Premier cours : division euclidienne sur $\mathbf{Z}$ et $\mathbf{K}[X]$

Avant de donner la définition formelle d'anneau, notion qui sera l'objet principal de ce cours, on révise deux exemples importants : l'ensemble $\mathbf{Z}$ des entiers relatifs, et l'ensemble $\mathbf{K}[X]$ des polynômes à coefficients dans $\mathbf{K}$ (pour l'instant $\mathbf{K}$ est l'ensemble des nombres réels ou complexes).

Théorème 1. *Soient $a, b \in \mathbf{Z}$, avec $b \neq 0$. Il existe un couple $(q, r) \in \mathbf{Z} \times \mathbf{Z}$ tel que*

$$a = bq + r \text{ et } |r| < |b|.$$

Remarque 2. Si on exige de plus $r \geq 0$, le couple (q, r) est unique. En effet si

$$a = bq_1 + r_1 = bq_2 + r_2,$$

on a $-|b| < |b(q_1 - q_2)| < |b|$, d'où $q_1 = q_2$, et donc également $r_1 = r_2$.

Par exemple si $a = -7$, $b = 3$, on peut écrire les deux divisions euclidiennes suivantes :

$$-7 = 3 \times -3 + 2$$
$$\text{ou } -7 = 3 \times -2 - 1.$$

Preuve du théorème. Supposons d'abord $b > 0$. Soit $q \in \mathbf{Z}$ maximal tel que $a \geq bq$, et posons $r = a - bq \geq 0$. Par l'absurde, supposons $r \geq b$, donc $r - b = r - b(q+1) \geq 0$ ce qui contredit la maximalité de q. Ainsi on a trouvé un couple (q, r) qui convient, avec $r \geq 0$. A noter qu'en prenant $q \in \mathbf{Z}$ minimal tel que $a \leq bq$, on aurait trouvé un couple (q, r) qui convient, avec $r \leq 0$.

Considérons maintenant le cas $b < 0$. On applique le point précédent à $(-a, -b)$ pour trouver (q, r) vérifiant $-a = -bq + r$, et alors (multiplier cette égalité par -1) on voit que $(q, -r)$ convient. □

Théorème 3. *Soit $A, B \in \mathbf{K}[X]$, avec $B \neq 0$. Alors il existe un unique couple $(Q, R) \in K[X] \times \mathbf{K}[X]$ tel que*

$$A = BQ + R \text{ et } \deg R < \deg B.$$

Remarque 4. Il est d'usage de poser $\deg 0 = -\infty$. Avec cette convention l'énoncé du théorème reste correct même si B est un polynôme constant. A noter que la convention se justifie aussi pour que la relation suivante soit toujours vraie :

$$\deg PQ = \deg P + \deg Q$$

Preuve du théorème. Existence : On note $n = \deg A$, $m = \deg B$. Si $n < m$, il suffit de prendre $Q = 0$, $R = A$. Si $n \geq m$, on écrit

$$A(X) = a_n X^n + \dots \text{ et } B(X) = b_m X^m + \dots,$$

et on pose $A_0 = A$ et $A_1 = A - \frac{a_n}{b_m} X^{n-m} B$, qui vérifie $\deg A_1 < \deg A$. En itérant ce procédé on construit une suite A_i de polynômes de degrés décroissants, vérifiant $A_i = A_{i-1} - M_i B$ pour certains monômes M_i, jusqu'à atteindre un certain indice $r \geq 1$ tel que

$$\deg A_{r-1} \geq \deg B > \deg A_r.$$

Alors $Q = M_1 + M_2 + \dots + M_r$ et $R = A_r$ conviennent.

Unicité : Si $A = BQ_1 + R_1 = BQ_2 + R_2$, alors

$$B(Q_1 - Q_2) = R_2 - R_1.$$

On obtient

$$\deg B > \deg(R_2 - R_1) = \deg B + \deg(Q_1 - Q_2),$$

d'où $Q_1 - Q_2 = 0$, et donc également $R_2 = R_1$. □

Définition 5. Soit $a \in \mathbf{Z}$. On dit que $b \in \mathbf{Z}$ est un **diviseur** de a, ou que a est un **multiple** de b, s'il existe $c \in \mathbf{Z}$ tel que $a = bc$. On note $\mathrm{div}(a)$ l'ensemble de tous les diviseurs de a.

Exemple 6. $\mathrm{div}(6) = \{1, 2, 3, 6, -1, -2, -3, -6\}$.

Remarque 7. (1) Si $a = bq + r$, alors

$$\mathrm{div}(a) \cap \mathrm{div}(b) = \mathrm{div}(b) \cap \mathrm{div}(r).$$

En effet si c divise a et b, alors il divise aussi $r = a - bq$; et réciproquement si c divise b et r, il divise aussi $a = bq + r$.

(2) Si on applique la définition à $a = 0$ on obtient $\mathrm{div}(0) = \mathbf{Z}$. C'est ok, c'est même un ingrédient crucial de la preuve du théorème qui suit. Plus tard on utilisera la terminologie "diviseur de zéro" dans un sens plus restreint, mais pour l'instant on n'en dit pas plus...

Théorème 8 (Relation de Bezout via algorithme d'Euclide)**.** *Soient $a, b \in \mathbf{Z}$. Il existe $d \in \mathbf{Z}$ tel que*

$$\mathrm{div}(d) = \mathrm{div}(a) \cap \mathrm{div}(b).$$

De plus d est de la forme $d = au + bv$ pour certains $u, v \in \mathbf{Z}$.

Remarque 9. l'entier d du théorème est unique au signe près (par contre u et v ne sont pas uniques) : s'en convaincre. On appelle d "le" PGCD de a et b (ou "un" PGCD, si on veut souligner l'ambiguité sur le signe). Ici "plus grand" doit s'entendre au sens de la relation d'ordre "m est plus grand que n si m est un multiple de n". Si on se restreint aux entiers positifs l'ordre coïncide avec l'ordre usuel, mais à noter que par exemple -4 est plus grand que 2... Et par exemple -4 est un PGCD de 12 et -8.

Vocabulaire : on dit que deux entiers a et b sont **premiers entre eux** si 1 est un PGCD de a et b.

Preuve du théorème 8. On procède par algorithme d'Euclide, c'est-à-dire par divisions euclidiennes successives. Quitte à intervertir a et b on peut supposer $|a| \geq |b|$. On pose $r_0 = a$, $r_1 = b$, puis pour $i \geq 1$, r_i étant défini et non nul, on définit r_{i+1} en écrivant une division euclidienne

$$r_{i-1} = r_i q_{i+1} + r_{i+1}.$$

On obtient ainsi une suite strictement décroissante jusqu'à obtenir un reste nul.

$$|r_1| > |r_2| > \cdots > |r_k| > |r_{k+1}| = 0.$$

Par la remarque 7 on a

$$\mathrm{div}(a) \cap \mathrm{div}(b) = \mathrm{div}(r_1) \cap \mathrm{div}(r_2) = \mathrm{div}(r_2) \cap \mathrm{div}(r_3) = \cdots = \mathrm{div}(r_k) \cap \mathrm{div}(r_{k+1}) = \mathrm{div}(r_k).$$

Ainsi $d = r_k$, le premier reste non nul, convient.

On obtient les entiers u et v en "remontant l'algorithme ligne à ligne" : le faire en td. □

Exemple 10. On cherche le PGCD de 21 et 13 par algorithme d'Euclide.

Restes positifs :

$$\begin{aligned} 21 &= 13 \times 1 + 8 \\ 13 &= 8 \times 1 + 5 \\ 8 &= 5 \times 1 + 3 \\ 5 &= 3 \times 1 + 2 \\ 3 &= 2 \times 1 + \boxed{1} \\ 2 &= 2 \times 1 + 0 \end{aligned}$$

Restes négatifs (plus rapide sur cet exemple !) :

$$\begin{aligned} 21 &= 13 \times 2 - 5 \\ 13 &= 5 \times 3 - 2 \\ 5 &= 2 \times 3 - \boxed{1} \\ 2 &= 2 \times 1 + 0 \end{aligned}$$

Ça semble bien compliqué, pourquoi ne pas écrire simplement les décompositions en facteurs premiers $21 = 3 \times 7$, $13 = 13$ pour conclure directement ? Indication : calculer le PGCD de 66023 et 62177 par ces deux méthodes (algortithme d'Euclide ou décomposition en facteurs premiers)...

Remarque 11. Comme on dispose d'une division euclidienne sur $\mathbf{K}[X]$, on peut exactement de la même manière obtenir l'énoncé suivant. Cette fois le PGCD est unique à une constante multiplicative près. A nouveau, la méthode par algorithme d'Euclide évite d'avoir à décomposer en facteurs premiers, qui est un calcul difficile en général.

Théorème 12 (Relation de Bezout pour les polynômes)**.** *Soient $A, B \in \mathbf{K}[X]$. Il existe $D \in \mathbf{K}[X]$ tel que*

$$\mathrm{div}(D) = \mathrm{div}(A) \cap \mathrm{div}(B).$$

De plus D est de la forme $D = AU + BV$ pour certains $U, V \in \mathbf{K}[X]$.

On termine avec quelques applications.

Recherche d'un inverse modulo n.

Proposition 13. *Soit n un entier, et a un entier premier avec n. Alors a admet un inverse modulo n, c'est-à-dire qu'il existe un entier b tel que*

$$ab = 1 \mod n.$$

Preuve. On écrit une relation de Bezout entre a et n : $au + nv = 1$. Alors $b = u$ convient. □

Remarque 14. C'est l'occasion d'introduire (de rappeler ?) la notation $\mathbf{Z}/n\mathbf{Z}$ (de façon "naïve", on reformulera ça plus tard à l'aide de la notion d'anneau quotient). Si n est un entier positif (et disons $n \geq 2$, même si on pourra réfléchir aux cas $n = 0$ ou 1...), et $a \in \mathbf{Z}$, on note $\bar{a}$ l'ensemble des entiers égaux à a modulo n, c'est-à-dire de la forme $a + kn$, $k \in \mathbf{Z}$. A noter que pour tout a, il existe $0 \leq r \leq n-1$ tel que $\bar{a} = \bar{r}$ (reste de la division euclidienne de a par n). On note

$$\mathbf{Z}/n\mathbf{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}.$$

Par exemple si $n = 3$, $\mathbf{Z}/3\mathbf{Z} = \{\bar{0}, \bar{1}, \bar{2}\}$, où

$$\begin{aligned} \bar{0} &= \{\ldots, -6, -3, 0, 3, 6, \ldots\} \\ \bar{1} &= \{\ldots, -5, -2, 1, 4, 7, \ldots\} \\ \bar{2} &= \{\ldots, -4, -1, 2, 5, 8, \ldots\} \end{aligned}$$

On peut munir $\mathbf{Z}/n\mathbf{Z}$ d'une addition et d'une multiplication, en posant

$$\begin{aligned} \bar{a} + \bar{b} &:= \overline{a+b} \\ \bar{a} \cdot \bar{b} &:= \overline{a \cdot b} \end{aligned}$$

On vérifie que ces définitions ne dépendent pas d'un choix de représentants : si a et a' sont égaux modulo n, et b et b' sont égaux modulo n, alors $a+b$, $a'+b'$ d'une part, et $a \cdot b$, $a' \cdot b'$ d'autre part, sont égaux modulo n.

L'énoncé de la proposition peut s'écrire : pour tout a premier avec n, il existe $\bar{b}$ tel que $\bar{a}\bar{b} = \bar{1}$ dans $\mathbf{Z}/n\mathbf{Z}$.

Le nombre d'entiers $0 \leq a \leq n-1$ premiers avec n se note classiquement $\varphi(n)$, on dit que φ est l'**indicatrice d'Euler**.

Résolution d'une équation diophantienne linéaire. On considère une équation de la forme suivante, où $a, b, c \in \mathbf{Z}$ sont des paramètres fixés, et $x, y \in \mathbf{Z}$ sont des inconnues :

$$(E) \quad ax + by = c$$

Proposition 15. *Notons d un PGCD de a et b. L'équation (E) admet des solutions ssi d divise c. De plus, si d divise c, l'ensemble des solutions s'obtient en faisant la somme d'une solution particulière et des solutions de l'équation homogène associée*

$$(E_0) \quad ax + by = 0$$

Remarque 16. Vu en td :

- Une solution particulière s'obtient à partir d'une relation de Bezout pour a et b.
- En divisant (E_0) par le PGCD de a et b on obtient une équation équivalente

  $$(E_0') \quad a'x + b'y = 0$$

  avec $a' \wedge b' = 1$, dont les solutions sont $x = kb'$, $y = -ka'$, $k \in \mathbf{Z}$.

Résolution d'un système de congruence. Considérons d'abord un système à deux lignes de la forme :

$$(S) \begin{cases} x \equiv a_1 \mod n_1 \\ x \equiv a_2 \mod n_2 \end{cases}$$

Autrement dit on cherche s'il existe $x, k_1, k_2 \in \mathbf{Z}$ tel que

$$\begin{cases} x = a_1 + k_1 n_1 \\ x = a_2 + k_2 n_2 \end{cases}$$

Supposons que x, k_1, k_2 soit une solution. Alors par différence on obtient

$$k_1 n_1 - k_2 n_2 = a_2 - a_1$$

Soit $d \geq 0$ le PGCD de n_1 et n_2. Si $a_2 - a_1$ n'est pas un multiple de d, une telle relation est impossible.

Si par contre $a_2 - a_1$ est un multiple de d (c'est toujours le cas si $d = 1$), on peut partir d'une relation de Bezout

$$un_1 + vn_2 = d$$

puis multiplier par l'entier $\frac{a_2 - a_1}{d}$ pour obtenir k_1 et k_2 vérifiant une relation de la forme

$$k_1 n_1 - k_2 n_2 = a_2 - a_1.$$

On obtient ainsi une solution particulière du système (S).

On trouve alors toutes les solutions du système en ajoutant à cette solution particulière les solutions du système homogène

$$(S_0) \begin{cases} x \equiv 0 \mod n_1 \\ x \equiv 0 \mod n_2 \end{cases}$$

qui sont exactement les multiples de $\mathrm{PPCM}(n_1, n_2)$.

Pour résumer la discussion précédente, voici deux exemples d'énoncés possibles :

Proposition 17. *Considérons un système de congruence de la forme*

$$(S)\begin{cases} x \equiv & a_1 \mod n_1 \\ x \equiv & a_2 \mod n_2 \end{cases}$$

Si $n_1 \wedge n_2 = 1$, alors ce système admet une infinité de solutions, qui sont de la forme $x_0 + kn_1n_2$, $k \in \mathbf{Z}$, et x_0 une solution particulière.

Proposition 18. *Considérons un système de congruence de la forme*

$$(S)\begin{cases} x \equiv & a_1 \mod n_1 \\ x \equiv & a_2 \mod n_2 \end{cases}$$

Si (S) admet une solution, alors il en admet une infinité, qui sont de la forme $x_0 + kn_1n_2$, $k \in \mathbf{Z}$, et x_0 une solution particulière.

Remarque 19. L'énoncé ne précise pas que la solution x_0 s'obtient en cherchant (via l'algorithme d'Euclide par exemple !) une relation de Bezout, c'est pourtant un point important à savoir mettre en œuvre.

L'énoncé dit qu'on peut remplacer le système (S) de deux lignes par le système équivalent d'une seule ligne $x \equiv x_0 \mod n_1n_2$.

Cela donne un moyen de résoudre un système de congruence à un nombre quelconque de lignes, par récurrence sur le nombre de lignes (voir exemple en td).

Formule générale pour la solution d'un système de congruence.

Proposition 20. *Considérons un système de congruence à r lignes de la forme*

$$(S)\begin{cases} x \equiv & a_1 \mod n_1 \\ & \vdots \\ x \equiv & a_r \mod n_r \end{cases}$$

avec les n_i premiers entre eux deux à deux. Pour tout $i = 1, \ldots, r$, posons $b_i = n_1 \ldots \hat{n}_i \ldots n_r$ (produit des n_k en omettant n_i), et notons c_i un inverse de b_i modulo n_i. Alors

$$x_0 := a_1b_1c_1 + a_2b_2c_2 + \cdots + a_rb_rc_r$$

est une solution du système (S), et les solutions sont les entiers de la forme $x = x_0 + kn_1 \ldots n_r$, $k \in \mathbf{Z}$.

Remarque 21. Avoir une formule pour la solution est séduisant, mais à noter que le calcul des inverses c_i est plus long que la résolution par récurrence sur le nombre de lignes évoquée plus haut. Cette formule devient rentable si l'on doit résoudre un grand nombre de systèmes avec les mêmes n_i (mais des a_i différents) : voir exo Barry Botter...

Résolution de systèmes de congruence sur $\mathbf{K}[X]$. Tout le discours précédent se transpose à l'identique dans le contexte des polynômes : voir exemples en TD.