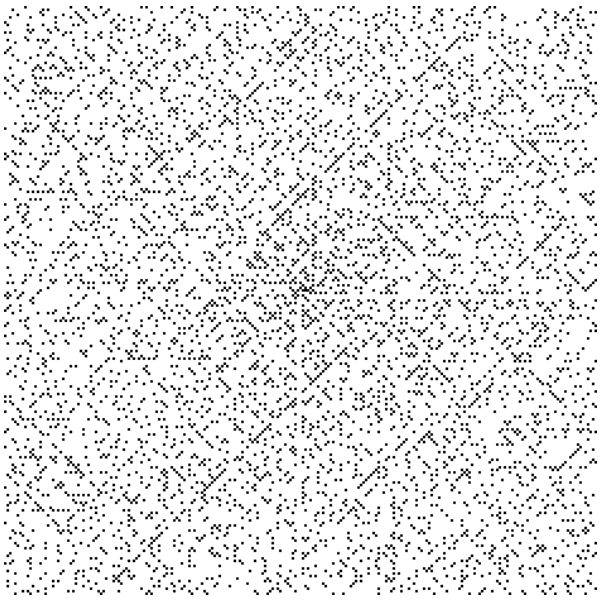
Ag5 : Arithmétique : rappels et compléments sur les anneaux et les idéaux



La spirale d'Ulam

L'arithmétique est une discipline fort ancienne. La démonstration donnée par Euclide (~ -300) de l'infinitude de l'ensemble des nombres premiers est célèbre, et a déjà été posée à l'écrit du concours des Mines, dans des exercices d'oral...Les congruences, introduites par Gauss (Disquisitiones Arithmeticae, 1801) sont un outil remarquablement efficace pour résoudre des problèmes arithmétiques. A partir des travaux de Riemann (milieu du XIXème siècle) les problèmes posés par la théorie des nombres sont abordés avec des outils plus élaborés. La très célèbre preuve (Wiles, 1995) du non moins célèbre théorème de Fermat (1641) n'est pas d'une grande simplicité. Néanmoins, avec l'arrivée de l'informatique, des outils arithmétiques relativement simples (ceux qui sont au programme) ont des applications très importantes : par exemple en cryptographie (code RSA, Rivest-Shamir-Adleman) ou dans certains codes correcteurs (codes Reed-Solomon, BCH (Bose-Chauduri-Hocquenghem...). L'algorithme AKS (Agrawal-Kayal-Saxena) découvert en 2002 est le premier algorithme déterministe permettant, avec un temps polynomial, de répondre à la question « n est-il premier? » pour tout entier naturel n. Sa preuve, certes élaborée, peut être à peu près complètement comprise avec le programme de cette année.

Une partie de ce chapitre (idéaux, arithmétique des polynômes) se trouve dans le chapitre Ag2.

I La division euclidienne dans Z et K$[X]$

On peut se contenter du **I.1.**

I.1 Théorèmes

Proposition 1 (division euclidienne dans Z) : Soit (a,b) un couple d'éléments de **Z**, tels que $b \neq 0$. Il existe alors un unique couple (q, r) d'entiers vérifiant

$$a = bq + r \quad \text{et} \quad 0 \leq r < |b|$$

On appelle q et r quotient et reste de la division euclidienne de a par b.

Proposition 2 (division euclidienne dans $\mathbf{K}[X]$) : On considère $(\mathbf{K}, +, \times)$ un corps commutatif. Soit (A,B) un couple d'éléments de $\mathbf{K}[X]$, tels que $B \neq 0$. Il existe alors un unique couple (Q, R) de polynômes (dans $\mathbf{K}[X]$) vérifiant

$$A = BQ + R \quad \text{et} \quad \deg(R) < \deg(B)$$

On appelle Q et R quotient et reste de la division euclidienne de A par B.

On dit que **Z** *et* $\mathbf{K}[X]$ *sont des anneaux euclidiens. Cette terminologie est complètement hors-programme. Les deux divisions, dans* **Z** *et* $\mathbf{K}[X]$*, se ressemblent. Mais l'une utilise la valeur absolue, l'autre le degré, qui sont, sur leurs anneaux respectifs, des exemples de « stathmes »…*

Remarque : Sur l'anneau $\mathbf{Z}[i] = \left\{a + ib\,;\ (a,b) \in \mathbf{Z}^2\right\}$ on peut définir une division euclidienne. Elle a une particularité : il n'y a pas unicité du quotient et du reste. Cette division permet par exemple de démontrer le théorème des deux carrés (voir exercice).

I.2 Démonstrations

a. Division euclidienne dans Z

Démonstration pas vraiment importante pour les concours, on peut passer.

Existence

Commençons par supposer $a \geq 0$, et $b > 0$. L'ensemble

$$A = \{k \in \mathbf{N} \,;\; kb \leq a\}$$

est une partie non vide majorée de **N**. Et donc a un plus grand élément q (une partie non vide majorée de **R** n'a qu'une borne supérieure, mais une partie non vide majorée de **N** a un plus grand élément). On a alors

$$qb \leq a \quad (\text{car } q \in A) \qquad \text{et} \qquad (q+1)b > a \quad (\text{car } q+1 \notin A)$$

Donc $r = a - qb$ vérifie $0 \leq r < b$. Le théorème est démontré pour des nombres positifs.
Si $a < 0$ et $b > 0$, on commence par diviser $-a$ par b :

$$-a = bq + r \qquad \text{avec} \quad 0 \leq r < b$$

Si la division « tombe juste » (r=0), on a $a = b(-q)$. Sinon,

$$a = -bq - r = (-q-1)b + b - r \quad \text{où} \quad 0 < b - r < b \quad \text{car} \quad 0 < r < b$$

On a donc bien l'existence dans ce cas aussi.
Si $b < 0$, maintenant, on divise a par $-b$:

$$a = (-b)q + r \qquad \text{avec } 0 \leq r < -b$$

c'est-à-dire

$$a = (-q)b + r \qquad \text{avec } 0 \leq r < -b$$

ce qui conclut.

Il y a beaucoup d'autres façons d'aborder cette démonstration, par exemple on peut partir du fait que

$$A' = \{k \in \mathbf{N} \,;\; kb > a\}$$

est une partie non vide de **N** (si $b > 0$), donc a un plus petit élément,...

Unicité
Si $a = bq_1 + r_1 = bq_2 + r_2$, $0 \leq r_1 < |b|$, $0 \leq r_2 < |b|$, on a

$$r_2 - r_1 = b(q_1 - q_2)$$

Mais si $q_1 \neq q_2$, on a $|b(q_1 - q_2)| \geq |b|$, or

$$-|b| < r_2 - r_1 < |b|$$

d'où une contradiction. Finalement, $q_1 = q_2$, et donc $r_1 = r_2$.

b. Division euclidienne dans $\mathbf{K}[X]$

Démonstration pas vraiment importante pour les concours, on peut passer!

Existence

On fixe $B \neq 0$, et on fait une récurrence (que l'on qualifie parfois de forte, ou de faible, cela dépend des époques ou des modes...) sur le degré de A. On montre donc

$(\mathscr{P}_n)$: Si $\deg(A) \leq n$, il existe Q et R tels que $A = BQ + R$ et $\deg(R) < \deg(B)$

Pour montrer $\mathscr{P}_0$, il suffit de prendre $Q = 0$, et $R = A$, sauf dans le cas très particulier où B serait constant. Mais dans ce cas, tout polynôme A s'écrit $A = \left(\frac{1}{B}A\right)B + 0$, la division est donc toute faite.

Pour montrer $\mathscr{P}_n \Rightarrow \mathscr{P}_{n+1}$, on note $d = \deg(B)$, et on note comme d'habitude $B = \sum_{k=0}^{d} b_k X^k$. Donc $b_d \neq 0$. Soit A de degré $n+1$, $A = \sum_{k=0}^{n+1} a_k X^k$. On peut se limiter au cas $n+1 \geq d$, sinon la division est vite faite (quotient nul, reste A). On commence alors la division : $A = \frac{a_{n+1}}{b_d} X^{n+1-d} B + \cdots$; plus formellement, on constate que, si on définit

$$A_1 = A - \frac{a_{n+1}}{b_d} X^{n+1-d} B$$

alors $\deg(A_1) \leq n$. Il existe donc, par $\mathscr{P}_n$, Q_1 et R_1 tels que

$$A_1 = Q_1 B + R_1 \quad , \quad \deg(R_1) < \deg(B)$$

En remplaçant A_1 par son expression, on obtient

$$A = \left(Q_1 + \frac{a_{n+1}}{b_d}\right) B + R_1 \quad , \quad \deg(R_1) < \deg(B)$$

et on obtient bien la récurrence.

Unicité

Si $A = BQ_1 + R_1 = BQ_2 + R_2$, alors $B(Q_1 - Q_2) = R_2 - R_1$. Donc B divise $R_2 - R_1$. Mais si $\deg(R_1) < \deg(B)$ et $\deg(R_2) < \deg(B)$, alors $\deg(R_2 - R_1) < \deg(B)$. Et donc, nécessairement, $Q_1 - Q_2 = 0$, par suite $R_2 - R_1 = 0$.

Remarque
La démonstration de l'existence est « constructive » : elle donne un algorithme de détermination du quotient et du reste, qui est celui qu'on utilise (en général !) quand on effectue une division polynomiale « à la main ».

I.3 Pratique

La pratique de la division euclidienne des entiers se fait à la calculatrice en général, même si c'est bien de savoir poser une division comme au CM2.
La division euclidienne des polynômes est bien plus pénible à poser, mais il faut savoir faire (même si on ne le fera à peu près jamais).
⚠Il arrive qu'on ait besoin du reste d'une division euclidienne. L'obtention de ce reste se fait en général sans effectuer de division, donc sans s'occuper du quotient. Par exemple, on devrait arriver à
Exercice : Déterminer le reste de la division de X^n par $(X-1)(X-2)(X-3)$.
Déterminer le reste de la division de X^n par $(X-1)^2(X-2)$.

Utilisation : On trouve ce problème de reste de la division de X^n par un polynôme dans certains exercices d'oral sur l'exponentielle de matrice, par exemple : déterminer $\exp(A)$, où A est une matrice telle que $A^2 - A = 6I_n$.

II Morphismes d'anneaux, idéaux

II.1 Morphismes d'anneaux

a. Définition :

Soit $(A,+,\times)$ un anneau, $(B,+,*)$ un anneau. On appelle **morphisme d'anneaux** toute application $\phi : A \to B$ qui vérifie :

1. $\forall (x,y) \in A^2 \qquad \phi(x+y) = \phi(x) + \phi(y)$
2. $\forall (x,y) \in A^2 \qquad \phi(x \times y) = \phi(x) * \phi(y)$
3. $\phi(1_A) = 1_B$

où 1_A et 1_B désignant les éléments neutres pour les lois $\times$ sur A et $*$ sur B respectivement.
⚠Attention à ne pas oublier la propriété 3. Pour un morphisme de groupe, on n'a pas besoin de vérifier que l'élément neutre est transformé en élément neutre, c'est automatique. D'ailleurs, ici, remarquons qu'on ne demande pas de vérifier $\phi(0_A) = 0_B$. Ce sera une conséquence de 1.

Donc un morphisme d'anneaux, ce n'est pas seulement un morphisme pour les lois...Pour se rappeler de 3., il peut être utile de remarquer que l'application $a \mapsto 0_B$ vérifie 1. et 2. mais ne vérifie pas 3. Ce n'est pas un morphisme d'anneaux.
⚠Insistons : les morphismes d'anneaux sont les seuls morphismes que l'on rencontrera pour lesquels il ne suffit pas d'assurer la propriété de morphisme pour les lois. Et comme on les rencontrera rarement, il y a d'autant plus de risques d'oublier.

b. Exemple 1

On vérifie sans peine que l'ensemble $A = \{0,1\}$, muni de la loi $\times$ habituelle et de $+$ définie par $0+0 = 1+1 = 0$, $0+1 = 1+0 = 1$, est un anneau commutatif.

Si $x \in \mathbf{Z}$, on pose $\phi(x) = 0$ si x est pair, $\phi(x) = 1$ si x est impair. Alors ϕ est un morphisme d'anneaux de $(\mathbf{Z}, +, \times)$ dans A.

c. Exemple 2

Soit $(A, +, *)$ un anneau, 0_A et 1_A les éléments neutres pour les loi $+$ et $*$. On peut alors définir

$$\begin{array}{rccc} \phi : & \mathbf{Z} & \longrightarrow & A \\ & n & \longmapsto & n1_A \end{array}$$

On vérifie alors que ϕ est un morphisme d'anneaux.
La propriété $\forall (n,m) \in \mathbf{Z}^2 \quad (m+n)1_A = m1_A + n1_A$ est une propriété des puissances d'un élément d'un groupe (le groupe étant ici $(A, +)$, ce qui rend additives les « puissances »).
La propriété $\forall (n,m) \in \mathbf{Z}^2 \quad (mn)1_A = m1_A * n1_A$ est une conséquence de la distributivité de $*$ sur $+$ (détails en annexe si on n'est pas d'accord avec « c'est évident »).

d. Exemple 3

Commençons par remarquer que $(\mathbf{Z}[X], +, \times)$, ensemble des polynômes à coefficients entiers, est un anneau. Si $(A, +, *)$ est aussi un anneau, et si $a \in A$, on définit pour tout $P = \sum_{k=0}^{d} z_k X^k \in \mathbf{Z}[X]$,

$$P(a) = \sum_{k=0}^{d} z_k a^k$$

(avec la convention $a^0 = 1_A$ quelque soit l'élément a de A). L'application
$P \longmapsto P(a)$ est alors un morphisme d'anneaux de $(\mathbf{Z}[X], +, \times)$ dans $(A, +, *)$.

e. Un exercice

Soit f un morphisme d'anneaux de $(\mathbf{R}, +, \times)$ dans lui-même.

1. Montrer que, pour tout $n \in \mathbf{Z}$, $f(n) = n$.
2. Montrer que, pour tout $r \in \mathbf{Q}$, $f(r) = r$.
3. Montrer que, pour tout $x \geq 0$, $f(x) \geq 0$ (on pourra caractériser à l'aide de la loi $\times$ les réels positifs).

4. Montrer que $\forall x \in \mathbf{R} \quad f(x) = x$

f. Isomorphisme

On appelle **isomorphisme** d'anneaux tout morphisme d'anneaux bijectif. La bijection réciproque est alors aussi un morphisme d'anneaux (vérification simple).

II.2 Image d'un morphisme d'anneaux

Définition Si ϕ est un morphisme d'anneaux de $(A,+,\times)$ dans $(B,+,*)$,

$$\mathrm{Im}(\phi) = \phi(A) = \{\phi(x)\ ;\ x \in A\}$$

Ce n'est pas une définition, c'est un rappel...En effet, si ϕ est un morphisme d'anneaux, alors en particulier c'est un morphisme du groupe $(A,+)$ dans le groupe $(B,+)$, or on sait définir l'image d'un tel morphisme.

Proposition 1 C'est un sous-anneau de $(B,+,*)$.

Proposition 2 ϕ est surjectif si et seulement si $\mathrm{Im}(\phi) = B$.

La proposition 2 est très simple. Pour la proposition 1, la vérification est très directe, et permet de s'entraîner à manipuler les définitions.

Mais les morphismes d'anneaux sont décidément bien ennuyeux : le noyau d'un morphisme de groupes est un sous-groupe, le noyau d'une application linéaire est un sous-espace vectoriel, mais le noyau d'un morphisme d'anneaux n'est en général pas un sous-anneau. C'est un idéal.

II.3 Idéaux d'un anneau commutatif

Ce nom étrange vient de la notion de nombre complexe « idéal » étudiée par Kummer au XIXème siècle.

a. Noyau d'un morphisme d'anneaux

Remarquons qu'un morphisme ϕ de l'anneau $(A,+,\times)$ dans l'anneau $(B,+,*)$ est en particulier un morphisme de groupes additifs de $(A,+)$ dans $(B,+)$ (il suffit de considérer la propriété 1.). On peut donc reprendre

Définition

$$\mathrm{Ker}(\phi) = \phi^{-1}(\{0_B\}) = \{x \in A \ / \ \phi(x) = 0_B\}$$

Proposition Le morphisme ϕ est injectif si et seulement si son noyau est $\{0_A\}$

Tout cela a déjà été vu.

b. Particularité des noyaux de morphismes d'anneaux

Le noyau d'un morphisme de groupes est un sous-groupe du groupe de départ (vu).
Le noyau d'une application linéaire est un sous-espace vectoriel de l'espace vectoriel de départ (à revoir).
Insistons
⚠Le noyau d'un morphisme d'anneaux n'est, en général, pas un sous-anneau de l'anneau de départ.

Il suffit de considérer l'exemple 1 pour s'en convaincre.

On peut néanmoins, si ϕ est un morphisme d'anneaux de $(A,+,\times)$ dans $(B,+,*)$, dire des choses :
• $\mathrm{Ker}\phi$ est un sous-groupe de $(A,+)$.
• Si $a \in A$, si $x \in \mathrm{Ker}\phi$, $a \times x \in \mathrm{Ker}\phi$, et $x \times a \in \mathrm{Ker}\phi$.

c. Définition :

Soit $(A,+,\times)$ un anneau commutatif. On appelle idéal de A toute partie I de A vérifiant :

1. I est un sous-groupe de $(A,+)$
2. $\forall a \in A \quad \forall x \in I \quad a \times x \in I$

On dit parfois qu'un idéal est un sous-groupe pour + absorbant pour $\times$.

Pour un anneau commutatif, la notion d'idéal se décline en trois versions : idéal à gauche, idéal à droite, idéal bilatère. Nous ne nous en occupons pas.

d. Caractérisation pratique

Une partie I d'un anneau commutatif $(A,+,\times)$ est un idéal de A si et seulement si

1. $I \neq \emptyset$
2. $\forall (x,y) \in I^2 \quad x-y \in I$
3. $\forall a \in A \quad \forall x \in I \quad a \times x \in I$

e. Exemple fondamental

Proposition : Le noyau d'un morphisme d'anneaux est un idéal de l'anneau de départ.

f. Idéal des multiples d'un élément

Si x et y sont deux éléments de l'anneau commutatif $(A,+,\times)$, on dit que x **divise** y, et on note $x|y$, lorsqu'il existe $z \in A$ tel que $y = x \times z$. On dit que y est un **multiple** de x.

Proposition-Définition Soit $(A,+,\times)$ un anneau commutatif. Si $x \in A$, considérons l'ensemble des multiples de x : c'est $A \times x = \{z \times x \ ; \ z \in A\}$. C'est un idéal de l'anneau A. On le note souvent (a). Autrement dit,

$$A \times x = x \times A = (a)$$

Le programme dispense de la notion d'idéal engendré par une partie. Elle n'est pas plus compliquée que ses analogues (sous-groupe engendré, sous-espace vecrotiel engendré...) avec les mêmes étapes :

1. L'intersection d'une famille quelconque d'idéaux est un idéal : si, pour tout $k \in K$, I_k est un idéal de $(A,+,\times)$, alors $\bigcap_{k\in K} I_k$ est un idéal de $(A,+,\times)$.
2. Etant donnée une partie X de A, il y a un plus petit idéal (pour l'inclusion) contenant X : c'est l'intersection des idéaux contenant X.
3. Cet idéal s'appelle l'idéal engendré par X

On remarque que

$$x|y \quad \Leftrightarrow \quad y \in Ax \quad \Leftrightarrow \quad Ay \subset Ax$$

Autrement dit, la relation de divisibilité s'exprime en termes d'inclusion d'idéaux. Grâce à cette remarque assez simple, on peut présenter les idées de base de l'arithmétique (divisibilité, pgcd, ppcm...) en termes d'idéaux.

II.4 Annexe

On veut montrer que, dans un anneau,

$$\forall (n,m) \in \mathbf{Z}^2 \qquad (mn)1_A = (m1_A) * (n1_A)$$

On fixe par exemple n, on remarque d'abord que

$$(0n)1_A = 01_A = 0_A \qquad \text{et} \qquad (01_A) * (n1_A) = 0_A * (n1_A) = 0_A$$

puis que, si $m \in \mathbf{N}$,

$$((m+1)n)\,1_A = (mn+n)\,1_A = (mn)1_A + n1_A$$

ce qui fait que, si $(mn)1_A = (m1_A) * (n1_A)$,

$$((m+1)n)\,1_A = (m1_A)*(n1_A)+1_A*(n1_A) = (m1_A+1_A)*(n1_A) = ((m+1)1_A)*(n1_A)$$

et donc, par récurrence,

$$\forall m \in \mathbf{N} \qquad (mn)1_A = (m1_A) * (n1_A)$$

Maintenant, il suffit de remarquer que, si $m \in \mathbf{N}$,

$$\begin{aligned} 0_A &= ((m+(-m))\,n)\,1_A \\ &= (mn+(-m)n)1_A \\ &= (mn)1_A + ((-m)n)1_A \\ &= (m1_A) * (n1_A) + ((-m)n)1_A \end{aligned}$$

pour conclure que

$$((-m)n)1_A = -(m1_A) * (n1_A) = (-(m1_A)) * (n1_A) = ((-m)1_A) * (n1_A)$$

ce qui termine une démonstration d'un inintérêt certain.

III Idéaux de Z et de K[X]

Théorème

Sur Z : Soit I un idéal de $\mathbf{Z}$. Il existe un unique $n \in \mathbf{N}$ tel que

$$I = (n) = n\mathbf{Z}$$

Sur K$[X]$: soit I un idéal de $\mathbf{K}[X]$; il existe un unique polynôme nul ou unitaire P tel que

$$I = P\mathbf{K}[X] = (P)$$

Remarque : Lorsque deux éléments d'un anneau se divisent mutuellement, ils sont dits associés. Deux éléments a et b sont donc associés si et seulement si $(a) = (b)$ (i.e. les multiples de l'un sont les multiples de l'autre).

Dans $\mathbf{Z}$: deux entiers a et b sont associés (i.e. $(a) = (b)$) si et seulement si

Dans $\mathbf{K}[X]$: deux polynômes A et B sont associés (i.e. $(A) = (B)$) si et seulement si

Plus généralement, dans un anneau intègre, a et b sont associés si et seulement si il existe $u \in A^*$ (autrement dit u inversible dans A) tel que $a = ub$.

Remarque : On traite les entiers et les polynômes en parallèle, mais ce n'est pas quand même tout-à-fait la même chose. Dans $\mathbf{Z}$, les idéaux sont les sous-groupes pour $+$. La notion d'idéal n'a donc pas vraiment d'intérêt. Dans $\mathbf{K}[X]$, c'est très différent. Par exemple, les $\mathbf{K}_n[X]$ sont des sous-groupes pour $+$, mais ne sont pas des idéaux.
On peut comprendre cela assez aisément : dans $\mathbf{Z}$, la multiplication n'existe pas vraiment…c'est une notation pour une addition. nz, si $n \in \mathbf{N}$, c'est $z + \cdots + z$ n fois. Et si n est négatif, on prend l'opposé. Alors que dans $\mathbf{K}[X]$, il y a une vraie multiplication, qui ne se réduit pas à de l'addition.

Parenthèse culturelle (h.p) Un anneau sur lequel on peut définir une division euclidienne est dit. . .euclidien. Un anneau tel que tout idéal soit l'ensemble des multiples d'un de ses éléments est dit principal. Un anneau dans lequel tout élément se décompose en produit de facteurs irréductibles est dit factoriel. Euclidien ⇒ Principal ⇒ Factoriel.

Table des matières