Algèbre et arithmétique élémentaires

Notes de cours de l'unité d'enseignement LSMA101,
automnes 2005, 2006, 2007

Nicolas Pouyanne

Département de mathématiques
Université de Versailles - Saint-Quentin
45, avenue des Etats-Unis
78035 Versailles cedex

pouyanne@math.uvsq.fr

Table des matières

1 Algorithme de division euclidienne des polynômes

1- Exemple de division euclidienne dans $\mathbb{N}$: on effectue au tableau 472 501 : 81 en posant la division comme à l'Ecole élémentaire.

2- Un polynôme à coefficients dans $\mathbb{R}$ est une expression de la forme $a_0 + a_1X + \cdots + a_dX^d$ où $d \in \mathbb{N}$ et $a_i \in \mathbb{R}$ pour tout i. Le X est appelé l'**indéterminée** ; on lui donnera un sens précis plus tard. Pour les règles de calcul, penser aux fonctions polynomiales $x \mapsto a_0 + a_1x + \cdots + a_dx^d$. Les coefficients peuvent aussi être pris dans $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Z}$, ou ...

3- L'algorithme de division euclidienne des polynômes. On pose au tableau les divisions suivantes.

Exemple 1 : $X^5 + 2X^4 + 1 = (X^2 + 4X - 1)(X^3 - 2X^2 + 9X - 38) + 161X - 37$, vocabulaire dividende, diviseur, quotient, reste ; degré du reste $<$ degré du diviseur.

Exemple 2 : $A = 3X^3 + 2X^2 - 1$, $B = 5X^2 + 4$. On trouve $A = B \times (\frac{3}{5}X + \frac{2}{5}) - \frac{12}{5}X - \frac{13}{5}$. Si $Q = \frac{3}{5}X + \frac{2}{5}$ et $R = -\frac{12}{5}X - \frac{13}{5}$, on obtient $A = BQ + R$ avec $1 = \deg(R) < \deg(B) = 2$.

S'entraîner, savoir faire l'algorithme.

A et B étant deux polynômes donnés, $B \neq 0$, l'algorithme calcule deux polynômes Q et R tels que

$$\begin{cases} A = BQ + R \\ R = 0 \text{ ou } \deg(R) < \deg(B). \end{cases}$$

Remarque : ce qu'on voit sur l'algorithme, c'est que si $A, B \in \mathbb{R}[X]$, alors $Q, R \in \mathbb{R}[X]$. Idem pour $\mathbb{Q}[X]$. En revanche, $A, B \in \mathbb{Z}[X] \not\Longrightarrow Q, R \in \mathbb{Z}[X]$ comme le montre l'exemple 2 (seulement $\mathbb{Q}[X]$ à l'arrivée).

Le premier cours portera sur les polynômes. On utilisera la division euclidienne, outil fondamental pour l'arithmétique des polynômes.

2 Signes $\sum$ et $\prod$

Outils de notation (apprendre l'alphabet grec !).

Si $u_0, \dots, u_d$ sont des nombres, on note la somme et le produit des u_k respectivement

$$u_0 + \cdots + u_d = \sum_{k=0}^{d} u_k = \sum_{0 \le k \le d} u_k$$

$$u_0 \times \cdots \times u_d = \prod_{k=0}^{d} u_k = \prod_{0 \le k \le d} u_k.$$

On note aussi $\sum_{0 \le k \le d} u_k$, $\sum_{k,\ 0 \le k \le d} u_k$, $\sum_{\{k,\ 0 \le k \le d\}} u_k$, $\sum_{0 \le w \le d} u_w$ (n'importe quelle lettre ou n'importe quel symbole à la place de k).

Exemple 1 (lycée). *Si x est un réel différent de 0 et 1 et si $n \ge 1$ est un entier, alors* $\sum_{j=0}^{n} x^j = \frac{1-x^{n+1}}{1-x}$(suite géométrique ; pourquoi exclure 0 et 1 ?).

Faire au tableau une preuve en détail (trop de détails, le dire) sur deux colonnes, l'une avec des notations condensées, l'autre avec les mêmes expressions utilisant des pointillés :

$$\begin{array}{c|c} (1-x) \times \left(\sum_{j=0}^{n} x^j\right) & (1-x)(1+x+\cdots+x^n) \\ = \left(\sum_{j=0}^{n} x^j\right) - x\left(\sum_{j=0}^{n} x^j\right) & = (1+x+\cdots+x^n) - x(1+x+\cdots+x^n) \\ \cdots & \cdots \end{array}$$

Autre rédaction moins détaillée mais suffisante de la preuve :

$$(1-x)\left(\sum_{j=0}^{n} x^j\right) = \sum_{j=0}^{n} x^j - \sum_{j=1}^{n+1} x^j = 1 - x^{n+1}.$$

Exemple 2 (polynômes). Si $a_0, \dots, a_d \in \mathbb{R}$, avec la convention $X^0 = 1$, on a $\sum_{k=0}^{d} a_k X^k = a_0 + a_1 X + \cdots + a_d X^d$.

Autre notation : on sous-entend $a_{d+1} = \cdots = 0$ et on note $\sum_{k=0}^{d} a_k X^k = \sum_{k \ge 0} a_k X^k$ (il y a une infinité d'indices mais seul un nombre fini de termes sont non nuls : la somme est finie. Elle a un sens).

Exemple 3 (au tableau ou en exercice). Si n est un entier naturel,

$$\sum_{\{j,\ 0 \le j \le n,\ j \text{ pair}\}} x^j = \sum_{k=0}^{\lfloor n/2 \rfloor} x^{2k} = \frac{1 - x^{2(1+\lfloor n/2 \rfloor)}}{1-x^2} = \begin{cases} \frac{1-x^{n+2}}{1-x^2} & \text{si } n \text{ est pair} \\ \frac{1-x^{n+1}}{1-x^2} & \text{si } n \text{ est impair.} \end{cases}$$

Remarque. On convient que la somme sur l'ensemble vide est nulle et que le produit sur l'ensemble vide égale 1 (exercice : justifier).

3 Théorème de récurrence

Exemple de raisonnement par récurrence : *pour tout entier naturel n,*

$$\sum_{q=0}^{n} q^2 = \frac{n(n+1)(2n+1)}{6}.$$

Preuve : on raisonne par récurrence sur n. Si $n = 0$, l'égalité est vraie. Si $n \geq 1$, on suppose l'égalité vraie pour tout entier $\leq n-1$ (hypothèse de récurrence). Alors, $\sum_{q=0}^{n} q^2 = \left(\sum_{q=0}^{n-1} q^2\right) + n^2 = \frac{(n-1)n(2n-1)}{6} + n^2 = \frac{n(n+1)(2n+1)}{6}$, la deuxième égalité étant due à l'hypothèse de récurrence au rang $n-1$. Ainsi, pour tout $n \in \mathbb{N}$, l'égalité est vraie.
[Se préparer à des question sur le $\leq n-1$ de la preuve.]

Autre exemple (reprise) : *si $x \neq 0$, $(1-x)\left(\sum_{k=0}^{n} x^k\right) = 1 - x^{n+1}$ (pourquoi enlever 0 ?).*

C'est vrai si $n = 0$. Si $n \geq 1$, $(1-x)\left(\sum_{k=0}^{n-1} x^k + x^n\right) = 1 - x^n + (1-x)x^n = 1 - x^{n+1}$, la première égalité étant due à l'hypothèse de récurrence au rang $n-1$.
[Noter que ce qui est en jeu, au fond, c'est la définition par récurrence du signe $\sum_{k=0}^{n}$.]

Théorème de récurrence *Soit $E \subseteq \mathbb{N}$ et soit $n_0 \in E$. Si $\forall n \geq n_0$, $n \in E \Longrightarrow n+1 \in E$, alors $\forall n \geq n_0$, $n \in E$.*

Conséquence du théorème : "*raisonnement par récurrence*". Pour chaque $n \in \mathbb{N}$, soit $\mathcal{P}(n)$ une assertion. L'application du théorème de récurrence à l'ensemble $E = \{n \in \mathbb{N},\ \mathcal{P}(n) \text{ est vraie}\}$ conduit à l'implication

$$\left(\begin{array}{l} \mathcal{P}(n_0) \text{ est vraie} \\ \text{et } \forall n \geq n_0,\ (\mathcal{P}(n) \Longrightarrow \mathcal{P}(n+1)) \text{ est vraie} \end{array}\right) \Longrightarrow \forall n \geq n_0,\ \mathcal{P}(n) \text{ est vraie}$$

qui constitue le fondement du "raisonnement par récurrence".

Preuve du théorème de récurrence : soit $F = \{n \geq n_0,\ n \notin E\}$. On suppose que $F \neq \emptyset$. Soit alors $m = \min F$ (commentaire sur l'existence de ce minimum). On a $m \geq n_0$ (car $m \in F$) et $m \neq n_0$ (car $n_0 \notin F$) ; donc $m - 1 \geq n_0$. En outre, $m - 1 \notin F$ puisque m est le minimum. Ainsi, $m - 1 \in E$. D'après l'hypothèse du théorème, il vient alors $m = (m-1)+1 \in E$ ce qui est impossible puisque $m \in F$. L'hypothèse $F \neq \emptyset$ ne tient pas ; d'où $F = \emptyset$, ce qu'il fallait démontrer.
[NB : on a fait un raisonnement "par l'absurde"]

Voir dans la littérature (ou en TD) les multiples variantes du théorème de récurrence et du raisonnement qui en découle (récurrence "forte", notamment).

4 Polynômes à une indéterminée

4.1 Définition des polynômes

Définition Un *polynôme* à coefficients complexes est une suite presque nulle $(a_0, a_1, \dots)$ de nombres complexes (*i.e.* $\exists N,\ \forall n \geq N,\ a_n = 0$).

On considérera d'autres coefficients : $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, ou plus généralement un *anneau commutatif* (commentaire : opération sur des nombres, des objets, structures algébriques, on verra plus tard).

Opération sur les polynômes

- Somme : $(a_0, a_1, \dots) + (b_0, b_1, \dots) = (a_0 + b_0, a_1 + b_1, \dots)$.
- Produit externe : $x.(a_0, a_1, \dots) = (xa_0, xa_1, \dots)$.
- Produit interne : $(a_0, a_1, \dots) \times (b_0, b_1, \dots) = (c_0, c_1, \dots)$ où

$$\forall n \in \mathbb{N},\ c_n = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{p+q=n} a_p b_q.$$

Ces opérations sont définies de telle sorte qu'elles rendent opératoire la notation suivante, que l'on adopte, dans laquelle le symbole X se comporte, pour la somme et le produit, comme s'il était un nombre :

$$(a_0, a_1, a_2, \dots) = a_0 + a_1 X + a_2 X^2 + \dots \qquad \text{(somme finie)}.$$

Si $P = (a_0, a_1, a_2, \dots)$ est un polynôme, on note indifféremment $P = P(X) = (a_0, a_1, a_2, \dots) = a_0 + a_1 X + a_2 X^2 + \cdots = \sum_{n\geq 0} a_n X^n$. Avec cette notation, $(a, 0, 0, \dots) = a \in \mathbb{C}$, $(0, 1, 0, \dots) = X$, $(0, 0, 1, 0, \dots) = X^2$, *etc.* et les règles de calcul avec $+$ et $\times$ pour les nombres sont encore valables pour les polynômes (vérification fastidieuse mais immédiate).

On note $\mathbb{C}[X]$ l'ensemble des polynômes à coefficients complexes. On note également $\mathbb{Z}[X]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$, ... Noter que $X = (0, 1, 0, \dots)$ donne un sens précis (et définitif) à l'*indéterminée* X.

Exemple : si $P = (1, 2, 0, 3, 0, \dots) = 1 + 2X + 3X^2$ et $Q = (0, 0, 0, 1, 0, 1, 0, \dots) = X^3 + X^5$, on a $P + Q = (1, 2, 0, 4, 0, 1, 0, \dots) = 1 + 2X + 3X^2 + 4X^3 + X^5$, $PQ = X^3 + 2X^4 + X^5 + 5X^6 + 3X^8$ et $\sqrt{2}P = \sqrt{2} + 2\sqrt{2}X + 3\sqrt{2}X^3$.

Définition Si P est un polynôme non nul, $P = \sum_{n\geq 0} a_n X^n$, le *degré* de P est le plus grand entier n tel que $a_n \neq 0$ (il existe). On note $\deg(P)$. Si $d = \deg(P)$, le *coefficient dominant* de P est a_d. On dit qu'un polynôme est *unitaire* lorsque son coefficient dominant est 1.

Proposition *Soient $P, Q \in \mathbb{C}[X]$. Si $P \neq 0$ et $Q \neq 0$, alors $PQ \neq 0$ et* $\deg(PQ) = \deg(P) + \deg(Q)$.

Preuve : soient $p = \deg(P)$, $q = \deg(Q)$, $P = \sum_{k=0}^{p} p_k X^k$ et $Q = \sum_{k=0}^{q} q_k X^k$. Alors, $PQ = p_p q_q X^{p+q} + \textit{termes de degré} \leq p+q$, ce qui montre le résultat puisque $p_p \neq 0$ *et* $q_q \neq 0 \Longrightarrow p_p q_q \neq 0$.

On verra des exemples de polynômes P et Q non nuls tels que $PQ \neq 0$ et $\deg(PQ) < \deg(P) + \deg(Q)$. Plus tard. Pas à coefficients complexes. Le calcul de la preuve ci-dessus montre qu'on a toujours l'inégalité $\deg(PQ) \leq \deg(P) + \deg(Q)$ si $PQ \neq 0$.

Si $P = \sum_{n \geq 0} a_n X^n \in \mathbb{C}[X]$ et si $x \in \mathbb{C}$, on note $P(x)$ le nombre complexe $P(x) = \sum_{n \geq 0} a_n x^n$, *valeur* de P en x ou *spécialisation* de P en x (rappel : la somme est finie). On notera encore P la *fonction polynomiale* associée à P, définie par $P : \mathbb{C} \to \mathbb{C}$, $x \mapsto P(x)$.

Exercice : faire dessiner par une machine des fonctions polynomiales $\mathbb{R} \to \mathbb{R}$ définies par des polynômes de degrés $0, 1, 2, 3, \ldots$.

Théorème *Si $P \in \mathbb{R}[X]$ et si la fonction polynomiale associée à P s'annule sur un intervalle de $\mathbb{R}$, alors $P = 0$.*

La preuve a été faite en T.D.

4.2 Division euclidienne des polynômes

Dans ce paragraphe, $k = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ (ou un autre "sous-corps" de $\mathbb{C}$). Pas $\mathbb{Z}$, par exemple.

Théorème de division euclidienne des polynômes sur un corps *Pour tous $A, B \in k[X]$, si $B \neq 0$, il existe un unique couple $(Q, R) \in k[X]^2$ tel que*

$$\begin{cases} A = BQ + R, \\ R = 0 \quad \text{ou} \quad \deg(R) \leq \deg(B) - 1. \end{cases}$$

L'algorithme de division euclidienne a été vu. Ce théorème en établit la validité générale, et l'unicité.

Preuve. • Unicité : si $A = BQ + R = BQ' + R'$ avec les conditions sur les restes, alors $B(Q - Q') = R' - R$. Si $Q \neq Q'$, alors $R \neq R'$ et $\deg(R - R') = \deg(B) + \deg(Q - Q') \geq \deg(B)$, ce qui contredit l'hypothèse sur les restes (si R et R' sont non nuls, $\deg(R' - R) \leq \max\{\deg(R), \deg(R')\}$).
• Existence : si $A = 0$, prendre $Q = R = 0$. Si $\deg(B) = 0$ (*i.e.* si B est une constante non nulle), prendre $R = 0$ et $Q = B^{-1}A$. On suppose que $A \neq 0$ et $\deg(B) \geq 1$, et on procède par récurrence sur $n = \deg(A)$. On note $m = \deg(B) \geq 1$, $A = \sum_{k=0}^{n} a_k X^k$ et $B = \sum_{k=0}^{m} b_k X^k$. Si $n \leq m-1$, prendre $Q = 0$ et $R = A$. Si $n \geq m$, on applique l'hypothèse de récurrence au polynôme $A - \frac{a_n}{b_m} X^{n-m} B$ dont le degré est $< n$ (comme dans l'algorithme ; N.B. : $b_m \neq 0$) : soient Q_1 et R_1 tels

que $A - \frac{a_n}{b_m} X^{n-m} B = BQ_1 + R_1$ avec $R_1 = 0$ ou $\deg(R_1) \leq \deg(B) - 1$. L'écriture $A = (\frac{a_n}{b_m} X^{n-m} + Q_1)B + R_1$ prouve le résultat : $Q = \frac{a_n}{b_m} X^{n-m} + Q_1$ et $R = R_1$ conviennent.

Remarques. 1- Attention à $\mathbb{Z}$.
2- Ce théorème a beaucoup de conséquences. Plus tard.

Définition Si $A, B \in k[X]$, on dit que A *divise* B et on note $A|B$ si, et seulement s'il existe $Q \in k[X]$ tel que $B = AQ$.

Cela signifie, lorsque B est non nul, que le reste de la division euclidienne de A par B est nul. On dit aussi que A est un *diviseur* de B, ou que B est un *multiple* de A.

Exemple : dans $\mathbb{R}[X]$, $X^4 + 1 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1)$ (le voir à partir de $X^4 + 1 = (X^2 + 1)^2 - 2X^2$). Ainsi, $X^2 - \sqrt{2}X + 1 | X^4 + 1$ dans $\mathbb{R}[X]$.

4.3 Polynôme dérivé, formule de Taylor

Définition Si $P = \sum_{n \geq 0} a_n X^n \in \mathbb{C}[X]$, le *polynôme dérivé* de P est le polynôme $P' = \sum_{n \geq 1} n a_n X^{n-1} = \sum_{n \geq 0} (n+1) a_{n+1} X^n$. On le note aussi $\frac{dP}{dX}$.

Dérivées d'ordres supérieurs : on note $P^{(0)} = P$, $P^{(1)} = P'$, $P^{(2)} = P'' = \frac{d^2 P}{dX^2}$ et par récurrence $P^{(n)} = \left(P^{(n-1)}\right)' = \frac{d^n P}{dX^n}$ pour tout entier naturel n (*dérivée n-ième* de P).

La définition est formelle (par opposition à la définition de la dérivation en un point d'une fonction de la variable réelle, par exemple). Les règles de dérivation des fonctions polynomiales sont encore valides pour les polynômes (preuves élémentaires à faire en exercice) : $(P+Q)' = P' + Q'$, $(\lambda P)' = \lambda P'$, $(PQ)' = P'Q + PQ'$ et $(P \circ Q)' = P' \circ Q \times Q'$.

Théorème (formule de Taylor pour les polynômes)

1- Si $P \in \mathbb{C}[X]$, alors $P = \sum_{n \geq 0} \frac{1}{n!} P^{(n)}(0) X^n$;

2- Si $P \in \mathbb{C}[X]$ et $a \in \mathbb{C}$, alors

$$P(X + a) = \sum_{n \geq 0} \frac{1}{n!} P^{(n)}(a) X^n \ ;$$

$$P(X) = \sum_{n \geq 0} \frac{1}{n!} P^{(n)}(a) (X - a)^n.$$

Preuve. Une récurrence immédiate montre que pour tous entiers naturels n et p,

$$\frac{d^p}{dX^p}(X^n) = \begin{cases} 0 \text{ si } p \geq n+1 \text{ ;} \\ n(n-1)\dots(n-p+1)X^{n-p} \text{ si } p \leq n. \end{cases}$$

Ainsi, si $P = \sum_n a_n X^n$, a-t-on $P^{(p)}(0) = p!a_p$. D'où le *1-*. Si $a \in \mathbb{C}$, soit $Q \in \mathbb{C}[X]$ défini par $Q(X) = P(X+a)$. On applique *1-* à Q : $Q = \sum_n Q^{(n)}(0)/n!X^n = \sum_n P^{(n)}(a)/n!X^n$ puisque $\forall n$, $Q^{(n)}(X) = P^{(n)}(X+a)$. La dernière égalité est conséquence de la deuxième (substituer $X-a$ à X).

4.4 Polynômes d'interpolation de Lagrange

Question : étant donnés $a_1, a_2, \dots, a_n$ distincts dans $\mathbb{R}$ et $b_1, b_2, \dots, b_n$ dans $\mathbb{R}$, existe-t-il des fonctions polynomiales dont le graphe passe par les points (a_1, b_1), (a_2, b_2), $\dots$, (a_n, b_n) ?

Proposition (théorème d'interpolation de Lagrange)
Soient $a_1, a_2, \dots, a_n \in \mathbb{C}$, distincts, et $b_1, b_2, \dots, b_n \in \mathbb{C}$ ($n \geq 1$). Il existe un unique polynôme P à coefficients complexes tel que
i) $P = 0$ ou $\deg(P) \leq n-1$;
ii) $\forall i \in \{1, \dots, n\}$, $P(a_i) = b_i$.
En outre,

$$P = \sum_{k=1}^{n} b_k \prod_{j \neq k} \frac{X - a_j}{a_k - a_j}.$$

Preuve. Existence : la formule la prouve. Unicité : si P et Q sont solutions de *i)* et *ii)*, alors $P - Q$ est nul ou a un degré $\leq n-1$. Comme $P - Q$ a n racines distinctes (les a_i), on verra plus tard que cela impose que $P - Q = 0$.

Exercice (T.D. ?) : dans la situation de la proposition, trouver tous les polynômes qui vérifient *ii)* (division euclidienne par le produit des $X - a_i$).

5 Arithmétique de $\mathbb{Z}$ et de $k[X]$

Dans tout le chapitre, k égale $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ (plus généralement, un *corps commutatif*).

Pour obtenir des énoncés communs, on note $A = \mathbb{Z}$ ou $k[X]$.

5.1 Pgcd, théorème de Bézout

Définition Soient a et b dans A. On dit qu'un élément d de A est *un pgcd* de a et b s'il divise a et b et si tout diviseur commun à a et b divise d.

Autrement dit, $d|a$, $d|b$ et $\forall e \in A$, $(e|a \text{ et } e|b \Longrightarrow e|d)$. Pgcd est une abréviation de "plus grand diviseur commun".

Proposition (association des pgcd)
1- Dans $\mathbb{Z}$, si d_1 et d_2 sont deux pgcd de a et b où $a \neq 0$, alors $d_1 = d_2$ ou $d_1 = -d_2$.
2- Dans $k[X]$, si d_1 et d_2 sont deux pgcd de a et b où $a \neq 0$, alors il existe $c \in k\backslash\{0\}$ tel que $d_1 = cd_2$.

Preuve. $d_1|d_2$ et $d_2|d_1$: soient u et $v \in A$ tels que $d_1 = ud_2$ et $d_2 = vd_1$. Alors, $(1 - uv)d_1 = 0$. Comme $d_1 \neq 0$ (puisque $a \neq 0$), on obtient $uv = 1$. Dans $\mathbb{Z}$, cela implique que $u = \pm 1$; dans $k[X]$, cela impose $\deg(u) = 0$.

NB : un élément x de A est dit *inversible* lorsqu'il existe $y \in A$ tel que $xy = 1$. Les inversibles de $\mathbb{Z}$ sont 1 et -1 ; ceux de $k[X]$ sont les constantes non nulles (polynômes de degré 0). La proposition précédente s'énonce ainsi : deux pgcd sont l'un produit de l'autre par un inversible (on dit qu'ils sont *associés*).

Théorème (principalité de $\mathbb{Z}$ et de $k[X]$) *Soient a et b dans A, non nuls.*
1- a et b admettent un pgcd.
2- Si $d \in A$ est un pgcd de a et b, alors il existe $(u, v) \in A^2$ tel que $au + bv = d$.
3- Si $d \in A$ est un pgcd de a et b, alors l'ensemble des éléments de A de la forme $au + bv$ où $(u, v) \in A^2$ est l'ensemble des multiples de d.

Preuve (l'ingrédient majeur est la division euclidienne dans A).
i) Dans $\mathbb{Z}$. Soit $I = \{ua + vb,\ (u, v) \in A^2\}$ et soit d le minimum de $I \cap \mathbb{N}^*$ (il existe, commentaire). Soient u_0, v_0 dans $\mathbb{Z}$ tels que $d = u_0a + v_0b$.
• On montre que $I = d\mathbb{Z}$ (l'ensemble des multiples de d).
Si $w \in \mathbb{Z}$, $dw = (u_0w)a + (v_0w)b \in I$; donc $d\mathbb{Z} \subseteq I$.
Soit $p = ua + vb \in I$. On fait la division euclidienne de p par d : $p = dq + r$ avec $0 \leq r \leq d - 1$. Alors, $r = p - dq = (u - u_0q)a + (v - v_0q)b \in I \cap \mathbb{N}$. Comme $d = \min(I \cap \mathbb{N}^*)$, nécessairement, $d = 0$. Donc $p \in d\mathbb{Z}$.
• On montre que d est un pgcd de a et b (et on a fini).

Comme d divise tout élément de I, il divise a et b qui sont dans I. Si e divise a et b, il divise $d = au_0 + bv_0$. Et voilà.
ii) Dans $k[X]$: exercice, la preuve est semblable. Prendre pour d un polynôme non nul de degré minimum dans I (s'assurer que cela existe).

Définition Si a et b sont dans $\mathbb{Z} \setminus \{0\}$, **le** pgcd de a et b est l'unique pgcd strictement positif de a et b. Si a et b sont dans $k[X] \setminus \{0\}$, **le** pgcd de a et b est l'unique pgcd unitaire de a et b. On note $\text{pgcd}(a, b)$ ou $a \wedge b$ dans les deux cas.

Définition a et b dans A sont dits *étrangers* ou *premiers entre eux* lorsqu'ils n'ont pas de diviseur commun non inversible,
i.e. $\forall u \in A,\ u|a \text{ et } u|b \Longrightarrow u \text{ est inversible.}$
Autrement dit, a et b sont étrangers si, et seulement si $\text{pgcd}(a, b) = 1$.

Théorème de Bézout *Soient a et b dans A.*
a et b sont étrangers si, et seulement s'il existe $(u, v) \in A^2$ tel que $au + bv = 1$.

Remarque. Cela implique aussi que $a \wedge v = u \wedge b = u \wedge v = 1$.

Preuve. ($\Longrightarrow$) est conséquence directe du théorème précédent (*2-*).
($\Longleftarrow$) : si $1 = au + bv$, grâce au *3-* du théorème précédent, on sait que 1 est multiple de tout pgcd de a et b. Donc $\text{pgcd}(a, b) = 1$.

Algorithme d'Euclide

Si a et b sont dans A, l'algorithme permet de calculer le pgcd de a et b et de trouver des éléments u et v de A tels que $\text{pgcd}(a, b) = au + bv$ (on appellera u et v des *coefficients de Bézout*). On suppose a et b non nuls (!).

• Calcul du pgcd. On effectue une suite de divisions euclidiennes :
de a par b : $a = bq_0 + r_0$, avec condition sur les restes ;
de b par r_0 : $b = r_0q_1 + r_1$, avec condition sur les restes ;
de r_0 par r_1 : $r_0 = r_1q_2 + r_2$, avec condition sur les restes ;
d'une manière générale, de r_k par r_{k+1} : $r_k = r_{k+1}q_{k+2} + r_{k+2}$, avec condition sur les restes ; en terme algorithmique, tant que le reste est non nul, on effectue la division suivante.

Dans $\mathbb{Z}$, $b > r_0 > r_1 > \cdots > r_k > r_{k+1} > \cdots \geq 0$. Dans $k[X]$, $r_0 = 0$ ou $\deg(r_0) < \deg(b)$ et plus généralement $r_{k+1} = 0$ ou $\deg(r_{k+1}) < \deg(r_k)$, pour tout k. Dans les deux cas, la "suite" $(r_k)_k$ s'arrête lorsqu'un premier reste r_p est nul, *i.e.* lorsque $r_{p-2} = r_{p-1}q_p$.

Lemme *x, y, z, t dans A tels que $x = yz + t$. Alors* $\text{pgcd}(x, y) = \text{pgcd}(y, t)$.

Preuve. Si $d|x$ et $d|y$, alors $d|t = x - yz$; donc $d|\,\text{pgcd}(y, t)$. Inversement, si $d|y$ et $d|t$, alors $d|x$; donc $d|\,\text{pgcd}(x, y)$. Ainsi, $\text{pgcd}(y, t)$ et $\text{pgcd}(x, y)$ se divisent-ils

l'un l'autre : comme ils sont positifs (dans $\mathbb{Z}$) ou unitaires (dans $k[X]$), ces pcgd sont égaux.

Dans l'algorithme, on a ainsi les égalités successives $\text{pgcd}(a,b) = \text{pgcd}(b,r_0) = \text{pgcd}(r_0,r_1) = \cdots = \text{pgcd}(r_{p-2},r_{p-1})$; comme $r_{p-2} = r_{p-1}q_p$, ce dernier pgcd est associé à r_{p-1}.

Conclusion : *dans la suite des divisions euclidiennes de l'algorithme d'Euclide, le dernier reste non nul r_{p-1} est un pgcd de a et b.*

• Calcul de coefficients de Bézout. On note $d = r_{p-1}$ (un pgcd de a et b). On "remonte" l'algorithme :

$$\begin{aligned} d = r_{p-1} &= r_{p-3} - r_{p-2}q_{p-1} \\ &= r_{p-3} - q_{p-1}(r_{p-4} - r_{p-3}q_{p-2}) = (1 + q_{p-1}q_{p-2})r_{p-3} - q_{p-1}r_{p-4} \\ &= \cdots \end{aligned}$$

Exemple (dans $\mathbb{Z}$) : 537 et 72. La suite des divisions euclidiennes est $537 = 72 \times 7 + 33$; $72 = 33 \times 2 + 6$; $33 = 6 \times 5 + 3$; $6 = 3 \times 2$. Le pgcd de 537 et 72 est donc 3 (cette méthode de calcul pour des petits nombres n'est pas forcément la mieux conseillée ; voir T.D.). On remonte l'algorithme : $3 = 33 - 6 \times 5 = 33 - 5 \times (72 - 2 \times 33) = 11 \times 33 - 5 \times 72 = 11(537 - 7 \times 72) - 5 \times 72 = 11 \times 537 - 82 \times 72$.

Exercice : combien y a-t-il de (u,v) tels que $a \wedge b = au + bv$?

5.2 Théorème de Gauss, décomposition en produit d'irréductibles

Définition $a \in A$ est dit *irréductible* lorsque a n'est ni inversible ni le produit de deux non inversibles.

Deux formulations équivalentes : i) les diviseurs de a sont les inversibles et les au où u est inversible ; ii) a n'est pas inversible et pour tous u, v de A, ($a = uv \Longrightarrow$ u est inversible ou v est inversible).

Exemples. Dans $\mathbb{Z}$, 3, -7, 11. Dans $k[X]$, tous les polynômes de degré un (exo). Dans $\mathbb{R}[X]$, $X^2 + 1$, $X^2 + X + 1$ (exo). Dans $\mathbb{Q}[X]$, $X^2 - 2$, $X^4 + 1$ (exo).

Définition Un nombre $p \in \mathbb{Z}$ est dit *premier* si, et seulement si p est irréductible et > 0.

Le début de la liste : $2, 3, 5, 7, 11, 13, 17, \ldots$.

Théorème de Gauss *Soient a, b et c dans A. Si $a|bc$ et si a est premier avec b alors $a|c$.*

Preuve (l'ingrédient est le théorème de Bézout). Soient u et v dans A tels que $1 = au + bv$. Soit $d \in A$ tel que $bc = ad$. Alors, $c = auc + vad = a(uc + vd) \in a\mathbb{Z}$.

Attention à l'hypothèse : $6|4 \times 3$ mais $6 \not| 4$ et $6 \not| 3$. De même, $X^2|X(X^2+X)$ mais $X^2 \not| X$ et $X^2 \not| X^2 + X$.

Corollaire (lemme d'Euclide) *Soient a, b et p dans A. On suppose que p est irréductible. Dans ces conditions, si $p|ab$, alors $p|a$ ou $p|b$.*

Preuve. Puisque $p \not| a$ et p est irréductible, $a \wedge p = 1$ (les diviseurs de p sont les u et les up où u est inversible). On applique le théorème de Gauss : $p|b$.

Théorème de factorialité de $\mathbb{Z}$ et $k[X]$

1- Dans $\mathbb{Z}$: tout nombre entier $a \in \mathbb{Z}$ différent de 0, 1 et -1 s'écrit sous la forme $a = up_1p_2 \dots p_r$ où $u \in \{-1, 1\}$ et où les p_i sont des nombres premiers. A l'ordre près des facteurs p_i, cette décomposition est unique.

2- Dans $k[X]$: tout polynôme $a \in k[X]$ non nul et non inversible (i.e. de degré ≥ 1) s'écrit sous la forme $a = up_1p_2 \dots p_r$ où $u \in k \setminus \{0\}$ et où les p_i sont des polynômes irréductibles unitaires. A l'ordre près des facteurs p_i, cette décomposition est unique.

Notation : on notera $\mathcal{P}$ la partie de A suivante :

$\mathcal{P}$ est l'ensemble des nombres premiers si $A = \mathbb{Z}$;

$\mathcal{P}$ est l'ensemble des polynômes irréductibles unitaires si $A = k[X]$.

Preuve (l'ingrédient, pour l'unicité, est le lemme d'Euclide (ou le théorème de Gauss)).

• Unicité : si $a = up_1 \dots p_r$, alors u est le signe de a (cas de $\mathbb{Z}$) ou le coefficient dominant de a (cas de $k[X]$) ; le u est donc unique. Supposons que $p_1 \dots p_r = q_1 \dots q_s$ où les p_i et les q_i sont dans $\mathcal{P}$. Quitte à simplifier par les facteurs communs, on peut supposer que $p_i \neq q_j$ pour tout (i, j). Or $p_1|q_1 \dots q_s$ et p_1 est irréductible. D'après le lemme d'Euclide, soit $j \in \{1, \dots, s\}$ tel que $p_1|q_j$ (récurrence sur s). Comme p_1 et q_j sont dans $\mathcal{P}$, cela impose $p_1 = q_j$. L'hypothèse $p_1 \dots p_r = q_1 \dots q_s$ avec $p_i \neq q_j$ pour tout (i, j) ne tient pas.

• Existence. 1- Cas de $\mathbb{Z}$. Il suffit de le montrer pour $a \geq 2$; on procède par récurrence sur a. Si $a = 2$, on prend $p_1 = a$ et $r = 1$. Si $a \geq 3$, ou bien a est irréductible et donc premier, ou bien il existe b et c dans $\{2, \dots, c-1\}$ tels que $a = bc$ et on applique l'hypothèse de récurrence à b et c.

2- Cas de $k[X]$. Il suffit de le montrer pour a unitaire. Le raisonnement est identique, par récurrence sur le degré de a.

Corollaire *Tout élément non nul a de A s'écrit de manière unique sous la forme*

$$a = u \prod_{p \in \mathcal{P}} p^{a_p}$$

où u est inversible et où la suite $(a_p)_p$ est une suite presque nulle d'entiers naturels.

Preuve. Regrouper les termes de $a = p_1 \dots p_r$.

Notation. Si $a \neq 0$ et $p \in \mathcal{P}$, on appelle l'entier naturel a_p du corollaire la *p-valuation* de a. On notera $a_p = v_p(a)$. Ainsi, tout $a \in A \setminus \{0\}$ s'écrit sous la forme

$$a = u \prod_{p \in \mathcal{P}} p^{v_p(a)}$$

où u est inversible.

Exemple. $v_3(18) = 2$, $v_5(18) = 0$, $v_{X-1}((X^2-1)^2(X^3-1)) = 3$.

Proposition *Soient a, $b \in A$, non nuls.*

1- *$a|b$ si, et seulement si $\forall p \in \mathcal{P}$, $v_p(a) \leq v_p(b)$.*

2- $\operatorname{pgcd}(a,b) = \prod_{p \in \mathcal{P}} p^{\min\{v_p(a), v_p(b)\}}$.

Preuve. 1- Si $ac = b$ alors $v_p(a) = v_p(b) - v_p(c) \leq v_p(b)$, pour tout p. Inversement, si $v_p(a) \leq v_p(b)$ pour tout p, soit c défini par $c = \prod_{p \in \mathcal{P}} p^{v_p(b) - v_p(a)}$ (il est bien défini puisque les exposants sont positifs et presque tout nuls); alors ac et b sont associés puisqu'ils ont les mêmes valuations (unicité du théorème de factorialité). 2- Soit $d = \prod_{p \in \mathcal{P}} p^{\min\{v_p(a), v_p(b)\}}$, bien défini car la suite des exposants est positive et presque nulle. Comme d est positif ($\mathbb{Z}$) ou unitaire ($k[X]$), il suffit de montrer que d est *un* pgcd de a et b. Pour tout $p \in \mathcal{P}$, $\min\{v_p(a), v_p(b)\} \leq v_p(a)$; donc $d|a$. De même, $d|b$. Enfin si e est un diviseur commun à a et b alors pour tout $p \in \mathcal{P}$, $v_p(e) \leq v_p(a)$ et $v_p(e) \leq v_p(b)$, d'où $v_p(e) \leq v_p(d)$; ainsi, $e|d$. On a montré que $d = a \wedge b$.

Exercice : a et b non nuls. Montrer que a et b sont associés si, et seulement si $v_p(a) = v_p(b)$ pour tout $p \in \mathcal{P}$.

Définition a, $b \in A \setminus \{0\}$. Un *ppcm (plus petit multiple commun)* de a et b est un élément m de A tel que $a|m$, $b|m$ et $\forall n \in A$, ($a|n$ *et* $b|n \Longrightarrow m|n$).

Autrement dit, m est multiple de a et b, et divise tout multiple commun à a et b.

Proposition *Soient a et b dans A, non nuls.*

1- $\prod_{p\in\mathcal{P}} p^{\max\{v_p(a),v_p(b)\}}$ *est un ppcm de* a *et* b*. On le note* $\mathrm{ppcm}(a,b)$ *ou* $a\vee b$*. On dit que c'est* **le** *ppcm de* a *et* b*.*
2- Tout ppcm de a *et* b *est associé à* $\mathrm{ppcm}(a,b)$*.*
3- Il existe un unique $u\in A$*, inversible, tel que* $ab = u\,\mathrm{pgcd}(a,b)\,\mathrm{ppcm}(a,b)$*.*

Preuve. 1- Soit $m = \prod_{p\in\mathcal{P}} p^{\max\{v_p(a),v_p(b)\}}$ (bien défini). D'après la proposition précédente, m est multiple de a et b. Si n est multiple commun à a et b, alors pour tout $p\in\mathcal{P}$, $v_p(n)\geq v_p(a)$ et $v_p(n)\geq v_p(b)$, d'où $v_p(n)\geq v_p(m)$. Ainsi, m divise-t-il n.
2- Il suffit de montrer que tous les ppcm de a et b sont associés. Si m et m' sont deux ppcm de a et b, soient u et v tels que $m = um'$ et $m' = vm$. Alors, $1 = uv$: u et v sont inversibles.
3- Pour tout $p\in\mathcal{P}$, $v_p(a)+v_p(b) = \max\{v_p(a),v_p(b)\}+\min\{v_p(a),v_p(b)\}$, c'est-à-dire $v_p(ab) = v_p(\mathrm{pgcd}(a,b)\,\mathrm{ppcm}(a,b))$. D'où le résultat : ab et $\mathrm{pgcd}(a,b)\,\mathrm{ppcm}(a,b)$ sont associés.

Proposition *Soient* a*,* b *et* c *dans* A*. Si* $a|c$ *et* $b|c$ *et si* a *et* b *sont étrangers, alors* $ab|c$*.*

Preuve. Dans ces conditions, c est multiple du ppcm de a et b qui est ab puisque a et b sont premiers entre eux.

Proposition *1- Il existe une infinité de nombres premiers.*
2- Il existe une infinité de polynômes irréductibles unitaires.

Preuve (Euclide). On veut montrer que $\mathcal{P}$ est infini. On suppose que $\mathcal{P} = \{p_1,\dots,p_n\}$ est fini. Soit alors $a = 1+\prod_{1\leq k\leq n} p_k$ et soit $p\in\mathcal{P}$ un diviseur de a. Comme aucun des p_k ne divise a, $p\notin\{p_1,\dots,p_n\}$, ce qui contredit le fait que $\mathcal{P} = \{p_1,\dots,p_n\}$: l'hypothèse $\mathcal{P}$ est fini ne tient pas.

5.3 L'équation diophantienne linéaire

Etant donnés a, b, $c\in\mathbb{Z}$ (ou $k[X]$), il s'agit de déterminer tous les $(x,y)\in\mathbb{Z}^2$ (ou $k[X]^2$) tels que $ax+by = c$. On supposera a et b non tous les deux nuls.

Premier cas : $c = 0$.

Si $a' = a/a\wedge b$ et $b' = b/a\wedge b$ (ce sont des entiers), a' et b' sont étrangers et l'équation équivaut à $a'x+b'y = 0$. Supposons que (x,y) soit solution. Alors $b'|a'x$; comme $a'\wedge b' = 1$, cela impose que $b'|x$ d'après le théorème de Gauss. Soit $t\in\mathbb{Z}$ tel que $x = tb'$. Alors, $y = -ta'$. Par ailleurs, pour tout entier t, $(x,y) = (tb',-ta')$ est solution.

Conclusion : soit $(a,b)\in\mathbb{Z}^2\backslash\{0\}$. Alors, pour tout couple d'entiers (x,y), $ax+by =$

0 si, et seulement s'il existe $t \in \mathbb{Z}$ tel que $(x, y) = (ta/a \wedge b, -tb/a \wedge b)$. Autrement dit, l'ensemble des solutions de $ax + by = 0$ est $\mathbb{Z}(a/a \wedge b, -b/a \wedge b)$.

Second cas : $c \neq 0$.

• S'il existe $(x, y) \in \mathbb{Z}^2$ tel que $ax + by = c$, alors c est multiple du pgcd de a et b (théorème de principalité). Ainsi, si $\text{pgcd}(a, b) \not| c$, l'équation $ax + by = c$ n'a-t-elle pas de solution.

• On suppose que $\text{pgcd}(a, b)|c$ et on note $a' = a/a \wedge b$, $b' = b/a \wedge b$ et $c' = c/a \wedge b$ (ce sont des entiers). L'équation équivaut à $a'x + b'y = c'$, avec $a' \wedge b' = 1$. On bézoute : soient u et $v \in \mathbb{Z}$ tels que $1 = a'u + b'v$. Alors, $c' = a'(uc') + b'(vc')$: le couple $(x_0, y_0) = (uc', vc')$ est solution. Par ailleurs, si (x, y) est une (autre) solution, alors $a'(x - x_0) + b'(y - y_0) = 0$. D'après le premier cas, $(x - x_0, y - y_0) \in \mathbb{Z}(b' - a')$. Par ailleurs, pour tout $t \in \mathbb{Z}$, $(x_0 + tb', y_0 - ta')$ est solution de l'équation initiale.

Conclusion : soit $(a, b) \in \mathbb{Z}^2 \setminus \{0\}$ et $c \in \mathbb{Z}$. On considère l'équation $ax + by = c$.

i) Si $a \wedge b \not| c$, l'équation n'a pas de solution en nombres entiers.

ii) Si $a \wedge b | c$, on calcule une solution particulière (x_0, y_0) à l'aide d'une relation de Bézout entre a et b. L'ensemble des solutions est alors

$$(x_0, y_0) + \mathbb{Z}(\frac{b}{a \wedge b}, \frac{-a}{a \wedge b}) = \{(x_0 + t\frac{b}{a \wedge b}, y_0 - t\frac{-a}{a \wedge b}),\ t \in \mathbb{Z}\}.$$

6 L'anneau $\mathbb{Z}/n\mathbb{Z}$

6.1 Congruences

Définition Soit $n \in \mathbb{Z}$. Soient x et $y \in \mathbb{Z}$. On dit que x *est congru à* y *modulo* n (ou que x *égale* y *modulo* n) lorsque n divise $x - y$. On note $x \equiv y\ [n]$ (ou $x \equiv y\ (n)$, ou $x \equiv y\ (\mathrm{mod}\, n)$, ou $x = y\ [n]$, ou ...).

Notation : si $n \in \mathbb{Z}$, on note $n\mathbb{Z} = \{nk,\ k \in \mathbb{Z}\}$ l'ensemble des multiples de n.

Remarques. 1.1- $x \equiv y\ [0]$ équivaut à $x = y$ (!!).
1.2- Pour tous x et y, $x \equiv y\ [1]$ (!!).
1.3- $x \equiv y\ [n] \Longleftrightarrow x \equiv y\ [-n]$.
A cause de ces trois remarques, on ne considérera souvent que le cas $n \geq 2$.
2- Pour tous x et y, $x|y$ équivaut à $y \equiv 0\ [x]$.

Proposition *Soient n, x et $y \in \mathbb{Z}$. Les assertions suivantes sont équivalentes.*
1- $x \equiv y\ [n]$.
2- $x - y \in n\mathbb{Z}$.
3- $\exists k \in \mathbb{Z},\ x - y = nk$.
4- x *et* y *ont le même reste dans la division euclidienne par* n.

Preuve. (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3) : exercice. On suppose $n \geq 1$ (si $n = 0$, rien à dire ; remplacer n par $-n$ si n est négatif). On effectue les divisions euclidiennes par n : $x = na + r$ et $y = nb + s$, avec $0 \leq r, s \leq n - 1$. Alors, $x - y = n(a - b) + r - s$. Si $r = s$ alors $x \equiv y\ [n]$; inversement si $x \equiv y\ [n]$, alors $r - s \in n\mathbb{Z}$. Comme $-(n-1) \leq r - s \leq n - 1$, cela impose $r = s$.

Proposition $n \in \mathbb{N}^*$. *Pour tout $x \in \mathbb{Z}$, il existe un unique $k \in \{0, 1, \ldots, n-1\}$ tel que $x \equiv k\ [n]$. C'est le reste de la division euclidienne de x par n.*

Preuve. Division euclidienne : $x = an + k$, $0 \leq k \leq n - 1$. D'abord, $x \equiv k\ [n]$. Ensuite, si k et $k' \in \{0, 1, \ldots, n-1\}$ sont $\equiv x\ [n]$, alors k et k' ont même reste dans la division euclidienne par n. Ces restes sont respectivement k et k' : $k = k'$.

Proposition (compatibilité de $+$ et $\times$ avec la congruence) *Soient n, x, x', y, y' des entiers relatifs.*
1- Si $x \equiv y\ [n]$ *et* $x' \equiv y'\ [n]$, *alors* $x + x' \equiv y + y'\ [n]$;
2- si $x \equiv y\ [n]$ *et* $x' \equiv y'\ [n]$, *alors* $xx' \equiv yy'\ [n]$;
3- si $x \equiv y\ [n]$, *alors* $\forall k \in \mathbb{N}^*,\ x^k \equiv y^k\ [n]$.

Preuve. On suppose $x \equiv y\ [n]$ et $x' \equiv y'\ [n]$. Soient a et $a' \in \mathbb{Z}$ tels que $x - y = an$ et $x' - y' = a'n$. Alors, $(x + x') - (y + y') = (a - a')n \in n\mathbb{Z}$ et $xx' - yy' = x'(x - y) + y(x' - x) = (ax' - a'y)n \in n\mathbb{Z}$. D'où 1- et 2-. Le 3- se

démontre à partir du 2- par récurrence sur k : si $k = 1$, rien à dire. Si $k \geq 2$, on applique 2- à $x \equiv y$ $[n]$ et $x^{k-1} \equiv y^{k-1}$ $[n]$ (hypothèse de récurrence).

Exemples. 1- $\dots 7 \equiv -8$ [5] ; $7 \equiv -3$ [5] ; $7 \equiv 2$ [5] (le reste de la D.E. de 7 par 5) ; $7 \equiv 7$ [5] ; $7 \equiv 12$ [5] $\dots$

2- $8 \equiv 2$ [6] et $9 \equiv 3$ [6] (et $3 \equiv -3$ [6]). Somme : $17 \equiv 7$ [6] ; produit : $72 \equiv 6$ [6], *i.e.* $72 \equiv 0$ [6]. Attention : notamment, $3 \neq 0$ [6], $2 \neq 0$ [6] mais $2 \times 3 \equiv 0$ [6].

3- Il n'existe pas de nombre x tel que $3x \equiv 1$ [6]. En effet, si un tel x existait, on aurait $2 \times 3 \times x = 2 \times 1$ [6], c'est-à-dire $2 \equiv 0$ [6] ce qui n'est pas [un autre raisonnement consiste à dresser la liste des multiples de 3 modulo 6 ; parmi les nombres de 0 à 5, seuls 0 et 3 y figurent].

4- Critère de divisibilité par 3. Soit $x = \overline{a_1 \dots a_n} = a_n + 10a_{n-1} + \dots + 10^{n-1}a_1 = \sum_{k=1}^{n} a_k 10^{n-k} \in \mathbb{Z}$ (développement décimal), où les a_k sont dans $\{0, \dots, 9\}$.
Alors, $x \equiv a_1 + \dots a_n$ [3] ; en particulier, $3|x$ si, et seulement si $3| \sum_{k=1}^{n} a_k$.
Preuve : $10 \equiv 1$ [3], d'où $x \equiv \sum_{k=1}^{n} a_k 1^{n-k} \equiv \sum_{k=1}^{n} a_k$ [3].

Exercice : trouver un critère de divisibilité par 11 qui soit du même accabit. Quel est le reste de la division euclidienne de 375 097 par 11 ? Idem pour $10^{473} - 7$.

5- **Proposition** *Si p est un nombre premier, alors $\forall k \in \{1, \dots, p-1\}$, $p| \binom{p}{k}$.*

Preuve (déjà vu en T.D.). Le nombre $\binom{p}{k}$ est entier et p divise $k!(p-k)! \binom{p}{k}$ pour tout $k \in \{0, \dots, p\}$ (ce nombre vaut $p!$). Comme p est premier, il est étranger à tous les $k!$ et les $(p-k)!$, $k \in \{1, \dots, p-1\}$. Selon le théorème de Gauss appliqué deux fois, p divise $\binom{p}{k}$.

Conséquence : si x et y sont des entiers et p un nombre premier, en développant $(x+y)^p$ par la formule du binôme, on voit que $\boxed{(x+y)^p \equiv x^p + y^p \ [p]}$.

Par récurrence sur a, on montre ainsi que pour tout entier naturel non nul a et pour tous entiers x et y, $(x+y)^{p^a} \equiv x^{p^a} + y^{p^a}$ $[p]$. En développant $(x+y)^{p^a}$ par la formule du binôme, cela montre la proposition suivante, qui généralise la précédente.
Proposition *Si p est un nombre premier et a un entier naturel non nul, alors $\forall k \in \{1, \dots, p^a - 1\}$, $p| \binom{p^a}{k}$.*
Remarque : essayer de trouver une preuve directe de cette dernière proposition sans l'aide des congruences...

6- Résoudre dans $\mathbb{Z}$ l'équation (E) $13x \equiv 4$ [18] *(commentaire : analogie avec $\mathbb{R}$).*

• On cherche un $u \in \mathbb{Z}$ tel que $13u \equiv 1$ [18] (un *"inverse modulo* 18*"* à 13 ; en existe-t-il ?), *i.e.*tel qu'il existe $v \in \mathbb{Z}$ tel que $13u - 18v = 1$. C'est une relation de Bézout. Comme 18 et 13 sont premiers entre eux, une telle relation existe. L'algorithme d'Euclide permet d'en trouver une ; par exemple $1 = 7 \times 13 - 5 \times 18$. D'où $13 \times 7 \equiv 1$ [18] (7 est inverse de 13 modulo 18).
• Si x est solution de (E), alors $7 \times 13 \times x \equiv 7 \times 4$ [18], ce qui s'écrit aussi $x \equiv 10$ [18]. Par ailleurs, tous les entiers x tels que $x \equiv 10$ [18] sont solutions de (E).
• Ainsi, $13x \equiv 4$ [18] $\iff x \equiv 10$ [18]. L'ensemble des solutions de (E) est $10 + 18\mathbb{Z}$.

6.2 Relation d'équivalence, ensemble quotient

Définition Soit E un ensemble. Une *relation binaire* sur E est une partie $\mathcal{R}$ du produit cartésien $E \times E$. Lorsque $(x, y) \in \mathcal{R}$, on note $x\mathcal{R}y$ et on dit que x *est en relation avec* y.

Exemples de relations binaires.
Sur $\mathbb{R}$, $x \leq y$, *ordre naturel* ($\mathcal{R} = \{(x, y) \in \mathbb{R}^2,\ x \leq y\}$).
Sur $\mathbb{Z}$, l'ordre naturel $x \leq y$ ($\mathcal{R} = \{(x, y) \in \mathbb{Z}^2,\ x \leq y\}$).
Sur $\mathbb{Z}$ encore, la divisibilité $x|y$ ($\mathcal{R} = \{(x, y) \in \mathbb{Z}^2,\ x|y\}$).
Sur $\mathbb{R}^2$, la *colinéarité*, définie par $(x_1, y_1)\mathcal{R}(x_2, y_2) \iff x_1y_2 - x_2y_1 = 0$.
Dans le plan affine euclidien muni d'un repère orthonormé (O, i, j), la relation définie par $M\mathcal{R}N$ si, et seulement s'il existe une rotation r de centre O telle que $r(M) = N$.

Définition Soient E un ensemble et $\mathcal{R}$ une relation binaire sur E.
$\mathcal{R}$ est dite *réflexive* lorsque $\forall x \in E$, $x\mathcal{R}x$.
$\mathcal{R}$ est dite *symétrique* lorsque $\forall (x, y) \in E^2$, $x\mathcal{R}y \implies y\mathcal{R}x$.
[$\mathcal{R}$ est dite *antisymétrique* lorsque $\forall (x, y) \in E^2$, $(x\mathcal{R}y$ *et* $y\mathcal{R}x) \implies x = y$.]
$\mathcal{R}$ est dite *transitive* lorsque $\forall (x, y, z) \in E^3$, $(x\mathcal{R}y$ *et* $y\mathcal{R}z) \implies x\mathcal{R}z$.

Définition Une *relation d'équivalence* est une relation binaire réflexive, symétrique et transitive [dire ce qu'est une relation d'ordre, pour info]. Si $\mathcal{R}$ est une relation d'équivalence, on note souvent $x\mathcal{R}y = x \sim y$.

Exemples de relations d'équivalence.
Sur $\mathbb{Z}$, la congruence modulo n (pour un entier n fixé) $x \sim y \iff x \equiv y$ [n] (exo).
Sur n'importe quel ensemble, l'égalité (!).
Sur $\mathbb{R}$, la relation définie par $x \sim y \iff \exists k \in \mathbb{Z},\ x - y = k$ (exo).
Sur $\mathbb{R}^2$, la relation définie par $(x_1, y_1) \sim (x_2, y_2) \iff \exists k \in \mathbb{R}_+^*,\ (x_2, y_2) = k(x_1, y_1)$ (exo). Cette relation est aussi une relation d'équivalence sur $\mathbb{R}^2 \setminus \{(0, 0)\}$.
Sur $\mathbb{R}^2$, la relation définie par $(x_1, y_1) \sim (x_2, y_2) \iff x_1y_2 = x_2y_1$ (exo).

Définition E un ensemble, $\sim$ une relation d'équivalence sur E. Pour chaque $x \in E$, la *classe d'équivalence de* x est le sous-ensemble $\mathrm{cl}(x) = \{y \in E,\ x \sim y\}$. On note aussi $x^{\cdot}$, ou $\overline{x}$, ou ...

Proposition *E un ensemble, $\sim$ une relation d'équivalence sur E et $x, y \in E$.*
1- $x \sim y \iff \mathrm{cl}(x) = \mathrm{cl}(y)$ *;*
2- $\mathrm{cl}(x) \neq \mathrm{cl}(y) \iff \mathrm{cl}(x) \cap \mathrm{cl}(y) = \emptyset$ *;*
3- E est la réunion de toutes les classes d'équivalence.

Preuve. 1- Si $\mathrm{cl}(x) = \mathrm{cl}(y)$, alors $x \in \mathrm{cl}(y)$ puisque $x \in \mathrm{cl}(x)$; donc $x \sim y$. Inversement, supposons que $x \sim y$. Pour tout $z \in \mathrm{cl}(x)$, $x \sim z$ et comme $x \sim y$ et $\sim$ est transitive, $y \sim z$; ainsi, $\mathrm{cl}(x) \subseteq \mathrm{cl}(y)$. De la même façon, $\mathrm{cl}(y) \subseteq \mathrm{cl}(x)$. Donc $\mathrm{cl}(x) = \mathrm{cl}(y)$.
2- ($\Leftarrow$) est trivial puisqu'une classe est non vide. On suppose que $\mathrm{cl}(x) \cap \mathrm{cl}(y) \neq \emptyset$. Soit alors $z \in \mathrm{cl}(x) \cap \mathrm{cl}(y)$. Alors, $x \sim z$ et $y \sim z$. Donc $x \sim y$. On conclut avec le 1-.
3- Tout élément de E est dans sa propre classe. Donc E contient la réunion de ses classes. Par ailleurs, toute classe est incluse dans E ; donc leur réunion aussi.

[Une *partition* d'un ensemble E est une famille de sous-ensembles $(E_j)_{j \in J}$ qui soient non vides, disjoints ($\forall (j, j') \in J^2,\ j \neq j' \Rightarrow E_j \cap E_{j'} = \emptyset$) et dont la réunion soit E. Les classes d'équivalence forment une partition.]

Corollaire *Soit E un ensemble fini muni d'une relation d'équivalence. Alors, le cardinal de E est la somme des cardinaux de ses classes d'équivalence.*

Preuve. E est l'union disjointe de ses classes.

Définition E un ensemble, $\sim$ une relation d'équivalence sur E. L'ensemble des classes d'équivalence est appelé *ensemble quotient*. On le note $E/\sim$.

Exemples. 1- $E = \mathbb{R}$, $x \sim y \iff x - y \in \mathbb{Z}$. L'application $[0,1[\to \mathbb{R}/\sim$, $x \mapsto \mathrm{cl}(x)$ définit une bijection de $[0,1[$ sur $\mathbb{R}/\sim$. En effet, elle est surjective (si $x \in \mathbb{R}$, $x \sim x - \lfloor x \rfloor \in [0,1[$) et injective (si $x, y \in [0,1[$, $x \sim y \Leftrightarrow x = y$ puisque $\mathbb{Z} \cap [0,1[= \{0\}$).

2- $E = \mathbb{R}^2 \setminus \{(0,0)\}$, $(x,y) \sim (x',y') \iff \exists \lambda > 0,\ (x,y) = \lambda(x',y')$ (exercice : c'est une relation d'équivalence). Soit $S^1 = \{(x,y) \in E,\ x^2 + y^2 = 1\}$, cercle triginométrique. L'application $S^1 \to E/\sim$, $(x,y) \mapsto \mathrm{cl}(x,y)$ est une bijection (exercice).

3- $E = \mathbb{Z}$, muni de la congruence modulo n ($n \geq 1$ un entier fixé). L'application $P : \{0, \ldots n-1\} \to \mathbb{Z}/\sim$, $x \mapsto \mathrm{cl}(x)$ est bijective (exercice). Construction de l'application réciproque : soit $R : \mathbb{Z} \to \{0, \ldots n-1\}$, $x \mapsto R(x)$ où $R(x)$ est le

reste de la division euclidienne de x par n. Si $x \sim y$, alors $R(x) = R(y)$. Ainsi, $\forall x \in \mathbb{Z}$, $\forall y \in \mathrm{cl}(x)$, $R(x) = R(y)$. On peut donc définir $\overline{R} : \mathbb{Z}/\sim \to \{0, \dots n-1\}$, $x \mapsto \overline{R}(x) = R(x)$ ($\overline{R}(x)$ est la valeur commune des $R(y)$, $y \sim x$). Il est alors clair que $P \circ \overline{R} = \mathrm{id}_{\mathbb{Z}/\sim}$ et $\overline{R} \circ P = \mathrm{id}_{\{0,\dots n-1\}}$: $\overline{R}$ est la réciproque de P.

Application injective, surjective, bijective

Définitions Soit $f : E \to F$ une application. On dit que f est *injective* (ou une *injection*) lorsque $\forall (x,y) \in E^2,\ x \neq y \Longrightarrow f(x) \neq f(y)$. On dit que f est *surjective* (ou une *surjection*) lorsque $\forall y \in F,\ \exists x \in E,\ f(x) = y$. On dit que f est *bijective* (ou une *bijection*) lorsque f est injective et surjective.

Propriétés. *Soient $f : E \to F$ et $g : F \to G$ deux applications.*
• *f est injective* $\Longleftrightarrow \forall (x,y) \in E^2,\ f(x) = f(y) \Longrightarrow x = y$.
• *f est surjective* $\Longleftrightarrow \mathrm{im}(f) = F$ *(NB :* $\mathrm{im}(f) = f(E) = \{f(x),\ x \in E\}$*).*
• *f est bijective* $\Longleftrightarrow \exists g : F \to E,\ f \circ g = \mathrm{id}_F$ *et* $g \circ f = \mathrm{id}_E$ *(g est alors unique est est appelée réciproque de f).*
• *f et g injectives* $\Longrightarrow g \circ f$ *injective.*
• *f et g surjectives* $\Longrightarrow g \circ f$ *surjective.*
• *$g \circ f$ injective* $\Longrightarrow f$ *injective.*
• *$g \circ f$ surjective* $\Longrightarrow g$ *surjective.*
• *Si f est bijective, on note f^{-1} sa réciproque. Si f et g sont bijectives, alors $g \circ f$ l'est aussi et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Preuves en exercice.

Exemples. 1- $f_1 : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$ n'est ni injective ni surjective. $f_2 : \mathbb{R} \to \mathbb{R}_+$, $x \mapsto x^2$ est surjective mais pas injective. $f_3 : \mathbb{R}_+ \to \mathbb{R}$, $x \mapsto x^2$ est injective mais pas surjective. $f_4 : \mathbb{R}_+ \to \mathbb{R}_+$, $x \mapsto x^2$ est bijective.
2- Prototype de surjection : $\mathbb{R}^2 \to \mathbb{R}$, $(x,y) \mapsto x$.
Prototype d'injection : $F \to E$, $x \mapsto x$ si F est une partie d'un ensemble E.

Définition E un ensemble et $\sim$ une relation d'équivalence sur E. L'application $\pi : E \to E/\sim$, $x \mapsto \mathrm{cl}(x)$ est appelée *projection canonique* de la relation $\sim$. On dit aussi *surjection canonique* (elle est à l'évidence toujours surjective) ou simplement *application canonique*.

[En T.D., le théorème de factorisation.]

6.3 L'anneau $\mathbb{Z}/n\mathbb{Z}$

Définition Soit $n \in \mathbb{Z} \setminus \{0\}$. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient $\mathbb{Z}/\sim$, où $\sim$ désigne la congruence modulo n. Si $x \in \mathbb{Z}$, on note $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ sa classe

d'équivalence (on parle de sa *classe modulo* n).

Ainsi, $\overline{x} = \{y \in \mathbb{Z},\ x \equiv y\ [n]\}$.

Proposition *Soit $n \geq 1$. $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ a pour cardinal n.*

Preuve. A déjà été vu dans 6.2. On a les bijections réciproques l'une de l'autre $\{0, \ldots, n-1\} \to \mathbb{Z}/n\mathbb{Z}$, $x \mapsto \overline{x}$ (projection canonique) et $\mathbb{Z}/n\mathbb{Z} \to \{0, \ldots, n-1\}$, $\overline{x} \mapsto$ {reste de la division euclidienne de x par n} (cette dernière est bien définie car l'application $x \mapsto$ {reste de la division euclidienne de x par n} est constante sur les classes modulo n).

Exemple : dans $\mathbb{Z}/5\mathbb{Z}$, $\overline{7} = \overline{2}$, $\overline{-6} = \overline{4} = \overline{9}$, $\overline{15} = \overline{0} = \overline{5}$.

Addition et multiplication dans $\mathbb{Z}/n\mathbb{Z}$

Si x, x', y, $y' \in \mathbb{Z}$ vérifient $x \equiv x'\ [n]$ et $y \equiv y'\ [n]$, alors $x + y \equiv x' + y'\ [n]$ et $xy \equiv x'y'\ [n]$ d'après le théorème de compatibilité. Autrement dit, si $\overline{x} = \overline{x}'$ et $\overline{y} = \overline{y}'$, alors $\overline{x+y} = \overline{x'+y'}$ et $\overline{xy} = \overline{x'y'}$.

Cela permet de donner du sens aux **définitions** suivantes, addition et multiplication dans $\mathbb{Z}/n\mathbb{Z}$:

$$\forall \overline{x}, \overline{y} \in \mathbb{Z}/n\mathbb{Z},\ \overline{x} \mathbin{\overline{+}} \overline{y} = \overline{x+y} \ \text{ et } \ \overline{x} \mathbin{\overline{\times}} \overline{y} = \overline{x \times y}.$$

Plus tard, on s'affranchira des $\overline{\cdots}$ sur $+$ et $\times$, et même sur les entiers pour désigner leur classe. Un slogan qui résume le sens donné à ces définitions : les classes de $x + y$ et de xy modulo n ne dépendent que des classes de x et y modulo n.

Proposition *$n \in \mathbb{Z} \setminus \{0\}$. Les classes sont entendues modulo n.*
1- $\forall x, y, z \in \mathbb{Z}$, $\overline{x} \mathbin{\overline{+}} (\overline{y} \mathbin{\overline{+}} \overline{z}) = (\overline{x} \mathbin{\overline{+}} \overline{y}) \mathbin{\overline{+}} \overline{z}$. *On note alors $\overline{x} \mathbin{\overline{+}} \overline{y} \mathbin{\overline{+}} \overline{z}$.*
2- $\forall x \in \mathbb{Z}$, $\overline{x} \mathbin{\overline{+}} \overline{0} = \overline{0} \mathbin{\overline{+}} \overline{x} = \overline{x}$.
3- $\forall x \in \mathbb{Z}$, $\overline{x} \mathbin{\overline{+}} \overline{-x} = \overline{-x} \mathbin{\overline{+}} \overline{x} = \overline{0}$ *; on note alors* $\overline{-x} = \ \overline{-}\ \overline{x}$ *et* $\overline{x} \mathbin{\overline{-}} \overline{y} = \overline{x-y}$.
4- $\forall x, y \in \mathbb{Z}$, $\overline{x} \mathbin{\overline{+}} \overline{y} = \overline{y} \mathbin{\overline{+}} \overline{x}$.
5- $\forall x, y, z \in \mathbb{Z}$, $\overline{x} \mathbin{\overline{\times}} (\overline{y} \mathbin{\overline{\times}} \overline{z}) = (\overline{x} \mathbin{\overline{\times}} \overline{y}) \mathbin{\overline{\times}} \overline{z}$. *On note alors $\overline{x} \mathbin{\overline{\times}} \overline{y} \mathbin{\overline{\times}} \overline{z}$.*
6- $\forall x \in \mathbb{Z}$, $\overline{x} \mathbin{\overline{\times}} \overline{1} = \overline{1} \mathbin{\overline{\times}} \overline{x} = \overline{x}$.
7- $\forall x, y \in \mathbb{Z}$, $\overline{x} \mathbin{\overline{\times}} \overline{y} = \overline{y} \mathbin{\overline{\times}} \overline{x}$.
8- $\forall x, y, z \in \mathbb{Z}$, $\overline{x} \mathbin{\overline{\times}} (\overline{y} \mathbin{\overline{+}} \overline{z}) = (\overline{x} \mathbin{\overline{\times}} \overline{y}) \mathbin{\overline{+}} (\overline{x} \mathbin{\overline{\times}} \overline{z})$.

Preuve. Pas drôle ; en exercice. Par exemple, $\overline{x} \mathbin{\overline{+}} (\overline{y} \mathbin{\overline{+}} \overline{z}) = \overline{x} \mathbin{\overline{+}} \overline{y+z} = \overline{x+y+z} = \overline{x+y} \mathbin{\overline{+}} \overline{z} = (\overline{x} \mathbin{\overline{+}} \overline{y}) \mathbin{\overline{+}} \overline{z}$. Le reste est du même accabit.

Autrement dit, les règles usuelles de l'addition, de la soustraction et de la multiplication sur les nombres entiers sont encore valides dans $\mathbb{Z}/n\mathbb{Z}$.

Référence au polycopié sur groupes et anneaux (et corps). La proposition précédente se traduit ainsi :

Proposition (bis) *Soit n un entier ≥ 2. Pour les lois $\overline{+}$ et $\overline{\times}$ ainsi définies, $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif.*

Remarque : attention aux équations linéaires. Dans $\mathbb{Z}/6\mathbb{Z}$, $\overline{2} \neq \overline{0}$ et $\overline{3} \neq \overline{0}$, mais $\overline{2} \,\overline{\times}\, \overline{3} = \overline{0}$. On note aussi $2 \neq 0$, $3 \neq 0$ mais $2 \times 3 = 0$.
[On dit que l'anneau $\mathbb{Z}/6\mathbb{Z}$ n'est pas *intègre*, et que 2 et 3 sont des *diviseurs de zéro* dans $\mathbb{Z}/6\mathbb{Z}$.]

Définition Soit A un anneau. On dit que $a \in A$ est *inversible* lorsqu'il admet un symétrique pour la multiplication (on dit un *inverse*), *i.e.* lorsqu'il existe $b \in A$ tel que $ab = 1$ et $ba = 1$.

Théorème *Soient n et x dans $\mathbb{Z}$, $n \geq 2$. Alors, $\overline{x}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si* $\text{pgcd}(x, n) = 1$. *Dans ces conditions, l'inverse de $\overline{x}$ dans $\mathbb{Z}/n\mathbb{Z}$ se calcule à l'aide d'une relation de Bézout entre n et x.*

Preuve. ($\Rightarrow$) On suppose que $\overline{x}$ est inversible. Soit $y \in \mathbb{Z}$ tel que $\overline{x}\,\overline{y} = \overline{1}$. Alors, $xy - 1 \in n\mathbb{Z}$: soit $m \in \mathbb{Z}$ tel que $xy - 1 = mn$. Ceci est une relation de Bézout entre n et x : $x \wedge n = 1$.

($\Leftarrow$) On suppose que $x \wedge n = 1$. Soit $xy + mn = 1$ une relation de Bézout entre n et x. Alors $xy \equiv 1\ [n]$, *i.e.* $\overline{x}\,\overline{y} = \overline{1}$ (et $\overline{y}\,\overline{x} = \overline{1}$) dans $\mathbb{Z}/n\mathbb{Z}$: $\overline{x}$ est inversible.

Exemple : $8 \wedge 35 = 1$, donc $\overline{8}$ est inversible dans $\mathbb{Z}/35\mathbb{Z}$. On Bézoute (Euclide) : $1 = 3 \times 35 - 13 \times 8$. Donc $\overline{-13}$ est l'inverse de $\overline{8}$ dans $\mathbb{Z}/35\mathbb{Z}$. Par ailleurs, $\overline{-13} = \overline{22}$, d'où $\overline{22}.\overline{8} = \overline{1}$.

Proposition *Soit $n \geq 2$. Alors, $\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si n est un nombre premier.*

Preuve. ($\Rightarrow$) Si $\mathbb{Z}/n\mathbb{Z}$ est un corps, $\overline{1}, \ldots, \overline{n-1}$ sont tous inversibles dans $\mathbb{Z}/n\mathbb{Z}$. Ainsi n n'a-t-il pas de facteur commun avec $2, \ldots, n-1$, exceptés 1 et -1 : n est premier.

($\Leftarrow$) Si n est premier, alors $\forall k \in \{1, \ldots, n-1\}$, $\text{pgcd}(n, k) = 1$. Donc $\overline{1}, \ldots, \overline{n-1}$ sont inversibles dans $\mathbb{Z}/n\mathbb{Z}$. Comme $\mathbb{Z}/n\mathbb{Z} = \overline{0}, \ldots, \overline{n-1}$, c'est un corps.

Exercice. On a aussi : $\mathbb{Z}/n\mathbb{Z}$ est un anneau intègre si, et seulement si n est un nombre premier.

Remarque. On a ainsi des exemples de corps finis : $\mathbb{Z}/2\mathbb{Z}$ (deux éléments), $\mathbb{Z}/7\mathbb{Z}$, $\mathbb{Z}/97\mathbb{Z}$, ...

6.4 Le théorème des restes chinois

Problème chinois: on se donne m et n, entiers non nuls, et a et b des entiers. Trouver tous les $x \in \mathbb{Z}$ tels que

$$(\text{PC}) \quad \left\{ \begin{array}{l} x \equiv a \ [m] \\ x \equiv b \ [n]. \end{array} \right.$$

• On suppose que x est solution. Soient alors A et B entiers tels que $x = a + Am = b + Bn$. Nécessairement, $a - b = Bn - Am \in \mathbb{Z}m \wedge n$. Ainsi, si $m \wedge n \not| a - b$, (PC) n'a-t-il pas de solution.

• On suppose que $m \wedge n$ divise $a - b$. Soit $a - b = um + vn$ une relation de Bézout (il en existe). Alors, le nombre $x_0 = a - um = b + vn$ est une solution de (PC). Par ailleurs, si x et y sont deux solutions de (PC), alors $x - y$ est multiple commun de m et n, donc de $m \vee n$. Ainsi, l'ensemble des solutions de (PC) est-il $x_0 + \mathbb{Z}m \vee n$.

Conclusion 1- Si $\text{pgcd}(m, n) \not| a - b$, (PC) n'a pas de solution.
2- Si $\text{pgcd}(m, n) | a - b$, on cherche une solution particulière x_0 à l'aide d'une relation de Bézout entre m et n (si $a - b = km \wedge n$ et $m \wedge n = mu + nv$, alors $x_0 = a - kum = b + kvn$ convient). L'ensemble des solutions de (PC) est alors $x_0 + \mathbb{Z}m \vee n$.

Exemple : résoudre dans $\mathbb{Z}$ le système $x \equiv 91 \ [365]$ *et* $x \equiv 23 \ [29]$ (365= cycle solaire, 91= 1er avril ; 29= cycle lunaire, 23= au pif. Commentaires sur "chinois" et sur "restes").

Algorithme d'Euclide : $365 \wedge 29 = 1 = 12 \times 365 - 151 \times 29$. D'où $91 - 23 = 68 = 68 \times 12 \times 365 - 68 \times 151 \times 29 = 816 \times 365 - 10268 \times 29$. On prend $x_0 = 91 - 816 \times 365 = 23 - 10268 \times 29 = -297749$ qui est solution. Comme $365 \vee 29 = 365 \times 29 = 10585$, l'ensemble des solutions est $-297749 + 10585\mathbb{Z} = 9216 + 10585\mathbb{Z}$.

Théorème des restes chinois *Soient a, b, m et n des entiers, avec m et $n \geq 2$.*
1- Le système (PC) admet une solution entière x si, et seulement si le pgcd de m et n divise $a - b$. Dans ces conditions, cette solution est unique modulo le ppcm de m et n (i.e. si x_0 est une solution, alors $\mathcal{S} = x_0 + \mathbb{Z}m \vee n$).
2- En particulier, si m et n sont premiers entre eux, le système (PC) admet toujours une solution, unique modulo mn.

Preuve. Tout est déjà démontré.

Autre expression du TRC

Soient m et $n \geq 2$. Si $x \in \mathbb{Z}$, on note $\overline{x}^m$ et $\overline{x}^n$ les classes de x modulo m et n respectivement. Soit alors

$$\begin{array}{rccc} f: & \mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ & x & \mapsto & (\overline{x}^m, \overline{x}^n) \, . \end{array}$$

Dire que (PC) admet une solution pour tout $(a,b) \in \mathbb{Z}^2$ signifie exactement que f est surjective. On en apporte une autre preuve (sans calcul, non constructive).

Théorème des restes chinois (bis) *Si $m \wedge n = 1$, alors f est surjective et induit un isomorphisme d'anneaux $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.*

Preuve (différente de la précédente).
• f est constante sur les classes modulo mn. On peut ainsi définir $\overline{f} : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ par $\overline{f}(\overline{x}) = f(x)$ puisque $f(x)$ ne dépend que de la classe de x modulo mn.
• $\overline{f}$ est injective. En effet, $\overline{f}(\overline{x}^{mn}) = \overline{f}(\overline{y}^{mn}) \Leftrightarrow f(x) = f(y) \Leftrightarrow x \equiv y\ [m]$ *et* $x \equiv y\ [n] \Leftrightarrow mn|x-y \Leftrightarrow \overline{x}^{mn} = \overline{y}^{mn}$.
• Comme les cardinaux de $\mathbb{Z}/mn\mathbb{Z}$ et de $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont finis et égaux, $\overline{f}$ est également surjective. Donc f aussi (voir le NB ci-dessous).
• f est un homomorphisme d'anneaux pour les lois $(x,y)+(x',y') = (x+x', y+y')$ et $(x,y) \times (x',y') = (xx', yy')$ sur le produit cartésien $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ (loi *d'anneau produit*). Il résulte directement de la définition de l'addition et de la multiplication sur $\mathbb{Z}/n\mathbb{Z}$ que $\overline{f}$ est également un homomorphisme d'anneaux. Ainsi $\overline{f}$ est-il un isomorphisme d'anneaux.

NB : on a utilisé le théorème important suivant.

Théorème *Soient E et F deux ensembles* **finis** *de même cardinal et $f : E \to f$ une application. Il y a équivalence entre*
1- f est injective ;
2- f est surjective ;
3- f est bijective.

Preuve. Exercice, pas si facile. Ou voir la littérature.

7 Polynômes et racines

k est un corps commutatif (par exemple $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$ où p est un nombre premier).

7.1 Racines, multiplicité

Définition Soient $P \in k[X]$ et $a \in k$. On dit que a est racine de P lorsque $P(a) = 0$ (fonction polynomiale).

Proposition *Soient $P \in k[X]$ et $a \in k$. Alors, a est racine de P si, et seulement si $X - a | P$ dans $k[X]$.*

Preuve. Division euclidienne : $P = (X - a)Q + R$ avec $R = 0$ ou $\deg(R) = 0$. Comme R est constant, en substituant, on obtient que $R = P(a)$.

Corollaire *Soit $P \in k[X]$. Si $a_1, \dots a_n \in k$ sont des racines distinctes de P, alors $\prod_{1 \leq k \leq n}(X - a_k)$ divise P.*

Preuve. Par récurrence sur n. Si $n = 1$, c'est la proposition. On suppose $n \geq 2$. Comme les $X - a_k$ sont irréductibles et comme $X - a_n$ ne divise aucun des autres $X - a_k$, les polynômes $X - a_n$ et $\prod_{1 \leq k \leq n-1}(X - a_k)$ sont étrangers. On applique le théorème de Gauss à la situation $X - a_n | P = Q \times \prod_{1 \leq k \leq n-1}(X - a_k)$; cela montre que $X - a_n | Q$, et le résultat.

Corollaire *Soit $P \in k[X]$. On suppose que $P \neq 0$ et que $\deg(P) = n$. Alors, P a au plus n racines distinctes.*

Preuve. On raisonne par l'absurde. On suppose que $a_1, \dots, a_{n+1}$ sont $n+1$ racines distinctes de P. Alors, $\prod_{k=1}^{n+1}(X - a_k)$ divise P. Comme $\deg(P) = n$, l'hypothèse "$n + 1$ racines distinctes" ne tient pas.

Corollaire *On suppose que k est un corps infini et que $P \in k[X]$. Dans ces conditions, si $\forall x \in k$, $P(x) = 0$, alors $P = 0$.*

Preuve. P a une infinité de racines.

Exemples. 1- Dans $\mathbb{Z}/2\mathbb{Z}$, $P = X^2 - X \neq 0$ mais $\forall x \in \mathbb{Z}/2\mathbb{Z}$, $P(x) = 0$.
2- Plus généralement, si p est un nombre premier

$$X^p - X = \prod_{k=0}^{p-1}(X - k) \text{ dans } \mathbb{Z}/p\mathbb{Z}.$$

Ce polynôme non nul définit une fonction polynomiale nulle dans $\mathbb{Z}/p\mathbb{Z}$.

Preuve de la relation : $P = X^p - X$ vérifie $P(0) = 0$ et $P(X-1) = P(X)$. Ainsi, P a-t-il pour racines tous les éléments de $\mathbb{Z}/p\mathbb{Z}$. Donc $\prod_{k=0}^{p-1}(X-k)|P$. Comme ces polynômes sont unitaires et de même degré, ils sont égaux.
[N.B. : le coefficient de X est $(p-1)! = -1$: c'est le théorème de Wilson.]
3- Le corollaire permet de finir la preuve du théorème d'interpolation de Lagrange (partie unicité).
4- Soit $n \in \mathbb{N}^*$. Pour tout $k \in \{0, \dots, n-1\}$, $\exp(2ik\pi/n)$ est racine de $X^n - 1$ dans $\mathbb{C}$, et ces n nombres sont distincts Ainsi, $\prod_{k=0}^{n-1}(X - \exp(2ik\pi/n))$ divise-t-il $X^n - 1$. Ils ont même degré et même coefficient dominant. La factorisation de $X^n - 1$ dans $\mathbb{C}[X]$ est donc

$$X^n - 1 = \prod_{k=0}^{n-1}(X - e^{2ik\pi/n}).$$

Cas $n = 3$: on note $j = \exp(2i\pi/3)$. Factorisation de $X^3 - 1$ sur $\mathbb{C}$: $X^3 - 1 = (X-1)(X-j)(X-j^2)$. En regroupant les facteurs non réels, on obtient la factorisation dans $\mathbb{R}[X]$: $X^3 - 1 = (X-1)(X^2+X+1)$. C'est aussi la factorisation rationnelle.

Cas $n = 4$: $X^4 - 1 = (X-1)(X-i)(X+1)(X+i) = (X-1)(X+1)(X^2+1)$ (factorisation réelle).

Cas $n = 5$: on pose $\omega = \exp(2i\pi/5)$. $X^5 - 1 = (X-1)(X-\omega)(X-\omega^2)(X-\omega^3)(X-\omega^4) = (X-1)(X-e^{2i\pi/5})(X-e^{-2i\pi/5})(X-e^{4i\pi/5})(X-e^{-4i\pi/5}) = (X-1)(X^2 - 2\cos\frac{2\pi}{5}X + 1)(X^2 + 2\cos\frac{2\pi}{5}X + 1)$ (factorisation dans $\mathbb{R}[X]$) $= (X-1)(X^4+X^3+X^2+X+1)$ (factorisation dans $\mathbb{Q}[X]$, on a vu en exercice que $\cos\frac{2\pi}{5} \notin \mathbb{Q}$).

Définition Soient $P \in k[X]$, $a \in k$ et n un entier naturel. On dit que a est racine de P *de multiplicité* n (ou *d'ordre* n) lorsque $(X-a)^n|P$ et $(X-a)^{n+1} \not| P$, *i.e.* lorsque $v_{X-a}(P) = n$ (valuation selon l'irréductible $X - a$).

Exemple : la multiplicité de la racine 1 de $(X^2-1)(X^5-1)^3(X^2+X+1)$ est 4.

Corollaire *Soient $P \in k[X]$, $a \in k$ et n un entier ≥ 1.*
1- Si a est racine d'ordre $\geq n$ de P, alors $P(a) = 0$ et a est racine d'ordre $\geq n-1$ de P'.
2- Si a est racine d'ordre $\geq n$ de P, alors $\forall k \in \{0, \dots, n-1\}$, $P^{(k)}(a) = 0$.
3- Si $k \subseteq \mathbb{C}$, il y a équivalence dans 1- et 2-. En outre, dans ces conditions, a est racine d'ordre n si, et seulement si $\forall k \in \{0, \dots, n-1\}$, $P^{(k)}(a) = 0$ et $P^{(n)}(a) \neq 0$.

Preuve. 1- Division euclidienne de P par $(X-a)^n$: $P = (X-a)^n Q + R$ avec $R = 0$ ou $\deg(R) \leq n-1$. Alors, $P' = (X-a)^{n-1}[nQ + (X-a)Q'] + R'$ est la division euclidienne de P' par $(X-a)^{n-1}$. Si $(X-a)^n|P$ alors $R = 0$; d'où

$R' = 0$ et $(X-a)^{n-1}|P'$. Inversement, si $(X-a)^{n-1}|P'$ et $P(a) = 0$, alors $R' = 0$; dans le cas où $k \subseteq \mathbb{C}$, cela entra^ ne que R est constant et vaut $R = P(a) = 0$, c'est-à-dire que $(X-a)^n|P$.
2- Récurrence sur n.
3- Si $k \subseteq \mathbb{C}$, la formule de Taylor est valide. Ainsi, si $P(a) = P'(a) = \cdots = P^{(n-1)}(a) = 0$, alors $(X-a)^n|P$. Fin de la preuve en exercice (avec la formule de Taylor).

Exemples. 1- $k = \mathbb{Z}/p\mathbb{Z}$ où p est un nombre premier, $P = X^p - 1 = (X-1)^p$ et $a = 1$. Dans cet exemple, 1 est racine de multiplicité p de P. Par ailleurs, comme $P' = 0$, $P^{(k)}(1) = 0$ pour tout $k \geq 0$: il n'y a pas équivalence dans le 2- du théorème si $k = \mathbb{Z}/p\mathbb{Z}$.
2- $(X-1)^3|P = X^7 + 7X^4 - 4X^3 - 3X^6 - 6X^2 + 7X - 2$ car $P(1) = 0$, $P'(1) = 0$ et $P''(1) = 0$ (faire le calcul).

Exercice : toute application $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ est polynomiale.

7.2 Irréductibilité de polynômes

7.2.1 Sur $\mathbb{C}$

Théorème de d'Alembert-Gauss *Tout polynôme non constant de $\mathbb{C}[X]$ admet au moinis une racine.*

Preuve. On l'admet. Toute preuve contient de l'analyse (construction de $\mathbb{R}$).

Corollaire *$P \in \mathbb{C}[X]$ est irréductible si, et seulement si* $\deg(P) = 1$.

Preuve. Si P est constant, il est nul ou inversible, donc réductible. Si $\deg(P) = 1$, alors P est irréductible. Enfin, si $\deg(P) \geq 2$, soit a une racine (complexe) de P. Alors, $P = (X-a)Q$ où $\deg(Q) \geq 1$. Comme Q n'est pas inversible (il n'est pas constant), P est réductible.

Corollaire *Tout polynôme de $\mathbb{C}[X] \setminus \{0\}$ est produit de polynômes de degré un.*

Si $P \in \mathbb{C}[X]$ a $u \in \mathbb{C}$ pour coefficient dominant, il existe $a_1, \ldots, a_n \in \mathbb{C}$ tels que $P = u \prod_{1 \leq k \leq n} (X - a_k)$.

Preuve. Décomposer en produit d'irréductibles, ou faire une récurrence sur $\deg(P)$.

Définition un polynôme de $k[X]$ est dit *scindé* lorsqu'il est produit de polynômes de degré un.

Ainsi, tout polynôme complexe est-il scindé.

7.2.2 Sur $\mathbb{R}$

Si $P \in \mathbb{R}[X]$, on peut voir P comme élément de $C[X]$. Si $z \in \mathbb{C}$ est racine de P, alors $\overline{z}$ est aussi racine de P (car $P(\overline{z}) = \overline{P(z)}$ puisque les coefficients de P sont réels). Par ailleurs, on a la formule (preuve en exercice) suivante :

$$\forall z \in \mathbb{C},\ (X - z)(X - \overline{z}) = X^2 - 2\Re(z)X + |z|^2.$$

Proposition *Soient $P \in \mathbb{R}[X]$ et $z \in \mathbb{C} \setminus \mathbb{R}$. Alors, z est racine de P si, et seulement si $X^2 - 2\Re(z)X + |z|^2$ divise P.*

Preuve. ($\Leftarrow$) résulte de la formule ci-dessus. ($\Rightarrow$) : si z est racine, $\overline{z}$ aussi. Comme $X - z$ et $X - \overline{z}$ sont premiers entre eux ($z \neq \overline{z}$), leur produit divise P (lemme d'Euclide).

Corollaire *Les polynômes irréductibles de $\mathbb{R}[X]$ sont :*
1- les polynômes de degré un ;
2- les polynômes de degré deux qui n'ont pas de racine réelle, i.e. dont le discriminant est négatif.

Preuve. Ceux-ci sont irréductibles (un polynôme réductible de degré deux a une racine). Inversement, si P est irréductible et de degré ≥ 2, il n'a pas de racine réelle. Soit z une racine complexe non réelle de P. Alors, $X^2 - 2\Re(z)X + |z|^2$ divise P. Comme P est irréductible, il existe $u \in \mathbb{C}$ non nul tel que $P = u(X^2 - 2\Re(z)X + |z|^2)$.

Corollaire *Si $P \in \mathbb{R}[X]$, la décomposition de P en produit de facteurs irréductibles est de la forme*

$$P = u \prod_{1 \leq k \leq r} (X - a_k) \prod_{1 \leq k \leq s} Q_k$$

où u et les a_k sont des nombres réels et les Q_k des polynômes unitaires irréductibles de degré deux.

Preuve. Décomposer en produit d'irréductibles, ou décomposer dans $\mathbb{C}[X]$ et regrouper les facteurs conjugués.

7.2.3 Sur $\mathbb{Q}$

La question est beaucoup plus épineuse. On donne ci-dessous une condition suffisante d'irréductibilité d'un polynôme à coefficients entiers.

Notation : si $P = \sum_k p_k X^k \in \mathbb{Z}[X]$ et si p est un nombre premier, on note $\overline{P} = \sum_k \overline{p_k} X^k \in \mathbb{Z}/p\mathbb{Z}[X]$, où $\overline{p_k}$ désigne la classe de p_k modulo p. On appelle $\overline{P}$ la *réduction de P modulo p.*

Proposition *Soient $P \in \mathbb{Z}[X]$ et p un nombre premier. Si $\overline{P}$ est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$, alors P est irréductible dans $\mathbb{Q}[X]$.*

Preuve. Si $P = QR$, alors $\overline{P} = \overline{Q}.\overline{R}$ (exercice).

Exemples. 1- $3971X^3 + 496X^2 - 1615X + 217$ est irréductible sur $\mathbb{Q}$. En effet, il l'est dans $\mathbb{Z}/2\mathbb{Z}$ car sa réduction modulo 2 égale $X^3 + X + 1$ qui est irréductible dans $\mathbb{Z}/2\mathbb{Z}[X]$ (il est sans racine et de degré trois).

2- **Proposition (critère d'Eisenstein)** *Soient $P = \sum_{0 \leq k \leq d} a_k X^k \in \mathbb{Z}[X]$ et p un nombre premier. On suppose que*
i) $p \not| a_d$;
ii) $\forall k \in \{0, \ldots, d-1\}$, $p | a_k$;
iii) $p^2 \not| a_0$.
Dans ces conditions, P est irréductible sur $\mathbb{Q}$.

Preuve. On suppose que $P = QR$ où Q et R sont à coefficients entiers et de degrés ≥ 1. Par réduction modulo p, il vient $\overline{P} = \overline{Q}.\overline{R} = \overline{a_d} X^d$. Par unicité dans le théorème de factorialité dans $\mathbb{Z}/p\mathbb{Z}[X]$, soient q et r des entiers ≥ 1 et b et c des entiers non multiples de p tels que $\overline{Q} = \overline{b} X^q$ et $\overline{R} = \overline{c} X^r$. Alors, $p|Q(0)$ et $p|R(0)$, d'où $p^2|P(0)$ ce qui contredit l'hypothèse iii).

Exemple d'application : *si p est un nombre premier, alors $X^{p-1} + \cdots + X + 1$ est irréductible dans $\mathbb{Q}[X]$ (et dans $\mathbb{Z}[X]$ puisqu'il est unitaire).*

En effet, soient $P = \sum_{k=0}^{p-1} X^k$ et $Q(X) = P(X+1)$. Il suffit de montrer que Q est irréductible dans $\mathbb{Q}[X]$. Comme $(X-1)P = X^p - 1$, on a $XQ = (X+1)^p - 1$. Modulo p, $X\overline{Q} = X^p$, d'où $\overline{Q} = X^{p-1}$. Ainsi, Q vérifie-t-il le critère d'Eisenstein puisque $Q(0) = P(1) = p \notin p^2\mathbb{Z}$.

7.3 Relations entre racines et coefficients d'un polynôme

7.3.1 Relations racines-coefficients (en bref)

Il s'agit d'écrire les coefficients d'un polynôme scindé en fonction de ses racines.
$(X - a_1)(X - a_2) = X^2 - (a_1 + a_2)X + a_1 a_2$ (problème : étant donnés S et P, trouver deux nombres dont la somme valle S et le produit valle P ; ce sont, quand elles existent, les racines de $X^2 - SX + P$).
$(X-a_1)(X-a_2)(X-a_3) = X^3 - (a_1+a_2+a_3)X^2 + (a_1a_2+a_1a_3+a_2a_3)X - a_1a_2a_3$ (quel problème analogue ?).
$(X-a_1)(X-a_2)(X-a_3)(X-a_4) = X^4 - (a_1+a_2+a_3+a_4)X^3 - (a_1a_2+a_1a_3+a_1a_4+a_2a_3+a_2a_4+a_3a_4)X^2 + (a_1a_2a_3+a_1a_2a_4+a_1a_3a_4+a_2a_3a_4)X - a_1a_2a_3a_4$.

Plus généralement, pour chaque $n \geq 1$ et $k \in \{1 \ldots, n\}$, on note

$$\sigma_k(a_1, \ldots, a_n) = \sum_{1 \leq j_1 < \cdots < j_k \leq n} a_{j_1} \ldots a_{j_k}$$

le *k-ième polynôme symétrique élémentaire en $a_1, \ldots, a_n$*, et $\sigma_0 = 1$. Alors,

$$\prod_{k=1}^{n} (X - a_k) = \sum_{k=0}^{n} (-1)^k \sigma_k(a_1, \ldots, a_n) X^{n-k}.$$

Exemple. Si $n \geq 1$, $\sum_{1 \leq k \leq n} a_k^2 = \sigma_1(a_1, \ldots, a_n)^2 - 2\sigma_2(a_1, \ldots, a_n)$ (formule du multinôme de degré deux).

7.3.2 Equations polynomiales (en encore plus bref)

La question consiste à écrire les racines d'un polynôme en fonction de ses coefficients, c'est-à-dire à résoudre l'équation polynomiale $P(x) = 0$ dans $\mathbb{C}$ par exemple, $P \in \mathbb{C}[X]$ étant donné.

Si $\deg(P) \leq 2$, les solutions s'expriment aisément (programme du second degré).

Si $\deg(P) = 3$ ou 4, on peut exprimer les racines de P à l'aide des fonctions racine carrée et racine cubique, de sommes, différences, produits et quotients des coefficients de P (formules de Cardan en degré trois, on s'y ramène en degré quatre).

En revanche, l'"équation générale" de degré ≥ 5 n'est pas "résoluble par radicaux" (math plus avancées, théorie de Galois).

8 Le groupe des racines de l'unité

8.1 Racines de l'unité

Définition Soit $n \in \mathbb{N}^*$. Les *racines n-ièmes de l'unité* sont les nombres complexes racines de $X^n - 1$.

Exercice : les racines de $X^n - 1$ sont toutes simples.

Proposition *Si $\zeta_n = \exp(2i\pi/n)$, les racines n-ièmes de l'unité sont les n nombres ζ_n^k, $0 \leq k \leq n-1$.*

Preuve. Ces nombres sont solutions de $x^n = 1$. Ils sont distincts et au nombre de $n = \deg(X^n - 1)$.

On note $U_n = \{z \in \mathbb{C},\ z^n = 1\}$ l'ensemble des racines n-ièmes de l'unité (notation non universelle).

Dessin des racines sur le cercle. Angles. Rotations. Premières valeurs de n.

Exercice. Calculer $\sum_{\zeta \in U_n} \zeta$, $\sum_{\zeta \in U_n} \zeta^2$, $\sum_{\zeta, \zeta' \in U_n} \zeta\zeta'$.

Notations. Si $(G, \times)$ est un groupe dont la loi est notée multiplicativement, si $g \in G$ et $k \in \mathbb{N}^*$, on note $g^k = g \dots g$ (k fois ; définition par récurrence) et $g^{-k} = (g^{-1})^k$. On note également $g^0 = 1$ (le neutre). On note enfin $\langle g \rangle = \{g^n,\ n \in \mathbb{Z}\}$, qui est un sous-groupe de G.

Si $(G, +)$ est un groupe noté additivement, on note $kg = g + \dots + g$ (k fois), $(-k)g = k(-g)$ et $0g = 0$ (le neutre). On note encore $\langle g \rangle = \{ng,\ n \in \mathbb{Z}\}$.

Définition Un groupe G est dit *monogène* lorsqu'il existe $g_0 \in G$ tel que $G = \langle g_0 \rangle$. On dit alors que g_0 est un *générateur* de G. On dit que G est *cyclique* lorsqu'il est monogène et fini. L'*ordre* d'un groupe fini est son cardinal.

Exemples : $U_3 = \langle j \rangle = \langle j^2 \rangle$ (dessin).
$U_4 = \langle i \rangle = \langle i^3 \rangle$ mais $U_3 \neq \langle i^2 \rangle$ (dessin).
$U_5 = \langle \zeta \rangle = \langle \zeta^2 \rangle = \langle \zeta^3 \rangle = \langle \zeta^4 \rangle$ (dessin).
$U_6 = \langle \omega \rangle = \langle \omega^5 \rangle$ mais $U_6 \neq \langle \omega^2 \rangle$, $U_6 \neq \langle \omega^3 \rangle$ et $U_6 \neq \langle \omega^4 \rangle$ (dessin).

Proposition *Pour tout $n \in \mathbb{N}^*$, U_n est un sous-groupe cyclique d'ordre n de $(\mathbb{C}^*, \times)$. Si $\zeta_n = \exp(2i\pi/n))$ et si $k \in \mathbb{Z}$, alors ζ_n^k est un générateur de U_n si, et seulement si* $\operatorname{pgcd}(k, n) = 1$.

Preuve. 1- Selon la proposition précédente, U_n est non vide, stable pour la multiplication et le passage à l'inverse et $U_n = \langle \zeta_n \rangle$. Donc U_n est un sous-groupe engendré par ζ_n.

2- Les générateurs. On suppose que $\langle \zeta_n^k \rangle = U_n$. Soit $l \in \mathbb{Z}$ tel que $(\zeta_n^k)^l = \zeta_n$. Alors, n divise $1 - kl$: ceci est une relation de Bézout qui montre que k et n sont étrangers. Réciproquement, si $k \wedge n = 1$, soit $1 = kl + mn$ une relation de Bézout entre k et n. Alors, $\zeta_n = (\zeta_n^k)^l$ est une puissance de ζ_n^k. Donc toute racine n-ième est une puissance de ζ_n^k : $U_n = \langle \zeta_n^k \rangle$.

Exercice : l'ensemble de toute les racines de l'unité forme un sous-groupe de $(\mathbb{C}^*, \times)$. On notera ce groupe $\mathbb{U}$ (notation non universelle).
Définition Une racine n-ième ζ de l'unité est dite *primitive* lorsqu'elle engendre U_n.
Ainsi, $\exp(2ik\pi/n)$ est-il racine primitive n-ième de l'unité si, et seulement si $k \wedge n = 1$.

Exercice : toute racine de l'unité est une racine primitive N-ième (pour un N bien choisi).

8.2 Le groupe $\mathbb{Z}/n\mathbb{Z}$

Soit n un entier naturel non nul. Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique, engendré par 1 (exercice, attention à la notation additive).

Proposition *Soient $n \in \mathbb{N}^*$ et $k \in \mathbb{Z}$. La classe de k modulo n engendre $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si k est premier avec n.*

Preuve. $\overline{k}$ engendre $\mathbb{Z}/n\mathbb{Z}$ si, et seulement s'il existe $l \in \mathbb{Z}$ tel que $\overline{k}.\overline{l} = \overline{1}$, c'est-à-dire si, et seulement si $\overline{k}$ est inversible dans l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.

8.3 L'exponentielle

Soit n un entier naturel non nul, et soit

$$\begin{array}{rl} \varepsilon : & \mathbb{Z} \to U_n \\ & k \mapsto \exp(2ik\pi/n). \end{array}$$

Les propriétés de la fonction exponentielle font de ε un homomophisme de groupes $(\mathbb{Z}, +) \to (U_n, \times)$, surjectif (exercice).

Dessin de l'enroulement de $\mathbb{R}$ et de $\mathbb{Z}$ sur le cercle.

En outre, ε est constant sur les classes modulo n (*i.e.* si $k \equiv k'\ [n]$, alors $\varepsilon(k) = \varepsilon(k')$). Ainsi ε induit-il un homomorphisme de groupes $\overline{\varepsilon} : \mathbb{Z}/n\mathbb{Z} \to U_n$, surjectif (exercice). Comme $\mathbb{Z}/n\mathbb{Z}$ et U_n ont le même cardinal fini, $\overline{\varepsilon}$ est également injectif.

Conclusion : la fonction exponentielle induit un isomorphisme de groupes

$$\begin{array}{rccc} \overline{\varepsilon}: & (\mathbb{Z}/n\mathbb{Z},+) & \to & (U_n,\times) \\ & \overline{k} & \mapsto & \exp(2ik\pi/n). \end{array}$$

Exercices. 1- Si G est un groupe cyclique d'ordre n, alors G est isomorphe à $(\mathbb{Z}/n\mathbb{Z},+)$. Si G est monogène et infini, alors G est isomorphe à $(\mathbb{Z},+)$.
2- L'application $(\mathbb{Q},+) \to (\mathbb{U},\times)$ $r \mapsto \exp(2i\pi r)$ est un homomorphisme surjectif de groupes, dont le noyau est $\mathbb{Z}$.

9 Appendice : axiomatique des structures abstraites de groupes, anneaux et corps

9.1 Groupes

9.1.1 Définition, axiomes

Un **groupe** est un ensemble G muni d'une *loi de composition interne* notée ici $\times$ (*i.e.* une application $G \times G \to G$, $(x, y) \mapsto x \times y$) vérifiant les trois axiomes suivants :

1- la loi $\times$ est *associative (i.e.* $(x \times y) \times z = x \times (y \times z)$ pour tous x, y, et z de G ; on note $x \times y \times z$ ce produit) ;

2- G possède un *élément neutre* e pour $\times$ (*i.e.* $x \times e = e \times x = x$ pour tout $x \in G$; on note souvent 1 l'élément neutre) ;

3- tout élément de G possède un *symétrique* pour $\times$ (*i.e.* pour tout $x \in G$, il existe $y \in G$ tel que $x \times y = y \times x = e$; on note souvent $y = x^{-1}$).

Si en outre $\times$ est *commutative* (*i.e.* $x \times y = y \times x$ pour tous x et y de G), le groupe est dit *commutatif* ou *abélien*.

On omet souvent le symbole $\times$ de la loi en notant $xy = x \times y$. On note parfois $+$ la loi des groupes commutatifs ; dans ces conditions, l'élément neutre est noté 0 et le symétrique de tout $x \in G$ est noté $-x$.

9.1.2 Sous-groupe, homomorphisme de groupes

Un **sous-groupe** d'un groupe G est une partie de G qui soit un groupe pour la loi de G.

Proposition *Une partie H d'un groupe G est un sous-groupe de G si, et seulement si :*

1- H est stable pour la loi de G (i.e. $x \times y \in H$ pour tous x et y de H) ;

2- le symétrique (pour la loi de G) de tout élément de H est dans H.

Un **homomorphisme de groupes** est une application f d'un groupe G dans un groupe G' qui préserve les lois de G et de G', c'est-à-dire telle que $f(xy) = f(x)f(y)$ pour tous x et y de G.

9.1.3 Exemples fondamentaux

L'addition usuelle dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/n\mathbb{Z}$ où $n \in \mathbb{Z}$, et dans leurs puissances.

La multiplication usuelle dans $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{R}_+^*$ ou $\mathbb{C}^*$, dans l'ensemble des nombres complexes de module un, dans l'ensemble des racines n-ièmes de l'unité ($n \geq 1$) et dans l'ensemble de toutes les racines de l'unité.

La composition dans $\mathfrak{S}_A$ (groupe symétrique de l'ensemble A) ; dans $\mathrm{GL}(E)$ (groupe linéaire de l'espace vectoriel E) et dans ses sous-groupes $\mathrm{SL}(E)$, $\mathrm{O}(E)$, $\mathrm{SO}(E)$, $\mathrm{U}(E)$, $\mathrm{SU}(E)$; dans l'ensemble des similitudes (resp. des similitudes directes) vectorielles planes ; dans $\mathrm{GA}(E)$ (groupe affine de l'espace affine E) et dans ses sous-groupes des translations, des homothéties-translations, des isométries, des rotations, des similitudes) etc...

Le produit matriciel dans $\mathrm{GL}_n(A)$ (matrices carrées $n \times n$ inversibles à coefficients dans l'anneau A), $\mathrm{SL}_n(A)$, $\mathrm{O}_n(\mathbb{R})$, $\mathrm{SO}_n(\mathbb{R})$, $\mathrm{U}_n(\mathbb{C})$, $\mathrm{SU}_n(\mathbb{C})$; dans l'ensemble des matrices triangulaires supérieures (resp. inférieures) inversibles, dans l'ensemble des matrices diagonales inversibles, etc...

9.2 Anneaux

9.2.1 Définition, axiomes

Un **anneau** (unitaire) est un ensemble A muni de deux lois de composition interne notées ici $+$ (addition) et $\times$ (multiplication) vérifiant les axiomes suivants :

1- $(A, +)$ est un groupe abélien ; on note souvent son élément neutre 0 et $-a$ le symétrique de $a \in A$ pour $+$ (on parle de l'*opposé* de a) ;

2- la loi $\times$ est associative et admet un élément neutre souvent noté 1 ;

3- la multiplication est *distributive* par rapport à l'addition (*i.e.* $a \times (b + c) = (a \times b) + (a \times c)$ et $(a + b) \times c = (a \times c) + (b \times c)$ pour tous a, b et c de A).

Si en outre la multiplication est commutative, l'anneau est dit *commutatif*.

Les règles de calcul dans un anneau commutatif sont celles de $\mathbb{Z}$; en particulier, la formule du binôme de Newton est vraie dans un anneau commutatif (ou dans un anneau général entre deux éléments qui commutent). Dans les systèmes de parenthésages, on donne la priorité à la multiplication ; ainsi, $a \times b + c = (a \times b) + c$.

9.2.2 Sous-anneau, idéal, homomorphisme d'anneaux

Un **sous-anneau** d'un anneau A est une partie de A qui soit un anneau pour les lois de A. Une partie B d'un anneau $(A, +, \times)$ est un sous-anneau de A si, et seulement si $(B, +)$ est un sous-groupe de $(A, +)$ contenant 1, et B est stable pour la multiplication de A.

Un **idéal** d'un anneau commutatif A est une partie I de A telle $(I, +)$ soit un sous-groupe de $(A, +)$ et $ia \in I$ pour tous $i \in I$ et $a \in A$.

Une application f d'un anneau A dans un anneau B est un **homomorphisme d'anneaux** si, et seulement si elle préserve les unités et les lois de A et B, c'est-à-dire si, et seulement si $f(1) = 1$, $f(x + y) = f(x) + f(y)$ et $f(xy) = f(x)f(y)$ pour tous x et y de A.

9.2.3 Exemples fondamentaux

Pour leurs lois usuelles, $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ pour $n \geq 2$, les corps de nombres $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, l'ensemble des nombres décimaux.

L'anneau $A[X]$ des polynômes à coefficients dans un anneau A ; également l'anneau $A[X_1, \ldots, X_n]$ des polynômes à n indéterminées.

L'anneau des endomorphismes d'un espace vectoriel (la multiplication est la composition), l'anneau des matrices carrées à coefficients dans un anneau (la multiplication est le produit matriciel).

L'ensemble des applications d'un ensemble E dans un anneau A (pour les lois usuelles $(f+g)(x) = f(x) + g(x)$ et $(fg)(x) = f(x)g(x)$).

9.3 Corps

9.3.1 Définition, axiomes

Un **corps** est un anneau K dans lequel tout élément non nul x admet un symétrique pour la multiplication (on parle alors de l'*inverse* de x, souvent noté x^{-1}). Cela revient à demander que $K \setminus \{0\}$ soit un groupe pour la multiplication.

9.3.2 Sous-corps

Un **sous-corps** d'un corps L est une partie K de L qui soit un corps pour les lois de L. Cela revient à demander que $(K, +)$ soit un sous-groupe de $(L, +)$ et que $(K \setminus \{0\}, \times)$ soit un sous-groupe de $(L \setminus \{0\}, \times)$.

9.3.3 Exemples fondamentaux

$\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ pour leurs lois usuelles. Le corps des nombres algébriques.
$\mathbb{Z}/p\mathbb{Z}$ si p est un nombre premier, les corps finis $\mathbb{F}_{p^a}$.
$k[X]/(P)$ si k est un corps et si P est un polynôme irréductible de $k[X]$.
L'ensemble des fractions rationnelles sur un corps.
Le corps des quaternions (non commutatif).