Partiel de Cryptologie

11 mars 2020
Durée 1h45

Auteurs
Jérémy Berthomieu & Valérie Ménissier-Morain

Version du 4 avril 2020

Le seul document autorisé est une feuille manuscrite A4 recto-verso.
L'utilisation d'un appareil électronique est proscrite pendant toute la durée de l'épreuve.
Le barème sur 25,25 points (plus 2 de bonus) est indicatif. La note finale sera le minimum entre les points obtenus et 20.

Exercice 1 – Chiffrement à quatre carrés – 4 points

Le chiffre des quatre carrés est un chiffre apparenté au chiffrement de Playfair, mais inventé par le français Félix Delastelle sans qu'il ait connaissance du chiffrement anglais.

Il se présente sous la forme de 4 tableaux carrés 5×5, que l'on écrit eux-mêmes dans un carré plus grand. Chaque carré contient les 25 lettres de l'alphabet (on identifie le I et le J, ou on oublie le W). Dans les carrés en haut à gauche et en bas à droite, ces 25 lettres sont écrites dans l'ordre alphabétique. Dans les deux autres carrés, elles sont écrites dans un ordre quelconque, par exemple en utilisant un mot-clef, comme nous l'avons vu pour le carré de Polybe. Par exemple avec les mots-clefs `JULES` et `CESAR`, on obtient le tableau :

A	B	C	D	E
F	G	H	I	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

I	U	L	E	S
A	B	C	D	F
G	H	K	M	N
O	P	Q	R	T
V	W	X	Y	Z

C	E	S	A	R
B	D	F	G	H
I	K	L	M	N
O	P	Q	T	U
V	W	X	Y	Z

A	B	C	D	E
F	G	H	I	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

Comme pour le chiffrement de Playfair, on analyse le texte par groupe de 2 caractères : on cherche
— le premier caractère c_1 dans le carré en haut à gauche
— le second c_2 dans le carré en bas à droite,
on leur associe
— le caractère du carré en haut à droite de même ligne que c_1 et de même colonne que c_2
— le caractère du carré en bas à gauche de même colonne que c_1 et de même ligne que c_2.
Par exemple le bigramme `VM` est chiffré en `WI`.

Si le texte contient un nombre impair de caractères on ajoute un caractère neutre tel que `X` pour avoir un bigtamme complet à chiffrer.

1. (**1 point**) Chiffrer le message `À l'ouest rien de nouveau` avec le carré ci-dessus.

Solution :
On doit chiffrer
`AL OU ES TR IE ND EN OU VE AU`, ce qui est chiffré par
`II NT LU PT FA MS LN NT ZC SO`, soit au format classique `IINTL UPTFA MSLNN TZCSO`.

2. (**1 point**) Déchiffrer le message `RFTTZ CQZGC GRCYH USNUO INUBT RPPLZ` avec le carré ci-dessus.

Solution :
On doit déchiffrer `RF TT ZC QZ GC GR CY HU SN UO IN UB TR PP LZ`. On identifie pour le premier bigramme, le caractère `R` dans le carré en haut à droite et le caractère `F` dans le carré en bas à gauche, ils correspondent à `S` en haut à gauche et `I` en bas à droite. On continue de la même façon pour les autres bigrammes. ON constate que le dernier bigramme `LZ` correspond à `EX`, le message d'origine était de longueur impaire et on a donc ajouté un caractère neutre pour le chiffrement.
Pour récapituler, on devait déchiffrer
`RF TT ZC QZ GC GR CY HU SN UO IN UB TR PP LZ` et on obtient
`SI TU VE UX LA PA IX PR EP AR EL AG UE RR EX`, soit `Si tu veux la paix prépare la guerre(x)`.

3. (**2 points**) Que pouvez-vous dire de la difficulté de chiffrement, de déchiffrement et de cryptanalyse de ce cryptosystème ?

Solution :
Lorsqu'on dispose des 4 carrés, le chiffrment et le déchiffrement sont plus simples que ceux de Playfair puisqu'il y a moins de cas particuliers.
Cependant, son utilisation en pratique est plus lourde puisqu'elle nécessite la mise en place de deux carrés non trivuax et deux carrés triviaux, et préparer la feuille de chiffrement / déchiffrement prend du temps : on peut imaginer que l'opérateur dun groupe d'éclaireurs garde dans un coin de sa tête `JULES` et `CESAR` comme clef plutôt qu'il ne s'approche de l'ennemi avec un papier où les carrés sont prêts à être employés, la sécurité de la clef retarde la transmission de messages cruciaux.
La clef est composée de deux carrés de 25 caractères, pour chacun il y a 25! possibilités si on choisit des permutations complètement aléatoires, il y a donc $25!^2$ clefs possibles, ce qui est significativement plus que pour Playfair. Cependant une clef complètement aléatoire est plus difficile à transporter : deux carrés aléatoires sont trop difficiles à mémoriser et à reproduire sur le terrain donc il est nécessaire d'avoir toujours avec soi un papier avec les quatre carrés ce qui est une brèche de sécurité. En pratique on privilégie l'usage de deux mots-clefs, ce qui diminue significativement la sécurité du cryptosystème et au final on ne gagne pas grand chose par rapport à la sécurité d'un Playfair avec mot-clef.
Il y a cependant deux aspects en quoi ces chiffrements diffèrent :
- dans Playfair, si m_1m_2 est chiffré en c_1c_2 alors m_2m_1 est chiffré en c_2c_1, ce qui divise par 2 le nombre d'associations de bigrammes à retrouver.
- de même dans Playfair il n'y a de pas bigrammes composés de deux lettres identiques, ce qui apporte une nouvelle réduction du nombre de possibilités pour la substitution.

Ici il n'y a pas de telle symétrie et les bigrammes composés de lettres identiques sont autorisés donc la complexité de ce cryptosystème est tout de même nettement supérieure à celle de Playfair.
En pratique, étant donné que :
- la mise en œuvre du chiffrement et déchiffrement du chiffrement à 4 carrés est plus pénible,
- la cryptanalyse du chiffrement à 4 carrés avec mots-clefs n'est que marginalement plus difficile que celle de Playfair,
- les deux systèmes nécessitent les mêmes techniques de cryptanalyse,

Playfair a été beaucoup plus utilisé.

Exercice 2 – Questions de base – 9 points

1. (**1,5 point**) Qu'est-ce qu'un chiffrement polygrammique ? Comment le modélise-t-on ? Quels sont les chiffrements polygrammiques vus dans cette UE ?

> **Solution :**
> Il s'agit de substituer plusieurs caractères à la fois sur un alphabet A 0.5 point, on modélise ce chiffrement par $\mathcal{P} = \mathcal{C} = A^n$ et $\mathcal{K} \subseteq (A^n)^2$ 0.5 point. Par exemple dans le chiffrement de Playfair on chiffre par couples de caractères ($n = 2$) 0.25 point. On a aussi vu le chiffrement de Hill en TD présenté pour n quelconque et détaillé pour $n = 2$ 0.25 point.

2. (**1 point**) Que vous évoque le nom Venona ? À quelle notion de cryptologie est-il associé ?

> **Solution :**
> Le projet Venona est le travail de cryptanalyse effectué par les services de renseignement américains pour tenter de casser les codes des communications des services de renseignement soviétiques, émises de 1940 à 1948. Ce travail dura de 1943 à 1980 et permit de décrypter partiellement ou totalement environ 3 000 messages. Ces messages décryptés furent, durant les premières années de la guerre froide, une source importante d'information sur les activités des services de renseignement soviétiques, permettant notamment de découvrir le réseau des « cinq de Cambridge »et de plusieurs espions travaillant dans le domaine nucléaire.
>
> Ces services de renseignement avaient à leur disposition de grandes quantités de trafic chiffré émis par les services diplomatiques et commerciaux de l'URSS. Ce trafic était intercepté soit par des stations d'écoute, soit photographié dans les postes de censure instaurés dans les bureaux des opérateurs de télécommunications pendant la Seconde Guerre mondiale.
>
> Ce trafic était en partie chiffré selon un système *one-time-pad*, il fut conservé et analysé en secret.
>
> La génération de clés à usage unique était à l'époque un processus lent et demandant beaucoup d'efforts, et la guerre avec l'Allemagne à partir de juin 1941 créa un besoin de plus en plus grand de clés secrètes. Il est fort probable que les opérateurs chargés de générer les codes soviétiques aient commencé à dupliquer les clés de chiffrement pour pouvoir répondre à la demande.
>
> En octobre 1943, l'analyse de milliers de messages du trafic commercial par des calculateurs mécaniques montra que les Soviétiques faisaient du recyclage de clés, offrant un espoir de décrypter les messages.
>
> Les services de renseignement américains utilisèrent toutes ces données pour décrypter ce qui s'avéra être du trafic du ministère de l'Intérieur soviétique. Le 20 décembre 1946, ils mirent au jour les premiers morceaux de données décryptées, qui révélèrent l'existence d'espions soviétiques au sein du projet Manhattan.

3. (**1,5 point**) Quel est l'angle d'attaque des substitutions mono-alphabétiques ? Quels types de chiffrement ont été proposé pour contrer ce type d'attaque jusqu'à la première guerre mondiale ?

> **Solution :**
> On casse une substitution mono-alphabétique avec l'analyse de fréquences des caractères et des bigrammes de l'alphabet.
>
> Pour y remédier on va brouiller l'analyse de fréquences par du
> - chiffrement homophonique : les caractères les plus fréquents de la langue sont chiffrés par plusieurs symboles ;
> - chiffrement poly-alphabétique : on combine plusieurs substitutions sur un même texte ;
> - chiffrement polygrammique : on chiffre plusieurs caractères à la fois, ce qui conduit à travailler sur un alphabet beaucoup plus grand avec des fréquences beaucoup moins nette ;

— surchiffrement : on applique un second système de chiffrement sur le message chiffré une première fois, pour cela on utilise deux cryptosystèmes différents ou bien le même cryptosystème mais avec des clefs différentes.

4. (**1 point**) Soit n un entier et a un élément de $\mathbb{Z}/n\mathbb{Z}$. Si a est inversible peut-il être un diviseur de zéro (argumentez votre réponse) ? Si a est diviseur de zéro, comment calculer l'entier $b \in \mathbb{Z}/n\mathbb{Z}$ tel que $ab = 0$?

Solution :
Supposons qu'un élément a soit inversible et qu'il existe b tel que $ab = 0$. Alors $b = 1\,b = (a^{-1}\,a)\,b = a^{-1}\,(ab) = a^{-1}\,0 = 0$ donc $b = 0$. Par conséquent si a est inversible alors a n'est pas diviseur de zéro. 0.5 point
Si a est un diviseur de zéro, alors le pgcd de a et de n dans $\mathbb{Z}$ est $d > 1$ avec $a = a'd$ et $n = n'd$, a' et b' entiers premiers entre eux et $0 < n' < n$ donc $b = n' \in \mathbb{Z}/n\mathbb{Z}$ vérifie $ab = a'dn' = a'n = 0 \mod n$0.5 point.
$u_{k+1}\,a + v_{k+1}\,n = r_{k+1} = 0$ à la dernière étape de l'algorithme d'Euclide étendu $|u_{k+1}| < n$ est un témoin de diviseur de zéro de a pour n 0.5 point.

5. (**3 points**) En utilisant l'algorithme d'Euclide étendu, dites si $a = 714$ est inversible modulo $n = 819$ et si oui quel est son inverse ? est-il un diviseur de zéro dans $\mathbb{Z}/n\mathbb{Z}$? et si oui quel est son témoin de diviseur de zéro de a pour n ?
Mêmes questions pour $a = 727$.

Solution :
On va appliquer l'algorithme d'Euclide étendu à $a = 714$ et $b = 819$.
On utilise les notations usuelles, l'algorithme s'écrit

$$\begin{cases} u_0 = 1, & v_0 = 0, & r_0 = a \\ u_1 = 0, & v_1 = 1, & r_1 = b \\ u_{i+1} = u_{i-1} - q_i u_i, & v_{i+1} = v_{i-1} - q_i v_i, & r_{i+1} = r_{i-1} - q_i r_i \quad i \geqslant 1 \end{cases}$$

avec $q_i = \left\lfloor \dfrac{r_{i-1}}{r_i} \right\rfloor$ si $r_i \neq 0$ et sinon on s'arrête.
On a $r_i = u_i\,a + v_i\,b \ \ \forall i$.
On produit le tableau suivant :

i	r_{i-1}	q_i	r_i	r_{i+1}	u_{i+1}	v_{i+1}
				819	1	0
			819	714	0	1
0	819	1	714	105	1	−1
1	714	6	105	84	−6	7
2	105	1	84	21	7	−8
3	84	4	21	0	−34	39

On constate qu'à l'étape $i = 3$, $r_{i+1} = 0$, donc $r_3 = 21$ est le dernier reste non nul, c'est-à-dire le pgcd de a et b, et on lit la relation de Bézout à la ligne $i = 2$: $7 * 819 - 8 * 714 = 21$ d'une part à la ligne 2 et sur la ligne suivante $-34 * 819 + 39 * 714 = 0$. $r_3 \neq 1$ donc 714 n'est pas inversible modulo 819. En revanche 714 est un diviseur de zéro modulo 819 de témoin 39.

De même pour $a = 727$ on applique l'algorithme d'Euclide à 727 et 819 et on dresse le tableau

i	r_{i-1}	q_i	r_i	r_{i+1}	u_{i+1}	v_{i+1}
				819	1	0
			819	727	0	1
0	819	1	727	92	1	−1
1	727	7	92	83	−7	8
2	92	1	83	9	8	−9
3	83	9	9	2	−79	89
4	9	4	2	1	324	−365
5	2	2	1	0	−727	819

On constate qu'à l'étape $i = 5$, $r_{i+1} = 0$, donc $r_4 = 1$ est le dernier reste non nul, c'est-à-dire le pgcd de a et b et on lit la relation de Bézout $324 * 819 - 365 * 727 = 1$ à la ligne 4. $r_4 = 1$ donc 727 est inversible modulo 819 d'inverse $727^{-1} = -365 = 819 - 365 = 454 \bmod 819$.

6. (**1 point**) Donner un groupe cyclique d'ordre $n > 0$ où le problème du logarithme discret est facile ? Quel algorithme utilise-t-on pour le résoudre et avec quelle complexité ?

Solution :
0,25 point $\mathbb{Z}/n\,\mathbb{Z}$.
0,25 point L'algorithme d'Euclide étendu. 0 point BSGS de Shanks car il est bien trop lent dans ce cas !
0,5 point Sa complexité est quadratique en la taille de n, c'est-à-dire en $O((\log n)^2)$.

Exercice 3 – 12,25 points

On considère l'ensemble $\mathcal{E}$ muni de la loi $\circ$, supposée associative. Les éléments de $\mathcal{E}$ sont tous de la forme $P = (x, y)$ avec x et y modulo 11 sauf un, noté $\mathcal{O}$. De plus, $P = (x, y) \in \mathcal{E}$ si, et seulement si, $y^2 = x^3 + 3\,x + 3 \bmod 11$.

1. (**1 point**) Vérifier que $(0, 5), (5, 0), (9, 0), (7, 2) \in \mathcal{E}$.

Solution :
- $0^3 + 3 \times 0 + 3 = 3$ et $5^2 = 25 = 3$;
- $5^3 + 3 \times 5 + 3 = 3 \times 5 + 3 \times 5 + 3 = 0$ et $0^2 = 0$;
- $9^3 + 3 \times 9 + 3 = 9 \times 4 + 5 + 3 = 0$ et $0^2 = 0$;
- $7^3 + 3 \times 7 + 3 = 7 \times 5 + 10 + 3 = 4$ et $2^2 = 4$.

On admet dans la suite qu'avec $(0, 6), (7, 9), (8, 0)$ ce sont les seuls éléments de $\mathcal{E} - \{\mathcal{O}\}$.

2. (**0,5 point**) Pour $P, Q \in \mathcal{E}$, on note $R = P \circ Q \in \mathcal{E}$. De plus,
   (i). si $Q = \mathcal{O}$, alors $R = P$, sinon si $P = \mathcal{O}$, alors $R = Q$;
   (ii). sinon, si $P = (x_1, y_1)$ et $Q = (x_1, -y_1)$, alors $R = \mathcal{O}$;
   (iii). sinon, $P = (x_1, y_1)$, $Q = (x_2, y_2) \neq (x_1, -y_1)$ et $R = (x_3, y_3)$ avec

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda\,(x_1 - x_3) - y_1$$

   et $\lambda = 7\,(x_1^2 + 1)\,y_1^{-1} \bmod 11$ si $P = Q$ ou $\lambda = (y_2 - y_1)\,(x_2 - x_1)^{-1} \bmod 11$ sinon.

Quel est le neutre pour $\circ$? Quel est l'inverse de $P \in \mathcal{E}$ pour $\circ$?

Solution :
0,25 point Par la propriété (i), $\mathcal{O}$ est le neutre.
0,25 point Donc si $P = \mathcal{O}$, alors naturellement il est son propre inverse. Sinon, la propriété (ii) nous dit que l'inverse de (x_1, y_1) est $(x_1, -y_1)$.

3. (**1 point**) Montrer que $(\mathcal{E}, \circ)$ est un groupe.

Solution :
Par hypothèse, si $P, Q \in \mathcal{E}$, alors $P \circ Q \in \mathcal{E}$ et $\circ$ est associative. De plus, $\circ$ admet un élément neutre $\mathcal{O}$ et pour tout $P \in \mathcal{E}$, il existe un inverse de P, noté P^{-1}, tel que $P \circ P^{-1} = \mathcal{O}$. Ainsi $(\mathcal{E}, \circ)$ est un groupe.

4. (**1 point**) Quel est l'ordre de $\mathcal{E}$? Sans calcul, quels peuvent être les ordres des éléments de $\mathcal{E}$?

Solution :
0,25 point Par la question 1, $\mathcal{E} = \{\mathcal{O}, (0,5), (0,6), (5,0), (7,2), (7,9), (8,0), (9,0)\}$ donc $\mathcal{E}$ est d'ordre 8.
0,25 point pour la liste + 0,5 point pour Lagrange Les ordres possibles, par le corollaire du théorème de Lagrange, des éléments de $\mathcal{E}$ sont tous les diviseurs de $|\mathcal{E}| = 8$, à savoir 1, 2, 4 et 8.

5. (**2,5 points**) Montrer que $\circ$ est commutative.

Solution :
0,5 point Il faut montrer que $P \circ Q = Q \circ P$ pour $P, Q \neq \mathcal{O}$. Si $Q = P$, c'est évident donc on peut supposer $Q \neq P$. Si $R = P \circ Q = \mathcal{O}$, alors $S = Q \circ P = \mathcal{O}$ donc on peut supposer que $S \neq \mathcal{O}$.
Notons $S = (x_4, y_4) = Q \circ P$, alors, par la propriété (iii), $x_4 = \mu^2 - x_2 - x_1$ et $y_4 = \mu(x_1 - x_4) - y_2$ avec 0,5 point $\mu = (y_1 - y_2)(x_1 - x_2)^{-1} \bmod 11 = (y_2 - y_1)(x_2 - x_1)^{-1} \bmod 11 = \lambda$.
0,5 point Ainsi, $x_4 = \lambda - x_1 - x_2 = x_3$.
1 point ou 0,5 si tentative de développer y_3 et y_4 Il reste à montrer que $y_4 = \lambda(x_2 - x_3) - y_2 = y_3$. On calcule $y_3 - y_4 = \lambda(x_1 - x_3) - y_1 - \lambda(x_2 - x_3) + y_2 = \lambda(x_1 - x_2) - (y_1 - y_2) = (y_2 - y_1)(x_2 - x_1)^{-1}(x_1 - x_2) - (y_1 - y_2) = 0$.
Donc $S = R$ et $\circ$ est commutative.

6. (**0,25 point**) Montrer que si $P = (x_1, 0) \in \mathcal{E}$, alors $[2]P = P \circ P = \mathcal{O}$.

Solution :
0,25 point Par la propriété (ii), $[2]P = P \circ P = (x_1, 0) \circ (x_1, -0) = \mathcal{O}$.

7. (**1,5 point**) Réciproquement, montrer que si $P = (x_1, y_1) \in \mathcal{E}$ avec $y_1 \neq 0$, alors $[2]P = (9, 0)$. Qu'en déduit-on sur l'ordre d'un tel P ?

Solution :
0,25 point par calcul
- $P = (0,5)$, $\lambda = 7 \times 5^{-1} = 7 \times 9 = 8$, $x_3 = 8^2 - 0 = 9$ et $y_3 = 8(0 - 9) - 5 = 0$.
- De même, $P = (0,6)$, $\lambda = 7 \times 6^{-1} = 7 \times 2 = 3$, $x_3 = 3^2 - 0 = 9$ et $y_3 = 3(0 - 9) - 6 = 0$.
- $P = (7,2)$, $\lambda = 7(7^2 + 1)2^{-1} = 7 \times 6 \times 6 = 10$, $x_3 = 10^2 - 7 - 7 = 9$ et $y_3 = 10(7 - 9) - 2 = 0$.
- De même, $P = (7,9)$, $\lambda = 7(7^2 + 1)9^{-1} = 7 \times 6 \times 5 = 1$, $x_3 = 1^2 - 7 - 7 = 9$ et $y_3 = 1(7 - 9) - 9 = 0$.

0,5 point Comme $[2]P = (9,0)$ et $[2](9,0) = \mathcal{O}$ par la question précédente, alors $[4]P = \mathcal{O}$ et P est d'ordre 4.

8. (**1 point**) $(\mathcal{E}, \circ)$ est-il cyclique ?

Solution :
1 point Il n'existe aucun élément d'ordre $|\mathcal{E}| = 8$ donc non, il n'est pas cyclique.
Alternative, 1 point On aurait aussi pu constater qu'il y a 3 éléments d'ordre 2 qui engendrent 3 sous-groupes distincts d'ordre 2. Ceci n'est pas possible dans un groupe cyclique d'ordre n où pour tout diviseur d de n, il existe un unique sous-groupe d'ordre d, comme vu dans le TD1, exercice 19, question 6.

9. (**1 point**) Calculer $(0,5) \circ (9,0)$. En déduire le sous-groupe engendré par $(0,5)$.

Solution :
0,5 point Par la propriété (iii), on a $R = (x_3, y_3) = (0,5) \circ (9,0)$ avec $\lambda = (0-5)\,(9-0)^{-1} = -5 \times 5 = -25 = 8$, $x_3 = 8^2 - 0 - 9 = 0$ et $y_3 = 8\,(0-0) - 5 = 6$ donc $R = (0,6)$.
0,5 point Or, $(9,0) = [2]\,(0,5)$ donc $R = [3]\,(0,5)$, ainsi, $\langle (0,5) \rangle = \{\mathcal{O}, (0,5), (9,0), (0,6)\}$.

10. (**2 points**) On considère l'ensemble $\mathcal{F}$ des éléments de $\mathcal{E}$ qui s'écrivent sous la forme $[i]\,P \circ [j]\,Q$ avec $P = (0,5)$ et $Q = (5,0)$, $(i,j) \in \{0,1,2,3\} \times \{0,1\}$, avec la convention que $[0]\,P = [0]\,Q = \mathcal{O}$.
Montrer que $\mathcal{F}$ est sous-groupe de $\mathcal{E}$ d'ordre supérieur ou égal à 5.

Solution :
0,25 point Par définition, le neutre, $\mathcal{O}$, est dans $\mathcal{F}$.
0,25 point Si $R = [i]\,P \circ [j]\,Q$ et $S = [k]\,P \circ [\ell]\,Q$ sont dans $\mathcal{F}$, alors $R \circ S = [i]\,P \circ [j]\,Q \circ [k]\,P \circ [\ell]\,Q = [i]\,P \circ [k]\,P \circ [j]\,Q \circ [\ell]\,Q = [i+k]\,P \circ [j+\ell]\,Q$.
0,5 point Or, P est d'ordre 4 donc $i+k$ peut être réduit modulo 4 et de même Q est d'ordre 2 donc $j+\ell$ peut être réduit modulo 2. Ainsi, $R \circ S \in \mathcal{F}$.
0,5 point L'inverse de R est S tel que $i + k = 0 \bmod 4$ et $j + \ell = 0 \bmod 2$, c'est-à-dire $k = 4 - i \bmod 4$ et $\ell = 2 - j \bmod 2 = j$ donc $S \in \mathcal{F}$.
0,5 point Enfin, $\mathcal{F}$ contient tout le sous-groupe engendré par $P = (0,5)$, c'est-à-dire $\{\mathcal{O}, (0,5), (9,0), (0,6)\}$, et $Q = (5,0)$ donc au moins 5 éléments distincts.

11. (**0,5 point**) En déduire que $\mathcal{F} = \mathcal{E}$.

Solution :
0,25 point pour Lagrange + 0,25 point pour son application Par le théorème de Lagrange, $|\mathcal{F}|$ divise $|\mathcal{E}| = 8$. Or, $|\mathcal{F}| \geq 5$ donc $|\mathcal{F}| = 8$ et $\mathcal{F} = \mathcal{E}$.