Ag6 : Arithmétique sur **Z** et **K**[X]

I PGCD, PPCM

I.1 Définition du pgcd par les idéaux

Sur Z : On considère a, b deux éléments de $\mathbf{Z}$, $(a,b) \neq (0,0)$. Alors

$$I = \{au + bv \ ; \ (u,v) \in \mathbf{Z}^2\}$$

est un idéal non nul (i.e. différent de (0)) de $(\mathbf{Z}, +, \times)$. Il existe un unique $d \in \mathbf{N}_*$ tel que $I = (d)$; d est appelé **pgcd** (plus grand commun diviseur) de a et b, et noté $a \wedge b$.
En résumé :
Le pgcd de a et de b est l'unique entier strictement positif d tel que

$$\{au + bv \ ; \ (u,v) \in \mathbf{Z}^2\} \ = (d) = \ \{dw \ ; \ w \in \mathbf{Z}\}$$

Sur K$[X]$: On considère A, B deux éléments de $\mathbf{K}[X]$, $(A,B) \neq (0,0)$. Alors

$$I = \{AU + BV \ ; \ (U,V) \in (\mathbf{K}[X])^2\}$$

est un idéal non nul (i.e. différent de (0)) de $(\mathbf{K}[X], +, \times)$. Il existe un unique D unitaire tel que $I = (D)$; D est appelé **PGCD** (plus grand commun diviseur) de A et B, et parfois noté $A \wedge B$ (même si la seule notation au programme est pgcd(A,B)).
Autrement dit,
le pgcd de A et de B est l'unique polynôme unitaire D tel que

$$\{AU + BV \ ; \ (U,V) \in \mathbf{K}[X]^2\} \ = \ \{DW \ ; \ W \in \mathbf{K}[X]\}$$

I.2 (bis)

On peut être (il faut être) ensembliste jusqu'au bout :

$$(d) = (a) + (b)$$

I.3 Equivalence avec la définition habituelle

Sur $\mathbf{Z}$ ou sur $\mathbf{K}[X]$, définissons $a \wedge b$ comme ci-dessus. Alors les diviseurs communs à a et b sont les diviseurs de $a \wedge b$. Autrement dit :

$$d|a \quad \text{et} \quad d|b \quad \Leftrightarrow \quad d|a \wedge b$$

Si a et b sont des entiers, $a \wedge b$ est donc littéralement le plus grand diviseur commun à a et b (!).
Si A et B sont des polynômes, $A \wedge B$ est le polynôme unitaire de plus grand degré qui divise à la fois A et B.

I.4 Détermination pratique (algorithme d'Euclide)

a. Evocation de l'algorithme

Si $b = 0$, c'est fini (avant d'avoir commencé) : la pgcd est a (supposé non nul, car pgcd$(0,0)$ n'est pas défini).
Si $b \neq 0$, on remarque que

$$a \wedge b \; = \; b \wedge (a - bq)$$

pour tout entier q. C'est d'ailleurs, quoique facile, très intéressant à montrer car on utilise une technique importante : la double divisibilité. Interprétée en termes d'idéaux, ce n'est d'ailleurs rien d'autre que la double inclusion.
On en déduit que, si r_1 est le reste de la division de a par b, $a \wedge b = b \wedge r_1$. On peut alors continuer, et dire que $a \wedge b = r_1 \wedge r_2$, r_2 étant le reste de la division de b par r_1. C'est le point de départ de l'algorithme d'Euclide, ou algorithme des divisions successives. Le pgcd est le dernier reste non nul obtenu dans l'algorithme.

b. Un exemple

Déterminer par cette méthode le pgcd de 2514 et 1002.

c. Un exercice

1. On se place dans l'anneau $(\mathbf{K}[X], +, \times)$ des polynômes à une indéterminée sur un corps commutatif $(\mathbf{K}, +, \times)$.

   Soit (a, b) deux entiers naturels non nuls. Montrer que, si le reste de la division de a par b est r, le reste de la division de $X^a - 1$ par $X^b - 1$ est $X^r - 1$.
2. Sous les mêmes hypothèses que dans la question précédente, écrire le pgcd de $X^a - 1$ et $X^b - 1$ à l'aide de $a \wedge b$.
3. Comment retrouver ce résultat sur $\mathbf{C}[X]$ par une autre méthode ?

I.5 Eléments premiers entre eux, théorème de Bezout

a. Eléments premiers entre eux

On dit que a et b sont premiers entre eux lorsque $a \wedge b = 1$. Cela signifie que les seuls diviseurs communs à a et b sont...
...1 et -1 si $A = \mathbf{Z}$
...les polynômes constants si $A = \mathbf{K}[X]$.

b. Théorème de Bezout

Théorème de Bezout a et b sont premiers entre eux si et seulement si il existe u et v tels que $au + bv = 1$.

Inutile ici de distinguer les deux contextes : entiers ou polynômes. C'est bien l'intérêt des structures algébriques de pouvoir dans une certaine mesure s'abstraire des objets concernés.

c. Obtention de coefficients de Bezout par l'algorithme d'Euclide

L'algorithme d'Euclide permet non seulement d'obtenir le pgcd de deux éléments a et b, mais aussi de déterminer u, v tels que

$$au + bv = a \wedge b$$

I.6 Une caractérisation utile du pgcd

Proposition : Soit $(a,b) \neq (0,0)$, et $d \neq 0$, positif si on est sur $\mathbf{Z}$, unitaire si on est sur $\mathbf{K}[X]$; d est le PGCD de a et b si et seulement si les deux conditions suivantes sont réalisées :

(i) d divise a et b

(ii) les quotients de a et b par d sont premiers entre eux.

Autrement dit, d est le PGCD de a et b si et seulement s'il existe a' et b' tels que

$$a = da' \quad , \quad b = db' \quad , \quad a' \wedge b' = 1$$

Ici aussi, entiers et polynômes se traitent de la même manière.

Ce résultat s'utilise souvent de la manière suivante : on veut appliquer un résultat, pour cela on a besoin de l'hypothèse $a \wedge b = 1$, or ce n'est pas le cas. Qu'à cela ne tienne : on divise a et b par leur pgcd, les quotients a' et b' sont premiers entre eux, on travaille avec a' et b'.

I.7 Théorème (ou lemme...) de Gauss

a. Le lemme de Gauss

Théorème : Soit a, b, c trois entiers ou trois polynômes ; si a divise bc et est premier avec b, alors a divise c. Ou :

$$(a|bc \quad \text{et} \quad a \wedge b = 1) \Longrightarrow (a|c)$$

Démonstration 1 : On utilise le théorème de Bezout : il existe u et v tels que

$$ua + vb = 1$$

On multiplie tout par c. Comme a divise uac (évident) et vbc (hypothèse), il divise leur somme, qui vaut c.

Démonstration 2 : Plaçons-nous dans le cas des entiers. Rappelons que $\nu_p(a)$ désigne la puissance à laquelle p figure dans la décomposition de a en produit de facteur premiers. Ecrivons cette décomposition :

$$a = \epsilon \prod_{p \in \mathscr{P}} p^{\nu_p(a)} \qquad (\epsilon = \pm 1)$$

Comme a divise bc, alors pour tout nombre premier p on a

$$\nu_p(a) \leq \nu_p(bc) = \nu_p(b) + \nu_p(c)$$

Si $1 \leq \nu_p(a)$, alors $0 = \nu_p(b)$ (hypothèse $a \wedge b = 1$), donc $\nu_p(a) \leq \nu_p(c)$. Et si $\nu_p(a) = 0$, alors $\nu_p(a) \leq \nu_p(c)$ évidemment. Donc on conclut.

La démonstration 2 n'est pas forcément à négliger : penser à la decomposition en facteurs premiers est parfois moins élégant mais aussi moins astucieux. Par exemple, essayez de montrer les corollaires...

Corollaire 1 : Si $a|c$ et $b|c$ et $a \wedge b = 1$, alors $ab|c$.

Corollaire 2 : $(a \wedge bc = 1) \iff (a \wedge b = a \wedge c = 1)$.

Corollaire 2 bis : $\big(a \wedge b_1 \dots b_p = 1\big) \iff \big(a \wedge b_1 = a \wedge b_2 = \dots = a \wedge b_p = 1\big)$.

Corollaire 3 : Si $a \wedge b = 1$, alors $a \wedge bc = a \wedge c$.

b. Un exemple d'application

Le théorème de Gauss est très utile ; en voici une application simple :

Proposition Soit P un polynôme de $\mathbf{K}[X]$, $\alpha_1, \dots, \alpha_m$ des éléments distincts de $\mathbf{K}$. Chaque α_i est racine de P de mutiplicité au moins m_i si et seulement si le polynôme $\prod_{i=1}^{m} (X - \alpha_i)^{m_i}$ divise P.

c. Un exercice à savoir faire

Ecrire le triangle de Pascal jusqu'à la ligne des $\binom{7}{\dots}$ au moins (mais si on va plus loin, il faut aller jusqu'à 11). Quelle remarque de divisibilité peut-on faire sur les $\binom{p}{\dots}$ lorsque p est premier ? Le démontrer.

Tant qu'on y est à avoir le triangle de Pascal sous les yeux, s'il est bien construit, on peut faire les sommes des diagonales...qu'observe-t-on ? le démontrer !

I.8 Equations $ax + by = c$ (h.p. mais classique)

L'étude de ces équations est assez classique, et permet de manipuler les pgcd et le théorème de Gauss

Dans les exercices qui suivent, les inconnues sont toujours des nombres entiers.

Exercice 1 Résoudre l'équation $7x + 11y = 1$.

Exercice 2 Résoudre l'équation $13x + 6y = 9$.

Exercice 3 Résoudre l'équation $42x + 54y = 12$.

Exercice 3 On considère deux entiers a et b, tels que $(a,b) \neq (0,0)$. Trouver une condition nécessaire et suffisante sur l'entier c pour que l'équation $ax + by = c$ ait une solution. Lorsque cette condition est réalisée, dire comment on peut trouver une solution, puis comment les trouver toutes.

I.9 PPCM

Les idéaux sont plus naturels lorsqu'on définit le ppcm que lorsqu'on définit le pgcd. Mais le ppcm est une notion beaucoup moins importante que le pgcd.

Définition : Supposons a **et** b non nuls ; $I = (a) \cap (b)$ est un idéal non nul. Il existe donc un unique ($m > 0$ si on est sur $\mathbf{Z}$) (m unitaire si on est sur $\mathbf{K}[X]$) tel que

$$(a) \cap (b) = (m)$$

On appelle m le PPCM de a et b. On peut le noter $a \vee b$.

Proposition Supposons a et b non nuls : soit d leur PGCD, m leur PPCM. Alors ab et md sont associés (i.e. égaux au signe près s'il s'agit d'entiers, égaux à un coefficient multiplicatif non nul près d'il s'agit de polynômes).

Là encore, la décomposition en facteurs premiers est une bonne méthode.

I.10 PGCD de plus de deux éléments

On note A un anneau qui peut être $\mathbf{Z}$ ou $\mathbf{K}[X]$.

a. Définition

Définition Soit $(a_1,\dots,a_p)\in\mathbf{A}^p$, non tous nuls. Considérons

$$I=\{u_1a_1+u_2a_2+\cdots+u_pa_p\ ;\ (u_1,\dots,u_p)\in\mathbf{A}^p\}$$

Alors I est un idéal non nul (non $\{0\}$) de A. Il existe donc un unique d (strictement positif si $A=\mathbf{Z}$) (unitaire si $A=\mathbf{K}[X]$) tel que $I=(d)$; on appelle d le PGCD de $(a_1,\dots,a_p)$.

Remarque I est le plus petit idéal contenant les a_i ; on dit parfois que c'est l'idéal engendré par $(a_1,\dots,a_p)$.

b. Caractérisation

Proposition

$$\Big(\forall i\in\{1,\dots,p\}\quad d|a_i\Big)\Leftrightarrow\Big(d|\operatorname{pgcd}(a_1,\dots,a_p)\Big)$$

Ou encore : les diviseurs communs à tous les a_i sont les diviseurs de leur pgcd.

c. Associativité du pgcd

Proposition

$$\operatorname{pgcd}(a_1,\dots,a_{p+1})=\operatorname{pgcd}\big(\operatorname{pgcd}(a_1,\dots,a_p),a_{p+1}\big)$$

($a_1,\dots a_p$ n'étant pas tous nuls)

Extension Plus généralement, avec des hypothèses évidentes :

$$\operatorname{pgcd}(a_1,\dots,a_p,b_1,\dots,b_q)=\operatorname{pgcd}\big(\operatorname{pgcd}(a_1,\dots,a_p),\operatorname{pgcd}(b_1,\dots,b_q)\big)$$

Intérêt Ceci permet de calculer un pgcd de p éléments en se ramenant à des calculs successifs de pgcd de deux éléments. Calculer, par exemple, $\operatorname{pgcd}(21,35,56)$.

d. Eléments premiers entre eux (dans leur ensemble)

Définition On dit que $a_1, \ldots, a_p$ sont premiers entre eux (dans leur ensemble) lorsque leur PGCD est égal à 1.

Théorème de Bezout $a_1, \ldots, a_p$ sont premiers entre eux dans leur ensemble si et seulement s'il existe $u_1, \ldots, u_p$ dans A tels que

$$u_1 a_1 + u_2 a_2 + \cdots + u_p a_p = 1$$

Remarque Il ne faut pas confondre « premiers entre eux » (dans leur ensemble) et « premiers entre eux deux à deux ».
L'exemple du pgcd de $(2 \times 3\ ;\ 2 \times 5\ ;\ 3 \times 5)$ peut être instructif.

II Nombres premiers, polynômes irréductibles

II.1 Nombres premiers

a. Définition

Un entier naturel supérieur ou égal à 2 est dit premier lorsque ses seuls diviseurs positifs sont 1 et lui-même.

Pour insister : 1 n'est pas premier. La plupart des nombres premiers sont impairs.

b. Décomposition en facteurs premiers

Tout entier strictement supérieur à 1 se décompose de manière unique (à l'ordre des facteurs près en produit de nombres premiers :

$$n = \prod_{i=1}^{d} p_i^{m_i}$$

où les p_i sont premiers distincts, et les m_i sont des entiers naturels non nuls.

La démonstration se fait bien par récurrence (« « forte » »), à partir d'un lemme qu'il est utile de savoir montrer.

Lemme Tout entier naturel ≥ 2 a au moins un diviseur premier

c. Théorème

Il y a une infinité de nombres premiers.

La démonstration classique a été posée dans un problème d'écrit des Mines. Elle fait partie de la culture générale. Et, surtout, son principe est utilisé dans des preuves de résultats analogues.

Démonstration, donc :
Réutilisation de la méthode : Adapter la démonstration précédente pour montrer qu'il y a une infinité de nombres premiers de la forme $4n+3$, $n \in \mathbf{N}$.

d. Théorème d'Euclide

Un nombre premier divise un produit d'entiers si et seulement si il divise l'un des facteurs.

e. Valuation p-adique

Soit p un nombre premier. Si $n \in \mathbf{Z} \setminus \{0\}$, il existe un unique entier naturel m tel que

$$p^m | n \qquad , \qquad p^{m+1} \not| n$$

On note $m = \nu_p(n)$, ν_p est la valuation p-adique. Autrement dit, notant $\mathscr{P}$ l'ensemble des nombres premiers, la décomposition en facteurs premiers d'un entier naturel n est

$$n = \prod_{p \in \mathscr{P}} p^{\nu_p(n)}$$

f. Valuation p-adique et divisibilité

Proposition On note $\mathscr{P}$ l'ensemble des nombres premiers. Soit a, b deux entiers non nuls.

$$\big(a \text{ divise } b\big) \Leftrightarrow \big(\forall p \in \mathscr{P} \quad \nu_p(a) \leq \nu_p(b)\big)$$

g. Utilisation pour le calcul du pgcd et du ppcm

Soit a, b deux entiers non nuls. On écrit

$$a = \prod_{i=1}^{d} p_i^{m_i} \qquad b = \prod_{i=1}^{d} p_i^{n_i}$$

où les p_i sont des nombres premiers deux à deux distincts, les n_i et les m_i des entiers naturels (qui peuvent être nuls). Alors

$$\text{pgcd}(a,b) = \prod_{i=1}^{d} p_i^{\min(m_i,n_i)} \qquad \text{ppcm}(a,b) = \prod_{i=1}^{d} p_i^{\max(m_i,n_i)}$$

On peut aussi formuler ce résultat de la manière suivante :

$$a \wedge b = \prod_{p \in \mathscr{P}} p^{\min(\nu_p(a),\nu_p(b))}$$

Autrement dit, $a \wedge b$ est l'unique entier naturel d non nul tel que

$$\forall p \in \mathscr{P} \qquad v_p(d) = \min(v_p(a), v_p(b))$$

Et aussi :

$$a \vee b = \prod_{p \in \mathscr{P}} p^{\max(v_p(a), v_p(b))}$$

L'utilisation de la décompositions en facteurs premiers pour un calcul de pgcd ou de ppcm n'est pas raisonnable algorithmiquement : on ne sait pas décomposer efficacement un nombre de grande taille en facteurs premiers, c'est même une raison de la fiabilité du codage RSA. Mais pour des résultats théoriques, ou pour le calcul du pgcd de petits nombres, c'est intéressant. Par exemple, le pgcd de 2514 et 1002 se calcule facilement par cette méthode.

De plus, cette écriture du pgcd et du ppcm permet par exemple de montrer, peut-être plus facilement,

$$|ab| = \text{pgcd}(a, b) \times \text{ppcm}(a, b)$$

h. Parenthèse : culture générale (h.p !)

Il serait dommage de ne pas connaître deux résultats célèbres :

Théorème de Dirichlet Dans toute progression arithmétique $\{an+b; n \in \mathbf{N}\}$ avec $a \wedge b = 1$ (a, b naturels non nuls), il y a une infinité de nombres premiers.

Théorème des nombres premiers Si $\pi(x)$ désigne le nombre de nombres premiers inférieurs ou égaux à x,

$$\pi(x) \underset{x \to +\infty}{\sim} \frac{x}{\ln x}$$

Ce n'est pas évident, mais on sait faire...En revanche, il serait intéressant de montrer

$$\pi(x) = \text{li}(x) + \underset{x \to +\infty}{O}\left(x^{1/2+\epsilon}\right)$$

pour tout $\epsilon > 0$, où

$$\text{li}(x) = \int_2^x \frac{\mathrm{d}t}{\ln t}$$

II.2 Polynômes irréductibles

a. Définition

Un polynôme non constant est dit **irréductible** lorsque ses diviseurs sont tous associés soit à 1, soit à lui-même : autrement dit, P est irréductible si et seulement si ses seuls diviseurs sont les polynômes constants et les polynômes λP où λ est un « scalaire » non nul (i.e. un élément de $\mathbf{K} \setminus \{0\}$). Encore dit autrement, P est irréductible si et seulement s'il n'existe pas de factorisation $P = AB$ où $0 < \deg(A) < \deg(P)$, i.e. A et b non constants.

b. Exemples

Dans $\mathbf{C}[X]$, les polynômes irréductibles sont les polynômes de degré 1 (à savoir).
Dans $\mathbf{R}[X]$, les polynômes irréductibles sont les polynômes de degré 1 et les polynômes de degré 2 à discriminant < 0 (à savoir).
Dans $\mathbf{Q}[X]$, les choses sont beaucoup plus compliquées...

Par exemple, dans $\mathbf{R}[X]$, $X^4 + 1$ n'est pas irréductible. Pourtant, il n'a pas de racine réelle.

c. Décomposition en facteurs irréductibles

Tout polynôme P se décompose de manière unique (à l'ordre des facteurs près sous la forme : $P = a \prod_{i=1}^{n} P_i^{\alpha_i}$ où les P_i sont irréductibles unitaires, les α_i des entiers naturels non nuls, a le coefficient dominant de P.

d. Théorème

Un polynôme irréductible divise un produit de polynômes si et seulement si il divise l'un des facteurs.

e. Utilisation pour le calcul du pgcd et du ppcm

Soit P, Q deux entiers non nuls. On écrit

$$P = \alpha \prod_{i=1}^{d} P_i^{m_i} \qquad Q = \beta \prod_{i=1}^{d} P_i^{n_i}$$

où les P_i sont des polynômes irréductibles unitaires deux à deux distincts, les n_i et les m_i des entiers naturels (qui peuvent être nuls). Alors

$$\text{pgcd}(P,Q) = \prod_{i=1}^{d} P_i^{\min(m_i,n_i)} \qquad \text{ppcm}(P,Q) = \prod_{i=1}^{d} P_i^{\max(m_i,n_i)}$$

Table des matières