Université Blaise Pascal
U.F.R. Sciences et Technologies
Département de Mathématiques et Informatique

Première année de licence

Polycopié du cours de

Logique et Arithmétique

Yves Stalder

Année 2010–2011

Table des matières

Quelques avant-propos

Par leur relecture attentive et critique, François Martin et Marusia Rebolledo m'ont permis de corriger de nombreuses fautes de frappe, et d'améliorer l'exposition des mathématiques contenues dans ce polycopié. Je les remercie vivement pour leur précieuse collaboration.

Si vous découvrez des erreurs dans le texte, je vous remercie par avance de m'en faire part. Vous pouvez m'écrire à l'adresse `yves.stalder@math.univ-bpclermont.fr` .

CHAPITRE 1

Expression mathématique et raisonnement

Référence. Pour préparer ce chapitre, je me suis notamment inspiré du chapitre 1 de l'ouvrage suivant : François Liret et Dominique Martinais, *Cours de mathématiques : Algèbre 1re année*, Dunod, 1997.

1. Le langage mathématique

Les phrases qui portent sur des objets mathématiques (on les appelle *énoncés*) peuvent être de nature très différente, et il est très important de bien faire la distinction entre ces catégories. Définir une nouvelle notion ou affirmer qu'un objet possède une propriété, ce n'est pas du tout la même chose !

1.1. Les propositions. Les phrases les plus intéressantes sont les *propositions*. Une proposition *affirme* quelque chose ; il est sensé de se demander si elle est vraie ou fausse. Le but d'un texte mathématique est de démontrer que certaines propositions, dont le contenu est jugé intéressant, sont vraies.

Exemples (de propositions). (1) On a $3 + 3 = 6$;

(2) le nombre 10^3 est supérieur à 2^{10} ;

(3) tout entier naturel est un carré ;

(4) il existe un nombre réel x tel que $x^2 = -2$;

(5) pour tout nombre complexe z, on a $z^2 \geq 0$;

(6) pour tout $n \in \mathbf{N}^*$, la relation $\sum_{i=1}^{n} i = n(n+1)/2$ est satisfaite.

On remarquera qu'une proposition peut très bien être fausse ! Parmi les exemples ci-dessus, certaines propositions sont vraies et d'autres fausses. On admettra les deux principes suivants.

Principe de non contradiction. *Une proposition ne peut pas être à la fois vraie et fausse.*

Principe du tiers exclu. *Toute proposition est vraie ou fausse ; il n'y a pas de troisième possibilité.*

Ces deux principes sont communément acceptés en mathématiques classiques, entre autres parce qu'ils sont intuitifs. Il n'est pas impossible de les remettre en cause (certains le font d'ailleurs) mais une discussion à ce sujet dépasserait très largement le cadre de ce cours !

1.2. Définitions et notations. Un texte mathématique n'est pas constitué que de propositions. On a besoin d'autres énoncés.

EXEMPLES. Les énoncés suivants ne sont pas des propositions :

(1) On appelle suite de nombres réels une application de l'ensemble $\mathbf{N}$ dans l'ensemble $\mathbf{R}$;

(2) soit ε un réel strictement positif ;

(3) posons $A = \frac{2^{12}-2^9}{3\cdot 5^2}$;

(4) dans ce qui suit, $P(f)$ désigne la primitive de la fonction f qui s'annule en 0.

Il est insensé de se demander si de telles phrases sont vraies ou fausses. L'exemple (1) introduit le concept de suite de nombres réels ; c'est une *définition*. Dans l'exemple (2), le mot «soit» indique qu'on va se fixer un objet mathématique (ici un nombre réel strictement positif) et lui donner un nom (ici ε). Les phrases (3) et (4) sont des *notations* : elles expliquent qu'un symbole (ou une combinaison de symboles) désignera un objet mathématique préalablement défini.

1.3. Quelques règles d'écriture. Certaines propositions peuvent s'écrire uniquement avec des symboles mathématiques, par exemple « $10 < 5$ » ou « $\sin(2\alpha) = 2\sin(\alpha)\cos(\beta)$ ». Cependant, un texte mathématique se doit de respecter, autant que faire se peut, les règles de grammaire de la langue dans laquelle il est écrit. Ainsi, une phrase ne sera pas constituée uniquement d'une formule. Par exemple, on n'écrit pas «$6 < 7$», mais «La relation $6 < 7$ est satisfaite.» ou plus simplement «On a $6 < 7$.». On n'écrit pas non plus «6 est strictement inférieur à 7.», car on évite de commençer une phrase par un symbole mathématique (ceci évite en particulier de commencer une phrase par une minuscule).

En particulier, une phrase comporte un *verbe*, qui ne peut pas être remplacé par un symbole mathématique. Dans l'exemple «$6 < 7$», c'est le symbole $<$ qui joue le rôle du verbe. Dans un texte, on écrirait «Le nombre 6 est strictement inférieur à 7.». On admet quelques entorses à cette règle, afin de ne pas trop alourdir la formulation. On se permet par exemple d'écrire «Si $a > 0$, alors l'équation $x^2 = a$ admet deux solutions dans $\mathbf{R}$.» ou «On a $\sqrt{2} < 3/2$, car $2 < \frac{9}{4}$.». On ne remplace en revanche jamais le verbe principal par un symbole mathématique.

1.4. Opérations sur les propositions. Il existe des opérateurs logiques qui permettent de construire des propositions (dites composées) à partir d'une ou plusieurs propositions.

1.4.1. *La négation.* Si P représente une proposition, on désigne par $\text{non}(P)$, $\text{non}\,P$ ou $\neg P$ la *négation* de P. Cette proposition est par définition vraie si P est fausse et fausse si P est vraie. Voici quelques exemples de négations :

P	$\text{non}\,P$
$6 < 7$.	$6 \geq 7$.
$\sqrt{2}$ est rationnel.	$\sqrt{2}$ est irrationnel.
L'ensemble E possède au moins 4 éléments.	L'ensemble E possède au plus 3 éléments.

1.4.2. *Les connecteurs «ou» et «et».* On rencontre souvent des propositions telles que «n est pair et satisfait $n^2 = 3$.» ou «$n \leq 4$ ou $f(n) = 0$.». Grâce aux connecteurs «ou» et «et», on peut les décomposer en propositions plus simples : «(n est pair) et (n satisfait $n^2 = 3$)» pour la première et «($n \leq 4$) ou ($f(n) = 0$)» pour la seconde.

Considérons deux propositions P, Q. La proposition P ou Q est vraie dès lors qu'une (au moins) des propositions P, Q est vraie ; elle est fausse si les propositions P, Q sont toutes les deux fausses. La proposition P et Q est vraie si les propositions P, Q sont toutes les deux vraies ; elle est fausse dans tous les autres cas.

EXEMPLE 1.1. Supposons que P est la proposition «Tout nombre complexe est un nombre réel.» et que Q est la proposition «On a $3 < 8$.». La proposition P et Q est fausse, tandis que la proposition P ou Q est vraie.

EXEMPLE 1.2. Supposons que P est la proposition «Tout nombre rationnel est un nombre réel.» et que Q est la proposition «On a $3 < 8$.». La proposition P et Q est vraie, ainsi que la proposition P ou Q.

On notera à ce propos qu'en mathématiques, le connecteur «ou» est *inclusif* : lorsque les deux propositions P, Q sont vraies, la proposition P ou Q est vraie. Ceci est contre-intuitif pour certains, car «ou» a souvent un sens exclusif dans la vie courante. Lorsqu'un menu propose «fromage ou dessert», vous ne pouvez le plus souvent pas avoir les deux !

EXERCICE 1.3. Ecrire la proposition «$3 < 5 < 2$» sous la forme «P et Q».

1.4.3. *L'implication.* Considérons la proposition «Si x est un nombre rationnel, alors x^2 est un nombre naturel.». Elle est de la forme «Si P, alors Q», où P est la proposition «x est un nombre rationnel» et Q est la proposition «x^2 est un nombre naturel». Dans le cas où x est un nombre rationnel, elle affirme que x^2 est un nombre naturel. Dans le cas contraire, elle n'affirme rien du tout. Autrement dit, notre proposition affirme qu'il est impossible que x soit un nombre rationnel et que x^2 ne soit pas un nombre naturel.

Supposons maintenant que P et Q sont deux propositions quelconques. La proposition (Si P, alors Q) est fausse lorsque P est vraie et que Q est fausse ; elle est vraie dans tous les autres cas.

Au lieu de «Si P, alors Q», on peut dire «P implique Q» ou encore «P entraîne Q». Lorsque P et Q sont constituées (presque) uniquement de symboles mathématiques, on peut aussi noter $P \Rightarrow Q$. Par exemple $(2 < x < 4) \Rightarrow (4 < x^2 < 16)$.

EXEMPLES.
(1) La proposition «Si x est un nombre réel satisfaisant $x > 2$, alors on a $x^2 > 4$.» est vraie ;
(2) La proposition «Si x est un nombre réel satisfaisant $x^2 > 4$, alors on a $x > 2$» est fausse. En effet, on peut avoir $x^2 > 2$ et $x \leq 2$, par exemple si $x = -3$.

1.4.4. *L'équivalence.* On dit que deux propositions P et Q sont *équivalentes* lorsque P implique Q et que Q implique P. Ceci signifie que les propositions P, Q sont soit toutes les deux vraies, soit toutes les deux fausses. Lorque P et Q sont équivalentes, on dit que la proposition

«P si et seulement si Q» est vraie. Dans le cas contraire, on dit que la proposition «P si et seulement si Q» est fausse. Au lieu de «P si et seulement si Q», on peut aussi écrire «P est équivalent à Q», ou $P \Leftrightarrow Q$ lorsque P et Q sont constituées (presque) uniquement de symboles mathématiques. Voici un résumé des quatre cas possibles :

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$P \Leftrightarrow Q$
vraie	vraie	vraie	vraie	vraie
vraie	fausse	fausse	vraie	fausse
fausse	vraie	vraie	fausse	fausse
fausse	fausse	vraie	vraie	vraie

Dans ce tableau, P et Q sont vus comme constituants de base des propositions $P \Rightarrow Q$, $Q \Rightarrow P$ et $P \Leftrightarrow Q$. Il peut cependant arriver que P, Q ou les deux soient elles mêmes des propositions composées. Autrement dit, P peut dépendre de propositions $P_1, \dots, P_k$ et Q peut dépendre de propositions $Q_1, \dots, Q_\ell$ (par exemple, P peut être de la forme P_1 et P_2 ; Q peut être de la forme $Q_1 \Leftrightarrow Q_2$). Dans un tel cas, si on veut écrire un tableau qui donne la valeur de vérité (vraie ou fausse) de $P \Leftrightarrow Q$ en fonction de celles de $P_1, \dots, P_k, Q_1, \dots, Q_\ell$, on a besoin de $2^{k+\ell}$ lignes.

1.5. Interactions entre les opérations. Avec les opérations vues à la section 1.4, on peut construire beaucoup de propositions composées. On va maintenant voir les cas d'équivalence les plus importants. Supposons que P, Q, R sont des propositions. On a les équivalences suivantes :

(1) $P \iff \text{non}(\text{non}\, P)$;
(2) $\text{non}(P \,\text{et}\, Q) \iff \big[(\text{non}\, P)\,\text{ou}(\text{non}\, Q)\big]$;
(3) $\text{non}(P \,\text{ou}\, Q) \iff \big[(\text{non}\, P)\,\text{et}(\text{non}\, Q)\big]$;
(4) $\big[P\,\text{et}(Q \,\text{ou}\, R)\big] \iff \big[(P \,\text{et}\, Q)\,\text{ou}(P \,\text{et}\, R)\big]$;
(5) $\big[P\,\text{ou}(Q \,\text{et}\, R)\big] \iff \big[(P \,\text{ou}\, Q)\,\text{et}(P \,\text{ou}\, R)\big]$;
(6) $\text{non}(P \Rightarrow Q) \iff \big[P\,\text{et}(\text{non}\, Q)\big]$;
(7) $\big[P \Rightarrow Q\big] \iff \big[(\text{non}\, P)\,\text{ou}\, Q\big]$;
(8) $\big[P \Rightarrow Q\big] \iff \big[(\text{non}\, Q) \Rightarrow (\text{non}\, P)\big]$;
(9) $\big[P \Rightarrow (Q \,\text{et}\, R)\big] \iff \big[(P \Rightarrow Q)\,\text{et}(P \Rightarrow R)\big]$.

A titre d'exemple, expliquons le point (3). La proposition $\text{non}(P \,\text{ou}\, Q)$ est fausse lorsqu'une au moins des propositions P, Q est vraie, et vraie lorsque les deux sont fausses. La proposition $(\text{non}\, P)\,\text{et}(\text{non}\, Q)$ est vraie lorque les deux propositions $\text{non}\, P, \text{non}\, Q$ sont vraies, et fausse lorsqu'une au moins est fausse, ce qui revient au même. Par conséquent, on a $(\text{non}(P \,\text{et}\, Q)) \iff ((\text{non}\, P)\,\text{ou}(\text{non}\, Q))$. D'autres cas pourront être traités en TD.

1.6. Les expressions «pour tout» et «il existe». L'énoncé «l'entier naturel x est pair» n'est pas vraiment une proposition, car il dépend de la variable x. Il est vrai pour certaines valeurs de x (par exemple 2) et faux pour d'autres (par exemple 3). Si le nombre x n'est pas fixé, il est vain de chercher à savoir si l'énoncé est vrai ou faux. Si on ne souhaite pas fixer x, on peut obtenir des propositions en *quantifiant* la variable x, au moyen des expressions «pour tout» et «il existe». A partir de l'énoncé «x est pair», on peut obtenir les propositions :

– «Pour tout $x \in \mathbf{Z}$, x est pair.», «Pour tout $x \in \mathbf{N}$, x est pair.» ;
– «Il existe $x \in \mathbf{Z}$ tel que x est pair.», «Il existe $x \in \mathbf{N}$ tel que x est pair.».
Les premières affirment que si on considère *n'importe quel* élément $x \in \mathbf{Z}$ (resp. $x \in \mathbf{N}$), ce nombre est nécessairement pair. Elle sont fausses, puisque 1 est un élément de $\mathbf{Z}$ (et aussi de $\mathbf{N}$) qui n'est pas pair. Les dernières propositions sont vraies, car 2 est un élément de $\mathbf{Z}$ (et aussi de $\mathbf{N}$) qui est pair.

REMARQUE 1.4. Au lieu de «Pour tout $x \in \mathbf{Z}$, x est pair.» on peut utiliser la formulation alternative «Soit $x \in \mathbf{Z}$. Alors x est pair.», qui permet d'éviter les phrases trop longues.

Dans les formules mathématiques, le signe $\forall$ signifie «pour tout» et le signe $\exists$ signifie «il existe». Ainsi la proposition «Pour tout $x \in \mathbf{N}$, on a $x > 2$.» peut s'écrire «$\forall x \in \mathbf{N}, x > 2$» ; la proposition «Il existe $x \in \mathbf{N}$ tel que $x > 2$.» peut s'écrire «$\exists x \in \mathbf{N}, x > 2$».

MISE EN GARDE. L'ensemble qu'on utilise pour quantifier est important ; en changer peut tranformer une proposition vraie en proposition fausse et inversement. Par exemple :
– la proposition «$\forall x \in \mathbf{R}, x^2 \geq 0$» est vraie, tandis que «$\forall x \in \mathbf{C}, x^2 \geq 0$» est fausse ;
– la proposition «$\exists x \in \mathbf{C}, x^2 = -1$» est vraie, tandis que «$\exists x \in \mathbf{R}, x^2 = -1$» est fausse.

Supposons maintenant plus généralement que pour chaque élément x d'un ensemble E on ait une proposition $P(x)$ (dans l'exemple du début, on prend $E = \mathbf{Z}$ et $P(x)$ est la proposition «x est pair»). La proposition «Pour tout $x \in E$, $P(x)$.» est vraie si pour *n'importe quel* élément $x \in E$, la proposition $P(x)$ est vraie. Elle est fausse s'il existe un élément $x \in E$ tel que $P(x)$ est fausse. La proposition «Il existe $x \in E$, $P(x)$.» est vraie si la proposition $P(x)$ est vraie pour au moins un élément de E. Elle est fausse si la proposition $P(x)$ est fausse, quel que soit l'élément $x \in E$ qu'on considère.
Il résulte de ce qui précède que :
– les propositions «non$(\forall x \in E, P(x))$» et «$\exists x \in E, \text{non}\, P(x)$» sont équivalentes ;
– les propositions «non$(\exists x \in E, P(x))$» et «$\forall x \in E, \text{non}\, P(x)$» sont équivalentes.

MISE EN GARDE. La proposition «Pour tout $x \in E$, $P(x)$.» n'affirme PAS qu'il existe un élément dans E. Ainsi, la proposition «Pour tout $x \in \mathbf{R}$ tel que $x^2 < 0$, on a $x > x + 1$.» est VRAIE, même si elle n'a aucun intérêt. En effet, comme aucun nombre réel x ne satisfait $x^2 < 0$, on ne peut *a fortiori* trouver aucun élément $x \in \mathbf{R}$ qui satisfasse $x^2 < 0$ mais pas $x > x + 1$.

2. Le raisonnement

En pratique, un mathématicien s'intéresse principalement aux propositions vraies. Différentes techniques de raisonnement permettent de démontrer qu'une proposition est vraie. Nous allons répertorier les méthodes les plus importantes. Les preuves données à titre d'exemple sont très simples, pour mieux faire ressortir leur structure logique.

2.1. Preuve d'une proposition existentielle. Il s'agit de propositions de la forme «Il existe $x \in E$ tel que $P(x)$». La technique la plus évidente, mais parfois aussi la plus difficile, pour démontrer une telle proposition consiste à exhiber explicitement un élément $x_0 \in E$ tel que $P(x_0)$ est vraie.

EXEMPLE 2.1. Démontrons la proposition «Il existe $x \in \mathbf{Z}$ tel que $x^2 - 5x + 6 = 0$».
On constate que $x_0 = 2 \in \mathbf{Z}$ et $x_0^2 - 5x_0 + 6 = 4 - 10 + 6 = 0$. □

Toutefois, il n'est pas toujours possible de trouver cet élément x_0. On recourt donc parfois à des preuves, dites non constructives, qui permettent de ne pas exhiber d'élément x_0 comme ci-dessus. Voici ce qu'on appelle un *argument de comptage*.

EXEMPLE 2.2. On convient qu'un nombre naturel n est un *carré* s'il s'écrit sous la forme k^2, avec $k \in \mathbf{N}$. Démontrons la proposition «Il existe $x \in \mathbf{N}$ tel que $x \leq 30$ et x n'est pas un carré».
Soit $A = \{0, 1, \ldots, 30\}$ et $B = \{x \in A : x \text{ est un carré}\}$. On doit montrer qu'il existe $x \in A$ tel que $x \notin B$. L'ensemble A possède 31 éléments. Par contre, dès que $k \geq 6$, on a $k^2 > 30$, d'où $x \notin B$. Par conséquent B possède seulement 6 éléments (au plus). Comme le cardinal de A est strictement supérieur à celui de B, il existe $x \in A$ tel que $x \notin B$. □

Dans cet exemple, on aurait bien sûr pu exhiber l'élément $x_0 = 2$, qui est un nombre naturel inférieur ou égal à 30 et qui n'est pas un carré. Néanmoins, les arguments de comptage peuvent parfois s'avérer fort utiles, notamment lorsque A et B sont des ensembles infinis.

REMARQUE CULTURELLE 2.3. Les arguments de comptage comparant deux ensembles infinis ne sont pas au programme de ce cours. Signalons cependant qu'ils permettent par exemple de démontrer l'existence de nombres irrationnels ou de nombres transcendants (c'est-à-dire de nombres qui ne sont solution d'aucune équation de la forme $a_k x^k + \cdots + a_1 x + a_0 = 0$ avec $a_0, \ldots, a_k \in \mathbf{Q}$) sans avoir à en trouver un seul !

Les arguments de comptage sont en fait des cas particuliers de raisonnements par l'absurde (cf. section 2.8).

2.2. Preuve d'une proposition universelle. Il s'agit de propositions de la forme «Pour tout $x \in E$, on a $P(x)$». Pour démontrer une telle proposition, il faut prouver que $P(x)$ est vraie *quel que soit* l'élément $x \in E$ qu'on considère. Pour ce faire, **on fixe un élément $x \in E$ arbitraire** (c'est-à-dire qu'on s'interdit de faire une quelconque autre hypothèse dessus) et on démontre $P(x)$.

EXEMPLE 2.4. Démontrons la proposition «Pour tout nombre naturel pair n, le nombre n^2 est un multiple de 4.»
Soit n un nombre naturel pair. On peut écrire $n = 2k$, où k est un nombre naturel. Par suite, on a $n^2 = 2k \cdot 2k = 4k^2$ et $k^2 \in \mathbf{N}$. Ceci prouve que n^2 est un multiple de 4. □

On peut parfois aussi raisonner par l'absurde (cf. section 2.8). Notons par ailleurs que souvent, les deux types de quantificateurs apparaissent dans une même proposition.

EXEMPLE 2.5. Démontrons la proposition «Pour tout $n \in \mathbf{Z}$, il existe $x \in \mathbf{Q}$ tel que $7x + 4 = n$.»
Soit $n \in \mathbf{Z}$. On doit démontrer qu'il existe $x \in \mathbf{Q}$ tel que $7x + 4 = n$. Or, on voit que le nombre $x_0 = \frac{n-4}{7}$ est rationnel et satisfait $7x_0 + 4 = n$. □

Notons que dans un tel cas, l'élément x_0 peut dépendre de n.

EXEMPLE 2.6. Démontrons la proposition «Il existe $x \in \mathbf{Q}$ tel que pour tout $y \in \mathbf{R}$ on ait $x < y^2$.»
Considérons le nombre rationnel $x_0 = -1$. Démontrons que pour tout $y \in \mathbf{R}$ on a $x_0 < y^2$. Pour ce faire, fixons $y \in \mathbf{R}$. On a alors $y^2 \geq 0 > x_0$. □

Notons qu'ici, il faut en revanche exhiber un UNIQUE x_0, qui convienne quel que soit l'élément $y \in \mathbf{R}$ qu'on considère ensuite.

2.3. Utilisation des implications. Lorsqu'on a démontré que deux propositions P et $P \Rightarrow Q$ sont vraies, on peut immédiatement en déduire que la proposition Q est vraie. Pour les besoins de l'exemple qui suit, admettons les propositions suivantes sans preuve.

PROPOSITION 2.7. *Soit f une fonction de $\mathbf{R}$ dans $\mathbf{R}$. Si f est dérivable (en tout point), alors f est continue (en tout point).*

PROPOSITION 2.8. *La fonction $g : \mathbf{R} \to \mathbf{R}$ définie par $g(x) = x^2$ est dérivable (en tout point).*

EXEMPLE 2.9. Démontrons la proposition «La fonction $g : \mathbf{R} \to \mathbf{R}$ définie par $g(x) = x^2$ est continue (en tout point).»
La proposition 2.7 s'applique à g. Ainsi, si g est dérivable (en tout point), alors est continue (en tout point). Par ailleurs, on sait que g est dérivable (en tout point) par la proposition 2.8. On en déduit que g est continue (en tout point). □

2.4. Preuve directe d'une implication. On sait qu'une proposition du type $P \Rightarrow Q$ est vraie, sauf lorque P est vraie et que Q est fausse. Pour démontrer $P \Rightarrow Q$ (c'est-à-dire démontrer que $P \Rightarrow Q$ est vraie), on peut faire l'*hypothèse* que P est vraie et en déduire que Q est alors nécessairement vraie.

EXEMPLE 2.10. Démontrons la proposition «Si $1 = 2$, alors on a $9 = 16$».
On suppose que la relation $1 = 2$ est satisfaite. En ajoutant 2 de chaque côté, il vient $3 = 4$. Enfin, en élevant chaque membre au carré, on trouve $9 = 16$. □

Pour démontrer une proposition du type de $P \Rightarrow Q$, on n'a pas besoin de savoir si P est vraie ou fausse. L'exemple précédent illustre bien ce fait. Rappelons tout de même que lorsque P est fausse, la proposition $P \Rightarrow Q$ est vraie par définition. Dans l'exemple, il aurait donc suffi de remarquer que la proposition $1 = 2$ est fausse.

EXEMPLE 2.11. Démontrons la proposition «Pour tous nombres naturels a et b, si a est multiple de 2 et si b est multiple de 3, alors ab est multiple de 6.»
Soit $a, b \in \mathbf{N}$. On suppose que a est multiple de 2 et que b est multiple de 3. Donc il existe $a', b' \in \mathbf{N}$ tels que $a = 2a'$ et $b = 3b'$, ce qui entraîne $ab = 2a' \cdot 3b' = 6a'b'$. On voit que ab est multiple de 6. □

2.5. Raisonnement par contraposée. Une proposition du type $P \Rightarrow Q$ est toujours équivalente à $(\text{non}\, Q) \Rightarrow (\text{non}\, P)$. En effet, les deux propositions sont fausses lorsque P est vraie et que Q est fausse (ce qui revient à dire que non(Q) est vraie et que non(P) est fausse) ; elles sont vraies toutes les deux dans tous les autres cas. Par conséquent, pour démontrer $P \Rightarrow Q$, on peut démontrer $(\text{non}\, Q) \Rightarrow (\text{non}\, P)$ si l'on préfère.

DÉFINITION 2.12. *La proposition* $(\text{non}\, Q) \Rightarrow (\text{non}\, P)$ *est appelée* contraposée *de* $P \Rightarrow Q$.

PROPRIÉTÉ ESSENTIELLE DE LA CONTRAPOSÉE.
Pour démontrer une proposition de la forme $P \Rightarrow Q$*, il suffit de démontrer sa contraposée.*

Très souvent, le raisonnement par contraposée est utilisé pour des propositions de la forme $\forall x \in E\ (P(x) \Rightarrow Q(x))$. C'est le cas dans l'exemple suivant.

EXEMPLE 2.13. Démontrons que pour tout $n \in \mathbf{N}$, si n^2 est pair, alors n est pair.
On procède par contraposée. Soit n un entier naturel quelconque. Supposons que n n'est pas pair. Dès lors, n est impair et on peut écrire $n = 2k+1$ avec $k \in \mathbf{N}$. Ainsi, on a $n^2 = 4k^2+4k+1$, donc n^2 est impair. □

EXERCICE 2.14. Démontrer de même la proposition «Soit $n \in \mathbf{N}$. Si n^2 est impair, alors n est impair».

EXEMPLE 2.15. Démontrons que pour tout $x \in \mathbf{R}$, si $|x-2| < 2$, alors on a $x > 0$.
On procède par contraposée. Soit $x \in \mathbf{R}$. Supposons $x \leq 0$. On a alors $x < 2$, ce qui entraîne $|x-2| = 2-x$. Comme $x \leq 0$, il vient $|x-2| \geq 2$.

MISE EN GARDE. Considérer les propositions $P \Rightarrow Q$ et $Q \Rightarrow P$ comme équivalentes est une erreur grave et, malheureusement, trop fréquente ! Supposons, par exemple, que P désigne la proposition «n est un entier relatif» et que Q désigne la proposition «n^2 est un nombre réel positif». Alors $P \Rightarrow Q$ est vraie tandis que $Q \Rightarrow P$ est fausse.
Une autre erreur grave consiste à considérer que $P \Rightarrow Q$ et $(\text{non}\, P) \Rightarrow (\text{non}\, Q)$ sont équivalentes. En fait, $(\text{non}\, P) \Rightarrow (\text{non}\, Q)$ n'est autre que la contraposée de $Q \Rightarrow P$ et on vient de voir que cette dernière proposition n'est pas équivalente à $P \Rightarrow Q$ en général.

2.6. Preuve d'une équivalence. Pour démontrer une proposition du type $P \Leftrightarrow Q$, il faut (par définition même) démontrer les deux propositions $P \Rightarrow Q$ et $Q \Rightarrow P$. Comme on vient de le voir, ces deux dernières propositions ne sont pas équivalentes : il faut donc bien les démontrer les deux ! Bien sûr, on peut effectuer une des deux preuves (ou même les deux) par contraposée.

EXEMPLE 2.16. Démontrons la proposition «Soit $x \in \mathbf{R}$. Alors, on a $(x-1)^2 \leq 4$ si et seulement si $x \in [-1, 3]$.».
Démontrons d'abord que $x \in [-1, 3]$ implique $(x-1)^2 \leq 4$. Pour ce faire, supposons que $x \in [-1, 3]$. On a alors $|x-1| \leq 2$, d'où $(x-1)^2 \leq 4$.
Démontrons ensuite que $(x-1)^2 \leq 4$ implique $x \in [-1, 3]$. On procède par contraposée et on suppose donc que x est un nombre réel tel que $x \notin [-1, 3]$. On a alors $|x-1| > 2$, si bien que $(x-1)^2 > 4$. □

INFORMATION ESSENTIELLE SUR LES ÉQUIVALENCES.
Lorsqu'on veut prouver une proposition du type $P \Leftrightarrow Q$*, il faut s'assurer qu'on prouve bien les deux implications* $P \Rightarrow Q$ *et* $Q \Rightarrow P$*.*

Une méthode alternative pour démontrer une proposition du type $P \Leftrightarrow Q$ consiste à établir une chaîne d'équivalences "évidentes" entre les propositions P et Q.

EXEMPLE 2.17. Redémontrons la proposition «Soit $x \in \mathbf{R}$. Alors, on a $(x-1)^2 \leq 4$ si et seulement si $x \in [-1,3]$.».
On procède par chaîne d'équivalences. On a $x \in [-1,3] \Leftrightarrow |x-1| \leq 2 \Leftrightarrow (x-1)^2 \leq 4$. □

MISE EN GARDE. Ce procédé est parfois plus court que la démonstration séparée des implications $P \Rightarrow Q$ et $Q \Rightarrow P$. Il est cependant dangereux, car on a vite fait de glisser une implication (unidirectionnelle) dans la chaîne à la place d'une équivalence. Lorsqu'on utilise une chaîne d'équivalences, il faut être absolument certain d'avoir une véritable équivalence à chaque étape, et le justifier lorsque c'est nécessaire !

2.7. Raisonnement au cas par cas. Il peut s'appliquer pour démontrer des propositions du type $(P_1 \text{ ou } P_2 \text{ ou } \ldots \text{ ou } P_k) \Rightarrow Q$. Pour démontrer une telle implication, on démontre séparément les propositions $P_1 \Rightarrow Q$, $P_2 \Rightarrow Q$, ... et $P_k \Rightarrow Q$. On peut présenter la preuve comme suit :

1er cas: Supposons que P_1 est vraie. ... On a prouvé Q.

2e cas: Supposons que P_2 est vraie. ... On a prouvé Q.

...

ke cas: Supposons que P_k est vraie. ... On a prouvé Q.

EXEMPLE 2.18. Démontrons que pour tout $a \in \mathbf{R}$, le système d'équations

$$(*) \begin{cases} ax & + & y & = & 2a \\ -ax & + & (a^2-1)y & = & 0 \end{cases}.$$

possède une solution dans $\mathbf{R}^2$.
Pour ce faire, on distingue deux cas :

1er cas: Supposons que $a = 0$. On voit que si on pose $x = 0$ et $y = 0$, $(*)$ est satisfait.

2e cas: Supposons que $a \neq 0$. En ajoutant la première ligne à la seconde, on voit que $(*)$ est équivalent à

$$(**) \begin{cases} ax & + & y & = & 2a \\ & & a^2y & = & 2a \end{cases}.$$

On trouve alors une solution en posant $y = \frac{2}{a}$ et $x = 2 - \frac{2}{a^2}$.

Dans les deux cas, on a trouvé une solution de $(*)$ dans $\mathbf{R}^2$. □

MISE EN GARDE. Dans un raisonnement au cas par cas, il faut être certain de traiter tous les cas possibles. Autrement dit, il faut veiller à ne pas oublier de cas. Dans l'exemple précédent, il est évident que l'un des deux cas doit se produire. Cependant, il peut arriver qu'il faille commencer par prouver qu'un cas au moins, parmi une certaine liste, doit se produire. Ensuite, on peut entamer un raisonnement au cas par cas.

2.8. Raisonnement par l'absurde. Le schéma d'un raisonnement par l'absurde pour démontrer une proposition P est le suivant :

(1) On suppose que la proposition P est fausse ;

(2) On montre que cela mène à une contradiction, c'est-à-dire à une proposition qui doit être vraie et fausse ;

(3) On en déduit que P est vraie.

EXEMPLE 2.19. Démontrons que l'équation $2x^7 - 4x^4 + 4x^2 = 6x^6 + 3$ ne possède pas de solution entière.
Supposons par l'absurde qu'un nombre entier n soit solution de cette équation. On a alors $2n^7 - 4n^4 + 4n^2 = 6n^6 + 3$. Mais c'est impossible, car le membre de gauche est un nombre pair tandis que le membre de droite est un nombre impair. On en déduit que l'équation ne possède pas de solution entière. □

EXEMPLE 2.20. Démontrons que pour tout $x \in \mathbf{R}$, on a $|x + 3| \geq 3$ ou $|x - 3| \geq 3$.
Par l'absurde, supposons qu'il existe $x \in \mathbf{R}$ tel que $|x + 3| < 3$ et $|x - 3| < 3$. On en déduit $|3 - x| < 3$, puis

$$|6| = |(x + 3) + (3 - x)| \leq |x + 3| + |3 - x| < 3 + 3 = 6,$$

ce qui est impossible, car $|6| = 6$. □

REMARQUE 2.21. Il est fréquent, comme dans l'exemple précédent, de ne pas écrire l'étape (3) du raisonnement par l'absurde si le contexte est suffisamment clair. Néanmoins, au début, il est conseillé de toujours l'écrire.

EXERCICE 2.22. Démontrer que le nombre $\sqrt{2}$ est irrationnel.

L'utilisation du raisonnement par l'absurde se justifie comme suit. L'hypothèse que P est fausse nous mène à une contradiction. En vertu du principe de non contradiction, on est conduit à écarter cette hypothèse. Finalement, la proposition P n'étant pas fausse, le principe du tiers exclu implique qu'elle est vraie.

Parmi les raisonnements par l'absurde, on trouve les arguments de comptage, déjà évoqués dans la section 2.1. Revoyons l'exemple 2.2, en explicitant la structure de raisonnement par l'absurde.

EXEMPLE 2.23. On rappelle qu'un nombre naturel n est un *carré* s'il s'écrit sous la forme k^2, avec $k \in \mathbf{N}$. (Re)démontrons la proposition «Il existe $x \in \mathbf{N}$ tel que $x \leq 30$ et x n'est pas un carré».
Soit $A = \{0, 1, \ldots, 30\}$ et $B = \{x \in A : x \text{ est un carré}\}$. On doit montrer qu'il existe $x \in A$ tel que $x \notin B$.

Pour ce faire, supposons par l'absurde que tout élément x de A est également dans B. On en déduit $A = B$, car il est évident que les éléments de B sont dans A. L'ensemble A possède 31 éléments. En revanche, dès que $k \geq 6$, on a $k^2 > 30$, d'où $x \notin B$. Par conséquent B possède seulement 6 éléments (au plus). Ceci contredit l'égalité $A = B$ démontrée plus haut. □

2.9. Raisonnement par récurrence (ou induction). Le raisonnement par récurrence se fonde sur le principe suivant, qui est une propriété fondamentale des nombres naturels.

PRINCIPE DE RÉCURRENCE (FORME FAIBLE). *Soit $a \in \mathbf{N}$. Pour tout $n \in \mathbf{N}$ tel que $n \geq a$, on se donne une proposition $P(n)$. Supposons que :*

(1) *la proposition $P(a)$ est vraie ;*

(2) *pour tout $k \in \mathbf{N}$ tel que $k \geq a$, la proposition $[P(k) \Longrightarrow P(k+1)]$ est vraie.*

Alors, pour tout $n \in \mathbf{N}$ tel que $n \geq a$, la proposition $P(n)$ est vraie.

EXEMPLE 2.24. Démontrons que pour tout entier naturel n, on a $2^n > n$.
On utilise le principe de récurrence (avec $a = 0$), en choisissant pour $P(n)$ la proposition «$2^n > n$». Premièrement, on a $2^0 = 1 > 0$, si bien que $P(0)$ est vraie. Deuxièmement, démontrons que pour tout $k \in \mathbf{N}$, on a $P(k) \Longrightarrow P(k+1)$. Pour ce faire, fixons k et supposons que $P(k)$ est vraie. On a donc $2^k > k$. Dès lors, il vient $2^{k+1} = 2 \cdot 2^k = 2^k + 2^k \geq 2^k + 1 > k + 1$; la dernière inégalité résulte de l'hypothèse de récurrence. Ainsi $P(k+1)$ est vraie.
On applique alors le principe de récurrence, qui entraîne $2^n > n$ pour tout $n \in \mathbf{N}$. □

En règle générale, on ne fait pas référence explicitement à une proposition $P(n)$ ou au principe de récurrence. Le raisonnement qui précède sera plutôt présenté comme suit.

EXEMPLE 2.25. (Re)démontrons que pour tout entier naturel n, on a $2^n > n$.
On procède par récurrence.
Initialisation (pour $n = 0$) : on a $2^0 = 1 > 0$.
Hypothèse de récurrence : on suppose que $2^k > k$.
Hérédité : par calcul, on trouve $2^{k+1} = 2 \cdot 2^k = 2^k + 2^k \geq 2^k + 1 > k + 1$, où la dernière inégalité résulte de l'hypothèse de récurrence. □

EXEMPLE 2.26. Démontrons que pour tout $n \in \mathbf{N}^*$, la fonction $f_n : \mathbf{R} \to \mathbf{R}; x \mapsto x^n$ est dérivable et que sa dérivée satisfait la formule $f_n'(x) = nx^{n-1}$.
Initialisation (pour $n = 1$) : On a $f_1(x) = x$ pour tout x. Donc f_1 est dérivable et on a $f_1'(x) = 1 = 1x^{1-1}$.
Hypothèse de récurrence : on suppose que $k \geq 1$, que f_k est dérivable et que $f_k'(x) = kx^{k-1}$.
Hérédité : on a $f_{k+1} = f_1 \cdot f_k$. Donc, par la formule de dérivation d'un produit, f_{k+1} est dérivable et on trouve

$$f_{k+1}'(x) = f_1'(x)f_k(x) + f_1(x)f_k'(x) = 1 \cdot x^k + x \cdot k \cdot x^{k-1} = (k+1)x^k \ .$$

C'est la formule qu'il fallait démontrer. □

EXERCICE 2.27. Démontrer qu'il n'existe aucune suite $(x_n)_{n \in \mathbf{N}}$ d'entiers naturels qui soit *strictement décroissante*, c'est-à-dire telle que $x_{n+1} < x_n$ pour tout $n \in \mathbf{N}$.

Dans certains cas, le principe de récurrence ne suffit pas ; on doit alors le renforcer. L'énoncé ci-dessous est en apprence plus fort que la forme faible du principe de récurrence (d'où le nom «forme forte»). Cependant, il peut être démontré à partir de la forme faible, ce que nous ne faisons pas ici.

Principe de récurrence (forme forte).
Soit $a \in \mathbf{N}$. Pour tout $n \in \mathbf{N}$ tel que $n \geq a$, on se donne une proposition $P(n)$. Supposons que :

(1) *la proposition $P(a)$ est vraie ;*

(2) *pour tout $k \in \mathbf{N}$ tel que $k \geq a$, la proposition $\big[\big(P(a)\,\text{et}\,P(a+1)\,\text{et}\ldots\text{et}\,P(k)\big) \Rightarrow P(k+1)\big]$ est vraie.*

Alors, pour tout $n \in \mathbf{N}$ tel que $n \geq a$, la proposition $P(n)$ est vraie.

Pour l'exemple qui suit, on donne une définition qui sera très importante dans le chapitre d'arithmétique entière.

Définition 2.28. *Un nombre naturel n est* premier *si $n \geq 2$ et si pour tous $a, b \in \mathbf{N}$, on a $n = ab \Rightarrow (a = 1\,\text{ou}\,b = 1)$.*

Autrement dit, n est premier si $n \geq 2$ et si les seules manières de l'écrire comme produit de nombres naturels sont $n = 1 \cdot n$ et $n = n \cdot 1$. A titre d'exemple, signalons que les nombres premiers inférieurs ou égaux à 20 sont $2, 3, 5, 7, 11, 13, 17$ et 19.

Exemple 2.29. Démontrons que pour tout nombre naturel $n \geq 2$, il existe $k \in \mathbf{N}^*$ et des nombres premiers $p_1, \ldots, p_k$ tels que $n = p_1 \cdots p_k$.
On procède par récurrence forte.
Initialisation (pour $n = 2$) : le nombre 2 est premier. On peut donc prendre $k = 1$ et $p_1 = 2$ dans ce cas.
Hypothèse de récurrence : supposons que pour tout $\lambda \in \mathbf{N}$ tel que $2 \leq \lambda \leq n$, il existe $k \in \mathbf{N}$ et des nombres premiers $q_1, \ldots q_k$ tels que $\lambda = q_1 \cdots q_k$.
Hérédité : on doit prouver qu'il existe $k \in \mathbf{N}^*$ et des nombres premiers $p_1, \ldots, p_k$ tels que $n + 1 = p_1 \cdots p_k$. On distingue deux cas :

1^{er} cas : supposons que $n + 1$ est premier. Dans ce cas, on peut prendre $k = 1$ et $p_1 = n + 1$.

2^{e} cas : supposons que $n + 1$ n'est pas premier. On peut alors écrire $n + 1 = \mu\nu$, avec $\mu, \nu \neq 1$. On doit alors avoir $2 \leq \mu, \nu \leq n$. Par hypothèse de récurrence, il existe $s, t \in \mathbf{N}$ et des nombres premiers $q_1, \ldots q_s, r_1, \ldots, r_t$ tels que

$$\mu = q_1 \cdots q_s \quad \text{et} \quad \nu = r_1 \cdots r_t \ .$$

On en déduit $n+1 = q_1 \cdots q_s \cdot r_1 \cdots r_t$. Donc $n+1$ a la forme souhaitée (avec $k = s+t$).

Dans les deux cas, on a bien trouvé un entier naturel k et des nombres premiers $p_1, \ldots, p_k$ tels que $n + 1 = p_1 \cdots p_k$. □

Exercice 2.30. Soit $(x_n)_{n \in \mathbf{N}^*}$ une suite de nombres réels telle que $x_1 < 1$, et $x_{n+1} < \frac{2}{n} \sum_{k=1}^{n} x_k$ pour tout $n \in \mathbf{N}^*$. Démontrer que $x_n < n$ pour tout $n \in \mathbf{N}^*$.

On termine ce hapitre avec deux exercices sur la récurrence formulés en langue naturelle.

Exercice 2.31. Le raisonnement par récurrence suivant est-il correct ?

« *On va démontrer que dans un groupe d'étudiants, tous ont toujours les yeux de la même couleur. Pour ce faire, on procède par récurrence sur le nombre d'étudiants du groupe. Si le groupe compte un seul étudiant, il n'y a rien à démontrer (ancrage).*

« *On pose alors l'hypothèse de récurrence suivante : si le groupe compte n étudiants, alors tous ont les yeux de la même couleur.*

« *On doit maintenant démontrer que si le groupe compte $n+1$ étudiants, alors tous ont les yeux de la même couleur. On fait sortir un étudiant et on obtient ainsi un groupe de n étudiants, qui ont tous les yeux de la même couleur (par hypothèse). On fait alors sortir un autre étudiant (et rentrer l'étudiant précédent) ; on obtient à nouveau un groupe de n étudiants, qui ont tous les yeux de la même couleur (par hypothèse). Par conséquent tous les étudiants du groupe ont les yeux de la même couleur. CQFD* »

Si vous pensez que le raisonnement est incorrect, explicitez l'erreur le plus précisément possible.

Exercice 2.32. Un contrôleur passe dans un wagon de chemin de fer et annonce aux passagers : «Certains d'entre vous ont le visage sale. Il n'est pas possible de se laver dans le train, mais à partir du prochain arrêt, il sera possible de se laver dans chaque gare.»
On suppose que :
- chaque passager peut voir les visages de tous les autres, mais n'a aucun moyen de voir le sien ;
- les passagers sont trop timides pour demander à quelqu'un d'autre s'ils sont sales ;
- les passagers sont trop paresseux pour descendre se laver dans une gare s'ils ne sont pas certains d'être sales ;
- personne ne descend du train pour d'autres raisons que pour se laver ;
- les passagers descendent se laver dans une gare dès qu'ils sont certains d'être sales ;
- les passagers sont capables de déduire les conséquences logiques de ce qu'ils voient (et en particulier des actes des autres).

Notons n le nombre de passagers qui ont le visage sale. Expliquer pourquoi ces n passagers descendront tous du train à la n-ième gare (ou avant) pour se laver.

Notons que ce dernier exercice n'a pas la rigueur qu'on exige habituellement d'un exercice de mathématiques : on ne peut pas donner suffisamment de précisions sur les hypothèses. On le donne néanmoins en raison de son côté amusant.

CHAPITRE 2

Ensembles et applications

Référence. Pour préparer ce chapitre, je me suis notamment inspiré du chapitre 2 de l'ouvrage suivant : François Liret et Dominique Martinais, *Cours de mathématiques : Algèbre 1re année*, Dunod, 1997.

1. Ensembles

1.1. Egalité et inclusion. On adopte ici une approche totalement naïve de la théorie des ensembles. Un ensemble est vu comme une collection d'objets, ses *éléments*. On considère que seuls les éléments permettent de distinguer les ensembles. Autrement dit, on adopte le principe suivant.

Principe (d'égalité des ensembles). *Deux ensembles sont égaux si et seulement s'ils possèdent les mêmes éléments.*

Introduisons quelques notations. Pour dire que a est un élément d'un ensemble E, on écrit $a \in E$. On dit aussi que «a appartient à E». La notation $a \notin E$ signifie que a n'est pas un élément de E. On dit aussi que «a n'appartient pas à E».

On peut définir un ensemble en donnant la liste de ses éléments (par exemple $A = \{0, 1, 2, 3, 4\}$ ou $B = \{1, 2, 4, 8, 16, 32\}$). On peut aussi le définir à partir d'un ensemble plus grand en ne conservant que les éléments satisfaisant une propriété (par exemple $C = \{n \in \mathbf{N} : n \text{ est pair}\}$ ou $D = \{x \in \mathbf{R} : x^2 - 3x + 2 \leq 0\}$). Décrivons l'ensemble B ci-dessus de cette manière :

$$B = \{n \in \mathbf{N} : \text{ il existe } k \in \mathbf{N} \text{ tel que } n = 2^k \text{ et } n \leq 40\} \ .$$

Remarque 1.1. Les deux-points apparaissant dans les définitions d'ensembles qui précèdent signifient «tel que». Beaucoup d'auteurs utilisent plutôt une barre verticale ou une barre oblique. Ils écrivent donc $C = \{n \in \mathbf{N} | n \text{ est pair}\}$ ou $C = \{n \in \mathbf{N} / n \text{ est pair}\}$.

Exemple 1.2 (les intervalles bornés de $\mathbf{R}$). Soit a, b deux nombres réels. On pose :

$$\begin{aligned} [a,b] &= \{x \in \mathbf{R} : a \leq x \leq b\} \\ ]a,b] &= \{x \in \mathbf{R} : a < x \leq b\} \\ [a,b[&= \{x \in \mathbf{R} : a \leq x < b\} \\ ]a,b[&= \{x \in \mathbf{R} : a < x < b\} \end{aligned}$$

Lorque $E = \mathbf{N}, \mathbf{Z}, \mathbf{Q}, \mathbf{R}$ ou $\mathbf{C}$, on notera E^* l'ensemble E privé de 0. Autrement dit, on pose

$$E^* = \{x \in E : x \neq 0\} \ .$$

Lorque $E = \mathbf{Z}, \mathbf{Q}$ ou $\mathbf{R}$, on pose $E_+ = \{x \in E : x \geq 0\}$ et $E_- = \{x \in E : x \leq 0\}$. Il est alors cohérent d'écrire $E_+^* = \{x \in E : x > 0\}$ et $E_-^* = \{x \in E : x < 0\}$.

Lorque le contexte est suffisamment clair, on s'autorisera à ne pas citer explicitement l'ensemble ambiant. On écrira par exemple $\{\frac{1}{n} : n \in \mathbf{N}^*\}$ au lieu de $\{x \in \mathbf{R} : \exists n \in \mathbf{N}^* \text{ tel que } x = \frac{1}{n}\}$.

DÉFINITION 1.3. *Soit A, B deux ensembles.*

(1) *On dit que A est* inclus *dans B et on note $A \subseteq B$ (ou $B \supseteq A$), si tout élément de A est également élément de B. On dit aussi que A est une* partie*, ou un* sous-ensemble*, de B.*

(2) *On dit que A est* strictement inclus *dans B et on note $A \subsetneq B$ (ou $B \supsetneq A$), si on a $A \subseteq B$ et $A \neq B$. On dit aussi que A est une* partie stricte*, ou un* sous-ensemble strict*, de B.*

REMARQUE 1.4. Beaucoup d'auteurs utilisent la notation $A \subset B$ pour signifier que A est inclus (pas forcément strictement) dans B. Cependant, d'autres l'utilisent pour signifier que A est strictement inclus dans B. En raison de cette ambiguité, nous ne l'utiliserons pas dans ce polycopié.

EXEMPLE 1.5 (ensembles de nombres fondamentaux). On a les inclusions (strictes)

$$\mathbf{N} \subsetneq \mathbf{Z} \subsetneq \mathbf{Q} \subsetneq \mathbf{R} \subsetneq \mathbf{C} .$$

EXEMPLE 1.6. L'ensemble ne contenant aucun élément est appelé *ensemble vide* et noté $\varnothing$. Pour tout ensemble E, on a $\varnothing \subseteq E$.

REMARQUE 1.7. Pour tous ensembles A, B, C, on a :

(1) $A \subseteq B \subseteq C \Longrightarrow A \subseteq C$;

(2) $A \subsetneq B \subseteq C \Longrightarrow A \subsetneq C$;

(3) $A \subseteq B \subsetneq C \Longrightarrow A \subsetneq C$.

Avec la notion d'inclusion, on obtient la reformulation suivante du principe d'égalité.

PROPRIÉTÉ DE LA DOUBLE INCLUSION.
Soit A, B deux ensembles. On a $A = B$ si et seulement si $A \subseteq B$ et $B \subseteq A$.

DÉMONSTRATION. Si $A = B$, on a $A \subseteq B$ et $B \subseteq A$ par définition. Réciproquement, supposons que $A \subseteq B$ et $B \subseteq A$. Considérons un objet x quelconque :

(1) On a $x \in A \Rightarrow x \in B$, car $A \subseteq B$;

(2) On a $x \in B \Rightarrow x \in A$, car $B \subseteq A$.

Par conséquent, on a $x \in A \Longleftrightarrow x \in B$, et donc A et B ont les mêmes éléments. On a prouvé que $A = B$. □

On utilise énormément la proriété de la double inclusion pour prouver des égalités ensemblistes. On dit alors qu'on fait une *preuve par double inclusion.*

EXEMPLE 1.8. Démontrons que les ensembles $A = \{0, 1\}$ et $B = \{x \in \mathbf{R} : x^2 = x\}$ sont égaux.
On a l'inclusion $A \subseteq B$, car $0^2 = 0$ et $1^2 = 1$.
Démontrons maintenant que $B \subseteq A$. Pour ce faire, considérons un élément $x \in B$. On a alors $x^2 = x$, et donc $x(x-1) = 0$. Par conséquent, il vient $x = 0$ ou $x - 1 = 0$, c'est-à-dire $x = 0$ ou $x = 1$. Dans les deux cas, on a $x \in A$. □

1.2. Opérations sur les ensembles.

DÉFINITION 1.9.
Soit A et B deux ensembles :

(1) *la* réunion *de A et B, notée $A \cup B$, est l'ensemble des objets qui appartiennent à un (au moins) des ensembles A et B ;*

(2) *l'*intersection *de A et B, notée $A \cap B$, est l'ensemble des objets qui appartiennent à la fois à A et à B ;*

(3) *la* différence ensembliste *de B et A, notée $B \setminus A$ est l'ensemble $\{x \in B : x \notin A\}$. On l'appelle également B* privé de *A.*

REMARQUE 1.10. Soit x un objet et A, B deux ensembles. Par définition, on a :

(1) $x \in A \cup B \iff (x \in A \text{ ou } x \in B)$;

(2) $x \in A \cap B \iff (x \in A \text{ et } x \in B)$.

EXEMPLE 1.11. Posons $A = \{0, 2, 4, 6, 8\}$ et $B = \{0, 2, 3, 5, 7\}$. On a alors $A \cap B = \{0, 2\}$, $A \cup B = \{0, 2, 3, 4, 5, 6, 7, 8\}$, $B \setminus A = \{3, 5, 7\}$ et $A \setminus B = \{4, 6, 8\}$.

EXEMPLE 1.12. Posons $A =]1, 3[$ et $B = [2, 4]$. On a alors $A \cap B = [2, 3[$, $A \cup B =]1, 4]$, $B \setminus A = [3, 4]$ et $A \setminus B =]1, 2[$.

REMARQUE 1.13. Pour tous ensembles A, B, on a :

(1) $A \subseteq A \cup B$ et $B \subseteq A \cup B$;

(2) $A \cap B \subseteq A$ et $A \cap B \subseteq B$.

LEMME 1.14. *Soit A, B, C trois ensembles. On a les équivalences suivantes :*

$$A \cup B \subseteq C \iff (A \subseteq C \text{ et } B \subseteq C) \qquad ; \qquad A \cap B \supseteq C \iff (A \supseteq C \text{ et } B \supseteq C)$$

DÉMONSTRATION. Démontrons l'implication $A \cup B \subseteq C \Rightarrow (A \subseteq C \text{ et } B \subseteq C)$. Supposons donc que $A \cup B \subseteq C$. On a alors $A \subseteq A \cup B \subseteq C$ et $B \subseteq A \cup B \subseteq C$.

Passons maintenant à l'implication $(A \subseteq C \text{ et } B \subseteq C) \Rightarrow A \cup B \subseteq C$. Supposons donc que $A \subseteq C$ et $B \subseteq C$ et montrons que $A \cup B \subseteq C$. Pour ce faire, considérons un élément $x \in A \cup B$. On a alors $x \in A$ ou $x \in B$; on distingue donc deux cas.

1^{er} cas : On suppose que $x \in A$. On a alors $x \in C$ puisque $A \subseteq C$.

2^{e} cas : On suppose que $x \in B$. On a alors $x \in C$ puisque $B \subseteq C$.

Dans les deux cas, on a prouvé que $x \in C$. Ceci prouve que $A \cup B \subseteq C$, comme souhaité. □

EXERCICE 1.15. Démontrer la seconde équivalence du lemme de manière similaire.

PROPOSITION 1.16.
Soit A, B, C trois ensembles. Les propriétés suivantes sont satisfaites :

$$A \cup (B \cup C) = (A \cup B) \cup C \quad ; \quad A \cup B = B \cup A$$
$$A \cap (B \cap C) = (A \cap B) \cap C \quad ; \quad A \cap B = B \cap A$$

DÉMONSTRATION. Démontrons l'inclusion $A \cup (B \cup C) \subseteq (A \cup B) \cup C$. On a $B \subseteq A \cup B \subseteq (A \cup B) \cup C$ et $C \subseteq (A \cup B) \cup C$; le lemme 1.14 donne donc $B \cup C \subseteq (A \cup B) \cup C$. En outre, on a $A \subseteq A \cup B \subseteq (A \cup B) \cup C$. Une nouvelle application du lemme 1.14 donne $A \cup (B \cup C) \subseteq (A \cup B) \cup C$. L'inclusion $A \cup (B \cup C) \supseteq (A \cup B) \cup C$ se prouve de manière analogue ; on obtient donc l'égalité $A \cup (B \cup C) = (A \cup B) \cup C$.

Si x est un objet quelconque, on a

$$x \in A \cup B \iff (x \in A \text{ ou } x \in B) \iff x \in B \cup A \ .$$

On a donc démontré l'égalité $A \cup B = B \cup A$. □

EXERCICE 1.17. Démontrer les dernières égalités de la proposition précédente.

EXERCICE 1.18. Démontrer (sans utiliser la proposition 1.24) que pour tout nombre naturel $n \geq 2$ et pour tous ensembles $A_1, A_2, \ldots, A_n$, on a

$$((\ldots(A_1 \cup A_2) \cup \ldots) \cup A_{n-1}) \cup A_n = A_1 \cup (A_2 \cup (\ldots \cup (A_{n-1} \cup A_n)\ldots)) \ .$$

On pourra procéder par récurrence sur $\mathbf{N}$. Démontrer également la formule similaire pour les intersections.

PROPOSITION 1.19.
Soit A, B, C trois ensembles. Les propriétés suivantes sont satisfaites :

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \qquad \text{et} \qquad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

EXERCICE 1.20. Démontrer cette proposition.

Les définitions de réunion et d'intersection se généralisent à des familles quelconques d'ensembles.

DÉFINITION 1.21. *Soit $\{A_i : i \in I\}$ une famille (ici, ce terme a le même sens que «ensemble») d'ensembles.*

(1) *La* réunion *de la famille $\{A_i\}$, notée $\bigcup_{i \in I} A_i$, est l'ensemble des objets appartenant à au moins un des ensembles de la famille $\{A_i\}$;*
(2) *L'*intersection *de la famille $\{A_i\}$, notée $\bigcap_{i \in I} A_i$, est l'ensemble des objets appartenant à tous les ensembles de la famille $\{A_i\}$.*

Lorsque $I = \{1, 2, \ldots, n\}$, on pourra noter $A_1 \cup A_2 \cup \ldots \cup A_n$ ou $\bigcup_{i=1}^{n} A_i$ au lieu de $\bigcup_{i \in I} A_i$. De même, on pourra noter $A_1 \cap A_2 \cap \ldots \cap A_n$ ou $\bigcap_{i=1}^{n} A_i$ au lieu de $\bigcap_{i \in I} A_i$.

REMARQUE 1.22. Soit $\{A_i : i \in I\}$ une famille d'ensembles et soit x un objet. Les équivalences suivantes sont des conséquences immédiates de la définition :

(1) $x \in \bigcup_{i\in I} A_i \iff$ il existe $i \in I$ tel que $x \in A_i$;
(2) $x \in \bigcap_{i\in I} A_i \iff$ pour tout $i \in I$, on a $x \in A_i$.

EXERCICE 1.23. Démontrer que $\bigcup_{n\in\mathbf{N}^*}[0, 1 - \frac{1}{n}] = [0, 1[$ et $\bigcap_{n\in\mathbf{N}^*}]-\frac{1}{n}, \frac{1}{n}[= \{0\}$.

PROPOSITION 1.24. *Soit $A_1, A_2, \ldots, A_n$ des ensembles. Démontrer les égalités :*

$$((\ldots(A_1 \cup A_2) \cup \ldots) \cup A_{n-1}) \cup A_n = \bigcup_{i=1}^{n} A_i = A_1 \cup (A_2 \cup (\ldots \cup (A_{n-1} \cup A_n)\ldots)) \ ;$$

$$((\ldots(A_1 \cap A_2) \cap \ldots) \cap A_{n-1}) \cap A_n = \bigcap_{i=1}^{n} A_i = A_1 \cap (A_2 \cap (\ldots \cap (A_{n-1} \cap A_n)\ldots)) \ .$$

EXERCICE 1.25. Démontrer cette proposition.

1.3. Ensemble des parties et complémentaire. Soit E un ensemble. On peut considérer l'ensemble des parties de E, qu'on note $\mathcal{P}(E)$. Lorsque A est inclus dans E, c'est-à-dire lorsqu'on a $A \in \mathcal{P}(E)$, la différence ensembliste $E \setminus A$ est elle-même un élément de $\mathcal{P}(E)$, qu'on appelle *complémentaire* de A dans E. S'il n'y a pas d'ambiguité sur l'ensemble ambient E, on peut écrire A^c au lieu de $E \setminus A$.

EXEMPLE 1.26. Si $E = \{0, 1, 2\}$, alors on a $\mathcal{P}(E) = \Big\{\varnothing, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, E\Big\}$. Si $A = \{0\}$, on a $A^c = \{1, 2\}$

REMARQUE 1.27. Quel que soit l'ensemble ambiant E, on a $\varnothing^c = E$ et $E^c = \varnothing$.

PROPOSITION 1.28. *Soit A et B des parties d'un ensemble E. On a alors :*

$$(A^c)^c = A \qquad ; \qquad (A \cap B)^c = A^c \cup B^c \qquad ; \qquad (A \cup B)^c = A^c \cap B^c$$

EXERCICE 1.29. Démontrer cette proposition.

1.4. Produit cartésien. Soit E et F deux ensembles. Le *produit cartésien* de E et F est l'ensemble, noté $E \times F$, dont les éléments sont les couples de la forme (x, y) avec $x \in E$ et $y \in F$. Deux tels couples (x, y) et (x', y') sont égaux si et seulement si $x = x'$ et $y = y'$. En particulier, l'ordre des éléments compte ! Même si $F = E$, on n'a $(x, y) = (y, x)$ que lorsque $x = y$. Lorsque $F = E$, on peut écrire E^2, à la place de $E \times E$.

EXEMPLE 1.30. Moyennant le choix d'un repère cartésien (orthonormé) du plan :

(1) $\mathbf{R}^2 = \mathbf{R} \times \mathbf{R}$ paramètre les points du plan ;
(2) $[0, 1]^2$ paramètre un carré ;
(3) $[0, 1] \times [0, 2]$ paramètre un rectangle.

Plus généralement, si $E_1, E_2, \ldots, E_n$ sont des ensembles, on note $E_1 \times \ldots \times E_n$ l'ensemble formé des n-uplets de la forme $(x_1, \ldots, x_n)$ avec $x_i \in E_i$ pour tout i. Deux tels n-uplets $(x_1, \ldots, x_n)$ et $(x'_1, \ldots, x'_n)$ sont égaux si et seulement si $x_i = x'_i$ pour tout i. Lorsque $E_1 = E_2 = \ldots = E_n = E$, on écrit E^n au lieu de $E \times E \times \ldots \times E$.

2. Applications

Soit E et F des ensembles. Une *application* de E dans F associe à CHAQUE élément x de E un UNIQUE élément de F, qu'on note $f(x)$. Cet élément s'appelle l'*image* de x par f. La notation $f : E \to F$ signifie que f est une application de E dans F. Lorsqu'on veut expliciter l'élément de F associé à x, on note $f : E \to F; x \mapsto f(x)$.

EXEMPLE 2.1. Soit E un ensemble. L'*application identité* de E est l'application, notée id, de E dans E, qui à chaque élément $x \in E$ associe x lui-même. On peut noter

$$\mathrm{id} : E \to E \ ; \ x \mapsto x \ .$$

EXEMPLE 2.2. La notation $f : \mathbf{R} \to \mathbf{R}; x \mapsto x^2$ désigne l'application de $\mathbf{R}$ dans $\mathbf{R}$ qui à chaque nombre réel associe son carré.

MISE EN GARDE. Il arrive qu'on parle d'application de E *vers* F, plutôt que d'application de E *dans* F. La signification est la même. Par contre, une application de E *sur* F est une application de E dans F qui est de plus SURJECTIVE (voir plus loin pour la définition).

De manière analogue à ce qu'on a fait pour les ensembles, on considère que seules les images des éléments de E permettent de différencier deux applications de E dans F. On adopte le principe suivant.

PRINCIPE (D'ÉGALITÉ DES APPLICATIONS).
Deux applications $f : E \to F$ et $f' : E' \to F'$ sont égales si et seulement si on a $E = E'$, $F = F'$ et $f(x) = f'(x)$ pour tout $x \in E$.

DÉFINITION 2.3. *Soit $f : E \to F$ une application. Le* graphe *de f est l'ensemble*

$$Gr(f) = \{(x, y) \in E \times F : y = f(x)\} = \{(x, f(x)) : x \in E\} \ .$$

2.1. Applications injectives et surjectives.

DÉFINITION 2.4.
Une application $f : E \to F$ est dite :

(1) injective *si pour tous $x, x' \in E$ tels que $f(x) = f(x')$, on a $x = x'$;*
(2) surjective *si pour tout $y \in F$, il existe $x \in E$ tel que $f(x) = y$;*
(3) bijective *si elle est injective et surjective.*

EXEMPLE 2.5. L'application $f_1 : \mathbf{R} \to \mathbf{R}; x \to \sin x$ n'est ni injective, ni surjective. En effet, on a $f(0) = f(2\pi)$ et -2 n'est l'image d'aucun nombre réel.

EXEMPLE 2.6. L'application $f_2 : \mathbf{R} \to \mathbf{R}_+; x \to |x|$ est surjective, mais pas injective. En effet, pour tout $y \in \mathbf{R}_+$, on a $y \in \mathbf{R}$ et $f_2(y) = y$. Donc f_2 est surjective. En revanche, on a $f(-2) = 2 = f(2)$, si bien que f_2 n'est pas injective.

EXEMPLE 2.7. L'application $f_3 : \mathbf{R}^* \to \mathbf{R}^*; x \mapsto \frac{1}{x}$ est bijective. En effet, pour tout $y \in \mathbf{R}^*$, on a $\frac{1}{y} \in \mathbf{R}^*$ et $f_3(\frac{1}{y}) = y$. Donc f_3 est surjective. En outre, si $x, x' \in \mathbf{R}^*$ satisfont $f_3(x) = f_3(x') =: y$, on a $x = \frac{1}{y} = x'$. Donc f_3 est injective.

EXEMPLE 2.8. L'application $f_4 : \mathbf{R}_+^* \to \mathbf{R}; x \mapsto \frac{1}{x}$ est injective, mais pas surjective. En effet, -1 n'est l'image d'aucun nombre réel positif. Par conséquent f_4 n'est pas surjective. Par contre, si $x, x' \in \mathbf{R}_+^*$ satisfont $f_4(x) = f_4(x') =: y$, alors on a $x = \frac{1}{y} = x'$. Donc, f_4 est injective.

REMARQUE 2.9. Une application $f : E \to F$ est injective si et seulement si, pour tous $x, x' \in E$ tels que $x \neq x'$, on a $f(x) \neq f(x')$. Cette caractérisation s'obtient en contraposant la définition.

PROPOSITION 2.10. *Une application $f : E \to F$ est bijective si et seulement si, pour tout $y \in F$, il existe un* UNIQUE *$x \in E$ tel que $y = f(x)$.*

DÉMONSTRATION. Supposons d'abord que f est bijective. Soit $y \in F$. Il existe $x \in E$ tel que $y = f(x)$ car f est surjective. De plus, si $x' \in E$ satisfait aussi $f(x') = y$, on a $f(x) = f(x')$ et donc $x' = x$ puisque f est injective. Ceci prouve l'unicité de x.

Supposons ensuite que pour tout $y \in F$, il existe un unique $x \in E$ tel que $y = f(x)$. En particulier, f est surjective. De plus, si x', x'' satisfont $f(x') = f(x'') =: y$, alors on a $x' = x''$ par unicité de l'élément $x \in E$ tel que $y = f(x)$. Donc f est aussi injective ; donc elle est bijective. □

2.2. Applications composées et applications inverses.

DÉFINITION 2.11.
Soit $f : E \to F$ et $g : F \to G$ des applications. La composée *de f et g est l'application $g \circ f$ de E dans G définie par la formule $(g \circ f)(x) = g(f(x))$.*

EXEMPLE 2.12. On a $\mathrm{id}_F \circ f = f$ pour toute application $f : E \to F$ et $g \circ \mathrm{id}_F = g$ pour toute application $g : F \to G$.

PROPOSITION 2.13. *Soit $f : E \to F$, $g : F \to G$ et $h : G \to H$ des applications. Alors, on a $h \circ (g \circ f) = (h \circ g) \circ f$.*

DÉMONSTRATION. Premièrement, $h \circ (g \circ f)$ et $(h \circ g) \circ f$ sont toutes deux des applications de E dans H. De plus, pour tout $x \in E$, on a $[h \circ (g \circ f)](x) = h(g \circ f(x)) = h(g(f(x))) = (h \circ g)(f(x)) = [(h \circ g) \circ f](x)$. □

Sous les hypothèses de la proposition, on peut donc définir l'application $h \circ g \circ f$ sans ambiguité.

EXEMPLE 2.14. Soit les applications

$$f : \mathbf{R} \to \mathbf{C} \ ; \ t \mapsto it \qquad g : \mathbf{C} \to \mathbf{C} \ ; \ z \mapsto e^z \qquad h : \mathbf{C} \to \mathbf{R} \ ; \ z \mapsto \mathrm{Re}(z) \ .$$

Alors $h \circ g \circ f$ est l'application de $\mathbf{R}$ dans $\mathbf{R}$ définie par $h \circ g \circ f(t) = \cos(t)$. En effet, on a $h \circ g \circ f(t) = \mathrm{Re}(e^{it}) = \cos(t)$ pour tout t.

EXERCICE 2.15. Trouver deux applications $f, g : \mathbf{R} \to \mathbf{R}$ telles que $f \circ g \neq g \circ f$.

Proposition 2.16.
Soit $f : E \to F$ et $g : F \to G$ des applications.

(1) *Si f et g sont injectives, alors $g \circ f$ est injective.*
(2) *Si f et g sont surjectives, alors $g \circ f$ est surjective.*
(3) *Si $g \circ f$ est injective, alors f est injective.*
(4) *Si $g \circ f$ est surjective, alors g est surjective.*

Exercice 2.17. Démontrer cette proposition.

Définition 2.18.
Soit des applications $f : E \to F$ et $g : F \to E$. On dit que g est inverse *de f si $g \circ f = \mathrm{id}_E$ et $f \circ g = \mathrm{id}_F$. Lorsqu'il existe un inverse de f, on dit que f est* inversible.

Remarque 2.19. Soit des applications $f : E \to F$ et $g : F \to E$.

(1) L'application g est inverse de f si et seulement si $g(f(x)) = x$ pour tout $x \in E$ et $f(g(y)) = y$ pour tout $y \in F$;
(2) L'application g est inverse de f si et seulement si f est inverse de g.

Exemple 2.20. (1) L'application $g : \mathbf{R} \to \mathbf{R}$ définie par $g(x) = \frac{x}{2} - \frac{7}{2}$ est inverse de $f : \mathbf{R} \to \mathbf{R}; x \mapsto 2x + 7$;
(2) Pour tout ensemble E, l'application id_E est sa propre inverse ;
(3) L'application $f : \mathbf{R}^* \to \mathbf{R}^*; x \mapsto \frac{1}{x}$ est sa propre inverse.

Proposition 2.21. *Si une application $f : E \to F$ est inversible, alors son inverse est unique et inversible.*

Lorsqu'une application f est inversible, on notera son inverse f^{-1}.

Démonstration. Supposons f inversible et considérons deux inverses g_1, g_2 de f. On a

$$g_1 = g_1 \circ \mathrm{id}_F = g_1 \circ f \circ g_2 = \mathrm{id}_E \circ g_2 = g_2 \ ,$$

ce qui démontre l'unicité de l'inverse. Par la remarque 2.19, cet inverse est inversible. □

Théorème 2.22.
Une application $f : E \to F$ est inversible si et seulement si elle est bijective.

Démonstration. Supposons d'abord que f est inversible. Pour tout $y \in F$, on a alors $f^{-1}(y) \in E$ et $f(f^{-1}(y)) = y$, de sorte que f est surjective. De plus, si $x, x' \in E$ satisfont $f(x) = f(x')$, alors on a $x = f^{-1}(f(x)) = f^{-1}(f(x')) = x'$. Autrement dit, f est aussi injective, et donc bijective.

Supposons maintenant que f est bijective. Pour tout $y \in F$ la proposition 2.10 garantit qu'il existe un unique $x \in E$ tel que $f(x) = y$. Notons cet élément $g(y)$, ce qui définit une application $g : F \to E$. On a alors $f(g(y)) = y$ pour tout $y \in F$ par construction. Soit maintenant $x \in E$ et

posons $y = f(x)$. On a $f(g(y)) = y = f(x)$. Par construction de g, on a $x = g(y) = g(f(x))$. On a démontré que $x = g(f(x))$ pour tout $x \in E$. Par la remarque 2.19, f est inversible. □

Comme exemple d'application, on a le résultat suivant.

EXERCICE 2.23. Soit A, B des parties de $\mathbf{R}$ et soit $f : A \to B$ une application surjective et *strictement croissante*, c'est-à-dire telle que pour tous $x, y \in A$ satisfaisant $x < y$, on a $f(x) < f(y)$. Démontrer que f est inversible et que $f^{-1} : B \to A$ est strictement croissante.

Ceci permet par exemple de définir rigoureusement[1] la fonction «racine carrée». On démontre que la fonction $g : \mathbf{R}_+ \to \mathbf{R}_+; x \mapsto x^2$ est surjective[2] et strictement croissante.

Montrons d'abord que g est surjective. Soit $y \in \mathbf{R}_+$. On distingue deux cas :

1^{er} cas : Supposons que $y = 0$. Alors $y = g(0)$.

2^{e} cas : Supposons que $y > 0$. Posons $x_0 = y + 1$; on a $x_0 > 0$ et $g(x_0) = y^2 + 2y + 1 > y$. Comme on a de plus $g(0) = 0 < y$, le théorème de la valeur intermédiaire assure qu'il existe $x \in [0, x_0]$ tel que $g(x) = y$.

Dans les deux cas, on a prouvé qu'il existe $x \in \mathbf{R}_+$ tel que $g(x) = y$. Donc g est surjective.

Montrons ensuite que g est strictement croissante. Si $x, y \in \mathbf{R}_+$ satisfont $x < y$, on a $g(y) - g(x) = y^2 - x^2 = (y - x)(y + x) > 0$, car $0 < y - x \leq y + x$. Donc on a $g(x) < g(y)$, comme souhaité.

On peut donc appliquer l'exercice 2.23, qui assure que g est inversible et poser $\sqrt{x} := g^{-1}(x)$ pour tout $x \in \mathbf{R}_+$. L'exercice 2.23 assure de plus que $\sqrt{x} < \sqrt{y}$ pour tous $x, y \in \mathbf{R}_+$ tels que $x < y$.

2.3. Images directes et images réciproques.

DÉFINITION 2.24.
Soit $f : E \to F$ une application ; soit $A \subseteq E$ et $C \subseteq F$:

(1) *l'*image *de A par f est l'ensemble $f(A) := \{y \in F : \exists a \in A \text{ tel que } f(a) = y\}$;*

(2) *l'*image réciproque *de C par f est l'ensemble $f^{-1}(C) := \{x \in E : f(x) \in C\}$.*

Autrement dit, $f(A)$ est l'ensemble des images des éléments de A par f et $f^{-1}(C)$ est l'ensemble des éléments de E dont l'image par f est dans C.

REMARQUE 2.25. L'application f est surjective si et seulement si $f(E) = F$.

On prendra garde au fait que la notation $f^{-1}(C)$ s'utilise même lorsque l'application f n'est PAS inversible ! Ainsi, pour $C \subseteq F$, on peut considérer $f^{-1}(C)$, l'image réciproque de C par f, quelle que soit l'application $f : E \to F$. En revanche, pour $y \in F$, on a besoin que l'application $f : E \to F$ soit inversible pour pouvoir considérer $f^{-1}(y)$, l'image de y par l'application inverse de f.

[1] On utilise le théorème de la valeur intermédiaire, pour lequel on renvoie au module d'analyse réelle.

[2] Pour ce faire, on admet qu'elle est continue ; voir le module d'analyse réelle.

EXERCICE 2.26. Soit $f : E \to F$ une application inversible et soit $C \subseteq F$. Démontrer que l'image de C par l'application inverse f^{-1} coïncide avec l'image réciproque de C par l'application f.

Cet exercice montre que l'écriture $f^{-1}(C)$ n'est jamais ambigüe.

EXERCICE 2.27. Soit $f : \mathbf{R} \to \mathbf{R}$ l'application définie par $f(x) = |x-2|$. Vérifier rigoureusement que $f([-2,2]) = [0,4]$ et $f^{-1}([2,5]) = [-3,0] \cup [4,7]$.

PROPOSITION 2.28.
Soit $f : E \to F$ une application et soit $C, D \subseteq F$. On a :

(1) $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$;
(2) $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$;
(3) $f^{-1}(D^c) = \big(f^{-1}(D)\big)^c$.

DÉMONSTRATION. (1) On a $f^{-1}(C \cap D) \subseteq E$ et $f^{-1}(C) \cap f^{-1}(D) \subseteq E$. De plus, pour tout $x \in E$, on a

$$\begin{aligned} x \in f^{-1}(C \cap D) &\Leftrightarrow f(x) \in C \cap D \Leftrightarrow (f(x) \in C \text{ et } f(x) \in D) \Leftrightarrow \\ &\Leftrightarrow (x \in f^{-1}(C) \text{ et } x \in f^{-1}(D)) \Leftrightarrow x \in f^{-1}(C) \cap f^{-1}(D)\ . \end{aligned}$$

Par conséquent, il vient $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$.
(2) On a $f^{-1}(C \cup D) \subseteq E$ et $f^{-1}(C) \cup f^{-1}(D) \subseteq E$. De plus, pour tout $x \in E$, on a

$$\begin{aligned} x \in f^{-1}(C \cup D) &\Leftrightarrow f(x) \in C \cup D \Leftrightarrow (f(x) \in C \text{ ou } f(x) \in D) \Leftrightarrow \\ &\Leftrightarrow (x \in f^{-1}(C) \text{ ou } x \in f^{-1}(D)) \Leftrightarrow x \in f^{-1}(C) \cup f^{-1}(D)\ . \end{aligned}$$

Par conséquent, il vient $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$.
(3) On a $f^{-1}(D) \subseteq E$ et $f^{-1}(D^c) \subseteq E$. De plus, pour tout $x \in E$, on a

$$\begin{aligned} x \in f^{-1}(D^c) &\Leftrightarrow f(x) \in D^c \Leftrightarrow f(x) \notin D \Leftrightarrow \\ &\Leftrightarrow x \notin f^{-1}(D) \Leftrightarrow x \in \big(f^{-1}(D)\big)^c\ . \end{aligned}$$

Par conséquent, il vient $f^{-1}(D^c) = \big(f^{-1}(D)\big)^c$. □

On peut en fait généraliser ce résultat à des familles d'ensembles quelconques.

PROPOSITION 2.29. *Soit $f : E \to F$ une application et soit $\{C_i : i \in I\}$ une famille de parties de F. On a alors $f^{-1}(\bigcap_{i\in I} C_i) = \bigcap_{i\in I} f^{-1}(C_i)$ et $f^{-1}(\bigcup_{i\in I} C_i) = \bigcup_{i\in I} f^{-1}(C_i)$.*

EXERCICE 2.30. Démontrer cette proposition.

PROPOSITION 2.31.
Soit $f : E \to F$ une application et soit $A, B \subseteq E$. On a :

(1) $f(A \cup B) = f(A) \cup f(B)$;
(2) $f(A \cap B) \subseteq f(A) \cap f(B)$.

DÉMONSTRATION. (1) Soit $y \in f(A \cup B)$. Il existe $x \in A \cup B$ tel que $f(x) = y$. Si $x \in A$, on a $y \in f(A)$; si $x \in B$, on a $y \in f(B)$. Dans tous les cas, y appartient à $f(A) \cup f(B)$; on a donc prouvé l'inclusion $f(A \cup B) \subseteq f(A) \cup f(B)$. Soit maintenant $y \in f(A)$. Il existe $x \in A$ tel que $y = f(x)$, ce qui implique $y \in f(A \cup B)$ puisque $x \in A \cup B$. On vient de démontrer l'inclusion $f(A) \subseteq f(A \cup B)$ et on obtient $f(B) \subseteq f(A \cup B)$ de manière analogue. Par conséquent, on obtient $f(A) \cup f(B) \subseteq f(A \cup B)$ par le lemme 1.14, d'où $f(A \cup B) = f(A) \cup f(B)$.

(2) Soit $y \in f(A \cap B)$. Il existe $x \in A \cap B$ tel que $f(x) = y$. Comme $x \in A$, on a $y \in f(A)$; comme $x \in B$, on a $y \in f(B)$. Ainsi, y appartient à $f(A) \cap f(B)$; on a donc démontré l'inclusion $f(A \cap B) \subseteq f(A) \cap f(B)$. □

MISE EN GARDE. En général, l'inclusion vue au point (2) de la proposition précédente n'est pas une égalité. Par exemple, avec $A = [-2, 0]$, $B = [0, 2]$ et $f : \mathbf{R} \to \mathbf{R}; x \mapsto x^2$, on trouve $f(A \cap B) = f(\{0\}) = \{0\}$ et $f(A) \cap f(B) = [0, 4] \cap [0, 4] = [0, 4]$.

EXERCICE 2.32. Soit $f : E \to F$ une application. Trouver une condition nécessaire et suffisante sur f pour que $f(A \cap B) = f(A) \cap f(B)$ pour tous $A, B \subseteq E$.

PROPOSITION 2.33. *Soit $f : E \to F$ une application. Soit $A \subseteq E$ et $C \subseteq F$. On a :*

(1) $f^{-1}(f(A)) \supseteq A$;

(2) $f(f^{-1}(C)) \subseteq C$.

EXERCICE 2.34. Démontrer cette proposition. Pour chaque cas, trouver un exemple pour lequel on a égalité et un exemple pour lequel l'inclusion est stricte.

EXERCICE 2.35. Soit $f : E \to F$ une application :

(1) trouver une condition nécessaire et suffisante sur f pour que $f^{-1}(f(A)) = A \ \forall A \subseteq E$;

(2) trouver une condition nécessaire et suffisante sur f pour que $f(f^{-1}(C)) = C \ \forall C \subseteq F$.

3. Partitions et relations d'équivalence

DÉFINITION 3.1.
Soit E un ensemble. Une partition *de E est une famille $\{A_i : i \in I\}$ de parties non vides de E telle que :*

(1) $\bigcup_{i \in I} A_i = E$;

(2) *pour tous $i, j \in I$ tels que $A_i \neq A_j$, on a $A_i \cap A_j = \varnothing$.*

REMARQUE 3.2. Une famille de parties de E n'est rien d'autre qu'une partie de l'ensemble $\mathcal{P}(E)$. Par conséquent, une famille de parties non vides de E n'est rien d'autre qu'une partie de l'ensemble $\mathcal{P}(E) \setminus \{\varnothing\}$.

EXEMPLES. (1) Si $E \neq \varnothing$, la famille $\{E\}$, à un seul élément, est une partition de E ;

(2) Si $E = \varnothing$, la famille vide $\varnothing$ est une partition de E. C'est la seule, car la réunion d'une famille non vide de parties non vides est non vide.

(3) Pour tout ensemble E, la famille $\{\{x\} : x \in E\}$ forme une partition de E.

(4) Si $E \neq \varnothing$, les partitions de E à deux éléments sont les $\{A, A^c\}$, où $A \in \mathcal{P}(E) \setminus \{\varnothing, E\}$.

(5) Pour $i \in \{0, 1, 2, \ldots, 9\}$, notons A_i l'ensemble des nombres naturels n tels que le dernier chiffre de l'écriture de n en base 10 soit i. La famille $\{A_0, A_1, A_2, \ldots, A_9\}$ forme une partition de $\mathbf{N}$ à dix éléments.

(6) La famille $\{]n, n+1[: n \in \mathbf{Z}\}$ ne forme pas une partition de $\mathbf{R}$. En effet, on voit que $k \notin \bigcup_{n\in\mathbf{Z}}]n, n+1[$ pour tout $k \in \mathbf{Z}$ et donc $\bigcup_{n\in\mathbf{Z}}]n, n+1[\neq \mathbf{R}$.

(7) La famille $\{[n, n+1] : n \in \mathbf{Z}\}$ ne forme pas une partition de $\mathbf{R}$. En effet, on voit que $[0, 1] \cap [1, 2] \neq \varnothing$ et même $[k-1, (k-1)+1] \cap [k, k+1] = \{k\} \neq \varnothing$ pour tout $k \in \mathbf{Z}$.

PROPOSITION 3.3. *Soit $f : E \to F$ une application et soit $\{C_i : i \in I\}$ une partition de F. Alors, la famille $\{f^{-1}(C_i) : i \in I\}$ est une partition de E.*

DÉMONSTRATION. On utilise la proposition 2.29. Tout d'abord, on a

$$\bigcup_{i\in I} f^{-1}(C_i) = f^{-1}\Big(\bigcup_{i\in I} C_i\Big) = f^{-1}(F) = E\ .$$

Ensuite, si $i, j \in I$ satisfont $f^{-1}(C_i) \neq f^{-1}(C_j)$, alors on a $C_i \neq C_j$, et donc $C_i \cap C_j = \varnothing$ puisque la famille $\{C_i : i \in I\}$ est une partition. Ainsi, on a $f^{-1}(C_i) \cap f^{-1}(C_j) = f^{-1}(C_i \cap C_j) = f^{-1}(\varnothing) = \varnothing$. □

COROLLAIRE 3.4. *Soit $f : E \to F$ une application. La famille $\{f^{-1}(\{y\}) : y \in F\}$ forme une partition de E.*

Rappelons que $f^{-1}(\{y\}) = \{x \in E : f(x) = y\}$. Le corollaire signifie donc que les "courbes de niveau" de f forment une partition de E.

DÉMONSTRATION. Il suffit d'appliquer la proposition à la partition $\{\{y\} : y \in F\}$ de F. □

DÉFINITION 3.5. *Une* relation *sur un ensemble E est une application*

$$\mathcal{R} : E \times E \longrightarrow \{\text{vrai}, \text{faux}\}$$

Lorsque $\mathcal{R}(x, y) =$ vrai, on note $x\mathcal{R}y$.

EXEMPLES (DE RELATIONS). (1) La relation d'égalité $=$, sur n'importe quel ensemble E.

(2) La relation d'inclusion $\subseteq$, sur un ensemble de la forme $\mathcal{P}(E)$.

(3) La relation d'ordre $\leq$ sur $\mathbf{R}$;

(4) La relation $<$ sur $\mathbf{R}$.

DÉFINITION 3.6.
Une relation $\mathcal{R}$ sur un ensemble E est une relation d'équivalence *si :*

(1) *Pour tout $x \in E$, on a $x\mathcal{R}x$;*

(2) *Pour tous $x, y \in E$, on a $x\mathcal{R}y \iff y\mathcal{R}x$;*

(3) *Pour tous $x, y, z \in E$, on a $(x\mathcal{R}y \text{ et } y\mathcal{R}z) \implies x\mathcal{R}z$.*

Les propriétés (1), (2) et (3) sont appelées respectivement réflexivité, symétrie *et* transitivité.

EXEMPLES. (1) La relation d'égalité sur E est une relation d'équivalence.

(2) Si E est non vide, la relation d'inclusion $\subseteq$ sur $\mathcal{P}(E)$ n'est pas une relation d'équivalence. En effet, on a $\varnothing \subseteq E$, mais $E \not\subseteq \varnothing$, si bien que la propriété (2) n'est pas satisfaite. Par contre, on peut montrer que (1) et (3) sont satisfaites.

(3) La relation $\mathcal{U}$ sur $\mathbf{N}$ définie par

$$x\mathcal{U}y \iff x \text{ et } y \text{ ont le même chiffre des unités en base } 10$$

est une relation d'équivalence.

EXERCICE 3.7. (1) Soit X, Y deux ensembles et soit $\mathcal{F}(X,Y)$ l'ensemble des applications de X dans Y. Démontrer que la relation $\sim$ sur $\mathcal{F}(X,Y)$ définie par

$$f \sim g \iff \text{ l'ensemble } \{x \in X : f(x) \neq g(x)\} \text{ est fini}$$

est une relation d'équivalence.

(2) La relation d'ordre $\leq$ sur $\mathbf{R}$ est-elle une relation d'équivalence ?

PROPOSITION 3.8.
Soit $\{A_i : i \in I\}$ une partition d'un ensemble E. Alors la relation $\mathcal{R}$ sur E définie par

$$x\mathcal{R}y \iff \exists i \in I \text{ tel que } (x \in A_i \text{ et } y \in A_i)$$

est une relation d'équivalence.

DÉMONSTRATION. Premièrement, pour tout $x \in E$, il existe $i \in I$ tel que $x \in A_i$ car $\bigcup_{i\in I} A_i = E$. On a alors $(x \in A_i \text{ et } x \in A_i)$, et donc $x\mathcal{R}x$.
Deuxièmement, supposons que $x, y \in E$ satisfont $x\mathcal{R}y$. Il existe $i \in I$ tel que $(x \in A_i \text{ et } y \in A_i)$. Donc, on a $y\mathcal{R}x$.
Enfin, supposons que $x, y, z \in E$ satisfont $x\mathcal{R}y$ et $y\mathcal{R}z$. Il existe $i, j \in I$ tels que $(x \in A_i \text{ et } y \in A_i)$ et $(y \in A_j \text{ et } z \in A_j)$. Par conséquent, on a $y \in A_i \cap A_j$ et donc $A_i \cap A_j \neq \varnothing$. Comme on a affaire à une partition, il vient $A_i = A_j$, si bien que x et z appartiennent tous deux à A_i. Par conséquent, on a $x\mathcal{R}z$. □

EXEMPLE 3.9. Si on considère la partition $\{A_0, A_1, \ldots A_9\}$ de l'exemple numéro (5), alors la relation d'équivalence obtenue est la relation $\mathcal{U}$ sur $\mathbf{N}$ définie ci-dessus.

DÉFINITION 3.10. *Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E et soit $x \in E$. La* classe d'équivalence *de x dans E est l'ensemble $\{y \in E : x\mathcal{R}y\}$.*

PROPOSITION 3.11.
Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E. Etant donné $x \in E$, on note $\bar{x}$ sa classe d'équivalence. Alors, la famille $\{\bar{x} : x \in E\}$ est une partition de E.

DÉMONSTRATION. Commençons par montrer que $\bigcup_{x\in E} \bar{x} = E$. On a $\bigcup_{x\in E} \bar{x} \subseteq E$, car $\bar{x} \subseteq E$ pour tout $x \in E$. Réciproquement, si $x \in E$, on a $x\mathcal{R}x$ par réflexivité, et donc $x \in \bar{x}$ Ainsi, on a $\bigcup_{x\in E} \bar{x} \supseteq E$.

Montrons maintenant que si $x, y \in E$ satisfont $\bar{x} \neq \bar{y}$, alors $\bar{x} \cap \bar{y} = \varnothing$. On procède par contraposée et on suppose donc que $\bar{x} \cap \bar{y} \neq \varnothing$. Il existe $z \in \bar{x} \cap \bar{y}$, si bien qu'on a $x\mathcal{R}z$ et $y\mathcal{R}z$. Comme $\mathcal{R}$ est symétrique, on a aussi $z\mathcal{R}x$ et $z\mathcal{R}y$. Si $w \in \bar{y}$, on a $y\mathcal{R}w$; grâce à la transitivité, on obtient $x\mathcal{R}y$, puis $x\mathcal{R}w$, si bien que $w \in \bar{x}$. On a prouvé que $\bar{y} \subseteq \bar{x}$ et l'inclusion inverse est analogue. Par conséquent, on obtient $\bar{x} = \bar{y}$, ce qui termine notre démontration par contraposée. □

EXEMPLE 3.12. Si on part de la relation d'équivalence $\mathcal{U}$ sur $\mathbf{N}$ définie ci-dessus, on obtient la partition $\{A_0, A_1, \dots A_9\}$ de l'exemple numéro (5).

Comme l'exemple présenté le suggère, si l'on applique les deux constructions qu'on vient de voir l'une à la suite de l'autre, on retombe sur ses pieds. Plus précisément, on a le résultat suivant.

PROPOSITION 3.13.
Soit E un ensemble. Notons P l'ensemble des partitions de E et R l'ensemble des relations d'équivalence sur E. L'application $f : P \to R$ définie par la proposition 3.8 et l'application $g : R \to P$ définie par la proposition 3.11 sont inverses l'une de l'autre.

DÉMONSTRATION. Commençons par montrer que $g \circ f = \mathrm{id}_P$. Pour ce faire, considérons une partition $\{A_i : i \in I\}$ de E. Son image par f est la relation définie par

$$x\mathcal{R}y \iff \exists i \in I \text{ tel que } (x \in A_i \text{ et } y \in A_i)$$

et l'image de celle-ci par g est la partition $\{\bar{x} : x \in E\}$ des classes d'équivalence de $\mathcal{R}$. On doit donc montrer que $\{\bar{x} : x \in E\} = \{A_i : i \in I\}$.

ASSERTION. Pour tout $i \in I$ et pour tout $x \in A_i$, on a $\bar{x} = A_i$.

Si $y \in A_i$, alors, on a $(x \in A_i \text{ et } y \in A_i)$, d'où $y \in \bar{x}$. Réciproquement, si $y \in \bar{x}$, on a $x\mathcal{R}y$ et donc il existe $j \in I$ tel que $x \in A_j$ et $y \in A_j$. Mais on a alors $x \in A_i \cap A_j$. Comme on a affaire à une partition, il vient $A_i = A_j$, et donc $y \in A_i$. On obtient $\bar{x} = A_i$, ce qui démontre l'assertion.
Démontrons maintenant l'égalité $\{\bar{x} : x \in E\} = \{A_i : i \in I\}$ par double inclusion. Pour tout $x \in E$, il existe $i \in I$ tel que $x \in A_i$ car $\bigcup_{i \in I} A_i = E$ et on a alors $\bar{x} = A_i$ par l'assertion. Ainsi, on a $\{\bar{x} : x \in E\} \subseteq \{A_i : i \in I\}$. Réciproquement, Pour tout $i \in I$, l'ensemble A_i est non vide car on a une partition. En prenant $x \in A_i$, on trouve $A_i = \bar{x}$. Ainsi, on a $\{\bar{x} : x \in E\} \supseteq \{A_i : i \in I\}$.
Montrons maintenant que $f \circ g = \mathrm{id}_R$. Pour ce faire, considérons une relation d'équivalence $\mathcal{R}$ sur E. Son image par g est la partition $\{\bar{x} : x \in E\}$ des classes d'équivalence de $\mathcal{R}$ et l'image de cette dernière par f est la relation $\mathcal{S}$ définie par

$$x\mathcal{S}y \iff \exists z \in E \text{ tel que } (x \in \bar{z} \text{ et } y \in \bar{z}) \ .$$

On doit montrer que $\mathcal{R} = \mathcal{S}$, c'est-à-dire que pour tous $x, y \in E$, on a $x\mathcal{R}y \Leftrightarrow x\mathcal{S}y$. Supposons d'abord que $x\mathcal{R}y$. On a alors $y \in \bar{x}$. Par réflexivité, on a aussi $x \in \bar{x}$. Par définition, ceci entraîne $x\mathcal{S}y$. Supposons maintenant que $x\mathcal{S}y$. Il existe alors $z \in E$ tel que $x \in \bar{z}$ et $y \in \bar{z}$, c'est-à-dire tel que $z\mathcal{R}x$ et $z\mathcal{R}y$. Grâce à la symétrie et à la transitivité de $\mathcal{R}$, on trouve $x\mathcal{R}y$. On a bien montré que $\mathcal{R} = \mathcal{S}$. □

CHAPITRE 3

Arithmétique entière

1. Division dans Z

1.1. Relation de divisibilité.

Définition 1.1.
Soit $a, b \in \mathbf{Z}$. On dit que a divise *b, et on note $a|b$, s'il existe $k \in \mathbf{Z}$ tel que $b = ka$. On dit aussi que a est un* diviseur *de b, que b est un* multiple *de a ou que b est* divisible *par a.*

Exemple 1.2. (1) Le nombre 0 est divisible par a pour tout $a \in \mathbf{Z}$, car $0 = 0 \cdot a$;

(2) Les nombres 1 et -1 divisent n'importe quel entier $a \in \mathbf{Z}$, car $a = a \cdot 1 = (-a)(-1)$.

Etant donné un entier a, on note $D(a)$ l'ensemble des diviseurs de a et $M(a)$ celui des multiples de a. En formules, ceci s'écrit

$$D(a) = \{x \in \mathbf{Z} : x|a\} \quad \text{et} \quad M(a) = \{x \in \mathbf{Z} : a|x\} = \{ka : k \in \mathbf{Z}\} \ .$$

Remarque 1.3. Si $a \neq 0$, alors $D(a)$ est fini. En effet, si $x \in D(a)$, il existe $y \in \mathbf{Z}$ tel que $xy = a$. On a $y \neq 0$ et $|x| \cdot |y| = |a|$. Comme $|y| \geq 1$, il vient $|x| \leq |a|$. Ainsi, on a $D(a) \subseteq \{-|a|, \ldots, -1, 0, 1, \ldots, |a|\}$.

Remarque 1.4. Si $a \neq 0$, alors $M(a)$ est infini, car $M(a) = \{ax : x \in \mathbf{Z}\}$ et $(x \neq y \Rightarrow ax \neq ay)$.

Exemples. On a :

(1) $D(0) = \mathbf{Z}$ et $M(0) = \{0\}$.

(2) $D(1) = D(-1) = \{\pm 1\}$ et $M(1) = M(-1) = \mathbf{Z}$.

(3) $D(10) = \{\pm 1, \pm 2, \pm 5, \pm 10\}$.

(4) $D(12) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$.

(5) $M(10) = \{10x : x \in \mathbf{Z}\} = \{0, \pm 10, \pm 20, \pm 30, \pm 40, \pm 50, \pm 60, \ldots\}$.

(6) $M(12) = \{12x : x \in \mathbf{Z}\} = \{0, \pm 12, \pm 24, \pm 36, \pm 48, \pm 60, \ldots\}$.

Proposition 1.5. *Pour tous $a, b, c \in \mathbf{Z}$, les propriétés suivantes sont satisfaites :*

(1) *a divise a ;*

(2) *$(a|b \text{ et } b|a) \Longrightarrow a = \pm b$;*

(3) *$(a|b \text{ et } b|c) \Longrightarrow a|c$.*

DÉMONSTRATION. (1) On a $a = 1 \cdot a$ et donc a divise a.

(2) Supposons que a divise b et b divise a ; écrivons $b = ka$ et $a = \ell b$ avec $k, \ell \in \mathbf{Z}$. On va distinguer deux cas. Supposons d'abord que $a = 0$. Alors $b = k \cdot 0 = 0 = a$. Donc $b = \pm a$. Passons au cas $a \neq 0$. On écrit alors $a = \ell b = \ell k a$, de sorte qu'on a $a(1 - \ell k) = 0$. Comme $a \neq 0$, il vient $\ell k = 1$. Cette équation n'a que deux solutions entières, à savoir $k = 1 = \ell$ et $k = -1 = \ell$. Par suite, on a $b = ka = \pm a$.

(3) Supposons que a divise b et b divise c ; écrivons $b = ka$ et $c = \ell b$ avec $k, \ell \in \mathbf{Z}$. On a alors $c = \ell b = \ell k a$, de sorte que a divise c. □

PROPOSITION 1.6. *Pour tous $a, b \in \mathbf{Z}$, on a les équivalences suivantes :*

(1) $D(a) \subseteq D(b) \iff a|b \iff M(b) \subseteq M(a)$;

(2) $D(a) = D(b) \iff a = \pm b \iff M(b) = M(a)$.

EXERCICE 1.7. Démontrer cette proposition.

1.2. Division euclidienne. Etant donnés deux nombres entiers a, b, avec $b \neq 0$, le quotient a/b n'est pas nécessairement entier. Pour disposer d'une opération de division qui reste dans $\mathbf{Z}$, il faut autoriser les divisions à avoir des restes. Voici le meilleur résultat possible dans cette direction.

THÉORÈME 1.8.
Soit $n \in \mathbf{Z}$ et $d \in \mathbf{Z}^*$. Il existe un unique couple $(q, r) \in \mathbf{Z}^2$ tel que $0 \leq r < |d|$ et $n = qd + r$.

DÉFINITION 1.9. *Les nombres q et r apparaissant dans le théorème 1.8 sont appelés* quotient *et* reste *de la division euclidienne de n par d.*

La preuve que nous donnerons du théorème 1.8 n'est pas la plus courte, mais elle a l'avantage de montrer comment calculer le couple (q, r) — ou le faire calculer par un ordinateur. Nous appellerons «fonction signe» l'application

$$\operatorname{sgn} : \mathbf{R} \to \mathbf{R} \ ; \ x \mapsto \begin{cases} 1 & \text{si } x > 0 \\ 0 & \text{si } x = 0 \\ -1 & \text{si } x < 0 \end{cases} .$$

Rappelons qu'on a alors $|x| = x \cdot \operatorname{sgn}(x)$ et $x = |x| \cdot \operatorname{sgn}(x)$ pour tout $x \in \mathbf{R}$.

PREUVE DU THÉORÈME 1.8. Commençons par démontrer l'existence du couple (q, r). On distingue trois cas.

1ER CAS : on suppose que $n = 0$. Il suffit alors de prendre $(q, r) = (0, 0)$.

2E CAS : on suppose que $n > 0$. On pose alors $q_0 = 0$ et $r_0 = n$. Ensuite, pour tout $k \in \mathbf{N}$:

(1) si $r_k \geq |d|$, on pose $\alpha_k = \max\{s \in \mathbf{N} : 10^s \cdot |d| \leq r_k\}$, puis

$$r_{k+1} = r_k - 10^{\alpha_k} \cdot |d| \quad \text{et} \quad q_{k+1} = q_k + 10^{\alpha_k} \cdot \operatorname{sgn}(d) \ ;$$

(2) si $r_k < d$, on pose $r_{k+1} = r_k$ et $q_{k+1} = q_k$.

Montrons alors que pour tout $k \in \mathbf{N}$, on a $n = q_k d + r_k$ et $r_k \geq 0$, en procédant par récurrence sur k. L'initialisation (pour $k = 0$) est évidente : on a $q_0 d + r_0 = 0 \cdot d + n = n$ et $r_0 = n \geq 0$.

Hypothèse de récurrence : on suppose que $n = q_k d + r_k$ et $r_k \geq 0$.

Hérédité : on a $q_{k+1} d + r_{k+1} = q_k d + r_k = n$ si $r_k < |d|$ et

$$q_{k+1} d + r_{k+1} = q_k d + 10^{\alpha_k} \cdot \mathrm{sgn}(d) \cdot d + r_k - 10^{\alpha_k} \cdot |d| = q_k d + r_k = n$$

si $r_k \geq |d|$. Dans les deux cas, on a $q_{k+1} d + r_{k+1} = n$. En outre, on a $r_{k+1} = r_k \geq 0$ si $r_k < |d|$ et $r_{k+1} = r_k - 10^{\alpha_k} \cdot |d| \geq 0$ si $r_k \geq |d|$. Dans les deux cas, on trouve $r_{k+1} \geq 0$, ce qui termine la récurrence.

Supposons par l'absurde que $r_k \geq |d|$ pour tout $k \in \mathbf{N}$. Alors, on a $r_{k+1} = r_k - 10^{\alpha_k} \cdot |d| \leq r_k - 1$ pour tout k, de sorte que $r_k \leq r_0 - k$ pour tout k (récurrence sur k). En particulier, on trouve, $r_{n+1} \leq r_0 - (n+1) = -1$, ce qui contredit les propriétés prouvéees ci-dessus.

Ceci prouve qu'il existe ℓ tel que $r_\ell < |d|$. On conclut ce cas en posant $q = q_\ell$ et $r = r_\ell$.

3^{E} CAS : on suppose que $n < 0$. On pose $n' = -n$ et on trouve $q', r' \in \mathbf{Z}$ tels que $0 \leq r' < |d|$ et $n' = q' d + r'$ (voir le cas précédent). On a alors $n = (-q')d + (-r')$. Si $r' = 0$, on conclut en posant $q = -q'$ et $r = 0$; si $r' > 0$, on a $n = (-q' - sgn(d)) \cdot d + |d| - r'$ et $0 < |d| - r' < |d|$, si bien qu'on peut prendre $q = -q' - \mathrm{sgn}(d)$ et $r = |d| - r'$.

Passons maintenant à la preuve de l'unicité. Supposons que deux couples $(q_1, r_1), (q_2, r_2)$ satisfont $0 \leq r_i < |d|$ et $n = q_i d + r_i$ pour $i = 1, 2$. Oa a alors $(q_1 - q_2)d = r_2 - r_1$. Or, le nombre $|r_2 - r_1|$ est compris entre 0 et $|d| - 1$, tandis que $|(q_1 - q_2)d|$ est soit nul, soit supérieur ou égal à $|d|$. On en déduit que $(q_1 - q_2)d = 0 = r_2 - r_1$, d'où $(q_1, r_1) = (q_2, r_2)$ puisque d n'est pas nul. □

Concrètement, pour effectuer une division euclidienne, on peut écrire les valeurs des q_k, r_k, et α_k dans un tableau.

EXEMPLE 1.10. Effectuons la division euclidienne de 7000 par 23. L'algorithme (2^{e} cas) donne les résultats suivants :

i	0	1	2	3	4	5	6	7	8
q_i	0	100	200	300	301	302	303	304	304
r_i	7000	4700	2400	100	77	54	31	8	8
α_i	2	2	2	0	0	0	0		

En posant $q = q_7 = 304$ et $r = r_7 = 8$, on a bien $0 \leq r < |23|$ et $7000 = q \cdot 23 + r$.

EXEMPLE 1.11. Effectuons la division euclidienne de -970 par 8. On tombe dans le 3^{e} cas. On applique donc l'algorithme du 2^{e} cas à 970 et 8. Il vient :

i	0	1	2	3	4	5
q_i	0	100	110	120	121	121
r_i	970	170	90	10	2	2
α_i	2	1	1	0		

On est donc conduit à poser $q' = q_4 = 121$ et $r' = r_4 = 2$, puis $q = -q' - sgn(d) = -122$ et $r = |d| - r' = 6$. On a bien $0 \leq r < |8|$ et $-970 = q \cdot 8 + r$.

EXEMPLE 1.12. Effectuons la division euclidienne de 6325 par -27. L'algorithme (2^{e} cas) donne les résultats suivants :

i	0	1	2	3	4	5	6	7	8	9
q_i	0	-100	-200	-210	-220	-230	-231	-232	-233	-234
r_i	6325	3625	925	655	385	115	88	61	34	7
α_i	2	2	1	1	1	0	0	0	0	

En posant $q = q_9 = -234$ et $r = r_9 = 7$, on a bien $0 \leq r < |-27|$ et $6325 = q \cdot (-27) + r$.

1.3. Congruences.

DÉFINITION 1.13.
Soient a, b, m trois entiers. On dit que a est congru à b modulo m, *et on note $a \equiv b\ [m]$, si $a - b$ est divisible par m.*

REMARQUE 1.14. On a $a \equiv b\ [m] \iff a \equiv b\ [-m]$. En effet, on a $km = (-k)(-m)$ pour tout $k \in \mathbf{Z}$. C'est la raison pour laquelle on ne traitera aucun exemple avec $m < 0$.

Les congruences sont très commodes pour modéliser des situations de la vie courante, par exemple le comptage des heures ou des jours de la semaine.

EXEMPLE 1.15. S'il est onze heures, dans quinze heures il sera deux heures, car $11 + 15 \equiv 2\ [24]$.

EXEMPLE 1.16. Le 1^{er} janvier 2009 était un jeudi. Le 1^{er} janvier 2010 sera un vendredi, car l'année 2009 n'est pas bissextile et on a $365 \equiv 1\ [7]$.

PROPOSITION 1.17. *Soit $m \in \mathbf{Z}$. La relation de congruence modulo m est une relation d'équivalence. Autrement dit, elle satisfait les propriétés suivantes :*

(1) *Pour tout $a \in \mathbf{Z}$, on a $a \equiv a\ [m]$;*
(2) *Pour tous $a, b \in \mathbf{Z}$, on a $a \equiv b\ [m] \iff b \equiv a\ [m]$;*
(3) *Pour tous $a, b, c \in \mathbf{Z}$, on a $(a \equiv b\,[m] \text{ et } b \equiv c\,[m]) \implies a \equiv c\,[m]$.*

DÉMONSTRATION. (1) Pour tout $a \in \mathbf{Z}$, on a $a - a = 0$, et donc $a \equiv a\ [m]$.
(2) Supposons que $a \equiv b\ [m]$. On peut écrire $a - b = km$ avec $k \in \mathbf{Z}$. Alors on a $b - a = (-k)m$, et donc $b \equiv a\ [m]$. L'autre implication se prouve de manière analogue.
(3) Supposons que $a \equiv b\,[m]$ et $b \equiv c\,[m]$. On peut écrire $a - b = km$ et $b - c = \ell m$ avec $k, \ell \in \mathbf{Z}$. Alors, on a $a - c = (k + \ell)m$, et donc $a \equiv c\ [m]$. □

Le résultat qui suit dit en substance que les opérations arithmétiques ont un sens modulo m.

PROPOSITION 1.18. *Soit $a_1, a_2, b_1, b_2, m \in \mathbf{Z}$ tels que $a_1 \equiv a_2\,[m]$ et $b_1 \equiv b_2\,[m]$. Alors, on a :*

(1) $a_1 + b_1 \equiv a_2 + b_2\,[m]$;
(2) $a_1 - b_1 \equiv a_2 - b_2\,[m]$;
(3) $a_1 \cdot b_1 \equiv a_2 \cdot b_2\,[m]$.

DÉMONSTRATION. Ecrivons $a_1 - a_2 = km$ et $b_1 - b_2 = \ell m$ avec $k, \ell \in \mathbf{Z}$.

On a $(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) = (k + \ell)m$ et donc $a_1 + b_1 \equiv a_2 + b_2\,[m]$; la congruence $a_1 - b_1 \equiv a_2 - b_2\,[m]$ s'obtient de manière analogue.

Finalement, on a $a_1b_1 - a_2b_2 = a_1(b_1 - b_2) + (a_1 - a_2)b_2 = (a_1\ell + kb_2)m$ et donc $a_1 \cdot b_1 \equiv a_2 \cdot b_2\,[m]$. □

Ce résultat permet de simplifier des calculs lorsqu'on travaille modulo m.

EXEMPLE 1.19. Calculons les premières puissances de 8 modulo 11. On a $8^1 = 8$, $8^2 = 64 \equiv 9\,[11]$, $8^3 \equiv 8 \cdot 9 = 72 \equiv 6\,[11]$, $8^4 \equiv 8 \cdot 6 = 48 \equiv 4\,[11]$, $8^5 \equiv 8 \cdot 4 = 32 \equiv 10\,[11]$, etc. Contrairement à ce qui se passe lorsqu'on calcule les puissances successives de 8 dans $\mathbf{Z}$, la complexité n'augmente pas à chaque étape.

EXERCICE 1.20. Soit $m \in \mathbf{Z}$. Montrer que pour tout $a \in \mathbf{Z}$, la classe d'équivalence de a pour la relation de congruence modulo m est l'ensemble $a + m\mathbf{Z} := \{a + my : y \in \mathbf{Z}\}$. Combien y a-t-il de classes d'équivalence distinctes ? (La réponse dépend de m.)

Nous reviendrons aux congruences dans la section 3.2.

2. Multiples et diviseurs communs

2.1. Définitions et premières propriétés. Etant donnés deux entiers a et b, on pose :

$$D(a,b) = \{x \in \mathbf{Z} : x|a \text{ et } x|b\} \quad \text{et} \quad M(a,b) = \{x \in \mathbf{Z} : a|x \text{ et } b|x\}\ .$$

Les éléments de $D(a,b)$ sont les *diviseurs communs* de a et b ; ceux de $M(a,b)$ sont les *multiples communs* de a et b. On a bien sûr $D(a,b) = D(a) \cap D(b) = D(b,a)$ et $M(a,b) = M(a) \cap M(b) = M(b,a)$.

REMARQUE 2.1. Les ensembles $D(a,b)$ et $M(a,b)$ ne sont jamais vides. En effet, quels que soient a et b, on a $\pm 1 \in D(a,b)$ et $0 \in M(a,b)$.

REMARQUE 2.2. Si $a \neq 0$, alors $D(a,b)$ est fini, car $D(a)$ est fini. De même, si $b \neq 0$, alors $D(a,b)$ est fini.

REMARQUE 2.3. Si $a \neq 0$ et $b \neq 0$, alors $M(a,b)$ est infini car $ab \neq 0$ et $M(a,b)$ contient $M(ab)$ par la proposition 1.6.

EXEMPLES. On a :

(1) $D(10,12) = \{\pm 1, \pm 2\} = D(2)$.

(2) $M(10,12) = \{0, \pm 60, \pm 120, \pm 180, \ldots\}$. On verra que $M(10,12) = M(60)$.

(3) $D(0,a) = D(a)$ et $D(1,a) = D(-1,a) = \{\pm 1\}$ pour tout $a \in \mathbf{Z}$.

(4) $M(0,a) = \{0\}$ et $M(1,a) = M(-1,a) = M(a)$ pour tout $a \in \mathbf{Z}$.

DÉFINITION 2.4. *Soit $a, b \in \mathbf{Z}$. Si $a \neq 0$ ou $b \neq 0$, le* plus grand diviseur commun *de a et b, noté* $\operatorname{pgcd}(a,b)$*, est le plus grand élément de l'ensemble $D(a,b)$. Si $a = 0 = b$, on pose* $\operatorname{pgcd}(a,b) = 0$*. Lorsque* $\operatorname{pgcd}(a,b) = 1$*, on dit que a et b sont* premiers entre eux*, ce qu'on note $a \perp b$.*

Le plus grand diviseur commun est bien défini car l'ensemble $D(a,b)$ est fini et non vide lorsque $a \neq 0$ ou $b \neq 0$.

MISE EN GARDE. La notation $a \perp b$ n'est pas standard.

DÉFINITION 2.5. *Soit $a, b \in \mathbf{Z}$. Si $a \neq 0$ et $b \neq 0$, le* plus petit multiple commun *de a et b, noté* $\operatorname{ppcm}(a,b)$*, est le plus petit élément strictement positif de l'ensemble $M(a,b)$. Si $a = 0$ ou $b = 0$, on pose* $\operatorname{ppcm}(a,b) = 0$.

Si $a, b \in \mathbf{Z}^*$, alors $M(ab)$ contient le nombre strictement positif $|ab|$, car $|ab| = |a| \cdot \operatorname{sgn}(b) \cdot b$ et $|ab| = |b| \cdot \operatorname{sgn}(a) \cdot a$. Le plus petit multiple commun de a et b est bien défini car toute partie non vide de $\mathbf{N}$ possède un plus petit élément.

EXEMPLES. Les exemples ci-dessus nous donnent : $\operatorname{pgcd}(10,12) = 2$ et $\operatorname{ppcm}(10,12) = 60$.

Les définitions de pgcd et ppcm, avec leur distinction de cas, peuvent paraître artificielles. On verra des caratérisations (voir les propositions 2.9 et 2.17) qui ne distinguent pas de cas et qui contitueraient les "bonnes" définitions d'un point de vue algébrique. Les définitions ci-dessus ont pour avantage de rendre l'existence du pgcd et du ppcm évidente pour tout couple d'entiers (a,b). De plus, avec ce point de vue, le pgcd et le ppcm de a et b sont uniques.

PROPOSITION 2.6. *On a :*

(1) $\operatorname{pgcd}(0,a) = |a|$ *et* $\operatorname{pgcd}(1,a) = \operatorname{pgcd}(-1,a) = 1$ *pour tout* $a \in \mathbf{Z}$ *;*

(2) $\operatorname{ppcm}(1,a) = \operatorname{ppcm}(-1,a) = |a|$ *pour tout* $a \in \mathbf{Z}$.

(3) $\operatorname{pgcd}(a,b) = \operatorname{pgcd}(|a|,|b|)$ *et* $\operatorname{ppcm}(a,b) = \operatorname{ppcm}(|a|,|b|)$ *pour tous* $a, b \in \mathbf{Z}$.

DÉMONSTRATION. (1) Comme on a $D(1,a) = D(-1,a) = \{\pm 1\}$, on obtient $\operatorname{pgcd}(1,a) = \operatorname{pgcd}(-1,a) = 1$. Par ailleurs, on a $D(0,a) = D(a)$. Ainsi, $|a|$ appartient à $D(0,a)$, puisque $a = \operatorname{sgn}(a) \cdot |a|$. De plus, $D(a)$ ne contient aucun élément strictement supérieur à $|a|$. Donc on a finalement $\operatorname{pgcd}(0,a) = |a|$.

(2) Si $a = 0$, on a $\operatorname{ppcm}(1,a) = \operatorname{ppcm}(-1,a) = 0 = |a|$. Supposons donc désormais que a est non nul. L'ensemble $M(\pm 1, a)$ contient $|a|$, car $|a| = \pm|a| \cdot \pm 1$ et $|a| = \operatorname{sgn}(a) \cdot a$. De plus, si on suppose que $k \in \mathbf{N}^* \cap M(\pm 1, a)$, on trouve $\ell \in \mathbf{Z}^*$ tel que $k = \ell \cdot a$, d'où $k = |k| = |\ell| \cdot |a| \geq |a|$. Par conséquent, aucun entier k tel que $0 < k < |a|$ n'appartient à $M(\pm 1, a)$, si bien qu'on trouve $\operatorname{ppcm}(\pm 1, a) = |a|$.

(3) Lorsque $(a,b) \neq (0,0)$, par la proposition 1.6, on a $D(a,b) = D(a) \cap D(b) = D(|a|) \cap D(|b|) = D(|a|,|b|)$. Par suite, on a $\operatorname{pgcd}(a,b) = \operatorname{pgcd}(|a|,|b|)$. Lorsque $a = 0 = b$, on a $\operatorname{pgcd}(a,b) = 0 = \operatorname{pgcd}(|a|,|b|)$.

Lorsque $a \neq 0 \neq b$, on montre que $M(a,b) = M(|a|,|b|)$ grâce à la proposition 1.6. Par suite, $\operatorname{ppcm}(a,b) = \operatorname{ppcm}(|a|,|b|)$. Lorsque $a = 0$ ou $b = 0$, on a $\operatorname{ppcm}(a,b) = 0 = \operatorname{ppcm}(|a|,|b|)$. □

PROPOSITION 2.7. *Pour tous $a, b, k \in \mathbf{Z}$, on a* $\operatorname{pgcd}(a + kb, b) = \operatorname{pgcd}(a,b)$.

DÉMONSTRATION. Remarquons qu'on a $(a + kb, b) = (0,0)$ si et seulement si $(a,b) = (0,0)$. Lorsque $(a + kb, b) = (0,0) = (a,b)$, on a $\operatorname{pgcd}(a + kb, b) = 0 = \operatorname{pgcd}(a,b)$.

Supposons maintenant que $(a+kb,b) \neq (0,0) \neq (a,b)$. Soit x un diviseur de b ; écrivons $b = \ell x$. On a alors

$$\begin{aligned} x \in D(a) &\Leftrightarrow \exists j \in \mathbf{Z} \text{ tel que } a = jx \\ &\Leftrightarrow \exists j \in \mathbf{Z} \text{ tel que } a + kb = jx + k\ell x \\ &\Leftrightarrow \exists j' \in \mathbf{Z} \text{ tel que } a + kb = j'x \Leftrightarrow x \in D(a+kb)\ . \end{aligned}$$

Par conséquent, on a $D(a) \cap D(b) = D(a+kb) \cap D(b)$, c'est-à-dire $D(a+kb,b) = D(a,b)$, d'où $\operatorname{pgcd}(a+kb,b) = \operatorname{pgcd}(a,b)$. □

2.2. Caractérisation du ppcm. On commence par un résultat intermédiaire.

LEMME 2.8. *Soit $a,b \in \mathbf{Z}^*$ et $m = \operatorname{ppcm}(a,b)$. Alors, on a $M(a,b) = M(m)$.*

DÉMONSTRATION. Par définition, m est multiple de a et b ; donc la proposition 1.6 entraîne $M(m) \subseteq M(a) \cap M(b)$, c'est-à-dire $M(m) \subseteq M(a,b)$.

Réciproquement, soit $x \in M(a,b)$. On effectue la division euclidienne de x par m ; on trouve $q, r \in \mathbf{Z}$ tels que $0 \leq r < m$ (rappelons que m est par définition strictement positif) et $x = qm+r$. On constate alors que $r = x - qm$ est multiple de a et de b. En effet, on peut écrire $x = ia = jb$ et $m = ka = \ell b$, car $x, m \in M(a,b)$, et on trouve $r = (i-qk)a = (j-q\ell)b$. Comme m est le plus petit élément strictement positif de $M(a,b)$ et que r est un élement de $M(a,b)$ strictement inférieur à m, on doit avoir $r \leq 0$, d'où $r = 0$. Ceci entraîne $x = qm$, d'où $x \in M(m)$. □

PROPOSITION 2.9 (CARACTÉRISATION DU PPCM).
Soit $a,b,m \in \mathbf{Z}$. Les assertions suivantes sont équivalentes :

(i) $m = \pm \operatorname{ppcm}(a,b)$;

(ii) *pour tout $x \in \mathbf{Z}$, on a $m|x \Longleftrightarrow (a|x \text{ et } b|x)$;*

(ii') $M(m) = M(a,b)$.

DÉMONSTRATION. Les assertions (ii) et (ii') sont équivalentes : en effet, la seconde n'est que la traduction ensembliste de la première. Il reste à prouver que (i) et (ii') sont équivalentes.

Lorsque $a = 0$ ou $b = 0$, on a $\operatorname{ppcm}(a,b) = 0$, et $M(a,b) = \{0\}$. Dans ce cas, les assertions (i) et (ii') sont équivalentes, car :
– si $m = 0$, elles sont vraies toutes les deux ;
– si $m \neq 0$, elles sont fausses toutes les deux.
On suppose donc dorénavant que $a \neq 0 \neq b$. Remarquons qu'on a $M(-m) = M(m)$ par la proposition 1.6. L'implication (i)⇒(ii') est donc une conséquence immédiate du lemme 2.8. Montrons réciproquement que (ii') implique (i). D'après (ii'), on a $M(|m|) = M(m) = M(a,b)$. Par conséquent, $|m|$ appartient à $M(a,b)$ tandis que les entiers k tels que $0 < k < |m|$ n'y appartiennent pas. Par définition, il vient $\operatorname{ppcm}(a,b) = |m|$, ce qui prouve (i). □

Notons qu'à ce stade, on n'a pas de moyen performant pour calculer un ppcm. Etant donnés $a,b \in \mathbf{Z}^*$, on sait que $\operatorname{ppcm}(a,b)$ divise ab par la proposition 2.9. On peut donc chercher le plus petit élément strictement positif de $D(ab)$ qui soit multiple de a et de b. Cet élément est le ppcm

de a et b. Cependant, il est long de faire la liste des diviseurs de ab si ab est grand, ce qui rend cette idée peu applicable en pratique.

2.3. Calcul du pgcd — Algorithme d'Euclide. On va maintenant voir une méthode efficace permettant de calculer le pgcd de deux entiers a et b.

ALGORITHME D'EUCLIDE. Soit $a, b \in \mathbf{Z}$. On pose $k_0 = |a|$ et $\ell_0 = |b|$, puis, tant que $\ell_n \neq 0$:

(1) On trouve $q_n, r_n \in \mathbf{Z}$ tels que $0 \leq r_n \leq |\ell_n|$ et $k_n = q_n\ell_n + r_n$ (par division euclidienne) ;

(2) On pose $\begin{pmatrix} k_{n+1} \\ \ell_{n+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} \begin{pmatrix} k_n \\ \ell_n \end{pmatrix}$, c'est-à-dire $\begin{pmatrix} k_{n+1} \\ \ell_{n+1} \end{pmatrix} = \begin{pmatrix} \ell_n \\ r_n \end{pmatrix}$.

Ensuite, dès que $\ell_n = 0$, on pose $k_{n+1} = k_n$ et $\ell_{n+1} = \ell_n = 0$.

THÉORÈME 2.10.
Avec les notations ci-dessus, il existe n tel que $\ell_n = 0$. De plus, on a alors $\operatorname{pgcd}(a, b) = k_n$.

DÉMONSTRATION. Montrons qu'on a $\ell_{|b|} = 0$. Supposons par l'absurde que $\ell_{|b|} \neq 0$. Alors, pour tout n tel que $0 \leq n \leq |b|$, on a $\ell_n \neq 0$, car la suite $(\ell_n)_n$ reste constante dès qu'elle atteint la valeur 0. Par construction, il vient $|\ell_{n+1}| \leq |\ell_n| - 1$ pour tout n tel que $0 \leq n \leq |b|$, et donc $|\ell_{|b|+1}| \leq |\ell_0| - |b| - 1 < 0$. Contradiction.

Montrons maintenant par récurrence que $k_n, \ell_n \in \mathbf{N}$ et $\operatorname{pgcd}(k_n, \ell_n) = \operatorname{pgcd}(a, b)$ pour tout $n \in \mathbf{N}$.

Initialisation (pour $n = 0$) : On a $k_0 = |a|$ et $\ell_0 = |b|$, et donc $\operatorname{pgcd}(k_0, \ell_0) = \operatorname{pgcd}(a, b)$ par la proposition 2.6. De plus, on a bien $k_0, \ell_0 \in \mathbf{N}$.

Hypothèse de récurrence : On suppose que $k_n, \ell_n \in \mathbf{N}$ et $\operatorname{pgcd}(k_n, \ell_n) = \operatorname{pgcd}(a, b)$.

Hérédité : Il s'agit de montrer que k_{n+1}, ℓ_{n+1} sont des entiers naturels et que $\operatorname{pgcd}(k_{n+1}, \ell_{n+1}) = \operatorname{pgcd}(a, b)$. On distingue deux cas :

– Si $\ell_n \neq 0$, alors on a $k_{n+1} = \ell_n \in \mathbf{N}$ par l'hypothèse de récurrence et $\ell_{n+1} = r_n \in \mathbf{N}$. De plus, la proposition 2.7 donne $\operatorname{pgcd}(k_{n+1}, \ell_{n+1}) = \operatorname{pgcd}(\ell_n, k_n - q_n\ell_n) = \operatorname{pgcd}(\ell_n, k_n)$. On trouve $\operatorname{pgcd}(k_{n+1}, \ell_{n+1}) = \operatorname{pgcd}(a, b)$ grâce à l'hypothèse de récurrence.
– Si $\ell_n = 0$, on a $k_{n+1} = k_n$ et $\ell_{n+1} = \ell_n$; il suffit d'appliquer l'hypothèse de récurrence.

En particulier, dès que $\ell_n = 0$, on a $|k_n| = \operatorname{pgcd}(k_n, \ell_n) = \operatorname{pgcd}(a, b)$, par la proposition 2.6, et donc $\operatorname{pgcd}(a, b) = k_n$ puisque $k_n \in \mathbf{N}$. □

EXEMPLE 2.11. Calculons le plus grand diviseur commun de $a = 8$ et $b = 14$. L'algorithme d'Euclide donne les résultats suivants :

n	0	1	2	3	4
k_n	8	14	8	6	2
ℓ_n	14	8	6	2	0
q_n	0	1	1	3	

On a $\ell_4 = 0$, et donc $\operatorname{pgcd}(8, 14) = k_4 = 2$.

EXEMPLE 2.12. Calculons le plus grand diviseur commun de $a = 65$ et $b = -42$. L'algorithme d'Euclide donne les résultats suivants :

n	0	1	2	3	4	5	6
k_n	65	42	23	19	4	3	1
ℓ_n	42	23	19	4	3	1	0
q_n	1	1	1	4	1	3	

On a $\ell_5 = 0$, et donc $\operatorname{pgcd}(65, -42) = k_5 = 1$. Les nombres 65 et -42 sont premiers entre eux.

2.4. Théorème de Bézout — Algorithme d'Euclide étendu. On va voir que le pgcd de deux entiers a et b peut s'exprimer comme combinaison, à coefficients dans $\mathbf{Z}$, de a et b.

THÉORÈME DE BÉZOUT.
Soit $a, b \in \mathbf{Z}$ et soit $d = \operatorname{pgcd}(a, b)$. Alors, il existe $u, v \in \mathbf{Z}$ tels que $d = ua + vb$.

MISE EN GARDE. Il ne suffit pas toujours de se souvenir de l'énoncé de ce théorème. On vous demandera de savoir trouver les coefficients u et v !

Ce théorème est une conséquence de la version algorithmique que nous prouverons plus loin.

COROLLAIRE 2.13 (AU THÉORÈME DE BÉZOUT). *Deux entiers a et b sont premiers entre eux si et seulement s'il existe $u, v \in \mathbf{Z}$ tels que $ua + vb = 1$.*

DÉMONSTRATION. Si $\operatorname{pgcd}(a, b) = 1$, le théorème de Bézout entraîne l'existence d'entiers u, v tels que $ua + vb = 1$. Réciproquement, s'il existe $u, v \in \mathbf{Z}$ tels que $ua + vb = 1$, le pgcd de a et b divise 1 car il divise a et b. Comme $D(1) = \{\pm 1\}$, on trouve $\operatorname{pgcd}(a, b) = 1$. □

ALGORITHME D'EUCLIDE ÉTENDU. Soit $a, b \in \mathbf{Z}$. On pose

$$\begin{pmatrix} k_0 \\ \ell_0 \end{pmatrix} = \begin{pmatrix} |a| \\ |b| \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} u_0 & v_0 \\ u'_0 & v'_0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

puis, tant que $\ell_n \neq 0$:

(1) On trouve $q_n, r_n \in \mathbf{Z}$ tels que $0 \leq r_n \leq |\ell_n|$ et $k_n = q_n \ell_n + r_n$ (par division euclidienne) ;

(2) On pose $\begin{pmatrix} k_{n+1} \\ \ell_{n+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} \begin{pmatrix} k_n \\ \ell_n \end{pmatrix}$ et $\begin{pmatrix} u_{n+1} & v_{n+1} \\ u'_{n+1} & v'_{n+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} \begin{pmatrix} u_n & v_n \\ u'_n & v'_n \end{pmatrix}$.

Ensuite, dès que $\ell_n = 0$, on pose

$$\begin{pmatrix} k_{n+1} \\ \ell_{n+1} \end{pmatrix} = \begin{pmatrix} k_n \\ \ell_n \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} u_{n+1} & v_{n+1} \\ u'_{n+1} & v'_{n+1} \end{pmatrix} = \begin{pmatrix} u_n & v_n \\ u'_n & v'_n \end{pmatrix}.$$

VERSION ALGORITHMIQUE DU THÉORÈME DE BÉZOUT.
(On conserve les notations de l'agorithme d'Euclide étendu.) Il existe un nombre naturel n tel que $\ell_n = 0$. De plus, on a alors $k_n = u_n \cdot |a| + v_n \cdot |b| = \operatorname{pgcd}(a, b)$.

DÉMONSTRATION. Les règles de définition des coefficients k_n et ℓ_n sont exatement les mêmes que dans l'algorithme d'Euclide. L'existence de n tel que $\ell_n = 0$ et l'égalité $k_n = \text{pgcd}(a, b)$ dans ce cas découlent donc du théorème 2.10.

Posons maintenant pour $n \in \mathbf{N}$:

$$X_n = \begin{pmatrix} k_n \\ \ell_n \end{pmatrix} \quad , \quad M_n = \begin{pmatrix} u_n & v_n \\ u'_n & v'_n \end{pmatrix} \quad \text{et} \quad Q_n = \begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} \text{ lorsque } \ell_n \neq 0 \ .$$

Montrons par récurrence qu'on a $X_n = M_n X_0$ pour tout $n \in \mathbf{N}$.

Initialisation (pour $n = 0$) : La matrice M_0 est la matrice identité, et donc on a $X_0 = M_0 X_0$

Hypothèse de récurrence : Supposons qu'on a $X_n = M_n X_0$.

Hérédité : Montrons qu'on a $X_{n+1} = M_{n+1} X_0$. Distinguons deux cas. Si $\ell_n = 0$, on a $X_{n+1} = X_n$ et $M_{n+1} = M_n$ par définition. Donc l'hypothèse de récurrence donne $X_{n+1} = M_{n+1} X_0$. Si $\ell_n \neq 0$, on a $X_{n+1} = Q_n X_n$ et $M_{n+1} = Q_n M_n$. Grâce à l'hypothèse de récurrence, on trouve $X_{n+1} = Q_n M_n X_0 = M_{n+1} X_0$.

Plaçons nous maintenant dans le cas $\ell_n = 0$. La formule $X_n = M_n X_0$ donne en particulier $k_n = u_n k_0 + v_n \ell_0$, et donc $\text{pgcd}(a, b) = k_n = u_n \cdot |a| + v_n \cdot |b|$. □

Reprenons les exemples de pgcd vus précédemment.

EXEMPLE 2.14. Soit $a = 8$ et $b = 14$. L'algorithme d'Euclide étendu donne les résultats suivants :

n	0	1	2	3	4
k_n	8	14	8	6	2
ℓ_n	14	8	6	2	0
u_n	1	0	1	-1	2
u'_n	0	1	-1	2	
v_n	0	1	0	1	-1
v'_n	1	0	1	-1	
q_n	0	1	1	3	

On a $\ell_4 = 0$; par conséquent, on trouve $\text{pgcd}(8, 14) = k_4 = 2$ et $2 = 2 \cdot 8 + (-1) \cdot 14$. Les valeurs de u'_4 et v'_4 n'ont pas été calculées, car on n'en a pas besoin.

REMARQUE 2.15. On remarque que les calculs des u_n, u'_n d'une part et des v_n, v'_n d'autre part sont indépendants, dans le sens qu'on peut calculer tous les u_n, u'_n sans avoir trouvé un seul v_n, v'_n, et réciproquement. Cela permet de se passer du calcul de tous les v_n, v'_n. On illustre ce point dans le second exemple.

EXEMPLE 2.16. Soit $a = 65$ et $b = -42$. L'algorithme d'Euclide étendu donne les résultats suivants :

n	0	1	2	3	4	5	6
k_n	65	42	23	19	4	3	1
ℓ_n	42	23	19	4	3	1	0
u_n	1	0	1	-1	2	-9	11
u'_n	0	1	-1	2	-9	11	
q_n	1	1	1	4	1	3	

On a $\ell_6 = 0$, et donc $\operatorname{pgcd}(65, -42) = k_6 = 1$. Les nombres 65 et -42 sont premiers entre eux. On ne connaît pas la valeur de v_6, mais on sait que $1 = u_6 \cdot 65 + v_6 \cdot 42 = 11 \cdot 65 + v_6 \cdot 42$. On trouve $v_6 = -714/42 = -17$. Par conséquent, on a $1 = 11 \cdot 65 + 17 \cdot (-42)$.

2.5. Application du théorème de Bézout — Caractérisation du pgcd. Le pgcd de deux entiers admet la caractérisation suivante, analogue à celle que nous avons obtenue précédemment pour le ppcm.

PROPOSITION 2.17 (CARACTÉRISATION DU PGCD).
Soit a, b, d trois entiers. Les assertions suivantes sont équivalentes :

(i) $d = \pm \operatorname{pgcd}(a, b)$;

(ii) *pour tout $x \in \mathbf{Z}$, on a $x|d \iff (x|a \text{ et } x|b)$;*

(ii') $D(d) = D(a, b)$.

DÉMONSTRATION. Les assertions (ii) et (ii') sont équivalentes : en effet, la seconde n'est que la traduction ensembliste de la première. Il reste à prouver qu'elles sont équivalentes à (i).

1er cas : On suppose que $a = 0 = b$. On a $\operatorname{pgcd}(a, b) = 0$, et $D(a, b) = \mathbf{Z}$. Dans ce cas, les assertions (i) et (ii') sont équivalentes, car :
– si $d = 0$, elles sont vraies toutes les deux ;
– si $d \neq 0$, elles sont fausses toutes les deux.

2e cas : On suppose que $(a, b) \neq (0, 0)$. On suppose d'abord que (i) est vérifiée et on prouve (ii). Si x divise d, alors par (i), on a $x| \operatorname{pgcd}(a, b)$. Alors on a $(x|a \text{ et } x|b)$, car $\operatorname{pgcd}(a, b)$ divise a et b. Réciproquement, si x divise a et b, on peut écrire $\operatorname{pgcd}(a, b) = ua + vb$ grâce au théorème de Bézout ; il vient alors $d = \pm ua \pm vb$ par (i) et on constate que x divise d.

Supposons maintenant que (ii') est vérifiée et prouvons (i). On a $D(|d|) = D(d) = D(a, b)$ d'après la proposition 1.6 et l'hypothèse (ii'). Ainsi, $|d|$ appartient à $D(a, b)$ tandis que les entiers k tels que $k > |d|$ n'y appartiennent pas. Par définition, il vient $\operatorname{pgcd}(a, b) = |d|$, ce qui prouve (i). □

Ici l'énoncé du théorème de Bézout nous a suffi. Nous verrons plus loin d'autres applications pour lesquelles la version algorithmique s'avèrera utile.

2.6. Propriétés des nombres premiers entre eux. Tout d'abord, voici comment produire des couples d'entiers premiers entre eux.

LEMME 2.18. *Soit $a, b \in \mathbf{Z}$ tels que $(a, b) \neq (0, 0)$, soit $d \in D(a, b)$ et soit $a' = \frac{a}{d}$ et $b' = \frac{b}{d}$. Alors, les nombres a' et b' sont des entiers et satisfont* $\operatorname{pgcd}(a', b') = \frac{\operatorname{pgcd}(a,b)}{|d|}$.

En particulier, si $d = \pm \operatorname{pgcd}(a, b)$, alors $a' = \frac{a}{d}$ et $b' = \frac{b}{d}$ sont des entiers premiers entre eux.

DÉMONSTRATION. Remarquons que l'hypothèse $(a, b) \neq (0, 0)$ entraîne $d \neq 0$. Comme, d divise a et b, il divise aussi $\operatorname{pgcd}(a, b)$; donc a', b' et $\frac{\operatorname{pgcd}(a,b)}{d}$ sont des entiers. Soit $k \in \mathbf{Z}$.

– Si k divise a' et b', alors kd divise $a = a'd$ et $b = b'd$. Donc kd divise $\operatorname{pgcd}(a, b)$ par la proposition 2.17, si bien que k divise $\frac{\operatorname{pgcd}(a,b)}{d}$.
– Si k divise $\frac{\operatorname{pgcd}(a,b)}{d}$, alors kd divise $\operatorname{pgcd}(a, b)$. Donc, kd divise $a = a'd$ et $b = b'd$, si bien que k divise a' et b'.

Ainsi k divise a' et b' si et seulement s'il divise $\frac{\operatorname{pgcd}(a,b)}{d}$. La proposition 2.17 donne alors

$$\frac{\operatorname{pgcd}(a, b)}{d} = \pm \operatorname{pgcd}(a', b'), \quad \text{d'où} \quad \operatorname{pgcd}(a', b') = \frac{\operatorname{pgcd}(a, b)}{|d|} .$$

Lorsque $d = \pm \operatorname{pgcd}(a, b)$, on obtient $\operatorname{pgcd}(a', b') = 1$, c'est-à-dire que a' et b' sont premiers entre eux. □

EXEMPLE 2.19. On a vu que le pgcd de 8 et 14 est 2. Les nombres 4 et 7 sont donc premiers entre eux.

On établit maintenant trois résultats dans lesquels la notion de nombres premiers entre eux est fondamentale.

PROPRIÉTÉ DE GAUSS.
Pour tous $a, b, c \in \mathbf{Z}$, si a et b sont premiers entre eux et si a divise bc, alors a divise c.

DÉMONSTRATION. Supposons qu'on a $a \perp b$ et $a|bc$. Par le théorème de Bézout, il existe $u, v \in \mathbf{Z}$ tels que $ua + vb = 1$. Ecrivons $bc = ka$ avec $k \in \mathbf{Z}$. On obtient alors

$$c = c \cdot 1 = cua + cvb = cua + vka = (cu + vk)a .$$

Par conséquent, a divise c. □

EXEMPLE 2.20. Les nombres 7 et 8 sont premiers entre eux. Comme 7 divise $7000 = 8 \cdot 875$, il divise aussi 875.

PROPRIÉTÉ D'EUCLIDE.
Soit $a, b, c \in \mathbf{Z}$,avec a et b premiers entre eux. Si a et b divisent c, alors ab divise c.

DÉMONSTRATION. Supposons que a et b divisent c. Ecrivons $c = kb$. On a $a|bk$; comme a et b sont premiers entre eux, la propriété de Gauss entraîne $a|k$. Par conséquent, on a $ab|kb$, c'est-à-dire $ab|c$. □

EXEMPLE 2.21. Les nombres 4 et 7 sont premiers entre eux et divisent tous deux le nombre 700. Par conséquent $28 = 4 \cdot 7$ divise 700.

PROPOSITION 2.22. *Pour tous $a, b \in \mathbf{Z}$, on a* $\operatorname{pgcd}(a,b) \cdot \operatorname{ppcm}(a,b) = |ab|$.
En particulier, si a et b sont premiers entre eux, alors $\operatorname{ppcm}(a,b) = |ab|$.

DÉMONSTRATION. Si $a = 0 = b$, on a $\operatorname{pgcd}(a,b) \cdot \operatorname{ppcm}(a,b) = 0 = |ab|$. Supposons donc dès maintenant que $(a,b) \neq (0,0)$. On pose $d = \operatorname{pgcd}(a,b)$; par le lemme 2.18, $a' = \frac{a}{d}$ et $b' = \frac{b}{d}$ sont des entiers premiers entre eux. Soit maintenant $k \in \mathbf{Z}$:
– Si a et b divisent k, alors d divise k ; on écrit $xd = k$ et on a $a'|x$ et $b'|x$. Comme a' et b' sont premiers entre eux, la propriété d'Euclide donne $a'b'|x$. Par conséquent, le nombre $\frac{ab}{d} = a'b'd$ divise $xd = k$.
– Si $\frac{ab}{d}$ divise k, alors a et b divisent k, car on a $\frac{ab}{d} = a\frac{b}{d} = b\frac{a}{d}$.
Ainsi k est divisible par a et b si et seulement s'il est divisible par $\frac{ab}{d}$. Par la proposition 2.9, on a $\operatorname{ppcm}(a,b) = \left|\frac{ab}{d}\right| = \frac{|ab|}{\operatorname{pgcd}(a,b)}$. □

EXEMPLE 2.23. Les nombres 4 et 7 sont premiers entre eux. Donc, on a $\operatorname{ppcm}(4,7) = |4 \cdot 7| = 28$.

3. Applications à la résolution d'équations

3.1. Equations diophantiennes linéaires. On s'intéresse à résoudre des équations de la forme $ax + by = c$, où a, b, c sont des coefficients fixés et où x, y sont les inconnues. Rappelons que lorsqu'on travaille dans $\mathbf{R}$, la solution est très simple :
– si $(a,b) = (0,0)$ et $c = 0$, tout couple (x,y) est solution ;
– si $(a,b) = (0,0)$ et $c \neq 0$, l'équation n'a aucune solution ;
– si $a \neq 0$, l'ensemble des solutions est $\{(a^{-1}(c - by), y) : y \in \mathbf{R}\}$;
– si $b \neq 0$, l'ensemble des solutions est $\{(x, b^{-1}(c - ax)) : x \in \mathbf{R}\}$.
Dans $\mathbf{C}$, ou même dans $\mathbf{Q}$, la solution est analogue.

Le problème qui nous intéresse est, lorsque a, b, c sont des entiers donnés, de trouver les solutions *entières* de l'équation $ax + by = c$, c'est-à-dire l'ensemble des couples $(x,y) \in \mathbf{Z}^2$ tels que $ax + by = c$. Ce problème est plus difficile, car étant donné un entier $a \neq 0$, l'inverse a^{-1} n'est pas nécessairement entier.

DÉFINITION 3.1. *On appelle* équation diophantienne (linéaire) *une équation de la forme*

$$ax + by = c, \qquad \text{avec } a, b, c \in \mathbf{Z} \text{ fixés,}$$

où x, y sont les inconnues. Une solution *de cette équation est un couple $(u,v) \in \mathbf{Z}^2$ tel que $au + bv = c$.*

Voyons, de manière générale, comment traiter des équations de ce type.

RÉSOLUTION D'UNE ÉQUATION DIOPHANTIENNE.
On procède en trois étapes :

(1) *déterminer s'il existe des solutions (voir le lemme 3.2) ;*
(2) *se ramener à une équation sans second membre (voir le lemme 3.5) ;*
(3) *résoudre l'équation sans second membre (voir le lemme 3.7).*

Le théorème 3.9 donnera la solution de n'importe quelle équation diophantienne. Il est cependant plus facile de se souvenir de la méthode que du théorème ! En outre, on retrouve des méthodes analogues dans d'autres cas, par exemple la résolution d'équations différentielles linéaires.

LEMME 3.2. *Soit $a, b, c \in \mathbf{Z}$. L'équation diophantienne $ax + by = c$ possède (au moins) une solution si et seulement si* $\operatorname{pgcd}(a, b)$ *divise c.*

DÉMONSTRATION. Pour tous $x, y \in \mathbf{Z}$, le nombre $ax + by$ est multiple de $\operatorname{pgcd}(a, b)$. Donc, s'il existe $(u, v) \in \mathbf{Z}^2$ tel que $au + bv = c$, alors $\operatorname{pgcd}(a, b)$ divise c.

Réciproquement, si $\operatorname{pgcd}(a, b)$ divise c, on peut écrire $c = k \operatorname{pgcd}(a, b)$ avec $k \in \mathbf{Z}$. Le théorème de Bézout assure l'existence de $u', v' \in \mathbf{Z}$ tels que $u'a + v'b = \operatorname{pgcd}(a, b)$. Dès lors, le couple $(u = ku', v = kv') \in \mathbf{Z}^2$ est une solution de l'équation $ax + by = c$. □

EXEMPLE 3.3. On a $\operatorname{pgcd}(8, 14) = 2$ (voir l'exemple 2.11). Par conséquent, l'équation diophantienne $8x + 14y = 4$ possède des solutions, tandis que l'équation diophantienne $8x + 14y = 3$ n'en possède pas. Comme on a $\operatorname{pgcd}(65, -42) = 1$ (voir l'exemple 2.12), l'équation diophantienne $65x - 42y = c$ possède des solutions, quelle que soit la valeur de c.

DÉFINITION 3.4. *Une équation diophantienne $ax + by = c$ étant donnée, l'*équation homogène associée *est l'équation diophantienne $ax + by = 0$.*

LEMME 3.5. *Considérons une équation diophantienne (E) $ax + by = c$ (d'inconnues x et y). Si (E) possède une solution (u_0, v_0), alors ses solutions sont exactement les couples de la forme $(u_0 + s, v_0 + t)$ où (s, t) parcourt les solutions de l'équation homogène associée.*

On résume souvent ce résultat par le **slogan** suivant :

«La solution générale de l'équation inhomogène est la somme d'une solution particulière de l'équation inhomogène et de la solution générale de l'équation homogène associée.»

DÉMONSTRATION. Supposons que (E) possède une solution (u_0, v_0). Si (s, t) est une solution de l'équation homogène associée, on a

$$a(u_0 + s) + b(v_0 + t) = (au_0 + bv_0) + (as + bt) = c + 0 = c,$$

et donc $(u_0 + s, v_0 + t)$ est une solution de l'équation (E).

Réciproquement, si (u, v) est une solution de (E), on pose $s = u - u_0$ et $t = v - v_0$. On a immédiatement $(u, v) = (u_0 + s, v_0 + t)$; de plus, il vient

$$as + bt = a(u - u_0) + b(v - v_0) = (au + bv) - (au_0 - bv_0) = c - c = 0 \ ,$$

si bien que (s, t) est une solution de l'équation homogène associée à (E). □

EXEMPLE 3.6. Admettons pour cet exemple (ceci résultera du lemme 3.7) que les solutions de l'équation diophantienne $8x + 14y = 0$ sont les couples de la forme $(7k, -4k)$ avec $k \in \mathbf{Z}$.

On sait que $\operatorname{pgcd}(8, 14) = 2$ et que $2 = 2 \cdot 8 + (-1) \cdot 14$ (voir l'exemple 2.14). Par conséquent, le couple $(4, -2)$ est solution de l'équation diophantienne $8x + 14y = 4$. Par le lemme 3.5, les solutions de cette dernière équation sont les couples de la forme $(4 + 7k, -2 - 4k)$, avec $k \in \mathbf{Z}$.

LEMME 3.7. *Considérons une équation diophantienne homogène* (H) $ax + by = 0$*, avec* $(a, b) \neq (0, 0)$*. Posons* $d = \text{pgcd}(a, b)$*,* $a' = \frac{a}{d}$ *et* $b' = \frac{b}{d}$*. Alors* (H) *a les mêmes solutions que l'équation* (H') $a'x + b'y = 0$*. Ces solutions sont les couples de la forme* $(b'k, -a'k)$ *avec* $k \in \mathbf{Z}$*.*

DÉMONSTRATION. Remarquons que d est non nul ; donc a' et b' sont bien définis.

L'équation (H) peut s'écrire $d(a'x + b'y) = 0$; elle a donc les mêmes solutions que (H').

Montrons maintenant que les solutions de (H') sont les couples de la forme $(b'k, -a'k)$ avec $k \in \mathbf{Z}$. Pour tout $k \in \mathbf{Z}$, on a $a'(b'k) + b'(-a'k) = a'b'k - a'b'k = 0$, si bien que $(b'k, -a'k)$ est une solution de (H'). Réciproquement, considérons une solution (u, v) de (H'). On traite le cas où a est non nul (si c'est b qui est non nul, la démonstration est analogue et laissée en exercice). On a $a'u = -b'v$. Comme a' et b' sont premiers entre eux (voir le lemme 2.18), la propriété de Gauss assure que a' divise $-v$. Ecrivons $-v = ka'$ avec $k \in \mathbf{Z}$. On trouve alors $a'u = a'b'k$, d'où $u = b'k$. On a bien $(u, v) = (b'k, -a'k)$. □

EXEMPLE 3.8. Les solutions de l'équation diophantienne $8x + 14y = 0$ sont les couples de la forme $(7k, -4k)$ avec $k \in \mathbf{Z}$, car $\text{pgcd}(8, 14) = 2$, $\frac{14}{2} = 7$ et $\frac{8}{2} = 4$.

Résumons maintenant la discussion qui précède.

THÉORÈME 3.9.
Soit une équation diophantienne (E) $ax + by = c$ *(d'inconnues* x *et* y*) :*

(1) *Si* c *n'est pas multiple de* $\text{pgcd}(a, b)$*, alors* (E) *n'admet aucune solution.*

(2) *Si* $(a, b, c) = (0, 0, 0)$*, alors tout couple d'entiers* (u, v) *est solution de* (E)*.*

(3) *Si* $(a, b) \neq (0, 0)$ *et si* c *est multiple de* $\text{pgcd}(a, b)$*, on pose* $d = \text{pgcd}(a, b)$*,* $a' = \frac{a}{d}$ *et* $b' = \frac{b}{d}$*. L'équation* (E) *possède alors des solutions ; de plus, les solutions de (E) sont les couples de la forme* $(u_0 + b'k, v_0 - a'k)$*, avec* $k \in \mathbf{Z}$*, où* (u_0, v_0) *est une solution particulière de* (E)*.*

Notons que ce théorème couvre tous les cas. En effet, si on n'est pas dans les cas (1) et (3) , on a $(a, b) = (0, 0)$ et c est multiple de $\text{pgcd}(a, b)$. On a donc nécessairement $c = 0$. Autrement dit on est dans le cas (2).

DÉMONSTRATION. Le point (1) résulte du lemme 3.2. Le point (2) est évident.

Démontrons le point (3). L'équation homogène associée (H) $ax + by = 0$ a pour solutions les couples de la forme $(b'k, a'k)$, avec $k \in \mathbf{Z}$, par le lemme 3.7 et (E) possède une solution (u_0, v_0) par le lemme 3.2. On conclut avec le lemme 3.5. □

Pour conclure, effectuons la résolution complète d'une équation diophantienne à l'aide du théorème 3.9.

EXEMPLE 3.10. Résolvons l'équation diophantienne

$$8330 \cdot x - 12376 \cdot y = 19992 \ . \tag{E}$$

On applique l'algorithme d'Euclide étendu à $a = 8330$ et $b = -12376$. On trouve :

n	0	1	2	3	4
k_n	8330	12376	8330	4046	238
ℓ_n	12376	8330	4046	238	0
u_n	1	0	1	-1	3
u'_n	0	1	-1	3	
q_n	0	1	2	17	

On a donc $\mathrm{pgcd}(8330, 12376) = 238$. On constate que $19992 = 84 \cdot 238$; donc l'équation (E) admet des solutions (voir le théorème 3.9). Trouvons une solution particulière. On sait (voir la version algorithmique du théorème de Bézout) qu'il existe $v \in \mathbf{Z}$ tel que

$$238 = u_4 \cdot 8330 + v \cdot (-12376) = 3 \cdot 8330 + v \cdot (-12376) \ .$$

On trouve $v = 2$. En multipliant par 84, il vient $19992 = 252 \cdot 8330 + 168 \cdot (-12376)$; par conséquent, le couple $(252, 168)$ est une solution particulière de (E). Comme on a $8330 = 35 \cdot 238$ et $-12376 = (-52) \cdot 238$, les solutions de (E) sont les couples de la forme

$$(252 - 52 \cdot k, 168 - 35 \cdot k), \quad \text{avec } k \in \mathbf{Z} \ ,$$

par le théorème 3.9(3).

Remarque 3.11. En prenant $k = 4$, on voit que le couple $(-8, -7)$ est également solution de (E). Le théorème 3.9 permet de dire que les solutions de (E) sont les couples de la forme

$$(-8 - 52 \cdot k, -7 - 35 \cdot k), \quad \text{avec } k \in \mathbf{Z} \ .$$

De plus, en faisant le changement de variable $\ell = -k$, on voit que les solutions de (E) sont les couples de la forme

$$(-8 + 52 \cdot \ell, -7 + 35 \cdot \ell), \quad \text{avec } \ell \in \mathbf{Z} \ .$$

L'ensemble des solutions est bien sûr le même que précédemment, mais exprimé différemment. Le plus souvent, on peut décrire les solutions d'une équation diophantienne d'une infinité de manières différentes.

3.2. Equations modulo un entier n. Etant donnés des entiers a, c, n, on cherche à résoudre l'équation $ax \equiv c\,[n]$, où x est l'inconnue. Une *solution* de cette équation est un entier u tel qu'on ait $au \equiv c\,[n]$.

Définition 3.12. *Soit une équation (E) $ax \equiv c\,[n]$, avec $a, c, n \in \mathbf{Z}$, où x est l'inconnue. L'*équation diophantienne associée *est (D) $ax + ny = c$, d'inconnues x et y.*

Lemme 3.13. *Soit une équation (E) $ax \equiv c\,[n]$, avec $a, c, n \in \mathbf{Z}$, où x est l'inconnue. Les solutions de (E) sont les entiers u tels que l'équation diophantienne associée possède une solution de la forme (u, v) avec $v \in \mathbf{Z}$.*

Démonstration. L'équation diophantienne associée est (D) $ax + ny = c$, d'inconnues x et y. Si un couple (u, v) est solution de cette équation, on a $au + nv = c$, et donc $au \equiv c\,[n]$. Par conséquent, u est une solution de (E).

Réciproquement, considérons une solution u de (E). On a $au \equiv c\,[n]$; par conséquent, il existe $w \in \mathbf{Z}$ tel que $au - c \equiv wn$. En posant $v = -w$, on trouve $au + nv = c$; donc (u, v) est une solution de (D). □

Théorème 3.14.
Soit une équation (E) $ax \equiv c\,[n]$, avec $a, c, n \in \mathbf{Z}$, où x est l'inconnue :

(1) *Si c n'est pas multiple de* $\operatorname{pgcd}(a, n)$*, alors (E) n'admet aucune solution.*

(2) *Si $(a, n, c) = (0, 0, 0)$, alors tout entier u est solution de (E).*

(3) *Si $(a, n) \neq (0, 0)$ et si c est multiple de* $\operatorname{pgcd}(a, n)$*, alors on pose $d = \operatorname{pgcd}(a, n)$ et $n' = \frac{n}{d}$. L'équation (E) possède des solutions ; de plus, les solutions de (E) sont les entiers de la forme $u_0 + n'k$ avec $k \in \mathbf{Z}$ (c'est-à-dire les entiers congrus à u_0 modulo n'), où u_0 est une solution particulière de (E).*

Comme le théorème 3.9, ce théorème couvre tous les cas possibles.

Démonstration. L'équation diophantienne associée à (E) est (D) $ax+ny = c$, d'inconnues x et y. Si c n'est pas multiple de $\operatorname{pgcd}(a, n)$, l'équation (D) n'admet pas de solution, par le théorème 3.9. En vertu du lemme 3.13, (E) n'admet pas de solution. Si $(a, n, c) = (0, 0, 0)$, tout couple d'entiers (u, v) est solution de (D), par le théorème 3.9. En vertu du lemme 3.13, tout entier u est solution de (E). Ceci prouve les points (1) et (2).

Passons au point (3). Posons de plus $a' = \frac{a}{d}$. Par le théorème 3.9, (D) possède des solutions ; donc (E) possède des solutions par le lemme 3.13. Soit u_0 une solution particulière de (E). Alors il existe $v_0 \in \mathbf{Z}$ tel que (u_0, v_0) soit solution de (D). Par le théorème 3.9, les solutions de (D) sont les couples de la forme $(u_0+n'k, v_0-a'k)$, avec $k \in \mathbf{Z}$. Ainsi, par le lemme 3.13, les solutions de (E) sont les entiers de la forme $u_0 + n'k$, avec $k \in \mathbf{Z}$. □

Pour ce type d'équation également, on va résoudre complètement un exemple à l'aide du théorème 3.14.

Exemple 3.15. Résolvons l'équation

$$\text{(E)} \qquad 378 \cdot x \equiv 522\,[612]\ .$$

On applique l'algorithme d'Euclide étendu à $a = 378$ et $n = 612$. On trouve :

n	0	1	2	3	4	5	6	7	8
k_n	378	612	378	234	144	90	54	36	18
ℓ_n	612	378	234	144	90	54	36	18	0
u_n	1	0	1	-1	2	-3	5	-8	13
u'_n	0	1	-1	2	-3	5	-8	13	
q_n	0	1	1	1	1	1	1	2	

On a donc $\operatorname{pgcd}(378, 612) = 18$. On constate que $522 = 29 \cdot 18$; donc l'équation (E) admet des solutions (voir le théorème 3.14). Trouvons une solution particulière. On sait (voir la version

algorithmique du théorème de Bézout) qu'il existe $v \in \mathbf{Z}$ tel que

$$18 = u_8 \cdot 378 + v \cdot 612 = 13 \cdot 378 + v \cdot 612 \ .$$

En multipliant par 29, il vient $522 = 377 \cdot 378 + 29 \cdot v \cdot 612$, d'où $377 \cdot 378 \equiv 522\,[612]$. Par conséquent, l'entier 377 est une solution particulière de (E). Comme on a $612 = 34 \cdot 18$, les solutions de (E) sont les entiers de la forme

$$377 + 34k, \quad \text{avec } k \in \mathbf{Z} \ ,$$

par le théorème 3.14(3). Autrement dit, ce sont les entiers congrus à 377 modulo 34, ou encore les entiers congrus à 3 modulo 34.

EXERCICE 3.16. Soit une équation (E) $ax \equiv c\,[n]$, avec $a, c, n \in \mathbf{Z}$, où x est l'inconnue :

(1) Montrer que si u est une solution de (E) et si $v \equiv u\,[n]$, alors v est aussi une solution de (E).

(2) En déduire que l'ensemble des solutions de (E) est une réunion de classes d'équivalence de la relation de congruence modulo n.

(3) Posons $d = \mathrm{pgcd}(a, n)$. Montrer que l'ensemble des solutions de (E) est réunion d'exactement d classes d'équivalence de la relation de congruence modulo n.

4. Nombres premiers

4.1. Définition et premières caractérisations des nombres premiers.

DÉFINITION 4.1. *Un* nombre premier *est un entier $p \geq 2$ tel que pour tous $k, \ell \in \mathbf{N}$, on ait*

$$p = k\ell \Longrightarrow (k = 1 \text{ ou } \ell = 1) \ .$$

EXEMPLES. (1) 4 n'est pas un nombre premier, car $4 = 2 \cdot 2$;

(2) 21 n'est pas un nombre premier, car $21 = 7 \cdot 3$;

(3) 2 est premier. En effet, si $2 = k\ell$ avec $k, \ell \in \mathbf{Z}$, on a obligatoirement $(k, \ell) = (1, 2)$ ou $(k, \ell) = (2, 1)$.

REMARQUE 4.2. Soit p un entier supérieur ou égal à 2. Les assertions suivantes sont équivalentes :

(i) p est un nombre premier ;

(ii) les diviseurs positifs de p sont exactement 1 et p ;

(iii) les diviseurs de p sont ± 1 et $\pm p$.

EXERCICE 4.3. Vérifier que les nombre premiers inférieurs ou égaux à 15 sont $2, 3, 5, 7, 11$ et 13.

EXERCICE 4.4. Soit p un nombre premier. Démontrer les assertions suivantes :

(1) pour tout $a \in \mathbf{Z}$, p divise a ou p et a sont premiers entre eux ;

(2) pour tout nombre premier q distinct de p, p et q sont premiers entre eux.

On donne maintenant une première caractérisation importante des nombres premiers.

Proposition 4.5.
Soit $n \in \mathbf{Z} \setminus \{-1, 0, 1\}$ Les assertions suivantes sont équivalentes :

(i) *le nombre $|n|$ est premier ;*

(ii) *pour tous $k, \ell \in \mathbf{Z}$, on a $n = k\ell \Longrightarrow (k = \pm 1 \text{ ou } \ell = \pm 1)$;*

(iii) *pour tous $a, b \in \mathbf{Z}$, on a $n|ab \Longrightarrow (n|a \text{ ou } n|b)$.*

Démonstration. (ii)⇒(i) : Ecrivons $|n| = k\ell$ avec $k, \ell \in \mathbf{N}$. On a $n = (k \operatorname{sgn}(n))\ell$, d'où $k \operatorname{sgn}(n) = \pm 1$ ou $\ell = \pm 1$ par (ii). Comme k et ℓ sont positifs, il vient $k = 1$ ou $\ell = 1$.
(i)⇒(iii) : Soit $a, b \in \mathbf{Z}$ tels que n divise ab. Supposons que n ne divise pas a et montrons que n divise b. Posons $m = |n|$; on a aussi $m|ab$ et $m \nmid a$. Comme m est premier, par (i), le seul diviseur positif commun de m et a est 1. Donc, m et a sont premiers entre eux et, par la propriété de Gauss, m divise b. Comme $n = \pm m$, on a aussi $n|b$.
(iii)⇒(ii) : Soit $k, \ell \in \mathbf{Z}$ tels que $n = k\ell$. En particulier, on a $n|k\ell$ et, par (iii), $n|k$ ou $n|\ell$. Si n divise k, on écrit $vn = k$ avec $v \in \mathbf{Z}$ et on trouve $n = nv\ell$, d'où $v\ell = 1$ puisque n est non nul. Ainsi, il vient $\ell = \pm 1$. Si n divise ℓ, on trouve de même $k = \pm 1$. □

4.2. Décomposition d'un entier en produit de facteurs premiers. On a déjà vu que tout entier naturel supérieur ou égal à 2 peut s'écrire comme un produit de nombres premiers au chapitre 1. Par exemple, on a $12 = 2 \cdot 2 \cdot 3$ ou $50 = 2 \cdot 5 \cdot 5$. On va maintenant voir que cette décomposition est unique, à l'ordre des facteurs près.

Théorème 4.6.
Soit n un entier supérieur ou égal à 2. Il existe un entier $k \geq 1$ et des nombres premiers $p_1, \ldots, p_k$ tels que

$$n = p_1 \cdots p_k \quad \text{et} \quad p_1 \leq \ldots \leq p_k \ .$$

De plus, cette décomposition est unique.

Démonstration. L'existence a déjà été démontrée dans l'exemple 2.29 du chapitre 1 — lorsque $n = p_1 \cdots p_k$ avec $p_1, \ldots p_k$ premiers, il suffit de réordonner les p_j pour avoir de plus $p_1 \leq \ldots \leq p_k$.
Passons à la preuve de l'unicité. Cela revient à prouver l'assertion suivante :

Assertion. Pour tout $k \in \mathbf{N}^*$, pour tout $\ell \in \mathbf{N}^*$, si $p_1, \ldots, p_k, q_1, \ldots, q_\ell$ sont des nombres premiers tels que $p_1 \cdots p_k = q_1 \cdots q_\ell$, $p_1 \leq \ldots \leq p_k$ et $q_1 \leq \ldots \leq q_\ell$, alors $k = \ell$ et $p_j = q_j$ pour tout $j = 1, \ldots, k$.

On procède par récurrence sur k.
Initialisation (pour $k = 1$) : Soit $\ell \in \mathbf{N}^*$ et $p_1, q_1, \ldots, q_\ell$ des nombres premiers tels que $p_1 = q_1 \cdots q_\ell$ et $q_1 \leq \ldots \leq q_\ell$. Comme q_1 divise p_1, qui est premier, on a $p_1 = q_1$. Si on suppose par l'absurde que $\ell \geq 2$, on obtient alors $1 = q_2 \cdots q_\ell > 1$; c'est une contradiction. Donc, on a $\ell = 1$.

Hypothèse de récurrence : pour tout $\ell \in \mathbf{N}^*$, si $p_1, \ldots, p_k, q_1, \ldots, q_\ell$ sont des nombres premiers tels que $p_1 \cdots p_k = q_1 \cdots q_\ell$, $p_1 \leq \ldots \leq p_k$ et $q_1 \leq \ldots \leq q_\ell$, alors $k = \ell$ et $p_j = q_j$ pour tout $j = 1, \ldots, k$.
Hérédité : Soit $\ell \in \mathbf{N}^*$ et $p_1, \ldots, p_{k+1}, q_1, \ldots, q_\ell$ des nombres premiers tels que $p_1 \cdots p_{k+1} = q_1 \cdots q_\ell$, $p_1 \leq \ldots \leq p_{k+1}$ et $q_1 \leq \ldots \leq q_\ell$. Par la proposition 4.5, il existe $i \in \{1, \ldots, \ell\}$ tel que p_{k+1} divise q_i ; comme q_i est premier, on a $p_{k+1} = q_i$. De même, il existe $i' \in \{1, \ldots, k+1\}$ tel que $p_{i'} = q_\ell$. Par maximalité de p_{k+1} et q_ℓ, il vient $p_{k+1} = q_\ell$, d'où $p_1 \cdots p_k = q_1 \cdots q_{\ell-1}$. On peut alors appliquer l'hypothèse de récurrence : on a $k = \ell - 1$ et $p_j = q_j$ pour tout $j = 1, \ldots, k$. Au total, on a $k + 1 = \ell$ et $p_j = q_j$ pour tout $j = 1, \ldots, k + 1$. □

Voici maintenant deux conséquences immédiates de ce théorème.

COROLLAIRE 4.7. *Soit n un entier inférieur ou égal à -2. Il existe un entier $k \geq 1$ et des nombres premiers $p_1, \ldots, p_k$ tels que*

$$n = -p_1 \cdots p_k \quad \text{et} \quad p_1 \leq \ldots \leq p_k \ .$$

De plus, cette décomposition est unique.

COROLLAIRE 4.8. *Soit n un entier satisfaisant $|n| \geq 2$. Il existe des entiers $\varepsilon \in \{\pm 1\}$ et $s \in \mathbf{N}^*$, des nombres premiers $p_1, \ldots, p_s$ et des entiers $\alpha_1, \ldots, \alpha_s \in \mathbf{N}^*$ tels que*

$$n = \varepsilon \cdot p_1^{\alpha_1} \cdots p_s^{\alpha_s} \quad \text{et} \quad p_1 < \ldots < p_s \ .$$

De plus, cette décomposition est unique.

DÉFINITION 4.9. *Soit n un entier satisfaisant $|n| \geq 2$. La décomposition du corollaire 4.8 est appelée* décomposition en facteurs premiers *de n.*

REMARQUE 4.10. Soit n un entier satisfaisant $|n| \geq 2$ et p un nombre premier. Alors, p divise n si et seulement si p apparaît dans la décomposition en facteurs premiers de n.

4.3. Le théorème d'Euclide. Comme première application de la décomposition en facteurs premiers, démontrons le résultat suivant.

THÉORÈME 4.11. *Il existe une infinité de nombres premiers.*

DÉMONSTRATION. Supposons par l'absurde qu'il n'existe qu'un nombre fini de nombres premiers et notons les $p_1, \ldots, p_k$. Soit alors le nombre $Q = p_1 \cdots p_k + 1$. On a $Q \equiv 1 \, [p_j]$ pour tout j, de sorte qu'aucun nombre premier ne divise Q. Dès lors, Q n'admet pas de décomposition en produit de facteurs premiers, en contradiction avec le corollaire 4.8. □

4.4. Décomposition en facteurs premiers, pgcd et ppcm. On peut détecter à l'aide des nombres premiers si deux entiers sont premiers entre eux ou non.

PROPOSITION 4.12. *Deux entiers a et b sont premiers entre eux si et seulement s'ils ne possèdent aucun diviseur premier commun.*

DÉMONSTRATION. On procède par contraposée (dans les deux sens). Si a et b possèdent un diviseur premier commun p, alors $\text{pgcd}(a,b)$ est multiple de p, si bien que a et b ne sont pas premiers entre eux.

Si a et b ne sont pas premiers entre eux, ils possèdent un diviseur commun $d \neq \pm 1$. Ce nombre d possède un divseur premier p, par le corollaire 4.8, qui est un diviseur premier commun de a et b. □

Notre prochain objectif, étant donnés deux entiers a, b satisfaisant $|a|, |b| \geq 2$, est de déterminer les décompositions en facteurs premiers de $\text{pgcd}(a,b)$ et $\text{ppcm}(a,b)$, en fonction de celles de a et b.

On se donne donc deux entiers a, b non nuls ; considérons une liste finie $p_1 < \ldots < p_k$ (avec $k \geq 1$) de nombres premiers qui contient tous les diviseurs premiers de a et tous ceux de b. Grâce au corollaire 4.8, on peut écrire :

$$\text{(4.1)} \qquad \begin{cases} a &= \delta \cdot p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \quad \text{avec } \delta = \pm 1 \text{ et } \alpha_1, \ldots, \alpha_k \in \mathbf{N} \ ; \\ b &= \varepsilon \cdot p_1^{\beta_1} \cdots p_k^{\beta_k}, \quad \text{avec } \varepsilon = \pm 1 \text{ et } \beta_1, \ldots, \beta_k \in \mathbf{N} \ . \end{cases}$$

Lorsque p_i n'apparaît pas dans la décomposition en facteurs premiers de a (resp. b), on a $\alpha_i = 0$, (resp. $\beta_i = 0$). Les nombres ± 1 s'écrivent $\pm 1 \cdot p_1^0 \cdots p_k^0$

EXEMPLE 4.13. Si $a = 60 = 2^2 \cdot 3 \cdot 5$ et $b = 70 = 2 \cdot 5 \cdot 7$, on trouve $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ et $p_4 = 7$ (on pourrait rajouter $p_5 = 11$ ou $p_5 = 17$, par exemple, mais cela ne serait d'aucune utilité). On écrit alors $a = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^0$ et $b = 2^1 \cdot 3^0 \cdot 5^1 \cdot 7^1$.

PROPOSITION 4.14. *Soit a, b deux entiers non nuls. Avec les notations de (4.1), a divise b si et seulement si on a $\alpha_i \leq \beta_i$ pour tout $i = 1, \ldots, k$.*

DÉMONSTRATION. Supposons d'abord qu'on a $\alpha_i \leq \beta_i$ pour tout $i = 1, \ldots, k$. On peut alors écrire $b = (\varepsilon/\delta) \cdot p_1^{\beta_1 - \alpha_1} \cdots p_k^{\beta_k - \alpha_k} \cdot a$. Comme $\varepsilon/\delta = \pm 1$, on voit que a divise b.

Supposons maintenant que a divise b, et supposons par l'absurde qu'il existe j tel que $\alpha_j > \beta_j$. Remarquons qu'on a alors $|b| \geq |a| \geq 2$. En effectuant le produit $b = (b/a) \cdot a$, on trouve une décomposition en facteurs premiers de b dans laquelle l'exposant de p_j est strictement supérieur à β_j. Ainsi, b possède deux décompositions en facteurs premiers distinctes, ce qui contredit le corollaire 4.8. On a ainsi démontré l'inégalité $\alpha_i \leq \beta_i$ pour tout $i = 1, \ldots, k$. □

EXEMPLE 4.15. Vu l'exemple 4.13, 60 ne divise pas 70 et 70 ne divise pas 60.

Bien sûr, on savait déjà démontrer cette assertion.

PROPOSITION 4.16.
Soit a, b deux entiers non nuls. Avec les notations de (4.1), on a

$$\text{pgcd}(a,b) = p_1^{\min(\alpha_1,\beta_1)} \cdots p_k^{\min(\alpha_k,\beta_k)} \qquad \textit{et} \qquad \text{ppcm}(a,b) = p_1^{\max(\alpha_1,\beta_1)} \cdots p_k^{\max(\alpha_k,\beta_k)} \ .$$

PREUVE DE LA PREMIÈRE ÉGALITÉ. Posons $d = p_1^{\min(\alpha_1,\beta_1)} \cdots p_k^{\min(\alpha_k,\beta_k)}$. Pour tout $n \in \mathbf{Z}$, on va montrer que n divise d si et seulement si n divise a et b ; pour ce faire, on distinguera deux cas. Soit $n \in \mathbf{Z}$.

1er cas : on suppose qu'il existe un nombre premier q, distinct de $p_1, \dots, p_k$, qui divise n. Alors n ne divise aucun des nombres d, a, b (voir le corollaire 4.8).

2e cas : on suppose que les diviseurs premiers de n font tous partie de la liste $p_1, \dots, p_k$ (en particulier, n n'est pas nul). On peut écrire $n = \zeta \cdot p_1^{\gamma_1} \cdots p_k^{\gamma_k}$ avec $\gamma, \dots, \gamma_k \in \mathbf{N}$ et $\zeta = \pm 1$; la proposition 4.14 nous donne alors la chaîne d'équivalences

$$n|d \Longleftrightarrow \gamma_i \leq \min(\alpha_i, \beta_i) \text{ pour tout } i \Longleftrightarrow [n|a \text{ et } n|b] \ .$$

Par la propostion 2.17, on trouve $\operatorname{pgcd}(a,b) = d = p_1^{\min(\alpha_1,\beta_1)} \cdots p_k^{\min(\alpha_k,\beta_k)}$. □

Exercice 4.17. Démontrer la seconde égalité de la proposition 4.16 de manière analogue.

Exemple 4.18. Vu l'exemple 4.13, on a

$$\operatorname{pgcd}(60,70) = 2^1 \cdot 3^0 \cdot 5^1 \cdot 7^0 = 10 \quad \text{et} \quad \operatorname{ppcm}(60,70) = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^1 = 420 \ .$$

4.5. Nombres premiers et congruences. Nous allons maintant établir quelques relations de congruence mettant en jeu des nombres premiers. Etant donnés deux entiers naturels $n \geq k$, rappelons que leur *coefficient binomial* est $\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}$, et que ce nombre est un entier. On rappelle également la *formule du binôme* : pour tous nombres complexes w, z et pour tout entier naturel n, on a $(w+z)^n = \sum_{j=0}^{n} \binom{n}{j} \cdot w^j z^{n-j}$.

Lemme 4.19. *Soit p un nombre premier. Pour tout entier k satisfaisant $1 \leq k \leq p-1$, le coefficient binomial $\binom{p}{k}$ est divisible par p.*

Démonstration. Soit k un entier satisfaisant $1 \leq k \leq p-1$. Comme k est strictement inférieur à p, aucun des nombres $1, 2, \dots, k$ n'est divisible par p. De même, comme $p-k$ est strictement inférieur à p, aucun des nombres $1, 2, \dots, p-k$ n'est divisible par p. Comme p est premier, $k!$ et $(p-k)!$ ne sont pas divisibles par p, par la proposition 4.5. Par ailleurs, on sait que p divise le nombre $p! = \binom{p}{k} \cdot k! \cdot (n-k)!$. Comme p est premier, il doit divisier un des facteurs $\binom{p}{k}$, $k!$ et $(n-k)!$ par la proposition 4.5. Ainsi, par élimination, p divise $\binom{p}{k}$. □

Proposition 4.20. *Soit p un nombre premier. Pour tous entiers a, b, on a $(a+b)^p \equiv a^p + b^p \, [p]$.*

Démonstration. On applique la formule du binôme : on a $(a+b)^p = \sum_{j=0}^{p} \binom{p}{j} \cdot a^j b^{p-j}$. Par le lemme précédent, on a $(a+b)^p \equiv \binom{p}{0} b^p + \binom{p}{p} a^p \equiv a^p + b^p \, [p]$. □

Exercice 4.21. Soit p est un nombre premier. Démontrer la formule $(a-b)^p \equiv a^p - b^p \, [p]$ pour tous entiers a, b. Distinguer les cas $p \neq 2$ et $p = 2$.

Proposition 4.22. *Soit p un nombre premier. Pour tout entier a, on a $a^p \equiv a \, [p]$.*

Démonstration. Montrons d'abord que pour tout $k \in \mathbf{N}$, on a $k^p \equiv k \, [p]$. On procède par récurrence sur k.

Initialisation (pour $k = 0$) : on a $0^p = 0$ et donc $0^p \equiv 0 \, [p]$.

Hypothèse de récurrence : on suppose que k^p est congru à k modulo p.

Hérédité : Par la proposition 4.20, on a $(k+1)^p \equiv k^p + 1 \, [p]$; l'hypothèse de récurrence donne alors $(k+1)^p \equiv k + 1 \, [p]$.

Soit maintenant a un entier. Si a est positif, on a prouvé la congruence $a^p \equiv a\,[p]$ ci-dessus. Si a est négatif, on a $(-1)^p a^p \equiv -a\,[p]$. On distingue alors deux cas :

1^{er} cas : supposons que p est impair. En multipliant par -1, on trouve $a^p \equiv a\,[p]$.

2^{e} cas : supposons que $p = 2$. On trouve alors $a^2 \equiv -a \equiv a\,[2]$.

Dans tous les cas, on a montré que $a^p \equiv a\,[p]$. □

COROLLAIRE 4.23. *Soit p un nombre premier, k, ℓ des entiers naturels non nuls et a un entier. Alors, on a $a^{k(p-1)+\ell} \equiv a^\ell\,[p]$.*

EXERCICE 4.24. Démontrer ce corollaire.

EXEMPLE 4.25. Calculons $55^{727236724}$ modulo 73. Par le corollaire, on a $55^{727236724} \equiv 55^4\,[73]$. Or, on a $55^2 = 3025 \equiv 32\,[73]$ et donc $55^4 \equiv 32^2 \equiv 1024 \equiv 2\,[73]$.

Terminons cette section par un résultat sur l'inversibilité des entiers modulo un nombre premier.

PETIT THÉORÈME DE FERMAT.
Si p est un nombre premier et si a est un entier tel que $a \not\equiv 0\,[p]$, alors $a^{p-1} \equiv 1\,[p]$.

EXERCICE 4.26. Démontrer ce théorème.

4.6. Détermination des nombres premiers. Le nombre 1573 est-il premier ? Quelle est la décomposition en facteurs premiers de 656845 ? Nous allons donner des méthodes pour répondre à ces questions. Cependant, elles sont difficiles d'utilisation, dans le sens que lorsque l'entier n devient grand, le temps de calcul nécessaire pour obtenir une réponse croît très vite. Ainsi, pour calculer le pgcd de deux grands nombres, l'algorithme d'Euclide s'avère plus efficace que le calcul des décompositions en facteurs premiers en vue d'appliquer la proposition 4.16.

LEMME 4.27. *Soit n un nombre naturel supérieur ou égal à 2. Si n n'est pas premier, alors il possède un diviseur premier p tel que $p \leq \sqrt{n}$.*

DÉMONSTRATION. Supposons que n n'est pas premier. Il existe des entiers naturels $k, \ell \geq 2$ tels que $n = k\ell$. Si on suppose que k et ℓ sont strictement supérieurs à $\sqrt{n}$, on obtient $n = k\ell > n$. Donc, quitte à échanger k et ℓ, on a $2 \leq k \leq \sqrt{n}$. Il suffit alors de choisir p parmi les diviseurs premiers de k. □

PREMIER TEST DE PRIMALITÉ. Pour savoir si un entier $n \geq 2$ est premier, il suffit de vérifier s'il possède un diviseur premier dans l'intervalle $[2, \sqrt{n}]$. En effet :
– s'il en possède un, alors il n'est pas premier ;
– s'il n'en possède pas, alors il est premier par le lemme précédent.

REMARQUE 4.28. Le test précédent est fastidieux, car il impose, si on ne sait pas lesquels sont premiers, de tester un par un tous les entiers entre 2 et $\sqrt{n}$.

TECHNIQUE DU CRIBLE D'ERATOSTHÈNE. Cette technique donne un algorithme qui permet de déterminer tous les nombres premiers jusqu'à un entier $n \geq 2$ fixé. On pose $E_0 = \{x \in \mathbf{N} : x \geq 2\}$

et $p_0 = 0$. Ensuite, on définit inductivement

$$p_k = \min\{x \in E_{k-1} : x > p_{k-1}\} \quad \text{et} \quad E_k = E_{k-1} \setminus \{y \cdot p_k : y \in \mathbf{N}, y \geq 2\}$$

pour tout $k \in \mathbf{N}^*$. Remarquons qu'à chaque étape E_{k-1} contient tous les nombres premiers ; en particulier, il est infini et donc p_k est bien défini..

Illustrons cette construction pour sur le sous-ensemble $\{x \in \mathbf{N} : 2 \leq x \leq 100\}$ à l'aide du tableau suivant, à compléter soi-même.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

$$\begin{aligned} p_1 &= 2 \\ p_2 &= \\ p_3 &= \\ p_4 &= \\ p_5 &= \\ p_6 &= \\ p_7 &= \end{aligned}$$

PROPOSITION 4.29. *Les trois ensembles suivants coïncident :*
– *l'ensemble* $E := \bigcap_{k \in \mathbf{N}} E_k$ *;*
– *l'ensemble* $\mathcal{P}$ *des nombres premiers ;*
– *l'ensemble* $P := \{p_1, p_2, \ldots, p_k, \ldots\}$.

DÉMONSTRATION. Remarquons tout d'abord que les trois ensembles sont contenus dans E_0 par définition. Démontrons les inclusions

$$\mathcal{P} \subseteq P \subseteq E \subseteq \mathcal{P} \ .$$

Soit $p \in \mathcal{P}$. On a déjà remarqué que E_k contient les nombres premiers pour tout k. On a donc $p \in E$. Comme on a $p_{j+1} \geq p_j + 1$ pour tout j, il existe $k \in \mathbf{N}$ tel que $p_k < p \leq p_{k+1}$. Comme p est un élément de E_k strictement supérieur à p_k, on doit avoir $p_{k+1} \leq p$ par définition de p_{k+1}. Donc, on a $p = p_{k+1} \in P$, ce qui prouve l'inclusion $\mathcal{P} \subseteq P$.

On démontre facilement (par récurrence) que p_k appartient à E_j pour tout $j \geq k$. De plus, on a $E_k \subseteq E_{k-1} \subseteq \ldots \subseteq E_0$. Ceci démontre l'inclusion $P \subseteq E$.

Enfin, soit $x \in E$ et soit p un diviseur premier de x. L'inclusion $\mathcal{P} \subseteq P$, déjà démontrée, entraîne $p \in P$. Ecrivons $p = p_k$ et $x = yp_k$ avec $y \in \mathbf{N}^*$. Comme x appartient à E_k, on doit avoir $y = 1$ et donc $x = p_k = p \in \mathcal{P}$. Ceci prouve l'inclusion $E \subseteq \mathcal{P}$. □

La proposition 4.29 caractérise les nombres premiers. Pour déterminer les nombres premiers jusqu'à un entier n fixé, le théorème suivant indique où on peut s'interrompre dans le calcul des nombres p_k et des ensembles E_k.

Théorème 4.30.
Soit k, n des nombres naturels tels que $n \geq 2$. Avec les notations ci-dessus, on a l'équivalence :

$$p_{k+1} > \sqrt{n} \iff \{p \in \mathcal{P} : p \leq n\} = \{x \in E_k : x \leq n\} \ .$$

On a déjà remarqué que $p_{k+1} \geq p_k + 1$, et donc $p_k \geq k$ (par récurrence). Par conséquent, pour tout $n \geq 2$, il existe $k \in \mathbf{N}$ tel que $\{p \in \mathcal{P} : p \leq n\} = \{x \in E_k : x \leq n\}$.

Démonstration. On procède par contraposée dans chacun des deux sens. Supposons d'abord que $p_{k+1} \leq \sqrt{n}$. On constate alors que p_{k+1}^2, dont les diviseurs positifs sont 1, p_{k+1} et p_{k+1}^2, n'est divisible par aucun des nombres $p_1, p_2, \ldots, p_k$. Par conséquent, p_{k+1}^2 appartient à $\{x \in E_k : x \leq n\}$, mais pas à $\{p \in \mathcal{P} : p \leq n\}$.
Supposons maintenant que $\{p \in \mathcal{P} : p \leq n\} \neq \{x \in E_k : x \leq n\}$. Comme on a $\mathcal{P} = E \subseteq E_k$ d'après la proposition 4.29, il existe un entier x tel que $x \leq n$ dans $E_k \setminus \mathcal{P}$. Par le lemme 4.27, x possède un diviseur premier p tel que $p \leq \sqrt{n}$. Comme x est dans E_k, on a $p \notin \{p_1, \ldots, p_k\}$ et donc, toujours en vertu de la proposition 4.29, $p = p_j$ avec $j \geq k+1$. On en déduit que $p_{k+1} \leq p_j \leq \sqrt{n}$. □

Exercice 4.31. (1) Faire la liste des nombres premiers jusqu'à 120.

(2) Quelle est la plus petite valeur de k telle que les ensembles $\{p \in \mathcal{P} : p \leq 10000\}$ et $\{x \in E_k : x \leq 10000\}$ coïncident ? Que vaut alors p_k ?

4.7. Calcul d'une décomposition en facteurs premiers. Soit a un entier satisfaisant $|a| \geq 2$. Commment calculer la décomposition en facteurs premiers de a ? Pour commencer, le calcul de la décomposition de a se ramène à celui de la décomposition de $|a|$, car $a = \mathrm{sgn}(a) \cdot |a|$. Ensuite, on peut :

(1) trouver la liste des nombres premiers inférieurs ou égaux à $\sqrt{|a|}$ grâce au crible d'Eratosthène — si un nombre $n \leq |a|$ n'a pas de diviseur dans cette liste, alors il est premier par le lemme 4.27 ;

(2) tester les nombres de la liste, jusqu'à ce qu'on trouve tous les facteurs premiers de $|a|$ — le dernier étant éventuellement un nombre qui n'est pas dans la liste, mais qui est premier en vertu du lemme 4.27.

Pour donner une idée plus précise de cet algorithme, voyons plus concrètement comment procéder sur deux exemples.

Exemple 4.32. Calculons la décomposition de $a = -1700$:

(1) le crible d'Eratosthène nous a déjà fourni la liste des nombres premiers jusqu'à 100 — et 100 est plus grand que $\sqrt{1700}$;

(2) on voit que 2^2 divise 1700, mais 2^3 ne divise pas 1700 ;

(3) on calcule $1700/2^2 = 425$;

(4) on voit que 3 ne divise pas 425 ;

(5) on voit que 5^2 divise 425, mais 5^3 ne divise pas 425 ;

(6) on calcule $425/5^2 = 17$;
(7) on voit que 7, 11 et 13 ne divisent pas 17 ;
(8) enfin, on voit que $17 = 17$.

Au total, on a $1700 = 2^2 \cdot 425 = 2^2 \cdot 5^2 \cdot 17$. La décomposition en facteurs premiers de -1700 est $(-1) \cdot 2^2 \cdot 5^2 \cdot 17$.

Exemple 4.33. Calculons la décomposition de $a = 7119$:

(1) le crible d'Eratosthène nous a déjà fourni la liste des nombres premiers jusqu'à 100 — et 100 est plus grand que $\sqrt{7119}$;
(2) on voit que 2 ne divise pas 7119 ;
(3) on voit que 3^2 divise 7119, mais 3^3 ne divise pas 7119 ;
(4) on calcule $7119/3^2 = 791$;
(5) on voit que 5 ne divise pas 791 ;
(6) on voit que 7 divise 791, mais 7^2 ne divise pas 791 ;
(7) on calcule $791/7 = 113$;
(8) on voit que 113 n'a aucun diviseur premier inférieur ou égal à $\sqrt{113} = 10,6301\ldots$;
(9) le lemme 4.27 assure que 113 est premier.

Au total, on a $7119 = 3^2 \cdot 791 = 3^2 \cdot 7 \cdot 113$. C'est la décomposition en facteurs premiers de 7119.

Remarque culturelle 4.34. L'algorithme de calcul de la décomposition en facteurs premiers peut être optimisé. On peut néanmoins retenir que ce calcul est très lent, même avec les meilleurs algorithmes connus. C'est d'ailleurs sur cette lenteur que se base la sécurité de la cryptographie RSA, qui est l'une des plus utilisées au monde.

CHAPITRE 4

Polynômes à coefficients dans Q, R ou C

Dans ce chapitre, la lettre $\mathbf{K}$ *désignera indifféremment l'un des corps* $\mathbf{Q}$, $\mathbf{R}$ *ou* $\mathbf{C}$ *;*
la lettre X *désignera l'application identité* $\mathbf{C} \to \mathbf{C}; z \mapsto z$.

1. «Rappels» sur les familles libres et les familles génératrices

Soit E un $\mathbf{K}$-espace vectoriel, où $\mathbf{K}$ est l'un des corps $\mathbf{Q}$, $\mathbf{R}$ ou $\mathbf{C}$; soit $(v_i)_{i\in I}$ une famille (éventuellement infinie) d'éléments de E.

DÉFINITION 1.1. *Le* $\mathbf{K}$-sous-espace vectoriel engendré *par la famille* $(v_i)_{i\in I}$ *est l'ensemble des vecteurs de* E *de la forme* $\sum_{j\in J} \alpha_j v_j$*, où* J *est une partie finie de* I *et* $\alpha_j \in \mathbf{K}$ *pour tout* $j \in J$.

Autrement dit, le $\mathbf{K}$-sous-espace vectoriel engendré par la famille $(v_i)_{i\in I}$ est l'ensemble des vecteurs de E de la forme $\sum_{i\in I} \alpha_i v_i$, où les coefficients α_i sont dans $\mathbf{K}$ pour tout $i \in I$ et tous nuls sauf un nombre fini.

A titre d'exercice, vous pouvez démontrer que c'est bien un $\mathbf{K}$-sous-espace vectoriel de E et qu'il est contenu dans tout $\mathbf{K}$-sous-espace vectoriel de E qui contient la partie $\{v_i : i \in I\}$.

DÉFINITION 1.2. *La famille* $(v_i)_{i\in I}$ *est* libre *si, pour tout* $n \in \mathbf{N}^*$*, pour tous indices* $i_1, \dots, i_n \in I$ DEUX À DEUX DISTINCTS *et pour tous* $\alpha_1, \dots, \alpha_n \in \mathbf{K}$*, on a l'implication*

$$\sum_{k=1}^{n} \alpha_k v_{i_k} = 0 \quad \Longrightarrow \quad (\alpha_1, \dots, \alpha_n) = (0, \dots, 0) \ .$$

Il est facile de vérifier que la famille $(v_i)_{i\in I}$ est libre si et seulement si, pour tout partie finie $J \subseteq I$, la sous-famille finie $(v_i)_{i\in J}$ est libre (au sens vu en S1).

DÉFINITION 1.3. *La famille* $(v_i)_{i\in I}$ *est une* base *de* E *si :*
– *elle est libre, et*
– *le* $\mathbf{K}$*-sous-espace vectoriel engendré par* $(v_i)_{i\in I}$ *est* E.

A titre d'exercice, vous pouvez démontrer que $(v_i)_{i\in I}$ est une base de E si et seulement si tout élément $x \in E$ s'écrit de manière unique sous la forme $x = \sum_{i\in I} \alpha_i v_i$, où les coefficients α_i sont dans $\mathbf{K}$ pour tout $i \in I$ et tous nuls sauf un nombre fini.

2. Préliminaires sur les fonctions de C dans C

On rappelle que l'ensemble, que nous noterons $\mathcal{F}(\mathbf{C}, \mathbf{C})$, des applications de $\mathbf{C}$ dans $\mathbf{C}$ est un $\mathbf{C}$-espace vectoriel pour les opérations d'addition et de multiplication définies par les formules

$$(f + g)(z) := f(z) + g(z) \quad \text{et} \quad (\lambda f)(z) := \lambda f(z) \ .$$

C'est donc *a fortiori* un **K**-espace vectoriel. Si vous n'avez jamais démontré ces points, la preuve est laissée en exercice. On peut également définir un produit sur $\mathcal{F}(\mathbf{C},\mathbf{C})$ par la formule

$$(f\cdot g)(z) := f(z)\cdot g(z)\ .$$

Dans la suite, nous noterons $\mathbf{1}$ l'application $\mathbf{C}\to\mathbf{C}; z\mapsto 1$. Rappelons que pour $f,g\in\mathcal{F}(\mathbf{C},\mathbf{C})$, la notation $g\circ f$ désigne l'application composée, qui est définie par la formule $(g\circ f)(z)=g(f(z))$.

PROPOSITION 2.1. *Pour toutes $f,g,h\in\mathcal{F}(\mathbf{C},\mathbf{C})$ et pour tout $\lambda\in\mathbf{C}$, les propriétés suivantes sont satisfaites :*

(1) $f\cdot(g\cdot h)=(f\cdot g)\cdot h$;
(2) $f\cdot g=g\cdot f$;
(3) $f\cdot(g+h)=(f\cdot g)+(f\cdot h)$ *et* $(f+g)\cdot h=(f\cdot h)+(g\cdot h)$;
(4) $(\lambda\mathbf{1})\cdot f=\lambda f=f\cdot(\lambda\mathbf{1})$ — *et donc en particulier* $\mathbf{1}\cdot f=f=f\cdot\mathbf{1}$;
(5) $(\lambda g)\circ h=\lambda(g\circ h)$;
(6) $(f+g)\circ h=(f\circ h)+(g\circ h)$;
(7) $(f\cdot g)\circ h=(f\circ h)\cdot(g\circ h)$.

EXERCICE 2.2. Démontrer cette proposition. Ensuite, vérifier (en donnant des contre-exemples) que les propriétés $f\circ(g+h)=(f\circ g)+(f\circ h)$ et $f\circ(g\cdot h)=(f\circ g)\cdot(f\circ h)$ ne sont pas satisfaites pour toutes $f,g,h\in\mathcal{F}(\mathbf{C},\mathbf{C})$.

En vertu du point (4) de la proposition 2.1, on peut se permettre l'abus de langage suivant : pour tout $\lambda\in\mathbf{C}$, on notera λ la fonction $\lambda\mathbf{1}$, c'est-à-dire la fonction constante de valeur λ. Ceci permet d'identifier $\mathbf{C}$ à la partie de $\mathcal{F}(\mathbf{C},\mathbf{C})$ formée des applications constantes. Rappelons qu'on note X l'application identité de $\mathbf{C}$ dans $\mathbf{C}$.

REMARQUE 2.3. Si on convient de poser $X^0=\mathbf{1}$, on vérifie facilement que X^n est l'application $\mathbf{C}\to\mathbf{C}; z\mapsto z^n$ pour tout $n\in\mathbf{N}$.

PROPOSITION 2.4. *Soit $P=\sum_{k=0}^n a_kX^k$ une combinaison linéaire (à coefficients dans $\mathbf{C}$) de vecteurs de la famille $(X^k)_{k\in\mathbf{N}}$. Si $P(x)=0$ pour tout $x\in\mathbf{R}$, alors les coefficients $a_0,\dots,a_n$ sont tous nuls.*

MISE EN GARDE. Les combinaisons linéaires sont par définition des sommes **finies**. Ainsi, par exemple, $\sum_{k\in\mathbf{N}}\frac{1}{k!}X^k$ n'est **pas** une combinaison linéaire de vecteurs de la famille $(X^k)_{k\in\mathbf{N}}$; ce n'est donc **pas** un polynôme (au sens de la définition 3.1 ci-dessous).

COROLLAIRE 2.5 (immédiat).
(1) *Pour tout entier naturel n, la famille $(X^0,X^1,\dots,X^n)$ est libre dans le **K**-espace vectoriel $\mathcal{F}(\mathbf{C},\mathbf{C})$.*
(2) *La famille $(X^k)_{k\in\mathbf{N}}$ est libre dans le **K**-espace vectoriel $\mathcal{F}(\mathbf{C},\mathbf{C})$.*

PREUVE DE LA PROPOSITION 2.4. Supposons par l'absurde qu'il existe un entier naturel n et des nombres complexes $a_0,a_1,\dots,a_n$, avec $a_n\neq 0$, tels que l'application

$$a_0X^0+a_1X^1+\cdots+a_nX^n$$

soit nulle sur $\mathbf{R}$. Pour tout k, on peut écrire $a_k = b_k + ic_k$ avec b_k, c_k réels. Pour tout $x \in \mathbf{R}$, on trouve

$$(b_0 + b_1 x + \cdots + b_n x^n) + i(c_0 + c_1 x + \cdots + c_n x^n) = 0 \ .$$

Comme le premier terme est réel et le second imaginaire pur, il vient

$$b_0 + b_1 x + \cdots + b_n x^n = 0 \quad \text{et} \quad c_0 + c_1 x + \cdots + c_n x^n = 0$$

pour tout $x \in \mathbf{R}$. En dérivant n fois ces égalités, on obtient $b_n \cdot n! = 0$ et $c_n \cdot n! = 0$, d'où $a_n = 0$. C'est une contradiction ; on a démontré la proposition. □

3. Définition des polynômes et règles de calcul

Définition 3.1.
On note $\mathbf{K}[X]$ *le* $\mathbf{K}$*-sous-espace vectoriel de* $\mathcal{F}(\mathbf{C}, \mathbf{C})$ *engendré par la famille* $(X^k)_{k\in\mathbf{N}}$*. On appelle* polynômes à coefficients dans $\mathbf{K}$ *les éléments de* $\mathbf{K}[X]$*.*

Remarque 3.2. On a les inclusions $\mathbf{Q}[X] \subseteq \mathbf{R}[X] \subseteq \mathbf{C}[X]$. On s'autorisera donc, dans ce cours, à écrire «polynôme» au lieu de «polynôme à coefficients dans $\mathbf{C}$».

Par le corollaire 2.5, la famille $(X^n)_{n\in\mathbf{N}}$ est une base du $\mathbf{K}$-espace vectoriel $\mathbf{K}[X]$. Autrement dit, $\mathbf{K}[X]$ est l'ensemble des $\sum_{k\in\mathbf{N}} a_k X^k$ telles que les coefficients a_k soient tous dans $\mathbf{K}$ et nuls à partir d'un certain rang ; de plus un polynôme P à coefficients dans $\mathbf{K}$ n'admet qu'une seule écriture sous la forme $P = \sum_{k\in\mathbf{N}} a_k X^k$ (telle que les coefficients a_k soient tous dans $\mathbf{K}$ et nuls à partir d'un certain rang).

Remarque 3.3. Les sommes $\sum_{k\in\mathbf{N}} a_k X^k$ telle que les coefficients a_k soient nuls à partir d'un certain rang sont en fait des sommes **finies**, dans le sens qu'elles ne comprennent qu'un nombre fini de termes non nuls.

Remarque culturelle 3.4. La définition 3.1 n'est pas la définition standard de la notion de polynôme. Dans la plupart des ouvrages, elle correspond plutôt à la notion de *fonction polynomiale*, qui est "équivalente" à la notion de polynôme lorsqu'on prend les coefficients dans $\mathbf{Q}$, $\mathbf{R}$ ou $\mathbf{C}$. La définition 3.1 a été choisie pour ses vertus simplificatrices, mais il faut être conscient qu'elle ne se laisse pas généraliser facilement à d'autres types de coefficients !

Définition 3.5.
Soit $P = \sum_{k\in\mathbf{N}} a_k X^k$ *un polynôme non nul. Le* degré *de* P *est l'entier naturel*

$$\deg(P) := \max\{n \in \mathbf{N} : a_n \neq 0\} \ .$$

On convient en outre que le degré du polynôme nul est $-\infty$*.*

Remarquons que si $P = \sum_{k\in\mathbf{N}} a_k X^k$ est un polynôme non nul et si $m = \deg(P)$, alors le coefficient a_m est non nul.

Définition 3.6. *Soit* $P = \sum_{k\in\mathbf{N}} a_k X^k$ *un polynôme non nul et soit* $m = \deg(P)$*. Le coefficient* a_m *est appelé* coefficient dominant *de* P*. Si ce coefficient est* 1*, on dit que* P *est* unitaire*.*

EXEMPLE 3.7. On a $\deg(1) = 0$, $\deg(2X) = 1$ et $\deg(1 + 5X - 7X^2 - 4X^7) = 7$. Les coefficients dominants des polynômes 1, $2X$ et $1+5X-7X^2-4X^7$ sont respectivement 1, 2 et -4. (Suivant la convention énoncée précédemment, on note 1 le polynôme $1 \cdot X^0 = 1 \cdot \mathbf{1}$.)

REMARQUE 3.8. Les fonctions constantes (à valeur dans $\mathbf{K}$) sont des polynômes à coefficients dans $\mathbf{K}$. De plus, un polynôme est constant (c'est-à-dire est une fonction constante) si et seulement si son degré est égal à 0 ou $-\infty$.

PROPOSITION 3.9 (RÈGLES DE CALCUL POUR LES POLYNÔMES)**.**
Soit $P = \sum_{k\in\mathbf{N}} a_k X^k$ et $Q = \sum_{k\in\mathbf{N}} b_k X^k$ deux polynômes à coefficients dans $\mathbf{K}$. Alors :

(1) *la somme $P+Q$ est un polynôme à coefficients dans $\mathbf{K}$ et $P+Q = \sum_{k\in\mathbf{N}}(a_k+b_k)X^k$; de plus on a $\deg(P+Q) \leq \max\{\deg(P), \deg(Q)\}$, avec égalité si $\deg(P) \neq \deg(Q)$;*

(2) *le produit $P \cdot Q$ est un polynôme à coefficients dans $\mathbf{K}$ et $P \cdot Q = \sum_{k\in\mathbf{N}} c_k X^k$, où $c_k = \sum_{j=0}^{k} a_j b_{k-j}$ pour tout k ; de plus on a $\deg(P \cdot Q) = \deg(P) + \deg(Q)$;*

(3) *la composée $P \circ Q$ est un polynôme à coefficients dans $\mathbf{K}$ et $P \circ Q = \sum_{k\in\mathbf{N}} a_k Q^k$; de plus, si P et Q sont non constants, on a $\deg(P \circ Q) = \deg(P) \cdot \deg(Q)$.*

Pour calculer la somme $\deg(P) + \deg(Q)$ lorsque $P = 0$ ou $Q = 0$, on utilise la convention de calcul classique : $(-\infty) + n = -\infty = n + (-\infty)$ pour tout $n \in \mathbf{N}$ et $(-\infty) + (-\infty) = -\infty$

REMARQUE 3.10. Si P est un polynôme à coefficients dans $\mathbf{K}$ et $\lambda \in \mathbf{K}$, alors λP est un polynôme à coefficients dans $\mathbf{K}$. De plus, si $\lambda \neq 0$, on a $\deg(\lambda P) = \deg(P)$.

Cette remarque est très simple à vérifier pour elle-même ; en utilisant l'identification $\lambda = \lambda\mathbf{1}$, on peut aussi la voir comme un cas particulier du point (2) de la proposition 3.9.

PREUVE DE LA PROPOSITION 3.9. Si $P = 0$ ou $Q = 0$, les assertions (1) à (3) sont faciles à vérifier (ce point est laissé en exercice). Démontrons les lorsque P et Q sont non nuls. Posons $m = \deg(P)$ et $n = \deg(Q)$; ce sont des entiers naturels.

(1) Comme $(X^k)_{k\in\mathbf{N}}$ est une base du $\mathbf{K}$-espace vectoriel $\mathbf{K}[X]$, on voit que $P + Q \in \mathbf{K}[X]$ et $P + Q = \sum_{k\in\mathbf{N}}(a_k + b_k)X^k$. Si $k > \max\{m, n\}$, on trouve $a_k + b_k = 0 + 0 = 0$ et donc $\deg(P + Q) \leq \max\{m, n\}$. Si $m < n$, on obtient $a_n + b_n = 0 + b_n \neq 0$ et donc $\deg(P + Q) = n = \max\{m, n\}$. Si $m > n$, on trouve de même $\deg(P + Q) = m = \max\{m, n\}$.

(2) Posons $c_k := \sum_{j=0}^{k} a_j b_{k-j} = 0$ pour tout $k \in \mathbf{N}$. Notons que les coefficients c_k sont dans $\mathbf{K}$, puisque $\mathbf{K}$ est stable par multiplication et par addition. Par la proposition 2.1, on a

$$P \cdot Q = \left(\sum_{j=0}^{m} a_j X^j\right) \cdot \left(\sum_{\ell=0}^{n} b_\ell X^\ell\right) = \sum_{j=0}^{m}\sum_{\ell=0}^{n} a_j b_\ell X^{j+\ell} = \sum_{k=0}^{m+n} c_k X^k \ .$$

Ainsi $P \cdot Q$ est un polynôme à coefficients dans $\mathbf{K}$ et satisfait $\deg(P \cdot Q) \leq \deg(P) + \deg(Q)$. En particulier, on a

$$\begin{aligned} c_{m+n} &= \sum_{j=0}^{m+n} a_j b_{m+n-j} = \sum_{j=0}^{m-1} a_j b_{m+n-j} + a_m b_n + \sum_{j=m+1}^{m+n} a_j b_{m+n-j} \\ &= \sum_{j=0}^{m-1} a_j \cdot 0 + a_m b_n + \sum_{j=m+1}^{m+n} 0 \cdot b_{m+n-j} = a_m b_n \ . \end{aligned}$$

Par hypothèse, a_m et b_n sont non nuls, et donc c_{m+n} aussi. Ceci démontre l'égalité $\deg(P \cdot Q) = \deg(P) + \deg(Q)$. Enfin, un calcul analogue au précédent montre que $c_k = 0$ pour tout $k > m+n$, ce qui achève la preuve de la formule $P \cdot Q = \sum_{k \in \mathbf{N}} c_k X^k$.

(3) Par la proposition 2.1, on a

$$P \circ Q = \left(\sum_{k=0}^{m} a_k X^k \right) \circ Q = \sum_{k=0}^{m} a_k (X \circ Q)^k = \sum_{k=0}^{m} a_k Q^k \ .$$

Ceci prouve que $P \circ Q = \sum_{k \in \mathbf{N}} a_k Q^k$. De plus, par (1) et (2) $P \circ Q$ est un polynôme à coefficients dans $\mathbf{K}$. Supposons maintenant que P et Q sont non constants, c'est-à-dire que $m \geq 1$ et $n \geq 1$. Par (1) et (2), on a immédiatement $\deg(Q^k) = kn$ pour tout k, ce qui entraîne $\deg(\sum_{k=0}^{m-1} a_k Q^k) \leq (m-1)n < \deg(a_m Q^m)$. En appliquant le point (1) une fois encore, on trouve $\deg(P \circ Q) = mn$. □

COROLLAIRE 3.11. *Pour tout entier naturel n, les polynômes à coefficients dans $\mathbf{K}$ et de degré inférieur ou égal à n forment un $\mathbf{K}$-sous-espace vectoriel de $\mathbf{K}[X]$, que nous noterons $\mathbf{K}[X]_{\leq n}$.*

Ce corollaire découle immédiatement de la proposition 3.9. Il est alors très facile de vérifier que $(X^0, X^1, \ldots, X^n)$ est une base de ce sous-espace vectoriel.

PROPOSITION 3.12. *Soit $a \in \mathbf{K}$; posons $(X-a)^0 := \mathbf{1}$.*

(1) *Pour tout $n \in \mathbf{N}$, la famille $\big((X-a)^0, \ldots, (X-a)^n\big)$ est une base de $\mathbf{K}[X]_{\leq n}$.*

(2) *La famille $\big((X-a)^k\big)_{k \in \mathbf{N}}$ est une base de $\mathbf{K}[X]$.*

EXERCICE 3.13. Démontrer cette proposition.

EXEMPLE 3.14. Posons $P = X^2 + X + 1$ et $Q = X^3 + 1$. Les calculs donnent :

$$\begin{aligned} P + Q &= X^3 + X^2 + X + 2 = Q + P \\ P \cdot Q &= X^5 + X^4 + X^3 + X^2 + X + 1 = Q \cdot P \\ P \circ Q &= (X^3+1)^2 + (X^3+1) + 1 = X^6 + 3X^3 + 3 \\ Q \circ P &= (X^2+X+1)^3 + 1 = (X^2+X+1)(X^4 + 2X^3 + 3X^2 + 2X + 1) + 1 = \\ &= X^6 + 3X^5 + 6X^4 + 7X^3 + 6X^2 + 3X + 2 \ . \end{aligned}$$

On remarque que $P \circ Q \neq Q \circ P$.

NOTATION. Si $P, Q \in \mathbf{K}[X]$ avec $Q = \sum_{k \in \mathbf{N}} b_k X^k$, on s'autorise à écrire $P(\sum_{k \in \mathbf{N}} b_k X^k)$ au lieu de $P \circ (\sum_{k \in \mathbf{N}} b_k X^k)$. Ainsi, si $P = X^2 + X + 1$ et $Q = X^3 + 1$ comme avant, on écrira

$$P(X^3+1) = X^6 + 3X^3 + 3 \ \text{ et } \ Q(X^2+X+1) = X^6 + 3X^5 + 6X^4 + 7X^3 + 6X^2 + 3X + 2 \ .$$

REMARQUE 3.15. Si $P = X^2 - 3X + 2$ et $Q = 2$, on voit que $P \circ Q = 0$ par calcul. Dans ce cas, l'égalité $\deg(P \circ Q) = \deg(P) \cdot \deg(Q)$ n'est pas satisfaite.

4. Division de polynômes

DÉFINITION 4.1. *Soit $A, B \in \mathbf{K}[X]$. On dit que A* divise *B dans $\mathbf{K}[X]$ s'il existe un polynôme $Q \in \mathbf{K}[X]$ tel que $B = A \cdot Q$.*

Lorsque le contexte est suffisamment clair, on s'autorise à écrire «A divise B» plutôt que «A divise B dans $\mathbf{K}[X]$». Comme dans le cas des nombres entiers, il arrive que B ne soit pas divisible par A. C'est le cas, par exemple, si $A = X^2 + X + 1$ et $B = X + 1$.

EXERCICE 4.2. Soit $A, B \in \mathbf{K}[X]$, avec $B \neq 0$. Démontrer les assertions suivantes :

(1) si A divise B, alors on a $\deg A \leq \deg B$;
(2) si A divise B et si $A(z) = 0$ (pour un certain $z \in \mathbf{C}$), alors $B(z) = 0$.

Comme dans le cas des nombres entiers, il existe une opération de *division euclidienne* sur $\mathbf{K}[X]$.

THÉORÈME 4.3.
Pour tous polynômes $A, B \in \mathbf{K}[X]$, avec $B \neq 0$, il existe un unique couple $(Q, R) \in \mathbf{K}[X] \times \mathbf{K}[X]$ tel que

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

Ce théorème est à comparer avec le théorème 1.8 du chapitre 3.

DÉFINITION 4.4. *Les polynômes Q et R du théorème 4.3 sont le* quotient *et le* reste *de la division euclidienne de A par B.*

DÉMONSTRATION. On commence par démontrer l'existence. On pose $m = \deg(B)$, $Q_0 = 0$ et $R_0 = A$. Ensuite, tant que $n(k) := \deg(R_k) \geq m$, on pose

$$Q_{k+1} = Q_k + \frac{r_{n(k)}}{b_m} X^{n(k)-m} \quad \text{et} \quad R_{k+1} = R_k - \frac{r_{n(k)}}{b_m} X^{n(k)-m} \cdot B \ ,$$

où $B = \sum_{i=0}^{m} b_i X^i$ et $R_k = \sum_{j=0}^{n(k)} r_j X^j$. Enfin, dès que $n(k) := \deg(R_k) < m$, on pose $Q_{k+1} = Q_k$ et $R_{k+1} = R_k$. Ceci définit deux suites de polynômes $(Q_k)_{k \in \mathbf{N}}$ et $(R_k)_{k \in \mathbf{N}}$. Par récurrence, démontrons que $A = Q_k \cdot B + R_k$ pour tout $k \in \mathbf{N}$.

Initialisation : il est clair que $Q_0 \cdot B + R_0 = 0 + A = A$.

Hypothèse de récurrence : on suppose que $A = Q_k \cdot B + R_k$.

Hérédité : démontrons que $A = Q_{k+1} \cdot B + R_{k+1}$. On distingue deux cas. Si $n(k) < m$, on a $Q_{k+1} = Q_k$ et $R_{k+1} = R_k$, de sorte qu'il suffit d'appliquer l'hypothèse de récurrence. Si $n(k) \geq m$, on trouve

$$Q_{k+1} \cdot B + R_{k+1} = \left(Q_k + \frac{r_{n(k)}}{b_m} X^{n(k)-m} \right) \cdot B + R_k - \frac{r_{n(k)}}{b_m} X^{n(k)-m} \cdot B = Q_k \cdot B + R_k$$

et on conclut grâce à l'hypothèse de récurrence.

Démontrons maintenant qu'il existe k_0 tel que $n(k_0) < m$. Pour ce faire, supposons par l'absurde que $n(k) > m$ pour tout k. Avec les notations qui précèdent, on aurait

$$R_{k+1} = R_k - \frac{r_{n(k)}}{b_m} X^{n(k)-m} \cdot B = \sum_{j=0}^{n(k)} r_j X^j - \frac{r_{n(k)}}{b_m} X^{n(k)-m} \cdot \sum_{i=0}^{m} b_i X^i = \sum_{j=0}^{n(k)-1} c_j X^j + 0X^{n(k)} ,$$

de sorte que $n(k+1) \leq n(k) - 1$ pour tout k. Par suite, il viendrait alors $n(\deg(A) + 1) = n(n(0) + 1) < 0 \leq m$, ce qui est impossible. On a prouvé l'existence de k_0.

En posant, $Q = Q_{k_0}$ et $R = R_{k_0}$, on obtient un couple de polynômes (Q, R) qui satisfait aux conditions du théorème.

Démontrons maintenant l'unicité : considérons deux couples (Q, R) et (Q', R') satisfaisant aux conditions du théorème. On a l'égalité $(Q-Q')\cdot B = R'-R$, de sorte que le degré de $(Q-Q')\cdot B$ est strictement inférieur à $\deg(B)$ par la proposition 3.9. Comme B est non nul, la proposition 3.9 entraîne $\deg(Q-Q') + \deg(B) < \deg(B)$, d'où $\deg(Q-Q') < 0$. Par suite, il vient $Q = Q'$, puis $R = R'$. □

Exemple 4.5. Appliquons l'algorithme de la preuve aux polynômes $A = 2X^4 + 5X^3 - \frac{1}{2}X - 7$ et $B = 3X^2 - 7X + 4$. On trouve :

$$\begin{array}{lllllll} Q_0 & = & 0 & \text{et} & R_0 & = & 2X^4 + 5X^3 - \frac{1}{2}X - 7 \ ; \\ Q_1 & = & \frac{2}{3}X^2 & \text{et} & R_1 & = & \frac{29}{3}X^3 - \frac{8}{3}X^2 - \frac{1}{2}X - 7 \ ; \\ Q_2 & = & \frac{2}{3}X^2 + \frac{29}{9}X & \text{et} & R_2 & = & \frac{179}{9}X^2 - \frac{241}{18}X - 7 \ ; \\ Q_3 & = & \frac{2}{3}X^2 + \frac{29}{9}X + \frac{179}{27} & \text{et} & R_3 & = & \frac{1783}{54}X - \frac{905}{27} \ . \end{array}$$

Le degré de R_3 est strictement inférieur à celui de B ; la division euclidienne de A par B donne donc $Q = \frac{2}{3}X^2 + \frac{29}{9}X + \frac{179}{27}$ comme quotient et $R = \frac{1783}{54}X - \frac{905}{27}$ comme reste.

Remarque culturelle 4.6. L'analogie entre les nombres entiers et les polynômes peut être poussée plus loin (mais cela dépasse le programme de ce cours). On peut définir le plus grand diviseur commun et le plus petit multiple commun d'un couple de polynômes et démontrer des résultats analogues à ceux de la section 2 du chapitre 3. On peut ensuite les utiliser pour prouver que tout polynôme non constant à coefficients dans $\mathbf{K}$ admet une décomposition, essentiellement unique, en produit de polynômes "premiers" ; c'est un analogue du corollaire 4.8 du chapitre 3. Dans la suite, nous démontrerons un tel théorème de décomposition (voir le théorème 6.2) en faisant usage d'un autre outil : le théorème de d'Alembert-Gauss.

5. Racines et polynômes irréductibles

5.1. Racines d'un polynôme.

Commençons par la définition.

Définition 5.1. *Soit P un polynôme. Une* racine *de P est un nombre complexe z tel que $P(z) = 0$. Les racines sont parfois appelées* zéros. *On note $\mathcal{Z}(P)$ l'ensemble des racines de P.*

Proposition 5.2.
Soit $P \in \mathbf{K}[X]$ et $a \in \mathbf{K}$. Alors,

a est une racine de P si et seulement si P est divisible par $X - a$ dans $\mathbf{K}[X]$.

DÉMONSTRATION. Supposons d'abord que a est une racine de P. Par division euclidienne, on peut écrire $P = (X-a)\cdot Q + R$ avec $Q, R \in \mathbf{K}[X]$ et $\deg(R) < 1$. Par suite, R est un polynôme constant, disons $R = \lambda \in \mathbf{K}$. En évaluant en a, on trouve $P(a) = 0 + \lambda$. Comme a est une racine de P, on voit que $R = \lambda = 0$, si bien que $P = (X-a)\cdot Q$. On a prouvé que $X - a$ divise P.

Supposons maintenant que P est divisible par $X - a$; on a donc $P = (X-a)\cdot Q$ avec $Q \in \mathbf{K}[X]$. Par suite, on a $P(a) = (a-a)Q(a) = 0$. On a prouvé que a est une racine de P. □

PROPOSITION 5.3. *Soit P un polynôme non nul. Le nombre de racines de P est inférieur ou égal au degré de P. Autrement dit, on a l'inégalité $|\mathcal{Z}(P)| \leq \deg(P)$.*

DÉMONSTRATION. On procède par récurrence sur le degré de P.

Initialisation ($\deg(P) = 0$) : le polynôme P est constant et non nul ; donc $|\mathcal{Z}(P)| = 0 = \deg(P)$.

Hypothèse de récurrence : on suppose que pour tout polynôme Q de degré m, le nombre de racines de Q est inférieur ou égal à m.

Hérédité : Soit P un polynôme de degré $m+1$; montrons que le nombre de racines de P est inférieur ou égal à $m+1$. Sans nuire à la généralité, on peut supposer que P possède une racine $w \in \mathbf{C}$ — sinon, on a $|\mathcal{Z}(P)| = 0 \leq m+1$. Grâce à la proposition 5.2, on peut écrire $P = (X-w)\cdot Q$ avec $Q \in \mathbf{C}[X]$; par la proposition 3.9, on a $\deg(Q) = m$. L'hypothèse de récurrence assure alors que $|\mathcal{Z}(Q)| \leq m$. En outre, on a l'équivalence

$$P(z) = (z-w)Q(z) = 0 \Longleftrightarrow \big(z = w \text{ ou } Q(z) = 0\big)\ ,$$

qui entraîne $\mathcal{Z}(P) = \{w\} \cup \mathcal{Z}(Q)$. Par conséquent, on a $|\mathcal{Z}(P)| \leq 1 + |\mathcal{Z}(Q)| \leq m+1$. □

COROLLAIRE 5.4. *Soit $n \in \mathbf{N}$ et soit A, B des polynômes de degré inférieur ou égal à n. S'il existe $n+1$ nombres complexes $z_0, \ldots, z_n$ tels que $A(z_j) = B(z_j)$ pour tout j, alors $A = B$.*

DÉMONSTRATION. Le polynôme $A - B$ satisfait l'inégalité $\deg(A-B) \leq n$ et possède $n+1$ racines. Il est donc nul par la proposition 5.3. □

5.2. Polynômes irréductibles. Considérons un polynôme $P \in \mathbf{K}[X]$. Si a est un élément non nul de $\mathbf{K}$, on peut toujours écrire $P = A \cdot B$, avec $A = a\mathbf{1} \in \mathbf{K}[X]$ et $B = a^{-1}P \in \mathbf{K}[X]$.

DÉFINITION 5.5.
Soit $P \in \mathbf{K}[X]$ un polynôme non constant. S'il existe des polynômes non constants $A, B \in \mathbf{K}[X]$ tels que $P = A \cdot B$, on dit que P est réductible *dans $\mathbf{K}[X]$. Dans le cas contraire, on dit que P est* irréductible *dans $\mathbf{K}[X]$.*

REMARQUE 5.6. Soit P un polynôme non constant à coefficients dans $\mathbf{K}$. Les assertions suivantes sont équivalentes :

(1) P est irréductible dans $\mathbf{K}[X]$;

(2) pour tous $A, B \in \mathbf{K}[X]$, si $P = A \cdot B$, alors A est constant ou B est constant.

EXEMPLES. (1) Le polynôme $X^2 - 3X + 2$ est réductible dans $\mathbf{Q}[X]$; en effet, on voit par calcul que $X^2 - 3X + 2 = (X - 1) \cdot (X - 2)$;

(2) Si $P \in \mathbf{K}[X]$ est de degré 1, alors il est irréductible dans $\mathbf{K}[X]$. En effet, si on écrit $P = AB$ avec $A, B \in \mathbf{K}[X]$, on doit avoir $\deg(A) + \deg(B) = 1$; donc A est constant ou B est constant.

REMARQUE CULTURELLE 5.7. Les polynômes irréductibles dans $\mathbf{K}[X]$ jouent un rôle analogue à celui des nombres premiers dans $\mathbf{Z}$. Il est possible de démontrer le *théorème de factorisation* suivant :

Soit P un polynôme non constant à coefficients dans $\mathbf{K}$. Il existe $k \in \mathbf{N}^*$, $a \in \mathbf{K}^*$, $\mu_1, \ldots, \mu_k \in \mathbf{N}^*$, et des polynômes $P_1, \ldots, P_k$ unitaires, irréductibles dans $\mathbf{K}[X]$, distincts deux à deux et tels que

$$P = aP_1^{\mu_1} \cdots P_k^{\mu_k} = a \prod_{j=1}^{k} P_j^{\mu_j} \ .$$

De plus, cette décomposition est unique à permutation des facteurs près.

On démontrera ce résultat lorsque $\mathbf{K} = \mathbf{C}$ (voir la proposition 6.1 et le théorème 6.2). Le cas $\mathbf{K} = \mathbf{R}$ sera traité dans l'exercice 6.12 tandis que le cas $\mathbf{K} = \mathbf{Q}$ ne sera pas traité dans ce cours.

REMARQUE 5.8. Si un polynôme est réductible dans $\mathbf{R}[X]$, il est aussi réductible dans $\mathbf{C}[X]$; de même, si un polynôme est réductible dans $\mathbf{Q}[X]$, il est aussi réductible dans $\mathbf{R}[X]$ et $\mathbf{C}[X]$.

PROPOSITION 5.9.
Soit P un polynôme à coefficients dans $\mathbf{K}$.

(1) *Si $\deg(P) \geq 2$ et si P possède une racine dans $\mathbf{K}$, alors il est réductible dans $\mathbf{K}[X]$;*

(2) *Si $\deg(P) \in \{2, 3\}$ et si P est réductible dans $\mathbf{K}[X]$, alors il a une racine dans $\mathbf{K}$.*

EXERCICE 5.10. Démontrer cette proposition.

Remarquons les cas particuliers suivants :

(1) comme les racines du polynôme $X^2 + 1$ sont i et $-i$, ce polynôme est irréductible dans $\mathbf{Q}[X]$ et $\mathbf{R}[X]$, mais réductible dans $\mathbf{C}[X]$;

(2) comme les racines du polynôme $X^2 - 2$ sont $\sqrt{2}$ et $-\sqrt{2}$, ce polynôme est irréductible dans $\mathbf{Q}[X]$, mais réductible dans $\mathbf{R}[X]$ et $\mathbf{C}[X]$.

EXERCICE 5.11. Trouver un polynôme de degré 4 à coefficients réels, réductible dans $\mathbf{R}[X]$, mais qui ne possède aucune racine réelle.

6. Le théorème de d'Alembert-Gauss et ses conséquences

6.1. Polynômes irréductibles dans $\mathbf{C}[X]$. On admettra le résultat suivant, car sa preuve nécessite des connaissances d'analyse complexe.

THÉORÈME DE D'ALEMBERT-GAUSS. *Tout polynôme non constant possède une racine complexe.*

Ce théorème permet de caractériser les polynômes irréductibles dans $\mathbf{C}[X]$.

PROPOSITION 6.1. *Soit P un polynôme non constant. On a l'équivalence :*

$$P \text{ est irréductible dans } \mathbf{C}[X] \text{ si et seulement si } \deg(P) = 1.$$

DÉMONSTRATION. On a déjà vu que les polynômes de degré 1 sont irréductibles. Supposons maintenant P irréductible dans $\mathbf{C}[X]$. Par le théorème de d'Alembert-Gauss, P possède une racine z. On peut donc écrire $P = (X - z) \cdot Q$ avec $Q \in \mathbf{C}[X]$. Comme P est irréductible, Q doit être constant (et non nul, sans quoi P serait nul). Donc Q est de degré 0 et P est de degré $1 + 0 = 1$. □

Comme deuxième conséquence du théorème de d'Alembert-Gauss, établissons le théorème de factorisation dans $\mathbf{C}[X]$.

THÉORÈME 6.2.
Pour tout polynôme P à coefficients dans $\mathbf{C}$ et non constant, il existe $k \in \mathbf{N}^*$, $a \in \mathbf{C}^*$, des nombres complexes $z_1, \dots, z_k$ distincts et $\mu_1, \dots, \mu_k \in \mathbf{N}^*$ tels que

$$P = a(X - z_1)^{\mu_1} \cdots (X - z_k)^{\mu_k} = a \prod_{j=1}^{k} (X - z_j)^{\mu_j} \ .$$

De plus, cette décomposition est unique à permutation des facteurs près.

Remarquons que ce théorème, de même que le théorème de d'Alembert-Gauss, n'affirme **pas** que les racines de P sont faciles à calculer ! Si P est un polynôme de grand degré, donné sous la forme $P = \sum_{k=0}^{n} a_k X^k$, on peut être contraint d'approcher les racines de P par des techniques d'analyse numérique, faute de pouvoir les calculer exactement.

EXERCICE 6.3 (facile). Vérifier que le théorème 6.2 est bien équivalent au *théorème de factorisation* dans $\mathbf{C}[X]$ — au sens de la remarque 5.7.

Avant de démontrer le théorème 6.2, introduisons la notion de multiplicité.

DÉFINITION 6.4.
Soit P un polynôme et soit z une racine de P. La multiplicité *de la racine z (pour le polynôme P) est le nombre*

$$\mu_P(z) := \max \left\{ k \in \mathbf{N}^* : (X - z)^k \text{ divise } P \right\} .$$

Une racine est dite simple *si sa multiplicité est* 1, double *si sa multiplicité est* 2, *etc.*

EXERCICE 6.5 (facile). Vérifier que $\mu_P(z)$ est bien défini et compris entre 1 et $\deg(P)$.

EXEMPLE 6.6. Soit $P = X^3 - 3X + 2$. On a $P = (X - 1)^2(X + 2)$. Les racines de P sont -2, qui est une racine simple et 1, qui est une racine double.

EXERCICE 6.7. Soit $k \in \mathbf{N}^*$, $a \in \mathbf{C}^*$, $z_1, \dots, z_k$ des nombres complexes distincts, $\mu_1, \dots, \mu_k \in \mathbf{N}^*$ et $P = a(X - z_1)^{\mu_1} \cdots (X - z_k)^{\mu_k}$. Démontrer que pour tout $j \in \{1, \dots, k\}$, on a $\mu_P(z_j) = \mu_j$.

PREUVE DU THÉORÈME 6.2. Pour démontrer l'existence, on procède par récurrence sur le degré de P. Comme P n'est pas constant, ce degré est dans $\mathbf{N}^*$.

Initialisation : si $\deg(P) = 1$, on a $P = aX + b$, et donc $P = a(X - \frac{-b}{a})$, avec $a \in \mathbf{C}^*$ et $b \in \mathbf{C}$.

Hypothèse de récurrence : on suppose que pour tout polynôme Q de degré m (avec $m \in \mathbf{N}^*$), il existe $k \in \mathbf{N}^*$, $a \in \mathbf{C}^*$, des nombres complexes $z_1, \ldots, z_k$ distincts et $\mu_1, \ldots, \mu_k \in \mathbf{N}^*$ tels que

$$Q = a(X - z_1)^{\mu_1} \cdots (X - z_k)^{\mu_k} \ .$$

Hérédité : soit P un polynôme de degré $m+1$. Par le théorème de d'Alembert-Gauss, P possède une racine z. On peut alors écrire $P = (X - z) \cdot Q$ où Q est un polynôme de degré m. On applique l'hypothèse de récurrence à Q, ce qui nous donne $k \in \mathbf{N}^*$, $a \in \mathbf{C}^*$, des nombres complexes $z_1, \ldots, z_k$ distincts et $\mu_1, \ldots, \mu_k \in \mathbf{N}^*$ tels que

$$Q = a(X - z_1)^{\mu_1} \cdots (X - z_k)^{\mu_k} \ .$$

On distingue maintenant deux cas :

(1) si $z = z_i$ pour un certain $i \in \{1, \ldots, k\}$, on voit que

$$P = a \prod_{j=1}^{i-1} (X - z_j)^{\mu_j} \cdot (X - z_i)^{\mu_i + 1} \cdot \prod_{j=i+1}^{k} (X - z_j)^{\mu_j} \ ;$$

(2) si $z \notin \{z_1, \ldots, z_k\}$, on voit que $P = a(X - z) \cdot \prod_{j=1}^{k} (X - z_j)^{\mu_j}$.

Dans les deux cas, c'est une décomposition de la forme voulue ; ceci termine la récurrence.

Passons à la preuve de l'unicité à permutation des facteurs près. Si $P = a \prod_{j=1}^{k} (X - z_j)^{\mu_j}$, on constate facilement que a est le coefficient de plus haut degré de P et que $\{z_1, \ldots, z_k\}$ est l'ensemble des racines de P. Une autre décomposition sera donc nécessairement (à permutation des facteurs près) de la forme $P = a \prod_{j=1}^{k} (X - z_j)^{\nu_j}$. Enfin, on a $\mu_i = \mu_P(z_i) = \nu_i$ pour tout i d'après l'exercice 6.7. □

Comme application, on obtient un résultat plus précis que la proposition 5.3.

COROLLAIRE 6.8. *Soit P un polynôme non constant (à coefficients dans $\mathbf{C}$). L'égalité*

$$\sum_{z \in \mathcal{Z}(P)} \mu_P(z) = \deg(P)$$

est satisfaite (en particulier, le nombre de racines de P est inférieur ou égal au degré de P).

DÉMONSTRATION. C'est une conséquence directe du théorème 6.2 et de l'exercice 6.7. □

6.2. Polynômes irréductibles dans $\mathbf{R}[X]$. Dans $\mathbf{R}[X]$ on a déjà vu qu'il existe des polynômes irréductibles de degré 2, comme par exemple $X^2 + 1$. La situation n'est donc pas aussi simple que dans $\mathbf{C}[X]$. On peut néanmoins obtenir des résultats analogues à la proposition 6.1 et au théorème 6.2. Ces résultats sont laissés en exercice.

EXERCICE 6.9. Soit $P \in \mathbf{R}[X]$ et $z \in \mathbf{C}$. Démontrer que :

(1) z est racine de P si et seulement si $\bar{z}$ est racine de P ;

(2) dans ce cas les multiplicités de z et de $\bar{z}$ sont égales.

DÉFINITION 6.10. *Soit $P = aX^2 + bX + c$ un polynôme de degré 2 à coefficients dans $\mathbf{K}$. On appelle* discriminant *de P le nombre $\Delta = b^2 - 4ac$ (qui est dans $\mathbf{K}$).*

EXERCICE 6.11. Démontrer que les polynômes irréductibles dans $\mathbf{R}[X]$ sont exactement :
– les polynômes de degré 1 (à coefficients réels), et
– les polynômes de degré 2 (à coefficients réels) dont le discriminant est strictement négatif.

EXERCICE 6.12 (factorisation des polynômes à coefficients réels). Soit P un polynôme non constant à coefficients réels. Montrer qu'il existe $k \in \mathbf{N}^*$, $a \in \mathbf{R}^*$, $\mu_1, \ldots, \mu_k \in \mathbf{N}^*$, et des polynômes $P_1, \ldots, P_k$ unitaires, irréductibles dans $\mathbf{R}[X]$, distincts deux à deux et tels que

$$P = aP_1^{\mu_1} \cdots P_k^{\mu_k} = a \prod_{j=1}^{k} P_j^{\mu_j} \ .$$

De plus, démontrer que cette décomposition est unique à permutation des facteurs près.

Pour résoudre ce dernier exercice, on pourra utiliser le théorème 6.2.

7. Dérivation de polynômes

7.1. Définition et propriétés. La notion de polynôme dérivé est définie de manière algébrique. Celles et ceux qui sont intéressés à voir le lien avec la dérivation d'applications peuvent consulter la section 9.3.

DÉFINITION 7.1.
Soit $P = \sum_{k=0}^{m} a_k X^k$ est un polynôme. Le polynôme dérivé *de P est*

$$P' := \sum_{k=1}^{m} k a_k X^{k-1} = \sum_{n=0}^{m-1} (n+1) a_{n+1} X^n \ .$$

REMARQUE 7.2. Si P à coefficients dans $\mathbf{K}$, alors P' aussi. De plus, si P n'est pas constant, on a $\deg(P') = \deg(P) - 1$.

Notons les cas particuliers suivants : si $P = X^k$, avec $k \in \mathbf{N}^*$, alors $P' = kX^{k-1}$; si $Q = X^0 = \mathbf{1}$, alors $Q' = 0$.

PROPOSITION 7.3. *Soit P et Q deux polynômes. Les relations suivantes sont satisfaites :*

$$(P+Q)' = P' + Q' \quad , \quad (P \cdot Q)' = P' \cdot Q + P \cdot Q' \quad \text{et} \quad (Q \circ P)' = (Q' \circ P) \cdot P' \ .$$

EXERCICE 7.4. Démontrer cette proposition. (Cette preuve ne fait pas appel à la notion de dérivée d'une application.)

Soit P un polynôme. On peut définir une suite de polynômes récursivement par les formules $P^{(0)} = P$ et $P^{(n+1)} = (P^{(n)})'$. Le polynôme $P^{(n)}$ est appelé *n-ième polynôme dérivé* de P. Remarquons que si P est à coefficients dans $\mathbf{K}$, il en va de même pour tous les polynômes $P^{(n)}$.

EXERCICE 7.5. Soit $a \in \mathbf{C}$ et soit $P = (X-a)^n$, avec $n \in \mathbf{N}$.

(1) Vérifier que $P^{(k)} = n(n-1)\cdots(n-k+1)(X-a)^{n-k}$ si k est compris entre 1 et n ;

(2) En déduire que $P^{(n)}$ est le polynôme constant $n!$ et que $P^{(k)} = 0$ dès que $k > n$.

Rappelons que, pour tout couple (n, k) d'entiers naturels tel que $k \leq n$, la notation $\binom{n}{k}$ désigne le *coefficient binomial* de n et k, défini par $\binom{n}{k} = \frac{n!}{k!\cdot(n-k)!}$,

PROPOSITION 7.6. *Soit $P, Q \in \mathbf{K}[X]$. Pour tout entier naturel n, on a l'égalité*

$$(P \cdot Q)^{(n)} = \sum_{j=0}^{n} \binom{n}{j} P^{(j)} \cdot Q^{(n-j)} \ .$$

EXERCICE 7.7. Démontrer cette proposition. On rappelle que, pour tout couple (n, k) d'entiers naturels tel que $k \leq n$, l'égalité $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$ est satisfaite.

7.2. Formule de Taylor. Il s'agit du résultat suivant.

THÉORÈME 7.8.
Soit P un polynôme à coefficients dans $\mathbf{K}$ et soit $m = \deg(P)$. L'égalité suivante est satisfaite pour tout $a \in \mathbf{K}$:

$$P = \sum_{k=0}^{m} \frac{P^{(k)}(a)}{k!}(X-a)^k = P(a) + P'(a)\cdot(X-a) + \frac{P''(a)}{2}(X-a)^2 + \cdots + \frac{P^{(m)}(a)}{m!}(X-a)^m \ .$$

DÉMONSTRATION. On utilise la proposition 3.12 : il existe donc des coefficients $b_0, \ldots, b_m \in \mathbf{K}$ tels que $P = \sum_{j=0}^{m} b_j (X-a)^j$. Pour identifier b_k, on considère le k-ième polynôme dérivé de P. Par l'exercice 7.5, on a

$$P^{(k)} = \sum_{j=0}^{k-1} b_j \cdot 0 + b_k k! + \sum_{j=k+1}^{m} b_j \alpha_j (X-a)^{j-k}$$

où les coefficients α_j sont des entiers. En évaluant en a, on trouve $P^{(k)}(a) = b_k k!$, ce qui conclut la preuve. □

COROLLAIRE 7.9. *Soit k un entier naturel, a un élément de $\mathbf{K}$ et P un polynôme à coefficients dans $\mathbf{K}$. Les assertions suivantes sont équivalentes :*

(i) *P est divisible par $(X-a)^k$;*

(ii) *pour tout entier naturel j tel que $0 \leq j \leq k-1$, on a $P^{(j)}(a) = 0$.*

DÉMONSTRATION. Si k est nul, les deux assertions sont vraies ; supposons donc désormais que k est non nul.

Si la condition (ii) est réalisée, la formule de Taylor montre immédiatement que (i) l'est aussi.

Si la condition (ii) n'est pas réalisée, le polynôme $R := \sum_{j=0}^{k-1} \frac{P^{(j)}(a)}{j!}(X-a)^j$ est non nul par la proposition 3.12. Comme son degré est strictement inférieur à celui de $(X-a)^k$, il n'est pas divisible par $(X-a)^k$ — voir l'exercice 4.2. Par la formule de Taylor, P est somme de R et d'un multiple de $(X-a)^k$; donc P n'est pas divisible par $(X-a)^k$. □

Corollaire 7.10.
Soit P un polynôme non nul. Pour toute racine z de P, on a l'égalité

$$\mu_P(z) = \min\{j \in \mathbf{N} : P^{(j)}(a) \neq 0\} \ .$$

Exercice 7.11 (facile). Démontrer ce corollaire.

8. Détermination d'un polynôme par évaluations

8.1. Détermination d'un polynôme satisfaisant $n+1$ contraintes. La formule de Taylor montre qu'un polynôme de degré au plus n est entièrement déterminé par les valeurs $P(a)$, $P'(a)$,..., $P^{(n)}(a)$. Plus généralement, il est possible de déterminer un polynôme P de degré au plus n à partir de $n+1$ contraintes sur P et ses dérivées.

Théorème 8.1.
Soit $n \in \mathbf{N}$, soit $k \in \mathbf{N}^*$, soit $\mu_1, \ldots, \mu_k \in \mathbf{N}^*$ tels que $\mu_1 + \cdots + \mu_k = n+1$ et soit $z_1, \ldots, z_k$ des nombres complexes distincts. Alors, pour toute famille $(w_{j,\nu})_{1\leq j\leq k;\, 0\leq \nu\leq \mu_j - 1}$ de nombres complexes (notons qu'il y en a $n+1$), il existe un unique polynôme P tel que

$$\deg(P) \leq n \quad \text{et} \quad \forall j \in \{1, \ldots, k\},\ \forall \nu \in \{0, \ldots, \mu_j - 1\},\ P^{(\nu)}(z_j) = w_{j,\nu} \ .$$

Pour démontrer ce théorème, il serait plus commode d'utiliser des résultats d'algèbre linéaire qui sont au programme du S3. On peut cependant s'en tirer avec les résultats concernant les matrices vus au S1.

Corollaire 8.2. *Soit $z_1, \ldots, z_{n+1}$ des nombres complexes distincts. Alors, pour tous nombres complexes $w_1, \ldots, w_{n+1}$, il existe un unique polynôme P tel que*

$$\deg(P) \leq n \quad \text{et} \quad \forall j \in \{1, \ldots, n+1\},\ P(z_j) = w_j \ .$$

Exercice 8.3 (facile). Démontrer ce corollaire.

Preuve du théorème 8.1. *Première étape :* on démontre le théorème dans le cas où les $w_{j,\nu}$ sont tous nuls. Dans ce cas, il est clair que le polynôme nul satisfait aux conditions du théorème. Il reste à vérifier l'unicité, ce pour quoi on considère un polynôme P satisfaisant aux conditions du théorème. Par le corollaire 7.10, on a $\mu_P(z_j) \geq \mu_j$ pour tout j. Si P n'était pas constant, le corollaire 6.8 entraînerait $\deg(P) \geq \sum_{j=1}^k \mu_j = n+1$, ce qui est impossible[1]. Par conséquent, P est constant. Dès lors, il est nul puisqu'il possède une racine. Ceci achève la preuve de l'unicité.

Seconde étape : on démontre le théorème dans le cas général. Soit $P = \sum_{s=0}^n a_s X^s$ un polynôme de degré au plus n. Pout tout j et pour tout ν, on voit que

$$P^{(\nu)}(z_j) = \sum_{s=\nu}^n s(s-1)\cdots(s-\nu+1) a_s z_j^{s-\nu} = \sum_{s=\nu}^n s(s-1)\cdots(s-\nu+1) z_j^{s-\nu} \cdot a_s \ ,$$

[1]Ici, on peut s'affranchir de l'utilisation du théorème de d'Alembert-Gauss si on le souhaite en utilisant le théorème 9.4 plutôt que le corollaire 6.8.

en utilisant les résultats de l'exercice 7.5 (on convient que le produit $s(s-1)\cdots(s-\nu+1)$ vaut 1 lorsque $\nu = 0$). Ainsi, la condition $P^{(\nu)}(z_j) = w_{j,\nu}$ s'écrit sous la forme

$$\lambda_{j,\nu,0} \cdot a_0 + \lambda_{j,\nu,1} \cdot a_1 + \cdots + \lambda_{j,\nu,n} \cdot a_n = w_{j,\nu} \ ,$$

où $\lambda_{j,\nu,s} = s(s-1)\cdots(s-\nu+1)z_j^{s-\nu}$ si $s \geq \nu$ et $\lambda_{j,\nu,s} = 0$ sinon. Par conséquent, P satisfait aux conditions du théorème si et seulement si $A = {}^t(a_1, \ldots, a_n)$ est solution du système linéaire

$$\Lambda \cdot X = W \ ,$$

où

$$\Lambda = \begin{pmatrix} \lambda_{1,0,0} & \lambda_{1,0,1} & \cdots & \lambda_{1,0,n} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{1,\mu_1-1,0} & \lambda_{1,\mu_1-1,1} & \cdots & \lambda_{1,\mu_1-1,n} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{k,0,0} & \lambda_{k,0,1} & \cdots & \lambda_{k,0,n} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{k,\mu_k-1,0} & \lambda_{k,\mu_k-1,1} & \cdots & \lambda_{k,\mu_k-1,n} \end{pmatrix} \ , \quad X = \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ \vdots \\ \vdots \\ x_{n-1} \\ x_n \end{pmatrix} \quad \text{et} \quad W = \begin{pmatrix} w_{1,0} \\ \vdots \\ w_{1,\mu_1-1} \\ \vdots \\ w_{k,0} \\ \vdots \\ w_{k,\mu_k-1} \end{pmatrix} \ .$$

Notons que la matrice Λ est carrée, de taille $(n+1)\times(n+1)$, puisque $\sum_{j=1}^{k} \mu_j = n+1$. De plus, la première étape montre que l'unique solution du système $\Lambda \cdot X = {}^t(0, \ldots, 0)$ est le vecteur nul. Par conséquent, Λ est inversible et $P = \sum_{s=0}^{n} a_s X^s$ satisfait aux conditions du théorème si et seulement si ${}^t(a_1, \ldots, a_n) = \Lambda^{-1} \cdot W$. Ceci démontre à la fois l'existence et l'unicité de P. □

Exemple 8.4. Déterminons l'unique polynôme P de degré inférieur ou égal à 6 satisfaisant aux conditions $P(0) = 4$, $P'(0) = -7$, $P''(0) = 0$, $P'''(0) = -12$, $P(1) = -1$, $P'(1) = 8$ et $P(2) = 134$. On note $P = \sum_{j=0}^{6} a_j X^j$. En exprimant les conditions comme dans la preuve ci-dessus, on obtient le système linéaire

$$\begin{array}{rcrcrcrcrcrcrcr}
a_0 & & & & & & & & & & & & & = & 4 \\
 & & a_1 & & & & & & & & & & & = & -7 \\
 & & & & 2\cdot a_2 & & & & & & & & & = & 0 \\
 & & & & & & 6\cdot a_3 & & & & & & & = & -12 \\
a_0 & + & a_1 & + & a_2 & + & a_3 & + & a_4 & + & a_5 & + & a_6 & = & -1 \\
 & & a_1 & + & 2\cdot a_2 & + & 3\cdot a_3 & + & 4\cdot a_4 & + & 5\cdot a_5 & + & 6\cdot a_6 & = & 8 \\
a_0 & + & 2\cdot a_1 & + & 4\cdot a_2 & + & 8\cdot a_3 & + & 16\cdot a_4 & + & 32\cdot a_5 & + & 64\cdot a_6 & = & 134
\end{array}$$

En résolvant ce système (par exemple par la méthode du pivot de Gauss), on voit qu'il admet une unique solution, à savoir $a_0 = 4$, $a_1 = -7$, $a_2 = 0$, $a_3 = -2$, $a_4 = 0$, $a_5 = 3$ et $a_6 = 1$. Le polynôme P recherché est donc $X^6 + 3X^5 - 2X^3 - 7X + 4$.

8.2. Détermination du reste d'une division euclidienne. Voyons maintenant comment le théorème 8.1 permet de calculer le reste d'une division euclidienne sans avoir besoin de suivre l'algorithme décrit dans la preuve du théorème 4.3. Notons cependant que cette méthode ne permet pas de calculer le quotient.

Soit A un polynôme, B un polynôme non constant et R le reste de la division euclidienne de A par B. On suppose qu'on connaît toutes les racines de B et leurs multiplicités. On sait donc

écrire B sous la forme $B = b\prod_{j=1}^{k}(X - z_j)^{\mu_j}$ avec $b, z_1, \ldots, z_k \in \mathbf{C}$ et $b \neq 0$. Remarquons que $\mu_1 + \cdots + \mu_k = \deg(B)$.

Proposition 8.5.
Avec les notations qui précèdent, R est l'unique polynôme de degré strictement inférieur à $\deg(B)$ qui satisfait aux conditions $R^{(\nu)}(z_j) = A^{(\nu)}(z_j)$ pour tout $j \in \{1, \ldots, k\}$ et pour tout $\nu \in \{0, \ldots, \mu_j - 1\}$.

Remarque 8.6. Si B était constant (et non nul), alors R serait forcément nul.

Preuve de la proposition 8.5. Soit Q le quotient de la division euclidienne de A par B ; on a $A = QB + R$. Pour tout $j \in \{1, \ldots, k\}$ et pour tout $\nu \in \{0, \ldots, \mu_j - 1\}$, on a

$$A^{(\nu)}(z_j) = \sum_{\ell=0}^{\nu} \binom{\nu}{\ell} Q^{(\ell)}(z_j) \cdot B^{(\nu-\ell)}(z_j) + R^{(\nu)}(z_j)$$

par la proposition 7.6. De plus, le corollaire 7.9 implique que pour tout $\ell \in \{0, \ldots, \nu\}$ la dérivée $B^{(\nu-\ell)}$ s'annule en z_j, si bien que $R^{(\nu)}(z_j) = A^{(\nu)}(z_j)$. Donc R satisfait aux conditions de la proposition — son degré est par définition strictement inférieur à $\deg(B)$.
L'unicité, quant à elle, résulte du théorème 8.1 (poser $n = \deg(B) - 1$). □

Exemple 8.7. On veut calculer le reste R de la division euclidienne du polynôme

$$A = X^{14} - 4X^{13} + 5X^{12} - X^{11} - 4X^{10} + 4X^9 + 2X^8 - 4X^7 - X^6 + 8X^5 - 2X^4 - 2X^3 - 7X + 4$$

par le polynôme

$$B = X^7 - 4X^6 + 5X^5 - 2X^4 = X^4 \cdot (X - 1)^2 \cdot (X - 2)\ .$$

Par la proposition 8.5, R est l'unique polynôme de degré strictement inférieur à 7 satisfaisant aux conditions $R(0) = A(0)$, $R'(0) = A'(0)$, $R''(0) = A''(0)$, $R'''(0) = A'''(0)$, $R(1) = A(1)$, $R'(1) = A'(1)$ et $R(2) = A(2)$. Par calcul, on voit que

$$A' = 14X^{13} - 52X^{12} + 60X^{11} - 11X^{10} - 40X^9 + 36X^8 + 16X^7 - 28X^6 - 6X^5 + 40X^4 - 8X^3 - 6X^2 - 7$$

(on ne calcule pas A'' et A''' car il est facile de voir que $A''(0) = 0$ et $A'''(0) = -12$ à partir de l'expression de A'). Ainsi, R est l'unique polynôme de degré strictement inférieur à 7 satisfaisant aux conditions $R(0) = 4$, $R'(0) = -7$, $R''(0) = 0$, $R'''(0) = -12$, $R(1) = -1$, $R'(1) = 8$ et $R(2) = 134$. D'après l'exemple 8.4, ce polynôme est $X^6 + 3X^5 - 2X^3 - 7X + 4$.

En TD, cette méthode sera appliquée au calcul de puissances de matrices.

9. Annexes

9.1. Un cas particulier du théorème 8.1. Il s'agit du cas où les nombres complexes $z_0, \ldots z_n$ sont distincts. Dans ce cas, le système linéaire qui apparaît dans la preuve du théorème 8.1 est plus facile à expliciter. On verra de plus, bien que cela ne soit pas vraiment nécessaire, comment calculer la valeur exacte du déterminant de la matrice dans ce cas.

PROPOSITION 9.1 (corollaire 8.2). *Soit $z_0, \dots, z_n$ des nombres complexes distincts. Alors, pour tous nombres complexes $w_0, \dots, w_n$, il existe un unique polynôme P tel que*

$$\deg(P) \leq n \quad \text{et} \quad \forall j \in \{0, \dots, n\},\ P(z_j) = w_j \ .$$

PREUVE DE LA PROPOSITION 9.1. Commençons par démontrer l'existence. Soit P un polynôme de degré au plus n, qu'on écrit sous la forme $P = \sum_{j=0}^{n} a_j X^j$. On voit immédiatement que P satisfait les conditions $P(z_j) = w_j$ pour tout j si et seulement si ${}^t(a_0, a_1, \dots, a_n)$ est solution du système linéaire $ZX = W$, où

$$Z = \begin{pmatrix} 1 & z_0 & \cdots & z_0^n \\ 1 & z_1 & \cdots & z_1^n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & z_n & \cdots & z_n^n \end{pmatrix} \ , \quad X = \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_n \end{pmatrix} \quad \text{et} \quad W = \begin{pmatrix} w_0 \\ w_1 \\ \vdots \\ w_n \end{pmatrix} \ .$$

Il suffit donc de montrer que le système linéaire $ZX = W$ possède une unique solution. Or, c'est le cas puisque la matrice Z est inversible en vertu du lemme 9.2 ci-dessous. □

LEMME 9.2 (calcul des déterminants de Vandermonde). *Pour tout $n \in \mathbf{N}$, pour tous nombres complexes $z_0, z_1, \dots, z_n$ distincts, on a l'égalité*

$$\begin{vmatrix} 1 & z_0 & \cdots & z_0^n \\ 1 & z_1 & \cdots & z_1^n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & z_n & \cdots & z_n^n \end{vmatrix} = \prod_{0 \leq j < k \leq n} (z_k - z_j) \ . \tag{9.1}$$

En particulier, le déterminant est non nul.

REMARQUE 9.3. Si deux des nombres complexes $z_0, z_1, \dots, z_n$ sont égaux, l'égalité (9.1) est également vérifiée (les deux membres sont nuls).

PREUVE DU LEMME 9.2. On procède par récurrence sur n.

Initialisation ($n = 0$) : dans ce cas, les deux membres de l'équation (9.1) valent 1.

Initialisation ($n = 1$) : dans ce cas, les deux membres de l'équation (9.1) valent $z_1 - z_0$. (Cette seconde initilisation est surperflue, mais elle est plus parlante.)

Hypothèse de récurrence : on suppose que $n \geq 1$ et

$$\begin{vmatrix} 1 & z_0 & \cdots & z_0^{n-1} \\ 1 & z_1 & \cdots & z_1^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & z_{n-1} & \cdots & z_{n-1}^{n-1} \end{vmatrix} = \prod_{0 \leq j < k \leq n-1} (z_k - z_j) \ .$$

pour tous nombres complexes $z_0, \dots, z_{n-1}$ distincts.

Hérédité : Considérons $n+1$ nombres complexes $z_0, z_1, \ldots, z_n$ distincts et démontrons l'égalité (9.1). Considérons l'application $P : \mathbf{C} \to \mathbf{C}$ définie par la formule

$$P(z) = \begin{vmatrix} 1 & z_0 & \cdots & z_0^{n-1} & z_0^n \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & z_{n-1} & \cdots & z_{n-1}^{n-1} & z_{n-1}^n \\ 1 & z & \cdots & z^{n-1} & z^n \end{vmatrix}$$

En développant le déterminant selon la dernière ligne, on voit que P est un polynôme de degré au plus n. Il est même de degré exactement n, car son coefficient dominant est $\prod_{0\leq j<k\leq n-1}(z_k - z_j)$ d'après l'hypothèse de récurrence. De plus, $z_0, \ldots, z_{n-1}$ sont n racines (distinctes) de P, car un déterminant comportant deux lignes identiques est nul. Par le théorème 6.2, on a

$$P = \left(\prod_{0\leq j<k\leq n-1} (z_k - z_j) \right) \cdot (X - z_0) \cdots (X - z_{n-1}) \ .$$

Finalement, on trouve

$$\begin{aligned} \begin{vmatrix} 1 & z_0 & \cdots & z_0^n \\ 1 & z_1 & \cdots & z_1^n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & z_n & \cdots & z_n^n \end{vmatrix} &= P(z_n) = \left(\prod_{0\leq j<k\leq n-1} (z_k - z_j) \right) \cdot (z_n - z_0) \cdots (z_n - z_{n-1}) \\ &= \prod_{0\leq j<k\leq n} (z_k - z_j) \ . \end{aligned}$$

Ceci prouve l'égalité (9.1) et conclut la preuve. □

9.2. Annexe sur la mutiplicité des racines. Le but de cette section est de prouver une version faible du corollaire 6.8, à savoir le théorème 9.4 ci-dessous, sans utiliser le théorème de d'Alembert-Gauss.

THÉORÈME 9.4. *Soit P un polynôme non constant à coefficients dans $\mathbf{C}$. L'inégalité*

$$\sum_{z\in\mathcal{Z}(P)} \mu_P(z) \leq \deg(P)$$

est satisfaite (en particulier, le nombre de racines de P est inférieur ou égal au degré de P).

DÉMONSTRATION. On procède par récurrence forte sur le degré de P.

Initialisation ($\deg(P) = 1$) : On a $P = aX + b$ avec $b \in \mathbf{C}$ et $a \in \mathbf{C}^*$. L'unique racine de P est $-b/a$ et cette racine est simple. Donc, on a $\sum_{z\in\mathcal{Z}(P)} \mu_P(z) = \mu_P(-b/a) = 1 = \deg(P)$.

Hypothèse de récurrence : on fixe $m \in \mathbf{N}^*$; on suppose que pour tout polynôme $A \in \mathbf{C}[X]$ tel que $\deg(A) \leq m$, l'inégalité

$$\sum_{z\in\mathcal{Z}(A)} \mu_A(z) \leq \deg(A)$$

est satisfaite (et donc que le nombre de racines de A est inférieur ou égal à m).

Hérédité : Soit P un polynôme de degré $m+1$; montrons que l'inégalité

$$\sum_{z\in\mathcal{Z}(P)} \mu_P(z) \leq \deg(P)$$

est satisfaite. Si P n'a pas de racine[2], l'inégalité est trivalement satisfaite. Supposons maintenant que P possède une racine $w \in \mathbf{C}$, posons $\mu = \mu_P(w)$ et écrivons $P = (X-w)^\mu \cdot Q$ avec $Q \in \mathbf{C}[X]$. On voit que $\mathcal{Z}(P) = \{w\} \cup \mathcal{Z}(Q)$. Comme $(X-w)^{\mu+1}$ ne divise pas P, le polynôme $X-w$ ne divise pas Q. Par la proposition 5.2, w n'est pas racine de Q, de sorte que $\mathcal{Z}(P)$ est la réunion disjointe de $\{w\}$ et de $\mathcal{Z}(Q)$.

Assertion. Pour toute racine z de Q, on a $\mu_P(z) = \mu_Q(z)$.

Pour démontrer cette assertion, on utilise le corollaire 7.10 : on a donc $Q^{(j)}(z) = 0$ pour tout $j \in \{0, \ldots, \mu_Q(z)-1\}$ et $Q^{(j)}(z) \neq 0$ si $j = \mu_Q(z)$. Dès lors, l'égalité

$$P^{(k)} = \sum_{j=0}^{k} \binom{k}{j} \Big((X-w)^\mu\Big)^{(j)} \cdot Q^{(k-j)} \ ,$$

qui résulte de la proposition 7.6, implique que $P^{(k)}(z) = 0$ pour tout $k \in \{0, \ldots, \mu_Q(z)-1\}$, car toutes les dérivées de Q qui apparaissent dans la somme s'annulent en z. Elle implique également que $P^{(k)}(z) = (z-w)^\mu \cdot Q^{(k)}(z) \neq 0$ si $k = \mu_Q(z)$. Ainsi, en utilisant à nouveau le corollaire 7.10, on obtient l'égalité $\mu_P(z) = \mu_Q(z)$, ce qui prouve l'assertion.
Grâce à l'assertion, on obtient la formule

$$\sum_{z\in\mathcal{Z}(P)} \mu_P(z) = \mu_P(w) + \sum_{z\in\mathcal{Z}(Q)} \mu_P(z) = \mu + \sum_{z\in\mathcal{Z}(Q)} \mu_Q(z) \ .$$

On applique maintenant l'hypothèse de récurrence à Q (on a bien $\deg(Q) \leq m$), ce qui nous donne l'inégalité

$$\sum_{z\in\mathcal{Z}(P)} \mu_P(z) \leq \mu + \deg(Q) = \deg\big((X-w)^\mu \cdot Q\big) = \deg(P) \ .$$

Ceci termine la récurrence. □

9.3. Dérivation de fonctions complexes et de polynômes. Le but de cette annexe est de faire le lien entre les concepts de polynôme dérivé et d'application dérivée. Pour définir la notion de dérivabilité pour les fonctions complexes, on procède exactement comme en analyse réelle.

Définition 9.5. *Soit f une application de $\mathbf{C}$ dans $\mathbf{C}$ et soit $w \in \mathbf{C}$. On dit que f est* dérivable *en w si la limite*

$$f'(w) := \lim_{z\to w, z\neq w} \frac{f(z)-f(w)}{z-w}$$

existe dans $\mathbf{C}$. Dans ce cas, le nombre complexe $f'(w)$ est appelé dérivée *de f en w.*

[2]C'est impossible par le théorème de d'Alembert-Gauss, mais on n'a pas besoin d'utiliser ce fait ici

Autrement dit, f est dérivable en w s'il existe $\ell \in \mathbf{C}$ tel que, pour toute suite $(z_n)_n$ dans $\mathbf{C}\setminus\{w\}$ qui converge vers w, la suite de terme général $\frac{f(z_n)-f(w)}{z_n-w}$ converge vers ℓ (on a alors évidemment $f'(w)=\ell$).

DÉFINITION 9.6. *Une application f de $\mathbf{C}$ dans $\mathbf{C}$ est dite* dérivable *si elle est dérivable en tout point $w \in \mathbf{C}$. Dans ce cas, l'application $f' : \mathbf{C} \to \mathbf{C}; w \mapsto f'(w)$ est appelée* dérivée *de f.*

On consigne les résultats qui nous seront utiles dans la proposition suivante.

PROPOSITION 9.7. *Soit f et g deux applications de $\mathbf{C}$ dans $\mathbf{C}$.*

(1) *Si f et g sont dérivables, alors $f+g$, $f\cdot g$ et $g\circ f$ aussi. De plus, on a $(f+g)'=f'+g'$, $(f\cdot g)'=f'\cdot g+f\cdot g'$ et $(g\circ f)'=(g'\circ f)\cdot f'$.*
(2) *Si $f=X^k$, avec $k\in\mathbf{N}^*$, alors f est dérivable et $f'=kX^{k-1}$; si $g=X^0=\mathbf{1}$, alors g est dérivable et $g'=0$.*

EXERCICE 9.8. Démontrer cette proposition. Il s'agit en fait de vérifier qu'on peut recopier les preuves vues au cours d'analyse pour les applications de $\mathbf{R}$ dans $\mathbf{R}$.

COROLLAIRE 9.9. *Si $P=\sum_{k=0}^m a_kX^k$ est un polynôme (de degré m) à coefficients dans $\mathbf{K}$, alors P est dérivable et sa dérivée est donnée par la formule*

$$P'=\sum_{k=1}^{m} ka_kX^{k-1}=\sum_{n=0}^{m-1}(n+1)a_{n+1}X^n\ .$$

Autrement dit, la dérivée de P (au sens de la définition 9.6) et le polynôme dérivé de P (au sens de la définition 7.1) coïncident.

DÉMONSTRATION. C'est une conséquence immédiate de la proposition 9.7. □

La proposition 7.3 est une autre conséquence facile de la proposition 9.7 et du corollaire 9.9. Notre nouvelle approche permet donc de se passer de la preuve de la proposition 7.3 demandée dans l'exercice 7.4.