POUR BIEN DÉMARRER L'ANNÉE

Ce chapitre a un statut un peu particulier par rapport à tous ceux qui vont suivre : nous allons y étudier les bases de la logique mathématique et y définir quelques notions élémentaires que nous utiliserons toute l'année. Ne paniquez pas si vous n'aimez pas ce chapitre, les chapitres suivants ressembleront davantage aux chapitres que l'on vous a enseignés au lycée.

1 UN PEU DE LOGIQUE

Convenons d'appeler *proposition* toute phrase p au sujet de laquelle on peut poser la question : p est-elle vraie ? La plupart des phrases grammaticalement correctes sont des propositions, mais par exemple, « Dis-le-moi ! », « Bonjour » ou « Comment vas-tu ? » n'en sont pas ; la question « Est-il vrai que bonjour ? » n'a aucun sens.

La *valeur de vérité* d'une proposition est soit le vrai (V), soit le faux (F). Deux propositions qui ont la même valeur de vérité sont dites *équivalentes* ; cela veut dire qu'elles sont soit toutes les deux vraies, soit toutes les deux fausses. Cette notion est très importante : quand vous devez démontrer une proposition p, vous n'êtes pas obligé de démontrer p elle-même ; il suffit que vous démontriez n'importe quelle proposition q équivalente à p.

Exemple « Socrate n'est pas immortel » et « Socrate est mortel » sont deux propositions équivalentes ; démontrer l'une revient donc à démontrer l'autre.

1.1 CONNECTEURS LOGIQUES

On appelle *connecteur logique* tout moyen de construire une proposition unique à partir d'une ou plusieurs propositions. Par exemple, « et », « ou », « si, alors » et « parce que » sont des connecteurs ; à partir des propositions « J'ai faim » et « J'ai soif », on peut construire une nouvelle proposition « J'ai faim et (j'ai) soif ».

Un connecteur logique est dit *vérifonctionnel* si la valeur de vérité d'une proposition construite à l'aide de ce connecteur dépend seulement de la valeur de vérité des propositions utilisées dans la construction. Ainsi la proposition « p et q » est vraie si et seulement si les deux propositions p et q sont vraies. Peu importe le contenu exact de p et q : seule leur vérité compte.

En mathématiques, tous les connecteurs logiques sont vérifonctionnels. L'intérêt des connecteurs vérifonctionnels réside dans la facilité avec laquelle on peut les définir. Par exemple, pour définir le connecteur « et », il suffit de décrire, en fonction de la valeur de vérité de p et q, la valeur de vérité de la proposition « p et q » : par définition, « p et q » est vraie si p et q le sont, et fausse dans tous les autres cas. Par souci de clarté, on présente généralement cette définition sous forme d'un tableau appelé une *table de vérité* :

p	q	p et q
V	V	V
V	F	F
F	V	F
F	F	F

Pour votre propre culture, vous remarquerez que certains connecteurs logiques ne sont pas vérifonctionnels. C'est le cas du connecteur « parce que ». Imaginons en effet un contexte dans lequel il est vrai que « Ses lunettes sont cassées parce qu'il les a faites tomber ». Alors les deux propositions « Ses lunettes sont cassées » et « Il les a faites tomber » sont vraies. Remplaçons à présent « Il les a faites tomber » par « La glace est un solide », elle aussi vraie. Si le connecteur « parce que » était vérifonctionnel, notre nouvelle proposition « Ses lunettes sont cassées parce que la glace est un solide » devrait encore être vraie, ce qui n'est pas le cas. Cette absurdité prouve que « parce que » n'est pas vérifonctionnel.

1.1.1 NÉGATION non

La proposition « non p » est vraie si p est fausse, fausse si p est vraie.

p	non p
V	F
F	V

LOI DE LA DOUBLE NÉGATION : p et « non (non p) » sont deux propositions équivalentes. On s'en rend compte en observant la table suivante :

p	non p	non (non p)
V	F	V
F	V	F

Colonnes identiques

1.1.2 Conjonction et, disjonction ou

La proposition « p et q » est vraie si p et q sont vraies, fausse dans tous les autres cas. Quant à la proposition « p ou q », elle est vraie si p est vraie ou si q est vraie (éventuellement les deux), fausse dans le seul cas où p et q sont fausses toutes les deux.

p	q	p et q	p ou q
V	V	V	V
V	F	F	V
F	V	F	V
F	F	F	F

✖✖✖ Attention ! Dans le langage usuel, il arrive que le « ou » oppose les termes qu'il relie : dans l'expression « fromage ou dessert », le « ou » est *exclusif* car il exclut la possibilité qu'on choisisse les deux (fromage et dessert).
Au contraire, en mathématiques, « ou » est *inclusif* : « p ou q » est vraie même quand p et q sont vraies.

Lois de De Morgan :

- « non (p et q) » et « (non p) ou (non q) » sont deux propositions équivalentes.
- « non (p ou q) » et « (non p) et (non q) » sont deux propositions équivalentes.

p	q	non p	non q	p et q	non (p et q)	(non p) ou (non q)	p ou q	non(p ou q)	(non p) et (non q)
V	V	F	F	V	F	F	V	F	F
V	F	F	V	F	V	V	V	F	F
F	V	V	F	F	V	V	V	F	F
F	F	V	V	F	V	V	F	V	V

Colonnes identiques. Colonnes identiques

Exemple Ces deux phrases sont équivalentes : { « Je n'aime ni le chocolat ni la vanille » — « (non p) et (non q) »
« Il est faux que j'aime le chocolat ou la vanille » — « non (p ou q) »

1.1.3 Implication $\Longrightarrow$

La proposition « $p \Longrightarrow q$ » se lit « p implique q » ou « si p, alors q ». Elle est vraie si p est fausse ou si q est vraie, fausse uniquement lorsque p est vraie et q fausse. Elle répond à la question : si on suppose que p est vraie, q l'est-elle aussi ? La proposition p est appelée l'*antécédent* de l'implication « $p \Longrightarrow q$ », et q est appelée son *conséquent*.

p	q	$p \Longrightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

✎✎✎ **En pratique** Pour montrer la vérité d'une implication « $p \Longrightarrow q$ », il convient d'abord de supposer que p est vraie (ce n'est là qu'une hypothèse) ; puis de montrer d'une façon ou d'une autre que, sous cette hypothèse, q est vraie. Même si vous ne savez pas démontrer jusqu'au bout que l'implication « $p \Longrightarrow q$ » est vraie, vous devez sur votre copie, de vous-même, commencer bêtement par : « Supposons p vraie ».

✖✖✖ Attention !

- Une implication « $p \Longrightarrow q$ » peut être vraie alors que p et q n'ont rien de commun. Il suffit que leurs valeurs de vérité respectent la table de vérité de l'implication. Ainsi la phrase « Si $0 = 0$, alors les oiseaux ont des plumes » est vraie.
- Par définition, « $p \Longrightarrow q$ » est toujours vraie quand p est fausse. Ainsi la phrase étrange « Si $0 \neq 0$, alors $0 = 0$ » est vraie. Après un tel exemple, la définition du connecteur $\Longrightarrow$ peut sembler suspecte ; pourquoi donc avoir choisi cette table de vérité ? Nous le justifierons un peu plus loin.
- Affirmer que « $p \Longrightarrow q$ » est vraie n'implique ni que p est vraie, ni que q est vraie. Ainsi, il est vrai que « Si Pinocchio est Président de la République, alors il est le chef des armées » ; pourtant il est faux que Pinocchio est Président de la République, et il est également faux qu'il est chef des armées.

Négation d'une implication : « non ($p \Longrightarrow q$) » et « p et (non q) » sont deux propositions équivalentes.

p	q	non q	$p \Longrightarrow q$	non ($p \Longrightarrow q$)	p et (non q)
V	V	F	V	F	F
V	F	V	F	V	V
F	V	F	V	F	F
F	F	V	V	F	F

Colonnes identiques

✎✎✎ **En pratique** Conformément à ce qui précède, pour montrer qu'une implication « $p \Longrightarrow q$ » est fausse, on peut montrer que « p et (non q) » est vraie, i.e. que p est vraie mais que q est fausse.

Exemple Est-il vrai que, si on a 18 ans (p), alors on a le droit de vote (q) ? La réponse est... non. Car je peux très bien avoir 18 ans — p est vraie — et un casier judiciaire tel que le droit de vote m'a été supprimé — q est fausse.

Contraposition :
« $p \Longrightarrow q$ » et « (non q) $\Longrightarrow$ (non p) » sont deux propositions équivalentes. La proposition « (non q) $\Longrightarrow$ (non p) » est appelée la *contraposée* de l'implication « $p \Longrightarrow q$ ».

p	q	non q	non p	$p \Longrightarrow q$	(non q) $\Longrightarrow$ (non p)
V	V	F	F	V	V
V	F	V	F	F	F
F	V	F	V	V	V
F	F	V	V	V	V

Colonnes identiques

Exemple Ces deux phrases sont équivalentes : « S'il pleut, alors il y a des nuages » — « $p \Longrightarrow q$ » ; « S'il n'y a pas de nuages, alors il ne pleut pas » — « (non q) $\Longrightarrow$ (non p) »

1.1.4 Equivalence $\Longleftrightarrow$

La proposition « $p \Longleftrightarrow q$ » se lit « p si et seulement si q » ou « p et q sont équivalentes ». Elle est vraie si p et q ont la même valeur de vérité, fausse sinon.

p	q	$p \Longleftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

Equivalence et double implication :
« $p \Longleftrightarrow q$ » et « ($p \Longrightarrow q$) et ($q \Longrightarrow p$) » sont deux propositions équivalentes. La proposition « $q \Longrightarrow p$ » est appelée la *réciproque* de l'implication « $p \Longrightarrow q$ ».

p	q	$p \Longrightarrow q$	$q \Longrightarrow p$	$p \Longleftrightarrow q$	($p \Longrightarrow q$) et ($q \Longrightarrow p$)
V	V	V	V	V	V
V	F	F	V	F	F
F	V	V	F	F	F
F	F	V	V	V	V

Colonnes identiques

✎ ✎ ✎ **En pratique** Pour montrer qu'une équivalence « $p \Longleftrightarrow q$ » est vraie, on peut choisir l'une des trois méthodes suivantes :

1) aller de p jusqu'à q au moyen d'un raisonnement dont chaque étape est une équivalence :

$$p \Longleftrightarrow p_1 \Longleftrightarrow p_2 \Longleftrightarrow \dots \Longleftrightarrow p_n \Longleftrightarrow q \quad ;$$

2) montrer l'implication « $p \Longrightarrow q$ », puis sa réciproque « $q \Longrightarrow p$ » ;
3) montrer l'implication « $p \Longrightarrow q$ », puis la contraposée de sa réciproque « (non p) $\Longrightarrow$ (non q) ».

Revenons un instant sur le connecteur $\Longrightarrow$. Nous sommes restés sur un point d'interrogation tout à l'heure : pourquoi avoir décidé que « $p \Longrightarrow q$ » est vraie quand p est fausse ? Cela a pour conséquence étrange que la proposition « Si $0 \neq 0$, alors $0 = 0$ » est vraie.

En réalité avions-nous le choix ? Ce qui est sûr, c'est qu'il n'est pas question de toucher aux deux premières lignes de la table de vérité de l'implication. Seules les deux dernières lignes nous gênent, lorsque p est fausse. Et si on les changeait ? Le problème, c'est qu'en changeant les deux dernières lignes de la table de vérité de l'implication, on retombe sur des connecteurs déjà connus comme l'illustre la table ci-contre :

p	q	$p \Longrightarrow q$	q	$p \Longleftrightarrow q$	p et q
V	V	V	V	V	V
V	F	F	F	F	F
F	V	V	V	F	F
F	F	V	F	V	F

1.2 Quantificateurs universel $\forall$ et existentiel $\exists$

1.2.1 Définition

On appelle *prédicat* toute propriété portant sur un ou plusieurs objets donnés en arguments. Par exemple, « être un oreiller » est un prédicat ; si nous le notons $\mathcal{O}$, la notation $\mathcal{O}(x)$ signifiera « x est un oreiller ». De même, « être plus âgé que » est un prédicat, portant lui sur deux objets ; si nous le notons $\mathcal{A}$, la notation $\mathcal{A}(x, y)$ pourra signifier « x est plus âgé que y ». En mathématiques, nous connaissons quelques prédicats incontournables : $=$, $\leqslant$, $<$ ... sauf qu'au lieu de noter $\leqslant (x, y)$, on préfère employer la notation $x \leqslant y$.

Il existe deux quantificateurs en mathématiques : le *quantificateur universel* $\forall$ et le *quantificateur existentiel* $\exists$. Si E est un ensemble et si $\mathcal{P}$ est un prédicat à un objet :

- la proposition « Tous les éléments de E vérifient la propriété $\mathcal{P}$ » s'écrit : $\forall x \in E, \quad \mathcal{P}(x)$
  et se lit : « Pour tout x élément de E/quel que soit x élément de E, x vérifie $\mathcal{P}$ » ;
- la proposition « L'un (au moins) des éléments de E vérifie la propriété $\mathcal{P}$ » s'écrit : $\exists\, x \in E/ \quad \mathcal{P}(x)$
  et se lit : « Il existe un élément x de E tel que x vérifie $\mathcal{P}$ ».

✎✎✎ **En pratique** La remarque qui suit est TRÈS IMPORTANTE : je me ferai un plaisir de couper la tête à tous ceux qui n'apprendront pas vite à la respecter. Vous la retrouverez avec davantage de détails dans le « Petit manuel de bonne rédaction ».

- Supposons qu'on veuille démontrer un théorème à base de $\forall$ de la forme : $\forall x \in E, \quad \mathcal{P}(x)$. La plupart des théorèmes mathématiques peuvent se mettre sous cette forme.
  Vous avez le droit de ne pas savoir démontrer jusqu'au bout un tel théorème, mais vous n'avez pas le droit de ne pas savoir comment commencer votre démonstration. Sans réfléchir, vous la commencerez par : « Soit $x \in E$ ». Un élément x étant ainsi fixé, vous tenterez de montrer que ce x a la propriété $\mathcal{P}$. Si vous y parvenez, c'est terminé.
- Supposons qu'on veuille démontrer un théorème à base de $\exists$ de la forme : $\exists\, x \in E/ \quad \mathcal{P}(x)$.
  Montrer l'existence d'un objet mathématique — ici, l'existence d'un élément x de E qui vérifie la propriété $\mathcal{P}$ — revient à exhiber un tel objet. L'exemple suivant illustre la marche à suivre dans un tel contexte.

Exemple $\forall x, y \in \mathbf{R}, \quad \exists\, z \in \mathbf{R}/ \quad z > x + y$.

En effet Prouvons cette proposition. La formulation « $\forall x, y \in \mathbf{R}$ » est un raccourci d'écriture pour dire « $\forall x \in \mathbf{R}, \quad \forall y \in \mathbf{R}$ ».

Début de la démonstration : Soient $x, y \in \mathbf{R}$. Un x et un y étant fixés, nous devons montrer l'existence d'un réel z tel que $z > x + y$. Or démontrer l'existence d'un objet revient à donner un exemple de tel objet. Ici nous avons le choix : n'importe quel réel strictement supérieur à $x + y$ convient. Par exemple, posons $z = x + y + 1$. Alors $z = x + y + 1 > x + y$ et c'est terminé.

✖✖✖ **Attention** ! La lettre x de « $\forall x, \quad \mathcal{P}(x)$ » ou « $\forall y, \quad \mathcal{P}(x)$ » peut être remplacée par n'importe quel symbole n'apparaissant pas dans $\mathcal{P}$; tout symbole figurant dans $\mathcal{P}$ est exclu.
Pour comprendre cela, fixons un entier naturel n (quelconque) et intéressons-nous au prédicat « être inférieur ou égal à n ». Imaginons qu'on veuille répondre à la question : tous les entiers naturels sont-ils inférieurs ou égaux à n ? Bien sûr la réponse est non, car par exemple $n + 1$ n'est pas inférieur ou égal à n. En tout cas, la proposition à démontrer s'écrit : $\forall k \in \mathbf{N}, \quad k \leqslant n$. La lettre k pourrait ici être remplacée par les lettres x, p ... mais pas par la lettre n. En effet, la proposition obtenue serait alors : $\forall n \in \mathbf{N}, \quad n \leqslant n$, qui est vraie, tous les entiers naturels étant inférieurs ou égaux à eux-mêmes.

1.2.2 NÉGATION

NÉGATION DU QUANTIFICATEUR UNIVERSEL : Les propositions « non $\big(\forall x \in E, \quad \mathcal{P}(x)\big)$ » et « $\exists\, x \in E/ \quad$ non $\mathcal{P}(x)$ » sont équivalentes.

Exemple Ces deux phrases sont équivalentes :

« Il est faux que tout homme a les yeux bleus » — « non $\big(\forall x \in E, \quad \mathcal{P}(x)\big)$ »
« Certains hommes n'ont pas les yeux bleus »/« Il existe au moins un homme qui n'a pas les yeux bleus » — « $\exists\, x \in E/ \quad$ non $\mathcal{P}(x)$ »

NÉGATION DU QUANTIFICATEUR EXISTENTIEL : Les propositions « non $\big(\exists\, x \in E/ \quad \mathcal{P}(x)\big)$ » et « $\forall x \in E, \quad$ non $\mathcal{P}(x)$ » sont équivalentes.

Exemple Ces deux phrases sont équivalentes :

« Aucun homme n'a de cornes »/« Il est faux qu'il existe un homme à cornes » — « non $\big(\exists\, x \in E/ \quad \mathcal{P}(x)\big)$ »
« Tout homme est sans cornes » — « $\forall x \in E, \quad$ non $\mathcal{P}(x)$ »

✎✎✎ **En pratique** Pour nier une phrase contenant un ou plusieurs quantificateurs, on réécrit cette phrase : 1) en remplaçant tous les « $\forall$ » par des « $\exists$ » et tous les « $\exists$ » par des « $\forall$ », et 2) en niant le prédicat final.

Exemple La négation de la proposition :

$$\begin{array}{lccc} & \forall \varepsilon > 0, & \exists\, \alpha > 0/ & \forall x \in \mathbf{R}, \quad \left[|x| < \alpha \implies \left| \dfrac{\sqrt{x}}{x^2+1} \right| < \varepsilon \right] \\ & \updownarrow & \updownarrow & \updownarrow \text{ Négation} \\ \text{est :} & \exists\, \varepsilon > 0/ & \forall \alpha > 0, & \exists\, x \in \mathbf{R}/ \quad \left[|x| < \alpha \quad \text{et} \quad \left| \dfrac{\sqrt{x}}{x^2+1} \right| \geqslant \varepsilon \right]. \end{array}$$

1.2.3 Permutation des quantificateurs

On peut toujours permuter les quantificateurs universels $\forall$ entre eux, et les quantificateurs existentiels $\exists$ entre eux.

Exemple

- Les propositions « $\forall x \in \mathbb{R}_+, \quad \forall y \in \mathbb{R}_-, \quad x \geqslant y$ » et « $\forall y \in \mathbb{R}_-, \quad \forall x \in \mathbb{R}_+, \quad x \geqslant y$ » sont équivalentes.
- Les propositions « $\exists\, x \in \mathbb{R}_+, \quad \exists\, y \in \mathbb{R}_-, \quad x \geqslant y$ » et « $\exists\, y \in \mathbb{R}_-, \quad \exists\, x \in \mathbb{R}_+, \quad x \geqslant y$ » sont équivalentes.

✖✖✖ **Attention** ! La permutation d'un $\forall$ et d'un $\exists$ n'est pas aussi facile. Voyons cela sur deux exemples.

- « Dans toute cerise il y a un noyau ». Formellement, cette proposition s'écrit :

  $$\forall c \text{ cerise}, \quad \exists\, n \text{ noyau}/ \quad n \text{ est dans } c.$$

  Qu'arrive-t-il si nous permutons $\forall$ et $\exists$? Essayons : « $\exists\, n$ noyau/ $\forall c$ cerise, n est dans c ». En bon français, cela donne : « Il existe un noyau qui se trouve dans toutes les cerises ». Tiens donc : alors que nous étions convaincus de la vérité de la proposition initiale, cette nouvelle proposition nous paraît clairement fausse.
  Conclusion : quand une proposition de la forme « $\forall\exists$ » est vraie, la proposition « $\exists\forall$ » correspondante peut être fausse. L'opération de permutation qui fait passer d'une configuration « $\forall\exists$ » à une configuration « $\exists\forall$ » est interdite.

- « Il existe une femme qui est la mère de tous les être humains » (faisons comme si Eve existait). Formellement, cette proposition s'écrit :

  $$\exists\, f \text{ femme}/ \quad \forall h \text{ être humain}, \quad f \text{ est la mère de } h.$$

  A présent permutons $\forall$ et $\exists$: « $\forall h$ être humain, $\exists\, f$ femme/ f est la mère de h ». En bon français, cela donne : « Tout homme a une mère », proposition évidemment vraie. La permutation a ici fonctionné convenablement, mais la proposition obtenue après permutation est beaucoup moins forte, beaucoup moins contraignante que celle dont nous sommes partis : la première était vraie à condition qu'Eve ait existé ; la seconde au contraire est d'une banalité incroyable.
  Conclusion : quand une proposition de la forme « $\exists\forall$ » est vraie, la proposition « $\forall\exists$ » est elle aussi vraie. Ce genre de permutation est donc autorisé.

1.2.4 Le pseudo-quantificateur $\exists\,!$

Parfois on ne veut pas seulement affirmer qu'un objet existe avec certaines propriétés, mais affirmer en outre qu'il est le seul à posséder ces propriétés. La proposition « Il existe (un et) un seul élément de E qui possède la propriété $\mathcal{P}$ » s'écrit en mathématiques : $\exists\,!\, x \in E/ \quad \mathcal{P}(x)$ et se lit : « Il existe un unique x élément de E tel que x vérifie $\mathcal{P}$ ».

✎✎✎ **En pratique** Pour démontrer la proposition « $\exists\,!\, x \in E/ \quad \mathcal{P}(x)$ », on a deux choses à démontrer : l'existence d'un tel x et son unicité.

- Pour l'existence, on fait comme si on travaillait avec la proposition « $\exists\, x \in E/ \quad \mathcal{P}(x)$ ».
- Pour l'unicité, on suppose généralement que deux éléments x et x' de E ont la propriété $\mathcal{P}$ et on montre alors que $x = x'$. Cela montre qu'il ne peut y avoir deux objets distincts possédant la propriété $\mathcal{P}$, autrement dit qu'il n'y en a qu'un seul.

Exemple $\exists\,!\, x \in \mathbb{R}_+/ \quad x^2 = 1$.

En effet

- **Existence** : Posons $x = 1$. Alors $x \in \mathbb{R}_+$ et $x^2 = 1$ comme voulu.
- **Unicité** : Soient $x, x' \in \mathbb{R}_+$. On suppose que $x^2 = x'^2 = 1$. Montrons que $x = x'$. Or puisque $x^2 = x'^2$, on a $x = x'$ ou $x = -x'$.
  Peut-on avoir $x = -x'$? Si c'est le cas, alors comme x et x' sont positifs, $x = x' = 0$. Cela contredit le fait que $x^2 = x'^2 = 1$. On ne peut donc pas avoir $x = -x'$. Par conséquent $x = x'$ comme voulu.

1.3 Le raisonnement par récurrence

Soient $\mathcal{P}_0, \mathcal{P}_1, \mathcal{P}_2, \ldots$ une suite infinie de propositions. Supposons qu'on veuille démontrer la proposition : $\forall n \in \mathbb{N}, \quad \mathcal{P}_n$.
Le *raisonnement par récurrence* est LA technique générale de démonstration adaptée à ce problème.

Principe de la récurrence : Si $\overbrace{\mathcal{P}_0 \text{ est vraie}}^{\text{Initialisation}}$, et si, $\overbrace{\text{pour tout } n \in \mathbb{N}, \text{ la vérité de } \mathcal{P}_n \text{ implique la vérité de } \mathcal{P}_{n+1}}^{\text{Hérédité}}$, alors la proposition : $\forall n \in \mathbb{N}, \quad \mathcal{P}_n$ est vraie.

Plus généralement, n_0 étant un entier naturel fixé, si $\mathcal{P}_{n_0}$ est vraie, et si, pour tout $n \in \mathbb{N}$, $n \geqslant n_0$, la vérité de $\mathcal{P}_n$ implique la vérité de $\mathcal{P}_{n+1}$, alors la proposition : $\forall n \in \mathbb{N}, \ n \geqslant n_0, \quad \mathcal{P}_n$ est vraie.

Exemple Soit $(u_n)_{n\in\mathbb{N}}$ une suite géométrique de raison q, où $q \in \mathbb{C}$. Montrons que pour tout $n \in \mathbb{N}$: $u_n = q^n u_0$.

En effet

- **Initialisation :** On a $q^0 = 1$ par convention, donc $u_0 = q^0 u_0$.
- **Hérédité :** Soit $n \in \mathbb{N}$. On suppose que $u_n = q^n u_0$. Il s'agit de montrer que $u_{n+1} = q^{n+1} u_0$.

  Facile : $u_{n+1} = q u_n = q \times q^n u_0 = q^{n+1} u_0$ comme voulu. Fin de la récurrence.

Exemple Par définition, un entier $n \in \mathbb{Z}$ est pair s'il existe $k \in \mathbb{Z}$ tel que $n = 2k$, et impair s'il existe $k \in \mathbb{Z}$ tel que $n = 2k+1$. Nous allons démontrer que tout entier est pair ou impair.

En effet

- **Initialisation :** L'entier 0 est pair car il s'écrit $0 = 2 \times 0$.

  Hérédité : Soit $n \in \mathbb{N}$. On suppose n pair ou impair. Il s'agit de montrer que $(n+1)$ est lui aussi pair ou impair. Deux cas se présentent :

  1) si n est pair, de la forme $n = 2k$ où $k \in \mathbb{Z}$, alors $n+1 = 2k+1$ donc $(n+1)$ est impair ;
  2) si n est impair, de la forme $n = 2k+1$ où $k \in \mathbb{Z}$, alors $n+1 = (2k+1)+1 = 2(k+1)$ avec $k+1 \in \mathbb{Z}$ et donc $(n+1)$ est pair.

  Au final $(n+1)$ est pair ou impair comme voulu. Fin de la récurrence.

- Nous venons donc de montrer que tout entier naturel est pair ou impair. Qu'en est-il des entiers négatifs ? Soit n un tel entier. Alors $-n$ est un entier naturel, donc $-n$ est pair ou impair :

  1) si $-n$ est pair, on peut l'écrire $-n = 2k$ où $k \in \mathbb{Z}$, donc $n = 2(-k)$ est pair avec $-k \in \mathbb{Z}$;
  2) si $-n$ est impair, on peut l'écrire $-n = 2k+1$ où $k \in \mathbb{Z}$, donc $n = -2k-1 = 2(-k-1)+1$ est impair avec $(-k-1) \in \mathbb{Z}$.

  Dans les deux cas n est pair ou impair. C'est terminé.

✎✎✎ **En pratique** Pour rédiger vos récurrences, je vous recommande d'adopter la rédaction des deux exemples précédents.
1) D'abord on initialise ; c'est généralement facile, mais il faut quand même le faire.
2) Ensuite on se donne <u>un</u> entier naturel n quelconque — « Soit $n \in \mathbb{N}$ » — et on suppose que la propriété à démontrer est vraie au rang n. Il reste à démontrer, sous cette hypothèse, la proposition au rang $(n+1)$. Et c'est tout.

✖✖✖ <u>Attention</u> ! Dans la partie hérédité d'une récurrence, ne commencez jamais par : « On suppose que pour tout entier n, $\mathcal{P}_n$ est vraie... » Car si vous supposez ainsi le résultat qu'il faut montrer, vous ne le montrerez jamais. Cette erreur est TRÈS GRAVE.

Bien souvent, l'hypothèse que $\mathcal{P}_n$ est vraie ne suffit pas pour montrer que $\mathcal{P}_{n+1}$ est vraie : on peut avoir besoin de $\mathcal{P}_n$ et $\mathcal{P}_{n-1}$, voire de toute la suite $\mathcal{P}_0, \mathcal{P}_1, \ldots, \mathcal{P}_n$. Nous allons voir sur un exemple comment le raisonnement par récurrence peut être adapté à de tels cas.

Exemple Soit $(u_n)_{n\in\mathbb{N}}$ la suite réelle définie par $u_0 = -1$, $u_1 = 5$ et : $\forall n \in \mathbb{N}, \quad u_{n+2} = 3u_{n+1} - 2u_n$.
Alors : $\forall n \in \mathbb{N}, \quad u_n = 6.2^n - 7$.

En effet

- Tout terme de la suite $(u_n)_{n\in\mathbb{N}}$ ne peut être calculé que si les deux termes précédents sont déjà connus ; on ne peut calculer u_{n+2} que si l'on connaît u_n et u_{n+1}. Quant à nous, nous voulons montrer la propriété $\mathcal{P}_n$ « $u_n = 6.2^n - 7$ » pour tout $n \in \mathbb{N}$. Nous ne pouvons pas la démontrer par une récurrence classique, car pour montrer $\mathcal{P}_{n+1}$, nous aurions besoin de supposer $\mathcal{P}_n$ <u>et</u> $\mathcal{P}_{n-1}$ vraies.

- Pour tout $n \in \mathbb{N}$, notons $\mathcal{Q}_n$ la propriété « $\mathcal{P}_n$ et $\mathcal{P}_{n+1}$ ». Supposons qu'on ait réussi à montrer que $\mathcal{Q}_n$ est vraie pour tout $n \in \mathbb{N}$; alors on a en fait montré que $\mathcal{P}_n$ est vraie pour tout $n \in \mathbb{N}$. Montrer la proposition « $\forall n \in \mathbb{N}, \quad \mathcal{P}_n$ » revient donc à montrer la proposition « $\forall n \in \mathbb{N}, \quad \mathcal{Q}_n$ ». Mais alors que nous ne pouvions pas montrer la première par une récurrence classique, nous allons pouvoir montrer la deuxième très simplement.

1) **Initialisation :** $\overbrace{u_0 = -1 = 6.2^0 - 7}^{\mathcal{P}_0}$ et $\overbrace{u_1 = 5 = 6.2^1 - 7}^{\mathcal{P}_1}$. Bref, $\mathcal{Q}_0$ est vraie.

2) **Hérédité :** Soit $n \in \mathbb{N}$. Supposons $\mathcal{Q}_n$ vraie. Cela revient à supposer $\mathcal{P}_n$ et $\mathcal{P}_{n+1}$ vraies. Nous devons montrer que $\mathcal{Q}_{n+1}$ est vraie, i.e. que $\mathcal{P}_{n+1}$ et $\mathcal{P}_{n+2}$ le sont. Mais comme $\mathcal{P}_{n+1}$ est vraie par hypothèse, il ne nous reste plus qu'à montrer que $\mathcal{P}_{n+2}$ est vraie ; ce qui est facile :

$$u_{n+2} = 3u_{n+1} - 2u_n = 3(6.2^{n+1} - 7) - 2(6.2^n - 7) = 9.2^{n+2} - 21 - 3.2^{n+2} + 14 = 6.2^{n+2} - 7.$$

Fin de la récurrence.

- En pratique, ne vous embêtez pas à définir proprement la propriété double $\mathcal{Q}_n$. Rédigez votre preuve de la façon suivante :

  1) **Initialisation :** Comme ci-dessus (double initialisation).

  2) **Hérédité :** Soit $n \in \mathbb{N}$. On suppose que $u_n = 6.2^n - 7$ et que $u_{n+1} = 6.2^{n+1} - 7$. Montrons que $u_{n+2} = 6.2^{n+2} - 7$. C'est facile : $u_{n+2} = \ldots = 6.2^{n+2} - 7$. Et voilà, c'est terminé.

Remarque On a souvent l'impression, quand on fait des récurrences, que les initialisations ne servent à rien. Quelle erreur de le croire ! Tentons par exemple de montrer que : $\forall n \in \mathbb{N}, \quad n = n + 1$. Ce résultat est faux, bien entendu.

- **Hérédité :** Soit $n \in \mathbb{N}$. Nous supposons que $n = n + 1$ et voulons montrer que $n + 1 = (n + 1) + 1$. C'est facile, il suffit d'ajouter 1 aux deux membres de l'hypothèse de récurrence : puisque $n = n + 1$, alors $n + 1 = n + 2$. L'hérédité ne pose donc aucun problème.
- **Initialisation :** En fait c'est l'initialisation qui pose problème, car l'égalité $0 = 1$ est fausse.

1.4 Le raisonnement par l'absurde

Principe du raisonnement par l'absurde : Pour montrer que p est vraie, on suppose qu'elle est fausse et on tâche d'en tirer une *contradiction*, i.e. la vérité de deux propositions q et « non q » ; une proposition et sa négation ne pouvant être vraies toutes les deux, on en déduit que l'hypothèse selon laquelle p est fausse est fausse, i.e. que p est vraie.

Exemple Tout entier est pair ou impair, mais pas les deux.

En effet Soit $n \in \mathbb{Z}$. Nous avons déjà vu que n est pair ou impair. Peut-il être les deux à la fois ? Pour montrer que non, supposons que oui. Alors n s'écrit $n = 2k = 2l + 1$ où $k, l \in \mathbb{Z}$. On a donc $2(k - l) = 1$, et du coup $\frac{1}{2}$ est un entier ; ce qui est faux. L'hypothèse selon laquelle n est à la fois pair et impair est donc fausse ; par conséquent n est pair ou impair, mais pas les deux.

Exemple Rappelons qu'un nombre est dit *rationnel* s'il est le quotient d'un entier par un entier non nul, i.e. s'il est une fraction d'entiers ; au contraire, un nombre est dit *irrationnel* s'il n'est pas rationnel.

Nous allons montrer ci-dessous que : $\sqrt{2}$ est irrationnel.

En effet

- Commençons par un petit lemme : pour tout $n \in \mathbb{Z}$, n est pair si et seulement si n^2 est pair. Fixons donc $n \in \mathbb{Z}$.

  1) Si n est pair, alors on peut écrire $n = 2k$ où $k \in \mathbb{Z}$, et donc $n^2 = (2k)^2 = 2(2k^2)$ avec $2k^2 \in \mathbb{Z}$: cela montre que n^2 est pair.

  2) Pour la réciproque, raisonnons par contraposition : cela revient à montrer que si n n'est pas pair, alors n^2 n'est pas pair. Si donc n n'est pas pair, alors n est impair comme nous l'avons vu, donc de la forme $n = 2k + 1$ où $k \in \mathbb{Z}$. On a alors $n^2 = (2k + 1)^2 = 2(2k^2 + 2k) + 1$ avec $(2k^2 + 2k) \in \mathbb{Z}$, de sorte que n^2 est impair. L'exemple précédent implique aussitôt que n^2 n'est pas pair.

- Supposons à présent, par l'absurde, que $\sqrt{2}$ est rationnel. Alors $\sqrt{2}$ peut s'écrire sous la forme $\frac{p}{q}$ où p et q sont deux entiers. Choisissons p et q de façon à ce que la fraction $\frac{p}{q}$ soit irréductible — aucune simplification n'est plus possible.

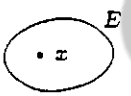
  1) L'égalité $p^2 = \left(q\sqrt{2}\right)^2 = 2q^2$ montre que p^2 est pair. Mais donc p est pair via le premier point et s'écrit $p = 2p'$ avec $p' \in \mathbb{Z}$.

2) Du coup $q^2 = \left(\frac{p}{\sqrt{2}}\right)^2 = \left(\frac{2p'}{\sqrt{2}}\right)^2 = (p'\sqrt{2})^2 = 2p'^2$. Ceci montre que q^2 est pair, et donc q aussi est pair, de la forme $q = 2q'$ avec $q' \in \mathbb{Z}$.

Concluons. Nous venons sans le voir de montrer que la fraction $\frac{p}{q}$ était réductible, contrairement à notre hypothèse, puisque $\frac{p}{q} = \frac{2p'}{2q'} = \frac{p'}{q'}$ — contradiction.

2 Un peu de théorie des ensembles

2.1 Appartenance et inclusion



Les notions intuitives d'ensemble et d'appartenance sont supposées connues : les ensembles sont des sacs de billes dont les éléments sont... les billes. Pour tout ensemble E, la relation « x est un élément de E » ou « x appartient à E » est notée $x \in E$; on note $x \notin E$ pour dire que x n'appartient pas à E. L'*ensemble vide*, i.e. qui n'a pas d'élément, est noté $\varnothing$.

Exemple

- On note $\mathbb{N}$ l'ensemble des *entiers naturels*, $\mathbb{Z}$ l'ensemble des *entiers relatifs*, $\mathbb{Q}$ l'ensemble des *rationnels*, $\mathbb{R}$ l'ensemble des *réels* et $\mathbb{C}$ l'ensemble des *nombres complexes*.
- On note en outre $\mathbb{E}_+$ l'ensemble des éléments positifs ou nuls de $\mathbb{E}$ quand $\mathbb{E}$ est l'un des ensembles $\mathbb{Q}$ ou $\mathbb{R}$; même principe pour la notation $\mathbb{E}_-$.
- On note enfin $\mathbb{E}^\times$ l'ensemble des éléments non nuls de $\mathbb{E}$ quand $\mathbb{E}$ est l'un des ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}_+$, $\mathbb{Q}_-$, $\mathbb{R}$, $\mathbb{R}_+$, $\mathbb{R}_-$, $\mathbb{C}$.

Définition (Egalité) Soient E et F deux ensembles. On dit que E et F sont *égaux* s'ils possèdent exactement les mêmes éléments, i.e. si : $\forall x, \quad (x \in E \iff x \in F)$.

Cette relation entre E et F est notée $E = F$.

Un ensemble peut être défini de deux façons : *en extension* ou *en compréhension*.

- Définir un ensemble en extension, c'est donner la liste complète explicite de tous ses éléments ; on note cette liste entre accolades, l'ordre des éléments listés n'ayant aucune importance. Par exemple, $\{0,1,2\}$ est un ensemble, le même que $\{2,1,0\}$. Un ensemble de la forme $\{x\}$, i.e. à seul élément, est appelé un *singleton* ; un ensemble de la forme $\{x,y\}$ avec $x \neq y$, i.e. à deux éléments, est appelé une *paire*. Il est bien évident qu'on ne peut définir en extension que des ensembles ayant un nombre fini d'éléments, incapables que nous sommes d'écrire une liste infinie de symboles.
- Définir un ensemble en compréhension, c'est donner une propriété vérifiée par les éléments de cet ensemble et eux seuls. Parler par exemple de l'ensemble des entiers naturels qui sont égaux à leur carré, c'est parler d'un ensemble unique que l'on note $\{n \in \mathbb{N} / \quad n^2 = n\}$; la lettre n pourrait être remplacée par n'importe quelle symbole ne figurant pas dans la définition de l'ensemble.

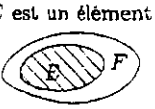
  Les éléments d'un ensemble sont souvent repérés dans une liste par un ou plusieurs « paramètres ». Ainsi $\{x_i\}_{i \in I}$ désigne l'ensemble des éléments notés x_i repérés par un indice i décrivant un certain ensemble I. Décrit en compréhension, cet ensemble s'écrit aussi $\{x / \quad \exists\, i \in I / \quad x = x_i\}$. Par exemple, $\{2^n\}_{n \in \mathbb{N}}$ désigne l'ensemble constitué des éléments $2^0, 2^1, 2^2, 2^3 \ldots$

Que ce soit bien clair : il n'y a pas deux sortes d'ensembles en mathématiques. Un même ensemble, s'il est fini, sera défini tour à tour en extension ou en compréhension selon les contextes. Ainsi les quatre ensembles décrits ci-dessous sont égaux :

$$\{0,1\} = \{n \in \mathbb{N} / \quad n^2 = n\} = \{z \in \mathbb{C} / \quad z^2 = z\} = \{n \in \mathbb{Z} / \quad n \geqslant 0 \text{ et } n < 2\}.$$

Définition (Inclusion) Soient E et F deux ensembles. On dit que E est *inclus dans* F si tout élément de E est un élément de F, i.e. si : $\forall x \in E, \quad x \in F$.

Cette relation entre E et F est notée $E \subseteq F$. On dit aussi que F *contient* E ou que E est une *partie de* F.



Exemple Les inclusions suivantes sont bien connues : $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

✖✖✖ Attention ! L'erreur classique consiste à confondre l'appartenance $\in$ et l'inclusion $\subseteq$. Soyez vigilants !

- L'ensemble $\Big\{0,\{0\}\Big\}$ est l'ensemble dont les éléments sont exactement 0 et $\{0\}$.
  1) Il est vrai que $0 \in \Big\{0,\{0\}\Big\}$ car 0 est bien un élément de $\Big\{0,\{0\}\Big\}$.
  2) Il est vrai que $\{0\} \in \Big\{0,\{0\}\Big\}$ car $\{0\}$ est bien un élément de $\Big\{0,\{0\}\Big\}$.
  3) Il est vrai que $\{0\} \subseteq \Big\{0,\{0\}\Big\}$. En effet, $\{0\}$ a pour seul élément 0. Tout élément de $\{0\}$ est donc bel et bien élément de $\Big\{0,\{0\}\Big\}$.
  4) Il est vrai enfin que $\Big\{\{0\}\Big\} \subseteq \Big\{0,\{0\}\Big\}$. En effet, $\Big\{\{0\}\Big\}$ a pour seul élément $\{0\}$. Tout élément de $\Big\{\{0\}\Big\}$ est donc bel et bien élément de $\Big\{0,\{0\}\Big\}$.
- On a $0 \in \mathbb{N}$, mais $0 \not\subseteq \mathbb{N}$. On a $\Big\{-1,0,1\Big\} \subseteq \mathbb{Z}$, mais $\Big\{-1,0,1\Big\} \notin \mathbb{Z}$.

✎✎✎ **En pratique** Si vous devez montrer une inclusion $E \subseteq F$ — vous aurez très souvent à le faire — commencer sans réfléchir ainsi : « Soit $x \in E$. Montrons que $x \in F$. » Vous avez le droit de ne pas réussir à aller plus loin, mais vous devez au moins penser à faire cela.

Exemple $\Big\{x \in \mathbb{R} /\ \ \exists\, y \in \mathbb{R}_+ /\ \ x \geqslant y\Big\} \subseteq \mathbb{R}_-$.

En effet Soit $x \in \mathbb{R}$ pour lequel il existe $y \in \mathbb{R}_-$ tel que $x \geqslant y$. Montrons que $x \in \mathbb{R}_-$.
Or $y \geqslant 0$ par hypothèse et $x \geqslant y$, donc $x \geqslant 0$. Cela montre bien que $x \in \mathbb{R}_+$.

Exemple Si E est l'ensemble des entiers de la forme $k(k+1)$ où $k \in \mathbb{N}$ et si $2\mathbb{N}$ est l'ensemble des entiers naturels pairs, alors : $E \subseteq 2\mathbb{N}$. En français, cela revient à dire que tout entier de la forme $k(k+1)$ avec $k \in \mathbb{N}$ est pair.

En effet Soit $n \in E$. Montrons que $n \in 2\mathbb{N}$. Par définition, il existe $k \in \mathbb{N}$ tels que $n = k(k+1)$. Or l'un des entiers k et $(k+1)$ est pair. En effet, k est pair ou impair, et si k est impair, alors $k+1$ est pair. Par produit, $n = k(k+1)$ est donc pair. En d'autres termes, $n \in 2\mathbb{N}$ comme annoncé.

Théorème Soient E et F deux ensembles. E et F sont égaux si et seulement si $E \subseteq F$ et $F \subseteq E$.

✎✎✎ **En pratique** Pour démontrer l'égalité de deux ensembles E et F, deux possibilités :

1) soit vous raisonnez directement par équivalence : $x \in E \iff \ldots \iff x \in F$;
   Il n'est malheureusement pas toujours possible de raisonner ainsi, cela peut s'avérer compliqué à rédiger.
2) soit vous raisonnez par double inclusion en vous appuyant sur le théorème précédent. Cela revient à raisonner en deux temps. Premier temps : vous vous donnez un élément de E et vous montrez qu'il appartient à F. Second temps : vous vous donnez un élément de F et vous montrez qu'il appartient à E.

L'exemple suivant illustre l'usage de la technique 2). La technique 1) sera illustrée plus loin par différents théorèmes.

Exemple $\mathbb{R}_- = \Big\{x \in \mathbb{R} /\ \ \forall y \in \mathbb{R}_+,\ \ x \leqslant y\Big\}$.

En effet

- Montrons que $\mathbb{R}_- \subseteq \Big\{x \in \mathbb{R} /\ \ \forall y \in \mathbb{R}_+,\ \ x \leqslant y\Big\}$.
  Soit $x \in \mathbb{R}_-$. Nous devons montrer que : $\forall y \in \mathbb{R}_+,\ \ x \leqslant y$. Soit donc $y \in \mathbb{R}_-$. On a bien $x \leqslant y$ comme voulu, puisque x est négatif et y positif.
- Montrons que $\Big\{x \in \mathbb{R} /\ \ \forall y \in \mathbb{R}_+,\ \ x \leqslant y\Big\} \subseteq \mathbb{R}_-$.
  Soit $x \in \mathbb{R}$ tel que : $\forall y \in \mathbb{R}_-,\ \ x \leqslant y$. Alors en particulier $x \leqslant 0$ (pour $y = 0$). Cela montre bien que $x \in \mathbb{R}_-$.

Définition (Ensemble des parties) Soit E un ensemble. L'ensemble des parties de E est noté $\mathscr{P}(E)$.
Pour tout ensemble A, on a donc : $A \in \mathscr{P}(E) \iff A \subseteq E$.

✖✖✖ Attention ! Dire que A **appartient à** $\mathscr{P}(E)$ équivaut à dire que A est **incluse dans** E. Il est ici particulièrement important de comprendre la différence entre appartenance et inclusion.

Exemple Soit E un ensemble. Alors $E \in \mathscr{P}(E)$ et $\varnothing \in \mathscr{P}(E)$.

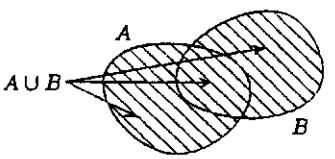
En effet

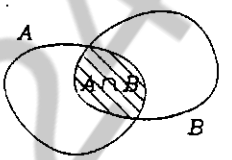
- Montrons que $E \in \mathscr{P}(E)$. Cela revient à montrer que $E \subseteq E$, ce qui est vrai car tout élément de E est un élément de E.
- Montrons que $\varnothing \in \mathscr{P}(E)$. Cela revient à montrer que tout élément de $\varnothing$ est un élément de E ; autrement dit que, pour tout x, si $x \in \varnothing$, alors $x \in E$; ce qui s'écrit encore : $\forall x, \quad (x \in \varnothing \implies x \in E)$.
  Or par définition $\varnothing$ n'a pas d'élément. D'antécédent faux, l'implication « $x \in \varnothing \implies x \in E$ » est donc vraie via la table de vérité de $\implies$. Il est donc vrai que : $\forall x, \quad (x \in \varnothing \implies x \in E)$ comme voulu.

2.2 Opérations sur les ensembles

Définition (Réunion, intersection) Soient A et B deux ensembles.

- On appelle *réunion de A et B*, notée $A \cup B$, l'ensemble des x tels que : $x \in A$ ou $x \in B$.
- On appelle *intersection de A et B*, notée $A \cap B$, l'ensemble des x tels que : $x \in A$ et $x \in B$.





Ces définitions se généralisent au cas de plus de deux ensembles. Soit $\{A_i\}_{i \in I}$ un ensemble d'ensembles — cela veut dire que I est un ensemble, et que pour tout $i \in I$, A_i est un ensemble.

- On appelle *réunion des A_i, $i \in I$*, notée $\bigcup_{i \in I} A_i$, l'ensemble des x tels que : $\exists\, i \in I / \quad x \in A_i$.
  « x est dans l'un des A_i »
- On appelle *intersection des A_i, $i \in I$*, notée $\bigcap_{i \in I} A_i$, l'ensemble des x tels que : $\forall i \in I, \quad x \in A_i$.
  « x est dans tous les A_i »

Explication On notera bien les parallélismes suivants : $\cup$/ou/$\exists$ d'une part, $\cap$/et/$\forall$ d'autre part.

Définition (Ensembles disjoints) Soient E et F deux ensembles. On dit que E et F sont *disjoints* si $E \cap F = \varnothing$, autrement dit si E et F n'ont aucun élément commun.

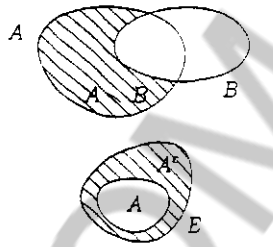
Théorème (Distributivité de la réunion et de l'intersection l'une sur l'autre) Soient $\{A_i\}_{i \in I}$ un ensemble d'ensembles et B un ensemble. $\left(\bigcup_{i \in I} A_i\right) \cap B = \bigcup_{i \in I} (A_i \cap B)$ et $\left(\bigcap_{i \in I} A_i\right) \cup B = \bigcap_{i \in I} (A_i \cup B)$.

Démonstration Contentons-nous de démontrer la première égalité. La deuxième se montre de la même façon.
Soit x.

$$x \in \left(\bigcup_{i \in I} A_i\right) \cap B \iff x \in \bigcup_{i \in I} A_i \text{ et } x \in B \iff (\exists\, i \in I / \ x \in A_i) \text{ et } x \in B$$
$$\iff \exists\, i \in I / \ (x \in A_i \text{ et } x \in B) \iff \exists\, i \in I / \ x \in A_i \cap B$$
$$\iff x \in \bigcup_{i \in I} (A_i \cap B).$$

■

Définition (Différence, complémentaire)



- Soient A et B deux ensembles.
On appelle *différence de B dans A*, notée $A \setminus B$, l'ensemble des x tels que : $x \in A$ et $x \notin B$.

- Soient E un ensemble et A une partie de E. L'ensemble $E \setminus A$ est appelé le *complémentaire de A dans E*. Il est noté A^c ou $\bar{A}$ quand il n'y a pas d'ambiguïté.

Théorème (Relations de De Morgan) Soit $\left(A_i\right)_{i\in I}$ un ensemble de parties d'un même ensemble E.

$$\left(\bigcup_{i\in I} A_i\right)^c = \bigcap_{i\in I} A_i^c \qquad \text{et} \qquad \left(\bigcap_{i\in I} A_i\right)^c = \bigcup_{i\in I} A_i^c.$$

Explication Pourquoi appeler ces égalités « relations de De Morgan » ? Dans le cas de deux ensembles A et B, elles s'écrivent : $(A \cup B)^c = A^c \cap B^c$ et $(A \cap B)^c = A^c \cup B^c$.
Si nous voyons la réunion comme un « ou », l'intersection comme un « et » et le passage au complémentaire comme un « non », ces égalités nous rappellent les lois de De Morgan de notre introduction à la logique. — À méditer.

Démonstration Contentons-nous de démontrer la première égalité. Soit donc $x \in E$.

$$x \in \left(\bigcup_{i\in I} A_i\right)^c \iff \text{non}\left(x \in \bigcup_{i\in I} A_i\right) \iff \text{non}\left(\exists\, i \in I/ \quad x \in A_i\right)$$

$$\iff \forall i \in I, \quad \text{non}\left(x \in A_i\right) \iff \forall i \in I, \quad x \in A_i^c \iff x \in \bigcap_{i\in I} A_i^c. \quad \blacksquare$$

Nous aurons l'occasion de revenir plus tard sur les définitions qui suivent. Contentons-nous ici d'une présentation intuitive.
Pour tout $m, n \in \mathbb{Z}$ tels que $m \leqslant n$, on note $[\![m, n]\!]$ l'ensemble des entiers compris entre m et n (m et n inclus) ; si on veut exclure m par exemple, on utilise la notation $]\!]m, n]\!]$;

Définition (Famille)

- Soient E et I deux ensembles. Une suite d'éléments de E repérés chacun par un élément de I est appelée une *famille d'éléments de E indexée par I*.

- Une telle famille est notée $(x_i)_{i\in I}$ — $x_i \in E$ étant repéré par l'indice $i \in I$. Dans le cas où $I = [\![m, n]\!]$ où $m, n \in \mathbb{Z}$ sont tels que $m \leqslant n$, on la note plus couramment $(x_i)_{m\leqslant i\leqslant n}$ ou $(x_m, x_{m+1}, \ldots, x_n)$.

- Deux familles $(x_i)_{i\in I}$ et $(y_i)_{i\in I}$ d'éléments de E indexées par I sont égales si et seulement si : $\forall i \in I, \quad x_i = y_i$.
L'élément x_i est appelé la *composante d'indice i de $(x_i)_{i\in I}$*.

Attention !

- Ne confondez surtout pas la **famille** $(x_i)_{i\in I}$ avec l'**ensemble** $\left\{x_i\right\}_{i\in I}$. Dans un ensemble, les éléments sont donnés sans ordre ; dans une famille l'ordre des éléments compte. Ainsi $\left\{1, 2, 3\right\} = \left\{2, 3, 1\right\}$, mais $(1, 2, 3) \neq (2, 3, 1)$.

- Dans une famille du type $(x_i)_{m\leqslant i\leqslant n}$, il y a $\left(n - m \boxed{+1}\right)$ éléments, et non pas $(n - m)$ comme on pourrait le penser.

Définition (Produit cartésien) Soient $E_1, E_2, \ldots, E_n$ des ensembles non vides. L'ensemble des familles $(x_1, x_2, \ldots, x_n)$ dans lesquelles $x_1 \in E_1$, $x_2 \in E_2$, … $x_n \in E_n$ est appelé le *produit (cartésien) de $E_1, E_2, \ldots, E_n$* et noté $E_1 \times E_2 \times \ldots \times E_n$.

Dans le cas où $E_1 = E_2 = \ldots = E_n = E$, le produit $E_1 \times E_2 \times \ldots \times E_n$ est généralement noté E^n.

Remarque Les débuts de proposition « $\forall x \in E_1, \ \forall y \in E_2, \ldots$ » et « $\forall (x, y) \in E_1 \times E_2 \ldots$ » sont rigoureusement identiques.

3 Un peu de calcul

3.1 Le symbole somme $\sum$

3.1.1 Définition

Définition (Symbole $\sum$) Soient I un ensemble fini et $(z_i)_{i\in I}$ une famille de nombres complexes indexée par I. La somme des z_i, i parcourant l'ensemble I, est notée $\sum_{i\in I} z_i$.

Dans le cas où $I = [\![m,n]\!]$ où $m,n \in \mathbb{Z}$ sont tels que $m \leqslant n$, on la note plus couramment $\sum_{k=m}^{n} z_k$ ou $\sum_{m\leqslant k\leqslant n} z_k$. Elle vaut $z_m + z_{m+1} + z_{m+2} + \ldots + z_n$.

Dans le cas où $I = [\![m,n]\!] \times [\![p,q]\!]$ où $m,n,p,q \in \mathbb{Z}$ sont tels que $m \leqslant n$ et $p \leqslant q$, on la note plus couramment $\sum_{\substack{m\leqslant k\leqslant n\\ p\leqslant l\leqslant q}} z_{kl}$.

Remarque La lettre k peut être remplacée par tout symbole distinct des bornes m et n et ne figurant pas dans les z_k.

En pratique Le symbole $\sum$ est utilisé très souvent en mathématiques. Quand vous êtes bloqués devant une somme quelconque, écrivez-la *in extenso*, i.e. en détaillant les termes qui la composent ; les choses peuvent vous paraître plus claires alors. Par exemple, pour étudier la somme $\sum_{k=1}^{n} \sqrt{k}$, on pourra l'écrire $\sqrt{1} + \sqrt{2} + \sqrt{3} + \ldots + \sqrt{n-1} + \sqrt{n}$.

Exemple Soit $\alpha \in \mathbb{C}$. $\displaystyle\sum_{k=m}^{n} \alpha = \overbrace{\alpha}^{k=m} + \overbrace{\alpha}^{k=m+1} + \ldots + \overbrace{\alpha}^{k=n} = \overbrace{\alpha+\alpha+\ldots+\alpha}^{(n-m+1)\text{ fois}} = (n-m+1)\alpha.$

Exemple $\displaystyle\sum_{k=1}^{n} \frac{1}{k} - 1 + \frac{1}{n+1} = \left(1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n-1} + \frac{1}{n}\right) - 1 + \frac{1}{n+1} = \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n-1} + \frac{1}{n} + \frac{1}{n+1} = \sum_{k=2}^{n+1} \frac{1}{k}.$

Attention ! Dans une somme du type $\sum_{k=1}^{n} z_k$, il convient de ne jamais confondre k et n. Ainsi $\sum_{k=1}^{n} k$ et $\sum_{k=1}^{n} n$ sont deux quantités tout à fait différentes : $\displaystyle\sum_{k=1}^{n} n = \underbrace{n+n+\ldots+n}_{n\text{ fois}} \neq 1+2+3+\ldots+(n-1)+n = \sum_{k=1}^{n} k.$

3.1.2 Changements d'indice

Le *changement d'indice* est une opération très courante. Les exemples valent ici mieux qu'un long discours.

Exemple

- $\displaystyle\sum_{k=0}^{n} \frac{1}{(k+1)^2} = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \ldots + \frac{1}{(n+1)^2} = \sum_{l=1}^{n+1} \frac{1}{l^2}$. On a effectué ici le changement d'indice $l = k+1$. Cela revient à remplacer tous les k de la somme initiale par des $l-1$. Mais il faut aussi changer les bornes. Quand k varie de 0 à n, que fait $l = k+1$? Il varie de $0+1 = 1$ à $n+1$.
- $\displaystyle\sum_{r=2}^{9} r^r = 2^2 + 3^3 + 4^4 + \ldots + 9^9 = \sum_{s=0}^{7} (s+2)^{s+2}$. On a effectué ici le changement d'indice $r = s+2$. Pendant que r varie de 2 à 9, $s = r-2$ varie de 0 à 7.

3.1.3 Simplifications télescopiques

Le résultat suivant est à la fois stupide et essentiel : les simplifications télescopiques sont partout.

Théorème (Simplifications télescopiques) Soit $(z_k)_{m\leqslant k\leqslant n+1}$ une famille de nombres complexes.

$$\sum_{k=m}^{n}(z_{k+1}-z_k)=z_{n+1}-z_m.$$

Démonstration

$$\sum_{k=m}^{n}(z_{k+1}-z_k)=(z_{n+1}\overbrace{-z_n)+(z_n}^{\text{simplification}}\overbrace{-z_{n-1})+(z_{n-1}}^{\text{simplification}}-z_{n-2})+\ldots+(z_{m+2}\overbrace{-z_{m+1})+(z_{m+1}}^{\text{simplification}}-z_m)=z_{n+1}-z_m.\ \blacksquare$$

Exemple $\displaystyle\sum_{k=1}^{n}\frac{1}{k(k+1)}=\sum_{k=1}^{n}\left(\frac{1}{k}-\frac{1}{k+1}\right)=1-\frac{1}{n+1}.$

3.1.4 Sommes doubles

Théorème (Permutation des $\sum$) Soit $(z_{ij})_{1\leqslant i,j\leqslant n}$ une famille de nombres complexes.

$$\sum_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant n}}z_{ij}=\sum_{i=1}^{n}\sum_{j=1}^{n}z_{ij}=\sum_{j=1}^{n}\sum_{i=1}^{n}z_{ij},\qquad\sum_{1\leqslant i\leqslant j\leqslant n}z_{ij}=\sum_{j=1}^{n}\sum_{i=1}^{j}z_{ij}=\sum_{i=1}^{n}\sum_{j=i}^{n}z_{ij},\qquad\sum_{1\leqslant i<j\leqslant n}z_{ij}=\sum_{j=2}^{n}\sum_{i=1}^{j-1}z_{ij}=\sum_{i=1}^{n-1}\sum_{j=i+1}^{n}z_{ij}.$$

Démonstration

- **Première série d'égalités :** La famille $(z_{ij})_{1\leqslant i,j\leqslant n}$ peut être présentée sous la forme d'un tableau à deux entrées :

i \ j	1	2	3	$\cdots$	n
1	z_{11}	z_{12}	z_{13}	$\cdots$	z_{1n}
2	z_{21}	z_{22}	z_{23}	$\cdots$	z_{2n}
3	z_{31}	z_{32}	z_{33}	$\cdots$	z_{3n}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
n	z_{n1}	z_{n2}	z_{n3}	$\cdots$	z_{nn}

Calculer la somme $\displaystyle\sum_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant n}}z_{ij}$, notée aussi $\displaystyle\sum_{1\leqslant i,j\leqslant n}z_{ij}$, c'est calculer la somme de tous les termes de ce tableau. On peut effectuer ce calcul de différentes manières. Voyons ce qui se passe si on effectue d'abord la somme des termes de chaque ligne, avant d'additionner les résultats obtenus.

Pour tout $i\in[\![1,n]\!]$, la somme des termes de la $i^{\text{ème}}$ ligne s'écrit $\displaystyle\sum_{j=1}^{n}z_{ij}$; c'est un certain nombre complexe qui dépend de i. Faire la somme des résultats ainsi obtenus sur chaque ligne, c'est faire la somme $\displaystyle\sum_{i=1}^{n}\sum_{j=1}^{n}z_{ij}$.

Ceci explique qu'on ait : $\displaystyle\sum_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant n}}z_{ij}=\sum_{i=1}^{n}\sum_{j=1}^{n}z_{ij}$. On démontre la seconde égalité en sommant d'abord sur chaque colonne.

- **Seconde série d'égalités :** Calculer la somme $\displaystyle\sum_{1\leqslant i\leqslant j\leqslant n}z_{ij}$, c'est calculer la somme de termes du tableau suivant :

i \ j	1	2	3	$\cdots$	n
1	z_{11}	z_{12}	z_{13}	$\cdots$	z_{1n}
2		z_{22}	z_{23}	$\cdots$	z_{2n}
3			z_{33}	$\cdots$	z_{3n}
$\vdots$				$\ddots$	$\vdots$
n					z_{nn}

Pour tout $j\in[\![1,n]\!]$, la somme des termes de la $j^{\text{ème}}$ colonne de ce tableau s'écrit $\displaystyle\sum_{i=1}^{j}z_{ij}$; c'est un certain nombre complexe qui dépend de j. Faire la somme des résultats ainsi obtenus sur chaque colonne, c'est faire la somme $\displaystyle\sum_{j=1}^{n}\sum_{i=1}^{j}z_{ij}$. Ceci explique qu'on ait : $\displaystyle\sum_{1\leqslant i\leqslant j\leqslant n}z_{ij}=\sum_{j=1}^{n}\sum_{i=1}^{j}z_{ij}$.

On démontre la seconde égalité en sommant d'abord sur chaque ligne.

• **Troisième série d'égalités :** A vous de jouer ! Je vous donne juste le tableau correspondant :

i \ j	1	2	3	$\cdots$	n
1	$\times$	z_{12}	z_{13}	$\cdots$	z_{1n}
2		$\times$	z_{23}	$\cdots$	z_{2n}
3			$\times$	$\cdots$	z_{3n}
$\vdots$				$\ddots$	$\vdots$
n					$\times$

■

3.2 Le symbole produit $\prod$

Nous passerons plus vite sur les produits que sur les sommes ; car une fois qu'on a compris $\sum$, on a compris $\prod$.

Définition (Symbole $\prod$) Soient I un ensemble fini et $(z_i)_{i\in I}$ une famille de nombres complexes indexée par I. Le produit des z_i, i parcourant l'ensemble I, est noté $\prod_{i\in I} z_i$.

Exemple Soit $\alpha \in \mathbb{C}$. $\prod_{k=m}^{n} \alpha = \overbrace{\alpha \times \alpha \times \ldots \times \alpha}^{(n-m+1) \text{ fois}} = \alpha^{n-m+1}$.

Définition (Factorielle) Pour tout $n \in \mathbb{N}^*$, on appelle *factorielle* n, notée $n!$, l'entier $n! = \prod_{k=1}^{n} k = 1 \times 2 \times 3 \times \ldots \times n$.
Par convention, $0! = 1$.

✖✖✖ Attention ! Dans un produit du type $\prod_{k=1}^{n} z_k$, il convient de ne jamais confondre k et n. Ainsi $\prod_{k=1}^{n} k$ et $\prod_{k=1}^{n} n$ sont deux quantités tout à fait différentes : $n^n = \prod_{k=1}^{n} n = \underbrace{n \times n \times \ldots \times n}_{n \text{ fois}} \neq 1 \times 2 \times 3 \times \ldots \times (n-1) \times n = \prod_{k=1}^{n} k = n!$.

Théorème (Simplifications télescopiques) Soit $(z_k)_{m\leqslant k\leqslant n+1}$ une famille de nombres complexes non nuls.

$$\prod_{k=m}^{n} \frac{z_{k+1}}{z_k} = \frac{z_{n+1}}{z_m}.$$

Théorème (Permutation des $\prod$) Soit $(z_{ij})_{1\leqslant i,j\leqslant n}$ une famille de nombres complexes.

$$\prod_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant n}} z_{ij} = \prod_{i=1}^{n}\prod_{j=1}^{n} z_{ij} = \prod_{j=1}^{n}\prod_{i=1}^{n} z_{ij}, \qquad \prod_{1\leqslant i\leqslant j\leqslant n} z_{ij} = \prod_{j=1}^{n}\prod_{i=1}^{j} z_{ij} = \prod_{i=1}^{n}\prod_{j=i}^{n} z_{ij}, \qquad \prod_{1\leqslant i<j\leqslant n} z_{ij} = \prod_{j=2}^{n}\prod_{i=1}^{j-1} z_{ij} = \prod_{i=1}^{n-1}\prod_{j=i+1}^{n} z_{ij}.$$

Exemple La notation $\prod_{1\leqslant i,j\leqslant n} (ij^2)$ est un résumé de la notation $\prod_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant n}} (ij^2)$.

$$\prod_{1\leqslant i,j\leqslant n} (ij^2) = \prod_{i=1}^{n}\prod_{j=1}^{n} (ij^2) = \prod_{i=1}^{n}\left(i^n \prod_{j=1}^{n} j^2\right) = \left(\prod_{i=1}^{n} i^n\right)\left(\prod_{j=1}^{n} j^2\right)^n = \left(\prod_{i=1}^{n} i\right)^n \left(\prod_{j=1}^{n} j\right)^{2n} = (n!)^n (n!)^{2n} = (n!)^{3n}.$$

✖✖✖ Attention ! Les symboles $\sum$ et $\prod$ ne peuvent être permutés en général. Ainsi :

$$\prod_{i=1}^{n}\sum_{j=1}^{n} 1 = \prod_{i=1}^{n} n = n^n \neq n = \sum_{j=1}^{n} 1 = \sum_{j=1}^{n}\prod_{i=1}^{n} 1.$$

Ce n'est pas étonnant, car c'est déjà faux avec deux termes : $(a+b)(c+d) \neq ab+cd$ en général.

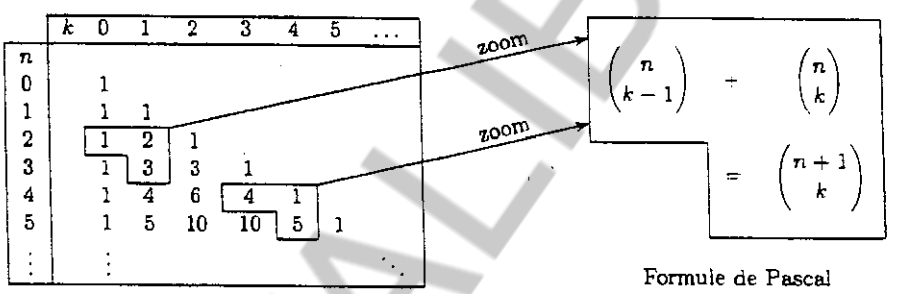
3.3 Quelques formules à connaître par cœur

La définition et les formules suivantes sont en principe de simples rappels.

Définition (Coefficients binomiaux)

- Pour tous $n, k \in \mathbb{N}$ tels que $k \leqslant n$, on appelle (*coefficient binomial*) k *parmi* n, noté $\binom{n}{k}$, le nombre :
$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$
- Pour tout $n \in \mathbb{N}$ et pour tout $k \in [\![0, n]\!]$: $\binom{n}{k} = \binom{n}{n-k}$.
- Pour tout $n \in \mathbb{N}$: $\binom{n}{0} = \binom{n}{n} = 1$, $\binom{n}{1} = \binom{n}{n-1} = n$ et $\binom{n}{2} = \binom{n}{n-2} = \frac{n(n-1)}{2}$.
- **Formule de Pascal :** Pour $n \geqslant 1$, et pour tout $k \in [\![1, n]\!]$: $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$.

Explication On peut calculer tous les coefficients binomiaux à l'aide de la formule de Pascal, en construisant un tableau qu'on appelle le *triangle de Pascal*. On y range $\binom{n}{k}$ dans la case qui se trouve à l'intersection de la ligne n et de la colonne k.



Formule de Pascal

Théorème (Formule du binôme de Newton) Soient $n \in \mathbb{N}$ et $a, b \in \mathbb{C}$. $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.

Démonstration Soient $a, b \in \mathbb{C}$ fixés. Raisonnons par récurrence.

- **Initialisation :** $(a+b)^0 = 1 = \binom{0}{0} a^0 b^{0-0} = \sum_{k=0}^{0} \binom{0}{k} a^k b^{0-k}$.
- **Hérédité :** Soit $n \in \mathbb{N}$. On suppose que $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n = (a+b)\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k} = a\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k} + b\sum_{l=0}^{n}\binom{n}{l}a^l b^{n-l} \\
&= \sum_{k=0}^{n}\binom{n}{k}a^{k+1}b^{n-k} + \sum_{l=0}^{n}\binom{n}{l}a^l b^{n-l+1} = a^{n+1} + \sum_{k=0}^{n-1}\binom{n}{k}a^{k+1}b^{n-k} + \sum_{l=1}^{n}\binom{n}{l}a^l b^{n-l+1} + b^{n+1} \\
&= a^{n+1} + \sum_{k'=1}^{n}\binom{n}{k'-1}a^{k'}b^{n-k'+1} + \sum_{l=1}^{n}\binom{n}{l}a^l b^{n-l+1} + b^{n+1} \qquad \text{(changement d'indice } k' = k+1\text{)} \\
&= a^{n+1} + \sum_{k=1}^{n}\left[\binom{n}{k-1} + \binom{n}{k}\right]a^k b^{(n+1)-k} + b^{n+1}
\end{aligned}$$

$$= a^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^k b^{(n+1)-k} + b^{n+1} \qquad \text{(formule de Pascal)}$$

$$= \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{(n+1)-k}. \qquad \text{Fin de la récurrence.}$$ ■

Théorème Soit $n \in \mathbb{N}$. $\displaystyle\sum_{k=0}^{n} k = \frac{n(n+1)}{2}, \qquad \sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}.$

Démonstration

- Posons $S_n = \displaystyle\sum_{k=0}^{n} k$. Effectuant dans S_n le changement d'indice $l = n - k$, nous obtenons la chaine d'égalités $S_n = \displaystyle\sum_{l=0}^{n}(n-l) = \sum_{l=0}^{n} n - \sum_{l=0}^{n} l = n(n+1) - S_n$. Ceci montre que $2S_n = n(n+1)$, donc que $S_n = \dfrac{n(n+1)}{2}$.

- Pour tout $k \in [\![0, n]\!]$: $(k+1)^3 - k^3 = 3k^2 + 3k + 1$ via la formule du binôme de Newton.
  Sommons toutes ces identités, de $k = 0$ à $k = n$: $\displaystyle\sum_{k=0}^{n}\left[(k+1)^3 - k^3\right] = 3\sum_{k=0}^{n} k^2 + 3\sum_{k=0}^{n} k + \sum_{k=0}^{n} 1$. La somme de gauche est le lieu d'une simplification télescopique ; d'autre part nous venons de calculer $\displaystyle\sum_{k=0}^{n} k$ et savons que $\displaystyle\sum_{k=0}^{n} 1 = (n+1)$. Du coup : $(n+1)^3 = 3\sum_{k=0}^{n} k^2 + 3\,\dfrac{n(n+1)}{2} + (n+1)$.
  Isolant $\displaystyle\sum_{k=0}^{n} k^2$ et simplifiant les calculs aisément, nous obtenons le résultat voulu. ■

Théorème Soient $n \in \mathbb{N}$ et $a, b \in \mathbb{C}$. $\quad a^n - b^n = (a-b)\displaystyle\sum_{k=0}^{n-1} a^k b^{n-k-1}.$

✖✖✖ <u>Attention</u> ! Gare à ceux qui confondent cette formule avec la formule du binôme de Newton !

Démonstration Développons le membre de droite de la formule :

$$(a-b)\sum_{k=0}^{n-1} a^k b^{n-k-1} = a\sum_{k=0}^{n-1} a^k b^{n-k-1} - b\sum_{k=0}^{n-1} a^k b^{n-k-1} = \sum_{k=0}^{n-1} a^{k+1} b^{n-(k+1)} - \sum_{k=0}^{n-1} a^k b^{n-k}$$

$$= a^n - b^n \qquad \text{par simplification télescopique.}$$ ■

En particulier, pour $b = 1$, on obtient l'identité fondamentale suivante :

Corollaire Pour tous $n \in \mathbb{N}$ et $q \in \mathbb{C}$: $\displaystyle\sum_{k=0}^{n-1} q^k = \begin{cases} \dfrac{q^n - 1}{q-1} & \text{si } q \neq 1 \\ n & \text{si } q = 1 \end{cases}.$

✎✎✎ **En pratique** Souvent, on n'a pas affaire à des sommes dont l'indice inférieur est 0. Si par exemple on doit calculer $\displaystyle\sum_{k=2}^{n} 2^k$, on commence par mettre en facteur le premier terme puis on effectue un changement d'indice :

$$\sum_{k=2}^{n} 2^k = 2^2 \sum_{k=2}^{n} 2^{k-2} \overset{l=k-2}{=} 4\sum_{l=0}^{n-2} 2^l = 4 \times \frac{2^{n-1} - 1}{2 - 1} = 2^{n+1} - 4.$$

Arithmétique des entiers relatifs

1 Division dans $\mathbb{Z}$

1.1 Relation de divisibilité

Définition (Divisibilité, diviseur, multiple) Soient $a, b \in \mathbb{Z}$. On dit que a *divise* b, ou que a est un *diviseur de* b, ou que b est un *multiple de* a, s'il existe $k \in \mathbb{Z}$ tel que $b = ak$; cette relation entre a et b se note $a|b$.

Théorème (Propriétés de la relation de divisibilité) Soient $a, b, c, d \in \mathbb{Z}$.

(i) La relation de divisibilité $|$ sur $\mathbb{Z}$ est réflexive et transitive ; elle n'est cependant pas antisymétrique puisque :

$$a|b \quad \text{et} \quad b|a \iff |a| = |b| \iff a = b \quad \text{ou} \quad a = -b.$$

En revanche, sa restriction à $\mathbb{N}$ l'est : c'est une relation d'ordre.

(ii) **Combinaisons linéaires :** Si $d|a$ et si $d|b$, alors $d|(au + bv)$ pour tous $u, v \in \mathbb{Z}$.

(iii) **Produit :** Si $a|b$ et si $c|d$, alors $ac|bd$. En particulier, si $a|b$, alors $a^k|b^k$ pour tout $k \in \mathbb{N}$.

(iv) **Multiplication/division par un entier :** Si $d \neq 0$: $a|b \iff ad|bd$.

Démonstration

(i) La réflexivité et la transitivité de $|$ ont été démontrées dans le chapitre sur les relations d'ordre. Contentons-nous de montrer l'équivalence relative au défaut d'antisymétrie de $|$. L'une des deux implications est triviale : si $|a| = |b|$, i.e. $a = b$ ou $a = -b$, il est clair que $a|b$ et que $b|a$.
Réciproquement, supposons qu'on ait $a|b$ et $b|a$. Alors il existe $k, l \in \mathbb{Z}$ tels que $b = ak$ et $a = bl$. Du coup $b = bkl$. Deux cas se présentent alors : si $b = 0$, alors $a = bl = 0$ et on a donc bien $|a| = |b|$; si au contraire $b \neq 0$, alors $kl = 1$ et donc, puisque k et l sont entiers, on a soit $k = l = 1$, soit $k = l = -1$, i.e. $a = b$ ou $a = -b$, i.e. $|a| = |b|$ comme voulu.

(ii) Supposons qu'on ait $d|a$ et $d|b$. Il existe donc $k, l \in \mathbb{Z}$ tels que $a = dk$ et $b = dl$. Alors $au + bv = d(ku + vl)$ avec $ku + vl \in \mathbb{Z}$ pour tous $u, v \in \mathbb{Z}$, et donc $d|(au + bv)$ comme annoncé.

(iv) Supposons $d \neq 0$. Si $a|b$, alors comme par ailleurs $d|d$, l'assertion (iii) affirme que $ad|bd$.
Réciproquement, supposons que $ad|bd$. Il existe alors $k \in \mathbb{Z}$ tel que $bd = kad$, et donc tel que $b = ak$. Ceci montre bien que $a|b$. ∎

1.2 Relation de congruence

Définition (Congruence modulo un entier) Soient $n \in \mathbb{N}$ et $a, b \in \mathbb{Z}$. On dit que a *est congru à* b *modulo* n si $n|(b - a)$, i.e. s'il existe $k \in \mathbb{Z}$ tel que $b = a + kn$; cette relation entre a et b se note $a \equiv b \mod n$.

Explication La relation de congruence est une généralisation de la relation de divisibilité ; il faut en effet avoir en tête le cas particulier suivant : $n|a \iff a \equiv 0 \mod n$.

Théorème (Propriétés de la relation de congruence) Soient $a, a', b, b' \in \mathbb{Z}$ et $m, n \in \mathbb{N}$.

(i) La relation $\cdot \equiv \cdot \mod n$ est réflexive, symétrique et transitive.

(ii) **Somme :** Si $a \equiv b \mod n$ et si $a' \equiv b' \mod n$, alors $a + a' \equiv b + b' \mod n$.

(iii) **Produit :** Si $a \equiv b \mod n$ et si $a' \equiv b' \mod n$, alors $aa' \equiv bb' \mod n$.
En particulier, si $a \equiv b \mod n$, alors $a^k \equiv b^k \mod n$ pour tout $k \in \mathbb{N}$.

(iv) **Multiplication/division par un entier :** Si $m \neq 0$: $a \equiv b \mod n \iff am \equiv bm \mod mn$.

Démonstration

(i) La réflexivité et la symétrie de $\cdot \equiv \cdot \mod n$ sont immédiates. Montrons seulement la transitivité. Trois entiers $a, b, c \in \mathbb{Z}$ étant donnés, supposons qu'on ait $a \equiv b \mod n$ et $b \equiv c \mod n$. Alors $n|(b-a)$ et $n|(c-b)$, donc par somme $n\Big|\big((c-b)+(b-a)\big)$, i.e. $n|(c-a)$, ou encore $a \equiv c \mod n$.

(ii) Si $a \equiv b \mod n$ et si $a' \equiv b' \mod n$, alors $n|(b-a)$ et $n|(b'-a')$, donc par somme $n\Big|\big((b-a)+(b'-a')\big)$, i.e. $n\Big|\big((b+b')-(a+a')\big)$, ou encore $a+a' \equiv b+b' \mod n$.

(iii) On remarque que $bb'-aa' = b(b'-a')+a'(b-a)$. Du coup, si $a \equiv b \mod n$ et si $a' \equiv b' \mod n$, alors $n|(b-a)$ et $n|(b'-a')$, et donc par combinaison linéaire $n\Big|\big(b(b'-a')+a'(b-a)\big)$, i.e. $n|(bb'-aa')$, ou encore $aa' \equiv bb' \mod n$.

(iv) Enfin : $a \equiv b \mod n \iff n|(b-a) \overset{m\neq 0}{\iff} mn|m(b-a) \iff am \equiv bm \equiv mn$. ■

1.3 Division euclidienne

Théorème (Division euclidienne) Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^\times$. Il existe un unique couple $(q,r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

$$a = bq + r \qquad \text{et} \qquad 0 \leqslant r \leqslant b-1 \quad \text{(ce qu'on peut aussi écrire : } 0 \leqslant r < b\text{)}.$$

Dans cet énoncé, a est appelé le *dividende*, b le *diviseur*, q le *quotient* et r le *reste*. On a : $q = \left\lfloor \frac{a}{b} \right\rfloor$ et $r \equiv a \mod b$.

Explication

- Le théorème de la division euclidienne est un résultat d'**existence** et d'**unicité** ; c'est cela qui est important.
- En termes de congruences, le théorème de la division euclidienne affirme simplement que tout entier relatif a est congru modulo b à un entier unique entier r **compris entre** 0 **et** $b-1$. Par exemple, on peut ramener l'entier $a = 12839$ à l'un des entiers 0, 1, 2, 3 ou 4 modulo $b = 5$; précisément : $\underbrace{12839}_{a} = \underbrace{5}_{b} \times \underbrace{2567}_{q} + \underbrace{4}_{r}$, et donc $12839 \equiv 4 \mod 5$.

Démonstration

- **Existence du couple** (q,r) : On démontre d'abord l'existence de (q,r) dans le cas où $a \geqslant 0$. Introduisons pour cela l'ensemble $Q = \Big\{k \in \mathbb{N} / \quad a - bk \geqslant 0\Big\}$. Cet ensemble Q est une partie non vide de $\mathbb{N}$ — non vide car elle contient 0. Mais par ailleurs Q est majoré (par a). En effet, soit $k \in Q$; alors $a - bk \geqslant 0$, donc $k \leqslant bk \leqslant a$. L'ensemble Q possède donc un plus grand élément q. Alors $a - bq \geqslant 0$. Mais comme $(q+1) \notin Q$, $a - b(q+1) < 0$. Ces deux inégalités s'écrivent aussi $0 \leqslant a - bq \leqslant b-1$.
  Posons donc $r = a - bq$. Alors tout va bien : nous l'avons trouvé, notre couple (q,r).

  Etendons à présent le résultat au cas où $a < 0$. Or si $a < 0$, alors $-a \geqslant 0$ et on est ramené au cas précédent : il existe un couple $(q,r) \in \mathbb{Z} \times \mathbb{N}$ tel que $-a = bq + r$ et $0 \leqslant r \leqslant b-1$. Là encore, deux cas doivent être distingués :
  1) Si $r = 0$, posons $q' = -q$ et $r' = 0$. Alors $a = -bq - r = bq' + r'$ et $0 \leqslant r' \leqslant b-1$.
  2) Si $r \geqslant 1$, posons $q' = -q-1$ et $r' = b-r$. Alors $a = -bq - r = bq' + r'$ et $0 \leqslant r' \leqslant b-1$. Et voilà !
- **Unicité du couple** (q,r) : Donnons-nous deux couples $(q,r), (q',r') \in \mathbb{Z} \times \mathbb{N}$ tels que $a = bq + r = bq' + r'$, $0 \leqslant r \leqslant b-1$ et $0 \leqslant r' \leqslant b-1$. Alors $|r' - r| \leqslant b-1$, mais par ailleurs $b(q-q') = r' - r$.
  Supposons $q \neq q'$. Alors $|q - q'| \geqslant 1$, donc $b|q-q'| \geqslant b$. On a donc : $b \leqslant b|q-q'| = |r'-r| \leqslant b-1$, donc $b \leqslant b-1$. Contradiction. Donc $q = q'$. On en déduit aussitôt que $r = a - bq = a - bq' = r'$ comme voulu.
- Enfin, les conditions sur q et r peuvent se réécrire ainsi : $0 \leqslant a - bq < b$, puis : $\frac{a}{b} - 1 < q \leqslant \frac{a}{b}$. On retrouve ici la définition de $\left\lfloor \frac{a}{b} \right\rfloor$. ■

En pratique (Algorithme de la division euclidienne) Comment calcule-t-on de fait le couple (q,r) de la division euclidienne de a par b ? On dispose d'un algorithme pour cela, qui n'est qu'une imitation de la preuve du théorème de la division euclidienne. On l'appelle l'*algorithme de la division euclidienne*, tout simplement.

Supposons d'abord que $a \geqslant 0$. L'algorithme est présenté ci-dessous dans ce cas sous la forme d'une procédure Maple. Le bon fonctionnement de cette procédure suppose que les arguments a et b sont des entiers naturels et que b est non nul. On écrira juste après une procédure complète capable de contrôler elle-même la nature de ses arguments et de traiter le cas $a < 0$; ce n'est pas notre objectif dans un premier temps.

```
> diveuc :=proc(a,b)          # La procédure "diveuc" imite la preuve du théorème de la division euclidienne.
  local q, r ;                # Elle requiert l'utilisation de deux variables locales q et r.
  q :=0 ;                     # Sachant que l'ensemble Q contient 0 dans tous les cas, on part de q=0.
  r :=a ;                     # On conservera à chaque étape l'égalité a=bq+r. C'est pourquoi au départ r=a.
  while r >= b do             # Voici le corps de la procédure. On y augmente q de 1 en 1,
      q :=q+1 ;               # avec l'idée que la valeur finale de q sera le plus grand élément de Q.
      r :=r-b ;               # La valeur de r est choisie conformément à l'égalité a=bq+r.
  od ;                        # Tant que r=a-bq>=b, on boucle. Après la dernière boucle, 0<=r<=b-1.
  q,r ;                       # On demande à la procédure de renvoyer q et r.
  end ;
```

Puisqu'une boucle `while` a été utilisée, nous devons justifier la terminaison de l'algorithme ainsi proposé. Mais en réalité, c'est notre démonstration du théorème de la division euclidienne qui justifie cette terminaison : l'ensemble Q possède un plus grand élément.

Venons-en maintenant au cas général. Nous allons réécrire `diveuc` en prenant aussi en charge le cas $a < 0$ — toujours en imitant la démonstration du théorème de la division euclidienne — et en contrôlant au passage la nature des arguments. Je vous laisse le soin de commenter seuls la procédure qui suit.

```
> diveuc :=proc(a,b)
  local q, r ;
  if type(a,integer)=false then RETURN('Le premier argument doit être un entier relatif.') ;fi ;
  if type(b,integer)=false or b<=0 then RETURN('Le second argument doit être un entier naturel non nul.') ;fi ;
  q :=0 ;
  r :=abs(a) ;
  while r >= b do
      q :=q+1 ;
      r :=r-b ;
  od ;
  if a<0 and r=0 then q :=-q ;
  elif a<0 then
      q :=-q-1 ;
      r :=b-r ;
  fi ;
  q,r ;
  end ;
```

Décidément, tout cela paraît bien pénible. Ne peut-on pas faire les choses plus simplement ? Oui et non. Vous pratiquez sans le savoir la division euclidienne depuis le primaire. Quand on effectue la division de deux entiers en « posant la division » comme on dit, on voit facilement apparaître le quotient et le reste de la division euclidienne associée. L'algorithme que nous venons de présenter est-il donc inutile ? Bien sûr que non : en réalité, la méthode qu'on vous a apprise en primaire est possible **parce que** l'algorithme de la division euclidienne existe ; ces méthodes apparemment différentes sont identiques. On vous a présenté en primaire la méthode classique de division comme une recette à appliquer sans jamais vous la justifier. Dix ans plus tard le mal est réparé, vous savez enfin pourquoi ça marche.

```
  3 4 7 |  5
- 3 0 (0)| 6 9
    4 7
  - 4 5
      2
```

Pour plus de précision, prenons l'exemple de la division posée ci-contre. On y divise 347 par 5. Dans un premier temps, en apparence, on retranche $6 \times 5 = 30$ de 34 ; en fait, on retranche $60 \times 5 = 300$ de 347, puisque le « 6 » apparaît comme chiffre des dizaines dans le quotient. Dans un second temps, on retranche $9 \times 5 = 45$ de 47. Au total, on a retranché $(60 + 9) \times 5 = 69 \times 5 = 345$ à 347 et le reste obtenu est 2.
Où est l'algorithme de la division euclidienne dans tout ça ? Avec cet algorithme, au lieu de retrancher en deux fois 345 de 347, on aurait retrancher 5 une première fois, 5 une seconde fois, une troisième fois... jusqu'à ce que le reste soit strictement inférieur à 5. En tout, on aurait effectué 69 soustractions.

Conclusion : les deux méthodes reposent sur un même principe de soustraction. Leur seule différence, c'est que dans la méthode étudiée en primaire, on suppose connues de l'élève les tables de multiplication usuelles ; c'est grâce à elles que l'on trouve les chiffres « 6 » et « 9 » du quotient dans l'exemple précédent. Quiconque connaît ses tables de multiplication préférera utiliser la méthode des classes primaires. Pour un ordinateur en revanche, il est plus facile d'effectuer bêtement des soustractions que d'aller fouiller dans sa mémoire pour trouver des tables de multiplication.

Exemple Le reste de la division euclidienne de 2^{65362} par 7 est égal à 2.

En effet On peut s'attendre à ce que la démonstration de ce résultat soit longue, si on applique l'algorithme précédent comme un rustre. Or on peut remarquer que $2^3 \equiv 8 \equiv 1 \mod 7$. Nous avons alors l'idée de chercher la division euclidienne de 65362 par 3 : en effet, si cette division s'écrit $65362 = 3q + r$ où $r \in \{0, 1, 2\}$, alors on pourra écrire que $2^{65362} \equiv 2^{3q+r} \equiv (2^3)^q 2^r \equiv 2^r \mod 7$ et ce sera terminé.
Or l'algorithme donne : $65362 = 3 \times 21787 + 1$, et du coup $2^{65362} \equiv 2^1 \equiv 2 \mod 7$ comme voulu.
De cet exemple, retenez bien qu'au lieu d'effectuer la division euclidienne de 2^{65362} par 7, nous avons effectué la division euclidienne de 65362 par 3, ce qui est BEAUCOUP moins long.

Exemple Soient $x, y, z \in \mathbb{Z}$, $(x, y, z) \neq (0, 0, 0)$, trois entiers solutions de l'équation de Fermat $x^3 + y^3 = z^3$. Alors l'un des entiers x, y ou z est divisible par 3.

En effet Raisonnons par l'absurde en supposant que ni x ni y ni z n'est divisible par 3. Alors le reste de la division euclidienne de x par 9 est l'un des entiers 1, 2, 4, 5, 7, 8 — on peut rejeter les cas 0, 3 et 6. Etudions un à un ces différents cas :

$x \mod 9$	$x^2 \mod 9$	$x^3 \mod 9$
1	1	1
2	4	$8 \equiv -1$
4	$16 \equiv -2$	$-8 \equiv 1$
$5 \equiv -4$	$16 \equiv -2$	$8 \equiv -1$
$7 \equiv -2$	4	$-8 \equiv 1$
$8 \equiv -1$	1	-1

Il ressort de ce tableau que $x^3 \equiv \pm 1 \mod 9$. On montrerait de même que $y^3 \equiv \pm 1 \mod 9$ et que $z^3 \equiv \pm 1 \mod 9$.

Or par hypothèse $x^3 + y^3 \equiv z^3 \mod 9$. A gauche on a modulo 9 soit $1 + 1 = 2$, soit $1 - 1 = 0$, soit $-1 + 1 = 0$, soit $-1 - 1 = -2$; à droite on a ± 1. L'égalité obtenue est impossible. C'est fini.

2 Diviseurs et multiples communs

Définition (Diviseur commun, multiple commun) Soient $a, b \in \mathbb{Z}$.

- On appelle *diviseur commun de a et b* tout entier $d \in \mathbb{Z}$ qui est à la fois un diviseur de a et un diviseur de b.
- On appelle *multiple commun de a et b* tout entier $m \in \mathbb{Z}$ qui est à la fois un multiple de a et un multiple de b.

2.1 PGCD

Définition (PGCD) Soient $a, b \in \mathbb{Z}$. On appelle *plus grand commun diviseur* (PGCD) *de a et b* tout entier $d \in \mathbb{Z}$ tel que :

- d est un diviseur commun de a et b : $d|a$ et $d|b$;
- d est un multiple de tout diviseur commun de a et b : $\forall \delta \in \mathbb{Z}, \quad \big(\delta|a \text{ et } \delta|b\big) \implies \delta|d$.

Explication Dans la définition d'un PGCD, la deuxième assertion signifie que d est plus grand (pour la relation de divisibilité) que tout autre diviseur commun de a et b, et qu'en ce sens d est le plus grand des diviseurs communs de a et b, comme son nom l'indique.
Si a et b sont des entiers naturels, un PGCD de a et b n'est jamais que la borne inférieure de l'ensemble $\{a, b\}$ pour la relation d'ordre $|$ sur $\mathbb{N}$. Si tout ceci n'est pas limpide pour vous, allez refaire un tour du côté des relations d'ordre, nous avons déjà évoqué ces résultats.

Un PGCD de deux entiers existe-t-il toujours ? Si oui, est-il unique ? Nous énonçons ci-après deux théorèmes essentiels. Tous deux seront prouvés simultanément au sein d'une preuve unique.

Théorème (Existence et « unicité » du PGCD) Soient $a, b \in \mathbb{Z}$. Il existe un et un seul PGCD **positif** de a et b ; ce PGCD est noté $\mathrm{PGCD}(a, b)$ ou $a \wedge b$ et appelé **le** PGCD *de a et b*. Le seul autre PGCD de a et b est alors $-\mathrm{PGCD}(a, b)$.

Explication On dira ainsi que -3 est **un** PGCD de 6 et 9, mais, au choix, que 3 est (**un** ou) **le** PGCD de 6 et 9.

Théorème (Théorème de Bézout, première partie) Soient $a, b \in \mathbb{Z}$.
Il existe des entiers $u, v \in \mathbb{Z}$ tels que $\mathrm{PGCD}(a, b) = au + bv$. Un tel couple (u, v) est appelé **un** *couple de coefficients de Bézout de (a, b)*.

Attention ! Les entiers u et v ne sont pas du tout uniques. Par exemple, $\mathrm{PGCD}(4, 6) = 2$ et on a à la fois $\underbrace{4}_{a} \times \underbrace{(-1)}_{u} + \underbrace{6}_{b} \times \underbrace{1}_{v} = 2$ et $\underbrace{4}_{a} \times \underbrace{2}_{u} + \underbrace{6}_{b} \times \underbrace{(-1)}_{v} = 2$.

Démonstration

- Montrons d'abord que a et b possèdent au plus deux PGCD qui sont l'opposé l'un de l'autre. Soient donc d et d' deux PGCD de a et b. Alors d est un diviseur commun de a et b, donc $d|d'$ puisque d' est un PGCD de a et b ; de même d' est un diviseur de a et b, donc $d'|d$ puisque d est un PGCD de a et b. Finalement on a bien $|d| = |d'|$; c'est le résultat voulu.

- Pour l'existence du PGCD et le théorème de Bézout, commençons par mettre de côté le cas $a = b = 0$. Il est clair dans ce cas que 0 est un diviseur commun de a et b, nécessairement le plus grand puisque tout entier divise 0.

  Nous pouvons désormais supposer $a \neq 0$ ou $b \neq 0$. L'ensemble $(a\mathbb{Z} + b\mathbb{Z}) \cap \mathbb{N}^\times$ est alors une partie non vide de $\mathbb{N}$ — il contient a ou b, l'un des deux étant non nul — donc possède un plus petit élément d : d est un entier naturel non nul et s'écrit $d = au + bv$ pour certains $u, v \in \mathbb{Z}$. Nous allons montrer que d est un PGCD de a et b. Cela montrera en même temps le théorème de Bézout puisque par définition $d = au + bv$ avec $u, v \in \mathbb{Z}$.

  1) Montrons que d divise à la fois a et b. Il suffit de le prouver pour a par symétrie des rôles de a et b. La division euclidienne de a par d s'écrit $a = dq + r$ où $q, r \in \mathbb{Z}$ et $0 \leqslant r < d$. Alors $r \in (a\mathbb{Z} + b\mathbb{Z}) \cap \mathbb{N}$ car $r = a - dq = a - (au + bv)q = a(1 - uq) - bvq$. Or $r < d$ et d est le plus petit élément de $(a\mathbb{Z} + b\mathbb{Z}) \cap \mathbb{N}^\times$ donc $r = 0$. Bref, $a = dq$, i.e. d divise a.

  2) Soit $\delta \in \mathbb{Z}$ divisant à la fois a et b. Alors δ divise d puisque $d = au + bv$. ■

La preuve précédente a ceci d'inconfortable qu'elle ne nous explique pas comment calculer le PGCD de deux entiers, ni comment calculer les deux entiers u et v du théorème de Bézout. Nous présentons ci-après deux algorithmes de calcul adaptés à ces questions : l'*algorithme d'Euclide* et l'*algorithme de Bézout*.

Lemme (Idée fondamentale de l'algorithme d'Euclide) Soient $a \in \mathbb{Z}$, $b \in \mathbb{N}^\times$ et r le reste de la division euclidienne de a par b. Alors $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(b, r)$.

Démonstration Notons q l'unique entier pour lequel $a = bq + r$. Montrer que $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(b, r)$ revient à montrer que ces deux entiers positifs ou nuls se divisent l'un l'autre.

- Pour commencer, $\mathrm{PGCD}(a, b)$ divise a et b, donc aussi b et r puisque $r = a - bq$. Par définition de $\mathrm{PGCD}(b, r)$, on peut donc affirmer que $\mathrm{PGCD}(a, b)$ divise $\mathrm{PGCD}(b, r)$.
- De même, $\mathrm{PGCD}(b, r)$ divise b et r, donc aussi a et b puisque $a = bq + r$. Par définition de $\mathrm{PGCD}(a, b)$, on peut donc affirmer que $\mathrm{PGCD}(b, r)$ divise $\mathrm{PGCD}(a, b)$. ■

✎✎✎ **En pratique (Algorithme d'Euclide)**

- Soient $a, b \in \mathbb{Z}$. L'*algorithme d'Euclide* va nous permettre de calculer rapidement le PGCD de a et b. Tout d'abord, $\mathrm{PGCD}(a, b) = |a|$ si $b = 0$ et $\mathrm{PGCD}(a, b) = |b|$ si $a = 0$. Ensuite, $\mathrm{PGCD}(a, b) = \mathrm{PGCD}\big(|a|, |b|\big)$. Enfin, évidemment, $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(b, a)$. Nous pouvons donc supposer que $0 < b \leqslant a$. On définit alors les entiers naturels $r_0, r_1, r_2 \ldots$ de la façon suivante :

  1) on commence par poser $r_0 = a$ et $r_1 = b$;

  2) ensuite, k désignant un entier naturel, tant que $r_{k+1} \neq 0$, on note r_{k+2} le reste de la division euclidienne de r_k par r_{k+1} — on a dans ce cas $r_{k+2} < r_{k+1}$.

  A l'issue de cette construction, on a les inégalités : $r_0 \geqslant r_1 > r_2 > r_3 > \ldots \geqslant 0$. Comme il n'existe qu'un nombre fini d'entiers naturels entre 0 et r_0, on obtient forcément $r_N = 0$ pour un certain $N \in \mathbb{N}^\times$. Alors r_{N-1} est le **dernier reste non nul** de la suite $r_0, r_1, r_2 \ldots$ et en vertu de l'idée fondamentale de l'algorithme d'Euclide :

  $$\mathrm{PGCD}(a, b) = \mathrm{PGCD}(r_0, r_1) = \mathrm{PGCD}(r_1, r_2) = \mathrm{PGCD}(r_2, r_3) = \ldots = \mathrm{PGCD}(r_{N-1}, r_N) = \mathrm{PGCD}(r_{N-1}, 0) = r_{N-1}.$$

  Bref, le PGCD de a et b est tout simplement le **dernier reste non nul** r_{N-1} de la suite des restes successifs $r_0, r_1, r_2 \ldots$

- Appliquons l'algorithme sur un exemple simple : $\mathrm{PGCD}(1542, 58) = 2$. Il s'agit seulement d'effectuer quelques divisions euclidiennes : $\underline{1542} = 26 \times \underline{58} + \underline{34}$, $\underline{58} = 1 \times \underline{34} + \underline{24}$, $\underline{34} = 1 \times \underline{24} + \underline{10}$, $\underline{24} = 2 \times \underline{10} + \underline{4}$, $\underline{10} = 2 \times \underline{4} + \underline{2}$ et $\underline{4} = 2 \times \underline{2} + 0$. Le dernier reste non nul obtenu est 2.

- Nous présentons ci-dessous l'algorithme d'Euclide sous la forme d'une procédure Maple. La boucle `while` de cette procédure est forcément quittée au bout d'un nombre fini de passages en vertu de la démonstration précédente.

```
> euclide :=proc(a,b)                    # La procédure "euclide" de calcul du PGCD
  local r,s,t;                           # requiert l'utilisation de trois variables locales r, s et t.
  r :=max(abs(a),abs(b)) ;               # On introduit la suite (r(n)) en posant r=r(0) et s=r(1)
  s :=min(abs(a),abs(b)) ;               # La variable t n'est qu'une variable de stockage
  t :=0;                                 # utilisée dans la boucle while ci-dessous.
  while s>0 do                           # Dans la boucle, r joue le rôle de r(n) et s celui de r(n+1).
      t :=s ;                            # Tant que s>0, on garde s=r(n+1) en mémoire en l'appelant t,
      s :=op(2, [diveuc(r,s)]) ;         # on calcule le reste s=r(n+2) de la division de r=r(n) par s=r(n+1),
      r :=t ;                            # et enfin on prépare le prochain coup en posant r=t=r(n+1).
  od;                                    # Au cran suivant dans la boucle, on aura r=r(n+1) et s=r(n+2).
  r;                                     # On demande à la procédure de renvoyer r, le dernier reste non nul.
  end;                                   # Ce n'est pas s car justement, à la fin, s=0.
```

Dans cette procédure, on n'a pas eu besoin de mettre à part le cas où l'un des deux nombres a et b est nul. En effet, si l'un des nombres est nul, alors dès l'initialisation des variables on a $s = 0$; Maple franchit donc la boucle `while` sans s'y arrêter et renvoie à l'utilisateur la valeur de `r` initiale, qui est justement dans ce cas égale au PGCD cherché.

✎✎✎ **En pratique (Algorithme de Bézout)** La méthode décrite ci-après est à connaître impérativement. Nous la présenterons seulement sur un exemple : cherchons par exemple le PGCD de 525 et 3080 ainsi qu'une identité de Bézout associée. Tout commence avec les divisions euclidiennes successives de l'algorithme d'Euclide :

$$\overbrace{3080}^{r_0} = 5 \times \overbrace{525}^{r_1} + \overbrace{455}^{r_2}, \qquad \overbrace{525}^{r_1} = 1 \times \overbrace{455}^{r_2} + \overbrace{70}^{r_3}, \qquad \overbrace{455}^{r_2} = 6 \times \overbrace{70}^{r_3} + \overbrace{35}^{r_4}, \qquad \overbrace{70}^{r_3} = 2 \times \overbrace{35}^{r_4} + \overbrace{0}^{r_5}.$$

Le dernier reste non nul est 35, c'est lui le PGCD de 525 et 3080. Partons alors de l'avant-dernière division écrite sous la forme $\overbrace{35}^{r_4} = \overbrace{455}^{r_2} - 6 \times \overbrace{70}^{r_3}$. Nous allons dans cette égalité éliminer progressivement r_3 puis r_2 et aurons ainsi exprimé $r_4 = 35$ en fonction de $r_0 = 3080$ et $r_1 = 252$.

$$\begin{aligned}
\mathrm{PGCD}(525, 3080) = \overbrace{35}^{r_4} &= \overbrace{455}^{r_2} - 6 \times \overbrace{70}^{r_3} \\
&= \overbrace{455}^{r_2} - 6 \times \left(\overbrace{525}^{r_1} - 1 \times \overbrace{455}^{r_2}\right) \qquad \text{(on élimine } r_3\text{)} \\
&= -6 \times \overbrace{525}^{r_1} + 7 \times \overbrace{455}^{r_2} \\
&= -6 \times \overbrace{525}^{r_1} + 7 \times \left(\overbrace{3080}^{r_0} - 5 \times \overbrace{525}^{r_1}\right) \qquad \text{(on élimine } r_2\text{)} \\
&= 7 \times \overbrace{3080}^{r_0} - 41 \times \overbrace{525}^{r_1}. \qquad \text{La voilà, notre identité de Bézout.}
\end{aligned}$$

Théorème (Propriétés du PGCD) Soient $a, b \in \mathbb{Z}$.

(i) Pour tout $k \in \mathbb{Z}$: $\mathrm{PGCD}(ak, bk) = |k| \, \mathrm{PGCD}(a, b)$.

(ii) Pour tout diviseur commun $d \neq 0$ de a et b : $\mathrm{PGCD}\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{\mathrm{PGCD}(a,b)}{|d|}$.

Démonstration

(i) Soit $k \in \mathbb{Z}$. Nous pouvons supposer $k \neq 0$. Notons $\delta = \mathrm{PGCD}(a, b)$ et $\Delta = \mathrm{PGCD}(ak, bk)$.

On a d'une part $\delta | a$ et $\delta | b$, donc $\delta k | ak$ et $\delta k | bk$, donc par définition de Δ, $\delta k | \Delta$.

D'autre part, $k | ak$ et $k | bk$, donc par définition de Δ, $k | \Delta$, de sorte qu'il existe $n \in \mathbb{Z}$ tel que $\Delta = nk$. Ensuite $nk = \Delta | ak$ et $nk = \Delta | bk$, donc $n | a$ et $n | b$ car $k \neq 0$. Par définition de δ, cela montre que $n | \delta$, puis que $\Delta = nk | \delta k$.

Nous obtenons ainsi la double divisibilité $\delta k | \Delta$ et $\Delta | \delta k$, et donc $|\delta k| = |\Delta|$, ou encore $\Delta = \delta |k|$.

(ii) Soit $d \neq 0$ un diviseur commun de a et b. Notons $\alpha = \frac{a}{d}$ et $\beta = \frac{b}{d}$. Alors via (i) :

$$\mathrm{PGCD}(a, b) = \mathrm{PGCD}(\alpha d, \beta d) = |d| \, \mathrm{PGCD}(\alpha, \beta) = |d| \, \mathrm{PGCD}\left(\frac{a}{d}, \frac{b}{d}\right), \qquad \text{d'où le résultat.} \quad \blacksquare$$

2.2 Nombres premiers entre eux

Définition (Nombres premiers entre eux) Soient $a, b \in \mathbb{Z}$. On dit que a et b sont *premiers entre eux* si leurs seuls diviseurs communs sont 1 et -1, i.e. si leur PGCD est égal à 1.

Exemple 15 et 28 sont premiers entre eux.

✎✎✎ **En pratique**

- La remarque suivante est utile dans de très nombreux exercices. Soient $a, b \in \mathbb{Z}$ de PGCD d. Il existe $a', b' \in \mathbb{Z}$ tels que $a = da'$ et $b = db'$. Alors $\text{PGCD}(a', b') = \text{PGCD}\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{\text{PGCD}(a,b)}{|d|} = \frac{\text{PGCD}(a,b)}{\text{PGCD}(a,b)} = 1$. Bref, a' et b' sont premiers entre eux.
- Quand on veut montrer que deux entiers sont premiers entre eux, il est toujours possible d'utiliser l'algorithme de Bézout étudié précédemment. Nous verrons dans le paragraphe sur les nombres premiers une autre technique parfois inutilisable mais souvent plus pratique.

Théorème (Théorème de Bézout, deuxième partie) Soient $a, b \in \mathbb{Z}$. Les assertions suivantes sont équivalentes :

(i) a et b sont premiers entre eux.

(ii) Il existe deux entiers $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.

Démonstration

(i) $\Longrightarrow$ (ii) Conséquence immédiate du théorème de Bézout, première partie.

(ii) $\Longrightarrow$ (i) Supposons l'existence de deux entiers $u, v \in \mathbb{Z}$ tels que $au + bv = 1$. Soit alors d un diviseur commun de a et b. Alors $d|(au + bv) = 1$, donc $d = \pm 1$ et finalement a et b sont premiers entre eux comme voulu. ■

Théorème (Théorème de Gauss) Soient $a, b, c \in \mathbb{Z}$. Si $a|bc$ et si a et b sont premiers entre eux, alors $a|c$.

Démonstration Faisons l'hypothèse que $a|bc$ et que a et b sont premiers entre eux. Alors $bc = ak$ pour un certain $k \in \mathbb{Z}$ et le théorème de Bézout affirme qu'il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$. Multiplions cette identité par c : $acu + bcv = c$, puis remplaçons bc par ak : $a(cu + kv) = c$. Il est bien clair que $a|c$ comme voulu. ■

Corollaire (Divisibilité par un produit) Soient $a, b, n \in \mathbb{Z}$. Si $a|n$, si $b|n$ et si a et b sont premiers entre eux, alors $ab|n$.

✖✖✖ Attention ! Il est impératif de supposer ici a et b premiers entre eux. En effet, pour $a = b = n = 2$, a et b divisent n mais ab ne divise pas n, et ce n'est pas étonnant puisque a et b ne sont pas premiers entre eux.

Démonstration Puisque $a|n$, il existe $k \in \mathbb{Z}$ tel que $n = ak$. Comme $b|n$, on peut donc dire que $b|ak$. Or a et b sont premiers entre eux. Le théorème de Gauss a donc pour conséquence que $b|k$. Finalement $ab|ak = n$ comme voulu. ■

Corollaire (Forme irréductible d'un nombre rationnel) Soit $r \in \mathbb{Q}$. Il existe un unique couple $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $r = \frac{p}{q}$ et tel que p et q soient premiers entre eux. Cette écriture $r = \frac{p}{q}$ est appelée la *forme irréductible de* r.

Démonstration

- Commençons par l'unicité du couple (p, q). Soient donc $(p, q), (p', q') \in \mathbb{Z} \times \mathbb{N}^*$. On suppose que $r = \frac{p}{q} = \frac{p'}{q'}$ et que p et q d'une part, p' et q' d'autre part sont premiers entre eux.
  On a donc $pq' = p'q$. En particulier $q|pq'$. Or p et q sont premiers entre eux, donc via le théorème de Gauss, $q|q'$. Par symétrie, $q'|q$, et donc $|q| = |q'|$. Mais q et q' sont positifs ou nuls, donc $q = q'$. Comme par ailleurs q et q' sont non nuls, on peut diviser l'égalité $pq' = p'q$ par $q = q'$ et du coup $p = p'$ comme voulu.

- Et l'existence à présent ? Ce qu'on sait par définition de r, c'est qu'il existe deux entiers a et b, $b \neq 0$, tels que $r = \frac{a}{b}$. On peut toujours supposer que b est positif. Notant d le PGCD de a et b, nous pouvons alors écrire $a = dp$ et $b = dq$ pour deux entiers $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$. Tout va bien : nous savons que p et q sont premiers entre eux, et d'autre part $r = \frac{a}{b} = \frac{dp}{dq} = \frac{p}{q}$. ■

Exemple La fraction $\frac{4}{6}$ n'est pas irréductible car $\text{PGCD}(4,6) = 2 \neq 1$. Pour la réduire, on divise au numérateur et au dénominateur par ce PGCD. On obtient ainsi une fraction égale à la première mais irréductible : $\frac{2}{3}$.

2.3 PPCM

Définition (PPCM) Soient $a, b \in \mathbb{Z}$. On appelle *plus petit commun multiple* (PPCM) *de a et b* tout entier $m \in \mathbb{Z}$ tel que :

- m est un multiple commun de a et b : $a|m$ et $b|m$;
- m est un diviseur de tout multiple commun de a et b : $\forall \mu \in \mathbb{Z}, \quad \Big(a|\mu \text{ et } b|\mu\Big) \implies m|\mu$.

Explication Dans la définition d'un PPCM, la seconde assertion signifie que m est plus petit (pour la relation de divisibilité) que tout autre multiple commun de a et b, et qu'en ce sens m est le plus petit des multiples communs de a et b, comme son nom l'indique. Cela dit, attention : insistons sur le fait qu'un PPCM est un **plus petit** commun multiple au sens de la relation de divisibilité $|$, pas au sens de la relation $\leqslant$; sans cela, 0 serait l'unique PPCM de a et b pour tous $a, b \in \mathbb{Z}$, ce qui serait peu intéressant.
Si a et b sont des entiers naturels, un PPCM de a et b n'est jamais que la borne supérieure de l'ensemble $\Big\{a, b\Big\}$ pour la relation d'ordre $|$ sur $\mathbb{N}$. Si tout ceci n'est pas limpide pour vous, allez refaire un tour du côté des relations d'ordre, nous avons déjà évoqué ces résultats.

Un PPCM de deux entiers existe-t-il toujours ? Si oui, est-il unique ? Le théorème suivant répond à ces questions.

Théorème (Existence et « unicité » du PPCM) Soient $a, b \in \mathbb{Z}$. Il existe un et un seul PPCM **positif** de a et b ; ce PPCM est noté $\text{PPCM}(a,b)$ ou $a \vee b$ et appelé le PPCM *de a et b*. Le seul autre PPCM de a et b est alors $-\text{PPCM}(a,b)$.
On a l'égalité : $$|ab| = \text{PGCD}(a,b)\ \text{PPCM}(a,b).$$

Explication On dira ainsi que -18 est un PPCM de 6 et 9, mais, au choix, que 18 est (un ou) le PPCM de 6 et 9.

Démonstration

- L'« unicité » du PPCM se démontre comme dans le cas des PGCD.
- Si a ou b est nul, comme 0 est le seul multiple de 0, a et b possèdent un PPCM unique, à savoir 0.
- Supposons désormais que $a \neq 0$ et que $b \neq 0$ et posons $d = \text{PGCD}(a,b) \neq 0$. Nous allons montrer que $\frac{ab}{d}$ est un PPCM de a et b. Cela prouvera d'un coup d'un seul l'existence d'un PPCM de a et b et la formule $|ab| = \text{PGCD}(a,b)\ \text{PPCM}(a,b)$.
  Commençons par introduire les deux entiers $a', b' \in \mathbb{Z}$ tels que $a = da'$ et $b = db'$. Nous savons que a' et b' sont premiers entre eux. En outre $\frac{ab}{d} = ba' = ab'$.
  1) Montrons que $\frac{ab}{d}$ est un multiple commun de a et b. C'est facile : $a\Big|ab' = \frac{ab}{d}$ et $b\Big|ba' = \frac{ab}{d}$.
  2) Montrons que $\frac{ab}{d}$ est un diviseur de tout multiple commun de a et b.
  Soit alors m un multiple commun de a et b. Il existe donc $u, v \in \mathbb{Z}$ tels que $m = au = bv$. L'égalité $au = bv$ devient aussitôt $ua' = vb'$ et donc $a'|vb'$. Or a' et b' sont premiers entre eux, donc via le théorème de Gauss, $a'|v$. Bref, on peut écrire $v = a'k$ pour un certain $k \in \mathbb{Z}$.
  Concluons : $m = bv = ba'k = k\,\frac{ab}{d}$. Cela montre bien que $\frac{ab}{d}\Big|m$ comme prévu. ■

En pratique La formule « $|ab| = \text{PGCD}(a,b)\text{PPCM}(a,b)$ » permet de calculer un PPCM à partir d'un PGCD, via l'algorithme d'Euclide. Partant de a et b, on détermine $\text{PGCD}(a,b)$ à l'aide de l'algorithme d'Euclide et on en déduit $\text{PPCM}(a,b)$.

Exemple $\text{PPCM}(1542, 58) = 44718$.

En effet Nous avons déjà montré que $\text{PGCD}(1542, 58) = 2$ dans un exemple précédent. Par conséquent $\text{PPCM}(1542, 58) = \dfrac{1542 \times 58}{2} = 44718$.

Pour la démonstration du théorème suivant, vous vous inspirerez de la démonstration donnée dans le cas analogue des PGCD.

Théorème (Propriétés du PPCM) Soient $a, b \in \mathbb{Z}$.

(i) Pour tout $k \in \mathbb{Z}$: $\text{PPCM}(ak, bk) = |k|\text{PPCM}(a, b)$.

(ii) Pour tout diviseur commun $d \neq 0$ de a et b : $\text{PPCM}\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = \dfrac{\text{PPCM}(a, b)}{|d|}$.

3 Nombres premiers

Définition (Nombre premier, nombre composé) Soit $p \in \mathbb{N}$. On dit que p est *premier* si $p \neq 1$ et si les seuls diviseurs positifs de p sont 1 et p ; on dit que p est *composé* si $p \neq 1$ et si p n'est pas premier.

L'ensemble des nombres premiers est parfois noté $\mathbb{P}$.

Exemple Il n'est pas inutile de connaître la liste des premiers nombres premiers : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37... Vous remarquerez que 2 est le seul nombre premier pair.

Lemme Soient $r \in \mathbb{N}^*$, $p_1, p_2, \ldots, p_r$ des nombres premiers distincts et $\alpha_1, \alpha_2, \ldots, \alpha_r$ des entiers naturels non nuls. Alors tout diviseur premier de $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ est l'un des p_i, $i \in [\![1, r]\!]$.

Démonstration Notons $\mathcal{D}$ l'ensemble des entiers de la forme $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ — comme dans le lemme — dont au moins un diviseur premier n'est pas l'un des p_i, $i \in [\![1, r]\!]$. Nous voulons montrer que $\mathcal{D}$ est vide.
Raisonnons par l'absurde en supposant $\mathcal{D}$ non vide. Alors $\mathcal{D}$ est une partie non vide de $\mathbb{N}$ et possède donc un plus petit élément $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ dont un certain diviseur premier p n'est aucun des p_i, $i \in [\![1, r]\!]$.
Par hypothèse $p | p_1(p_1^{\alpha_1 - 1} p_2^{\alpha_2} \ldots p_r^{\alpha_r})$, et par ailleurs p et p_1, en tant que nombres premiers distincts, sont premiers entre eux, donc via le théorème de Gauss, $p | p_1^{\alpha_1 - 1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$. Or $p_1^{\alpha_1 - 1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ n'est pas un élément de $\mathcal{D}$ car $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ en est par définition le plus petit. Par conséquent, puisque $p | p_1^{\alpha_1 - 1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, p est l'un des p_i, $i \in [\![1, r]\!]$, ce qui est contradictoire et nous permet d'affirmer que $\mathcal{D} = \varnothing$. ■

Le théorème suivant est parfois appelé le *théorème fondamental de l'arithmétique*.

Théorème (Existence et unicité de la décomposition en produit de facteurs premiers)

• Soient $n \in \mathbb{N}$, $n \geqslant 2$. Il existe un unique entier $r \in \mathbb{N}^*$, une unique famille $(p_1, p_2, \ldots, p_r)$ de nombres premiers rangés dans l'ordre $p_1 < p_2 < \ldots < p_r$ et une unique famille $(\alpha_1, \alpha_2, \ldots, \alpha_r)$ d'entiers naturels non nuls tels que :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}.$$

Les entiers $p_1, p_2, \ldots, p_r$ sont tous les nombres premiers qui divisent n. Pour tout $i \in [\![1, r]\!]$, $p_i^{\alpha_i}$ est la plus grande puissance de p_i qui divise n et α_i est appelé l'*ordre de multiplicité de p_i dans n*.

Par convention, on considère que l'entier 1 possède lui aussi une et une seule décomposition de ce genre, avec $r = 0$; bref, 1 est le « produit de zéro nombre premier ».

• Ce résultat gagne parfois à être énoncé sous la forme suivante. Soit $n \in \mathbb{N}^*$. Il existe une unique famille $(\nu_p)_{p \in \mathbb{P}}$ d'entiers naturels *presque tous nuls*, i.e. dont tous les éléments sont nuls sauf un nombre fini d'entre eux, telle que :

$$n = \prod_{p \in \mathbb{P}} p^{\nu_p}.$$

Explication Dans la deuxième formulation du théorème, le produit $\prod_{p \in \mathbb{P}} p^{\nu_p}$ est fini. Rien à voir avec un produit infini puisque la famille $(\nu_p)_{p \in \mathbb{P}}$ est presque nulle.

Démonstration Le programme stipule que vous n'êtes pas obligés de savoir refaire cette démonstration. Je vous conseille néanmoins de la travailler.

- **Existence :** Par récurrence sur n.

  1) **Initialisation :** 2 est premier donc produit de nombres premiers au sens de l'énoncé ci-dessus.

  2) **Hérédité :** Soit $n \in \mathbb{N}$, $n \geqslant 3$. Faisons l'hypothèse que tout entier supérieur ou égal à 2 mais strictement inférieur à n peut est un produit de nombres premiers. Qu'en est-il de n ? Deux cas possibles : soit n est premier, soit n est composé. Si n est premier, c'est terminé, il est produit de nombres premiers. Supposons-le donc composé. Il s'écrit donc $n = ab$ où a et b sont deux diviseurs positifs de n autres que 1 et n. Notre hypothèse de récurrence indique alors que a et b sont des produits de nombres premiers. A fortiori c'est aussi le cas de n par produit.

- **Unicité :** Egalement par récurrence sur n.

  1) **Initialisation :** Introduisons une décomposition de 2 en produit de nombres premiers. Avec des notations évidentes : $2 = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$. Aussitôt $2 = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} \geqslant 2^{\alpha_1+\alpha_2+\dots+\alpha_r}$ car 2 est le plus petit nombre premier. De cette inégalité découle immédiatement que $r = 1$, $p_1 = 2$ et $\alpha_1 = 1$. Comme voulu, la décomposition de 2 en produit de nombres premiers est unique.

  2) **Hérédité :** Soit $n \in \mathbb{N}$, $n \geqslant 3$. Faisons l'hypothèse que tout entier supérieur ou égal à 2 mais strictement inférieur à n se décompose d'une unique façon en un produit de nombres premiers. Qu'en est-il de n ? Soient $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} = q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s}$ deux décompositions de n en nombres premiers — notations évidentes. Alors via le lemme établi juste avant, $q_1 = p_i$ pour un certain $i \in [\![1, r]\!]$ et $p_1 = q_j$ pour un certain $j \in [\![1, s]\!]$. Du coup $p_1 = q_j \geqslant q_1 = p_i \geqslant p_1$, et donc $p_1 = q_1$.
  Dans ces conditions, $\dfrac{n}{p_1} = p_1^{\alpha_1 - 1} p_2^{\alpha_2} \dots p_r^{\alpha_r} = q_1^{\beta_1 - 1} q_2^{\beta_2} \dots q_s^{\beta_s}$. Or $\dfrac{n}{p_1}$ possède une unique décomposition en produit de nombres premiers par hypothèse de récurrence. On en déduit que $r = s$ et que $p_i = q_i$ et $\alpha_i = \beta_i$ pour tout $i \in [\![1, r]\!]$. Ainsi nos deux décompositions sont égales, c'est l'unicité cherchée. ■

Théorème (Infinité de l'ensemble des nombres premiers) L'ensemble $\mathbb{P}$ des nombres premiers est infini.

Démonstration Raisonnons par l'absurde en supposant $\mathbb{P}$ fini. Notons dans ce cas $p_1, p_2, \dots, p_r$ la liste **complète** des nombres premiers et posons $N = p_1 p_2 \dots p_r + 1$. Alors $N \in \mathbb{N}$, $N \geqslant 2$, et donc N peut être décomposé en produit de facteurs premiers en vertu du théorème fondamental de l'arithmétique. Soit p_k un tel diviseur premier de N, où $k \in [\![1, r]\!]$. Alors $N \equiv 0 \mod p_k$. Or par définition de N, $N \equiv 1 \mod p_k$, donc finalement $1 \equiv 0 \mod p_k$ — contradiction. ■

Théorème (PGCD, PPCM et nombres premiers) Soient $a, b \in \mathbb{N}^*$. Nous savons qu'il existe deux familles uniques $(\nu_p)_{p\in\mathbb{P}}$ et $(\mu_p)_{p\in\mathbb{P}}$ telles que $a = \prod_{p\in\mathbb{P}} p^{\mu_p}$ et $b = \prod_{p\in\mathbb{P}} p^{\nu_p}$.

Alors : $\mathrm{PGCD}(a,b) = \prod_{p\in\mathbb{P}} p^{\min(\mu_p,\nu_p)}$ et $\mathrm{PPCM}(a,b) = \prod_{p\in\mathbb{P}} p^{\max(\mu_p,\nu_p)}$.

✎ ✎ ✎ **En pratique** Quand on connaît la décomposition en facteurs premiers de a et b, on peut donc déterminer $\mathrm{PGCD}(a,b)$ et $\mathrm{PPCM}(a,b)$ sans utiliser l'algorithme de Bézout. La limite de cette méthode, c'est qu'il peut être TRÈS LONG de déterminer la décomposition d'un entier en produit de nombres premiers. Pour les grands nombres, l'algorithme de Bézout est infiniment plus utilisable.

Démonstration Contentons-nous de traiter le cas des PGCD. Posons $d = \prod_{p\in\mathbb{P}} p^{\min(\mu_p,\nu_p)}$. On a :

$$\mathrm{PGCD}(a,b) = \mathrm{PGCD}\left(d \times \frac{a}{d}, d \times \frac{b}{d}\right) = |d|\ \mathrm{PGCD}\left(\frac{a}{d}, \frac{b}{d}\right) = \prod_{p\in\mathbb{P}} p^{\min(\mu_p,\nu_p)} \times \mathrm{PGCD}\left(\frac{a}{d}, \frac{b}{d}\right).$$

Il ne nous reste plus qu'à montrer que $\mathrm{PGCD}\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = 1$, i.e. que $\dfrac{a}{d}$ et $\dfrac{b}{d}$ sont premiers entre eux.

Soit δ un diviseur commun positif de $\frac{a}{d}$ et $\frac{b}{d}$. Nous devons montrer que $\delta = 1$. Raisonnons par l'absurde et supposons $\delta \neq 1$. Nous pouvons alors nous donner un diviseur premier q de δ.
Dans ces conditions, puisque $q|\delta$ et $\delta \left| \frac{a}{d} = \prod_{p \in \mathbb{P}} p^{\mu_p - \min(\mu_p, \nu_p)} \right.$, alors q est au moins à la puissance 1 dans ce produit, i.e. $\mu_q - \min(\mu_q, \nu_q) \geqslant 1$. On montre de la même façon que $\nu_q - \min(\mu_q, \nu_q) \geqslant 1$. On a donc $\mu_q \geqslant \min(\mu_q, \nu_q) + 1$ et $\nu_q \geqslant \min(\mu_q, \nu_q) + 1$, donc $\min(\mu_q, \nu_q) \geqslant \min(\mu_q, \nu_q) + 1$ — contradiction.
Conclusion : $\delta = 1$. Les entiers $\frac{a}{d}$ et $\frac{b}{d}$ sont ainsi bien premiers entre eux, ce qui achève cette preuve. ■

Exemple Le PGCD de 600 et 740 est $20 = 2^2 \times 5$ car $600 = 2^3 \times 3 \times 5^2$ et $740 = 2^2 \times 5 \times 37$.
Voyez comme c'est facile ! Il est interdit de ne pas savoir faire cela.

CHAPITRE 6 L'ANNEAU DES POLYNÔMES

Vous avez étudié depuis la seconde jusqu'à la terminale les fonctions de variable réeelle de la forme $x \mapsto a_n x^n + \ldots + a_1 x + a_0$ et appris à résoudre les équations du premier et du second degré. Il est commode pour approfondir cette étude de considérer les expressions formelles du type $a_n x^n + \ldots + a_1 x + a_0$ et de travailler directement sur elles. C'est ce point de vue qu'on adopte ici : un polynôme est défini comme la suite de ses coefficients ; cela permet notamment de développer l'analogie entre les propriétés de divisibilité dans l'anneau des polynômes et dans l'anneau $\mathbf{Z}$. Bien entendu la notation $P = (a_0, \ldots, a_n)$, même si elle présente l'avantage d'insister sur le rôle des coefficients, est impraticable et on utilisera la notation usuelle $P = a_0 + \ldots + a_n X^n$, celle de tout le monde, même des mathématiciens.

6.1 POLYNÔMES

K désignera ici un sous-corps de $\mathbf{C}$ que l'on pourra prendre égal à $\mathbf{R}$ ou $\mathbf{C}$ pour simplifier.

Définition: Un *polynôme* à coefficient dans K est une suite d'éléments de K, disons $P = (a_0, a_1, \ldots, a_n, \ldots)$ telle qu'il existe n_0 avec $\forall n \geq n_0,\ a_n = 0$. Les a_i s'appellent les *coefficients* du polynôme P.

Un polynôme du type $(a_0, 0, 0, \ldots)$ s'appelle un *polynôme constant*. Le polynôme $(0, 0, \ldots)$ s'appelle le *polynôme nul*.

Le *degré* d'un polynôme non nul $P = (a_0, a_1, \ldots, a_n, \ldots)$ est l'entier

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

si $d^o P = n$ et $a_n = 1$ le polynôme est unitaire

Il nous faut bien sûr définir l'addition et la multiplication :

Définition: Soit $P = (a_0, a_1, \ldots, a_n, \ldots)$ et $Q = (b_0, b_1, \ldots, b_n, \ldots)$ deux polynômes, alors leur somme et leur produit sont définis par : $P+Q := (a_0+b_0, a_1+b_1, \ldots, a_n+b_n, \ldots)$ et $PQ := (c_0, c_1, \ldots, c_n, \ldots)$ avec $c_n := \sum_{i=0}^{n} a_i b_{n-i}$. si $\lambda \in K$ $\lambda P = (\lambda a_0, \lambda a_1, \ldots \lambda a_n, \ldots)$

THÉORÈME: *L'ensemble des polynômes, muni de l'addition et de la multiplication est un anneau commutatif ; l'élément neutre pour l'addition est le polynôme nul, l'élément neutre pour la multiplication est le polynôme constant $1 := (1, 0, 0, \ldots)$.*

On a les relations (lorsque ni P, ni Q ni $P+Q$ ne sont nuls) :

$$\deg(P+Q) \leq \max\{\deg(P), \deg(Q)\} \quad \text{et} \quad \deg(PQ) = \deg(P) + \deg(Q)$$

Démonstration: Il est immédiat de vérifier que l'addition définit une loi de groupe. Le polynôme constant dont le premier coefficient est 1 est bien l'élément neutre car si $b_0 = 1$ et $b_i = 0$ pour $i \geq 1$ on a bien $\sum_{i=0}^{n} a_i b_{n-i} = a_n$. Vérifier l'associativité est un exercice sur la notation "Sigma" que l'on laisse au lecteur.

Démontrons maintenant les formules sur les degrés : si $\deg(P) = d$ (resp. $\deg(Q) = e$) et p_d (resp. q_e) est le dernier coefficient non nul de P (resp. de Q) on voit facilement que

$p_i + q_i = 0$ dès que $i > \max(d, e)$ d'où la première inégalité. Remarquons que si $d > e$ le dernier coefficient non nul de $P + Q$ est p_d et donc dans ce cas on a $\deg(P + Q) = \max\{\deg(P), \deg(Q)\}$ (idem si $d < e$) alors que si $d = e$ tous les coefficients de $P + Q$ d'indice strictement supérieur à d sont nuls et le coefficient d'indice d vaut $p_d + q_e$ et donc peut fort bien être nul. Si $n > d + e$ alors $\sum_{i=0}^{n} p_i q_{n-i} = 0$ car chacun des termes est nul (ou bien $i > d$ ou bien $n - i > e$) ; par ailleurs le $(d+e)$-ème coefficient de PQ est $p_d q_e \neq 0$. De ces deux remarques on tire que $\deg(PQ) = d + e$. □

Voyons maintenant comment justifier et revenir à une notation plus usuelle : introduisons le polynôme $X = (0, 1, 0, 0 \ldots)$; on voit facilement que $X^2 = X.X = (0, 0, 1, 0, \ldots)$ et plus généralement que $X^n = (0, 0, \ldots, 0, 1, 0, \ldots)$ (où le 1 est le coefficient d'indice n). On en déduit une écriture plus commode (qui est celle que l'on utilisera dans toute la suite!) :

$$(a_0, a_1, \ldots, a_n, \ldots) = a_0 1 + a_1 X + a_2 X^2 + \ldots + a_n X^n$$

Ceci justifie la
Notation : l'ensemble des polynômes à coefficients dans K se note $K[X]$. On dit que X est une *indéterminée*.

Remarque : nous distinguons donc le polynôme $a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n$ de la fonction $x \mapsto a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$.

La propriété fondamentale de l'anneau des polynômes est, tout comme pour $\mathbf{Z}$, l'existence d'une division euclidienne :

THÉORÈME: *Soit $A \in K[X]$ et $B \in K[X] \setminus \{0\}$, il existe $Q, R \in K[X]$, uniques tels que :*

$$A = BQ + R \quad \text{et} \quad R = 0 \text{ ou } deg(R) < deg(B)$$

Démonstration: (unicité) Supposons $A = BQ + R = BQ' + R'$; alors $B(Q - Q') = R' - R$. Si R' était distinct de R alors $\deg(B) \leq \deg(B(Q - Q')) = \deg(R' - R) < \deg(B)$ amènerait une contradiction donc $R = R'$ et par conséquent $Q = Q'$.

(existence) La preuve se fait par récurrence sur $n := deg(A)$. Observons que si $\deg(A) < \deg(B)$ alors $A = 0.B + A$ fournit une division euclidienne. Supposons donc démontrée l'existence de la division euclidienne pour les polynômes de degré $\leq n - 1$ et établissons son existence pour A de degré n. On peut supposer $n \geq \deg(B) = m$ sinon on est dans un cas déjà traité ; écrivons $A = a_n X^n + \ldots$ et $B = b_m X^m + \ldots$ et considérons $A_1 := A - \frac{a_n}{b_m} X^{n-m} B$; si $A_1 = 0$ la démonstration est terminée et sinon, on voit aisément que $\deg(A_1) \leq n - 1$ car le coefficient de degré n s'annule (c'est fait pour!) donc d'après l'hypothèse de récurrence on sait que $A_1 = BQ_1 + R_1$ avec $\deg(R_1) < \deg(B)$ d'où l'on tire $A = B\left(Q_1 + \frac{a_n}{b_m} X^{n-m}\right) + R_1$ ce qui achève la démonstration de l'existence. □

Exemple : La démonstration fournit d'ailleurs un algorithme pour calculer Q et R ; illustrons cela avec $A = 2X^5 + 3X^3 + X^2 - X + 5$ et $B = X^2 + X - 1$: on peut présenter les calculs comme ceux de la division euclidienne usuelle (dans $\mathbf{Z}$) :

$$
\begin{array}{rc|l}
 & 2X^5+3X^3+X^2-X+5 & X^2+X-1 \\
\cline{3-3}
\ni & 2X^5+2X^4-2X^3 & 2X^3-2X^2+7X-8 \\
 & -2X^4+5X^3+X^2-X+5 & \\
\ni & -2X^4-2X^3+2X^2 & \\
 & 7X^3-X^2-X+5 & \\
\ni & 7X^3+7X^2-7X & \\
 & -8X^2+6X+5 & \\
\ni & -8X^2-8X+8 & \\
 & 14X-3 &
\end{array}
$$

ainsi $2X^5+3X3+X^2-X+5=(X^2+X-1)(2X^3-2X^2+7X-8)+(14X-3)$.

L'existence de la division euclidienne permet de développer les propriétés de divisibilité : PGCD,PPCM, théorème de Bézout, algorithme d'Euclide, théorème de Gauss, décomposition en produit de facteurs, de manière entièrement analogue à $\mathbf{Z}$. Nous donnons donc seulement les énoncés et renvoyons au chapitre précédent pour les démonstrations en signalant seulement les endroits où le vocabulaire introduit des différences. Les polynômes inversibles sont les constantes non nulles : en effet il est clair que ces polynômes sont inversibles et réciproquement si $PQ=1$ on a $\deg(P)+\deg(Q)=0$ et on conclut que P est constant. L'analogue des nombres premiers est donné par les polynômes *irréductibles*, i.e. par les polynômes P, non constants, qui ne peuvent s'écrire $P=QR$ avec Q,R deux polynômes non constants. Les polynômes inversibles sont les constantes non nulles.

Définition: Le *plus grand diviseur commun* ou PGCD de deux polynômes A et $B\in K[X]$ est un polynôme D qui divise A et B et tel que tout polynôme divisant A et B divise nécessairement D. Le *plus petit commun multiple* est un polynôme M multiple de A et B et tel que tout polynôme multiple de A et B soit divisible par M.

THÉORÈME: *Soient A,B deux polynômes, l'un d'entre eux non nul (au moins), le PGCD de A et B existe et, si l'on impose qu'il soit unitaire, il est unique. De même le PPCM existe et l'on a* $\mathrm{PPCM}(A,B)\,\mathrm{PGCD}(A,B)=AB$.

L'algorithme (d'Euclide) suivant fournit un calcul du PGCD :

$A=BQ_1+R_1$ (division de A par B)
$B=R_1Q_2+R_2$ (division de B par R_1)
$R_1=R_2Q_3+R_3$ (division de R_1 par R_2)
.....
$R_{n-1}=R_nQ_{n+1}+R_{n+1}$ (division de R_{n-1} par R_n)
Jusqu'à ce que $R_{n+1}=0$ *et alors* $\mathrm{PGCD}(A,B)=R_n$

Démonstration: La démonstration est identique au cas arithmétique : on doit seulement observer que $\deg(R_{i+1})<\deg(R_i)$ pour s'assurer que l'algorithme converge. □

Exemple de calcul : prenons $A:=X^6+X^5+X^4+X^2+X+1$ et $B=X^5+X^4+X^3+X^2+X+1$ alors
$A=BQ_1+R_1$ (avec $Q_1=X$ et $R_1=1-X^3$)
$B=R_1Q_2+R_2$ (avec $Q_2=-X^2-X-1$ et $R_2=2X^2+2X+2$)
$R_1=R_2Q_3+R_3$ (avec $Q_3=\frac{1}{2}$ et $R_3=0$)

donc $R_2 = 2(X^2+X+1)$ est le PGCD. Si l'on impose qu'ils soient unitaires $\mathrm{PGCD}(A,B) = X^2+X+1$ et $\mathrm{PPCM}(A,B) = (X^4+1)B = X^9+X^8+X^7+X^6+2X^5+2X^4+X^4+X^3+X^2+X+1$.

THÉORÈME: *(Bézout) Soit $A, B \in K[X]$ alors il existe $U, V \in K[X]$ tels que $AU+BV = \mathrm{PGCD}(A,B)$. De plus l'algorithme d'Euclide fournit également un calcul de U et V.*

Remarque : Les polynômes U et V ne sont pas uniques (en effet $U' = U+QB$ et $V' = V-QA$ font aussi l'affaire) mais on peut imposer (si A et B non constants) que $\deg(U) \leq \deg(B)-1$ et $\deg(V) \leq \deg(A)-1$.

Démonstration: On "copie" la démonstration faite pour $\mathbf{Z}$:
Considérons l'ensemble $I := \{AP+BQ \mid P,Q \in K[X]\}$; c'est un idéal de $K[X]$: la somme de deux éléments de I est dans I et le produit par un polynôme quelconque d'un élément de est encore dans I ; l'existence de la division euclidienne entraîne, comme dans $\mathbf{Z}$, que tout idéal est engendré par un élément, c'est-à-dire que $I = DK[X] = \{DP \mid P \in K[X]\}$. Par définition de I il existe $U, V \in K[X]$ tels que $D = AU+BV$. Voyons que $D = \mathrm{PGCD}(A,B)$: tout d'abord $A \in I$ donc A est un multiple de D, idem pour B donc D divise A et B ; si maintenant C divise A et B alors C divise $D = AU+BV$ donc D est bien le PGCD. □

Exemple : reprenons le cas précédent $A := X^6+X^5+X^4+X^2+X+1$ et $B = X^5+X^4+X^3+X^2+X+1$ alors en remontant les étapes de l'algorithme d'Eclide on obtient : $R_2 = B-R_1Q_2 = B-(A-BQ_1)Q_2$ d'où $PGCD(A,B) = X^2+X+1 = (-\frac{1}{2}Q_2)A + \frac{1}{2}(1+Q_1Q_2)B$.

Définition: Un polynôme $P \in K[X]$ est dit *irréductible* s'il n'est pas constant et si les seules factorisations $P = QR$ (avec $Q, R \in K[X]$) s'obtiennent avec P ou Q constant. (*)

Remarques : i) La notion de polynôme irréductible correspond à celle de nombre premier dans $\mathbf{Z}$.

ii) Les polynômes de degré 1 sont irréductibles car $X-a = QR$ entraîne Q ou R constant pour des raisons de degré. Néanmoins il y a beaucoup d'autres polynômes irréductibles en général ; par exemple X^2+1 est irréductible dans $\mathbf{R}[X]$, X^3-X+1 est irréductible dans $\mathbf{Q}[X]$

iii) Il est indispensable de préciser le corps K car par exemple X^2+1 n'est pas irréductible dans $\mathbf{C}[X]$ et X^3-X+1 n'est pas irréductible dans $\mathbf{R}[X]$ (ils ont chacun au moins une racine).

THÉORÈME:
(i) (Euclide) Soit P irréductible dans $K[X]$ et divisant QR alors P divise Q ou R.
(ii) (Gauss) Si $\mathrm{PGCD}(P,Q) = 1$ et P divise QR alors P divise R.

Démonstration: La démonstration est entièrement analogue à celle faite dans $\mathbf{Z}$. □

THÉORÈME: Soit $P \in K[X]$ un polynôme non constant, alors il existe $a \in K^*$ et des polynômes unitaires distincts $P_1, \ldots, P_r$ et des entiers $m_1, \ldots, m_r$ tous ≥ 1 tels que :

$$P = aP_1^{m_1} \ldots P_r^{m_r}$$

De plus les P_i, les m_i et a sont uniques.

Démonstration: La démonstration est entièrement analogue à celle faite dans $\mathbf{Z}$. Il faut seulement observer que les polynômes inversibles (i.e. les P tels qu'il existe Q avec $PQ = 1$) sont les polynômes constants non nuls. □

Exemple : reprenons les polynômes A et B dont nous avons calculé le PGCD. Dans $\mathbf{Q}[X]$ on a $A = (X^2+X+1)(X^4+1)$ et $B = (X^2+X-1)(X^2-X+1)(X+1)$ alors que sur $\mathbf{R}[X]$ on a $A = (X^2+X+1)(X^2+\sqrt{2}X+1)(X^2-\sqrt{2}+1)$ et $B = (X^2-X+1)(X^2-X+1)(X+1)$ et sur $\mathbf{C}[X]$ on a $A = (X-j)(X-\bar{j})$ et $B = (X-j)(X-\bar{j})(X+j)(X-\bar{j})(X+1)$ (où l'on note $j := -\frac{1}{2} + i\frac{\sqrt{3}}{2}$).

Remarque : on peut montrer que $K[X]$ possède une infinité de polynômes irréductibles unitaires en "copiant" la démonstration faite pour les nombres premiers.

6.2 RACINES D'UN POLYNÔME

On étudie dans ce paragraphe les premières propriétés de la fonction associée à un polynôme : si $P := a_0 + a_1X + \ldots + a_nX^n \in K[X]$ alors on peut lui associer la fonction de K dans K définie par $x \mapsto a_0 + a_1x + \ldots + a_nx^n$. En particulier on s'intéresse aux valeurs de cette fonction ; en fait il nous suffira de regarder quand la fonction s'annule, ce qui nous amène à la notion de racine d'un polynôme.

PROPOSITION: *Soit $P \in K[X]$ et soit $\alpha \in K$ alors $P(\alpha) = 0$ si et seulement si $(X - \alpha)$ divise P.*

Démonstration: *Si $P = (X-\alpha)Q$ alors visiblement $P(\alpha) = 0$. Supposons inversement que $P(\alpha) = 0$ et effectuons la division de P par $X - \alpha$. On a $P = (X-\alpha)Q + R$ avec $R = 0$ ou $\deg(R) < \deg(X-\alpha) = 1$: donc R est constant et en calculant $P(\alpha)$ on trouve que $R = P(\alpha)$ donc $R = 0$ et $X - \alpha$ divise P.* □

Définition: On dit que α est une *racine* de P si $P(\alpha) = 0$ ou si $(X - \alpha)$ divise P. On dit que α est une *racine d'ordre r* de P si $(X-\alpha)^r$ divise P mais $(X-\alpha)^{r+1}$ ne divise pas P.

THÉORÈME: *Un polynôme de degré n possède au plus n racines (comptée avec multiplicités).*

Démonstration: Supposons que $\alpha_1, \ldots, \alpha_s$ soient des éléments distincts et racines d'ordre $m_1, \ldots, m_s$ de P alors les polynômes $(X-\alpha_i)^{m_i}$ sont premiers entre eux (deux à deux) et divisent P donc leur produit divise P. Or le produit $\prod_{i=1}^{s}(X-\alpha_i)^{m_i}$ a pour degré $\sum_{i=1}^{s} m_i$ donc $\sum_{i=1}^{s} m_i \leq \deg(P) = n$. □

Par analogie avec le calcul différentiel, on peut définir la dérivée d'un polynôme et il est raisonnable de penser que l'annulation des dérivées correspond à une racine multiple. Pour démontrer cela on établit la "formule de Taylor pour les polynômes" qui servira de prototype pour la formule de Taylor générale (chapitre 14).

Définition: Soit $P = a_nX^n + a_{n-1}X^{n-1} \ldots + a_1X + a_0$ un polynôme, le *polynôme dérivé* est $P' := na_nX^{n-1} + (n-1)a_{n-1}X^{n-2} \ldots + a_1$. On note $P^{(r)}$ la *dérivée n-ème* définit par $P^{(r+1)} = (P^{(r)})'$.

Cette opération de dérivation est donc définie sans passage à la limite mais jouit des mêmes propriétés que la dérivation des fonctions :

PROPOSITION: $(P+Q)' = P' + Q'$
$(PQ)' = P'Q + PQ'$
Plus généralement on a la formule Leibniz

$$(PQ)^{(n)} = \sum_{i=0}^{n} C_n^i P^{(i)} Q^{(n-i)}$$

Les propriétés suivantes sont équivalentes :
(i) P possède un racine d'ordre r en $X = \alpha$
(ii) $P(\alpha) = P'(\alpha) = \ldots = P^{(r-1)}(\alpha) = 0$ et $P^{(r)}(\alpha) \neq 0$

Démonstration: La démonstration de la première formule est laissée en exercice. Pour la deuxième formule on se ramène facilement au cas où $P = X^m$ et $Q = X^n$; alors $PQ' + QP' = X^n(mX^{m-1}) + X^m(nX^{n-1}) = (m+n)X^{m+n-1} = (PQ)'$. Un calcul par récurrence, à partir de la formule précédente donne la formule de Leibniz (ce calcul est fait au chapitre 14 pour la dérivation usuelle).

Si P possède une racine d'ordre r en α alors $P = (X-\alpha)^r Q$ avec $X - \alpha$ ne divisant pas Q donc $Q(\alpha) \neq 0$. En appliquant la formule de Leibniz on voit que

$$P(\alpha) = P'(\alpha) = \ldots = P^{(r-1)}(\alpha) = 0$$

et $P^{(r)}(\alpha) = r!Q(\alpha) \neq 0$. Pour établir la réciproque on va se servir de la formule suivante :

PROPOSITION: *(Formule de Taylor pour les polynômes) Soit P un polynôme de degré n et $\alpha \in K$ alors*

$$P = P(\alpha) + P^{(1)}(\alpha)(X-\alpha) + \frac{P^{(2)}(\alpha)}{2!}(X-\alpha)^2 + \ldots + \frac{P^{(n)}(\alpha)}{n!}(X-\alpha)^n$$

Démonstration: (de la formule de Taylor) Tout polynôme P de degré n peut s'écrire $P = \sum_{i=0}^{n} a_i(X-\alpha)^i$ (en effet il suffit de le vérifier pour $P = X^k$ et $X^k = (X-\alpha+\alpha)^k = \sum_{i=0}^{k} C_k^i \alpha^{k-i}(X-\alpha)^i$). La dérivation étant additive il suffit de vérifier la formule de Taylor pour le polynôme $P = (X-\alpha)^k$. Mais dans ce cas $P(\alpha) = P'(\alpha) = \ldots = P^{(k-1)}(\alpha) = 0$ et $P^{(k)}(\alpha) = k!$ donc la formule est vraie.

Terminons maintenant la preuve de la proposition :
Si $P(\alpha) = P'(\alpha) = \ldots = P^{(r-1)}(\alpha) = 0$ et $P^{(r)}(\alpha) \neq 0$ alors

$$P = \sum_{i=0}^{n} \frac{P^{(i)}(\alpha)}{i!}(X-\alpha)^i = (X-\alpha)^r \left(\frac{P^{(r)}(\alpha)}{r!} + \sum_{i=r+1}^{n} \frac{P^{(i)}(\alpha)}{i!}(X-\alpha)^{i-r} \right)$$

et on a bien $P = (X-\alpha)^r Q$ avec $Q(\alpha) = \frac{P^{(r)}(\alpha)}{r!} \neq 0$. □

Remarque : Jusqu'à présent nous aurions pu supposer le corps K commutatif quelconque, par exemple $K = \mathbf{Z}/p\mathbf{Z}$ mais la formule de Taylor n'est pas valable (telle quelle) sur $\mathbf{Z}/p\mathbf{Z}$ et de "drôles de choses" peuvent arriver en dérivant les polynômes : considérons le polynôme $P = X^{3p} + X^p + 1$ alors P n'est pas constant et pourtant $P' = 0$; par ailleurs, d'après le "petit" théorème de Fermat, le polynôme $P = X^p - X$ a pour racine tous les éléments du corps $\mathbf{Z}/p\mathbf{Z}$.

Explicitons maintenant la factorisation des polynômes à coefficients dans $\mathbf{R}$ et $\mathbf{C}$

THÉORÈME: *(Factorisation dans $\mathbf{R}[X]$ et $\mathbf{C}[X]$)*

(i) Les polynômes irréductibles dans $\mathbf{C}[X]$ sont les polynômes du premier degré ; tout polynôme de degré n se factorise sous la forme :

$$P = a_n X^n + \ldots + a_0 = a_n (X - \alpha_1)^{m_1} \ldots (X - \alpha_r)^{m_r}$$

avec les α_i distincts et $m_1 + \ldots + m_r = n$.

(ii) Les polynômes irréductibles dans $\mathbf{R}[X]$ sont les polynômes du premier degré et les polynômes du second degré de la forme $P = aX^2 + bX + c$ avec $b^2 - 4ac < 0$;

Remarque : on voit ainsi que, sur $\mathbf{R}$, tout polynôme de degré n se factorise sous la forme :

$$P = a_n X^n + \ldots + a_0 = a_n (X - \alpha_1)^{m_1} \ldots (X - \alpha_r)^{m_r} (X^2 + b_1 X + c_1)^{n_1} \ldots (X^2 + b_s X + c_s)^{n_s}$$

avec les α_i réels distincts, les couples (b_i, c_i) distincts vérifiant $b_i^2 - 4c_i < 0$ et $m_1 + \ldots + m_r + 2(n_1 + \ldots + n_s) = n$.

Démonstration: (i) Il faut démontrer que les seuls polynômes unitaires irréductibles sur $\mathbf{C}$ sont les $X - \alpha$ mais ceci est clair car tout polynôme non constant possède un facteur de ce type d'après le théorème de d'Alembert-Gauss.

(ii) Il faut démontrer que les seuls polynômes unitaires irréductibles sur $\mathbf{R}$ sont les $X - \alpha$ et les $X^2 + bX + c$ (avec $b^2 - 4c < 0$). Pour cela soit P un polynôme unitaire irréductible ; il possède une racine complexe α. Si $\alpha \in \mathbf{R}$ alors $X - \alpha$ divise P et donc $P = X - \alpha$. Sinon, observons que, comme P est à coefficient réel :

$$P(\overline{\alpha}) = \bar{P}(\overline{\alpha}) = \overline{P(\alpha)} = 0$$

d'autre part $(X - \alpha)(X - \overline{\alpha}) = X^2 - 2Re(\alpha)X + |\alpha|^2$ est à coefficient réel et divise P donc $P = X^2 - 2Re(\alpha)X + |\alpha|^2$. □

Terminons ce paragraphe en étudiant, sur $\mathbf{R}$, le graphe des fonctions polynômes de degré ≤ 3 :

Si $P = aX + b$ on obtient une droite :

Si $P = aX^2 + bX + c$ on obtient une parabole qui a pour axe de symétrie la droite verticale $x = -\frac{b}{2a}$

Si $P = aX^3 + bX^2 + cX + d$ on obtient une cubique qui a toujours un point de symétrie : pour étudier le signe de la dérivée $P = 3ax^2 + 2bX + c$, on a besoin du signe de $\Delta := b^2 - 3ac$

6.3 FRACTIONS RATIONNELLES

Une fraction rationnelle F à une indéterminée est une expression du type $F = \frac{P}{Q}$ avec P et Q polynômes (Q est supposé non nul et bien sûr $\frac{PR}{QR} = \frac{P}{Q}$). L'ensemble des fractions rationnelles forme un corps qu'on peut construire formellement à partir de l'anneau des polynômes de la même façon que $\mathbf{Q}$ est construit à partir de $\mathbf{Z}$.

Définition: Un *élément simple* de $\mathbf{C}(X)$ est une fraction rationnelle de la forme :

$$F = \frac{b}{(X-a)^n}$$

avec $a, b \in \mathbf{C}$ et $n \in \mathbf{N}^*$.

Un *élément simple* de $\mathbf{R}(X)$ est une fraction rationnelle de la forme :

$$F = \frac{b}{(X-a)^n} \quad ou \quad F = \frac{cX+d}{(X^2+aX+b)^n}$$

avec $a, b, c, d \in \mathbf{R}$ et $n \in \mathbf{N}^*$ et (dans le deuxième cas $a^2 - 4b < 0$).

L'intérêt de cette notion est illustré par le théorème suivant :

THÉORÈME: *Soit $K = \mathbf{R}$ ou $\mathbf{C}$, une fraction rationnelle de $K(X)$ peut s'écrire de manière unique comme somme d'un polynôme et d'éléments simples, cette écriture s'appelle la décomposition en éléments simples de la fraction rationnelle.*

Exemples : La décomposition en éléments simples de $F = \frac{X^3+X^2-X-1}{X^2-X}$ est $F = 1 + \frac{1}{(X-1)} - \frac{1}{(X+1)} + \frac{1}{X}$

Remarque : l'unicité de cette décomposition est très utile pour la calculer comme on le verra sur les exemples. Nous allons faire la démonstration sur $\mathbf{C}$ et laissons le lecteur adapter l'argument au corps des réels ; en fait si F est une fraction à coefficient réels, on peut la décomposer en éléments simples sur $\mathbf{R}$ et sur $\mathbf{C}$.

Démonstration: (Unicité) Il suffit de voir que si :

$$F = P + \sum_{i=1}^{r} \sum_{j=1}^{m_i} \frac{b_{ij}}{(X-a_i)^j} = 0$$

alors les coefficients b_{ij} et le polynôme P sont nuls. Pour cela multiplions F par $(X-a_i)^{m_i}$; on obtient une égalité de la forme $0 = (X-a_i)^{m_i}F = b_{im_i} + (X-a_i)G$ avec G une fraction rationnelle sans pôle en a_i. En calculant les valeurs en a_i, on obtient donc $b_{im_i} = 0$. En répétant l'opération pour chaque coefficient on obtient $b_{ij} = 0$ et donc $P = 0$.

(existence) Commençons par observer que si P et Q sont des polynômes premiers entre eux alors, d'après le théorème de Bézout, il existe deux polynômes A, B tels que $AP+BQ = 1$; donc toute fraction rationnelle de la forme $F = \frac{R}{PQ}$ peut s'écrire $F = \frac{R(AP+BQ)}{PQ} = \frac{AR}{Q} + \frac{BR}{P}$. Par ailleurs tout polynôme s'écrit à un coefficient près $D = \prod_{i=1}^{r}(X-a_i)^{m_i}$ donc toute fraction rationnelle $F = \frac{C}{D}$ va se décomposer en $\sum_{i=1}^{r} \frac{P_i}{(X-a_i)^{m_i}}$ mais si on utilise maintenant la "formule de Taylor" pour P_i au point a_i on obtient $P_i = \sum_{j=0}^{\deg(P_i)} p_{ij}(X-a_i)^j$ d'où en reportant une expression de F comme somme d'éléments simples et de polynômes. □

L'utilisation la plus fréquente de la décomposition en éléments simples est le calcul de primitives (voir chapitre 17) mais elle peut être utilisée aussi pour calculer la dérivée n-ème ; par exemple si $F = \frac{X^3+X^2+X-1}{X^3-X} = 1 + \frac{1}{X-1} - \frac{1}{X+1} + \frac{1}{X}$ alors, comme on sait que $\int \frac{dt}{(t-a)} = Log|t-a| + C'$ on en tire

$$\int F(t)dt = t + \log|\frac{t^2-t}{t+1}| + C$$

En observant que $(\frac{d}{dt})^m(\frac{1}{t-a}) = (-1)^m \frac{m!}{(t-a)^{m+1}}$ on en tire :

$$F^{(m)}(t) = (-1)^m m! \left(\frac{1}{(t-1)^{m+1}} - \frac{1}{(t+1)^{m+1}} + \frac{1}{t^{m+1}} \right)$$

Pratique de la décomposition en éléments simples : On peut appliquer la méthode suivante : on factorise le dénominateur, puis on écrit formellement le type de la décomposition en éléments simples avec des coefficients inconnus, on calcule ensuite ces coefficients à l'aide des lemmes qui suivent.

La partie polynômiale de la décomposition simple s'appelle la *partie entière* de la fraction rationnelle ; elle se calcule ainsi :

LEMME: *Soit $F = P/Q$ une fraction rationnelle et soit E le quotient de la division de P par Q, i.e. $P = EQ + R$ avec $\deg(R) < \deg Q$ alors E est la partie entière de la fraction F.*

Démonstration: En effet, en réduisant au même dénominateur la somme des éléments simples, on obtient une égalité de la forme $F = E + R/Q$ avec P, R polynômes et $\deg(R) \leq \deg(Q) - 1$. Après multiplication par Q cette égalité devient $P = EQ + R$ qui indique que E est le quotient de P par Q et R le reste puisque $\deg(R) < \deg(Q)$. □

Il est également aisé de trouver le coefficient correspondant à un pôle d'ordre maximal :

LEMME: *Soit $Q = (X-a)^m Q_1$ avec $Q_1(a) \neq 0$ et $F = P/Q$ dont la décomposition s'écrit : $F = \frac{u_m}{(X-a)^m} + \ldots$ alors $u_m = P(a)/Q_1(a) = m!P(a)/Q^{(m)}(a)$.*

Démonstration: On a $(X-a)^m F = P/Q_1 = u_m + (X-a)G$ avec G fraction rationnelle sans pôle en a ; en calculant les valeurs pour $X = a$, on en déduit $u_m = P(a)/Q_1(a)$. Par ailleur la formule de Leibniz nous donne $Q^{(m)}(a) = m!Q_1(a)$ d'où la deuxième expression. □

Ces deux lemmes sont déjà suffisants pour calculer la décomposition d'une fraction rationnelle sans pôle double.

Exemple : soit $F = \frac{X^{2n}}{X^n - 1}$ on effectue la division $X^{2n} = (X^n + 1)(X^n - 1) + 1$; on sait que les racines de $X^n - 1$ sont les racines n-èmes de l'unité et on peut factoriser $X^n - 1 = \prod_{h=0}^{n-1}(X - \alpha_h)$ avec $\alpha_h := exp(\frac{2\pi i h}{n})$ d'où une expression a priori :

$$F = E + \sum_{h=0}^{n-1} \frac{u_h}{X - \alpha_h}$$

D'après le premier lemme on a $E = X^n + 1$ et si on applique le deuxième lemme avec $P = X^{2n}$ et $Q = X^n - 1$ on obtient $u_h = \frac{(\alpha_h)^{2n}}{n(\alpha_h)^{n-1}} = \alpha_h/n$ et donc

$$F = \frac{X^{2n}}{X^n - 1} = X^n + 1 + \frac{1}{n}\sum_{h=0}^{n-1} \frac{\alpha_h}{(X - \alpha_h)}$$

Pour traiter les calculs avec des pôles multiples le plus économique est d'utiliser le lemme suivant :

LEMME: *(division aux puissances croissantes) Soit $\alpha \in K$, $P, Q \in K[X]$ avec $Q(\alpha) \neq 0$ alors pour tout $k \in \mathbf{N}$ il existe $a_i \in K$ et $R \in K[X]$ tels que :*

$$P = (a_0 + a_1(X - \alpha) + \ldots + a_{k-1}(X - \alpha)^{k-1})Q + (X - \alpha)^k R$$

En particulier si $F := P/(X - \alpha)^k Q$ alors la partie de la décomposition en éléments simples de F correspondant au pôle α s'écrit :

$$\frac{a_0}{(X - \alpha)^k} + \ldots + \frac{a_{k-1}}{(X - \alpha)}$$