Sorbonne Université, Algèbre 2, année 2025-2026

Feuille de TD numéro 3 : arithmétique de $\mathbb{Z}$ et $\mathbb{K}[X]$

1 Arithmétique dans $\mathbb{Z}$

Exercice 1. Calculer le PGCD de 84 et 52 au moyen de l'algorithme d'Euclide, puis exhiber une relation de Bezout entre eux.

Exercice 2. Démontrer à l'aide du lemme de Gauss que si a et b sont deux entiers naturels, le produit ab est égal au produit de $\mathrm{PGCD}(a,b)$ par $\mathrm{PPCM}(a,b)$.

Exercice 3.

(1) Soit $n \geq 1$ un entier. Quels sont les éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$?

(2) Quels sont ses diviseurs de zéro ?

Exercice 4. Donner les ordres des éléments du groupe des inversibles de $\mathbb{Z}/7\mathbb{Z}$.

Exercice 5.

(1) Décomposer 561 en facteurs premiers.

(2) Montrer que si a est premier avec 561, alors $a^{560} = 1$ [3] et $a^{560} = 1$ [11] et $a^{560} = 1$ [17].

(3) En déduire que $a^{560} = 1$ [561]. Qu'en concluez-vous ?

Exercice 6. Soit p un nombre premier.

(1) Quelles sont les solutions de l'équation $x^2 = \bar{1}$ dans $\mathbb{Z}/p\mathbb{Z}$?

(2) En déduire le théorème de Wilson : $(p-1)! = -1$ [p].

Exercice 7. Déterminer les solutions modulo 231 du système suivant, d'inconnue x :

$$\begin{cases} x = 2 \ [3] \\ x = 1 \ [7] \\ x = 3 \ [11] \end{cases}$$

Exercice 8. Résoudre l'équation suivante, d'inconnue x :

$$24x + 5 = 0 \ [137].$$

Exercice 9. Résoudre les équations suivantes, d'inconnue x :

$$x^2 = 9 \ [73] \quad \text{et} \quad x^4 = 81 \ [73].$$

Exercice 10. Soit G un groupe fini dont on note e l'élément neutre. Soient $a, b \in G$ tels que $aba^{-1} = b^2$ et $bab^{-1} = a^2$. Le but de cet exercice est de démontrer que $a = e$ et $b = e$.

(1) Montrer que a et b sont simultanément triviaux ou simultanément non triviaux.

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) Montrer que $b^k a b^{-k} = a^{2^k}$ pour tout entier k.

(3) Montrer que m divise $2^n - 1$.

(4) On note p le plus petit diviseur premier de m. Montrer que p est impair et que $2^n = 1\ [p]$.

(5) En utilisant le petit théorème de Fermat, montrer qu'il existe un nombre premier $q < p$ qui divise n.

(6) Conclure.

2 Arithmétique dans $\mathbb{K}[X]$

Exercice 11.

(1) Soient $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$ un polynôme irréductible. Montrer que $\mathbb{K}[X]/(P)$ est un corps.

(2) Application : montrer que $\mathbb{Q}[X]/(X^3 - 2)$ est un corps.

(3) L'anneau $\mathbb{Q}[X]/(X^3 - 1)$ est-il un corps ?

Exercice 12. Effectuer la division euclidienne de $A(X) = X^4 - 2X^3 + 3X - 1$ par $B(X) = X^2 - 1$ dans $\mathbb{R}[X]$.

Exercice 13. Soit $\mathbb{K}$ un corps. Montrer que tout idéal de $\mathbb{K}[X]$ est principal.

Exercice 14. Calculer le PGCD de $A(X) = X^4 - 1$ et $B(X) = X^3 - 1$ dans $\mathbb{R}[X]$. En déduire un générateur de l'idéal de $\mathbb{R}[X]$ engendré par A et B (on renvoie à la définition de l'idéal engendré par une partie donnée dans l'exercice 16 de la feuille de TD numéro 2).

Exercice 15. Montrer que $A(X) = X^3 - X^2 + 1$ et $B(X) = X^2 - 2X + 2$ n'ont pas de racine commune dans $\mathbb{C}$. En déduire qu'ils sont premiers entre eux.

Exercice 16. Montrer, en utilisant l'algorithme d'Euclide, que $A(X) = X^3 - 2$ et $B(X) = 2X^2 - 3$ sont premiers entre eux.

Exercice 17.

(1) Montrer que $A(X) = X^2 + X + 1$ divise $B(X) = X^{10} + X^5 + 1$ (on pourra remarquer que $X^3 = 1$ modulo $A(X)$).

(2) A quelle condition sur l'entier $n \geq 1$ le polynôme $A(X)$ divise-t-il $C(X) = X^{2n} + X^n + 1$?

Exercice 18. Montrer que X^2 divise $P(X) = (X + 1)^n - nX - 1$ pour tout entier $n \in \mathbb{N}$.

Exercice 19. Factoriser $X^4 - 1$ et $X^5 - 1$ dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$.

Exercice 20. Déterminer le PGCD de $A(X) = X^4 + 1$ et $B(X) = X^3 - X^2 + 1$ puis exhiber une relation de Bezout.

Exercice 21. Soient $n \geq 1$ et $k \geq 1$ deux entiers.

(1) Montrer que si k divise n, alors $X^k - 1$ divise $X^n - 1$.

(2) On note r le reste de la division euclidienne de n par k. Montrer que $X^r - 1$ est le reste de la division euclidienne de $X^n - 1$ par $X^k - 1$.

(3) On note d le pgcd de n et k. Montrer que $X^d - 1$ est le pgcd de $X^n - 1$ et $X^k - 1$.