Sorbonne Université, Algèbre 2, année 2025-2026

Corrigé de la feuille de TD numéro 3

1 Arithmétique dans $\mathbb{Z}$

Exercice 1. On écrit $84 = 1 \times 52 + 32$ puis $52 = 1 \times 32 + 20$ puis $32 = 1 \times 20 + 12$ puis $20 = 1 \times 12 + 8$ puis $12 = 1 \times 8 + 4$ puis $8 = 2 \times 4 + 0$. Le PGCD de 84 et 52 est le dernier reste non nul de l'algotithme, c'est-à-dire 4. On exhibe ensuite une relation de Bezout : $4 = 12 - 8 = 12 - (20 - 12) = 2 \times 12 - 20 = 2 \times (32 - 20) - 20 = 2 \times 32 - 3 \times 20 = 2 \times 32 - 3 \times (52 - 32) = 5 \times 32 - 3 \times 52 = 5 \times (84 - 52) - 3 \times 52 = 5 \times 84 - 8 \times 52$.

Exercice 2. On note $d = \mathrm{PGCD}(a, b)$ et $a = da'$, $b = db'$. On veut démontrer que ab/d est égal à $\mathrm{PPCM}(a, b)$. On a $ab/d = da'b = dab'$, donc ab/d est un multiple commun à a et b. Soit maintenant un multiple commun à a et b, noté m. On peut écrire $m = ka = \ell b$ avec $k, \ell \geq 1$, donc $ka' = \ell b'$. Comme a' divise $\ell b'$ et $\mathrm{PGCD}(a', b') = 1$, il découle du lemme de Gauss que a' divise ℓ. On peut donc écrire $m = \ell' a' b = \ell'(ab/d)$ avec $\ell' \geq 1$. Ainsi, m est un multiple de ab/d, qui est donc bien égal à $\mathrm{PPCM}(a, b)$.

Exercice 3.

(1) D'après le cours, les inversibles sont les classes $\overline{k}$ telles que $k \wedge n = 1$.

(2) Les diviseurs de zéro sont les classes non nulles et non inversibles : soit $1 \leq k < n$ non inversible, on peut écrire $d = \gcd(k, n) \geq 2$ et $k = k'd$, $n = n'd$. On obtient $n'k = k'n = 0$ $[n]$, donc k est un diviseur de 0.

Exercice 4. Les ordres des éléments du groupe des inversibles de $\mathbb{Z}/7\mathbb{Z}$ sont des diviseurs de 6, donc appartiennent à $\{1, 2, 3, 6\}$. Il est clair que $\bar{1}$ est d'ordre 1 et que $-\bar{1} = \bar{6}$ est d'ordre 2. On a $\bar{2}^3 = \bar{1}$, donc $\bar{2}$ est d'ordre 3. De même, $\bar{3}^3 = \overline{27} = -\bar{1}$, donc $\bar{3}$ est d'ordre 6, et $\bar{4}^3 = \overline{64} = \bar{1}$, donc $\bar{4}$ est d'ordre 3. Enfin, $\bar{5}^2 = -\bar{3}$ et $\bar{5}^3 = -\overline{15} = -\bar{1}$, donc $\bar{5}$ est d'ordre 6.

Exercice 5.

(1) 561=31.

(2) D'après le petit théorème de Fermat, on a $a^2 = 1$ [3], d'où $(a^2)^{280} = 1^{280}$ [3], donc $a^{560} = 1$ [3]. On démontre de même que $a^{560} = 1$ [11] et $a^{560} = 1$ [17].

(3) Les entiers 3, 7, 11 divisent $a^{560} - 1$ et sont premiers entre eux, donc leur produit 561 divise encore $a^{560} - 1$. Ainsi, il existe des nombres qui ne sont pas premiers mais qui satisfont la conclusion du petit théorème de Fermat (on les appelle les nombres de Carmichael).

Exercice 6.

(1) Les classes de 1 et -1.

(2) Pour tout x dans $\mathbb{Z}/p\mathbb{Z}$ différent de $\bar{1}$ et $-\bar{1}$, il existe y dans $\mathbb{Z}/p\mathbb{Z}$ tel que $xy = \bar{1}$ et $y \neq x$. En faisant le produit de tous les éléments de $\mathbb{Z}/p\mathbb{Z}$, on obtient donc $-\bar{1}$, d'où le résultat.

Exercice 7. En vertu du théorème des restes chinois, il existe une unique solution modulo 231. On peut écrire $x = 3k + 2 = 7\ell + 1$ avec $k, \ell \in \mathbb{Z}$. Une solution particulière est $k = 2$ et $\ell = 1$, et les couples de solutions sont de la forme $(k, \ell) = (7m + 2, 3m + 1)$ avec $m \in \mathbb{Z}$. On obtient donc $x = 21m + 8$. D'autre part, on peut écrire $x = 11n + 3$. Comme $2 \cdot 11 + (-1) \cdot 21 = 1$, on a $10 \cdot 11 + (-5) \cdot 21 = 5$, donc une solution particulière de l'équation $21m + 8 = 11n + 3$ est donnée par $m = 5$ et $n = 10$, et les couples de solutions sont de la forme $(m, n) = (11s + 5, 21s + 10)$ avec $s \in \mathbb{Z}$. On obtient ainsi $x = 113 + 231s$. Ainsi, l'unique solution modulo 231 est 113.

Exercice 8. Comme 137 est premier, 24 est inversible modulo 137. En notant a son inverse, on obtient $x = -5a$ [137]. Pour trouver a, on cherche une relation de Bezout entre 24 et 137 grâce à l'algorithme d'Euclide : $137 = 5 \cdot 24 + 17$, $24 = 17 + 7$, $17 = 2 \cdot 7 + 3$, $7 = 2 \cdot 3 + 1$. On écrit ensuite $1 = 7 - 2 \cdot 3 = 7 - 2 \cdot (17 - 2 \cdot 7) = 5 \cdot 7 - 2 \cdot 17 = \cdots = 40 \cdot 24 - 7 \cdot 137$. Ainsi, $a = 40$ et $x = -200 = 74$ [137].

Exercice 9. Pour la première équation, on écrit $x^2 - 9 = (x+3)(x-3) = 0$ [73]. Puisque 73 est un nombre premier, l'anneau $\mathbb{Z}/73\mathbb{Z}$ est intègre, donc $x = 3$ [73] ou $x = -3 = 70$ [73]. Pour la seconde équation, on écrit $x^4 - 81 = (x + 3)(x - 3)(x^2 + 9) = 0$ [73]. On remarque que $9 = -64$ [73], donc $x^2 + 9 = (x + 8)(x - 8)$ [73]. Les solutions modulo 73 sont donc ± 3 et ± 8.

Exercice 10.

(1) Si $a = e$ alors $b = b^2$, donc $b = e$. De même, si $b = e$ alors $a = e$.

On suppose dorénavant, en vue d'obtenir une contradiction, que $a \neq e$ et $b \neq e$. On note $m \geq 2$ l'ordre de a et $n \geq 2$ l'ordre de b.

(2) Par récurrence.

(3) En prenant $k = n$ dans l'équation obtenue à la question (2), on obtient $a = a^{2^n}$, donc $a^{2^n - 1} = e$, d'où l'ordre de a divise $2^n - 1$.

(4) L'entier $2^n - 1$ étant impair, p (qui le divise) est nécessairement impair. D'autre part, m divise $2^n - 1$ (question (3)), donc p divise $2^n - 1$, i.e., $2^n = 1[p]$.

(5) Comme p est impair, 2 est différent de p, donc 2 est inversible dans $\mathbb{F}_p$. Le petit théorème de Fermat donne $2^{p-1} = 1$ $[p]$. Ainsi, l'ordre (multiplicatif) de 2 dans $\mathbb{F}_p^*$, noté k, divise $p - 1$. D'après la question (3), k divise aussi n. Il existe donc un nombre premier $q \leq p - 1$ qui divise n.

(6) On a $q < p$. Comme a et b jouent des rôles symétriques, on a aussi $p < q$, contradiction.

2 Arithmétique dans $\mathbb{K}[X]$

Exercice 11.

(1) Si $\bar{Q}$ est un élément non trivial de $\mathbb{K}[X]/(P)$, alors Q n'est pas divisible par P. On en déduit que Q et P sont premiers entre eux (si D désigne le PGCD de P et Q, alors D divise P donc $D = 1$ ou $D = \lambda P$, et ce second cas est exclu), donc qu'il existe A, B tels que $AQ + BP = 1$.

(2) On commence par observer que $X^3 - 2$ n'a pas de racine rationnelle (sinon, en écrivant $r = p/q$ une racine avec p et q premiers entre eux, on obtient $p^3 = 2q^3$, donc 2 divise p, puis $p = 2p'$ donc $4p'^3 = q^3$ donc 2 divise q, contradiction). Comme ce polynôme est de

degré 3, il est irréductible dans $\mathbb{Q}[X]$, donc $\mathbb{Q}[X]/(X^3-2)$ est un corps en vertu de la question (1).

(3) En revanche, l'anneau $\mathbb{Q}[X]/(X^3-1)$ n'est pas un corps car on peut écrire $X^3-1=(X-1)(X^2+X+1)$, donc $\bar{X}-1$ est un diviseur de zéro dans $\mathbb{Q}[X]/(X^3-1)$.

Exercice 12. On cherche Q, R tels que $A = BQ + R$ avec $\deg R < 2$. On obtient :

$$Q(X) = X^2 - 2X + 1, \quad R(X) = X.$$

Ainsi

$$A(X) = B(X)(X^2 - 2X + 1) + X.$$

Exercice 13. Soit I un idéal non nul de $K[X]$. Soit P un polynôme de degré minimal dans I. Pour tout $Q \in I$, la division euclidienne de Q par P donne $Q = PU + R$ avec $\deg R < \deg P$. Comme R appartient à I, on obtient $R = 0$, donc $Q \in (P)$. Ainsi $I = (P)$.

Exercice 14. On effectue l'algorithme d'Euclide : $X^4 - 1 = X(X^3 - 1) + (X - 1)$ puis $X^3 - 1 = (X^2 + X + 1)(X - 1)$. Donc le PGCD de A et B est $P(X) = X - 1$. D'après l'exercice précédent ou le cours, il existe un polynôme Q tel que l'idéal engendré par A et B est égal à (Q). On peut écrire $Q = UA+VB$ pour des polynômes U, V. Comme P divise A et B, il divise aussi Q, donc $(Q) \subset (P)$. Par ailleurs, P appartient à l'idéal engendré par A et B (puisqu'il existe une relation de Bezout de la forme $P = CA + DB$), donc $(P) \subset (Q)$. Ainsi, $X - 1$ est un générateur de l'idéal de $\mathbb{R}[X]$ engendré par A et B.

Exercice 15. Soit $\alpha \in \mathbb{C}$ une racine de B. Alors $\alpha^2 - 2\alpha + 2 = 0$. On en déduit que $\alpha^3 - \alpha^2 + 1 = \alpha(2\alpha - 2) - (2\alpha - 2) + 1 = 2(\alpha^2 - 2\alpha) + 3 = -1 \neq 0$. Ainsi, A et B n'ont pas de racine commune, ils sont donc premiers entre eux (sinon ils auraient un diviseur commun de degré ≥ 1, donc une racine commune dans $\mathbb{C}$).

Exercice 16. On écrit $X^3 - 2 = (2X^2 - 3)(1/2)X + (3/2)X - 2$ puis $2X^2 - 3 = [(3/2)X - 2][(4/3)X + (16/9)] + 5/9$. Ainsi, $5/9$ est le dernier reste non nul de l'algorithme d'Euclide, donc le plus grand diviseur commun de A et B est 1 (car, par définition, le PGCD est unitaire).

Exercice 17.

(1) On remarque que $X^3 - 1 = (X - 1)(X^2 + X + 1)$. Ainsi, $X^3 = 1$ modulo $A(X)$, donc $X^{10} = X$ modulo $A(X)$ et $X^5 = X^2$ modulo $A(X)$, donc $B(X) = A(X) = 0$ modulo $A(X)$.

(2) Si $n = 3k + 1$ alors $X^n = X$ modulo $A(X)$ et la preuve précédente fonctionne encore. Si $n = 3k + 2$ alors $X^{2n} = X^2$ modulo $A(X)$ et $X^n = X$ modulo $A(X)$, donc la preuve marche encore. Si $n = 3k$ alors $X^n = 0$ modulo $A(X)$, donc ça ne marche pas. Ainsi, A divise C si et seulement si n n'est pas un multiple de 3.

Exercice 18. On remarque que $P(0) = 0$ et que $P'(0) = 0$, donc 0 est une racine double de P.

Exercice 19. Dans $\mathbb{C}[X]$, $X^4-1 = \prod_{k=1}^{4}(X-e^{2ik\pi/4})$ et $X^5-1 = \prod_{k=1}^{5}(X-e^{2ik\pi/5})$. Dans $\mathbb{R}[X]$, $X^4 - 1 = (X^2 - 1)(X^2 + 1) = (X - 1)(X + 1)(X^2 + 1)$ et (en groupant par deux les racines complexes conjuguées) $X^5-1 = (X-1)(X^2-\cos(2\pi/5)X+1)(X^2-\cos(4\pi/5)X+1)$.

Exercice 20. On a $A(X) = B(X)(X+1) + X^2 - X$ puis $B(X) = (X^2 - X)X + 1$, donc le PGCD vaut 1. On fait ensuite les opérations en sens inverse : $1 = B(X) - (X^2 - X)X = B(X) - X(A(X) - B(X)(X+1)) = -XA(X) + (1 + X(X+1))B(X) = -XA(X) + (X^2 + X + 1)B(X)$.

Exercice 21.

(1) On écrit $n = k\ell$ avec $\ell \geq 1$. En divisant $Y^\ell - 1$ par $Y - 1$, on obtient $Y^\ell - 1 = (Y-1)P(Y)$ où $P(Y) = \sum_{i=0}^{\ell-1} Y^i$. En posant $Y = X^k$, on obtient $X^n - 1 = (X^k - 1)P(X^k)$.

(2) On peut écrire $(X^n - 1) - (X^r - 1) = X^n - X^r = X^r(X^{n-r} - 1)$. Comme k divise $n - r$, $X^k - 1$ divise $(X^n - 1) - (X^r - 1)$ (d'après la première question). Par ailleurs, le degré de $X^r - 1$ est strictement inférieur à celui de $X^k - 1$, d'où le résultat.

(3) On utilise l'algorithme d'Euclide. Grâce à la question (2), on constate que $X^d - 1$ est le dernier reste non nul, donc le pgcd.