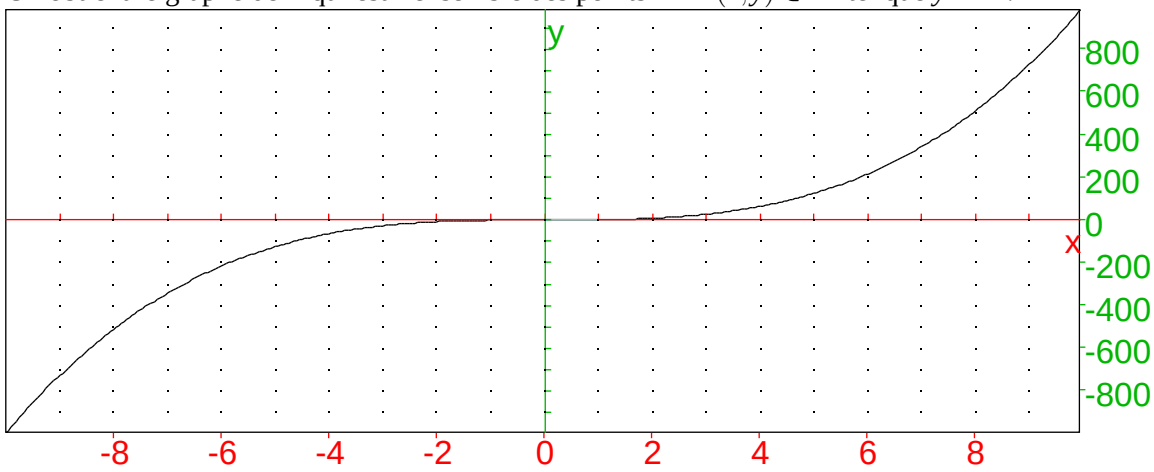
1. Dans cette question, on prend la cubique $\Gamma$ définie par le polynôme :

$$P=X^3-Y\in\mathbb{R}[X,Y]$$

(a) *La tracer à main levée.*
Avec `Xcas`, on tape :

```
plot(x^3)
```

On obtient le graphe de $\Gamma$ qui est l'ensemble des points $M=(x,y)\in\mathbb{R}^2$ tel que $y=x^3$.




On démontre facilement que $x->x^3$ est une bijection de $\mathbb{R}$ dans $\mathbb{R}$ et que $\Gamma$ admet le point (0,0) comme centre de symétrie.

(b) *Démontrer que toute droite coupe $\Gamma$ en exactement 1 ou 3 points en comptant leur multiplicité éventuelle et que lorsqu'il y a 3 points d'intersection notés $A=(x_A,y_A)$, $B=(x_B,y_B)$, $C=(x_C,y_C)$ on a : $x_A+x_B+x_C=0$.*

Les points d'intersection de $\Gamma$ avec la droite d'équation : $ux+vy+w=0$ ont des abscisses qui vérifient :

$$ux+vx^3+w=0$$

L'équation en $x$, $vx^3+ux+w=0$ est une équation du troisième degré à coefficients réels. Cette équation admet donc soit 1 racine réelle et 2 racines complexes conjuguées, soit 3 racines réelles en comptant leur multiplicité éventuelle.
On remarque que le terme en $x^2$ a un coefficient nul donc la somme des racines vaut 0 et donc lorsqu'il y a 3 racines, il y 3 points d'intersection $A=(x_A,y_A)$, $B=(x_B,y_B)$, $C=(x_C,y_C)$ et on a :$x_A+x_B+x_C=0$.

(c) *On note $\Omega$ le point (0,0) de $\Gamma$. Pour tout couple de points $(A,B)$ de $\Gamma$, on note $d$ la droite passant par $A$ et $B$ (ou la tangente en $A$ si $A=B$) et on considère le point $C=\Gamma\cap d$. On définit $A*B$ comme étant le point d'intersection de $\Gamma$ avec la droite $\Omega C$ (ou avec la tangente en $\Omega$ si $\Omega=C$).*
*Démontrer que $(\Gamma,*)$ est un groupe isomorphe à $(\mathbb{R},+)$.*
La droite $d$ passe par $A$ et par $B$ donc recoupe $\Gamma$ en un troisième point $C$ dont l'abscisse $x_C$ vaut :

$$x_C=-(x_A+x_B)$$

Puisque $\Omega$ est un centre de symétrie pour $\Gamma$, la droite $\Omega C$ coupe $\Gamma$ au point $D=A*B$ d'abscisse :

$$x_{A*B}=x_D=-x_C=(x_A+x_B)$$

Soit $f$ la projection des points de $\Gamma$ sur l'axe des $x$ c'est à dire l'application de $(\Gamma,*)$ dans $(\mathbb{R},+)$ définie par : $f(M)=x_M$ pour tout $M\in\Gamma$.
On vérifie que $f$ est bijective, en effet soit $a\in\mathbb{R}$ alors il existe un seul point $A$ de $\Gamma$ tel que $f(A)=a$ : c'est le point de coordonnées $a,a^3$. De plus :

$$f(A*B)=f(D)=x_D=x_A+x_B=f(A)+f(B)$$

Donc $f$ est un isomorphisme du groupe $(\Gamma,*)$ sur $(\mathbb{R},+)$ puisque $f$ est bijective et vérifie $f(A*B)=f(A)+f(B)$.

2. *Reprendre la question 1/ pour $P=X^3-3XY-1\in\mathbb{R}[X,Y]$ et $\Omega=(0,1)$ en précisant à quel groupe usuel est isomorphe $(\Gamma,*)$ dans cet exemple.*
Le graphe de $\Gamma$ de $x^3-3xy-1=0$ admet l'axe des $y$ comme asymptote et admet une branche parabolique de direction l'axe des $y$.
En effet, si $x\neq 0$ on a

$$y=\frac{x^3-1}{3x}=\frac{x^2}{3}-\frac{1}{3x}$$

donc, lorsque x tend vers 0 alors $y$ tend vers l'infini et lorsque x tend vers l'infini alors $y$ tend vers l'infini et $y/x$ tend vers l'infini.
Avec `Xcas`, on tape :

```
G :=plot((x^3-1)/(3x),x=-3..3);
affichage(point(1,0),point_width_3+rouge);
d :=tangente(G,1);
```

Le point (1,0) appartient à $\Gamma$ et la tangente en ce point au graphe de $\Gamma$ est la droite $y=x-1$. Toutes les droites sauf l'asymptote $x=0$ coupent le graphe de $\Gamma$ en 1 ou 3 points, les verticales $x=a$ coupent $\Gamma$ en 1 seul point et les droites $y=ax+b$ coupent $\Gamma$ en un ou trois points $M=(x,y)$ d'abscisse vérifiant :

$$x^3-3ax^2-3bx-1=0$$

On remarque que le produit des racines de ce polynôme est indépendant de $a$ et $b$. Donc, lorsqu'une droite coupe le graphe de $\Gamma$ en trois points $A=(x_A,y_A)$, $B=(x_B,y_B)$ et $C=(x_C,y_C)$ on a :

$$x_A\times x_B\times x_C=1$$

Si $C$ est confondu avec $\Omega$, la droite $\Omega C$ est la tangente en $\Omega$ d'équation $y=x-1$ et $D$ est confondu avec $\Omega$.

Cherchons l'intersection de la droite $\Omega C$ avec $\Gamma$ lorsque $C \neq \Omega$ i.e. lorsque $x_C \neq 1$. La droite $\Omega C$ coupe $\Gamma$ en $\Omega, C$ et $D = A * B$. Les abscisses de ces points d'intersection vérifient :

$$1 \times x_C \times x_D = 1$$

et on sait que $x_A \times x_B \times x_C = 1$, donc

$$x_{A*B} = x_D = 1/x_C = x_A \times x_B$$

On note toujours $f$ la projection des points de $\Gamma$ sur l'axe des $x$, c'est une bijection de $\Gamma$ sur $\mathbb{R}^*$ car pour tout $a \in \mathbb{R}^*$ il existe un seul point $A$ de $\Gamma$ vérifiant $f(A) = a$ : c'est le point de coordonnées $(a, (a^3-1)/(3a))$. De plus

$$f(A*B) = x_A \times x_B = f(A) \times f(B)$$

Donc $f$ est un isomorphisme du groupe $(\Gamma, *)$ sur $(\mathbb{R}^*, \times)$ puisque $f$ est bijective et vérifie $f(A*B) = f(A)f(B)$. Donc $(\Gamma, *)$ est un groupe isomorphe à $(\mathbb{R}^*, \times)$.

3. *On étudie dans la suite des cubiques du plan projectif. Au polynôme P de degré 3, on associe le polynôme homogéne :*

$$\overline{P}(X,Y,Z) = Z^3 P(X/Z, Y/Z)$$

$\Gamma$ *est alors l'ensemble des points du plan projectif dont les coordonnées homogénes* $(X,Y,Z)$ *vérifient* $\overline{P}(X,Y,Z) = 0$.

*Démontrer que que l'intersection de* $\Gamma$ *avec toute droite du plan projectif est constituée d'exactement 1 ou 3 points en comptant les multiplicités éventuelles.*

Une droite $d$ du plan projectif a pour équation $uX + vY + wZ = 0$ avec $u, v, w$ non tous nuls donc l'une des coordonnées s'exprime en fonction des deux autres dite variables principales, donc les variables principales des points d'intersection de $d$ et de la cubique vérifient une équation homogène de degré 3 donc cela donne 1 ou 3 couples de variables principales solutions donc 1 ou 3 points d'intersection.

4. *Soit* $P = y^3 - y^2 - x^2$ *et* $\overline{P} = Y^3 - Y^2Z - X^2Z$.

   (a) *Soit* $\gamma$ *la courbe d'équation* $y^3 - y^2 - x^2 = 0$ *privée du point (0,0). En choisissant un paramétrage de* $\gamma$ *(par exemple en coordonnées polaires) étudier cette courbe et la tracer, en précisant l'allure des branches infinies si il en existe. On ne demande pas les points d'inflexion.*

   Puisque $(0,0)$ est exclu, $y^2 + x^2 \neq 0$ et $y \neq 0$, en effet si $y = 0$ et si $y^3 - (y^2 + x^2) = 0$ alors $x = 0$.

   De plus on voit que $\gamma$ est situé dans le demi-plan $y \geq 1$ (puisque $y^3 \geq y^2$) et $\gamma$ est symétrique par rapport à l'axe des $y$.

   On a en coordonnées polaires $x = r\cos(\theta), y = r\sin(\theta)$ pour $\theta \in ]0, \pi[$, donc

$$y^3 - (y^2 + x^2) = r^3 \sin(\theta)^3 - r^2 = 0$$

   Puisque $r \neq 0$, on en déduit un paramétrage de $\gamma$ en coordonnées polaires :

$$r = 1/\sin(\theta)^3, \quad \text{pour } \theta \in ]0, \pi[$$

   On peut aussi trouver un un paramétrage de $\gamma$ en coordonnées paramétriques en posant pour $t \in \mathbb{R}$, $x = ty$. On a alors puisque $y \neq 0$ :

$$y^3 - (y^2 + x^2) = y^2(y - (1+t^2)) = 0 \Rightarrow y = (1+t^2)$$

Donc un paramétrage de $\gamma$ en coordonnées paramétriques est :

$$x = t(1+t^2), y = (1+t^2) \text{ pour } t \in \mathbb{R}$$

Pour l'étude de la courbe en coordonnées polaires, il suffit de prendre $\theta \in ]0, \pi/2]$ et de compléter par la symétrie d'axe l'axe des $y$.

Pour étudier les branches infinies, en coordonnées polaires, $x$ et $y$ tendent vers l'infini quand $\theta$ vers 0. On a alors $y/x = \tan(\theta)$ qui tend vers 0 quand $\theta$ vers 0. Donc $\gamma$ admet donc une branche parabolique de direction l'axe des $x$.

On a donc deux branches paraboliques de direction l'axe des $x$. Ces deux branches paraboliques sont symétriques par rapport à l'axe des $y$ et correspondent au tracé de la courbe quand $\theta$ tend vers 0 pour l'une et au tracé de la courbe quand $\theta$ tend vers $\pi$ pour l'autre.

Pour l'étude de la courbe en coordonnées paramétriques, il suffit de prendre $t > 0$ car $x$ est une fonction impaire en $t$ et $y$ est une fonction paire en $t$. La courbe est donc symétrique par rapport à l'axe des $y$. Pour étudier les branches infinies, en coordonnées paramétriques, on fait tendre $t$ vers plus l'infini alors $x$ et $y$ tendent vers plus l'infini et $y/x = 1/t$ tend vers 0. Donc $\gamma$ admet donc deux branches paraboliques symétriques de direction l'axe des $x$.

Avec `Xcas`, on tape en coordonnées polaires :

```
plotpolar(1/sin(t)^3,t,0,pi)
```

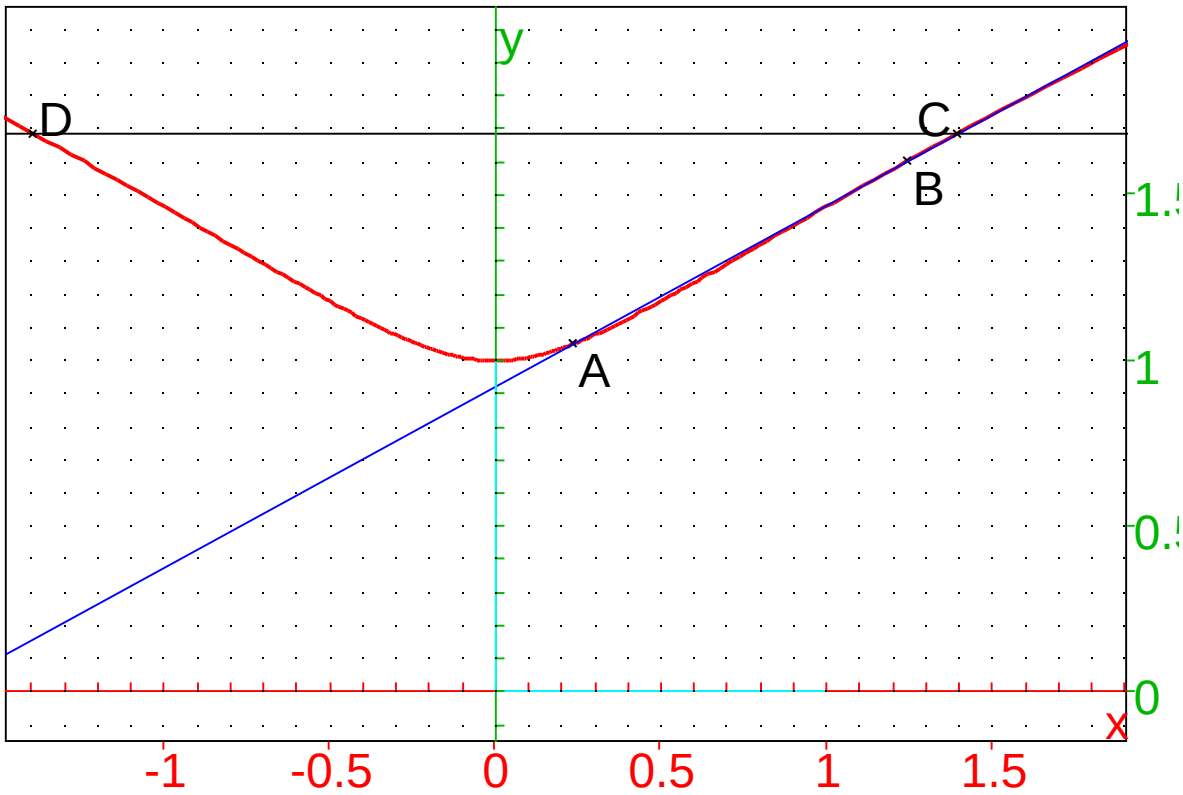
Ou en en coordonnées paramétriques :

```
plotparam((1+t^2)*(t+i),t)
```

(b) *Dans la suite de la question 4, on considère dans le plan projectif la cubique* $\Gamma$ *d'équation* $Y^3 - Y^2Z - X^2Z = 0$, *privée du point (0,0,1).*
*On choisit* $\Omega = (1,0,0)$ *le point à l'infini du plan dans la direction de la droite des x, et on définit le composé* $A * B$ *de deux points de* $\Gamma$ *comme en IV.1. Montrer que* $\Gamma$ *admet comme paramétrage :*

$$X = \cos(\theta), Y = \sin(\theta), Z = \sin(\theta)^3 \text{ pour } \theta \in \mathbb{R}$$

*Si A et B sont deux points de* $\Gamma$ *caractériser le point C d'intersection de la droite AB avec* $\Gamma$, *puis le point* $D = A * B$. *Démontrer que* $(\Gamma, *)$ *est isomorphe à un groupe usuel que l'on précisera.*
*Quels sont les points d'ordre 6 ?*




On prend les points du plan projectif correspondant aux points de $\gamma$ paramétrés en coordonnées polaires $(r\cos(\theta), r\sin(\theta), 1)$, donc ce sont les points $(\cos(\theta), \sin(\theta), 1/r) = (\cos(\theta), \sin(\theta), \sin(\theta)^3)$ Les branches infinies de $\gamma$ correspondent à $\theta = 0 \pmod{\pi}$.
Cherchons l'intersection d'une droite $aX + bY + cZ = 0$ avec $\Gamma$, cela revient à chercher les $\theta$ tels que

$$a\cos(\theta) + b\sin(\theta) + c\sin(\theta)^3 = 0$$

Si $a = 0$, alors $\theta = 0$ est solution et réciproquement, si de plus $c \neq 0$ est de signe opposé à $b$, les 2 autres solutions dans $[-\pi/2, \pi/2]$ sont de sinus opposés, donc sont opposées.
Après division par $\sin(\theta)$ pour $\theta \neq 0 \pmod{\pi}$, et en notant $t = 1/\tan(\theta) = \cot(\theta)$ on a (puisque $1 + \cot(\theta)^2 = 1/\sin(\theta)^2$) :

$$at + b + c\frac{1}{1+t^2} = 0$$

soit :

$$at^3 + bt^2 + at + b + c = 0$$

Pour $a \neq 0$, cette équation admet 3 solutions (dont 1 ou 3 réelles), qui vérifient

$$t_1t_2 + t_1t_3 + t_2t_3 = 1$$

donc :

$$t_3 = \frac{1 - t_1t_2}{t_1 + t_2}$$

Puisque $\cot(\theta_1 + \theta_2) = \dfrac{\cot(\theta_1)\cot(\theta_2) - 1}{\cot(\theta_1) + \cot(\theta_2)}$, s'il y a 3 solutions réelles, l'angle $\theta_3$ correspondant à $t_3$ vérifie alors $\cot(\theta_3) = -\cot(\theta_1 + \theta_2)$ donc :

$$\theta_3 = -(\theta_1 + \theta_2) \pmod{\pi}$$

Donc le 3ème point d'intersection $C$ d'une droite coupant la cubique en 2 points $A$ et $B$ de paramètres $\theta_1$ et $\theta_2$ vérifie dans tous les cas

$$\theta_3 = -(\theta_1 + \theta_2) \pmod{\pi}$$

De plus si on trace la droite passant par les points de paramètre $\theta_3$ et 0, elle coupe à nouveau la cubique au point $D$ de paramètre $-\theta_3 = \theta_1 + \theta_2$. Finalement la loi de composition de 2 points sur la cubique revient à additionner les paramètres modulo $\pi$, elle munit donc la cubique d'une structure de groupe isomorphe à $\mathbb{R}/\pi\mathbb{Z}, +$.

Les points d'ordre 6 correspondent aux angles $\theta$ tels que $6\theta = 0 \pmod{\pi}$, ce sont donc les 6 points d'angles respectifs $0, \pm\pi/6, \pm\pi/3, \pi/2$.

# 5 Partie V

*Dans cette partie, on étudie $\Gamma'$ définie dans le plan $\mathbb{F}_{16}^2$ par :*

$$P(x,y) = -y^2 - y + (x^3 + x) = 0$$

1. *Montrer que la courbe $\Gamma'$ contient au plus 32 points de $\mathbb{F}_{16}^2$.*
   À chaque $a \in \mathbb{F}_{16}$ il correspond deux valeurs au plus de $b \in \mathbb{F}_{16}$ vérifiant $b^2 + b = d = a^3 + a$ puisqu'il s'agit d'une équation de degré 2 sur un corps.
   Comme $\mathbb{F}_{16}$ a 16 éléments, la courbe $\Gamma'$ contient au plus 2*16=32 points.
2. *On introduit le polynôme homogène :*

   $$\overline{P}(X,Y,Z) = X^3 + XZ^2 - Y^2 - YZ^2$$

   *Définir un point à l'infini $\Omega$ et une multiplication interne dans $\Gamma = \Gamma' \cup \Omega$.*
   Le point $\Omega$ correspond à $Z = 0$ et doit vérifier $\overline{P}(X,Y,0) = X^3 = 0$ donc on prend $\Omega$ correspondant au point de coordonnées homogènes (0,1,0), le point à l'infini dans la direction de l'axe des $y$.
   Par analogie avec la partie IV, $\Omega$ sera l'élément neutre de la loi.
   On remarque que si $b$ est une solution de $y^2 + y = d$ alors $b+1$ est aussi solution de $y^2 + y = d$. Donc la droite $x = a \in \mathbb{F}_{16}$ coupe la courbe $\Gamma$ en 1 ou 3 points qui sont $\Omega$ et éventuellement $(a,b)$ et $(a,b+1)$ lorsque l'équation $y^2 + y = a^3 + a$ admet une solution $y = b$ dans $\mathbb{F}_{16}$. L'inverse de $(a,b) \in \Gamma'$ sera donc $(a,b+1)$ (qui est aussi dans $\Gamma'$).
   L'intersection d'une droite $y = mx + p$ avec $\Gamma'$ est donnée par une équation du 3ème degré sur $\mathbb{F}_{16}$ donc si elle admet 2 solutions, elle en admet forcément une 3ème. On définit le composé des 2 solutions comme le symétrique de la 3ème.
   Finalement la loi * est définie par :
   - $\Omega * \Omega = \Omega$
   - $(a,b) * \Omega = (a,b)$ si $(a,b) \in \Gamma'$
   - Si la droite $AB$ recoupe $\Gamma$ en $C = (c_1, c_2)$, on pose :

     $$A * B = D = (c_1, c_2 + 1)$$

   - Le cas $A = B$ est traité plus bas.
3. Cette loi est évidemment commutative, admet $\Omega$ comme neutre et on a $(a,b)^{-1} = (a,b+1)$ pour tout $(a,b) \in \Gamma'$.

4. *On se propose de calculer $A^2 = A*A$ pour $A = (a,b) \in \Gamma'$. On cherche la droite $D$ dont l'intersection avec $\Gamma'$ admet un point double en $A$.*

   (a) *Montrer que $D$ a pour équation :*

   $$P'_x(a,b)(x-a) + P'_y(a,b)(y-b) = 0$$

   Pour $A = (a,b) \in \Gamma'$ on a $P(a,b) = 0$, donc :

   $$\begin{aligned} P(x,y) &= P(x,y) - P(a,b) \\ &= P(x,y) - P(x,b) + P(x,b) - P(a,b) \\ &= (y-b)Q(x,y) + (x-a)R(x,y) \end{aligned}$$

   en factorisant $y-b$ dans $P(x,y) - P(x,b)$ et $x-a$ dans $P(x,b) - P(a,b)$ (par exemple par la méthode de Horner). On faisant $x = a$ et en dérivant par rapport à $y$ puis en faisant $y = b$, on a $Q(a,b) = P'_y(a,b)$, de même $R(a,b) = P'_x(a,b)$. Finalement :

   $$P(x,y) = (x-a)P'_x(a,b) + (y-b)P'_y(a,b) + P_2(x-a, y-b)$$

   où $P_2$ ne contient que des monomes de degré total $\geq 2$. Donc la droite $D$ d'équation $(x-a)P'_x(a,b) + (y-b)P'_y(a,b) = 0$ et la courbe $\Gamma'$ admettent un point double en commun. On a $P'_x(a,b) = a^2+1$ et $P'_y(a,b) = 1$ donc la tangente à $\Gamma'$ en $A$ a pour équation :

   $$(a^2+1)(x-a) + (y-b) = 0$$

   ou encore $(a^2+1)x + a^3 + a + b = y$ or $a^3 + a = b^2 + b$, donc

   $$y = (a^2+1)x + b^2$$

   (b) *Déterminer les coordonnées de $A*A$.*

   La tangente à $\Gamma'$ en $A$ recoupe $\Gamma'$ en un point $(x,y)$ qui vérifie :

   $$x^3 + x = y^2 + y = (a^2+1)^2 x^2 + b^4 + (a^2+1)x + b^2$$

   On calcule le terme en $x^2$ de cette équation en $x$, on trouve $a^4+1$, or c'est la somme des 3 racines, et comme $x = a$ est racine double, la troisième racine est $x = a^4 + 1$. Il reste à calculer :

   $$y = (a^2+1)(a^4+1) + b^2 = a^6 + a^4 + a^2 + 1 + b^2 = a^4 + b^4 + 1$$

   car $a^6 + a^2 = b^4 + b^2$. La tangente au point $A = (a,b)$ avec $a^3 + a = b^2 + b$ coupe $\Gamma'$ en $C = (x = a^4+1, y = a^4 + b^4 + 1)$ donc le point $D$ intersection de $\Omega C$ avec $\Gamma'$ est le point :

   $$D = A*A = (a^4+1, a^4 + b^4)$$

   Donc si $A = (a,b)$ alors $A*A = (a^4+1, a^4+b^4)$.

   (c) *En déduire que, pour tout point $A$ de $\Gamma'$ on a :*

   $$A^4 = A^{-1}$$

   On calcule $A^4$ :

   $$A^4 = (A*A)*(A*A) = (a^4+1, a^4+b^4)*(a^4+1, a^4+b^4)$$

donc puisque pour tout $a \in \mathbb{F}_{16}$ on a $a^{15} = 1$,

$$\begin{aligned} A^4 &= ((a^4+1)^4+1, (a^4+1)^4+(a^4+b^4)^4) \\ &= (a+1+1, a+1+a+b) \\ &= (a, b+1) \\ &= A^{-1} \end{aligned}$$

(d) *En déduire le cardinal de* $\Gamma$ *et sa décomposition en produit direct de groupes cycliques.*

$\Gamma$ contient $n$ points avec $n \leq 32$ et $n$ est une puissance de 5 puisque tous les éléments sont d'ordre 5, donc $n = 1$, $n = 5$ ou $n = 25$.

Posons pour $\omega \in \mathbb{F}_{16}$ :

$$A = (1,0), \quad B = (\omega^3, \omega^9)$$

On a $A \in \Gamma$ car $0^2 + 0 = 1^3 + 1$ et $B \in \Gamma$ car $\omega^{18} + \omega^9 = \omega^9 + \omega^3$ puisque $\omega^{15} = 1$.

On a :

$$A = (1,0), \quad A*A = (0,1), \quad A*A*A = (1,0)*(0,1) = (0,0)$$

$$A*A*A*A = (0,1)*(0,1) = (1,1), \quad A*A*A*A*A = \Omega$$

Donc $B$ n'est pas une puissance de $A$. Donc $n = 25$ et les 25 èléments sont :

$$\Omega, A, A^2..A^4, B, B*A..B*A^4, ....B^4, B^4*A.B^4*A^4.$$

Avec `Xcas`, on définit l'ensemble $K$ des éléments du corps $\mathbb{F}_{16}$ :

```
F16 :=GF(2,4,['t','F16']);
w :=F16(t);
K :=append(seq(w^k,k,1,15),F16(0)) :;
```

On tape pour avoir les valeurs de $a^3 + a$ pour $a \in \mathbb{F}_{16}$ :

```
La :=seq(K[k]^3+K[k],k,0,15)
```

On obtient :

```
[F16(t^3+t),F16(t^3+t+1),F16(t^3+t^2+1),F16(t^3+t),
F16(t^3+t),F16(t^2+t+1),F16(t^3),F16(t^3+t+1),F16(t^2+t),
F16(t^3+t+1),F16(t^2+1),F16(t^3+t^2),F16(t+1),
F16(t^3+t^2+t+1),F16(0),F16(0)]
```

On tape pour avoir les valeurs différentes de $a^3 + a$ pour $a \in \mathbb{F}_{16}^*$ :

```
A :=set[op(La)];
size(A);
```

On obtient 11 valeurs différentes :

```
set[F16(t^3+t),F16(t^3+t+1),F16(t^3+t^2+1),F16(t^2+t+1),
F16(t^3),F16(t^2+t),F16(t^2+1),F16(t^3+t^2),
F16(t+1),F16(t^3+t^2+t+1),F16(0)]
```

Pour chacune de ces valeurs $a$ l'équation $y^2 + y = a$ a-t-elle des solutions ?

On tape pour avoir les valeurs de $b^2 + b$ pour $b \in \mathbb{F}_{16}$ :

```
Lb :=seq(K[k]^2+K[k],k,0,15)
```

On obtient :

```
[F16(t^2+t),F16(t^3+t^2+1),F16(t^2+t+1),F16(t^2+t+1),F16(1),
F16(t^3+t^2),F16(t^3+t+1),F16(t^3+t^2),F16(t^3+t^2+1),F16(1),
F16(t^3+t),F16(t^2+t),F16(t^3+t+1),F16(t^3+t),F16(0),F16(0)]
```

On tape pour avoir les valeurs différentes de $b^2+b$ pour $b \in \mathbb{F}_{16}$ :

```
B :=set[op(Lb)];
    size(B);
```

On obtient 8 valeurs différentes :

```
set[F16(t^2+t),F16(t^3+t^2+1),F16(t^2+t+1),F16(1),
   F16(t^3+t^2),F16(t^3+t+1),F16(t^3+t),F16(0)]
```

Comme 2*8=16 cela prouve que dans $\mathbb{F}_{16}$ l'équation en $y$, $y^2+y=d$ n'a pas de solutions doubles (on peut aussi le voir en faisant la somme des racines).

On tape pour avoir les valeurs communes de $a^3+a$ et de $b^2+b$ pour $a \in \mathbb{F}_{16}^*$ et $b \in \mathbb{F}_{16}$ :

```
C := A intersect B;
     size(C);
```

On obtient 7 valeurs différentes :

```
set[F16(t^3+t),F16(t^3+t+1),F16(t^3+t^2+1),F16(t^2+t+1),
          F16(t^2+t),F16(t^3+t^2),F16(0)]
```

On compte le nombre de solutions dans $\mathbb{F}_{16}$ de l'équation en $x$, $x^3+x=d$ lorsque $d \in$`La`. On tape :

```
seq(count_eq(C[p],La),p,0,6)
```

On obtient `[3,3,1,1,1,1,2]`. Les 7 valeurs différentes de $a^3+a$ sont donc obtenues pour 3+3+1+1+1+2=12 valeurs de $a$ lorsque $a \in \mathbb{F}_{16}$, à chaque $a$ correspond alors 2 valeurs de $b$, ce qui nous donne bien 24 éléments dans $\Gamma'$ et $\Gamma$ contient 25 points.

**Remarques**

- `3` indique que l'équation en $x$, $x^3+x=d$ lorsque $d \in$`La` a 3 racines distinctes,
- `2` indique que l'équation en $x$, $x^3+x=d$ lorsque $d \in$`La` a 3 racines dont une racine double,
- `1` indique que l'équation en $x$, $x^3+x=d$ lorsque $d \in$`La` a 1 racine simple ou 1 racine triple.

On peut écrire le programme qui va calculer $A*B$ pour 2 éléments différents $A=(xa,ya)$ et $B=(xb,yb)$ de $\Gamma$.

Équation de la droite $AB$ :

$$(ya+yb)*x+(xa+xb)*y+xa*yb+xb*ya=0$$

si $xa \neq xb$ alors $xa+xb$ est inversible. Son inverse est : $(xa+xb)^{14}$ puisque $(xa+xb)^{15}=1$. Donc

$$y=(xa+xb)^{14}*((ya+yb)*x+xa*yb+xb*ya)$$

Donc le coefficient de $x^2$ lorsque l'on a remplacé $y$ en fonction de $x$ dans $x^3+x+y^2+y$ est :

$$(xa+xb)^{28}*(ya+yb)^2=(xa+xb)^{13}*(ya^2+yb^2)$$

On a $xa,xb,xc$ vérifient :

$$x^3+(xa+xb)^{13}*(ya^2+yb^2)*x^2+....=0$$

La somme des racines $S$ vérifie :

$$S = (xa+xb)^{13} * (ya^2+yb^2)$$

donc

$$S = xa+xb+xc = (xa+xb)^{13} * (ya^2+yb^2)$$

donc

$$\begin{aligned} xc &= (xa+xb)^{13} * (ya^2+yb^2)+xa+xb \\ yc &= (xa+xb)^{14} * ((ya+yb)*xc+xa*yb+xb*ya) \\ xd &= xc \\ yd &= yc+1 \end{aligned}$$

si $xa == xb$ avec $ya \neq yb$ alors $etoile(xa,ya,xb,yb) = \Omega$
On tape pour définir la loi `etoile` de 2 éléments de $\Gamma$ en notant $\Omega$ `infinity` :

```
// F16:=GF(2,4,['t','F16'])
// xa et ya sont dans F16 par ex xa:=F16(w^3) ...
estdansgamma(xa,ya):=(xa^3+xa+ya^2+ya==0);

// a:=[xa,ya] b:=[xb,yb] ou xa,ya,xb,yb sont dans F16
etoile(a,b):={
 local xa,xb,ya,yb,xc,yc;
 if (a==infinity and b==infinity) return infinity;
 if (a==infinity) {
  if (estdansgamma(op(b))==0) return "b pas dans gamma";
  return b;
 }
 if (b==infinity) {
  if (estdansgamma(op(a))==0) return "a pas dans gamma";
  return a;
 }
 xa:=a[0]; xb:=b[0]; ya:=a[1]; yb:=b[1];
 if (estdansgamma(xa,ya)==0) return "a pas dans gamma";
 if (estdansgamma(xb,yb)==0) return "b pas dans gamma";
 if (xa!=xb) {
  xc:=(xa+xb)^13*(ya^2+yb^2)+xa+xb;
  yc:=(xa+xb)^14*((ya+yb)*xc+xa*yb+xb*ya)+F16(1);
  return [xc,yc];
 }
 if ((xa==xb) and (ya==yb)) {
  xc:=xa^4+F16(1);
  yc:=xa^4+ya^4;
  return [xc,yc];
 }
 return infinity;
}:;
```

On tape :

```
u :=[F16(1),F16(0)]
v :=[w^3,w^9]
```

On sait que : u est dans Γ et que : v est dans Γ.

On tape pour avoir les 25 éléments de Γ :

```
G:=seq(seq(etoile(
  puissrapide(u,k,etoile,infinity,0),
  puissrapide(v,j,etoile,infinity,0)
 ),k=1..5),j=1..5):;
G:=[G];
```

On obtient :

```
 [[F16(t+1),F16(t^3+t^2+t)],[F16(t^3+t^2+t),F16(t^2+t+1)],
   [F16(t^3+t+1),F16(t^3+t^2)],[F16(t^2),F16(t^2+t+1)],
[F16(t^3),F16(t^2+1)],[F16(t^3+t),F16(t^2+t)],[F16(t^3+1),
  F16(t^3+t^2)],[F16(t^3+t^2+t+1),F16(t^3)],[F16(t^2+1),
   F16(t)],[F16(t),F16(t^3+t^2)],[F16(t^2+1),F16(t+1)],
        [F16(t^3+t^2+t+1),F16(t^3+1)],[F16(t^3+1),
    F16(t^3+t^2+1)],[F16(t^3+t),F16(t^2+t+1)],[F16(t),
   F16(t^3+t^2+1)],[F16(t^2),F16(t^2+t)],[F16(t^3+t+1),
       F16(t^3+t^2+1)],[F16(t^3+t^2+t),F16(t^2+t)],
     [F16(t+1),F16(t^3+t^2+t+1)],[F16(t^3),F16(t^2)],
     [F16(1),F16(0)],[F16(0),F16(1)],[F16(0),F16(0)],
                [F16(1),F16(1)],infinity]
```

On tape :

```
size(set[op(G)])
```

On obtient :

```
25
```

5. *Indiquer brièvement comment implanter un système de cryptographie du type de celui de la partie II à l'aide de* Γ.

   Comme on n'a que 25 éléments pour coder les 26 lettres de l'alphabet, on peut convenir de dire que : *A* sera codée par 0, *B* sera par 1, ..., les lettres *V* et *W* seront codées par 21, *X* sera codée par 22, les lettres *I* et *Y* seront codées par 7, *Z* par 23, l'espace sera codé par 24.
   Les éléments de *G* seront indicés par 0..24. On écrit la fonction de codage `lettre2n` qui convertit une lettre majuscule en un entier entre 0 et 24 et de décodage `n2lettre` qui convertit un entier entre 0 et 24 en une lettre majuscule :

```
lettre2n(a):={
 local c;
 c:=op(asc(a));
 if (c==32) return 24;
 if (c<87) return c-65;
 if (c==87) return 21;
 if (c==88) return 22;
 if (c==89) return 7;
 if (c==90) return 23;
}:;
```

```
n2lettre(n):={
 if (n<22) return char(n+65);
 if (n==24) return " ";
 if (n==22) return "X";
 if (n==23) return "Z";
};;
```

Puis on écrit la fonction qui code une lettre par un élément de $G$ :

```
//a est un caractere majuscule
lettre2G(a,G):={
 local c;
 c:=lettre2n(a);
 return G[c];
};
```

On suppose le groupe $G$ ainsi que les éléments $\pi$ et $\alpha$ de $G$ connus de tous. On garde secret l'entier $e$ et $\alpha = \pi^e$. Avec `Xcas` $\pi$ sera noté `pii`, $e$ sera noté `ex` et $\alpha$ sera noté `alpha`, par exemple :

```
pii :=G[10]
  ex :=3
alpha :=puissrapide(pii,ex,etoile,infinity,0)
```

La fonction $f_\alpha$, notée `falpha` sera définie par :

```
// tau est un element de G par exemple tau:=lettre2G("A",G)
// falpha(k,tau) renvoie une matrice 2*2 d'elements de F16
falpha(k,tau):={
 local a;
 return [puissrapide(pii,k,etoile,infinity,0),
         etoile(puissrapide(alpha,k,etoile,infinity,0),tau)];
};;
```

La fonction $\phi_e$ sera alors `phie` :

```
// a et b sont des elements de G
//inva:=a^(5-ex) est l'inverse de a^ex car a^5=1
phie(a,b,ex):={
 local inva;
 ex:=irem(ex,5);
 inva:=puissrapide(a,5-ex,etoile,infinity,0);
 return etoile(inva,b);
};;
```

Voici enfin la fonction de codage d'une chaine de caractères :

```
//s est une chaine de caracteres majuscules
//on choisit k de facon aleatoire
codage(s,G):={
 local L,n,j,k,f;
 L:=[];
 n:=size(s);
 for (j:=0;j<n;j++){
```

```
  k:=rand(25);
  f:=falpha(k,lettre2G(s[j],G));
  L:=append(L,f);
 }
 return L;
};
```

et la fonction de décodage :

```
//indice d'un element tau de G
indice(tau,G):={
 local n,k;
 n:=size(G);
 k:=0;
 while (tau!=G[k]){
  k:=k+1;
 }
 return k;
};;

//decodage d'une liste L envoyee par la fonction codage
//ex et l'element tenu secret
decodage(L,ex,G):={
 local n,j,M,tau,k,a,b;
 M:="";
 n:=size(L);
 for (j:=0;j<n;j++){
  a:=L[j,0];
  b:=L[j,1];
  tau:=phie(a,b,ex);
  k:=indice(tau,G);
  M:=M+n2lettre(k);
 }
 return M;
};;
```

On reprend l'exemple de la partie I, on tape

```
message :=codage("COGITO",G)
```

on obtient une "matrice" de couples de $\mathbb{F}_{16}$ que l'on peut décoder en tapant :

```
decodage(message,ex,G)
```