# Mathématiques générales 2007 - Corrigé

Michel Coste*

29 février 2008

## Partie I

1. Puisque $G$ est de cardinal $N$, tout élément $a$ de $G$ vérifie $a^N = 1$, et donc $a\,a^{N-1} = 1$, ce qui montre que $a^{N-1}$ est l'inverse de $a$ dans $G$.
2. On écrit $N-1$ en base 2 : $N-1 = \sum_{i=0}^{k} x_i 2^i$ où $x_i \in \{0,1\}$.
   (a) On a, par récurrence sur $i$, $b_i = a^{2^i}$ et aussi $a_i = a^{n_i}$, où $n_i = \sum_{j=0}^{i-1} x_j 2^j$. Donc $a_{k+1} = a^{N-1}$ est l'inverse de $a$ dans $G$.
   (b) La construction des suites $b_i$ et $a_i$ de la question précédente donne en fait un algorithme de calcul de $a^{-1}$.
   Les calculs de $b_1, \ldots, b_k$ nécessitent chacun une multiplication dans $G$, et ceux de $a_2, \ldots, a_{k+1}$ chacun une ou zéro multiplication. On a donc au plus $2k$ multiplications dans $G$. Comme $2^k \leq N-1 < 2^{k+1}$, le nombre de multiplications est majoré par 2 fois la partie entière de $\log_2(N-1)$.
   On peut calculer les chiffres $x_i$ de l'écriture de $N-1$ en base 2 en même temps, de la manière suivante : on définit la suite $(m_i)$ d'entiers positifs ou nuls strictement décroissante et la suite $x_i$ ainsi :
   – $x_0$ et $m_0$ sont le reste et le quotient de la division de $N-1$ par 2 ;
   – tant que $m_i > 0$, $x_{i+1}$ et $m_{i+1}$ sont le reste et le quotient de la division de $m_i$ par 2.
   Voici un algorithme de calcul de $a^{-1}$ écrit "à la Maple". On suppose donné un type `G` pour les éléments du groupe $G$, et que la multiplication dans le groupe s'écrit `*`. La procédure "Inverse" prend en entrée un élément $a$ de $G$ et un entier $N$. On a des variables locales $m$ et $x$ entières qui reçoivent les valeurs successives des $m_i$ et des $x_i$, $b$ et $c$ de type `G` qui reçoivent les valeurs successives des $b_i$ et des $a_i$.

```
Inverse:= proc(a::G, N::integer)
local m::integer, x::integer, b::G, c::G
x:= irem(N-1,2); m:= iquot(N-1,2) ; b:= a ;
if x=1 then c:= a else c:= 1 end if;
while m>0 do
     x:= irem(m,2); m:= iquot(m,2); b:= b*b;
     if x=1 then c:= c*b end if
end do;
c;
```

3. (a) La décomposition de 148 en facteurs premiers est $148 = 2^2 \times 37$. D'après le théorème chinois, $\mathbb{Z}/148\mathbb{Z}$ est isomorphe à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/37\mathbb{Z}$ et son groupe des éléments inversibles $G$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$, qui a 72 éléments.
   (b) Puisque 5 est premier avec 148, sa classe modulo 148 est inversible et appartient donc à $G$. On a ici $N-1 = 71 = 2^6 + 2^2 + 2^1 + 2^0$. Les élévations au carré successives à partir de 5

*Merci à bs pour ses corrections

donnent, modulo 148 : $5, 25, 33, 53, -3, 9, 81$. On calcule ensuite modulo 148 : $5 \times 25 \equiv -23$ ; $-23 \times 33 \equiv -19$ ; $-19 \times 81 \equiv -59$. Donc $-59$ est inverse de 5 modulo 148.

(c) L'inverse de 5 modulo 148 peut aussi se calculer (plus facilement !) par l'algorithme d'Euclide étendu qui calcule une identité de Bezout entre 5 et 148 : on a $148 = 29 \times 5 + 3$, d'où $1 = 2 \times 3 - 5 = 2 \times (148 - 29 \times 5) - 5 = 2 \times 148 - 59 \times 5$, et on retrouve bien $(-59) \times 5 \equiv 1$ modulo 148.

# Partie II

1.

$$\begin{array}{rcl} f_a : \mathbb{Z} \times G & \longrightarrow & G^2 \\ (k, \tau) & \longmapsto & (\pi^k, \tau\, \alpha^k) \end{array}$$

(a) Puisque $(\pi^k)^e = \alpha^k$, si on pose

$$\begin{array}{rcl} \varphi_e : G^2 & \longrightarrow & G \\ (\lambda, \mu) & \longmapsto & \mu\, \lambda^{-e}\,, \end{array}$$

alors $\varphi_e \circ f_\alpha(k, \tau) = \tau$.

(b) Puisque **A** connaît $e$, il peut appliquer $\varphi_e$ à chacun des $(\lambda_i, \mu_i)$ pour récupérer $\tau_i$ et donc décrypter le message.

2. $G = \mathbb{F}_{29}^*$, $\pi = 2$, $\alpha = 18$.

(a) Le calcul de $\varphi_e$ nécessite un calcul de puissance $-e$-ème dans $G$ (donc modulo 29). La table des puissances 17-èmes (ou encore des puissances $17 - 28 = -11$-èmes est bien ce dont on a besoin pour $e = 11$. Ceci est confirmé par le fait que $\pi^{11} = 2048$ est bien congru à $18 = \alpha$ modulo 29.

(b) En utilisant la table, on a modulo 29 : $17 \times 16^{17} \equiv 119 \equiv 3$, $24 \times 18^{17} \equiv -72 \equiv 15$, $22 \times 28^{17} \equiv -22 \equiv 7$, $21 \times 17^{17} \equiv -136 \equiv 9$, $23 \times 23^{17} \equiv -96 \equiv 20$, $8 \times 24^{17} \equiv 160 \equiv 15$. Le message est donc COGITO.

# Partie III

1. (a) $\mathbb{F}_{16}$ est une extension algébrique de degré 4 de $\mathbb{F}_2$. On peut la construire en quotientant $\mathbb{F}_2[X]$ par l'idéal engendré par un polynôme irréductible de degré 4 sur $\mathbb{F}_2$. Par exemple, $F = X^4 + X^3 + 1$ est un tel polynôme irréductible sur $\mathbb{F}_2$. En effet, il n'a pas de facteur du premier degré, c.-à-d. pas de racine dans $\mathbb{F}_2$, puisque $F(0) = F(1) = 1$. Il n'a pas non plus de facteur du 2-ème degré puisque sinon il devrait s'écrire $F = (X^2 + aX + 1)(X^2 + bX + 1)$ , avec $a$ et $b$ dans $\mathbb{F}_2$ ; mais alors en identifiant les coefficients de $X^3$ on devrait avoir $a + b = 1$, et en identifiant ceux de $X$ on devrait avoir $a + b = 0$, ce qui est impossible.

(b) Posons donc $\mathbb{F}_{16} = F_2[X]/(X^4 + X^3 + 1)$, et soit $\omega \in F_{16}$ l'image de $X$ dans ce quotient. Alors $(1, \omega, \omega^2, \omega^3)$ forme une base de $\mathbb{F}_{16}$ sur $\mathbb{F}_2$, et $\omega$ vérifie $\omega^4 = \omega^3 + 1$. En utilisant cette identité, on calcule les coordonnées des puissances successives de $\omega$ dans la base indiquée.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $1$ | $1000$ | $\omega^4$ | $1001$ | $\omega^8$ | $0111$ | $\omega^{12}$ | $1100$ |
| $\omega$ | $0100$ | $\omega^5$ | $1101$ | $\omega^9$ | $1010$ | $\omega^{13}$ | $0110$ |
| $\omega^2$ | $0010$ | $\omega^6$ | $1111$ | $\omega^{10}$ | $0101$ | $\omega^{14}$ | $0011$ |
| $\omega^3$ | $0001$ | $\omega^7$ | $1110$ | $\omega^{11}$ | $1011$ | $\omega^{15}$ | $1000$ |

Ceci montre que $\omega$ qui est d'ordre 15 et engendre le groupe multiplicatif $\mathbb{F}_{16}^* = \mathbb{F}_{16} \setminus \{0\}$.

(c) Rappelons que, comme on est en caractéristique 2, l'application $x \mapsto x^2$ de $\mathbb{F}_{16}$ dans lui-même est un automorphisme de corps (automorphisme de Frobenius), qui laisse fixes les éléments $0, 1$ de $\mathbb{F}_2$. Puisque $F = X^4 + X^3 + 1$ est à coefficients dans $\mathbb{F}_2$, on a $F(\xi)^2 = F(\xi^2)$ pour tout élément $\xi$ de $\mathbb{F}_{16}$. Le carré d'une racine de $F$ est donc encore une racine de $F$. Les élévations au carré successives à partir de la racine $\omega$ de $F$ donnent $\omega^2$, $\omega^4$, $\omega^8$ et on revient à $\omega = \omega^{16}$. On obtient ainsi les quatre racines de $F$ dans $\mathbb{F}_{16}$.

(d) On peut grâce au tableau ci-dessus calculer (en développant suivant les lignes) le déterminant de $(\omega, \omega^2, \omega^4, \omega^8)$ dans la base $(1, \omega, \omega^2, \omega^3)$ :

$$\begin{vmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{vmatrix} = 1 \, .$$

Ceci montre que $(\omega, \omega^2, \omega^4, \omega^8)$ est bien une base de $\mathbb{F}_{16}$ sur $\mathbb{F}_2$.

2. (a) Discutons l'équation $x^5 = a$ dans $\mathbb{F}_{16}$. Si $a = 0$, l'équation $x^5 = 0$ a bien sûr la solution $x = 0$ de multiplicité 5. L'homomorphisme $x \mapsto x^5$ du groupe $\mathbb{F}_{16}^*$ dans lui-même a pour image le sous-groupe d'ordre 3 engendré par $\omega^5$, et pour noyau le sous-groupe $K$ d'ordre 5 engendré par $\omega^3$. L'équation $x^5 = a$ avec $a$ élément non nul de $\mathbb{F}_{16}$ a des solutions si et seulement si $a = \omega^{5k}$ avec $k = 0, 1, 2$, et ses cinq solutions sont alors les $\omega^{k+3i}$ avec $i = 0, 1, 2, 3, 4$.

(b) Considérons l'ensemble des solutions de $x^5 = 1$, c.-à-d. le sous-groupe $K$ de $\mathbb{F}_{16}^*$ engendré par $\omega^3$. Soit $\gamma$ un élément de $K$ différent de 1 (on a quatre choix possibles pour $\gamma$). Puisque $\gamma$ est d'ordre 5, les éléments $\gamma$, $\gamma^2$, $\gamma^4$ et $\gamma^8 = \gamma^3$ sont les quatre éléments de $K$ différents de 1. Le produit de deux quelconques d'entre eux est encore un élément de $K$ et est donc égal à l'un des $\gamma, \gamma^2, \gamma^4, \gamma^8$ ou à 1. Pour vérifier que $(\gamma, \gamma^2, \gamma^4, \gamma^8)$ est une base, il suffit de calculer le déterminant de $(\omega^3, \omega^6, \omega^9, \omega^{12})$ (les mêmes, pas dans le même ordre) dans la base $(1, \omega, \omega^2, \omega^3)$ :

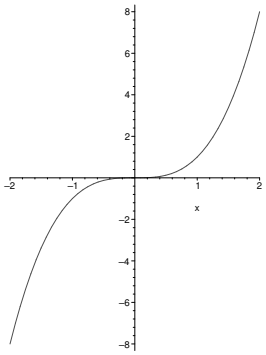
$$\begin{vmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{vmatrix} = 1 \, .$$

On peut remarquer qu'il n'y a pas d'autre manière de choisir $\gamma$ que les quatre que nous avons indiquées ; en effet, la condition sur le produit impose que $\{1, \gamma, \gamma^2, \gamma^4, \gamma^8\}$ est un sous-groupe d'ordre 5 du groupe cyclique $\mathbb{F}_{16}^*$, et donc égal à $K$.

Les calculs dans la base $(\gamma, \gamma^2, \gamma^4, \gamma^8)$ présentent l'avantage que la table de multiplication dans cette base est assez légère puisque le produit de deux éléments de la base est un élément de la base (pas une combinaison linéaire), sauf pour $\gamma \times \gamma^4 = \gamma^2 \times \gamma^8 = 1 = \gamma + \gamma^2 + \gamma^4 + \gamma^8$ (la dernière égalité vient du fait que $\gamma, \gamma^2, \gamma^4, \gamma^8$ sont les quatre racines de $X^4 + X^3 + X^2 + X + 1$).

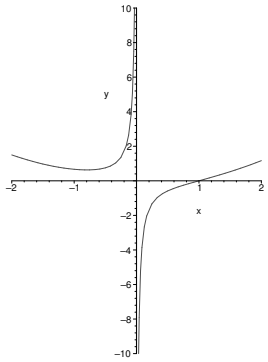
# Partie IV

1. Ici $P = X^3 - Y$.
   (a) La cubique $\Gamma$ définie par $P$ dans $\mathbb{R}^2$ est le graphe de la fonction $x \mapsto x^3$.



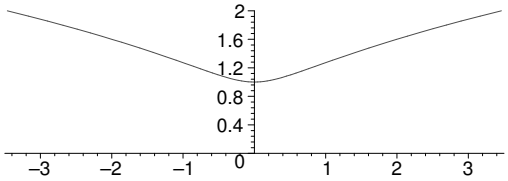

   (b) Une droite verticale $x = a$ coupe $\Gamma$ en un seul point $(a, a^3)$ (de multiplicité 1). Une droite $y = ax + b$ coupe $\Gamma$ en des points dont les abscisses sont les solutions de $x^3 - ax - b = 0$. Cette équation du troisième degré a une ou trois solutions réelles, comptées avec multiplicité. S'il y a trois solutions réelles $x_A, x_B, x_C$ comptées avec multiplicité, leur somme est 0 d'après les relations entre coefficients et racines, vu que le coefficient de $X^2$ dans $X^3 - aX - b$ est nul.
   (c) Remarquons d'abord que $A \mapsto x_A$ définit une bijection de $\Gamma$ sur $\mathbb{R}$. D'après la question précédente, si $C$ est le troisième point d'intersection de la droite $AB$ avec $\Gamma$, on a $x_C = -x_A - x_B$. Et si $A * B$ est le troisième point d'intersection de la droite $\Omega C$ avec $\Gamma$, on a $x_{A*B} = -x_\Omega - x_C = x_A + x_B$. Donc $(\Gamma, *)$ est un groupe isomorphe à $(\mathbb{R}, +)$ par $A \mapsto x_A$.

2. Ici $P = X^3 - 3XY - 1$. La cubique $\Gamma$ est le graphe de la fonction $x \mapsto \dfrac{x^3 - 1}{3x}$ définie sur $\mathbb{R} \setminus \{0\}$




   L'application $A \mapsto x_A$ qui associe à un point de $\Gamma$ son abscisse est une bijection de $\Gamma$ sur $\mathbb{R} \setminus \{0\}$. L'intersection avec une droite verticale $x = a$, $a \neq 0$ est réduite à un point (de multiplicité 1). Les abscisses de l'intersection avec une droite $y = ax + b$ sont les solutions de $x^3 - 3ax^2 - 3bx - 1 = 0$. Il y a une ou trois solutions réelles comptées avec multiplicité, et le produit de ces solutions est 1. Si une droite coupe $\Gamma$ en trois points $A, B, C$, leurs abscisses vérifient donc $x_A x_B x_C = 1$. Si $C$ est le point d'intersection de la droite $AB$ avec $\Gamma$, on a donc $x_C = x_A^{-1} x_B^{-1}$ et si $A * B$ est le point d'intersection de $\Omega C$ (où $\Omega = (1, 0)$) avec $\Gamma$, alors $x_{A*B} = x_\Omega^{-1} x_C^{-1} = x_A x_B$. Finalement $(\Gamma, *)$ est un groupe isomorphe à $(\mathbb{R} \setminus \{0\}, \times)$ par $A \mapsto x_A$.

3. Une droite du plan projectif a pour équation $\alpha X + \beta Y + \gamma Z = 0$, où $\alpha, \beta, \gamma$ ne sont pas tous les trois nuls. On peut supposer $\alpha \neq 0$ et alors on calcule l'intersection de la droite avec la cubique en remplaçant $X$ par $-\dfrac{\beta}{\alpha}Y - \dfrac{\gamma}{\alpha}Z$ dans l'équation $\overline{P}(X, Y, Z) = 0$. On obtient ainsi un polynôme homogène de degré trois en deux variables $Y, Z$. Il se peut que ce polynôme soit identiquement nul (cas où la droite est contenue dans $\Gamma$, qui n'est pas envisagé dans l'énoncé). S'il n'est pas identiquement nul, il se factorise sur $\mathbb{R}$ en un produit de trois formes linéaires réelles en $Y, Z$ ou en un produit d'une forme linéaire et d'un polynôme homogène irréductible du second degré en $Y, Z$. Dans le premier cas on obtient trois points du plan projectif sur $\mathbb{R}$, dans le deuxième un seul (en comptant les multiplicités).
4. Ici $\overline{P} = Y^3 - X^2Z - Y^2Z$. est le polynôme homogénéisé de $P = Y^3 - X^2 - Y^2$.
   (a) Ici $\gamma$ est la courbe d'équation $P = 0$ du plan euclidien, privée de l'origine. En coordonnées polaires $x = \rho\cos\theta$, $y = \rho\sin\theta$, l'équation de la courbe $\gamma$ devient $\rho\sin^3\theta = 1$, d'où la paramétrisation $\rho = \dfrac{1}{\sin^3\theta}$ pour $\theta \in ]0, \pi[$ (remarquer que $\rho(\theta + \pi) = -\rho(\theta)$, et aussi la symétrie par rapport à l'axe des $y$). Il y a deux branches infinies pour $\theta$ tendant vers 0 ou vers $\pi$, avec direction asymptotique horizontale mais pas d'asymptote car $y = 1/\sin^2\theta$ tend vers $+\infty$ quand $\theta$ tend vers 0 ou $\pi$.




   (b) Maintenant $\Gamma$ est la cubique d'équation $\overline{P} = 0$ du plan projectif, privée du point de coordonnées homogènes $(0, 0, 1)$. On a vu que sa partie affine (avec $Z \neq 0$) est paramétrée en coordonnées affines par $(\cos\theta/\sin^3\theta, 1/\sin^2\theta)$ ou encore, en coordonnées homogènes, par $(\cos\theta, \sin\theta, \sin^3\theta)$ pour $0 < \theta < \pi$. La valeur $(1, 0, 0)$ de cette dernière expression pour $\theta = 0$ est le système de coordonnées homogènes du point à l'infini de $\Gamma$, c.-à-d. de son intersection avec la droite $Z = 0$. En effet $\overline{P}(X, Y, 0) = Y^3$. Notons $\Phi$ l'application qui à $\theta \in \mathbb{R}$ associe le point du plan projectif de coordonnées homogènes $(\cos\theta, \sin\theta, \sin^3\theta)$ ; on remarque que $\Phi(\theta+\pi) = \Phi(\theta)$. L'application $\Phi$ induit donc une bijection de $\mathbb{R}/\pi\mathbb{Z}$ sur $\Gamma$.

   Montrons maintenant que si $a, b, c$ sont des réels tels que $a + b + c \equiv 0 \bmod \pi$, alors les points $\Phi(a), \Phi(b), \Phi(c)$ sont alignés. Il suffit pour ce faire de montrer que le déterminant

$$\Delta(a, b, c) = \begin{vmatrix} \cos a & \cos b & \cos c \\ \sin a & \sin b & \sin c \\ \sin^3 a & \sin^3 b & \sin^3 c \end{vmatrix}$$

   est nul. On a

$$\sin^3(a) = \left(\frac{e^{ia} - e^{-ia}}{2i}\right)^3 = -\frac{1}{4}(\sin 3a - 3\sin a)\ .$$

   On en déduit

$$-4\Delta(a, b, c) = \begin{vmatrix} \cos a & \cos b & \cos c \\ \sin a & \sin b & \sin c \\ \sin 3a & \sin 3b & \sin 3c \end{vmatrix}\ .$$

   Le cofacteur de $\sin 3c$ dans le dernier déterminant est $\cos a\sin b - \sin a\cos b = \sin(b - a)$, et $\sin(b - a)\sin 3c = \frac{1}{2}(\cos(3c + a - b) - \cos(3c - a + b))$. En utilisant $a + b + c = k\pi$ avec $k \in \mathbb{Z}$,

cette dernière quantité est égale à $\frac{(-1)^k}{2}(\cos(2c-2b)-\cos(2c-2a))$. En faisant la somme de toutes les expressions obtenues par permutation circulaire, on obtient

$$\begin{aligned}&(-1)^{k+1}8\,\Delta(a,b,c)\\ &= \cos(2c-2b)-\cos(2c-2a)+\cos(2a-2c)-\cos(2a-2b)+\cos(2b-2a)-\cos(2b-2c)\\ &= 0\end{aligned}$$

Du calcul que l'on vient de faire découle que si $a, b, -(a+b)$ sont différents modulo $\pi$, le troisième point d'intersection de la droite $\Phi(a)\Phi(b)$ avec la cubique est $\Phi(-(a+b))$. En utilisant un argument de continuité, ceci reste vrai si on autorise des égalités modulo $\pi$ entre ces nombres (la limite de la corde $AB$ quand $B$ tend vers $A$ sur $\Gamma$ est la tangente à $\Gamma$ en $A$). On a en particulier que le troisième point d'intersection de la droite $\Phi(a)\Phi(0) = \Phi(a)\Omega$ avec $\Gamma$ est $\Phi(-a)$. Ceci montre finalement, vu la définition de $*$, que

$$\Phi(a) * \Phi(b) = \Phi(a+b)\ .$$

Il ressort de la paramétrisation en coordonnées polaires que $\Phi(a)$ est l'intersection de $\Gamma$ avec la droite $D(a)$ passant par l'origine $O$ et telle que l'angle de droites $(Ox, D(a))$ soit égal à $a$ (modulo $\pi$). Donc, géométriquement, $A*B$ est l'intersection avec $\Gamma$ de la droite $D$ passant par $O$ telle que $(Ox, D) = (Ox, OA) + (Ox, OB)$.

(c) L'application $\Phi$ induit donc un isomorphisme du groupe $(\mathbb{R}/\pi\mathbb{Z}, +)$ sur le groupe $(\Gamma, *)$. Avec l'isomorphisme $a \mapsto e^{2ia}$ de $\mathbb{R}/\pi\mathbb{Z}$ sur le groupe $S^1$ des nombres complexes de module un, on obtient ainsi un isomorphisme de $S^1$ sur $\Gamma$ (on pourrait montrer que c'est aussi un difféomorphisme).

Les éléments d'ordre 6 de $\mathbb{R}/\pi\mathbb{Z}$ sont les classes de $\pi/6$ et $-\pi/6$. Les points d'ordre 6 de $\Gamma$ sont donc $\Phi(\pm\pi/6) = (\frac{\sqrt{3}}{2}, \pm\frac{1}{2}, \pm\frac{1}{8})$ soit en coordonnées affines $(4\sqrt{3}, 4)$ et $(-4\sqrt{3}, 4)$. On peut remarquer aussi que les points d'inflexion de $\Gamma$ (où la tangente a une intersection triple avec la courbe) sont les $\Phi(a)$ avec $3a \equiv 0 \bmod \pi$, soit $\Phi(0) = \Omega$ et $\Phi(\pm\frac{\pi}{3})$.

# Partie V

On note $\Gamma'$ la courbe d'équation $y^2 + y = x^3 + x$ dans $\mathbb{F}_{16}^2$.

1. Pour chaque $x$ de $\mathbb{F}_{16}$, l'équation $y^2 + y = x^3 + x$ du 2-ème degré en $y$ a au plus deux solutions dans $\mathbb{F}_{16}$. Il y a donc au plus 32 points $(x, y)$ dans $\Gamma'$.
2. Le polynôme homogène $\overline{P} = X^3 + XZ^2 - Y^2Z - YZ^2$ définit une cubique $\Gamma$ dans le plan projectif sur $\mathbb{F}_{16}$. Cette cubique a pour point à l'infini le point $\Omega$ de coordonnées homogènes $(0, 1, 0)$ ; en effet $\overline{P}(X, Y, 0) = X^3$. On a $\Gamma = \Gamma' \cup \{\Omega\}$.

   Si $A$ et $B$ sont deux points de $\Gamma$, alors la droite $AB$ (ou la tangente à $\Gamma$ passant par $A$ si $B = A$, voir plus loin la question 4) recoupe $\Gamma$ en un troisième point $C$. La droite $\Omega C$ recoupe $\Gamma$ en un troisième point $A * B$.

   Le fait qu'il n'y ait pas de droite contenue dans la cubique est conséquence du calcul explicite sur les tangentes fait dans la question 4.
3. (a) La multiplication $*$ définie ci-dessus est clairement commutative puisque la droite $AB$ est la même que la droite $BA$ ! L'élément neutre est $\Omega$, et l'inverse d'un élément $A \in \Gamma$ est le troisième point $i(A)$ d'intersection de la droite $A\Omega$ avec $\Gamma$. Le premier point est clair par définition de $*$. Pour vérifier que $i(A)$ est bien l'inverse de $A$, il faut voir que la tangente à $\Gamma$ en $\Omega$ est la droite de l'infini $Z = 0$, qui coupe $\Gamma$ en $\Omega$ avec multiplicité 3 comme on l'a vu ci-dessus.

(b) L'inverse d'un élément $(\alpha, \beta)$ est $(\alpha, 1+\beta)$. Les doites passant par $\Omega$ sont les droites d'équation $X = aZ$ dans le plan projectif (ou d'équation $x = a$ dans le plan affine) et la droite de l'infini $Z = 0$. L'intersection d'une droite $x = a$ avec $\Gamma'$ est donnée par les solutions dans $\mathbb{F}_{16}$ de l'équation $y^2 + y = a^3 + a$. Si $y_1$ est une solution de cette équation, alors $y_2 = y_1 + 1$ est l'autre solution (en effet $y_2 + 1 = y_1$). Ceci montre que l'inverse d'un élément $(\alpha, \beta)$ de $\Gamma'$ est l'élément $(\alpha, \beta + 1)$.

4. La tangente à $\Gamma'$ en $A = (\alpha, \beta) \in \Gamma'$ est la droite dont l'intersection avec $\Gamma'$ admet $A$ comme point de multiplicité au moins deux.

   (a) La droite passant par $A$ de vecteur directeur $(u, v)$ est paramétrée par $(\alpha + tu, \beta + tv)$ (avec $t \in \mathbb{F}_{16}$. Elle admet $A$ comme point d'intersection de multiplicité au moins 2 avec $\Gamma'$ si et seulement si 0 est racine multiple du polynôme $P(\alpha + tu, \beta + tv)$ (considéré comme polynôme en $t$). Le polynôme $P(\alpha + tu, \beta + tv)$ a un terme constant $P(\alpha, \beta)$ nul, et le coefficient de $t$ est $uP'_X(\alpha, \beta) + vP'_Y(\alpha, \beta)$. Remarquons que $P'_Y = 1$ n'est jamais nul. Donc il y a une seule droite dont l'intersection avec $\Gamma'$ admet $A$ comme point multiple, et cette droite est la droite d'équation
   $$P'_X(\alpha, \beta)(x - \alpha) + P'_Y(\alpha, \beta)(y - \beta) = 0 \, .$$

   (b) On a déjà dit que $P'_Y = 1$, et $P'_X = X^2 + 1$ (rappelons que tous les calculs se font en caractéristique 2 ; on peut remplacer tout entier par 0 ou 1 suivant la parité et ne pas tenir compte des signes). La tangente en $A$ est la droite d'équation
   $$(\alpha^2 + 1)(x - \alpha) + y - \beta = 0 \, .$$

   Pour trouver le troisième point d'intersection de cette tangente avec $\Gamma$, portons la représentation paramétrique $x = \alpha - t$, $y = \beta + (\alpha^2 + 1)t$ dans l'équation de $\Gamma'$. On trouve $t^2(1 + \alpha + \alpha^4 + t) = 0$, et donc le troisième point d'intersection correspond au paramètre $t = 1 + \alpha + \alpha^4$. Ce point d'intersection a pour coordonnées
   $$\begin{aligned} x &= 1 + \alpha^4, \\ y &= \beta + (1 + \alpha^2)(1 + \alpha + \alpha^4) = \beta + 1 + (\alpha + \alpha^3) + (\alpha^2 + \alpha^6) + \alpha^4 \\ &= \beta + 1 + (\beta + \beta^2) + (\beta^2 + \beta^4) + \alpha^4 = 1 + \beta^4 + \alpha^4 \, . \end{aligned}$$

   En prenant l'inverse, on obtient
   $$A * A = (1 + \alpha^4, \beta^4 + \alpha^4) \, .$$

   (c) En utilisant le dernier résultat, on trouve
   $$A^4 = (1 + (1 + \alpha^4)^4, (\beta^4 + \alpha^4)^4 + (1 + \alpha^4)^4) = (\alpha^{16}, 1 + \beta^{16}) = (\alpha, 1 + \beta) = A^{-1} \, .$$

   (d) Le groupe abélien $\Gamma$ est de cardinal inférieur ou égal à 33, et tout élément différent de l'élément neutre est d'ordre 5 d'après la question précédente. Donc $\Gamma$ est isomorphe soit à $\mathbb{Z}/5\mathbb{Z}$, soit à $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ (on peut invoquer le théorème de structure des groupes abéliens finis). On a déjà cinq éléments évidents dans $\Gamma$ : $\Omega$ et les points $(0, 0), (0, 1), (1, 0), (1, 1)$ de $\Gamma'$. En voici au moins un sixième : $(\gamma, \gamma^3)$ avec $\gamma$ élément d'ordre 5 de $\mathbb{F}_{16}^*$. En effet $(\gamma^3)^2 + \gamma^3 = \gamma^3 + \gamma$. On conclut que $\Gamma$ est isomorphe à $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ et a donc 25 éléments.

5. Le système de cryptographie décrit dans la partie II s'applique à n'importe quel groupe où l'on sait calculer effectivement, en particulier au groupe $\Gamma$. On peut tout de même remarquer que si $\alpha$ et $\pi$ sont des éléments connus de $\Gamma$ tels que $\alpha$ est une puissance de $\pi$, il n'est pas trop dur de trouver $e$ vérifiant $\alpha = \pi^e$ vu que $\pi$ est d'ordre 5.