Présentation des chapitres de mathématiques de MP

Arithmétique des entiers et des polynômes

Lorsque l'énoncé d'un exercice est accompagné du symbole « ✯ » dans la marge, cela signifie qu'il ne peut pas être traité avec toute la rigueur mathématique attendue tant qu'on est cantonné aux outils de MPSI (j'indique alors clairement ce qu'il est nécessaire d'admettre). Vous pourrez essayer de les traiter à nouveau, rigoureusement, au moment adéquat l'année prochaine.

1 Généraliser le vocabulaire arithmétique : motivation

Ce chapitre sur la reine des mathématiques commence à reformuler les principales notions de l'arithmétique (divisibilité, irréductibilité ou primalité) en des termes plus généraux. L'intérêt ? Pouvoir imiter les raisonnements d'arithmétique sur les entiers dans d'autres circonstances. Cette idée vient après un grand succès qu'eurent Euler puis Kummer dans l'étude d'équations diophantiennes. Leur idée est qu'en faisant de l'arithmétique contenant davantage de nombres que $\mathbb{Z}$, on obtient davantage de factorisations et donc de relations de divisibilité possibles ; ayant plus d'informations, cela permet de résoudre des équations diophantiennes plus facilement.

Un exemple pour illustrer cette idée, où l'on admettra que « tout se passe comme dans $\mathbb{Z}$ » : si l'on cherche à résoudre l'équation : $y^2+2=x^3$, d'inconnue $(x,y)\in\mathbb{Z}^2$, de l'arithmétique élémentaire permet dans un premier temps de montrer que x et y doivent tous les deux être impairs. De plus, dans l'anneau $\mathbb{Z}[i\sqrt{2}]=\left\{z\in\mathbb{C}\mid \exists(a,b)\in\mathbb{Z}^2,\ z=a+i\sqrt{2}b\right\}$ (qui contient $\mathbb{Z}$), on a la relation :

$$(y+i\sqrt{2})(y-i\sqrt{2})=x^3$$

et, si on s'autorise à faire de l'arithmétique dans $\mathbb{Z}[i\sqrt{2}]$ comme dans $\mathbb{Z}$: à ce stade, on démontre que les deux facteurs du membre de gauche sont premiers entre eux, c'est-à-dire que tout diviseur commun est inversible. En effet, si $d\in\mathbb{Z}[i\sqrt{2}]$ divise $y+i\sqrt{2}$ et $y-i\sqrt{2}$, alors il divise la différence $-2i\sqrt{2}=(i\sqrt{2})^3$. Or $i\sqrt{2}$ est un nombre premier dans $\mathbb{Z}[i\sqrt{2}]$ (voir l'exercice 2 pour comprendre ce qu'on entend par là), donc l'unicité de la décomposition en facteurs premiers dans $\mathbb{Z}[i\sqrt{2}]$ implique qu'il existe $u\in\mathbb{Z}[i\sqrt{2}]^\times$ et $k\in[\![0,3]\!]$ tels que : $d=u(i\sqrt{2})^k$. Justifions que $k=0$: si $k\geqslant 1$ alors, du fait que d divise $y+i\sqrt{2}$ et $y-i\sqrt{2}$, son carré d^2 divise leur produit, c'est-à-dire x^3 ; or : $d^2=u^2(i\sqrt{2})^{2k}=(-1)^k u^2 2^k$: par conséquent, si $k\geqslant 1$, alors 2 divise x^3, et donc x est pair. C'est impossible, on a affirmé tantôt que x est impair ! Par l'absurde : $k=0$, donc $d=u$ est inversible.

Ainsi $y+i\sqrt{2}$ et $y-i\sqrt{2}$ sont premiers entre eux, et leur produit est un cube, donc ils sont eux-mêmes des cubes. Soit $(a,b)\in\mathbb{Z}^2$ tel que : $y+i\sqrt{2}=(a+i\sqrt{2}b)^3$. En développant cette puissance et en identifiant parties réelles et imaginaires, on obtient :

$$y=a^3-6ab^2=a(a^2-6b^2),\quad 1=3a^2b-2b^3=b(3a^2-2b^2).$$

Partant de là, on déduit : $b=1$, $a^2=\frac{1+2b^2}{3}=1$, et il n'est plus difficile d'en déduire que les solutions $(x,y)\in\mathbb{Z}^2$ de l'équation initiale sont $(3,5)$ et $(3,-5)$ (la réciproque étant triviale à vérifier).

Exercice 1. Compléter les éléments non détaillés suivants :

1. Vérifier que $\mathbb{Z}[i\sqrt{2}]$ est un anneau. Pourquoi veut-on un anneau, d'ailleurs ?
2. Soit $(x,y)\in\mathbb{Z}^2$. Vérifier effectivement que si : $y^2+2=x^3$, alors x et y sont impairs.
3. Vérifier que la propriété utilisée dans $\mathbb{Z}[i\sqrt{2}]$ est vraie au moins dans $\mathbb{Z}$: si a et b sont deux entiers relatifs non nuls et premiers entre eux, et si $c\in\mathbb{Z}$ vérifie : $c^3=ab$, alors il existe $(u,v)\in\mathbb{Z}^2$ tel que : $a=\pm u^3$, $b=\pm v^3$.
4. Soit $x\in\mathbb{Z}$. Montrer que si 2 divise x^3, alors 2 divise x.
5. *A priori*, d^2 divise x^3 dans $\mathbb{Z}[i\sqrt{2}]$, et après j'en déduis que 2 divise x^3 au sens classique, c'est-à-dire dans $\mathbb{Z}$ (puisque je raisonne sur la parité, qui a été définie et établie dans $\mathbb{Z}$). C'est trop rapide : comment suis-je passé de $\mathbb{Z}[i\sqrt{2}]$ à $\mathbb{Z}$? Détailler cette étape.

On dit que a divise b dans $\mathbb{Z}[i\sqrt{2}]$ s'il existe $c\in\mathbb{Z}[i\sqrt{2}]$ tel que : $b=ac$.

6. Justifier les expressions de a, b, puis de (x, y) proposées (pourquoi n'a-t-on pas $b = -1$?).

Exercice 2.

1. Montrer que s'il existe $(z, z') \in \mathbb{Z}[i\sqrt{2}]^2$ tel que : $i\sqrt{2} = zz'$, alors soit z, soit z' est égal à ± 1.
   Indication : prendre le module au carré pour se ramener à une relation dans $\mathbb{Z}$.
2. Montrer qu'il en est de même avec 2, 3, $1+i\sqrt{5}$ et $1-i\sqrt{5}$, mais en remplaçant $(z, z') \in \mathbb{Z}[i\sqrt{2}]^2$ par $(z, z') \in \mathbb{Z}[i\sqrt{5}]^2$.
   Par définition, on a : $\mathbb{Z}[i\sqrt{5}] = \left\{z \in \mathbb{C} \mid \exists (a,b) \in \mathbb{Z}^2,\ z = a + i\sqrt{5}b\right\}$.

Exercice 3.

1. S'inspirer de cette approche pour démontrer que les triplets pythagoriciens (c'est-à-dire : les triplets $(x, y, z) \in \mathbb{Z}^3$ tels que : $x^2 + y^2 = z^3$) sont tous de la forme :
   $$\left(d(u^2 - v^2), 2duv, d(u^2 + v^2)\right),$$
   avec $(d, u, v) \in \mathbb{Z}^3$. On commencera par se ramener, par de l'arithmétique classique dans $\mathbb{Z}$, au cas où x, y et z sont premiers entre eux dans leur ensemble, puis on justifiera que sous cette hypothèse, exactement un de ces trois entiers est pairs, et que ce ne peut pas être z.
   On admettra qu'on peut faire de l'arithmétique dans $\mathbb{Z}[i]$ comme dans $\mathbb{Z}$.
2. Redémontrer ce résultat par la géométrie en notant que cela revient à expliciter les points $(x, y) \in \mathbb{Q}^2$ tels que : $x^2 + y^2 = 1$.
   Indication : considérer les droites de pente rationnelle et passant par $(-1,0)$. Montrer que les points d'intersection de ces droites avec le cercle unité donnent tous les points que l'on cherche.
3. Redémontrer ce résultat uniquement en recourant à l'arithmétique traditionnelle (dans $\mathbb{Z}$).

Néanmoins attention car l'hypothèse qu'on peut faire de l'arithmétique dans $\mathbb{Z}[i\sqrt{2}]$ comme dans $\mathbb{Z}$ est une très, très grosse hypothèse, loin d'être évidente. Si l'on se plaçait dans $\mathbb{Z}[i\sqrt{5}] = \left\{z \in \mathbb{C} \mid \exists (a,b) \in \mathbb{Z}^2,\ z = a + i\sqrt{5}b\right\}$, les égalités $6 = 2 \times 3 = \left(1 + i\sqrt{5}\right)\left(1 - i\sqrt{5}\right)$ empêchent l'unicité de la décomposition en facteurs premiers, puisque tous ces facteurs sont premiers au sens donné dans l'exercice 2 (en vérité on parle plutôt d'élément *irréductible*, je parle de primalité seulement pour mieux faire le parallèle avec les nombres premiers de $\mathbb{Z}$). Sans cette unicité, on se convainc qu'il n'y a pas non plus de lemme d'Euclide, de théorème de Gauß, de notion claire de pgcd ou ppcm, etc.

L'exemple ci-dessus permet néanmoins de voir que l'arithmétique ne se borne pas à $\mathbb{Z}$. Il s'agit d'étendre les définitions de l'arithmétique à d'autres anneaux, et il s'avère que les idéaux d'un anneau (dont nous parlions déjà dans la section précédente) donnent le bon langage pour cela. Outre la traduction de la divisibilité en termes d'idéaux, c'est pour la définition du pgcd et du ppcm, ainsi que pour les relations de Bezout, que les idéaux apportent davantage de confort, à condition d'être dans un anneau dit « principal » (c'est-à-dire : tout idéal de l'anneau est de la forme $aA = \{ab \mid b \in A\}$ avec $a \in A$). Au-delà de cette définition savante, il faut retenir qu'un anneau principal est un anneau « où on peut faire de l'arithmétique comme dans $\mathbb{Z}$ », et un anneau où il existe un théorème de division euclidienne est toujours principal.

2 Arithmétique des polynômes

Or il s'avère que $K[X]$ possède une division euclidienne ! Ainsi, en raisonnant par analogie avec $\mathbb{Z}$, nous montrerons que tous les théorèmes connus de l'arithmétique dans $\mathbb{Z}$ sont valables avec les polynômes : les polynômes se décomposent de manière unique en produit d'irréductibles (qu'il est donc intéressant expliciter, au moins dans $\mathbb{R}[X]$ ou $\mathbb{C}[X]$), le théorème de Bezout reste valable, ainsi que le lemme d'Euclide, etc. Cela aura des conséquences dans plusieurs domaines, en particulier :

— l'algèbre linéaire, puisque nous nous en servirons pour définir et étudier le *polynôme minimal* d'un endomorphisme ou d'une matrice (outil essentiel pour étudier leur « réduction », chose qu'on va motiver dans la section suivante), et pour démontrer le lemme des noyaux (qui permet de décomposer des espaces vectoriels en somme de sous-espaces plus petits, toujours suivant la discussion de la section suivante) ;

— l'étude des nombres algébriques, c'est-à-dire des nombres complexes annulés par un polynôme non nul à coefficients rationnels.

Deux choses rendent l'arithmétique des polynômes parfois plus simple que celle des entiers : il y a deux autres moyens d'obtenir des relations de divisibilité entre polynômes :

— la dérivation ;

— la caractérisation des racines :

$$P(\alpha) = 0 \iff X - \alpha \mid P,$$

que l'on peut généraliser à l'aide de la notion de *polynôme minimal* (soit K un sous-corps de $\mathbb{C}$; pour tout $\alpha \in \mathbb{C}$, on peut définir son polynôme minimal sur K comme le plus petit polynôme unitaire de $K[X]$, au sens du degré, qui annule α, du moins s'il en existe ; mais la meilleure définition est avec en termes d'idéaux) : si $\alpha \in \mathbb{C}$ admet $\pi_\alpha \in K[X]$ pour polynôme minimal sur K, et si $P \in K[X]$, alors :

$$P(\alpha) = 0 \iff \pi_\alpha \mid P.$$

Cela donne en général un facteur de plus haut degré que $X - \alpha$. Ainsi on peut démontrer des relations de divisibilité par une banale évaluation d'un polynôme (pourvu qu'elle soit nulle).

Exercice 4. Soit $\alpha \in \mathbb{C}$. Soit K un sous-corps de $\mathbb{C}$. On suppose qu'il existe des polynômes non nuls de $K[X]$ qui s'annulent en α, de sorte que $\pi_\alpha \in K[X]$ existe.

1. Justifier que π_α est irréductible (*montrer que le cas contraire contredirait sa minimalité*).
2. Montrer l'équivalence ci-dessus avec un bon usage de la division euclidienne.
3. Montrer que si $P \in K[X]$ est irréductible, unitaire, et annule α, alors : $P = \pi_\alpha$. C'est un moyen pratique de déterminer le polynôme minimal.
4. Soit $\theta \in \mathbb{R} \setminus \pi\mathbb{Z}$. Montrer que $X^2 - 2\cos(\theta)X + 1$ est le polynôme minimal sur $\mathbb{R}$ de $e^{i\theta}$.
5. Soit $\theta \in \mathbb{R} \setminus \pi\mathbb{Z}$. Montrer que pour tout $n \in \mathbb{N} \setminus \{0,1\}$, le polynôme $X^2 - 2\cos(\theta)X + 1$ divise le polynôme $\sin(\theta)X^n - \sin(n\theta)X + \sin((n-1)\theta)$.

Cette dernière question montre l'apport de cette équivalence qui n'a aucun... équivalent, dans $\mathbb{Z}$: comment obtiendrait-on cette relation de divisibilité sans s'en servir ?

3 Arithmétique modulo n

Enfin, une composante essentielle de l'arithmétique est ce qu'on appelle l'arithmétique modulaire (c'est-à-dire modulo un entier). À cet effet, nous étudierons $\mathbb{Z}/n\mathbb{Z}$ plus longuement que dans le chapitre précédent (qui ne s'intéressait à cet ensemble qu'en tant que groupe cyclique et non pour des questions arithmétiques). Il est aussi muni d'une structure d'anneau provenant de la structure d'anneau de $\mathbb{Z}$ (où l'on « pose $n = 0$ »). Cela permet de montrer des relations de divisibilité du type : « n divise ★ », en montrant que ★ est nul dans $\mathbb{Z}/n\mathbb{Z}$. Passer par cet anneau a de nombreux avantages : d'abord c'est un ensemble fini, ce qui est plus agréable à manipuler que $\mathbb{Z}$ pour de bêtes raisons combinatoires (dites-vous qu'au moins *en principe*, dans un ensemble fini, on peut par exemple résoudre des équations par recensement exhaustif) ; ensuite, les relations sur les ordres dont nous parlions dans l'introduction du chapitre précédent permettent de calculer très facilement des puissances modulo n. On retrouvera notamment le petit théorème de Fermat (si p est un nombre premier, alors pour tout $a \in \mathbb{Z}$ on a : $a^p \equiv a \bmod p$) et on le généralisera au cas où p n'est pas premier.

Le cas où n est premier est remarquable à bien des égards : dans ce cas $\mathbb{Z}/n\mathbb{Z}$ est un corps. Le fait que tout élément non nul soit inversible rend l'arithmétique modulo un nombre premier très agréable. Pour le cas où n n'est pas premier, un important résultat, appelé le *lemme chinois*, permettra de diluer encore la difficulté des études dans $\mathbb{Z}/n\mathbb{Z}$ en regardant ce qu'il se passe modulo les diviseurs premiers de n : ainsi on pourra (partiellement) se ramener au cas précédent.

4 Résumé : objectif du chapitre

Après avoir réinterprété les notions de base de l'arithmétique en termes d'idéaux, nous définirons ce qu'est un anneau principal, et montrerons que dans un anneau principal on « peut faire de l'arithmétique comme dans $\mathbb{Z}$ ». Parmi les propriétés au programme, on insistera plus spécifiquement sur l'existence du ppcm, du pgcd, et le théorème de Bezout. Nous retrouverons les résultats connus dans $\mathbb{Z}$ et vérifierons que l'anneau $K[X]$ est aussi principal : on peut faire de l'arithmétique dans $K[X]$.

Puis nous consacrerons le reste du chapitre à l'arithmétique dans $\mathbb{Z}/n\mathbb{Z}$. Nous aurons besoin pour cela de clarifier sa structure d'anneau, et nous verrons que les diviseurs premiers de n jouent un rôle essentiel pour la comprendre : d'abord, $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier (ce qui simplifie les calculs dans $\mathbb{Z}/n\mathbb{Z}$, du fait que tout élément non nul soit inversible et que $\mathbb{Z}/n\mathbb{Z}\setminus\{0\}$ soit un groupe) et, même dans le cas où n n'est pas premier, le lemme chinois nous permettra de ramener l'étude de $\mathbb{Z}/n\mathbb{Z}$ à l'étude de $\mathbb{Z}/p^{v_p(n)}\mathbb{Z}$ où p divise n.

Ces résultats profonds de structure nous permettront de démontrer à peu de frais le petit théorème de Fermat et de le généraliser (son intérêt étant de simplifier l'étude des relations de divisibilité vérifiées par les puissances d'entiers relatifs), grâce à l'indicatrice d'Euler que nous avons brièvement mentionnée dans la section précédente. Cette fonction indicatrice éclaire à la fois la structure de groupe de $\mathbb{Z}/n\mathbb{Z}$ en comptant ses générateurs, mais aussi la structure d'anneau en comptant le nombre d'inversibles de $\mathbb{Z}/n\mathbb{Z}$ pour la multiplication, comme nous le verrons. Le lemme chinois nous donnera un moyen de la calculer autrement qu'en revenant à sa définition.