

Correction de l'examen 20 juin 2018

Exercice 1

- 1) D'après le petit théorème de Fermat, on a $2^{10} \equiv 1 \pmod{11}$. Par suite, on a les congruences $2^{84} \equiv 2^4 \equiv 5 \pmod{11}$. Le reste cherché est donc égal à 5.
- 2) En utilisant l'algorithme d'Euclide, on obtient le tableau suivant :

	1	2	1	3	7	4	
451	331	120	91	29	4	1	0
1	0	1	-2	3	-11	80	
0	1	-1	3	-4	15	-109	

Il en résulte que l'on a $451 \times 80 - 109 \times 331 = 1$, donc le couple $(u, v) = (80, -109)$ convient.

- 3.1) Soit φ la fonction indicatrice d'Euler. Le nombre de générateurs de G est $\varphi(n)$ (th. 2.5 du cours).
- 3.2) L'entier cherché est donc $\varphi(150)$. On a $150 = 2 \times 3 \times 5^2$. On en déduit que l'entier cherché est $\varphi(2)\varphi(3)\varphi(5^2) = 40$.
- 4) On a $143 = 11 \times 13$. Ce n'est pas une puissance d'un nombre premier, donc il n'existe pas de corps de cardinal 143 (cor. 6.1).
- 5) Compte tenu du théorème 6.4, il s'agit d'expliciter un polynôme de degré 3 irréductible dans $\mathbb{F}_2[X]$. Tel est par exemple le cas de $f = X^3 + X + 1$, car il n'a pas de racines dans \mathbb{F}_2 . Par suite, $\mathbb{F}_2[X]/(f)$ est un corps de cardinal 8.

Exercice 2

- 1) On vérifie que le polynôme $X^2 + 1$ n'a pas de racines dans \mathbb{F}_7 , il est donc irréductible dans $\mathbb{F}_7[X]$, donc K est un corps.
- 2) La caractéristique de K est 7 et son cardinal est $7^2 = 49$ (cor. 6.3).
- 3) L'ensemble des ordres possibles est formé des diviseurs de l'ordre de K^* i.e. de 48, c'est donc $\{1, 2, 3, 4, 6, 8, 12, 16, 24, 48\}$.
- 4) Vérifions que \mathcal{B} est une famille libre. Soient a et b dans \mathbb{F}_7 tels que $a + b\alpha = 0$. Cela signifie que le polynôme $a + bX$ est multiple de $X^2 + 1$, d'où $a = b = 0$ et l'assertion. Vérifions que \mathcal{B} est une famille génératrice. Soit $\xi = F + (X^2 + 1)$ un élément de K . D'après le théorème de division euclidienne, il existe $Q \in \mathbb{F}_7[X]$ et $a, b \in \mathbb{F}_7$ tels que $F = (X^2 + 1)Q + a + bX$. On obtient $\xi = a + b\alpha$, d'où le résultat. (Dans le cas général, voir la démonstration du théorème 5.9.)

- 5) On vérifie que l'on a $\beta^2 = 5(\alpha + 1)$, $\beta^4 = \alpha$ puis $\beta^8 = \alpha^2 = -1$.
- 6) Il en résulte que $\beta^{16} = 1$ et que l'ordre de β est 16.
- 7) On a $2^3 = 8 = 1$, donc l'ordre de 2 dans K est égal à 3. D'après la question précédente, l'ordre de 2β est donc 48 (lemme 6.2).
- 8) D'après la question 5, on a $\beta^{16} = 1$, d'où $\beta^{-1} = \beta^{15}$. On a $\beta^8 = \alpha^2 = -1$, d'où $\beta^{-1} = -\beta^7$. En écrivant que l'on a $\beta^7 = \beta \cdot \beta^2 \cdot \beta^4$, on en déduit l'égalité

$$\beta^{-1} = 4 + 2\alpha.$$

Les coordonnées cherchées sont donc $(4, 2)$.

Exercice 3

- 1) L'anneau A est un \mathbb{F}_2 -espace vectoriel de dimension 3. Il en résulte que A est fini de cardinal 8.
- 2) On a $\alpha \neq 0$ et $\alpha^3 = 0$, donc A n'est pas intègre.
- 3) Parce que $(1, \alpha, \alpha^2)$ est une base de A sur \mathbb{F}_2 , on a

$$A = \{0, 1, \alpha, \alpha^2, \alpha + \alpha^2, 1 + \alpha, 1 + \alpha^2, 1 + \alpha + \alpha^2\}.$$

- 4) D'après le théorème 5.10, A^* est formé des classes de polynômes de $\mathbb{F}_2[X]$ premiers avec X . On en déduit que

$$A^* = \{1, 1 + \alpha, 1 + \alpha^2, 1 + \alpha + \alpha^2\}.$$

- 5) On a $|A^*| = 4$ d'où $(1 + \alpha)^4 = 1$. On a $2 = 0$, d'où $(1 + \alpha)^2 = 1 + \alpha^2$ qui est distinct de 1, donc $1 + \alpha$ est d'ordre 4 dans A^* . Par suite, A^* est cyclique.
- 6) Un groupe cyclique d'ordre 4 possède deux générateurs. On a $(1 + \alpha^2)^2 = 1$ donc $1 + \alpha^2$ est d'ordre 2. Les deux générateurs de A^* sont donc $1 + \alpha$ et $1 + \alpha + \alpha^2$.