

## Correction de l'examen du 16 janvier 2018

### Exercice 1

- 1) L'entier 51 est divisible par 3. On constate que 53 n'est pas divisible par les nombres premiers 2, 3, 5 et 7, donc 53 est l'entier cherché.
- 2.1) On a  $\varphi(100) = \varphi(4)\varphi(25)$ , d'où  $\varphi(100) = 40$ .
- 2.2) L'entier 3 est premier avec 100. D'après le théorème d'Euler, on a donc la congruence  $3^{40} \equiv 1 \pmod{100}$ . On en déduit que  $3^{200} \equiv 1 \pmod{100}$ . L'écriture décimale de  $3^{200}$  se termine donc par 01.
- 3) D'après le corollaire 2.2 du cours, l'ordre de la classe de  $a$  est  $\frac{n}{\text{pgcd}(n,a)}$ .
- 4) On a  $175 = 5^2 \times 7$ . En particulier les entiers 89 et 175 sont premiers entre eux. La classe de 89 est donc inversible dans l'anneau  $\mathbb{Z}/175\mathbb{Z}$ . Afin de calculer son inverse, déterminons une relation de Bézout entre les entiers 175 et 89. En utilisant l'algorithme d'Euclide, on obtient le tableau suivant :

	1	1	28	1	2	
175	89	86	3	2	1	0
1	0	1	-1	29	-30	
0	1	-1	2	-57	59	

On en déduit que l'on a  $-30 \times 175 + 59 \times 89 = 1$ . Par suite, la classe de 59 est l'inverse de celle de 89.

- 5) D'après le théorème 6.6 du cours, on a l'égalité  $X^{q^\ell} - X = \prod F$ , où  $F$  parcourt l'ensemble des polynômes irréductibles unitaires de  $K[X]$  de degré divisant  $\ell$ . Il y a  $q$  polynômes unitaires de degré 1. Parce que  $\ell$  est un nombre premier, on a donc  $q^\ell = q + I_\ell(q)\ell$ , d'où

$$I_\ell(q) = \frac{q^\ell - q}{\ell}.$$

### Exercice 2

- 1) On vérifie que dans  $\mathbb{F}_2[X]$  on a l'égalité

$$f = (X^2 + X + 1)(X^3 + X^2) + 1.$$

Ainsi, 1 est le reste de la division euclidienne de  $f$  par  $X^2 + X + 1$ .

- 2) Ce sont les polynômes  $X$ ,  $X + 1$  et  $X^2 + X + 1$ .
- 3) Le polynôme  $f$  n'a pas de racines dans  $\mathbb{F}_2$ . Par ailleurs,  $X^2 + X + 1$  est le seul polynôme irréductible de degré 2 de  $\mathbb{F}_2[X]$ . Il ne divise pas  $f$  (question 1). En particulier,  $f$  n'est pas divisible par un polynôme de  $\mathbb{F}_2[X]$  de degré 3, d'où le résultat.

- 4) Le polynôme  $f$  étant irréductible,  $K$  est un corps.
- 5) Sa caractéristique est 2 et son cardinal est  $2^5 = 32$ .
- 6) Le groupe  $K^*$  est d'ordre 31, qui est un nombre premier. Pour tout  $x \in K^*$ , distinct de 1, l'ordre de  $x$ , qui divise 31, est donc 31.
- 7) On a l'égalité  $\alpha^5 = \alpha^2 + 1$ , d'où  $\alpha^8 = \alpha^5 + \alpha^3$ , autrement dit

$$\alpha^8 = 1 + \alpha^2 + \alpha^3.$$

Ainsi les coordonnées de  $\alpha^8$  dans  $\mathcal{B}$  sont  $(1, 0, 1, 1, 0)$ .

- 8) On a  $\alpha^{10} = (\alpha^2 + 1)^2 = \alpha^4 + 1$ , d'où  $n = 10$ .
- 9) Parce que  $K^*$  est d'ordre 31, on a  $\alpha^{31} = 1$ . D'après la question précédente, l'inverse de  $\alpha^4 + 1$  est donc  $\alpha^{21}$ . On a les égalités (question 7)

$$\alpha^{20} = \alpha^8 + 1 = \alpha^2 + \alpha^3.$$

On obtient ainsi

$$(\alpha^4 + 1)^{-1} = \alpha^3 + \alpha^4.$$

Les coordonnées de  $(\alpha^4 + 1)^{-1}$  dans  $\mathcal{B}$  sont donc  $(0, 0, 0, 1, 1)$ .

- 10.1) On a  $\beta^3 = \beta + 1$ , d'où  $\beta^6 = \beta^2 + 1$ , puis  $\beta^7 = \beta^3 + \beta$ . On a donc

$$\beta^7 = 1.$$

On peut aussi remarquer que  $\beta^2$  et  $\beta^4$  sont les deux autres racines de  $g$ , d'où l'égalité  $g = (T - \beta)(T - \beta^2)(T - \beta^4)$ , ce qui implique  $\beta^7 = 1$ .

- 10.2) Supposons  $g$  réductible dans  $K[T]$ . Dans ce cas, le polynôme  $g$  étant de degré 3, il possède une racine  $\beta \in K$ . On a  $\beta \neq 1$ , donc  $\beta$  est d'ordre 7 dans  $K^*$ , ce qui conduit à une contradiction (car 7 ne divise pas 31).
- 11.1) Le  $K$ -espace vectoriel  $L$  est de dimension 3. On a donc  $q = 2^{15} = 32768$  (cor. 6.3).
- 11.2) Identifions  $K$  à un sous-corps de  $L$ . L'élément  $\alpha$  est d'ordre 31 dans  $L^*$  (question 6) et la classe de  $T$  modulo  $(g)$  est d'ordre 7 (question 10.1). Par suite, 7 et 31 divisent  $q - 1$  (th. 2.2). On a  $7 \times 31 = 217$  et

$$\frac{32767}{217} = 151.$$

Par ailleurs, 151 n'est pas divisible par un nombre premier plus petit que 12, donc 151 est premier. La décomposition cherchée est donc donnée par l'égalité

$$q - 1 = 7 \times 31 \times 151.$$

- 11.3) Le nombre de générateurs de  $L^*$  est  $\varphi(q - 1)$  où  $\varphi$  est la fonction indicatrice d'Euler. D'après la question précédente, il est donc égal à

$$6 \times 30 \times 150 = 27000.$$