

Corps finis

Solutions

Exercice 1 – En notant $\alpha \in \mathbb{F}_4$ la classe de X , on a la relation $\alpha^2 = \alpha + 1$, d'où les identités $\alpha^4 = (\alpha + 1)^2 = \alpha^2 + 1 = \alpha$. On remarquera que pour tout $a \in \mathbb{F}_2$, on a la relation $a^4 = a$. Tout élément $x \in \mathbb{F}_4$ s'écrivant de manière unique comme $x = a + b\alpha$, avec $a, b \in \mathbb{F}_2$, on obtient les égalités

$$x^4 = (a + b\alpha)^4 = a^4 + 4a^3b\alpha + 6a^2b^2\alpha^2 + 4ab^3\alpha^3 + b^4\alpha^4 = a^4 + b^4\alpha^4 = a + b\alpha = x,$$

ce qui amène à l'identité $x^4 = x$, ou encore $x(x^3 - 1) = 0$. Si x est non nul, on en déduit alors la relation $x^3 = 1$.

Exercice 2 – La relation étant clairement vérifiée pour $x = 0$, supposons que x non nul, ce qui revient à affirmer qu'il appartient au groupe K^\times , qui est d'ordre $q - 1$. Le théorème de Lagrange affirme alors que $x^{q-1} = 1$ et, en multipliant les deux termes de cette égalité par x , on obtient l'identité $x^q = x$.

Exercice 3 –

1. Un élément $x \in K^\times$ appartient au noyau de f si et seulement si $x^2 = 1$, ou encore $x^2 - 1 = (x - 1)(x + 1) = 0$, ce qui amène à $x = \pm 1$. L'image de f étant le sous-groupe $(K^\times)^2$ de K^\times formé par les éléments x tels qu'il existe $y \in K^\times$ avec $x = f(y) = y^2$, il coïncide avec l'ensemble des carrés de K^\times .
2. D'après le théorème de factorisation des homomorphismes de groupes, l'image de f est isomorphe au quotient $K^\times / \ker(f)$, qui est d'ordre $\frac{q-1}{2}$.
3. D'après le théorème de Lagrange, pour tout $a \in K^\times$, on a la relation $a^{q-1} = 1$. Si a est un carré, soit $a = b^2$, on obtient alors les identités

$$a^{\frac{q-1}{2}} = (b^2)^{\frac{q-1}{2}} = b^{q-1} = 1.$$

4. Le polynôme $X^{\frac{q-1}{2}} - 1 \in K[X]$ possède au plus $\frac{q-1}{2}$ racines et les points précédents affirment que ces racines sont précisément les carrés de K^\times , d'où le résultat.
5. Pour tout $a \in K^\times$, on a les relations $a^{q-1} - 1 = (a^{\frac{q-1}{2}} - 1)(a^{\frac{q-1}{2}} + 1) = 0$. Si a n'est pas un carré, nous venons de montrer que $a^{\frac{q-1}{2}} \neq 1$, d'où l'identité $a^{\frac{q-1}{2}} = -1$.

Exercice 4 – Le polynôme $X^2 + 1$ est irréductible si et seulement s'il ne possède pas de racine dans \mathbb{F}_p , ce qui revient à affirmer que -1 n'est pas un carré dans \mathbb{F}_p . Pour $p = 2$, on a les identités $-1 = 1 = 1^2$ et le polynôme n'est pas irréductible. Supposons

donc p impair. D'après le critère d'Euler (cf. l'exercice précédent), -1 est un carré si et seulement si $(-1)^{\frac{p-1}{2}} = 1$, ce qui revient à affirmer que $\frac{p-1}{2}$ est pair, ou encore que p est congru à 1 modulo 4, ce qui permet de conclure.

Exercice 5 –

1. On a les identités $2 = 1^2 + 1^2$, $5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$ et $17 = 1^2 + 4^2$.
2. La première assertion obtenue par une simple vérification directe. Supposons donc que p est somme de deux carrés, soit $p = a^2 + b^2$. Les entiers a^2 et b^2 étant congrus à 0 ou 1 modulo 4, on en déduit que p est congru à 0, 1 ou 2 modulo 4 (on remarquera que p étant premier, la première possibilité est exclue).
3. Si l'application f était injective, le cardinal de l'ensemble $S \times S$, qui est égal à $(n+1)^2 > p$, serait inférieur ou égal au cardinal de \mathbb{F}_p , qui est égal à p .
4. L'identité $f(x, y) = f(u, v)$ se traduit par les congruences $x + wy \equiv u + wv \pmod{p}$, ou encore $x - u \equiv (v - y)w \pmod{p}$, d'où la première assertion. On obtient alors les relations

$$a^2 \equiv (bw)^2 \equiv b^2 w^2 \equiv -b^2 \pmod{p},$$

ce qui implique que p divise $a^2 + b^2$.

5. Remarquons que les couples (x, y) et (u, v) étant distincts, les entiers a et b ne peuvent pas être tous les deux nuls, ce qui amène à l'inégalité $a^2 + b^2 > 0$. D'autre part, on a les relations

$$|a| = \max\{x, u\} - \min\{x, u\} \leq n - 0 < \sqrt{p}$$

et, de même, on obtient l'inégalité $|b| < \sqrt{p}$. On en déduit donc les relations $0 < a^2 + b^2 < 2p$. L'entier $a^2 + b^2$ étant un multiple de p , on a alors l'identité $p = a^2 + b^2$.

Exercice 6 –

1. Une vérification directe montre que le polynôme $X^2 - X - 1$ ne possède pas de racine dans \mathbb{F}_7 et est donc irréductible. L'anneau K est alors un corps de cardinal $7^2 = 49$.
2. Le groupe K^\times étant d'ordre 48, le théorème de Lagrange amène à l'identité $\alpha^{48} = 1$, ce qui entraîne les relations

$$\alpha^{483} = \alpha^3 \cdot \alpha^{480} = \alpha^3 \cdot (\alpha^{48})^{10} = \alpha^3 \cdot 1^{10} = \alpha^3.$$

Finalement, l'identité $\alpha^2 = \alpha + 1$ amène aux égalités

$$\alpha^3 = \alpha(\alpha + 1) = \alpha^2 + \alpha = 2\alpha + 1.$$

Exercice 7 – On utilise le résultat du cours (Théorème 6.6., page 107) appliqué au polynôme $X^8 - X = X^{2^3} - X$. L'ensemble des diviseurs irréductibles du polynôme $X^{2^3} - X$ est formé des polynômes irréductibles de $\mathbb{F}_2[X]$ de degré divisant 3.

Les polynômes unitaires irréductibles de $\mathbb{F}_2[X]$ de degrés 1 et 3 sont X , $X + 1$, $X^3 + X + 1$ et $X^3 + X^2 + 1$. On a donc la factorisation

$$X^8 - X = X(X^7 - 1) = X(X + 1)(X^3 + X + 1)(X^3 + X^2 + 1).$$

Donc $X^7 - 1 = (X + 1)(X^3 + X + 1)(X^3 + X^2 + 1)$.

Exercice 8 –

1. Le polynôme f étant de degré 2, il est irréductible si et seulement s'il ne possède pas de racine dans \mathbb{F}_p . La relation $(X - 1)f = X^3 - 1$ et le fait que $f(1) = 3 \neq 0$ impliquent que f possède une racine dans \mathbb{F}_p si et seulement si le groupe \mathbb{F}_p^\times , qui est d'ordre $p - 1$, possède un élément d'ordre 3. Les théorèmes de Cauchy et Lagrange affirment que cette dernière condition est remplie si et seulement si $p - 1$ est divisible par 3.
2. Pour $p = 2$, l'élément 3 étant clairement un carré, on suppose p impair. Le critère d'Euler (cf. l'exercice 3) affirme alors que 3 est un carré dans \mathbb{F}_p si et seulement si on a l'identité $3^{\frac{p-1}{2}} = 1$ dans \mathbb{F}_p . Le nombre premier p étant différent de 3, il est congru à ± 1 modulo 3. Traitons ces deux cas séparément :
— D'après le point précédent, pour $p \equiv 1 \pmod{3}$, le polynôme

$$4f = 4X^2 + 4X + 4 = (2X + 1)^2 + 3$$

possède une racine dans \mathbb{F}_p , ce qui implique que -3 est un carré dans \mathbb{F}_p , d'où l'identité $(-3)^{\frac{p-1}{2}} = 1$. On obtient alors les relations

$$3^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} (-3)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}}.$$

Il s'en suit que 3 est un carré si et seulement si $\frac{p-1}{2}$ est pair, ce qui revient à affirmer que p est congru à 1 modulo 4. Le théorème des restes chinois affirme alors que les congruences $p \equiv 1 \pmod{3}$ et $p \equiv 1 \pmod{4}$ sont équivalentes à $p \equiv 1 \pmod{12}$.

- Pour $p \equiv -1 \pmod{3}$, en procédant comme ci-dessus, on montre que -3 n'est pas un carré dans \mathbb{F}_p et le dernier point de l'exercice 3 amène à l'identité $(-3)^{\frac{p-1}{2}} = -1$, ce qui entraîne les relations

$$3^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} (-3)^{\frac{p-1}{2}} = (-1)^{\frac{p+1}{2}}.$$

On en conclut que 3 est un carré dans \mathbb{F}_p si et seulement si p est congru à -1 modulo 4 et, en appliquant une fois de plus le théorème des restes chinois, cette dernière condition est équivalente à $p \equiv -1 \pmod{12}$.

Exercice 9 –

1. Pour tout $x \in \mathbb{F}_9$, on a l'identité $x^9 = x$, d'où la relation $f(x) = 1$.
2. Pour tout $x \in \mathbb{F}_3$, on a $g(x) = -1$. Le polynôme g étant de degré 3 et ne possédant pas de racine sur \mathbb{F}_3 , il est irréductible.
3. On vérifie facilement les identités $f = g^3 + g = g(g^2 + 1)$.
4. Le polynôme g étant irréductible sur \mathbb{F}_3 , on a l'identité $\mathbb{F}_{27} = \mathbb{F}_3[X]/(g)$. On remarquera que pour tout $x \in \mathbb{F}_{27}$ et tout $y \in \mathbb{F}_3$, on a l'identité $g(x + y) = g(x)$. Il s'en suit que si $\alpha \in \mathbb{F}_{27}$ indique la classe de X , les racines de g dans \mathbb{F}_{27} sont $\alpha, \alpha + 1$ et $\alpha - 1$. De plus le critère d'Euler (cf. l'exercice 3) affirme que -1 n'est pas un carré dans \mathbb{F}_{27} et le polynôme $g^2 + 1$ n'admet donc pas de racine dans \mathbb{F}_{27} . On en déduit que les racines de f dans \mathbb{F}_{27} coïncident avec celles de g . Cette dernière affirmation aurait également pu être obtenue de manière directe en remarquant que si $x \in \mathbb{F}_{27}$ est une racine de f , on obtient les identités

$$0 = f(x)^3 = x^{27} - x^3 + 1 = x - x^3 + 1 = -g(x).$$

5. Montrons que le polynôme $h = g^2 + 1 = X^6 + X^4 + X^3 + X^2 - X + 1$ est irréductible sur \mathbb{F}_3 : si l'on avait $h = uv$, avec $0 < \deg(u) \leq \deg(v)$ et u irréductible, on en déduirait la relation $\deg(u) \in \{1, 2, 3\}$. Pour $\deg(u) \in \{1, 2\}$, le polynôme $f = gh$ posséderait une racine dans \mathbb{F}_9 , ce qui contredit le point 1. Pour $\deg(u) = 3$, le polynôme u étant irréductible, il posséderait une racine dans \mathbb{F}_{27} , et il en serait alors de même pour h , contredisant le point précédent. On en déduit donc la factorisation

$$f = (X^3 - X - 1)(X^6 + X^4 + X^3 + X^2 - X + 1).$$

Exercice 10 – On vérifie facilement que le polynôme f n'a pas de racine dans \mathbb{F}_3 et est donc irréductible, ce qui implique que K est un corps à 27 éléments. Le groupe K^\times étant d'ordre 26, le théorème de Lagrange affirme que les valeurs possibles pour l'ordre de x sont 1, 2, 13 ou 26. Les relations $x = 1$ et $x^2 = 1$ sont impossibles (car le polynôme $X^3 + 2X + 1$ ne divise pas $X^2 - 1$). Remarquons maintenant que x, x^3 et x^9 sont les trois racines de $X^3 + 2X + 1$ et leur produit, qui n'est autre que x^{13} , est égal à -1 (l'opposé du terme constant de $X^3 + 2X + 1$). On aurait également pu effectuer la division euclidienne de X^{13} par $X^3 + 2X + 1$, dont le reste est -1 . On en déduit que x est d'ordre 26 et engendre donc K^\times . Finalement, la relation $x^3 = x - 1$ amène aux identités $x^9 = (x - 1)^3 = x^3 - 1 = x + 1$, d'où l'égalité $x(x + 1) = x^{10}$.

Exercice 11 –

1. Soit $g \in \mathbb{F}_p[X]$ un facteur irréductible de $f = X^p - X - 1$ et notons K le corps $\mathbb{F}_p[X]/(g)$. Si $\alpha \in K$ désigne la classe de X , on a la relation $g(\alpha) = 0$, d'où $f(\alpha) = 0$. Pour tout entier $n \in \{0, 1, \dots, p-1\}$, l'élément $\alpha_n = \alpha^{p^n} \in K$ est également une racine de g et la relation $\alpha^p = \alpha + 1$ amène à l'identité $\alpha_n = \alpha + n$. Il s'en suit que g possède au moins p racines dans K , d'où les relations $p \leq \deg(g) \leq \deg(f) = p$. On a donc $\deg(f) = \deg(g)$, ce qui donne finalement $f = g$.
2. En suivant les notations du point précédent, dans le corps K , on a l'identité

$$X^p - X - 1 = \prod_{n=0}^{p-1} (X - \alpha_n).$$

En évaluant en 0, on en tire la relation $\alpha_0 \cdots \alpha_{p-1} = 1$, ce qui amène aux identités

$$\alpha^{\frac{p^p-1}{p-1}} = \alpha^{1+p+\dots+p^{p-1}} = \alpha_0 \cdots \alpha_{p-1} = 1.$$

L'élément α étant d'ordre divisant $\frac{p^p-1}{p-1} < p^p - 1$, il ne peut pas être un générateur de K^\times .

Exercice 12 –

1. On remarquera que f divise le polynôme $X^5 - 1$ et que $f(1) \neq 0$. Il s'en suit que si x est une racine de f dans une extension k de \mathbb{F}_3 , elle est d'ordre 5 (en tant qu'élément de k^\times) et le théorème de Lagrange affirme alors que 5 divise l'ordre de k^\times . Le groupe \mathbb{F}_9^\times étant d'ordre 8, le polynôme f n'admet pas de racine dans \mathbb{F}_9 .

2. Supposons d'avoir une factorisation $f = gh$ avec $g, h \in \mathbb{F}_3[X]$ et $\deg(g) \leq \deg(h)$. On a alors l'inégalité $\deg(g) \leq 2$. Si l'on avait $\deg(g) = 1$ ou $\deg(g) = 2$, le polynôme f posséderait une racine dans \mathbb{F}_9 , ce qui est exclu. On a donc $\deg(g) = 0$ et f est donc irréductible. Le quotient K est alors un corps de cardinal 81.
3. Pour tout $x \in K$, on a l'identité $x^{81} = x$, d'où les relations

$$y^9 = (x^9 - x)^9 = x^{81} - x^9 = x - x^9 = -y.$$

Si x n'appartient pas à \mathbb{F}_9 alors $x^9 \neq x$, ce qui donne $y \neq 0$. Si cette dernière condition est remplie, alors l'identité $y^9 = -y$ se traduit par la relation $x^8 = -1$. Il s'en suit que y est d'ordre d divisant 16. Si d divisait 8, on obtiendrait les égalités $1 = x^8 = -1$, ce qui est absurde. On a donc $d = 16$. Finalement, si y est d'ordre 16, il est non nul et donc $x^9 \neq x$, ou encore $x \notin \mathbb{F}_9$.

4. L'élément α étant d'ordre 5, on a les identités

$$\beta = \alpha(\alpha^{-1} - \alpha) = \alpha(\alpha^9 - \alpha).$$

D'après le premier point, on a $\alpha \notin \mathbb{F}_9$ et le point 3 affirme alors que $\alpha^9 - \alpha$ est d'ordre 16. Les éléments α et $\alpha^9 - \alpha$ étant d'ordres premiers entre eux, leur produit β est d'ordre $5 \cdot 16 = 80$ et engendre donc K^\times .

5. Les identités

$$\beta^3 = (1 - \alpha^2)^3 = 1 - \alpha^6 = 1 - \alpha \quad \text{et} \quad \beta^{40} = -1$$

amènent à la relation $\beta^{43} = \alpha - 1$ et la clé privée d'Alice est donc égale à 43. Notons $m \in K$ le message envoyé par Bob. En remarquant que $(1 + \alpha)^{37}$ est l'inverse de $(1 + \alpha)^{43}$, on obtient les identités

$$m = (1 + \alpha)^{-43}(1 + \alpha^3) = (1 + \alpha)^{37}(1 + \alpha)^3 = (1 + \alpha)^{40}.$$

L'élément $1 - \alpha = \beta^3$ étant un générateur de K^\times (car 3 est premier avec 80) on a les relations $\beta^{40} = (1 - \alpha)^{40} = -1$. L'identité $\beta = (1 - \alpha)(1 + \alpha)$ amène alors à la relation $m = 1$.

Exercice 13 – L'entier $p^2 - 1$ étant un multiple de $p + 1$, le polynôme $f = X^{p^2-1} - 1$ divise $g = X^{p^2} - X = X(X^{p^2-1} - 1)$. Ce dernier étant scindé sur \mathbb{F}_p^2 , il en est de même pour f . De plus, le polynôme g étant le produit des polynômes irréductibles, unitaires sur \mathbb{F}_p de degré divisant 2, tout facteur irréductible de f est de degré inférieur ou égal à 2. On remarquera que les facteurs irréductibles (unitaires) de f de degré 1 s'écrivent comme $X - x$, où $x \in \mathbb{F}_p$ est une racine de f et vérifie donc l'identité $x^p = x$. Dans ce cas, la relation $f(x) = 0$ se traduit par $x^2 = 1$, d'où $x = \pm 1$. On en déduit que pour $p > 2$, les polynômes $X - 1$ et $X + 1$ sont les deux seuls facteurs irréductibles de degré 1 de f et pour $p = 2$ on ne retrouve que le facteur $X - 1$. Pour $p = 5$, on a les identités

$$X^6 - 1 = (X^3 - 1)(X^3 + 1) = (X - 1)(X + 1)(X^2 + X + 1)(X^2 - X + 1)$$

et, d'après ce qui précède, les polynômes $X^2 + X + 1$ et $X^2 - X + 1$ sont irréductibles sur \mathbb{F}_5 (on aurait également pu le vérifier en montrant qu'ils n'ont pas de racine dans \mathbb{F}_5).