Algèbre et Analyse

Johannes Huisman

2 janvier 2006

Table des matières

Chapitre 1

Logique et Théorie des Ensembles

1.1 Calcul propositionnel

Les briques de base du bâtiment mathématique sont les assertions. En Logique, on peut définir très précisément ce qu'on entend par une assertion. Comme ça nous éloignerait trop de notre chemin, on se contentera d'une définition naïve : une *assertion* est une phrase qui est vraie ou qui est fausse.

Par exemple, la phrase "le nombre 6 est pair" est une assertion. Ou encore, la phrase "le nombre 141 est premier" est une assertion. Il n'est pas important de se souvenir de ce que ça signifie d'être premier, il suffit de savoir qu'un nombre est premier ou qu'il ne l'est pas, pour comprendre qu'il s'agit effectivement d'une assertion. Un exemple d'une phrase qui n'est pas une assertion est la phrase "le nombre x est impair". En effet, la vérité de cette phrase dépend de l'inconnue x dont on ne sait rien. La phrase n'est donc ni vraie ni fausse, et n'est donc pas une assertion. Par contre, la phrase " il existe un nombre x tel que x est impair" est bien une assertion. De plus, elle est vraie car le nombre 5, par exemple, est bien impair.

On peut composer des assertions simples pour en faire des assertions de plus en plus compliquées grâce aux *connecteurs logiques*. Dans un premier temps, il y a la négation, la conjonction et la disjonction. Lorsque A est une assertion, sa *négation*, notée (non A) est encore une assertion. Par exemple, la négation de l'assertion "le nombre 141 est premier" est l'assertion "(non le nombre 141 est premier)", ou en français "le nombre 141 n'est pas premier". La négation d'une assertion A est vraie si A est fausse.

Lorsque A et B sont des assertions, la *disjonction* de A et B est l'assertion (A ou B), la *conjonction* de A et B est l'assertion (A et B). La disjonction de deux assertions est vraie si au moins l'une des deux assertions

est vraie. La conjonction de deux assertions est vraie si les deux assertions sont vraies.

Concernant ces 3 connecteurs, il y a des règles du calcul logique dont les suivantes sont les plus importantes :

1. l'assertion (non(non A)) est équivalente à A,
2. l'assertion (non(A ou B)) est équivalente à ((non A) et (non B)).
3. (non(A et B)) est équivalente à ((non A) ou (non B)).
4. (A et (B ou C)) est équivalente à ((A et B) ou (A et C)).
5. (A ou (B et C)) est équivalente à ((A ou B) et (A ou C)).
6. (A ou B) est équivalente à (B ou A).
7. (A et B) est équivalente à (B et A).
8. (A ou (non A)) est vraie pour toute assertion A (la loi du tiers exclus)

Quand on dit que deux assertions sont équivalentes, comme ci-dessus, elles sont soit toutes les deux vraies, soit toutes les deux fausses. En fait, ça donne lieu a un autre connecteur logique : *l'équivalence*. Soient A et B deux assertions. La phrase "A est équivalente à B est une assertion, notée ($A \Leftrightarrow B$). Elle est vraie, par définition, si A et B sont des assertions équivalentes, i.e., ou bien A et B sont toutes les deux vraies, ou bien A et B sont toutes les deux fausses.

On aurait pu écrire les règles de calcul logique ci-dessus sous la forme ((non(non A)) $\Leftrightarrow A$) ou encore ((Aet(Bou$C$)) $\Leftrightarrow$ ((Aet$B$)ou(Aet$C$))), mais ça ne les aurait pas rendues plus comprhensibles. C'est pourquoi on vitera, dans la suite, d'crire des assertions trop formellement. On prfre les formuler en langage naturel, en s'assurant chaque fois qu'on saurait les formuler de manire prcise en utlisant des connecteurs logiques.

On introduit encore un autre connecteur logique : *l'implication*. Si A et B sont deux assertions, on a l'assertion "A implique B", notée plus brièvement $A \Rightarrow B$. L'assertion $A \Rightarrow B$ est vraie, par définition, si ((non A) ou B) est vraie. Autrement dit, $A \Rightarrow B$ est fausse si et seulement si A est vraie et B est fausse. Au lieu de "A implique B, on dira aussi "si A est vraie, alors B est vraie", ou tout simplement, "si A, alors B".

Par exemple, soit A l'assertion "il pleut" et soit B l'assertion "je porte mon K-Way". L'assertion ($A \Rightarrow B$) est vraie, car, en effet, s'il pleut, je porte mon K-Way. Mais l'assertion ((non A) $\Rightarrow B$) est également vraie, car, en fait, je mets mon K-way même s'il ne pleut pas. Une implication peut donc très bien être vraie sans qu'il y ait des liens de causalité. Ce dernier exemple illustre aussi le fait que l'implication réciproque ($B \Rightarrow A$) peut être fausse lorsque ($A \Rightarrow B$) est vraie.

Regardons encore un autre exemple. Soit A l'assertion "le prof mesure plus que 4 mètres" et soit B l'assertion "le prof est végétarien". Comme l'assertion A est évidemment fausse, l'assertion $(A \Rightarrow B)$ est vraie, même si on ne sait pas si le prof est végétarien ou pas.

Concernant l'équivalence et l'implication, on a les règles de calcul logique suivantes, entre autres :

1. $(A \Rightarrow B)$ est équivalente à $((\text{non}\, B) \Rightarrow (\text{non}\, A))$ (le principe du contraposé).
2. Si $(A \Rightarrow B)$ et $(B \Rightarrow C)$, alors $(A \Rightarrow C)$.
3. Si A et $(A \Rightarrow B)$, alors B est vraie (le principe du syllogisme ou modus ponens).
4. Si $((\text{non}\, A) \Rightarrow (B \text{ et } (\text{non}\, B)))$ est vraie, alors A est vraie (le principe de la démonstration par l'absurde).
5. $(A \Leftrightarrow B)$ est équivalente à l'assertion $((A \Rightarrow B) \text{ et } (B \Rightarrow A)$.

L'avant dernière règle permet des démonstration par l'abusrde. Supposons qu'on veut démontrer la vérité d'une assertion A. Au lieu de la démontrer directement, on démontre la vérité de $((\text{non}\, A) \Rightarrow (B \text{ et } (\text{non}\, B)))$, où B est une assertion quelconque. D'après la dernière règle logique, A sera alors vraie.

Les mathématiciens grecques comme Eculide se servaient déjà du principe de la démonstartion par l'absurde pour montrer qu'il y a une infinité de nombres premiers (voir le Théorème d'Euclide au paragraphe 3.3), ou encore pour montrer que $\sqrt{2}$ n'est pas un nombre rationnel (voir Proposition 3.3.7).

On peut vérifier des règles de calcul logique, comme toutes celles ci-dessus, en établissant des *table de vérité*. Par exemple, vérifions que $(A \Rightarrow B)$ est effectivement équivalente à $((\text{non}\, B) \Rightarrow (\text{non}\, A))$. Faisons la table de vérité de $(A \Rightarrow B)$ et $((\text{non}\, B) \Rightarrow (\text{non}\, A))$:

A	B	$A \Rightarrow B$	non A	non B	$(\text{non}\, B) \Rightarrow (\text{non}\, A)$
V	V	V	F	F	V
V	F	F	F	V	F
F	V	V	V	F	V
F	F	V	V	V	V

où, bien sûr, V signifie "vrai" et F signifie "faux". On constate que les assertions $(A \Rightarrow B)$ et $((\text{non}\, B) \Rightarrow (\text{non}\, A))$ ont la même valeur de vérité, pour chaque valeur de A et B. Elles sont donc bien équivalentes.

Ces 5 connecteurs logiques, $\text{non}, \text{ou}, \text{et}, \Rightarrow \Leftrightarrow$, permettent de construire déjà des assertions très compliqués. On verra avec les quantificateurs au paragraphe suivant encore un autre moyen de construire des assertions.

Comme toute définition naïve, la définition d'une assertion ci-dessus ne tient pas vraiement la route. En effet, elle repose sur la notion de vérité dont la définition a occupé bien des philosophes. Il faudrait donc mieux oublier la définition naïve basée sur la vérité, une fois qu'on a compris ce qu'on entend par une assertion. Il s'agit là d'une manière de faire peu orthodoxe dans un texte mathématique, mais on peut se rassurer par le fait qu'il existe, comme j'ai dit plus haut, une définition précise d'une assertion qui ne fait pas intervenir la notion de vérité. Du coup, en Mathématiques, on prend de l'avance sur les philosophes car on va pouvoir définir la notion de vérité sans tourner en rond. Ça commence par les axiomes.

On doit sélectionner—et c'est là où il y a un peu d'arbitraire—quelques assertions dont la vérité semble incontestable. On les appelle les *axiomes*. Les axiomes seront vrais par définition. Les Mathématiques de nos jours reposent sur un ensemble d'une dizaine d'axiomes dits de Zermelo et Fraenkel, augmenté de l'axiome du choix, *ZFC* en abrégé. Pour donner un exemple d'un tel axiome, on peut nommer celui qui prône l'existence d'un ensemble vide. Voilà le genre d'axiomes sur lesquels l'édifice mathématique est construit.

Une fois qu'on a arrêté les axiomes, on définit une assertion A à être *vraie* si il existe une démonstration de celle-ci. Par une *démonstration* d'une assertion A on entend une suite finie d'assertions chacune obtenue à partir de celles qui précèdent ou à partir des axiomes, en appliquant les règles de calcul logique ci-dessus. Une assertion dont arrive ainsi à démontrer la vérité est appelée théorème, corollaire, proposition ou lemme, selon l'importance de l'énoncé.

Une assertion est *fausse* si sa négation est vraie, i.e., s'il existe une démonstration de sa négation.

1.2 Quantificateurs

Soit x une inconnue et A une phrase dont la vérité dépend de x, comme, par exemple, la phrase "x est positif". Pour insister que A dépend de x, on écrit aussi $A(x)$ au lieu de A. Bien que $A(x)$ ne soit pas une assertion au sens du paragraphe précédent, on peut construire une assertion à partir de $A(x)$ grâce aux quantificateurs. Il y a, essentiellement, deux quantificateurs : le *quantificateur existentiel* $\exists$ et le *quantificateur universel* $\forall$. On obtient ainsi les assertions $(\exists x\colon A(x))$ et $(\forall x\colon A(x))$. On les prononce "il existe x tel que $A(x)$" et "pour tout x on a $A(x)$", respectivement. La première assertion est vraie, par définition, s'il existe x tel que $A(x)$ est vraie. La deuxième assertion est vraie si $A(x)$ est vraie quel que soit x. Si on veut être précis sur la nature de x, on peut encore écrire $(\exists x \in \mathbb{N}\colon A(x))$ ou $(\forall x \in \mathbb{N}\colon A(x))$ lorsque $A(x)$ est une phrase portant sur des nombres entiers naturels, par exemple. Là, on

prend un peu d'avance sur le paragraphe suivant qui portent sur la Théorie des Ensembles, où on introduira la notation $x \in \mathbb{N}$.

On a, entre autres, les règles de calcul suivantes :

1. L'assertion $(\text{non}(\exists x\colon A(x)))$ est équivalente à $(\forall x\colon (\text{non}\, A(x))$.
2. L'assertion $(\text{non}(\forall x\colon A(x)))$ est équivalente à $(\exists x\colon (\text{non}\, A(x))$.
3. $(\exists x\colon (\exists y\colon A(x,y)))$ est équivalente à $(\exists y\colon (\exists x\colon A(x,y)))$.
4. $(\forall x\colon (\forall y\colon A(x,y)))$ est équivalente à $(\forall y\colon (\forall x\colon A(x,y)))$.

Ces règles de calcul ne doivent pas surprendre. Par exemple, soit $A(x)$ la phrase "il fait beau à Brest au jour x". Le 2 ci-dessus est l'équivalence entre l'assertion "il ne fait pas beau à Brest tous les jours" et l'assertion "il y a des jours où il ne fait pas beau à Brest". Ces deux assertions ne sont pas équivalentes à l'assertion "qu'il ne fait jamais beau à Brest". Cette dernière est équivalente à l'assertion "qu'il n'y a pas de jour où il fait beau à Brest", d'après le 1.

Lorsque une assertion comporte des quantificateurs existentiels et universels, l'ordre de ceux-ci est très important. Par exemple, $(\forall x\colon (\exists y\colon A(x,y)))$ n'est pas équivalente à $(\exists y\colon (\forall x\colon A(x,y)))$, où $A(x,y)$ est une phrase dépendante des deux inconnues x et y. Pour un exemple concret, soit $A(x,y)$ la phrase "la ville y est la capitale du pays x". L'assertion $(\forall x\colon (\exists y\colon A(x,y)))$ est bien vraie ; tout pays a une capitale. Par contre, $(\exists y\colon (\forall x\colon A(x,y)))$ n'est pas vraie ; il n'existe pas de ville qui est capitale de tous les pays, en tout cas, pas encore. Donc, on ne peut changer l'ordre entre un quantificateur existentiel et un quantificateur universel. D'après les règles 3 et 4 ci-dessus, on peut changer l'ordre des quantificateurs du même type.

Parfois, on rencontre encore un troisième quantificateur, le *quantificateur d'existence unique* $\exists!$. Lorsque $A(x)$ est une phrase qui dépend de l'inconnue x, alors $(\exists!\, x\colon A(x))$ est une assertion. Elle est vraie s'il existe un et un seul x pour lequel $A(x)$ est vrai. Il faut noter que $(\exists x\colon A(x))$ est vraie s'il existe au moins un x pour lequel $A(x)$ est vraie. Les deux quantificateurs sont donc bien différents.

1.3 Ensembles

De même que pour la Logique, on ne peut éviter l'approche un peu naïve de la Théorie des Ensembles. Un *ensemble* est une collection d'objets, tels que des nombres, par exemple. On appelle ces objets les *éléments* de l'ensemble. Un ensemble est complètement déterminé par ses éléments, i.e., deux ensembles sont *égaux* s'ils ont les mêmes éléments.

Pour un ensemble E et un objet x, on dispose de l'assertion "x est un élément de E" ou encore "x appartient à E", notée $x \in E$. L'assertion $x \in E$

est vraie, par définition, si x est l'un des objets constituant l'ensemble E. Soient E et F deux ensembles. Par définition d'un ensemble, $E = F$ si et seulement si E et F ont les mêmes éléments, i.e., $(\forall x\colon x \in E \Leftrightarrow x \in F)$.

Dans le système axiomatique ZFC, on dispose des axiomes qui permettent de construire des ensembles. Supposons que $x_1, \ldots, x_n$ sont des objets. Alors, il existe un ensemble ayant précisément ces objets comme éléments. Il est noté $\{x_1, \ldots, x_n\}$. En particulier, si x est un objet, on dispose de l'ensemble $\{x\}$ qui contient un et un seul élément, à savoir x. On l'appelle *singleton* x. On dispose encore de *l'ensemble vide* n'ayant aucun élément. Il est noté $\emptyset$.

Exemples 1.3.1. 1. Singleton $\{1\}$ est un ensemble. Il est non vide car il contient 1.

2. L'ensemble $\{1, 2\}$ est égal à l'ensemble $\{2, 1\}$, car ils ont tous les deux les mêmes éléments.

3. L'ensemble $\{1, 2, 3\}$ est égal à l'ensemble $\{1, 2, 1, 3, 2\}$.

Comme illustre l'exemple 2 ci-dessus, l'ordre dans lequel on énumère les éléments d'un ensemble n'a pas d'importance. Aussi, si $E = \{x_1, \ldots, x_n\}$, on pourra supposer que les éléments $x_1, \ldots, x_n$ de E sont deux-à-deux distincts, comme illustre l'exemple 3 ci-dessus.

Définition 1.3.2. Soit E un ensemble. S'il existe un entier naturel n et des éléments $x_1, x_2, \ldots, x_n \in E$ tels que $E = \{x_1, \ldots, x_n\}$, on dit que E est un *ensemble fini*. Dans ce cas, l'entier n est le *cardinal* de E, si toutefois les éléments $x_1, \ldots, x_n$ sont deux-à-deux distincts. La cardinal de E est noté $\#E$ ou encore $|E|$. Si l'ensemble E n'est pas fini, E est un *ensemble infini*.

Exemples 1.3.3. L'ensemble vide est fini et de cardinal 0. L'ensemble singleton $\{x\}$ est fini et de cardinal 1. L'ensemble $\{x, y\}$ est fini et de cardinal 2, si $x \neq y$. L'ensemble $\mathbb{N}$ des entiers naturels est un ensemble infini.

Définition 1.3.4. Soient E et F deux ensembles. On dit que E est *inclus* dans F, noté $E \subseteq F$ lorsque tout élément de E appartient à F, i.e., lorsque $(\forall x \in E\colon x \in F)$. Dans ce cas on dit aussi que E est *contenu* dans F, ou encore, que E est une *partie* de F.

On a $E = F$ si et seulement si ($E \subseteq F$ et $F \subseteq E$). Pour montrer que deux ensembles E et F sont égaux, il sera donc pratique de montrer les deux inclusions $E \subseteq F$ et $F \subseteq E$.

Proposition 1.3.5. *Soit E un ensemble fini, et soit F un sous-ensemble de E. Alors, F est fini et $\#F \leq \#E$.*

Démonstration. Comme E est fini, $E = \{x_1, \ldots, x_n\}$ pour un certain entier naturel n. On peut supposer que les éléments $x_1, \ldots, x_n$ sont deux-à-deux distincts, de sorte que $\#E = n$. Comme F est un sous-ensemble de E, il existe des indices $i_1, \ldots, i_k \in \{1, \ldots, n\}$ tels que

$$F = \{x_{i_1}, x_{i_2}, \ldots, x_{i_k}\},$$

pour un certain entier k. En particulier, F est fini, et si on prend les indices $i_1, \ldots, i_k$ deux-à-deux distincts, $\#F = k$. Comme $i_1, \ldots, i_k$ sont des éléments de l'ensemble $\{1, \ldots, n\}$ on a $k \leq n$. □

Proposition 1.3.6. *Soient E, F, G des ensembles. Si $E \subseteq F$ et $F \subseteq G$, alors $E \subseteq G$.*

Démonstration. Pour montrer que E est contenu dans G, il faut montrer que tout élément de E appartient à G. Soit donc x un élément de E quelconque. On doit montrer que x appartient à G. Or, comme E est inclus dans F et $x \in E$, on a $x \in F$. De même, comme $F \subseteq G$ et $x \in F$, on a que x appartient à G. □

Définition 1.3.7. Soient E et F des ensembles. *L'intersection* de E et F est l'ensemble des éléments appartenant à E et à F. L'intersection de E et F est notée $E \cap F$. La *réunion* de E et F est l'ensemble des éléments appartenant à E ou à F. La réunion de E et F est notée $E \cup F$. On dit que E et F sont des *ensembles disjoints* lorsque $E \cap F = \emptyset$. La *différence* de E et F est l'ensemble des éléments de E qui n'appartiennent pas à F. La différence de E et F est notée $E \setminus F$. Lorsque $F \subseteq E$, la différence $E \setminus F$ est appelée le *complémentaire* de F dans E, et est noté E^c.

Proposition 1.3.8. *Soient E, F et G des ensembles. On a les règles de calculs suivantes.*

1. $E \cap (F \cap G) = (E \cap F) \cap G$ *(l'associativité de $\cap$),*
2. $E \cap F = F \cap E$ *(la commutativité de $\cap$),*
3. $E \cup (F \cup G) = (E \cup F) \cup G$ *(l'associativité de $\cup$),*
4. $E \cup F = F \cup E$ *(la commutativité de $\cup$),*
5. $E \cap (F \cup G) = (E \cap F) \cup (E \cap G)$ *(la distributivité de $\cap$ par rapport à $\cup$),*
6. $E \cup (F \cap G) = (E \cup F) \cap (E \cup G)$ *(la distributivité de $\cup$ par rapport à $\cap$),*
7. $(E \cap F) \setminus G = (E \setminus G) \cap (F \setminus G)$ *(la distributivité à droite de $\setminus$ par rapport à $\cap$),*

8. $(E \cup F) \setminus G = (E \setminus G) \cup (F \setminus G)$ *(la distributivité à droite de* $\setminus$ *par rapport à* $\cup$*),*
9. $E \setminus (F \cap G) = (E \setminus F) \cup (E \setminus G)$*,*

Démonstration. A titre d'exemple, montrons le 5, les autres énoncés sont laissés comme exercice. On montre les deux inclusions, et d'abord l'inclusion $E \cap (F \cup G) \subseteq (E \cap F) \cup (E \cap G)$. Pour cela, soit $x \in E \cap (F \cup G)$ un élément quelconque. Comme x appartient à l'intersection de E et $F \cup G$, x appartient à la fois à E et à $F \cup G$. En particulier, x appartient à F ou à G. Donc, ou bien x appartient à E et à F, ou bien x appartient à E et à G. D'où, x appartient à $E \cap F$ ou x appartient à $E \cap G$. Il s'ensuit que x est un élément de $(E \cap F) \cup (E \cap G)$. Cela montre bien la première inclusion.

Pour montrer la deuxième inclusion, soit x un élément quelconque de $(E \cap F) \cup (E \cap G)$, i.e., x appartient à $E \cap F$, ou x appartient à $E \cap G$. Si x appartient à $E \cap F$, x appartient à E et à F et donc, a fortiori, x appartient à E et à $F \cup G$, i.e., $x \in E \cap (F \cup G)$. De même, si x appartient à $E \cap G$, x appartient à $E \cap (F \cup G)$. Dans les deux cas, on a $x \in E \cap (F \cup G)$, ce qui montre la deuxième inclusion. □

Pour se convaincre de la vérité d'une assertion qui portent sur des ensembles, ou au contraire, pour chercher un contre-exemple à une telle assertion, il est souvent utile de dessiner des *diagrammes de Venn*.

Par exemple, pour avoir une idée sur la vérité de l'assertion

$$E \cup (F \cap G) = (E \cup F) \cap (E \cup G)$$

ci-dessus, on représente les ensembles E, F et G par 3 sous-ensembles du plan, en position générale les un par rapport aux autres, et on hachure les différentes étapes dans la détermination du premier membre $E \cup (F \cap G)$ (voir Figure 1.1).

Ensuite, on fait la même chose pour le second membre $(E \cup F) \cap (E \cup G)$ (voir Figure 1.2).

Et on constate, en l'occurrence, que $E \cup (F \cap G) = (E \cup F) \cap (E \cup G)$ devrait être vraie. Ceci ne constitue pas une démonstration, mais au moins nous permet d'avoir l'impression que l'assertion devrait être vraie.

Définition 1.3.9. Soit x et y deux objets. Le *couple* x, y est l'objet noté (x, y). Deux couples (x, y) et (x', y') sont *égaux* si $x = x'$ et $y = y'$. Soient E et F deux ensembles. Le *produit cartésien* de E et F est l'ensemble des couples (x, y), où $x \in E$, et $y \in F$.

On peut définir, de même façon, les *triplets*, *quadruplets* ou *n-uplets*, pour n'importe quel entier n, et les produits cartésiens multiples qui vont avec.

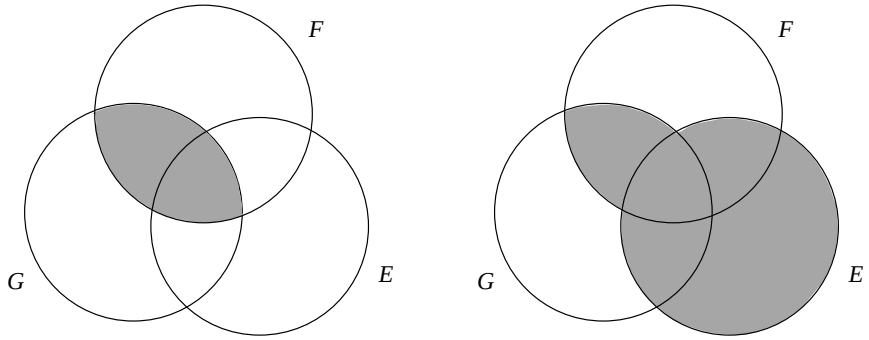

FIG. 1.1 – A gauche l'ensemble $F \cap G$, à droite l'ensemble $E \cup (F \cap G)$

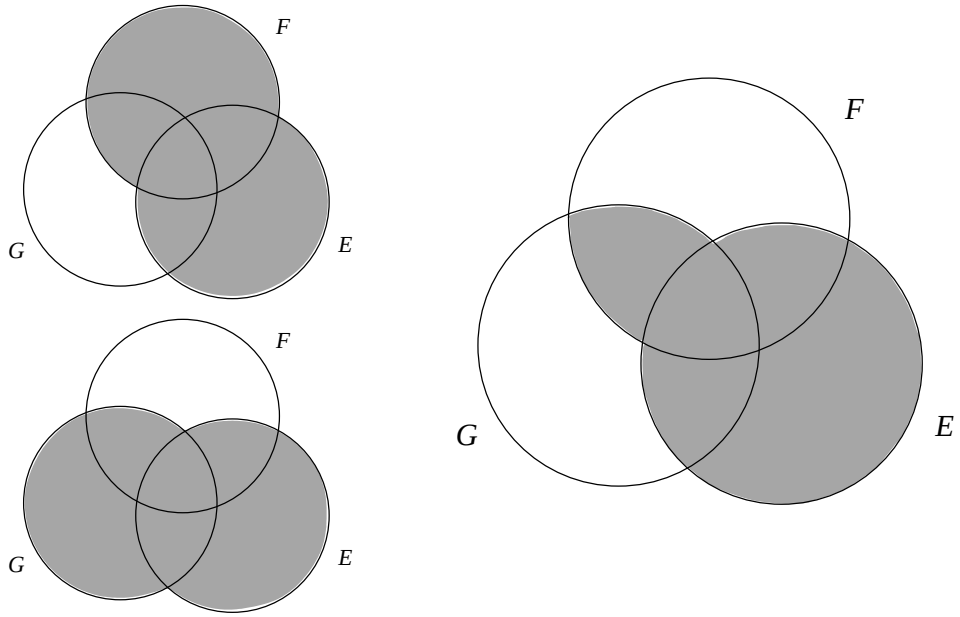

FIG. 1.2 – A gauche l'ensemble $E \cup F$ et $E \cup G$, à droite l'ensemble $(E \cup F) \cap (E \cup G)$

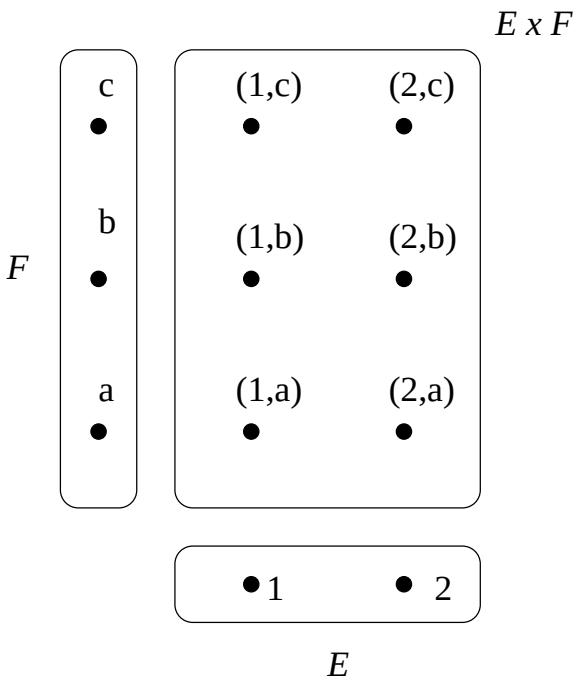

FIG. 1.3 – Il est commode de représenter le produit cartésien de deux ensembles comme un rectangle : ici le produit cartésien de $E = \{1, 2\}$ et $F = \{a, b, c\}$

Exemple 1.3.10. Soit $E = \{1, 2\}$ et $F = \{a, b, c\}$. Alors

$$E \times F = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}.$$

(voir Figure 1.3). Par exemple, $(1, c) \in E \times F$, mais $(c, 1) \notin E \times F$[1]. Il est à noter également que $E \times F$ n'est pas égal à $F \times E$.

Proposition 1.3.11. *Soient E et F des ensembles finis. Alors $E \times F$ est fini et $\#(E \times F) = \#E \times \#F$.*

Démonstration. Comme E et F sont finis, on a $E = \{x_1, \ldots, x_n\}$ et $F = \{y_1, \ldots, y_k\}$, où on suppose, comme d'habitude, que les $x_1, \ldots, x_n$ sont deux-à-deux distincts, et autant pour les $y_1, \ldots, y_k$. Comme

$$\begin{aligned} E \times F = \{&(x_1, y_1), (x_1, y_2), \ldots, (x_1, y_k), \\ &(x_2, y_1), (x_2, y_2), \ldots, (x_2, y_k), \\ &\ldots \\ &(x_n, y_1), (x_n, y_2), \ldots, (x_n, y_k)\}, \end{aligned}$$

[1] à moins que c soit égal à 1 ou 2, et 1 soit égal à a, b ou c

où les éléments énumérés sont deux-à-deux distincts, on voit que $\#(E\times F) = n \times k = \#E \times \#F$. □

Proposition 1.3.12. *Soient E, E', F et F' des ensembles. On a les règles de calculs suivantes.*

1. $(E \times F) \cap (E' \times F') = (E \cap E') \times (F \cap F')$,
2. $(E \cup E') \times (F \cup F') = (E \times F) \cup (E \times F') \cup (E' \times F) \cup (E' \times F')$,
3. $(E \times F) \setminus (E' \times F') = ((E \setminus E') \times F) \cup (E \times (F \setminus F'))$.

La démonstration est laissée en exercice.

Exemple 1.3.13. La réunion $(E\times F)\cup(E'\times F')$ n'est, en général, pas égale à $(E\cup E')\times(F\cup F')$. Contre-exemple : soit $E = F = \{1\}$ et $E' = F' = \{2\}$. On a $E\times F = \{(1,1)\}$ et $E'\times F' = \{(2,2,)\}$, de sorte que $(E\times F)\cup(E'\times F')$ est l'ensemble à 2 éléments $\{(1,1),(2,2)\}$. Par contre, $E\cup E' = F\cup F' = \{1,2\}$ et $(E\cup E')\times(F\cup F')$ est l'ensemble à 4 éléments $\{(1,1),(1,2),(2,1),(2,2)\}$.

Définition 1.3.14. Soit E un ensemble. L'ensemble $\mathcal{P}(E)$ est l'ensemble des parties de E, i.e., $F \in \mathcal{P}(E)$ si et seulement si $F \subseteq E$.

Exemple 1.3.15. Soit $E = \{1,2,3\}$. Alors,

$$\mathcal{P}(E) = \{\emptyset, \{1\}, \{2,\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$$

On voit que $\mathcal{P}(E)$ contient 8 éléments.

Proposition 1.3.16. *Soit E un ensemble fini de cardinal n. Alors $\mathcal{P}(E)$ est fini et*

$$\#\mathcal{P}(E) = 2^n.$$

La démonstration se fait par récurrence, un principe qu'on verra au paragraphe 1.6. On fera la démonstration à ce moment-là (voir.

La plupart des constructions d'ensembles à partir d'ensembles donnés comme ci-dessus sont un cas particuliers de la construction suivante.

Définition 1.3.17. Soit E un ensemble et $A(x)$ une propriété des éléments x de E. L'ensemble

$$\{x \in E \,|\, A(x) \text{ est vraie}\}$$

est le sous-ensemble de E contenant les éléments x de E qui satisfont la propriété $A(x)$.

Exemples 1.3.18. 1. Si $E = \{x_1, \ldots, x_n\}$, on a $E = \{x_i \,|\, i = 1, \ldots, n\}$.
2. $E \cap F = \{x \in E \,|\, x \in F\}$.
3. $E \setminus F = \{x \in E \,|\, x \notin F\}$.

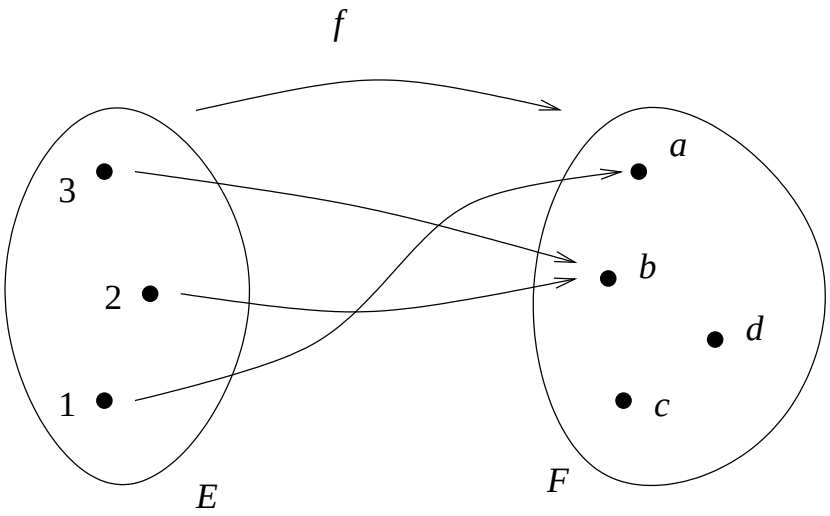

FIG. 1.4 – Il est commode de représenter une application comme ci-dessus

1.4 Applications ou fonctions

Définition 1.4.1. Soient E et F des ensembles. Une *correspondance* de E vers F est un sous-ensemble C de $E \times F$. Dans ce cas, E est *l'ensemble de départ* et F est *l'ensemble d'arrivée* de C. Si $x \in E$ et $y \in F$, on dit que x et y sont *en correspondance* relativement à C si $(x, y) \in C$.

Définition 1.4.2. Soit f une correspondance de E vers F. La correspondance f f est une *application* ou *fonction* de E vers F si pour tout $x \in E$ il existe un et un seul $y \in F$ tel que $(x, y) \in f$, plus précisément, f est une application si $\forall x \in E \exists! y \in F : (x, y) \in f$. Dans ce cas, on note $f : E \to F$. Au lieu d'écrire $(x, y) \in f$, on écrit $f(x) = y$ et on dit que y est *l'image* de x par f, et que x est un *antecédent* de y.

Exemple 1.4.3. Soient $E = \{1, 2, 3\}$ et $F = \{a, b, c, d\}$. Soit f le sous-ensemble de $E \times F$ défini par

$$f = \{(1, a), (2, b), (3, b)\}.$$

La correspondance f de E vers F est bien une application car pour tout $x \in E$ il existe un et un seul $y \in F$ tel que $(x, y) \in f$. En effet, pour $x = 1$, on a nécessairement $y = a$, pour $x = 2$, on a nécessairement $y = b$, et pour $x = 3$, on a nécessairement $y = b$. (voir Figure 1.4).

Proposition 1.4.4. *Soient $f : E \to F$ et $g : E \to F$ deux application. Alors, $f = g$ si et seulement si, pour tout $x \in E$, ona $f(x) = g(x)$.*

Démonstration. Supposons que les deux sous-ensembles f et g de $E \times F$ sont égaux. On doit montrer que $f(x) = g(x)$ pour tout $x \in E$. Soit donc x un élément quelconque de E. Soient $y = f(x)$ et $y' = g(x)$, i.e., on a $(x, y) \in f$ et $(x, y') \in g$. Comme $f = g$, on a aussi $(x, y) \in g$. Donc $(x, y) \in g$ et $(x, y') \in g$. Comme g est une application, on a $y = y'$. D'où $f(x) = g(x)$.

Réciproquement, supposons que $f(x) = g(x)$ quel que soit $x \in E$. Montrons que $f = g$. Pour a, il faut démontrer les deux inclusions. Pour montrer l'inclusion $f \subseteq g$, soit $(x, y) \in f$ un élément quelconque. Comme $y = f(x) = g(x)$, on a aussi $(x, y) \in g$. Cela montre l'inclusion $f \subseteq g$. L'autre inclusion $g \subseteq f$ se montre de la même manière. □

Définition 1.4.5. Soient $f\colon E \to F$ et $g\colon F \to G$ deux applications. On définit une correspondance de E vers G, appelée la *composée* de f et g. Elle est notée $g \circ f$ et est définie par

$$g \circ f = \{(x, z) \in E \times G \mid \exists y \in F\colon (x, y) \in f \text{ et } (y, z) \in g\}.$$

On verra ci-dessous que $g \circ f$ est une application de E dans G. On a donc

$$(g \circ f)(x) = g(f(x)),$$

pour tout $x \in E$.

Proposition 1.4.6. *Soient $f\colon E \to F$ et $g\colon F \to G$ deux applications. Alors, la correspondance $g \circ f$ est une application.*

Démonstration. Soit $x \in E$. Il faut démontrer qu'il existe un et un seul $z \in G$ tel que $(x, z) \in (g \circ f)$.

Montrons d'abord l'existence de z. Comme $x \in E$ et f est une application de E dans F, il existe $y \in F$ tel que $(x, y) \in f$. Comme $y \in F$ et g est une application de F dans G, il existe $z \in G$ tel que $(y, z) \in g$. D'après la définition de $g \circ f$, on a $(x, z) \in (g \circ f)$.

Puis, montrons l'unicité de z. Supposons qu'un élément $z' \in G$ a également la propriété que $(x, z') \in (g \circ f)$. On doit montrer que $z' = z$. Comme $(x, z') \in (g \circ f)$, il existe $y' \in F$ tel que $(x, y') \in f$ et $(y', z') \in g$. Comme f est une application de E dans F, et comme $(x, y) \in f$ et $(x, y') \in f$, on a $y = y'$. Comme g est une application de F dans G, et comme $(y, z) \in g$ et $(y, z') = (y', z') \in g$, on a $z = z'$. Cela montre bien l'unicité de z. □

Définition 1.4.7. Soit E un ensemble. L'application *identité* de E, notée id_E, est l'application de E dans E définie par $\mathrm{id}_E(x) = x$ pour tout $x \in E$.

Proposition 1.4.8. *Soit $f\colon E \to F$ une application. Alors $f \circ \mathrm{id}_E = f$ et $\mathrm{id}_F \circ f = f$.*

Démonstration. Pour démontrer que $f \circ \mathrm{id}_E = f$, il faut montrer que $(f \circ \mathrm{id}_E)(x) = f(x)$ quel que soit $x \in E$, d'après Proposition 1.4.4. Soit donc $x \in E$ un élément quelconque. On a $(f \circ \mathrm{id}_E)(x) = f(\mathrm{id}_E(x)) = f(x)$ car $\mathrm{id}_E(x) = x$. Comme x est quelconque dans E, on a bien $f \circ \mathrm{id}_E = f$.

On montre de la même manière que $\mathrm{id}_F \circ f = f$. □

L'énoncé suivant nous dit que la composition d'applications est associative. Sa démonstration est laissée comme exercice.

Proposition 1.4.9. *Soient $f\colon E \to F$, $g\colon F \to G$ et $h\colon G \to H$ des applications. Alors $(f \circ g) \circ h = f \circ (g \circ h)$.*

Définition 1.4.10. Soit $f\colon E \to F$ une application. Soit A un sous-ensemble de E. *L'image directe* de A par f est le sous-ensemble $f(A)$ de F défini par $f(A) = \{y \in F | \exists x \in A\colon f(x) = y\}$. *L'image* de f est le sous-ensemble $f(E)$.

Soit B un sous-ensemble de F. *L'image réciproque* de B est le sous-ensemble $f^{-1}(B)$ de E défini par $f^{-1}(B) = \{x \in E | f(x) \in B\}$. Lorsque $y \in F$, l'image réciproque $f^{-1}(\{y\})$ du sous-ensemble $\{y\}$ de B est notée $f^{-1}(y)$. On a

$$f^{-1}(y) = \{x \in E \mid f(x) = y\},$$

i.e., le sous-ensemble $f^{-1}(y)$ de E est l'ensemble des antécédents de y.

Exemple 1.4.11. Soit $f\colon E \to F$ l'application de l'Exemple 1.4.3. L'image directe du sous-ensemble $\{1, 2\}$ de E par f est le sous-ensemble $\{a, b\}$ de F. L'image directe de $\{2, 3\}$ est $\{b\}$. L'image de f est $\{a, b\}$ L'image réciproque du sous-ensemble $\{b, c, d\}$ de F est $\{2, 3\}$. L'image réciproque de $\{c, d\}$ est le sous-ensmble vide de E. Le sous-ensemble $f^{-1}(b)$ de E est égal à $\{2, 3\}$.

Proposition 1.4.12. *Soit $f\colon E \to F$ une application et soient $A, A' \subseteq E$ et $B, B' \subseteq F$. Alors*

1. *$A \subseteq f^{-1}(f(A))$,*
2. *$f(f^{-1}(B)) \subseteq B$,*
3. *$f(A \cup A') = f(A) \cup f(A')$,*
4. *$f(A \cap A') \subseteq f(A) \cap f(A')$,*
5. *$f^{-1}(B \cup B') = f^{-1}(B) \cup f^{-1}(B')$, et*
6. *$f^{-1}(B \cap B') = f^{-1}(B) \cap f^{-1}(B')$, et*

Démonstration. A titre d'exemple, on montre le 1. Les démonstrations des autres énoncés sont laissées comme exercice.

Soit $x \in A$ quelconque. Pour montrer que $x \in f^{-1}(f(A))$ il faut montrer que $f(x) \in f(A)$. Mais cette dernière assertion est claire car $x \in A$. □

Définition 1.4.13. Soit $f\colon E \to F$ une application. L'application f est *injective* si $\forall x, x' \in E\colon (f(x) = f(x') \Rightarrow x = x')$; dans ce cas on dit que f est une *injection*. L'application f est *surjective* si $\forall y \in F\colon \exists x \in E\colon f(x) = y$; dans ce cas on dit que f est une *surjection*. L'application f est *bijective* si f est injective et surjective ; dans ce cas on dit que f est une *bijection*.

L'énoncé suivant découle directement des définitions.

Proposition 1.4.14. *Soit $f\colon E \to F$ une application. L'application f est surjective si et seulement si son image est égale à F, i.e., si et seulement si $f(E) = F$.*

Proposition 1.4.15. *Soient $f\colon E \to F$ et $g\colon F \to G$ deux applications. Alors,*

1. *si f et g sont injectives, $g \circ f$ est injective,*
2. *si f et g sont surjectives, $g \circ f$ est surjective,*
3. *si f et g sont bijectives, $g \circ f$ est bijective,*

Démonstration. On démontre le 1. La démonstration du 2 est laissée en exercice. Le 3 est une conséquence des 1 et 2.

Supposons que $(g \circ f)(x) = (g \circ f)(x')$, où $x, x' \in E$. On a $g(f(x)) = g(f(x'))$. Comme g est injective, on en déduit que $f(x) = f(x')$. Comme f est injective, il vient que $x = x'$. Cela montre l'injectivité de $g \circ f$. □

On a les deux règles de simplification suivantes :

Proposition 1.4.16. *Soient $f\colon E \to F$ et $g, h\colon F \to G$ des applications. Si $g \circ f = h \circ f$ et f est surjective, alors $g = h$.*

Démonstration. Pour montrer que $g = h$, soit $y \in F$ et montrons que $g(y) = h(y)$. Comme f est surjective, il existe $x \in E$ tel que $f(x) = y$. Du coup,

$$g(y) = g(f(x)) = (g \circ f)(x) = (h \circ f)(x) = h(f(x)) = h(y).$$

D'où $g = h$. □

Proposition 1.4.17. *Soient $g, h\colon E \to F$ et $f\colon F \to G$ des applications. Si $f \circ g = f \circ h$ et f est injective, alors $g = h$.*

La démonstration est laissée en exercice.

Proposition 1.4.18. *Soit $f\colon E \to F$ une application. Alors, f est bijective si et seulement si il existe une application $g\colon F \to E$ telle que $g \circ f = \mathrm{id}_E$ et $f \circ g = \mathrm{id}_F$. Dans ce cas, g est la seule application ayant cette propriété.*

Démonstration. Supposons que f est une bijection. On montre l'existence et l'unicité de l'application g ayant les propriétés ci-dessus.

Montron d'abord l'unicité de g. Cela nous donnerait également une idée sur son existence. Supposons qu'il y des applications g et g' de F dans E qui ont les propriétés

$$g \circ f = \mathrm{id}_E,\ g' \circ f = \mathrm{id}_E,\ f \circ g = \mathrm{id}_F \text{ et } f \circ g' = \mathrm{id}_F.$$

On doit montrer que $g = g'$. Pour cela, soit $y \in F$ quelconque. Comme f est surjective, il existe $x \in E$ tel que $f(x) = y$. Du coup,

$$g(y) = g(f(x)) = (g \circ f)(x) = \mathrm{id}_E(x) = (g' \circ f)(x) = g'(f(x)) = g'(y),$$

et $g = g'$.

Pour montrer l'exsitence de g, définissons une correspondance g de F vers E par

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

Montrons que g est une application de F dans E. Soit $y \in F$. Comme f est surjcetive, il existe $x \in E$ tel que $f(x) = y$. D'où l'existence d'un élément $x \in E$ avec $(y, x) \in g$.

Montrons que x est l'unique élément de E tel que $(y, x) \in g$. Supposons que $x' \in E$ est tel que $(y, x') \in g$. Cela veut dire que $f(x'0 = y$. Comme $f(x) = y$ également, et comme f est injective, on a $x = x'$. Cela montre l'unicité de x, et donc que g est une application. Il est immédiat que $g \circ f = \mathrm{id}_E$ et que $f \circ g = \mathrm{id}_F$. Par conséquent, il existe une et une seule application $g\colon F \to E$ ayant la propriété voulue.

Réciproquement, supposons qu'il existe une application g de F dans E avec $g \circ f = \mathrm{id}_E$ et $f \circ g = \mathrm{id}_F$. Montrons que f est bijective.

Supposons que $f(x) = f(x')$, où $x, x' \in E$. Comme $g \circ f = \mathrm{id}_E$, on a

$$x = \mathrm{id}_E(x) = (g \circ f)(x) = g(f(x)) = g(f(x')) = (g \circ f)(x') = \mathrm{id}_E(x') = x'.$$

D'où l'injectivité de f. Pour en montrer la surjectivité, soit $y \in F$. Comme $f \circ g = \mathrm{id}_F$, on a

$$y = \mathrm{id}_F(y) = (f \circ g)(y) = f(g(y)).$$

Donc $y \in f(E)$. Il s'ensuit que f est surjective. □

Définition 1.4.19. Soit $f\colon E \to F$ une bijection, et soit $g\colon F \to E$ l'unique application de F dans E telle que $g \circ f = id_E$ et $f \circ g = id_F$. On appelle g *l'application réciproque* de f, ou *l'application inverse* de f, et on la note f^{-1}.

Remarque 1.4.20. Soit $f\colon E \to F$ une bijection et soit $B \subseteq F$. A priori, il y a maintenant une ambiguïté autour de la notation $f^{-1}(B)$. En effet, on a vu que $f^{-1}(B)$ est l'image réciproque de B par f. Mais, comme f^{-1} est une application de F dans E, la notation $f^{-1}(B)$ désigne également l'image directe de B par f^{-1} ! On vérifie facilement, que, heureusement, les deux sous-ensembles de E coïncident. Il n'y a donc pas d'ambiguïté.

Proposition 1.4.21. *Soit E un ensemble. L'identité id_E est une bijection et $\mathrm{id}_E^{-1} = \mathrm{id}_E$.*

Proposition 1.4.22. *Soient $f\colon E \to F$ et $g\colon F \to G$ des bijections. Alors, $g \circ f$ est une bijection et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

1.5 Relations

Définition 1.5.1. Soit E un ensemble. Une *relation* sur E est une correspondance de E vers lui-même, i.e., c'est un sous-ensemble du produit cartésien $E \times E$. Si R est une relation sur E et $(x, y) \in R$, on dit que x et y sont *en relation* relativement à R, et on note ceci par xRy.

On s'intéressera à deux types de relations : les relations d'ordre et les relations d'équivalence.

Définition 1.5.2. Soit R une relation sur un ensemble E. On dit que R est une *relation d'ordre*, ou plus précisément *relation d'ordre partiel*, lorsqu'elle vérifie

1. la réflexivité : pour tout $x \in E$, xRx,
2. l'antisymétrie : pour tous $x, y \in E$, si xRy et yRx, alors $x = y$, et
3. la transitivité : pour tous $x, y, z \in E$, si xRy et yRz, alors xRz.

Si elle satisfait, de plus,

4 la comparabilité : pour tous $x, y \in E$, xRy ou yRx,

alors R est une *relation d'ordre totale*.

Définition 1.5.3. Un *ensemble ordonné* est un couple (E, R) ou E est un ensemble et R est une relation d'ordre sur E. L'ensemble E est *totalement ordonneé* si R est une relation d'ordre total.

Au lieu de noter une relation d'ordre par une lettre comme R, on préfère souvent la noter par le symbole $\leq$. Dans ce cas $x < y$ signifie $x \leq y$ et $x \neq y$, $x \geq y$ signifie $y \leq x$, et $x > y$ signifie $x \geq y$ et $x \neq y$.

Exemples 1.5.4. 1. Soient $E = \{1, 2, 3\}$ et

$$R = \{(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)\}.$$

Alors R est une relation d'ordre totale sur E. C'est l'ordre total habituel sur E, i.e. $R = \leq$. La relation R' sur E obtenue à partir de R en rajoutant $(3, 1)$, i.e., $R' = R \cup \{(3, 1)\}$, n'est pas une relation d'ordre.

2. Soit L l'ensemble des mots français. On définit une relation R sur L par mRm' si et seulement si le mot m vient avant m' dans l'ordre lexicographique. Alors, R est une relation d'ordre totale sur L.

3. Soit P l'ensembles des pages web. Définissons une relation R sur P par xRy si et seulement si la page x contient un lien vers la page y. Alors, R n'est pas une relation d'ordre sur P.

4. Soit S un ensemble et $E = \mathcal{P}(S)$ l'ensemble des parties de S. Considérons la relation d'inclusion $\subseteq$ sur E, i.e., $P \subseteq P'$ si et seulement si P est contenu dans P', quels que soient $P, P' \in \mathcal{P}(S)$. Alors, $\subseteq$ est une relation d'ordre partiel sur E.

Définition 1.5.5. Soient $(E, \leq)$ et $(F, \leq)$ deux ensembles ordonnés. Soit $f\colon E \to F$ une application. L'application f est *croissante* si pour tous $x, x' \in E$, $x \leq x'$ implique que $f(x) \leq f(x')$. L'application f est *strictement croissante* si pour tous $x, x' \in E$, $x < x'$ implique que $f(x) < f(x')$. L'application f est *décroissante* si pour tous $x, x' \in E$, $x \leq x'$ implique $f(x) \geq x'$. L'application f est *strictement décroissante* si pour tous $x, x' \in E$, $x < x'$ implique $f(x) > f(x')$.

Définition 1.5.6. Soit R une relation sur un ensemble E. On dit que R est une *relation d'équivalence* si R vérifie

1. la réflexivité : pour tout $x \in E$, on a xRx,
2. la symétrie : pour tous $x, y \in E$, xRy implique yRx, et
3. la transitivité : pour tous $x, y, z \in E$, xRy et yRz impliquent xRz.

Si R est une relation d'équivalence et xRy, on dit que x et y sont *équivalents modulo* R.

Exemples 1.5.7. 1. Soit E un ensemble et R la relation d'égalité sur E, i.e. xRy si et seulement si $x = y$. Alors R est une relation d'équivalence sur E.

2. Soit E l'ensemble des étudiants. On définit une relation R sur E par xRy si et seulement si x et y font les mêmes études. Alors, R est une relation d'équivalence sur E.

3. Soit E l'ensemble des animaux. On définit une relation R sur E par xRy si et seulement si x et y sont de la même espèce. La relation R est-elle

une relation d'équivalence ? La réponse peut surprendre : elle n'est pas une relation d'équivalence. Il se trouve que le goéland argenté et le goéland brun qu'on rencontre dans nos régions sont des animaux d'espèce différente. Mais, en faisant le tour du monde vers l'ouest, le goéland argenté devient le goéland d'Amérique, qui sont tous les deux de la même espèce. En continuant vers l'ouest, le goéland d'Amérique devient le goéland de Vega, qui sont encore tous les deux de la même espèce. Puis, le goéland de Vega devient le goéland de Birula, de nouveau tous les deux de la même espèce. Ensuite, le goéland de Birula devient le goéland de Sibérie, tous les deux de la même espèce. Et enfin, ce goéland de Sibérie est de la même espèce que le goéland brun ! Pourtant, le goéland argenté et le goéland brun sont des espèces différentes ! La relation R n'est pas transitive.

4. Soit R la relation sur l'ensemble $\mathbb{Z}$ des entiers relatifs définie par mRn si et seulement si m et n ont le même reste dans la division euclidienne par 12. Pour le dire différemment, mRn si et seulement si 12 divise $m-n$. (Rappelons que 12 divise un entier relatif ℓ si et seulement s'il existe $k \in \mathbb{Z}$ tel que $12k = \ell$.) Montrons que R est une relation d'équivalence sur $\mathbb{Z}$.

En effet, R est réflexive car $m-m=0$ est divisible par 12 pour tout $m \in \mathbb{Z}$. Pour montrer que R est symétrique, supposons que mRn, c-à-d que $m-n$ est divisble par 12, où $m, n \in \mathbb{Z}$. Il existe don $k \in \mathbb{Z}$ tel que $12k = m-n$. D'où $n-m = 12(-k)$. Comme $-k \in \mathbb{Z}$, 12 divise $n-m$. Par conséquent nRm. Pour montrer la transitivité de R, on suppose que mRn et nRp, où $m, n, p \in \mathbb{Z}$. Cela veut dire qu'il existe $k, \ell \in \mathbb{Z}$ tels que $12k = m-n$ et $12\ell = n-p$. D'où $m-p = (m-n)+(n-p) = 12k+12\ell = 12(k+\ell)$. Comme $k+\ell \in \mathbb{Z}$, 12 divise $m-p$, i.e., mRp. Cela montre que R est une relation d'équivalence sur $\mathbb{Z}$, elle s'appelle la *relation de congruence modulo* 12.

On utilise la relation de congruence modulo 12 tout les jours dans le calcul avec les heures. Quand il est 15h, il est aussi 3h, car 15 et 3 sont équivalents modulo 12

5. Plus généralement, si on se fixe un entier relatif n, on a la *relation de congruence modulo* n sur $\mathbb{Z}$ qui est la relation d'équivalence sur $\mathbb{Z}$ définie par aRb si et seulement si n divise $a-b$. Si a et b sont congrus modulo n, on écrit $a \equiv b \mod n$.

Définition 1.5.8. Soit R une relation d'équivalence sur un en ensemble E. Soit $x \in E$. La *classe d'équivalence* de x, notée $\overline{x}$, est le sous-ensemble de E des éléments équivalents à x, i.e.,

$$\overline{x} = \{y \in E | xRy\}.$$

Exemple 1.5.9. Soit R la relation de congruence modulo 12 sur $\mathbb{Z}$. La classe

d'équivalence de 0 est le sous-ensemble

$$\overline{0} = \{0, 12, 24, 36, \ldots, -12, -24, -36, \ldots\}$$

de $\mathbb{Z}$. La classe de 1 modulo 12 est

$$\overline{1} = \{1, 13, 25, 37, \ldots, -11, -23, -35, \ldots\}.$$

Proposition 1.5.10. *Soit R une relation d'équivalence sur un ensemble E. Alors, E est la réunion disjointe de ses classes d'équivalence, i.e.,*

1. *pour tout $x, y \in E$ on a soit $\overline{x} = \overline{y}$, soit $\overline{x} \cap \overline{y} = \emptyset$, et*
2. *pour tout $x \in E$, il existe $y \in E$ tel que $x \in \overline{y}$.*

Démonstration. 1. Soient $x, y \in E$ et montrons que soit $\overline{x} = \overline{y}$, soit $\overline{x} \cap \overline{y} = \emptyset$. Pour cela supposons que $\overline{x} \cap \overline{y} \neq \emptyset$. Montrons que $\overline{x} \subseteq \overline{y}$. On montre que $\overline{x} \subseteq \overline{y}$. L'autre inclusion se traite de la même manière.

Soit $w \in \overline{x}$, i.e., $w \in E$ avec wRx. Comme $\overline{x} \cap \overline{y} \neq \emptyset$, il existe $z \in \overline{x} \cap \overline{y}$. On a donc zRx et zRy. Comme R est symétrique, on a aussi xRz. Par transitivité, on a wRz. Puis, encore par transitivité, on a wRy, i.e., $w \in \overline{y}$. Cela montre que $\overline{x} \subseteq \overline{y}$.

2. Soit $x \in E$. Comme R est réflexive, on a xRx, i.e., $x \in \overline{x}$. En particulier, il existe $y \in E$ tel que $x \in \overline{y}$. □

Exemple 1.5.11. Des classes modulo 12 dans $\mathbb{Z}$ sont $\overline{0}, \overline{1}, \ldots, \overline{11}$. Ils sont bien 2-à-2 disjointes, et il y en a pas d'autres. Pour voir cette dernière assertion, soit $m \in \mathbb{Z}$, on montre que sa classe $\overline{m}$ est égale à une des classe de la liste ci-dessus. D'après la division euclidienne de m par 12, on peut écrire $m = 12q + r$, où q est le quotient et r et le reste de la division de m par 12, i.e. $q, r \in \mathbb{Z}$ et $0 \leq r < 12$. Du coup, $m - r = 12q$, i.e., 12 divise $m - r$. Il s'ensuit que m est équivalent à r modulo 12. Donc $m \in \overline{r}$, et $\overline{m} = \overline{r}$ d'après la proposition précédente. Par conséquent, la classe $\overline{m}$ est égaleà l'une des classes $\overline{0}, \overline{1}, \ldots, \overline{11}$. On verra au Chapitre 3 que, plus généralement, il y a exactement n classes de congruence modulo n dans $\mathbb{Z}$ (voir Proposition 3.1.14.

Définition 1.5.12. Soit R une relation d'équivalence sur E. Le *quotient* de E par R, noté par E/R, est l'ensemble des classes d'équivalence de E modulo R. L'application

$$f \colon E \longrightarrow E/R$$

définie par $f(x) = \overline{x}$ est *l'application quotient*.

Exemple 1.5.13. Soit R la relation de congruence modulo 12 sur $\mathbb{Z}$. D'après l'exemple précédent, le quotient $\mathbb{Z}/R$ est l'ensemble $\{\overline{0}, \overline{1}, \ldots, \overline{11}\}$. On le note $\mathbb{Z}/12$, ou encore $\mathbb{Z}/12\mathbb{Z}$. L'application quotient est l'application

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}/12\mathbb{Z}$$

définie par $f(m) = \overline{m}$ pour tout $m \in \mathbb{Z}$. Deux entiers relatifs m et n ont même image par f si et seulement si $m - n$ est divisible par 12.

1.6 $\mathbb{N}$ et les axiomes de Peano

En mathématiques modernes, tout est ensemble. En effet, on a vu qu'une application est un ensemble, qu'une relation d'ordre est un ensemble etc. Ce n'est donc pas très surprenant de voir que même les nombres comme les entiers naturels sont des ensembles.

Jusqu'à maintenant, on a suggéré, par le choix des mots mais aussi par l'utilisation des majuscules et minuscules, qu'il y a une dichotomie comme quoi il y a des ensembles et des objets qui sont leurs éléments. En fait, ce n'est qu'une façon de parler. Les éléments d'un ensemble sont des ensembles eux aussi ! Du coup, on se permettra dans ce paragraphe de désigner des ensembles par des lettres minuscules.

On commence par une définition générale, avant de définir les entiers naturels.

Définition 1.6.1. Soit x un ensemble. Le *successeur* de x, noté $S(x)$, est l'ensemble $x \cup \{x\}$.

Exemple 1.6.2. Le successeur de l'ensemble $\{1, 3\}$ est l'ensemble $\{1, 3\} \cup \{\{1, 3\}\} = \{1, 3, \{1, 3\}\}$. Ce dernier contient 3 éléments à savoir 1, 3 et $\{1, 3\}$.

Définition 1.6.3. On définit les dix premiers *entiers naturels :*

$$\begin{aligned}
&0 = \emptyset,\\
&1 = S(0) = 0 \cup \{0\} = \emptyset \cup \{\emptyset\} = \{\emptyset\} = \{0\},\\
&2 = S(1) = 1 \cup \{1\} = \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\} = \{0, 1\},\\
&3 = S(2) = 2 \cup \{2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \{0, 1, 2\},\\
&4 = S(3) = \{0, 1, 2, 3\}\\
&\vdots\\
&9 = S(8) = \{0, 1, 2, \ldots, 8\}
\end{aligned}$$

Axiomes de Peano. *Il existe un ensemble* $\mathbb{N}$ *qui a les propriétés suivantes.*

1. $0 \in \mathbb{N}$.
2. *Pour tout* $n \in \mathbb{N}$, *on a* $S(n) \in \mathbb{N}$.
3. *Pour tout* $m, n \in \mathbb{N}$, *si* $S(m) = S(n)$, *alors* $m = n$.
4. *Pour tout* $n \in \mathbb{N}$, *il existe* $m \in \mathbb{N}$ *avec* $S(m) = n$ *si et seulement si* $n \neq 0$, *et*
5. *Pour tout sous-ensemble* A *de* $\mathbb{N}$ *tel que* $0 \in A$ *et* $n \in A \Rightarrow S(n) \in A$, *on a* $A = \mathbb{N}$.

Les éléments de $\mathbb{N}$ *sont les* entiers naturels.

Les axiomes de Péano ci-dessus sont conséquences des axiomes de Zermelo et Fraenkel de la théorie des ensembles (voir l'appendice pour les axiomes de Zermelo et Fraenkel). Ce ne sont donc pas des axiomes, mais des *théorèmes* de Péano. Malgré cela, on persiste à les appeler axiomes pour des raisons historiques. La démonstration des axiomes de Péano à partir des axiomes de Zermelo et Fraenkel sort du programme de ce cours. On admettra donc les axiomes de Péano comme si c'était des axiomes.

La propriété 2 nous dit que l'association $n \mapsto S(n)$ est une application de $\mathbb{N}$ dans lui-même. Comme $0 \in \mathbb{N}$ d'après la 1, on a aussi $1, 2, 3, \ldots, 9 \in \mathbb{N}$, et puis $S(9), S(S(9)) \in \mathbb{N}$ etc. Evidemment, on va avoir la notation 10 pour $S(9)$, et 11 pour $S(S(9))$ etc., mais seulement une fois qu'on aura démontré l'existence et l'unicité de l'écriture d'un entier naturel en base 10. Après tout, il ne faut pas confondre un entier naturel avec son écriture décimale ! La propriété 3 ci-dessus peutêtre reformulée en disant que l'application $S \colon \mathbb{N} \to \mathbb{N}$ est injective, La propriéte 4 nous dit que 0 est le seul entier naturel qui n'est pas successeur d'un entier. En fait, $0 = \emptyset$ n'est successeur de personne ! La propriété 5 ci-dessus est appelé "axiome de récurrence" et sert surtout dans son déguisement : le principe de récurrence ci-dessous.

Dans la suite on notera $n+1$ au lieu de $S(n)$, si $n \in \mathbb{N}$. On a donc $0+1 = 1$, $1 + 1 = 2$, $2 + 1 = 3$, etc.

Théorème (le principe de récurrence). *Soit* $\mathcal{P}(n)$ *une assertion qui dépend d'un entier naturel* n. *Supposons que*

1. $\mathcal{P}(0)$ *est vraie, et que,*
2. *l'implication* $\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$ *est vraie pour tout* n.

Alors, $\mathcal{P}(n)$ *est vraie quel que soit* $n \in \mathbb{N}$.

Démonstration. Soit A le sous-ensemble de $\mathbb{N}$ contenant exactement les entiers n tels que $\mathcal{P}(n)$ est vraie. D'après les hypothèses, $0 \in A$ et $n \in A \Rightarrow (n+1) \in A$. Il s'ensuit de l'axiome 3 ci-dessus que $A = \mathbb{N}$, i.e., $\mathcal{P}(n)$ est vraie quel que soit $n \in \mathbb{N}$. □

Théorème 1.6.4. *Soit n_0 un entier naturel. Soit $\mathcal{P}(n)$ une assertion qui dépend d'un entier n avec $n \geq n_0$. Supposons que*

1. *$\mathcal{P}(n_0)$ est vraie, et que,*
2. *l'implication $\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$ est vraie pour tout $n \geq n_0$.*

Alors, $\mathcal{P}(n)$ est vraie quel que soit l'entier $n \geq n_0$. □

Théorème (le principe de récurrence généralisé). *Soit $\mathcal{P}(n)$ une assertion qui dépend d'un entier naturel n. Supposons que*

1. *$\mathcal{P}(0)$ est vraie, et que,*
2. *l'implication $(\forall k \leq n \mathcal{P}(k)) \Rightarrow \mathcal{P}(n+1)$ est vraie pour tout $n \in \mathbb{N}$.*

Alors, $\mathcal{P}(n)$ est vraie quel que soit $n \in \mathbb{N}$. □

Définition 1.6.5. Pour $m, n \in \mathbb{N}$, on définit une relation $\leq$ sur $\mathbb{N}$ par $m \leq n$ si $m \subseteq n$.

Proposition 1.6.6. *$(\mathbb{N}, \leq)$ est un ensemble totalement ordonné.*

Démonstration. Vérifions d'abord que la relation $\leq$ est une relation d'ordre sur $\mathbb{N}$. Soit $x \in \mathbb{N}$. On a bien $x \subseteq x$. D'où $x \leq x$. Cela montre que $\leq$ est réflexive.

Soient $x, y \in \mathbb{N}$ tels que $x \leq y$ et $y \leq x$, c-à-d, on a $x \subseteq y$ et $y \subseteq x$. Du coup, $x = y$. Cela montre l'antisymétrie de $\leq$.

Soient $x, y, z \in \mathbb{N}$ tels que $x \leq y$ et $y \leq z$, c-à-d, $x \subseteq y$'et $y \subseteq z$. Par transitivité de l'inclusion, on a $x \subseteq z$, i.e., $x \leq z$. Par conséquent, $\leq$ est transitive et est une relation d'ordre.

On montre que la relation d'ordre $\leq$ est totale par récurrence. En effet, montrons que pour tout $m, n \in \mathbb{N}$ on a ou bien $m \leq n$, ou bien $n \leq m$. On montre cet énoncé par une double récurrence. L'énoncé est bien vrai pour $m = 0$. Supposons que l'énoncé est vrai au rang m pour un certain $m \in \mathbb{N}$ fixé, i.e., supposons que pour tout $n \in \mathbb{N}$ on a ou bien $m \leq n$ ou bien $n \leq m$. Montrons que cet énoncé est encore vrai au rang $m+1$, i.e., montrons que pour tout $n \in \mathbb{N}$ on a ou bien $m+1 \leq n$ ou bien $n \leq m+1$. On montre ce dernier énoncé par récurrence sur n.

Pour $n = 0$, ce dernier énoncé est bien vrai car $0 \leq m+1$. Supposons que lénoncé est vrai au rang n pour un certain $n \in \mathbb{N}$, i.e., supposons qu'on a ou bien $m+1 \leq n$ ou bien $n \leq m+1$. On montre que cet énoncé est encore vrai au rang $n+1$, i.e., on montre qu'on a ou bien $m+1 \leq n+1$ ou bien $n+1 \leq m+1$. D'après l'hypothèse de récurrence sur n, on a $m+1 \leq n$ ou $n \leq m+1$. On distingue donc deux cas : le cas $m+1 \leq n$ et le cas $n \leq m+1$.

Traitons d'abord le cas $m+1 \leq n$. Comme $n \leq n+1$, on a $m+1 \leq n+1$ si $m+1 \leq n$. Donc au premier cas, on a bien $m+1 \leq n+1$ ou $n+1 \leq m+1$.

On peut donc supposer qu'on est dans le deuxième cas, i.e., que $n \leq m+1$. D'après l'hypothèse de récurrence sur m, on a ou bien $m \leq n$ ou bien $n \leq m$. Si $n \leq m$, on a forcément $n \leq m+1$. Donc on peut supposer que $m \leq n$. Mais, dans ce cas, $m+1 \leq n+1$. Donc, a fortiori, on a ou bien $m+1 \leq n+1$ ou bien $n+1 \leq m+1$. □

Proposition 1.6.7. *Soient $m, n \in \mathbb{N}$ tels que $m \leq n$ et $n \leq m+1$. Alors, $n = m$ ou $n = m+1$.*

Démonstration. Comme $n \leq m+1$, l'ensemble n est un sous-ensemble de l'ensemble $m+1$. Comme $m+1 = S(m) = m \cup \{m\}$, l'ensemble m aussi est un sous-ensemble de $m+1$. Montrons que $n = m$ ou $n = m+1$. Pour cela, on peut supposer que $n \neq m$. Comme $m \leq n$, on a $m \subseteq n$. Comme $n \neq m$, il existe un éleément x de $m+1$ tel que $x \in n$ mais $x \notin m$. Comme $m+1 = m \cup \{m\}$, on a $x = m$. Il vient que $m \in n$ et $m \subseteq n$, i.e., $m+1 = m \cup \{m\} \subseteq n$. D'où $m+1 \leq n$. Comme on a $n \leq m+1$ par hypothèse, on a $n = m+1$ par antisymétrie de $\leq$. □

Proposition 1.6.8. *Soient $m, n \in \mathbb{N}$ tels que $m \leq n$ et $m \neq n$. Alors $m+1 \leq n$.*

Démonstration. Supposons, par l'absurde, que $m+1 \not\leq n$. Comme l'ordre $\leq$ est totale sur $\mathbb{N}$, on a donc $n \leq m+1$ et $n \neq m+1$. Comme $m \leq n$, on a $n = m$ ou $n = m+1$ d'après Proposition 1.6.7. Comme $m \neq n$, on a $n = m+1$. Contradiction. □

Définition 1.6.9. Soit $(E, \leq)$ un ensemble ordonné. Un élément x de E est *plus petit élément* ou *minimum* de E si pour tout $x' \in E$, $x' \geq x$. Un élément x de E est *plus grand élément* ou *maximum* de E si pour tout $x' \in E$, $x' \geq x$.

Proposition 1.6.10. *Soit $(E, \leq)$ un ensemble ordonné. Si E admet un minimum, le minimum de E est unique. Si E admet un maximum, le maximum de E est unique.*

Démonstration. Supoosons que x et x' sont deux éléments minimum de E. On a donc $x \leq x'$ car x est minimum, et on a $x' \leq x$ car x' est minmum. Par antisymétrie, $x = x'$. Un même argument montre qu'un élément maximum de E est unique. □

Définition 1.6.11. Soit $E(, \leq)$ un ensemble ordonné. On dit que E est *bien ordonné* si tout sous-ensemble non vide de E admet un plus petit élément.

Définition 1.6.12. Soit $(E, \leq)$ un ensemble ordonné et soit $A \subseteq E$. Un *majorant* de A est un élément M de E tel que $\forall x \in A$: $x \leq M$. Le sous-ensemble A de E is majoré s'il admet un majorant. Un *minorant* de A est un

élément m de E tel que $\forall x \in A$: $m \leq x$. Le sous-ensemble A de E is minoré s'il admet un minorant.

Proposition 1.6.13. *L'ensemble ordonné* $(\mathbb{N}, \leq)$ *est bien ordonné, i.e., tout sous-ensemble non vide de* $\mathbb{N}$ *contient un plus petit élément.*

Démonstration. Soit A un sous-ensemble non vide de $\mathbb{N}$. Soit B l'ensemble des minorants de A, i.e.,

$$B = \{m \in \mathbb{N} | \forall x \in A\colon m \leq x\}.$$

Comme $A \neq \emptyset$, il existe $a \in A$. Du coup, $a + 1 \notin B$, car $a + 1 \not\leq a$. D'où $B \neq \mathbb{N}$. Comme $0 \in B$, il existe $n \in \mathbb{N}$ tel que $n \in B$ et $n + 1 \notin B$. Sinon, on aurait $B = \mathbb{N}$ par le principe de récurrence.

Montrons que $n \in A$. En effet, si $n \notin A$, on a $n \leq x$ et $n \neq x$ pour tout $x \in A$. D'après Proposition 1.6.8, $n + 1 \leq x$ pour tout $x \in A$. Ce qui implique que $n+1 \in B$. Contradiction. Par conséquent $n \in A$. Comme $n \in B$, n est le minimum de A. □

Proposition 1.6.14. *Tout sous-ensemble majoré et non vide de* $\mathbb{N}$ *contient un plus grand élément.*

Démonstration. Sooit $A \subseteq \mathbb{N}$ non vide et majoré. Soit $B \subseteq \mathbb{N}$ l'ensembles des majorants de A. Comme A est majoré, B est non vide. D'après Proposition 1.6.13, B contient un plus petit élément m. Comem m est un majorant de A, il suffit de montrer que $m \in A$, pour conclure. Supposons, par l'absurde, que $m \notin A$. On a donc $x < m$ pour tout $x \in A$. Comme A est non vide, on a, en particulier, que $m \neq 0$. Il existe donc $m' \in \mathbb{N}$ tel que $m' + 1 = m$. Comme $x < m$ pour tout $x \in A$, on a $x \leq m'$ pour tout $x \in A$. Du coup, $m' \in B$. Contradiction car $m = m' + 1$ était le plus petit élément de B. □

Exemple 1.6.15. Montrons par récurrence que la somme des n premiers entiers naturels impairs est égale à n^2. Plus précisément, montrons que

$$1 + 3 + 5 + 7 + \cdots + (2n - 1) = n^2,$$

ou, avec la notation Σ pour une somme de termes indexés,

$$\sum_{k=1}^{n} (2k - 1) = n^2$$

quel que soit $n \in \mathbb{N}$. Appelons $\mathcal{P}(n)$ l'assertion ci-dessus.

Tout d'abord, on observe que $\mathcal{P}(n)$ est vrai pour $n = 0$. En effet, le premier membre est une somme pour $k = 1$ jusqu'à $k = 0$. C'est une somme

de 0 termes. Elle vaut 0 par convention. Le second membre vaut $0^2 = 0$. L'assertion $\mathcal{P}(0)$ est donc bien vraie.

Ensuite on montre que $\mathcal{P}(n+1)$ est vraie, si $\mathcal{P}(n)$ est vraie. Supposons donc que

$$\sum_{k=1}^{n}(2k-1) = n^2$$

et montrons que

$$\sum_{k=1}^{n+1}(2k-1) = (n+1)^2.$$

Or,

$$\begin{aligned}\sum_{k=1}^{n+1}(2k-1) &= \left(\sum_{k=1}^{n}(2k-1)\right) + 2(n+1) - 1 \\ &= n^2 + 2n + 1 = (n+1)^2.\end{aligned}$$

Par conséquent, l'ássertion $\mathcal{P}(n+1)$ est vraie lorsque $\mathcal{P}(n)$ est vraie. D'après le principe de récurrence, l'assertion $\mathcal{P}(n)$ est vraie pour tout $n \in \mathbb{N}$.

Voyons quelques instances de l'assertion $\mathcal{P}(n)$, pour $n = 1, 2, 3, 4, 5$:

$$\begin{aligned}1 &= 1^2 \\ 1+3 &= 4 = 2^2 \\ 1+3+5 &= 9 = 3^2 \\ 1+3+5+7 &= 16 = 4^2 \\ 1+3+5+7+9 &= 25 = 5^2 \quad \text{etc.}\end{aligned}$$

Un autre exemple de démonstration par récurrence est celle du fait que $\#\mathcal{P}(E) = 2^n$ lorsque E est un ensemble à n éléments :

Démonstration de Proposition 1.3.16. Si E contient 0 éléments, E est l'ensemble vide. L'ensemble vide contient exactement 1 sous-ensemble, à savoir l'ensemble vide lui-même. On a donc bien $\#\mathcal{P}(E) = 1 = 2^0$ lorsque $n = 0$.

Supposons maintenant que n est un entier naturel tel que pour tout ensembe E avec $\#E = n$, on a $\#\mathcal{P}(E) = 2^n$. Montrons que cette assertion est encore vrai au rang $n+1$. Soit donc E un ensemble à $n+1$ éléments. Comme n est un entier naturel, $n + 1 \neq 0$. L'ensemble E est donc non vide. Soit $x \in E$. Si F est un sous-ensemble de E, on a de deux choses l'une, ou bien $x \in F$ ou bien $x \notin F$.

Dans le dernier cas, F est un sous-ensemble de $E \setminus \{x\}$, et réciproquement, tout sous-ensemble de $E \setminus \{x\}$ est un sous-ensemble de E ne contenant pas x.

Par hypothèse de récurrence, le nombre de sous-ensembles de $E \setminus \{x\}$ est égal à 2^n. Il s'ensuit que le nombre de sous-ensembles F de E tels que $x \notin F$ est égal à 2^n.

Dans le premier cas, i.e., si $x \in F$, le sous-ensemble $F \setminus \{x\}$ de E est un sous-ensemble de $E \setminus \{x\}$. Et réciproquement, si F' est un sous-ensemble de $E \setminus \{x\}$, la réunion $F' \cup \{x\}$ est un sous-ensemble de E contenant x. Donc il y a autant de sous-ensembles F dans E qui ont la propriété que $x \in F$, qu'il y a des sous-ensembles de $E \setminus \{x\}$. Il s'ensuit encore que le nombre de sous-ensembles F de E avec $x \in F$ est égal à 2^n.

D'après ce qui précède, $\#\mathcal{P}(E) = 2^n + 2^n = 2 \times 2^n = 2^{n+1}$. □

Le principe de récurrence est donc très utile pour montrer des assertions qui dépendent d'un entier naturel. Parfois, on a besoin d'un pricipe de récurrence un peu plus général.

1.7 L'addition d'entiers naturels

Soit $m \in \mathbb{N}$ fixé. Maintenant qu'on a défini $m + 1$, pour un entier naturel m, on aimerait définir, plus généralement, la somme $m + n$ quel que soit $n \in \mathbb{N}$. L'idée c'est de définir $m + n$ par récurrence sur n, i.e., on définit $m + 0 = m$. Puis, en supposant que $m + n$ est définie pour un certain $n \in \mathbb{N}$, on définit $m + (n + 1)$ par $(m + n) + 1$.

Par exemple, pour déterminer $2 + 3$, on fait

$$2 + 3 = 2 + (2 + 1) = (2 + 2) + 1 = (2 + (1 + 1)) + 1 = \\ = ((2 + 1) + 1) + 1) = (3 + 1) + 1 = 4 + 1 = 5.$$

Mais, il faudrait préciser ce qu'on entend par une "définition par récurrence". Le principe de récurrence est un principe qui permet de démontrer une assertion qui dépend d'un entier naturel, mais ne permet pas de *définir* par récurrence. En effet, bien que la définition ci-dessus nous permette de déterminer $m+n$ quel que soit $n \in \mathbb{N}$, elle n'est pas la définition d'une application de $\mathbb{N}$ dans $\mathbb{N}$ qui associe à un entier naturel n l'entier $m + n$. Elle ne définit pas le sous-ensemble de $\mathbb{N} \times \mathbb{N}$ qui donnerait cette application. Une façon de rendre la définition précise est la suivante.

Soit $m \in \mathbb{N}$ fixé. Soit $G = G_m$ le plus petit sous-ensemble de $\mathbb{N} \times \mathbb{N}$ ayant les propriétés suivantes :

1. $(0, m) \in G$, et
2. si $(x, y) \in G$, alors $(x + 1, y + 1) \in G$.

Remarquons qu'un tel ensemble existe : il suffit de prendre l'intersection de tous les sous-ensembles de $\mathbb{N} \times \mathbb{N}$ qui satisfont les deux propriétés ci-dessus. On montre que G est une application de $\mathbb{N}$ dans $\mathbb{N}$.

Proposition 1.7.1. *Pour tout $m \in \mathbb{N}$, le sous-ensemble G_m de $\mathbb{N} \times \mathbb{N}$ est une application de $\mathbb{N}$ dans $\mathbb{N}$.*

Démonstration. Soit $m \in \mathbb{N}$ quelconque et fixe. On doit montrer que pour tout $x \in \mathbb{N}$ il existe un et un seul $y \in \mathbb{N}$ tel que $(x, y) \in G_m$. On montre cela par récurrence sur x. Pour aléger la notation, on écrit G au lieu de G_m.

Pour $x = 0$, on a $(0, m) \in G$. Donc il existe bien $y \in \mathbb{N}$ tel que $(0, y) \in G$. Montrons l'unicité de y. Supposons que $(0, y') \in G$ pour un certain $y' \in \mathbb{N}$. Si $y' \neq m$, le sous-ensemble $G \setminus \{(0, y')\}$ de $\mathbb{N} \times \mathbb{N}$ satisferait toujours les deux conditions ci-dessus. On aurait une contradiction car G était le plus petit sous-ensemble de $\mathbb{N} \times \mathbb{N}$ satisfaisant celles-ci. Par conséquent, $y' = m$. Cela montre bien qu'il existe un et un seul $y \in \mathbb{N}$ tel que $(0, y) \in G$.

Supposons maintenant qu'il existe un et un seul $y \in \mathbb{N}$ tel que $(x, y) \in G$, où $x \in \mathbb{N}$ est fixé. Montrons qu'il existe un et un seul $y' \in \mathbb{N}$ tel que $(x + 1, y') \in G$. Soit donc $y \in \mathbb{N}$ tel que $(x, y) \in G$. D'après la condition 2 ci-dessus, on a $(x+1, y+1) \in G$. Donc, on a bien l'existence de $y' \in \mathbb{N}$ tel que $(x+1, y') \in G$. Montrons l'unicité. Supposons que $(x + 1, y'') \in G$. On doit montrer que $y'' = y'$. Supposons, par l'absurde, que $y'' \neq y'$. Soit $G' = G \setminus \{(x+1, y'')\}$. Le sous-ensemble G' de $\mathbb{N} \times \mathbb{N}$ satisfait encore les deux conditions ci-dessus. En effet, comme $x + 1 \neq 0$, on a toujours $(0, m) \in G'$. Pour vérifier la deuxième condition, supposons que $(s, t) \in G'$. En particulier, $(s, t) \in G$. Donc on a $(s+1, t+1) \in G$. Du coup, $(s+1, t+1) \in G'$ sauf si $(s+1, t+1) = (x+1, y'')$. Mais dans ce cas, on aurait $s = x$ et $t = y$ car, d'après l'hypothèse de récurrence, y est le seul entier naturel tel que $(x, y) \in G$. On en déduirait que $y'' = t+1 = y+1 = y'$ ce qui était exclu. Par conséquent, G' satisfait bien les deux conditions ci-dessus. Comme G' est strictement contenu dans G, il y a contradiction. □

Comme G_m est une application de $\mathbb{N}$ dans $\mathbb{N}$, l'entier $G_m(n)$ est bien défini pour tout $n \in \mathbb{N}$. On écrit $m+n$ au lieu de $G_m(n)$. On a, par définition de G_m,

1. $m + 0 = m$, pour tout $m \in \mathbb{N}$, et
2. $m + (n + 1) = (m + n) + 1$, pour tout $m, n \in \mathbb{N}$.

Cela justifie la "définition par récurrence" dont on parlait ci-dessus.

Proposition 1.7.2. *Pour tout $n \in \mathbb{N}$ on a $0 + n = n$.*

Démonstration. L'application identité $\mathrm{id}_{\mathbb{N}}$ de $\mathbb{N}$ dans lui-même, vue comme sous-ensemble de $\mathbb{N}\times\mathbb{N}$, satisfait bien les deux conditions ci-dessus avec $m = 0$. On a donc $G_0 \subseteq \mathrm{id}_{\mathbb{N}}$. Mais comme G_0 et $\mathrm{id}_{\mathbb{N}}$ sont toutes les deux des applications, on a $G_0 = \mathrm{id}_{\mathbb{N}}$. D'où $0 + n = G_0(n) = \mathrm{id}_{\mathbb{N}}(n) = n$, pour tout $n \in \mathbb{N}$. □

Proposition 1.7.3. *Soient $m, n \in \mathbb{N}$. On a $(m + 1) + n = (m + n) + 1$.*

Démonstration. Soit $m \in \mathbb{N}$ quelconque. On considère S comme application de $\mathbb{N}$ dans lui-même. Le composé $S \circ G_m$ satisfait les deux conditons ci-dessus avec $m+1$ au lieu de m. On a donc $G_{m+1} \subseteq S \circ G_m$. Mais comme $S \circ G_m$ est aussi une application, on a $G_{m+1} = S \circ G_m$. D'où $(m + 1) + n = G_{m+1}(n) = (S \circ G_m)(n) = S(G_m(n)) = S(m + n) = (m + n) + 1$, pour tout $n \in \mathbb{N}$. □

Proposition 1.7.4. *Soient $k, m, n \in \mathbb{N}$. Alors, l'addition sur $\mathbb{N}$ est associative et commutative, i.e.,*

$$(k + m) + n = k + (m + n) \quad \textit{et} \quad m + n = n + m.$$

Démonstration. Montrons d'abord la commutativité de l'addition. On montre que $m + n = n + m$ pour tout $n \in \mathbb{N}$, par récurrence sur m. Pour $m = 0$, on a $0+n = n$ d'après Proposition 1.7.2. Comme $n+0 = n$ par définition, on a $0+n = n+0$. Cela montre bien que $m+n = n+m$ quel que soit $n \in \mathbb{N}$ au rang $m = 0$. Supposons, maintenant, que $m+n = n+m$ quel que soit $n \in \mathbb{N}$ pour un certain $m \in \mathbb{N}$. Montrons que $(m + 1) + n = n + (m + 1)$ quel que soit $n \in \mathbb{N}$. Or, $(m+1)+n = (m+n)+1$ d'après Proposition 1.7.3. D'après l'hypothèse de récurrence, $m+n = n+m$, donc aussi $(m+n)+1 = (n+m)+1$. Puis, $(n + m) + 1 = n + (m + 1)$. Il s'ensuit que $(m + 1) + n = n + (m + 1)$. Cela montre la commutativité de l'addition sur $\mathbb{N}$.

Montrons ensuite l'associativité de l'addition sur $\mathbb{N}$. On montre que $(k + m) + n = k + (m + n)$ quel que soient $k, n \in \mathbb{N}$ par récurrence sur m. Pour $m = 0$, on a bien $(k + 0) + n = k + n = k + (0 + n)$ quels que soient $k, n \in \mathbb{N}$. Supposons que $(k + m) + n = k + (m + n)$ quel que soient $k, n \in \mathbb{N}$ pour un certain $m \in \mathbb{N}$. On en déduit que

$$\begin{aligned}(k + (m + 1)) + n = ((k + m) + 1) + n = ((k + m) + n) + 1 = \\ = (k + (m + n)) + 1 = k + ((m + n) + 1) = k + ((m + 1) + n).\end{aligned}$$

en utilisant Proposition 1.7.3 et l'hypothèse de récurrence. □

Maintenant qu'on a démontré l'associativité de l'addition de deux entiers naturels, on peut définir naturellement l'addition de plusieurs entiers naturels. Par exemple, si $k, m, n \in \mathbb{N}$ on définit

$$k + m + n = (k + m) + n.$$

Ou encore, si $k, m, n, p \in \mathbb{N}$, on définit

$$k + m + n + p = ((k + m) + n) + p.$$

Ou plus généralement, si $n_1, \ldots, n_\ell \in \mathbb{N}$, où ℓ est un entier naturel, on définit

$$n_1 + n_2 + \cdots + n_{\ell-1} + n_\ell = ((\cdots(n_1 + n_2) + \cdots) + n_{\ell-1}) + n_\ell.$$

Plus précisément, on définit une somme de $\ell+1$ entiers naturels par récurrence, en supposant qu'une somme de ℓ entiers naturels a été définie,

$$n_1 + n_2 + \cdots + n_\ell + n_{\ell+1} = (n_1 + n_2 + \cdots + n_\ell) + n_{\ell+1}.$$

Une notation un peu plus précise utilise le symbol $\sum$. On définit par récurrence $\Sigma_{i=1}^{\ell} n_i$, prononcé comme "la somme pour $i = 1$ à ℓ de n_i." Pour $\ell = 0$ on définit

$$\sum_{i=1}^{0} n_i = 0,$$

et, si on suppose que la somme $\sum_{i=1}^{\ell} n_i$ est définie pour un certain $\ell \in \mathbb{N}$, on définit $\sum_{i=1}^{\ell+1} n_i$ par

$$\sum_{i=1}^{\ell+1} n_i = \left(\sum_{i=1}^{\ell} n_i\right) + n_\ell.$$

Par exemple,

$$\sum_{i=1}^{1} n_i = n_1, \quad \sum_{i=1}^{2} n_i = n_1 + n_2 \quad \text{et} \quad \sum_{i=1}^{3} n_i = n_1 + n_2 + n_3.$$

Grâce à l'associativité on a des formules comme celle-ci :

$$\sum_{i=1}^{\ell} n_i = \sum_{i=1}^{k} n_i + \sum_{i=k+1}^{\ell} n_i,$$

où k est un entier naturel tel que $0 \leq k \leq \ell$. Ici, on entend par la somme $\sum_{i=k+1}^{\ell} n_i$, la somme $\sum_{i=1}^{\ell-k} n_{k+i}$. Remarqons que la formule ci-dessus est effectivement correcte pour $k = 0$ ou $k = \ell$ grâce à la définition de la somme de zéro entier naturel ci-dessus.

Proposition 1.7.5. *Soient $k, m, n \in \mathbb{N}$. Alors, l'addition sur $\mathbb{N}$ est régulière, i.e.,*

$$m + k = n + k \Rightarrow m = n.$$

Démonstration. On montre, par récurrence sur k, que $m+k = n+k \Rightarrow m = n$ quels que soient $m, n \in \mathbb{N}$. Pour $k = 0$ c'est évident puisque $m + 0 = m$ et $n + 0 = n$. Supposons donc que l'implication $m + k = n + k \Rightarrow m = n$ est vrai quels que soient $m, n \in \mathbb{N}$, pour un certain $k \in \mathbb{N}$. Montrons que $m+(k+1) = n+(k+1)$ implique que $m = n$, quels que soient $m, n \in \mathbb{N}$. En effet, si $m + (k + 1) = n + (k + 1)$, on a, par associativité de l'addition, $(m + k) + 1 = (n + k) + 1$. Il s'esnuit que $m + k = n + k$, et donc, d'après l'hypothèse de récurrence, $m = n$. □

Proposition 1.7.6. *Soient $k, m, n \in \mathbb{N}$ avec $m \leq n$. Alors $m + k \leq n + k$.*

Démonstration. Par récurrence sur k. Au rang $k = 0$, on a bien $m \leq n \Rightarrow m + 0 \leq n + 0$. Supposons donc que $m \leq n \Rightarrow m + k \leq n + k$ quels que soient $m, n \in \mathbb{N}$ avec $m \leq n$, où $k \in \mathbb{N}$ est fixe. montrons que l'énoncé est encore vrai au rang $k + 1$. Soient $m, n \in \mathbb{N}$ avec $m \leq n$. D'après l'hypothèse de récurrence, on a $m + k \leq n + k$, i.e., $(m + k) \subseteq (n + k)$. Du coup

$$(m + k) + 1 = S(m + k) \subseteq S(n + k) = (n + k) + 1.$$

Comme $(m + k) + 1 = m + (k + 1)$ et $(n + k) + 1 = n + (k + 1)$, on a bien $m + (k + 1) \leq n + (k + 1)$. □

Proposition 1.7.7. *Soient $m, n \in \mathbb{N}$. Il existe $k \in \mathbb{N}$ tel que $m + k = n$ si et seulement si $m \leq n$. De plus, dans ce cas, l'entier naturel k est unique.*

Démonstration. Supposons qu'il existe $k \in \mathbb{N}$ tel que $m + k = n$. Montrons que $m \leq n$. En effet, comme $k \in \mathbb{N}$, on a $0 \leq k$. Du coup, $m = 0 + m \leq k + m = m + k = n$.

Réciproquement, supposons que $m \leq n$. Montrons qu'il existe $k \in \mathbb{N}$ tel que $m + k = n$. Soit $m \in \mathbb{N}$ fixe. On montre que pour tout $n \geq m$, il existe $k \in \mathbb{N}$ tel que $m + k = n$ par récurrence sur n. Au rang $n = m$, on prend $k = 0$ et on a bien $m+0 = n$. Soit $n \geq m$ et supposons qu'il existe $k \in \mathbb{N}$ tel que $m + k = n$. Montrons qu'il existe $k' \in \mathbb{N}$ tel que $m + k' = n + 1$. en effet, il suffit de prendre $k' = k + 1$ pour avoir $m + k' = m + (k + 1) = (m + k) + 1 = n + 1$.

L'unicité de k découle immédiatement de Proposition 1.7.5. □

Proposition 1.7.8. *Soient $m, n \in \mathbb{N}$ tels que $m + n = 0$. Alors $m = 0$ et $n = 0$.*

Démonstration. Supposons, par l'absurde, que l'un des deux entiers m et n est non nul. Dans ce cas, on a $m \geq 1$ où $n \geq 1$. D'après Proposition 1.7.6, on a $m + n \geq 1$. Contradiction, car $m + n = 0$. □

1.8 La multiplication d'entiers naturels

Soit $n \in \mathbb{N}$ fixe. De la même manière que pour l'addition, on peut définir, par récurrence sur m, le produit $m \times n$. En effet, on définit $0 \times n = 0$, et lorsque $m \times n$ est défini pour un entier naturel m, on définit $(m+1) \times n$ par $(m \times n) + n$. On peut justifier cette définition par récurrence comme pour celle de l'addition. De manière équivalente, on peut définir le produit $m \times n$ comme la somme répétée de m termes, tous égaux à n :

$$m \times n = \sum_{i=1}^{m} n.$$

Proposition 1.8.1. *On a $m \times 0 = 0$ quel que soit $m \in \mathbb{N}$.*

Démonstration. Par récurrence sur m. On a bien $0 \times 0 = 0$. Supposons que $m \times 0 = 0$ pour un certain $m \in \mathbb{N}$. On a

$$(m+1) \times 0 = m \times 0 + 0 = 0 + 0 = 0$$

d'après la définition de la multiplication et l'hypothèse de récurrence. □

Proposition 1.8.2. *On a $m \times (n+1) = m \times n + m$ quels que soient $m, n \in \mathbb{N}$.*

Démonstration. Montrons par récurrence sur m que $m \times (n+1) = m \times n + m$ quel que soit $n \in \mathbb{N}$. On a $0 \times (n+1) = 0$ et $0 \times n + 0 = 0$ d'après la définition de la multiplication. D'où $m \times (n+1) = m \times n + m$, quul que soit n, quand $m = 0$. Supposons maintenant que $m \times (n+1) = m \times n + m$, pour tout n, pour un certain $m \in \mathbb{N}$. D'après la définition de la multiplication, on a $(m+1) \times (n+1) = m \times (n+1) + n + 1$. D'après l'hypothès de récurrence, on a $m \times (n+1) + n + 1 = m \times n + m + n + 1$. Puis, $m \times n + m + n + 1 = m \times n + n + m + 1$ par commutativité de l'addition. Ensuite, $m \times n + n + m + 1 = (m+1) \times n + (m+1)$ par définition de la multiplication. Par conséquent, on a bien $(m+1) \times (n+1) = (m+1) \times n + (m+1)$, quel que soit $n \in \mathbb{N}$. □

Proposition 1.8.3. *La multiplication sur $\mathbb{N}$ est associative, commutative et distributive par rapport à l'addition, i.e.,*

$$k \times (m+n) = k \times m + k \times n \quad \textit{et} \quad (k+m) \times n = k \times n + m \times n$$

quels que soient $k, m, n \in \mathbb{N}$.

Démonstration. Soit $n \in \mathbb{N}$ fixe, et montrons par récurrence sur m que $m \times n = n \times m$. On a $m \times 0 = 0$ d'après Proposition 1.8.1. Comme $0 \times m = 0$ par définition, on a bien $m \times 0 = 0 \times m$. Supposons maintenant que $m \times n = n \times m$

pour un certain $m \in \mathbb{N}$. Par définition de la multiplication, on a $(m+1)\times n = m \times n + n$. D'après l'hypothèse de récurrence, on a $m \times n = n \times m$. D'où, $m\times n+n = n\times m+n$. D'après Proposition 1.8.2, $n\times m+n = n\times(m+1)$. Par conséquent $(m+1) \times n = n \times (m+1)$, et la multiplication est commutative.

Soient $m, n \in \mathbb{N}$ fixes. Montrons que $k \times (m+n) = k \times m + k \times n$ par récurrence sur k. Si $k = 0$, on a bien $0 \times (m+n) = 0 \times m + 0 \times n$ d'après la définition de la multiplication. Supposons que $k \times (m+n) = k \times m + k \times n$ pour en certain entier naturel k. D'après la définition de la multiplication, on a $(k+1) \times (m+n) = k \times (m+n) + (m+n)$. D'après l'hypothèse de récurrence, $k \times (m+n) = k \times m + k \times n$. Donc, $k \times (m+n) + (m+n) = k\times m+k\times n+m+n$. Comme l'addition est commutative, on a $k\times m+k\times n+m+n = k\times m+m+k\times n+n$. D'après la définitin de la multiplication, on a $k \times m + m + k \times n + n = (k+1) \times m + (k+1) \times n$. Cela montre la première loi de distributivité. La deuxième s'ensuit grâce ła commutativité de la multiplication qu'on a démontré ci-dessus.

Soient $m, n \in \mathbb{N}$ fixes. Montrons, par récurrence sur k, que $(k \times m) \times n = k \times (m \times n)$. D'après Proposition 1.8.1, on a bien $(0 \times m) \times n = 0 \times (m \times n)$. Supposons donc que $(k\times m)\times n = k\times(m\times n)$ pour un certain $k \in \mathbb{N}$. D'après la définition de la multiplication, on a $((k+1) \times m) \times n = (k \times m + m) \times n$. Daprès la distributivité, on a $(k \times m + m) \times n = (k \times m) \times n + m \times n$. Par hypothèse de récurrence, on a $(k \times m) \times n + m \times n = k \times (m \times n) + m \times n$. et finalement, par définition de la multiplication, on a $k \times (m \times n) + m \times n = (k+1) \times (m \times n)$. Cela montre que $((k+1) \times m) \times n = (k+1) \times (m \times n)$. □

Proposition 1.8.4. *On a $n \times 1 = n$ et $1 \times n = n$ quel que soit $n \in \mathbb{N}$.*

Démonstration. Par définition de la multiplication, on a $1\times n = (0+1)\times n = 0 \times n + n = 0 + n = n$ quel que soit $n \in \mathbb{N}$. Comme la multiplication est commutative, on a aussi $n \times 1 = n$ quel que soit $n \in \mathbb{N}$. □

Proposition 1.8.5. *Soient $k, m, n \in \mathbb{N}$. Si $m \leq n$, alors $k \times m \leq k \times n$.*

Démonstration. Par récurrence sur k. Au rang 0, on a bien $0 \times m \leq 0 \times n$ car $0 \times m = 0$ et $0 \times n = 0$ d'après la définition de la multiplication. Supposons que $k \times m \leq k \times n$ pour tout $m, n \in \mathbb{N}$ avec $m \leq n$. Montrons qu'on a aussi $(k+1) \times m \leq (k+1) \times n$ lorsque $m \leq n$. En effet, $(k+1) \times m = k \times m + m$ par définition de la multiplication. Par hypothèse de récurrence, $k \times m \leq k \times n$. D'après Proposition 1.7.6, on a $k \times m + m \leq k \times n + m$. Comme $m \leq n$, on a encore, par Proposition 1.7.6, $k \times n + m \leq k \times n + n$. D'où $(k+1) \times m = k \times m + m \leq k \times n + n = (k+1) \times n$. □

Proposition 1.8.6. *Soient $m, n \in \mathbb{N}$. Si $m \times n = 0$, alors $m = 0$ ou $n = 0$.*

Démonstration. Supposons, par l'absurde, que $m \neq 0$ et $n \neq 0$. Dans ce cas $1 \leq n$. D'après Proposition 1.8.5, on a $m \times 1 \leq m \times n$. Comme $m \neq 0$, $m \times 1 = m \neq 0$ et donc $1 \times m \geq 1$. Du coup, $m \times n \geq 1$. Contradiction, car $m \times n = 0$. □

On a la règle suivante de simplification.

Proposition 1.8.7. *Soient $k, m, n \in \mathbb{N}$ avec $k \neq 0$. Alors*

$$k \times m = k \times n \Rightarrow m = n.$$

Démonstration. Par récurrunce sur m. Si on a $k \times 0 = k \times n$, on a $k \times n = 0$. D'après Proposition 1.8.6, on a $k = 0$ ou $n = 0$. Comme $k \neq 0$, on a donc bien $n = 0$. D'où $m = n$. Supposons maintenant que l'énoncé est vrai au rang m. Montrons-le au rang $m + 1$. Soient donc $k, n \in \mathbb{N}$, avec $k \neq 0$, tels que $k \times (m+1) = k \times n$. On doit montrer que $m+1 = n$. Tout d'abord, $n \neq 0$ sinon, $k \times (m + 1) = 0$, ce qui est impossible puisque $k \neq 0$ et $m + 1 \neq 0$. Comme $n \neq 0$, il existe $n' \in \mathbb{N}$ tel que $n = n' + 1$. Du coup, on a

$$k \times m + k = k \times (m + 1) = k \times (n' + 1) = k \times n' + k.$$

D'après Proposition 1.7.5, on a $k \times m = k \times n'$. D'après l'hypothèse de récurrence, $m = n'$. Du coup $m + 1 = n' + 1 = n$. □

Chapitre 2

Algèbre

2.1 Groupes

Définition 2.1.1. Soit E un ensemble. Une *loi de composition interne sur E* est une application de $E \times E$ dans E.

Si $\star$ est une loi de composition interne sur un ensemble E, et si $x, y \in E$, on écrit $x \star y$ au lieu de $\star(x, y)$.

Exemples 2.1.2. L'addition sur $\mathbb{N}$ qu'on a définie au chapitre précédent est une loi de composition interne sur $\mathbb{N}$. En effet, l'addition $+$ associe à un couple d'entiers naturels (m, n) un troisième entier naturel $m + n$.

On définit la multiplication $\times$ sur $\mathbb{N}$ par récurrence. Soit $m \in \mathbb{N}$ fixe. On définit $m \times n$, pour tout $n \in \mathbb{N}$, par récurrence sur n. On pose $m \times 0 = 0$. Puis, par récurrence, on définit $m \times (n + 1) = (m \times n) + m$. La multiplication $\times$ sur $\mathbb{N}$ est une loi de composition interne sur $\mathbb{N}$.

Soit F un ensemble, et soit E l'ensemble des applications de F dans lui-même. Si f et g sont deux applications de F dans lui-même, $f \circ g$ est de nouveau une application de F dans lui-même. Par conséquent, la composition $\circ$ est une loi de composition interne sur E.

Définition 2.1.3. Soit $\star$ une loi de composition interne sur un ensemble E.

1. La loi $\star$ est *associative* si pour tous $x, y, z \in E$, $(x \star y) \star z = x \star (y \star z)$.
2. La loi $\star$ est *commutative* si pour tous $x, y \in E$, $x \star y = y \star x$.
3. Un élément e de E est *neutre* pour la loi $\star$ si $x \star e = x$ et $e \star x = x$ pour tout $x \in E$.

Exemple 2.1.4. Les lois de composition internes ci-dessus sont toutes associatives. Exactement deux entre elles sont commutatives. Chacune des trois lois admettent un élément neutre.

Proposition 2.1.5. *Soit $\star$ une loi decomposition interne sur E. S'il y a un élément neutre pour la loi $\star$, alors il est unique.*

Démonstration. Supposons que e et e' sont deux éléments neutres de E pour la loi $\star$. On montre que $e = e'$. En effet, comme e est neutre et $e' \in E$, on a $e \star e' = e'$. De même, comme e' est neutre et $e \in E$, on a $e \star e' = e$. Par conséquent, $e = e \star e' = e'$. □

On note l'élément neutre souvent par 0 lorsque la loi est notée par $+$, et par 1 lorsque la loi est notée par $\cdot$. Sinon, on le note par e.

Définition 2.1.6. Soit $\star$ une loi de composition interne sur un ensemble E. Supposons qu'il y a un élément neutre e pour la loi $\star$. Soit $x \in E$. Un *symétrique* de x est un élément $y \in E$ tel que $x \star y = e$ et $y \star x = e$.

Exemple 2.1.7. Très peu d'éléments de $\mathbb{N}$ ont un symétrique pour les lois $+$ ou $\times$. Par contre, beaucoup d'éléments de l'ensemble E des applications d'un ensemble F dans lui-même admettent des symétriques pour la loi de composition $\circ$. En effet, si $f \in E$ est une bijection, f admet un symétrique f^{-1}. Réciproquement, si un élément f de E admet un symétrique, il est une bijection.

Proposition 2.1.8. *Soit $\star$ une loi de composition interne sur un ensemble E. Supposons que $\star$ est associative et qu'il y a un élément neutre e. Soit $x \in E$. Si x admet un symétrique, alors il est unique.*

Démonstration. Supposons que y et y' sont des sym ertiques de x pour la loi $\star$ sur E. On calcule l'élément $(y \star x) \star y'$ de deux manières. D'un côté, $(y \star x) \star y' = e \star y' = y'$ car y est un symétrique de x et e est neutre. De l'autre côté, comme $\star$ est associative, on a $(y \star x) \star y' = y \star (x \star y')$. Puis, $y \star (x \star y') = y \star e = y$ car y' est un symétrique de x et e est neutre. Par conséquent, $y' = y$. □

Soit E un ensemble et soit $\star$ une loi de composition interne sur E. Supposons que $\star$ est associative et qu'il y a une élément neutre e. Soit $x \in E$. Si x admet un symétrique, on le note x^{-1}, sauf si la loi est notée par $+$ auquel cas on le note $-x$.

Définition 2.1.9. Soit E un ensemble muni d'une loi de composition interne $\star$. Le couple $(E, \star)$ est un *groupe* si la loi $\star$ est associative, si elle admet un élément neutre, et si tout élément admet un symétrique. Un groupe $(E, \star)$ est *commutatif* ou *abélien* lorsque la loi $\star$ est commutative.

Malheureusement, aucun des trois exemples ci-dessus n'est un exemple d'un groupe. Il y a, essentiellement, deux façon d'y remédier, comme on verra dans l'exemple suivant

Exemple 2.1.10. 1. L'ensemble $\mathbb{N}$ muni de l'addition n'est pas un groupe car 1, par exemple, n'admet pas de symétrique dans $\mathbb{N}$ pour l'addition. Par contre, on peut agrandir $\mathbb{N}$ pour obtenir un groupe : l'ensemble des entiers relatifs $\mathbb{Z}$, muni de l'addition, est un groupe, et même un groupe abélien.

2. L'ensemble $\mathbb{N}$ muni de la multiplication n'est pas un groupe car 0, par exemple, n'admet pas de symétrique. Ici, il n'y a pas moyen d'agrandir $\mathbb{N}$ pour en faire un groupe pour la multplication. On est obligé de lui retirer lélément 0 d'abord. On note $\mathbb{N}^\star = \mathbb{N} \setminus \{0\}$. L'ensemble $\mathbb{N}^\star$ n'est toujours pas un groupe pour la multiplication, mais cette fois-ci, on peut l'agrandir pour en faire un groupe : l'ensemble des nombres rationnels strictement positifs $\mathbb{Q}_+^\star$, muni de la multiplication, est un groupe, et même un groupe abélien.

3. Soit F un ensemble et E l'ensemble des applications de F dans lui-même. Alors, E n'est pas un groupe pour la composition. Par contre, le sous-ensemble S de E des bijections de F dans lui-même est un groupe pour la composition. Il s'appelle *le groupe symétrique* de F. Le groupe S n'est en général pas commutatif. Lorsque $F = \{1, 2, 3, \ldots, n\}$, le groupe symétrique de F est noté S_n. Donc, S_n est l'ensemble des bijections de $\{1, \ldots, n\}$ dans lui-même. Il est un groupe sous la composition d'applications.

Proposition 2.1.11. *Soit $(G, \star)$ un groupe. Soit $x, y \in G$. Alors $(x^{-1})^{-1} = x$, $e^{-1} = e$,et $(xy)^{-1} = y^{-1}x^{-1}$.*

Exemples 2.1.12. 1. L'ensemble des nombres rationnels $\mathbb{Q}$, muni de l'addition, est un groupe ablien.

2. L'ensemble des nombres réels $\mathbb{R}$, muni de l'addition, est un groupe abélien.

3. L'ensemble des nombres complexes $\mathbb{C}$, muni de l'addition, est un groupe abélien.

4. L'ensemble des nombres rationnels non nuls $\mathbb{Q}^\star$, muni de la multiplication, est un groupe ablien.

5. L'ensemble des nombres réels non nuls $\mathbb{R}^\star$, muni de la multiplication, est un groupe abélien.

6. L'ensemble des nombres complexes non nuls $\mathbb{C}^\star$, muni de la multiplication, est un groupe abélien.

7. Soit n un entier relatif. Soit $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence modulo n des entiers relatifs. On définit une loi sur $\mathbb{Z}/n\mathbb{Z}$ par $\overline{k}+\overline{m} = \overline{k+m}$, pour tout $\overline{k}, \overline{m} \in \mathbb{Z}/n\mathbb{Z}$. Alors, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ est un groupe abélien pour la loi $+$.

2.2 Anneaux et corps

Définition 2.2.1. Soit E un ensemble muni de deux lois $+$ et $\cdot$. On dit que $\cdot$ est *distributive* par rapport à $+$ lorsque $x \cdot (y+z) = x \cdot y + x \cdot z$ et $(x+y)\cdot z = x\cdot z + y \cdot z$ pour tous $x, y, z \in E$. Un *anneau* est un triplet $(E, +, \cdot)$ tel que

1. $(E, +)$ est un groupe abélien,
2. la loi $\cdot$ est distributive par rapport à la loi $+$, et
3. la loi $\cdot$ est associative.

Un anneau $(E, +, \cdot)$ est un *anneau unitaire* s'il admet un élément neutre pour la loi $\cdot$. Un anneau $(E, +, \cdot)$ est *commutatif*, si la loi $\cdot$ est commutative.

Dans un anneau unitaire $(A, +, \cdot)$ on a deux élément neutres : 0 et 1. Le premier est neutre pour $+$, le deuxième pour $\cdot$. On note souvent $A^\star$ pour $A \setminus \{0\}$.

Exemples 2.2.2. 1. L'ensemble $\mathbb{Z}$, muni de l'addition et la multiplication, est un anneau unitaire commutatif.

2. L'ensemble $\mathbb{Q}$, muni de l'addition et la multiplication, est un anneau unitaire commutatif.

3. L'ensemble $\mathbb{R}$, muni de l'addition et la multiplication, est un anneau unitaire commutatif.

4. L'ensemble $\mathbb{C}$, muni de l'addition et la multiplication, est un anneau unitaire commutatif.

5. Soit $n \in \mathbb{Z}$. On définit sur $\mathbb{Z}/n\mathbb{Z}$ une loi de multiplication $\times$ par $\overline{k} \times \overline{m} = \overline{km}$ pour tout $\overline{k}, \overline{m} \in \mathbb{Z}/n\mathbb{Z}$. L'ensemble $\mathbb{Z}/n\mathbb{Z}$, muni de l'addition et de la multiplication, est un anneau unitaire commutatif.

6. Soit A un anneau, et X une indéterminée. Un *polynôme* en X à coefficients dans A est une expression de la forme $a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$, où $a_0, \ldots, a_n \in A$ et $n \in \mathbb{N}$. L'ensemble des polynômes en X à coefficients dans A est notée $A[X]$. On définit deux lois de composition interne $+$ et $\cdot$ sur $A[X]$ par

$$\begin{aligned}(a_0 + a_1X + \cdots + a_nX^n) + (b_0 + b_1X + \cdots + b_nX^n) = \\ = (a_0 + b_0) + (a_1 + b_1)X + \cdots + (a_n + b_n)X^n\end{aligned}$$

et

$$\begin{aligned}(a_0 + a_1X + \cdots + a_nX^n) \cdot (b_0 + b_1X + \cdots + b_mX^m) = \\ = c_0 + c_1X + \cdots + c_{n+m}X^{n+m},\end{aligned}$$

où

$$c_p = a_0 b_p + a_1 b_{p-1} + \cdots + a_p b_0,$$

pour $p = 0, \ldots, n+m$. Là, il est sousentendu que $a_i = 0$ lorsque $i > n$, et que $b_i = 0$ lorsque $i > m$. L'ensemble $A[X]$, muni de ces deux lois, est un anneau. L'anneau $A[X]$ est unitaire si A l'est, et commutatif si A est commutatif.

Proposition 2.2.3. *Soit $(A, +, \cdot)$ un anneau unitaire. Soit $x \in A$. On a $0 \cdot x = 0$ et $(-1) \cdot x = -x$.*

Démonstration. Comme $0 \cdot x = (0+0) \cdot x = 0 \cdot x + 0 \cdot x$, on trouve $0 \cdot x = 0$ par simplifcation. On en déduit que $x + (-1) \cdot x = 1 \cdot x + (-1) \cdot x = (1 + (-1)) \cdot x = 0 \cdot x = 0$. Du coup, $(-1) \cdot x = -x$. □

Définition 2.2.4. Soit A un anneau commutatif unitaire. Un élément $a \in A$ est *inversible* s'il existe $b \in A$ tel que $ab = 1$. Dans ce cas, l'élément b est uniquement déterminé par a et est noté a^{-1}. L'ensemble des éléments inversibles de A est noté $A^\times$.

Proposition 2.2.5. *Soit A un anneau commutatif unitaire.*

1. *$1 \in A$ est inversible*
2. *Si $a \in A$ est inversible, alorsa^{-1} est inversible et $(a^{-1})^{-1} = a$, et $-a$ est inversible et $(-a)^{-1} = -(a^{-1})$.*
3. *Si $a, b \in A$ sont inversibles, alors ab est inversible et $(ab)^{-1} = b^{-1}a^{-1}$.*

Démonstration. Exercice. □

Corollaire 2.2.6. *Soit A un anneau commutatif unitaire. Le sous-ensemble $A^\times$ des inversibles de A est un groupe commutatif pour la multiplication.* □

Exemple 2.2.7. Le groupe des inversibles de l'anneau $\mathbb{Z}$ est le groupe commutatif $\{-1, +1\}$ muni la loi de multiplication.

Définition 2.2.8. Soit $(A, +, \cdot)$ un anneau commutatif unitaire. L'anneau A est *intègre* si $A \neq \{0\}$, et $xy = 0 \Rightarrow x = 0$ ou $y = 0$, pour tout $x, y \in A$. L'anneau A est un *corps* si $A \neq \{0\}$ et tout élément non nul de A est inversible.

Proposition 2.2.9. *Tout corps est intègre.*

Démonstration. Soit A un corps. Montrons que A est intègre. Supposons donc que $ab = 0$ où $a, b \in A$. On montre que $a = 0$ ou $b = 0$. Pour cela, on peut supposer que $a \neq 0$, et montrer que $b = 0$. Or, si $a \neq 0$, a est inversible car A est un corps. On a donc $a^{-1} \in A$. Multiplier l'équation $ab = 0$ à gauche par a^{-1} nous donne $a^{-1}(ab) = 0$. D'où $0 = a^{-1}(ab) = (a^{-1}a)b = 1 \cdot b = b$. □

Exemples 2.2.10. 1. L'anneau $\mathbb{Z}$ est intègre, mais il n'est pas un corps.

2. Les anneaux $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps.

3. L'anneau $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre car $\overline{2} \times \overline{3} = \overline{6} = \overline{0}$ dans $\mathbb{Z}/6\mathbb{Z}$. Donc, il n'est pas un corps non plus.

4. Soit $n \in \mathbb{Z}^\star$. On verra plus tard que $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est un nombre premier. Dans ce cas, $\mathbb{Z}/n\mathbb{Z}$ est même un corps.

5. Soit K un corps, et X une indéterminée. Une *fraction rationnel* en X à coefficients dans K est une expression de la forme P/Q, où P et Q sont des polynômes en X à coefficients dans K, avec $Q \neq 0$. Deux de telles fractions rationnelles P/Q et P'/Q' sont *égales* si $PQ' = Q'P$ dans $K[X]$. On définit deux lois de composition internes $+$ et $\cdot$ sur $K(X)$ par

$$\frac{P}{Q} + \frac{P'}{Q'} = \frac{PQ' + P'Q}{QQ'} \quad \text{et} \quad \frac{P}{Q} \cdot \frac{P'}{Q'} = \frac{PP'}{QQ'}.$$

On peut vérifier que $K(X)$, muni de ces lois, est un corps. C'est le corps des fractions rationnelles en X à coefficients dans K.

2.3 Le corps des nombres complexes

Définition 2.3.1. Un *nombre complexe* est un élément de $\mathbb{R}^2$. L'ensemble des nombres complexes est noté par $\mathbb{C}$, i.e., $\mathbb{C} = \mathbb{R}^2$. On définit des lois $+$ et $\cdot$ sur $\mathbb{C}$ par les formules suivantes :

$$(a, b) + (c, d) = (a + c, b + d) \quad \text{et} \quad (a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

Proposition 2.3.2. *$(\mathbb{C}, +, \cdot)$ est un corps.*

L'élément neutre additif de $\mathbb{C}$ est $(0, 0)$. On note donc $0 = (0, 0)$. L'élément neutre multiplicatif est $(1, 0)$. On note donc $1 = (1, 0)$. On définit $i = (0, 1)$. On a $i^2 = -1$. Soient $(a, b) \in \mathbb{C}$. Alors,

$$\begin{aligned}(a, b) &= (a, 0) + (0, b) = \\ &= a \cdot (1, 0) + b \cdot (0, 1) = \\ &= a \cdot 1 + b \cdot i = \\ &= a + bi.\end{aligned}$$

Par conséquent, pour tout $z \in \mathbb{C}$ il existe $a, b \in \mathbb{R}$ tels que $z = a + bi$. de plus, a et b sont uniquement déterminés par z.

Définition 2.3.3. Si $z = a + bi$, où $a, b \in \mathbb{R}$, a est la *partie réelle* de z, notée $\mathrm{Re}(z)$, et b est la *partie imaginaire* de z, notée $\mathrm{Im}(z)$. Le *conjugué* de $z = a + bi$, noté $\overline{z}$, est le nombre complexe $a - bi$. Le *module* de $z = a + bi$, noté $|z|$, est le nombre réel $\sqrt{a^2 + b^2}$.

Pour $z \in \mathbb{C}$, on a $|z| = 0$ si et seulement si $z = 0$. Pour $z \in \mathbb{C}$, on a $|z|^2 = z\overline{z}$. Pour $w, z \in \mathbb{C}$, on a l'inégalité triangulaire $|w + z| \leq |w| + |z|$, et l'inégalité triangulaire renversée $||w| - |z|| \leq |w - z|$. On a $|wz| = |w| \cdot |z|$. Soit $\mathbb{C}^\star = \mathbb{C} \setminus \{0\}$. Si $\alpha = a + bi \in \mathbb{C}^\star$, où $a, b \in \mathbb{R}$,

$$\alpha^{-1} = \frac{\overline{\alpha}}{|\alpha|^2} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i.$$

2.4 Equations de degré 2

Définition 2.4.1. Soit $\alpha \in \mathbb{C}$. Un nombre complexe z tel que $z^2 = \alpha$ est une *racine carrée* de α.

Proposition 2.4.2. *Soit $\alpha = a + bi \in \mathbb{C}^\star$, avec $a, b \in \mathbb{R}$. Alors, α admet exactement deux racines carrées, i.e., il existe exactement deux nombres complexes z tels que $z^2 = \alpha$. En effet,*

1. *si $b = 0$ et $a > 0$, $z = \pm\sqrt{a}$,*
2. *si $b = 0$ et $a < 0$, $z = \pm i\sqrt{-a}$, et*
3. *si $b \neq 0$,*

$$z = \pm \left(\sqrt{\tfrac{1}{2}(a + |\alpha|)} + \operatorname{sign}(b) i \sqrt{\tfrac{1}{2}(-a + |\alpha|)} \right),$$

où $\operatorname{sign}(b)$ *est le signe de b.*

Démonstration. Supposons que $z = x + yi$ est racine carrée de $\alpha = a + bi$, où $x, y \in \mathbb{R}$. On a donc $(x + yi)^2 = a + bi$, i.e. $(x^2 - y^2) + 2xyi = a + bi$. D'où le système d'équations

$$\begin{cases} x^2 - y^2 &= a \\ 2xy &= b \end{cases}$$

Si $b = 0$, on a $x = 0$ ou $y = 0$. Conmme $x^2 - y^2 = a$, on a $x = 0$ si $a < 0$, et on a $y = 0$ si $a > 0$. Dans le dernier cas, $x = \pm\sqrt{a}$ et $z = \pm\sqrt{a}$. Dans le premier cas, $y = \pm\sqrt{-a}$ et $z = \pm i\sqrt{-a}$. Cela montre bien que les énoncés 1 et 2 sont vrais. Dans la suite, on peut donc supposer que $b \neq 0$.

Comme $2xy = b \neq 0$, on a forcément $x \neq 0$. On peut donc diviser l'équation $2xy = b$ par $2x$ de deux côtés pour obtenir $y = b/2x$. On substitue $b/2x$ pour y dans l'équation $x^2 - y^2 = a$ et on obtient

$$x^2 - \frac{b^2}{4x^2} = a.$$

En multipliant de deux côtés par $4x^2$, on obtient

$$4x^4 - 4ax^2 - b^2 = 0.$$

On regarde cette équation comme équation de degré 2 en x^2. Comme son discriminant $(4a)^2 - 4 \times 4 \times (-b^2) = 16(a^2 + b^2)$ est positif, on en déduit que

$$x^2 = \frac{4a \pm \sqrt{16(a^2+b^2)}}{8} = \tfrac{1}{2}(a \pm |\alpha|).$$

Maintenant, $a - |\alpha| < 0$ car $b \neq 0$. Il vient que $x^2 = \frac{1}{2}(a + |\alpha|)$. Comme $a + |\alpha| \geq 0$, on obtient

$$x = \pm\sqrt{\tfrac{1}{2}(a + |\alpha|)}.$$

Supposons que $x = \sqrt{\frac{1}{2}(a + |\alpha|)}$. Dans ce cas,

$$\begin{aligned} y = \frac{b}{2x} = \frac{b}{2\sqrt{\frac{1}{2}(a+|\alpha|)}} = \\ = \frac{\mathrm{sign}(b)\sqrt{b^2}}{\sqrt{2(a+|\alpha|)}} = \mathrm{sign}(b)\sqrt{\frac{b^2}{2(a+|\alpha|)}} = \\ = \mathrm{sign}(b)\sqrt{\frac{b^2}{2(a+|\alpha|)} \cdot \frac{(a-|\alpha|)}{(a-|\alpha|)}} = \\ = \mathrm{sign}(b)\sqrt{\frac{b^2 \cdot (a-|\alpha|)}{2(a^2-(a^2+b^2))}} = \mathrm{sign}(b)\sqrt{\tfrac{1}{2}(-a+|\alpha|)}. \end{aligned}$$

D'où

$$z = \sqrt{\tfrac{1}{2}(a + |\alpha|)} + \mathrm{sign}(b) i \sqrt{\tfrac{1}{2}(-a + |\alpha|)},$$

lorsque $x = \sqrt{\frac{1}{2}(a + |\alpha|)}$.

On vérifie de la même manière que

$$z = -\left(\sqrt{\tfrac{1}{2}(a + |\alpha|)} + \mathrm{sign}(b) i \sqrt{\tfrac{1}{2}(-a + |\alpha|)}\right),$$

lorsque $x = -\sqrt{\frac{1}{2}(a + |\alpha|)}$. L'énoncé 3 s'ensuit. □

Exemple 2.4.3. Soit $\alpha = 3 - 4i$. Alors, $a = 3$ et $b = -4$, $|\alpha| = 5$ et les racines carrées de α sont

$$z = \pm\left(\sqrt{\tfrac{1}{2}(3+5)} - i\sqrt{\tfrac{1}{2}(-3+5)}\right) = \pm(2 - i) = 2 - i,\ -2 + i.$$

De même, les racines carrés de $-5+12i$ sont

$$z = \pm\left(\sqrt{\tfrac{1}{2}(-5+13)} + i\sqrt{\tfrac{1}{2}(5+13)}\right) = \pm(2+3i).$$

Proposition 2.4.4. *Soient $\alpha, \beta, \gamma \in \mathbb{C}$. Supposons que $\alpha \neq 0$. Les solutions dans $\mathbb{C}$ de l'équation $\alpha z^2 + \beta z + \gamma = 0$ sont*

$$z = \frac{-\beta \pm \delta}{2\alpha},$$

où δ est une racine carrée du discriminant $\Delta = \beta^2 - 4\alpha\gamma$.

Exemple 2.4.5. Résoudre l'équation $z^2 - (4+6i)z - 5 + 10i = 0$. Alors, $\alpha = 1$, $\beta = -4-6i$ et $\gamma = -5+10i$. D'où le discriminant $\Delta = -20 + 48i - 4(-5+10i) = 4(-5+12i+5-10i) = 4(2i)$. Une racine carrée de $2i$ est $1+i$. Soit $\delta = 2(1+i)$. Alors δ est une racine carrée de Δ, et les solutions de l'équation sont

$$z = \frac{4+6i \pm 2(1+i)}{2} = 2+3i \pm (1+i) = 1+2i,\ 3+4i.$$

2.5 Racines de l'unité

Définition 2.5.1. Pour $\theta \in \mathbb{R}$, on définit

$$e^{i\theta} = \cos(\theta) + i\sin(\theta).$$

Pou des raison de mise enpage, on écrit aussi $\exp(i\theta)$ au lieu de $e^{i\theta}$.

Proposition 2.5.2. *Soient $\theta, \theta' \in \mathbb{R}$. Alors*

1. $e^{i(\theta+\theta')} = e^{i\theta} \cdot e^{i\theta'}$,
2. $(e^{i\theta})^n = e^{in\theta}$, *pour tout $n \in \mathbb{Z}$,*
3. $e^{i\theta} = e^{i\theta'}$ *si et seulement si $\theta - \theta' = 2k\pi$, pour un certain $k \in \mathbb{Z}$,*
4. $|e^{i\theta}| = 1$.
5. $\overline{e^{i\theta}} = e^{-i\theta}$,
6. $\cos(\theta) = \frac{1}{2}(e^{i\theta} + e^{-i\theta})$ *et* $\sin(\theta) = \frac{1}{2i}(e^{i\theta} - e^{-i\theta})$.

Proposition 2.5.3. *Pour tout $\alpha \in \mathbb{C}^\star$, il existe $r \in \mathbb{R}^+$ et $\theta \in \mathbb{R}$ tel que*

$$\alpha = re^{i\theta}.$$

Le réel r est uniquement déterminé par α. Le réel θ est uniquement déterminé à un multiple entier de 2π près.

Définition 2.5.4. Soit $\alpha, r,$ *theta* comme ci-dessus. On appelle r le *module* de α, et θ un *argument* de α. L'écriture $\alpha = re^{i\theta}$ est l'écriture *trigonométrique* d'un nombre complexe α. Si θ et θ' sont des arguments de α, il existe un entier relatif k tel que $\theta = \theta' + 2k\pi$. On écrira $\theta \equiv \theta' \mod 2\pi$. On écrira aussi $\arg(\alpha)$ pour un argument de α.

Proposition 2.5.5. *Soient* $w, z \in \mathbb{C}^\star$.

1. $\arg(wz) \equiv \arg(w) + \arg(z) \mod 2\pi$,
2. $\arg(z^{-1}) \equiv -\arg(z) \mod 2\pi$.

Démonstration. 1. Ecrire $z = re^{i\theta}$ et $w = se^{i\eta}$. D'après Proposition 2.5.2, on a $wz = rse^{i(\eta+\theta)}$. D'où $\eta + \theta$ est un argument de wz. Comme η est un argument de w et θ est un argument de z, on a bien $\arg(wz) = \arg(w) + \arg(z) \mod 2\pi$.

2. Avec $w = z^-1$ le 1 nous donne que $\arg(z^{-1}) + \arg(z) \equiv 0 \mod 2\pi$, i.e., $\arg(z^{-1}) \equiv \arg(z) \mod 2\pi$. □

Définition 2.5.6. Soit $\alpha \in \mathbb{C}$ et $n \in \mathbb{N}$. Une *racine n-ième* de α est un nombre complexe z tel que $z^n = \alpha$. Une *racine n-ième d'unité* est une racine n-ième de 1.

Exemples 2.5.7. 1. Les racines carrées de l'unité sont ± 1. En effet, si $z \in \mathbb{C}$ satisfait $z^2 = 1$, on a $(z-1)(z+1) = z^2 - 1 = 0$. D'où $z = \pm 1$.

2. Les racines cubiques de l'unité sont 1, $-\frac{1}{2} + \frac{1}{2}i\sqrt{3}$ et $-\frac{1}{2} - \frac{1}{2}i\sqrt{3}$. En effet, si $z^3 = 1$, on a $0 = z^3 - 1 = (z-1)(z^2 + z + 1)$, i.e., $z = 1$ ou $z^2 + z + 1 = 0$. D'après la méthode du paragraphe précédent, les solutions de l'équation $z^2 + z + 1 = 0$ sont $-\frac{1}{2} \pm \frac{1}{2}i\sqrt{3}$.

3. Les racines 4-ième de l'unité sont ± 1 et $\pm i$. En effet, si $z^4 = 1$, on a

$$0 = z^4 - 1 = (z^2 -)(z^2 + 1) = (z-1)(z+1)(z-i)(z+i).$$

D'où $z = \pm 1, \pm i$.

4. Déterminons les racines 5-ième de l'unité. Soit $z \in \mathbb{C}$ tel que $z^5 = 1$. On a

$$0 = z^5 - 1 = (z-1)(z^4 + z^3 + z^2 + z + 1).$$

Donc $z = 1$ ou $z^4 + z^3 + z^2 + z + 1 = 0$. Comme 1 est bien une racine 5-ième de l'unité, supposons que $z \neq 1$ pour déterminer les autres racines 5-ième de l'unité. On a donc $z^4 + z^3 + z^2 + z + 1 = 0$.

On va résoudre cette équation de degré 4. Comme $z \neq 0$, on a, en divisant par z^2,

$$0 = z^2 + z + 1 + z^{-1} + z^{-2} = \\ (z + z^{-1})^2 + (z + z^{-1}) - 1 = (z + \overline{z})^2 + (z + \overline{z}) - 1,$$

car $z^{-1} = \overline{z}/|z|^2 = \overline{z}$. En écrivant $z = x + iy$, avec $x, y \in \mathbb{R}$, on a $z + \overline{z} = 2x$ et

$$(2x)^2 + (2x) - 1 = 0.$$

On en déduit que $2x = -\frac{1}{2} \pm \frac{1}{2}\sqrt{5}$, i.e. $x = -\frac{1}{4} \pm \frac{1}{4}\sqrt{5}$. Comme $|z| = 1$, on a $y^2 = 1 - x^2$. Après un petit calcul, on trouve

$$y = \begin{cases} \pm\sqrt{\frac{5}{8} + \frac{1}{8}\sqrt{5}} & \text{si } x = -\frac{1}{4} + \frac{1}{4}\sqrt{5}, \text{ et} \\ \pm\sqrt{\frac{5}{8} - \frac{1}{8}\sqrt{5}} & \text{si } x = -\frac{1}{4} - \frac{1}{4}\sqrt{5}. \end{cases}$$

Les racines 5-ièmes de l'unité sont donc les nombres complexes suivants

$$1, \quad -\frac{1}{4} + \frac{1}{4}\sqrt{5} \pm i\sqrt{\frac{5}{8} + \frac{1}{8}\sqrt{5}} \quad \text{et} - \frac{1}{4} - \frac{1}{4}\sqrt{5} \pm i\sqrt{\frac{5}{8} - \frac{1}{8}\sqrt{5}}.$$

Proposition 2.5.8. *Soit $n \in \mathbb{N}$. Les racines n-ièmes de l'unité sont*

$$e^{\frac{0i\pi}{n}} = 1,\ e^{\frac{2i\pi}{n}},\ e^{\frac{4i\pi}{n}}, \ldots,\ e^{\frac{2i(n-1)\pi}{n}}.$$

Démonstration. Vérifions d'abord que chacun des nombres complexes de la liste est bien une racine n-ième de l'unité. L'élément général de la liste est $\exp(\frac{2ik\pi}{n})$, où k est un entier naturel positif et inférieur à $n - 1$. Or,

$$\left(e^{\frac{2ik\pi}{n}}\right)^n = e^{\frac{2ikn\pi}{n}} = e^{2ik\pi} = 1,$$

quel que soit $k \in \{0, \ldots, n-1\}$. Donc, les nombres complexes de la liste ci-dessus sont bien des racines n-ièmes de l'unité.

Il reste à montrer qu'il n'y a pas d'autre racine n-ième de l'unité. Supposons que $z \in \mathbb{C}$ est une racine n-ième de l'unité, i.e., $z^n = 1$. Ecrire z sous la forme trigonométrique : $z = r\exp(i\theta)$, où $r \in \mathbb{R}^+$ et $\theta \in \mathbb{R}$. Comme $z^n = 1$, on a

$$1 = z^n = \left(re^{i\theta}\right)^n = r^n e^{in\theta}.$$

On en déduit que $r^n = 1$ et que $n\theta \equiv 0 \mod 2\pi$. Comme r est un nombre réel positif, $r^n = 1$ implique que $r = 1$. Par ailleurs, $n\theta \equiv 0 \mod 2\pi$ veut dire qu'il existe un entier relatif ℓ tel que $n\theta = 2\ell\pi$. On en déduit que $\theta = \frac{2\ell\pi}{n}$. Effectuons la division euclidienne de ℓ par n pour obtenir $\ell = qn + k$, où q est le quotient de la division de ℓ par n, et k est le reste. En paticulier, q et k sont des entiers relatifs et, de plus, $0 \leq k < n - 1$. Du coup,

$$z = re^{i\theta} = 1 \cdot e^{\frac{2i\ell\pi}{n}} = e^{\frac{2i(qn+k)\pi}{n}} = e^{2iq\pi + \frac{2ik\pi}{n}} = e^{2iq\pi} \cdot e^{\frac{2ik\pi}{n}} = e^{\frac{2ik\pi}{n}}.$$

Comme $k \in \{0, \ldots, n-1\}$, le nombre complexe z en est bien un de la liste ci-dessus. □

Exemple 2.5.9. 1. Les racines 6-ièmes de l'unité sont $e^{\frac{2ik\pi}{6}}$, pour $k = 0, \ldots, 5$. Donc, les racines 6-ième de l'unité sont

$$1,\ \tfrac{1}{2}+\tfrac{1}{2}i\sqrt{3},\ -\tfrac{1}{2}+\tfrac{1}{2}i\sqrt{3},\ -1,\ -\tfrac{1}{2}-\tfrac{1}{2}i\sqrt{3},\ \tfrac{1}{2}-\tfrac{1}{2}i\sqrt{3}.$$

2. Les racines 8-ième de l'unité sont ± 1, $\pm i$ et $\pm\frac{1}{2}\sqrt{2}\pm\frac{1}{2}i\sqrt{2}$.
3. Les racines 5-ièmes de l'unité sont

$$1,\ e^{\frac{2i\pi}{5}},\ e^{\frac{4i\pi}{5}},\ e^{\frac{6i\pi}{5}},\ e^{\frac{8i\pi}{5}}.$$

On déduit d'Exemple 2.5.7.4 que

$$e^{\frac{2i\pi}{5}} = -\frac{1}{4}+\frac{1}{4}\sqrt{5}+i\sqrt{\frac{3}{8}-\frac{1}{8}\sqrt{5}}.$$

D'où $\cos(\frac{2\pi}{5}) = -\frac{1}{4}+\frac{1}{4}\sqrt{5}$ et $\sin(\frac{2\pi}{5}) = \sqrt{\frac{5}{8}+\frac{1}{8}\sqrt{5}}$.

Proposition 2.5.10. *Soit $\alpha \in \mathbb{C}^\star$. Ecrire $\alpha = re^{i\theta}$. Les racines n-ièmes de α sont les nombres complexes*

$$r^{\frac{1}{n}} \cdot e^{i\frac{\theta}{n}} \cdot e^{\frac{2ik\pi}{n}},$$

pour $k = 0, \ldots, n-1$.

Exemple 2.5.11. Les racines 6-ièmes de $64 = 2^6$ sont

$$2,\ 1+i\sqrt{3},\ -1+i\sqrt{3},\ -2,\ -1-i\sqrt{3},\ 1-i\sqrt{3}.$$

Chapitre 3

Arithmétique des entiers relatifs

3.1 La division euclidienne

Définition 3.1.1. Soient $a, b \in \mathbb{Z}$. On dit que a *divise* b dans $\mathbb{Z}$, ou que a est un *diviseur* de b dans $\mathbb{Z}$, s'il existe $c \in \mathbb{Z}$ tel que $ca = b$. On dit aussi que b est un *multiple* de a dans $\mathbb{Z}$, lorsque a divise b dans $\mathbb{Z}$. Si a divise b dans $\mathbb{Z}$, on écrit $a|b$.

Exemples 3.1.2. 1. L'entier relatif -3 divise 12 car $(-4) \times (-3) = 12$ et $-4 \in \mathbb{Z}$.

2. L'entier relatif -3 ne divise pas 16. En effet, supposons qu'il existe $c \in \mathbb{Z}$ tel que $c \times (-3) = 16$. Comme $(-5) \times (-3) = 15$ et $(-6) \times (-3) = 18$, on voit que $-6 < c < -5$ ce qui est absurde pour un entier relatif c.

3. Les entiers relatifs 1 et -1 divisent tout autre entier relatif.

4. Tout entier relatif divise 0. Le seul entier relatif divisible par 0 est 0 lui-même.

Dans la suite on sera amené à déterminer l'ensemble de tous les diviseurs d'un entier relatif donné. Les deux propositions suivantes seront utiles pour ça.

Proposition 3.1.3. *Soient $a, b \in \mathbb{Z}$, avec $b \neq 0$, tel que a divise b. Alors $|a| \leq |b|$.*

Démonstration. Comme a divise b il existe $c \in \mathbb{Z}$ tel que $ca = b$. Comme $b \neq 0$, on a $c \neq 0$, et donc $1 \leq |c|$. Du coup, $|a| \leq |c| \cdot |a| = |ca| = |b|$. □

Soit $n \in \mathbb{N}$, rappelons que $\lfloor \sqrt{n} \rfloor$ désigne la partie entière de la racine carrée du nombre réel $\sqrt{n}$. Autrement dit, $\lfloor \sqrt{n} \rfloor$ est le plus grand entier naturel m tel que $m^2 \leq n$.

Proposition 3.1.4. *Soit $b \in \mathbb{Z}^\star$. Supposons que $a, c \in \mathbb{Z}$ satisfont $ca = b$. Alors, $|a| \leq \lfloor\sqrt{|b|}\rfloor$ ou $|c| \leq \lfloor\sqrt{|b|}\rfloor$.*

Démonstration. Supposons que $|a| > \lfloor\sqrt{|b|}\rfloor$. Dans ce cas $|a| > \sqrt{|b|}$. En multipliant par $|c|$ on a $|c| \cdot \sqrt{|b|} < |c| \cdot |a| = |b|$. En divisant par $\sqrt{|b|}$, on obtient $|c| < \sqrt{|b|}$. Du coup, $|c| \leq \lfloor\sqrt{|b|}\rfloor$. □

Exemple 3.1.5. Déterminons l'ensemble des diviseurs de l'entier 48. Comme $\lfloor\sqrt{48}\rfloor = 6$, il suffit de chercher les diviseurs de 48 parmi les entiers

$$\pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6.$$

Les autres diviseurs s'obtiennent en divisant 48 par ceux-ci, d'après Proposition 3.1.4. Or, les diviseurs de 48 parmi $\pm 1, \ldots, \pm 6$ sont $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6$. Du coup, les diviseurs de 48 sont

$$\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 16, \pm 24, \pm 48.$$

Proposition 3.1.6. *Soient $a, b, c \in \mathbb{Z}$.*

1. *$a|a$.*
2. *Si $a|b$ et $b|a$, alors $a = b$ ou $a = -b$.*
3. *Si $a|b$ et $b|c$, alors $a|c$.*
4. *Si $a|b$ et $a|c$, alors $a|b + c$.*
5. *Si $a|b$, alors $ca|cb$.*

Démonstration. 1. Comme $1 \cdot a = a$ et $1 \in \mathbb{Z}$, l'entier a divise bien lui-même.

2. Supposons que $a|b$ et que $b|a$. Comme $a|b$, il existe $c \in \mathbb{Z}$ tel que $ca = b$. Comme $b|a$, il existe $d \in \mathbb{Z}$ tel que $db = a$. Du coup, $a = db = dca$. Il vient que $(dc - 1)a = 0$. Comme $\mathbb{Z}$ est intègre, $dc - 1 = 0$ ou $a = 0$. Si $a = 0$, on a aussi $b = ca = 0$. Donc, si $a = 0$, on a bien $a = b$. On peut donc supposer que $a \neq 0$. On a donc $dc = 1$. Comme $d, c \in \mathbb{Z}$, on a $d = \pm 1$ et $c = \pm 1$. Comme $a = db$, on a bien $a = b$ ou $a = -b$.

3. Supposons que $a|b$ et que $b|c$. Comme $a|b$, il existe $d \in \mathbb{Z}$ tel que $da = b$. Comme $b|c$, il existe $e \in \mathbb{Z}$ tel que $eb = c$. Du coup, $(ed)a = e(da) = eb = c$. Comme $ed \in \mathbb{Z}$, on en déduit que $a|c$.

4. Supposons que $a|b$ et que $a|c$. Il existe donc $d, e \in \mathbb{Z}$ tels que $da = b$ et $ea = c$. Du coup, $(d + e)a = da + ea = b + c$. Comme $d + e \in \mathbb{Z}$, on a bien $a|b + c$.

5. Supposons que $a|b$. Il existe donc $d \in \mathbb{Z}$ tel que $da = b$. Du coup, en multipliant par c, on a $d(ca) = c(da) = cb$. Comme $d \in \mathbb{Z}$, on a bien $ca|cb$. □

La division euclidienne permettra de décider rapidement si un entier relatif en divise un autre.

Théorème (la division euclidienne). *Soient $a, b \in \mathbb{Z}$ avec $a \neq 0$. Il existe $q, r \in \mathbb{Z}$ tels que $b = qa + r$, où $0 \leq r < |a|$. De plus, q et r sont uniquement déterminés par ces conditions.*

Démonstration. Soit R le sous-ensemble de $\mathbb{N}$ défini par

$$R = \{b - qa \,|\, q \in \mathbb{Z} \text{ avec } b - qa \in \mathbb{N}\}.$$

Comme $a \neq 0$, il existe $q \in \mathbb{Z}$ tel que $qa \leq b$. Du coup, $b - qa \geq 0$ et le sous-ensemble R de $\mathbb{N}$ n'est pas vide. Comme $\mathbb{N}$ est bien ordonné, le sous-ensemble R admet un plus petit élément qu'on appelle r. Comme $r \in R$, il existe, de plus, $q \in \mathbb{Z}$ tel que $b - qa = r$.

Montrons que $0 \leq r < |a|$. Comme $r \in R \subseteq \mathbb{N}$, ona $r \geq 0$. Pour montrer que $r < |a|$, supposons, par l'absurde, que $r \geq |a|$. Soit $s = 1$ si $a > 0$, et $s = -1$ si $a < 0$. On a $|a| = sa$ et

$$b - (q + s)a = b - qa - sa = r - |a| \geq 0.$$

Donc $b - (q + s)a \in R$. Mais $b - (q + s)a = r - |a| < r$ ce qui contredit le fait que r soit le plus petit élément de R. Par conséquent $r < |a|$. Cela montre l'existence de q et r.

Pour montrer l'unicité de q et r, supposons que

$$b = qa + r \quad \text{et que} \quad b = q'a + r',$$

où $q, q', r, r' \in \mathbb{Z}$, $0 \leq r < |a|$ et $0 \leq r' < |a|$. On montre que $q = q'$ et que $r = r'$. Or, on a $qa + r = q'a + r'$. D'où $qa - q'a = r' - r$, ou encore $r' - r = (q - q')a$. Comme $0 \leq r < |a|$ et $0 \leq r' < |a|$, on a $r' - r < |a| - r < |a|$ et, de même $r - r' < |a|$. D'où $|r' - r| < |a|$ et

$$|(q - q')| \cdot |a| = |(q - q')a| = |r' - r| < |a|.$$

Il s'ensuit que $q - q' = 0$, i.e. $q = q'$. Du coup $r' - r = 0$, et $r = r'$. □

Définition 3.1.7. Soient $a, b \in \mathbb{Z}$ avec $a \neq 0$. Soient $q, r \in \mathbb{Z}$ tels que $b = qa + r$ avec $0 \leq r < |a|$. On dit que q est le *quotient* de la division euclidienne de b par a, et que r est le *reste* de la division euclidienne de b par a. L'entier b est la *dividende* et l'entier a est le *diviseur* dans la division euclidienne de b par a.

Exemples 3.1.8. 1. Effectuons la division euclidienne de 365 par 7. On écrit $365 = 50 \times 7 + 15 = 50 \times 7 + 2 \times 7 + 1 = 52 \times 7 + 1$. Le quotient est donc égal à 52, le reste est égal à 1.

2. Effectuons la division euclidienne de -365 par 7. Comme $365 = 52 \times 7 + 1$, on a $-365 = (-52) \times 7 - 1 = (-51) \times 7 + 6$. Le quotient est donc égal à -51, le reste est égal à 6.

3. Effectuons la division euclidienne de 365 par -7. Comme $-365 = (-51) \times 7 + 6$, on a aussi $-365 = 51 \times (-7) + 6$, Le quotient est donc 51, le reste est 6.

4. Effectuons la division euclidienne de -365 par -7. Comme $365 = 52 \times 7 + 1$, on a $-365 = 52 \times (-7) - 1 = 53 \times (-7) + 6$. Le quotient est donc 53, le reste est 6.

Proposition 3.1.9. *Soient $a, b \in \mathbb{Z}$ avec $a \neq 0$. Soit r le reste de la division euclidienne de b par a. Alors, a divise b si et seulement si $r = 0$.*

Démonstration. Supposons que a divise b. Il existe donc $c \in \mathbb{Z}$ tel que $ca = b$. Du coup $b = ca + 0$. D'après l'unicité de la division euclidienne, on a $r = 0$.

Réciproquement, supposons que $r = 0$. Soit q le quotient de la division euclidienne de b par a. On a $b = qa + r$. Comme $r = 0$, on a $b = qa$. Comme $q \in \mathbb{Z}$, cela montre que a divise b. □

Exemple 3.1.10. Dans Exemple 3.1.2.2 on a montré de manière délibérément élémentaire que -3 ne divise pas 16. Maintenant, avec le critère de la proposition précédente en mains, on peut montrer plus facilement que -3 ne divise pas 16. En effet, il faut effectuer la division euclidienne de 16 par -3 pour obtenir $16 = (-5) \times (-3) + 1$. Comme le reste vaut 1 et est non nul, -3 ne divise pas 16.

Cet exemple montre comment on se sert de la division euclidienne pour montrer qu'un entier en divise un autre. Comme on sait, la division euclidienne s'effectue très rapidement par le bias de la divisison longue, dès qu'on dispose de l'écriture décimal, ou l'écriture en base quelconque, des diviseur et dividende. L'existence et unicité de cette écriture sont également conséquences de la division euclidienne :

Théorème 3.1.11. *Soit $b \in \mathbb{N}$, avec $b \geq 2$. Pour tout $a \in \mathbb{N}^\star$ il existe $n \in \mathbb{N}$ et $a_0, \ldots, a_n \in \{0, 1, 2, \ldots, b-1\}$, avec $a_n \neq 0$, tels que*

$$a = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0.$$

De plus, les entiers n et $a_0, \ldots, a_n$ sont ainsi uniquement déterminés par a.

Démonstration. Par récurrence généralisé sur a. L'énoncé, i.e., l'existence et l'unicité, est clair pour $a = 1$. Soit maintenant $a \in \mathbb{N}$, avec $a \geq 2$, quelconque, et supposons que l'énoncé est vrai pour tout entier naturel non nul$a' < a$. Effectuons la division euclidienne de a par b. Soient a' le quotient et a_0 le reste. On a $a = a'b + a_0$, où $a_0 \in \{0, \ldots, b-1\}$ et $a' \in \mathbb{N}$. Comme $b \geq 2$, on a $a' < a$. Si $a' = 0$, on a $a = a_0$ ce qui montre bien l'énoncé dans ce cas. On peut donc supposer que $a' \neq 0$. Appliquons-lui l'hypothèse de récurrence : il existe des entiers naturels $n \in \mathbb{N}$ et $a_1, \ldots, a_n \in \{0, \ldots, b-1\}$, avec $a_n \neq 0$, tels que

$$a' = a_n b^{n-1} + a_{n-1} b^{n-2} + \cdots + a_2 b + a_1.$$

En multipliant par b et en rajoutant a_0, on obtient

$$a = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_2 b^2 + a_1 b + a_0$$

comme voulu. Cela montre l'existence pour a. Pour montrer l'unicité, supposons que $m \in \mathbb{N}$ et $a'_0, \ldots, a'_m \in \{0, \ldots, b-1\}$, avec $a'_m \neq 0$, sont tels que

$$a = a'_m b^m + a'_{m-1} b^{m-1} + \cdots + a'_1 b + a'_0.$$

En écrivant cette égalité sous la forme

$$a = (a'_m b^{m-1} + a'_{m-1} b^{m-2} + \cdots + a'_1) b + a'_0,$$

on voit que a'_0 est le reste et $a'_m b^{m-1} + \cdots + a'_1$ est le quotient dans la division euclidienne de a par b. D'où $a'_0 = a_0$ et $a' = a'_m b^{m-1} + \cdots + a'_1$. D'après l'hypothèse de récurrence, $m = n$, $a'_n = a_n$, ..., $a'_1 = a_1$. Cela montre l'unicité. □

Définition 3.1.12. Soit $b \in \mathbb{N}$ avec $b \geq 2$, et $a \in \mathbb{N}^\star$. Soient $n \in \mathbb{N}$ et $a_0, \ldots, a_n$ comme dans Théorème 3.1.11. *L'écriture de a en base b* est la suite $a_n a_{n-1} \cdots a_0$.

Exemple 3.1.13. 1. Comme on a tendance à identifier un entier avec son écriture décimale, on cherchera, à titre d'exemple, l'écriture décimale d'un entier en chiffres romains. On va déterminer l'écriture décimale de CCCLXV. Or,

$$\text{CCCLXV} = 300 + 50 + 10 + 5 = 3 \times 100 + 6 \times 10 + 5.$$

L'écriture décimale ed CCCLXV est donc 365.

2. Cherchons l'écriture de l'entier CCCLXV en base 7. On suit la démonstration du Théorème de l'écriture en base b pour l'obtenir, et on utilise

l'écriture de CCCLXV en base 10 qu'on vient de déterminer. On fait des divisions euclidiennes successives par 7 :

$$365 = 52 \times 7 + 1 = (7 \times 7 + 3) \times 7 + 1 = \\ = ((1 \times 7 + 0) \times 7 + 3) \times 7 + 1 = 1 \times 7^3 + 0 \times 7^2 + 3 \times 7 + 1.$$

L'écriture de CCCLXV en base 7 est donc 1031.

Une autre application de la division euclidienne est l'énoncé suivant.

Proposition 3.1.14. *Soit $n \in \mathbb{N}^\star$. L'ensemble des entiers relatifs $\mathbb{Z}$ contient exactement n classes de congruence modulo n :*

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

Démonstration. Montron d'abord que les classes $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ sont 2-à-2 distinctes. En effet, si $\overline{k} = \overline{m}$, où $k, m \in \{0, \ldots, n-1\}$, on a, en particulier, que $k \equiv m \mod n$. Donc n divise $k - m$. Soit $q \in \mathbb{Z}$ tel que $k - m = qn$. Comme $k, m \in \{0, \ldots, n-1\}$, on a $k - m \leq n - 1$ et $k - m \geq -(n-1)$. D'où $-(n-1) \leq qn \leq n - 1$. Il s'ensuit que $q = 0$ et que $k = m$. Par conséquent, les classes $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ sont bien 2-à-2 distinctes.

Montrons, ensuite, qu'il n'y a pas d'autre classe de congruence modulo n. En effet, soit $\overline{m}$ une classe de congruence modulo n, où $m \in \mathbb{Z}$. Effectuons la division euclidienne de m par n pour obtenir $m = qn + r$, où $q, r \in \mathbb{Z}$ avec $0 \leq r < n$. La différence $m - r$ est donc un multiple de n, i.e. $m \equiv r \mod n$. Du coup $m \in \overline{r}$, et il vient que $\overline{m} = \overline{r}$ d'après Proposition 1.5.10. Comme r satisfait $0 \leq r < n$, on a $r \in \{0, 1, \ldots, n-1\}$. Par conséquent, la classe $\overline{m}$ est bien égale à l'une des classes $\overline{0}, \overline{1}, \ldots, \overline{n-1}$. □

3.2 Le plus grand diviseur commun

Définition 3.2.1. Soient $a, b \in \mathbb{Z}$. Un entier relatif c est un *diviseur commun* de a et b si et seulement si $c|a$ et $c|b$. Un entier relatif c est un *plus grand* diviseur commun de a et b si les conditions suivantes sont vérifiées :

1. c est un diviseur commun de a et b, et
2. pour tout diviseur commun d de a et b, on a $d|c$.

On écrit $c = \text{pgcd}(a, b)$ pour dire que c est un plus grand diviseur commun de a et b.

Exemple 3.2.2. 1. Les diviseurs de 4 sont $\pm 1, \pm 2, \pm 4$. Le diviseurs de 6 sont $\pm 1, \pm 2, \pm 3, \pm 6$. Donc, les diviseurs communs de 4 et 6 sont $\pm 1, \pm 2$. Par conséquent, 2 et -2 sont les plus grands diviseurs communs de 4 et 6.

2. Déterminons les diviseurs communs de 48 et 30. On a vu dans Exemple 3.1.5, que les diviseurs de 48 sont

$$\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 16, \pm 24, \pm 48.$$

Parmi ces entiers, seulement les entiers $\pm 1, \pm 2, \pm 3, \pm 6$ divisent 30. Ces entiers-là sont donc les diviseurs communs de 48 et 30. Comme tous ces entiers divisent ± 6, on voit que ± 6 sont les plus grand diviseurs communs de 48 et 30.

3. $\text{pgcd}(a, 0) = a$, $\text{pgcd}(0, b) = b$ et $\text{pgcd}(0, 0) = 0$.

Proposition 3.2.3. *Soient $a, b \in \mathbb{Z}$. Si a et b admettent un plus grand diviseur commun, alors il est unique à signe près.*

Démonstration. Supposons que c et c' sont des plus grands diviseurs communs de a et b. Comme c est un plus grand diviseur commun et comme c' est un diviseur commun de a et b, l'entier c' divise c. Par symétrie, ou par un même argument, c divise c'. D'où $c' = \pm c$. □

L'énoncé suivant affirme que deux entiers relatifs admettent un plus grand diviseur commun. De plus, il donne un algorithme pour le déterminer, qui est bien plus rapide que la méthode suivie dans Exemple 3.2.2.2

Théorème (l'Algorithme d'Euclide). *Soient $a, b \in \mathbb{Z}$ avec $b \neq 0$. On pose $r_{-1} = a$, $r_0 = b$, et, par récurrence, r_i est le reste de la division euclidienne de r_{i-2} par r_{i-1}, pour $i = 1, 2, 3, \ldots$ tant que $r_{i-1} \neq 0$. Soit n l'unique entier naturel tel que $r_{n-1} \neq 0$ et $r_n = 0$. Alors, r_{n-1} est un plus grand diviseur commun de a et b.*

Démonstration. Remarquons qu'il existe bien en entier naturel $n \in \mathbb{N}$ tel que $r_n = 0$, sinon on aurait une suite infini d'entiers naturels

$$r_1 > r_2 > r_3 > \cdots$$

ce qui est absurde.

Soit c un entier relatif. Soit $i \in \{0, \ldots, n\}$. Par définition de r_i, on a

$$r_{i-2} = q_i r_{i-1} + r_i,$$

où q_i est le quotient de la division euclidienne de r_{i-2} par r_{i-1}. On voit que c divise r_{i-2} lorsque c divise r_{i-1} et r_i. On a aussi

$$r_i = r_{i-2} - q_i r_{i-1}.$$

D'où c divise r_i lorsque c divise r_{i-2} et r_{i-1}. Il s'ensuit que c est un diviseur commun de r_{i-2} et r_{i-1} si et seulement si c est un diviseur commun de r_{i-1} et r_i. On montre alors facilement, par récurrence sur i, que a et b ont les mêmes diviseurs communs que r_{i-1} et r_i, pour $i = 0, \ldots, n$. En particulier, a et b ont les mêmes diviseurs communs que r_{n-1} et r_n. Comme $r_n = 0$, les diviseurs communs de r_{n-1} et r_n sont les diviseurs de r_{n-1}. Donc, r_{n-1} et r_n admettent un plus grand diviseur commun, à savoir $\pm r_{n-1}$, et de plus, ce plus grand diviseur commun est aussi plus grand diviseur commun de a et b. □

Exemple 3.2.4. Déterminons le pgcd de 48 et 30 en effectuant l'algorithme d'Euclide :

$$\begin{aligned} 48 &= 1 \times 30 + 18 \\ 30 &= 1 \times 18 + 12 \\ 18 &= 1 \times 12 + 6 \\ 12 &= 2 \times 6 + 0. \end{aligned}$$

D'où $\text{pgcd}(48, 30) = 6$.

Théorème (l'Algorithme d'Euclide étendu). *Soient $a, b \in \mathbb{Z}$. On pose $r_{-1} = a$, $r_0 = b$, et, par récurrence, r_i est le reste de la division euclidienne de r_{i-2} par r_{i-1}, pour $i = 1, 2, 3, \ldots$ tant que $r_{i-1} \neq 0$. Soit n l'unique entier naturel tel que $r_{n-1} \neq 0$ et $r_n = 0$. Soit q_i le quotient de la division euclidienne de r_{i-2} par r_{i-1}, pour $i = 1, \ldots, n$. Soient $u_{-1} = 1$, $u_0 = 0$, $v_{-1} = 0$ et $v_0 = 1$. Définir u_i et v_i par récurrence pour $i = 1. \ldots, n-1$ par*

$$u_i = u_{i-2} - q_i u_{i-1} \quad \text{et} \quad v_i = v_{i-2} - q_i v_{i-1}.$$

Alors, r_{n-1} est un plus grand diviseur commun de a et b et

$$u_{n-1}a + v_{n-1}b = r_{n-1}.$$

Démonstration. On sait déjà que r_{n-1} est un plus grand diviseur commun de a et b. Montrons, par récurrence, que

$$u_i a + v_i b = r_i,$$

pour $i = -1, 0, 1, \ldots, n-1$. Par définition, c'est vrai pour $i = -1$ et $i = 0$. Supposons que c'est vrai jusqu'au rang $i-1$, pour un certain $i \geq 1$ et $\leq n-1$. Alors,

$$\begin{aligned} u_i a + v_i b &= (u_{i-2} - q_i u_{i-1})a + (v_{i-2} - q_i v_{i-1})b = \\ &= (u_{i-2}a + v_{i-2}b) - q_i(u_{i-1}a + v_{i-1}b) = \\ &= r_{i-2} - q_i r_{i-1} = r_i. \end{aligned}$$

On en déduit que, pour $i = n-1$, on a $u_{n-1}a + v_{n-1}b = r_{n-1}$. □

Exemple 3.2.5. On a vu que $\text{pgcd}(48, 30) = 6$. Déterminons des entiers relatifs u et v tels que $u \times 48 + v \times 30 = 6$. On effectue l'alogorithme d'Euclide étendu :

i	r_{i-2}	r_{i-1}	q_i	r_i	u_i	v_i
-1					1	0
0					0	1
1	48	30	1	18	1	-1
2	30	18	1	12	-1	2
3	18	12	1	6	2	-3
4	12	6	2	0		

Donc $u = 2$ et $v = -3$ conviennent, i.e., $2 \times 48 + (-3) \times 30 = 6$. Il faut noter que d'autres solutions existent, comme $u = -3$ et $v = 5$ ou encore $u = 7$ et $v = -11$, etc. En fait, l'équation $48 \times u + 30 \times v = 6$ admet une finitié de soltuions $(u, v) \in \mathbb{Z} \times \mathbb{Z}$. On verra au paragraphe 3.6 comment déterminer l'ensemble de toutes les solutions de cette équation dans $\mathbb{Z} \times \mathbb{Z}$.

Théorème de Bézout. *Soient $a, b \in \mathbb{Z}$. Soit c un diviseur commun de a et b. Alors, c est un plus grand diviseur commun de a et b si et seulement s'il existe des entiers relatifs u, v tels que*

$$ua + vb = c.$$

Démonstration. Supposons qu'il existe $u, v \in \mathbb{Z}$ tels que $ua + vb = c$. Montrons que c est un plus grand diviseur commun de a et b. D'après l'hypothèse, c est un diviseur commun de a et b. Montrons que tout autre diviseur commun de a et b divise c. Soit donc d un diviseur commun de A et b. Comme d divise a et b, d divise ua et vb, donc aussi leur somme $ua + vb = c$. Cela montre que c est un plus grand diviseur commun de a et b.

Réciproquement, supposons que c est un plus grand diviseur commun de a et b. D'après l'Algorithme étendu d'Euclide, il existe un plus grand diviseur commun d de a et b et des entiers relatifs u et v tels que $ua + vb = d$. Comme d est un plus grand diviseur commun de a et b, et comme c est un diviseur commun de a et b, c divise d. de même, d divise c, i.e., $c = \pm d$. Par conséquent, quitte à multiplier u et v par -1, il existe des entiers relatifs u et v tels que $ua + bv = c$. □

Proposition 3.2.6. *Soient $a, b, c \in \mathbb{Z}$. On a* $\text{pgcd}(ab, ac) = a\text{pgcd}(b, c)$.

Démonstration. Soit d le pgcd de b et c. Le produit ad est bien un diviseur commun de ab et ac. D'après le Théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tel que $ub + vc = d$. Du coup, $u(ab) + v(ac) = ad$. D'après le Théorème de Bézout, $\text{pgcd}(ab, ac) = ad$. □

La proposition précédente nous donne encore une autre manière de déterminer le pgcd de deux entiers, lorsqu'on voit que ceux-ci ont des diviseurs communs non triviaux.

Exemple 3.2.7. Déteminons encore une fois le pgcd de 48 et 30. On voit tout de suite que 2 est un diviseur commun de 48 et 30. On a donc $\text{pgcd}(48, 30) = \text{pgcd}(2 \times 24, 2 \times 15) = 2 \times \text{pgcd}(24, 15)$, d'après Proposition 3.2.6. Ensuite, on voit tout de suite que 24 et 15 sont tous les deux divisible par 3. D'où $\text{pgcd}(24, 15) = \text{pgcd}(3 \times 8, 3 \times 5) = 3 \times \text{pgcd}(8, 5)$. Comme le pgcd de 8 et 5 est clairement égal à 1, on a, de nouveau, $\text{pgcd}(48, 30) = 2 \times 3 = 6$.

Définition 3.2.8. Soient $a, b \in \mathbb{Z}$. On dit que a et b sont *premiers entre eux* si les seuls diviseurs communs de a et b sont ± 1. De manière équivalente, a et b sont premiers entre eux si le plus grand diviseur commun de a et b vaut 1.

Corollaire 3.2.9. *Soient $a, b \in \mathbb{Z}$. Les entiers relatifs a et b sont premiers entre eux si et seulement s'il existe des entiers relatifs u et v tels que*

$$ua + vb = 1.$$

Démonstration. Supposons qu'il existe $u, v \in \mathbb{Z}$ tels que $ua + vb = 1$. Comme 1 est un diviseur commun de a et b, 1 est un plus grand diviseur commun d'après le Théorème de Bézout. Par conséquent, a et b sont premiers entre eux.

Réciproquement, supposons que a et b sont premiers entre eux. Cela veut dire que 1 est un plus grand diviseur commun de a et b. D'après le Théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que $ua + vb = 1$. □

Exemple 3.2.10. Montrer que $\text{pgcd}(231, 65) = 1$ et trouver $u, v \in \mathbb{Z}$ tels que $231 \times u + 65 \times v = 1$. On effectue l'Algorithme d'Euclide étendu :

i	r_{i-2}	r_{i-1}	q_i	r_i	u_i	v_i
-1					1	0
0					0	1
1	231	65	3	36	1	-3
2	65	36	1	29	-1	4
3	36	29	1	7	2	-7
4	29	7	4	1	-9	32
5	7	1	7	0		

Donc $\text{pgcd}(231, 65) = 1$ et on a $-9 \times 231 + 32 \times 65 = 1$. De nouveau, la solution $u = -9$ et $v = 32$ est loin d'être unique.

Voci une application importante de Théorème de Bézout, ou plutôt de son corollaire.

Lemme de Gauss. *Soient $a, b, c \in \mathbb{Z}$ tels que a divise bc. Si a et b sont premiers entre eux, alors a divise c.*

Démonstration. Comme a et b sont premiers entre eux, il existe $u, v \in \mathbb{Z}$ tels que $ua+vb = 1$. Mulitplier cette équation par c donne $uac+vbc = c$. Comme a divise uac et a divise vbc par hypothèse, a divise leur somme qui est égale à c. □

Comme application du plus grand diviseur commun de deux entiers, on peut démontrer que tout nombre rationnel s'écrit de manière unique comme *fraction simple*, i.e., de la forme a/b où a et b sont des entiers relatifs premiers entre eux.

Proposition 3.2.11. *Soit $x \in \mathbb{Q}$. Il existe un unique couple (a, b) où $a \in \mathbb{Z}$, $b \in \mathbb{N}^\star$, avec a et b premiers entre eux et $x = a/b$.*

Démonstration. Montrons d'abord l'existence d'un tel couple. Comme x est un nombre rationnel, il existe $a \in \mathbb{Z}$ et $b \in \mathbb{N}$, avec $b \neq 0$, tels que $x = a/b$. Soit $c = \text{pgcd}(a, b)$. On peut supposer que c est positif, quitte à remplacer c par $-c$ si nécessaire. Ecrire $a = ca'$ et $b = cb'$, où $a' \in \mathbb{Z}$ et $b' \in \mathbb{N}$, avec $b' \neq 0$. On a $x = a'/b'$ et $\text{pgcd}(a', b') = 1$. Cela montre l'existence.

Quand à l'unicité, supposons qu'il existe encore un couple (r, s), où $r \in \mathbb{Z}$, $s \in \mathbb{N}$, avec $s \neq 0$ et r et s premiers entre eux, tels que $x = r/s$. On a donc $a/b = r/s$, i.e., $as = br$. En particulier, s divise br. Comme s et r sont premiers entre eux, s divise b, d'après le Lemme de Gauss. Par la même argument, b divise s. Comme b et s sont des entiers naturels, on en déduit que $b = s$. Du coup $as = br = sr$. Comme $s \neq 0$, on a aussi $a = r$. Cela montre l'unicité. □

3.3 Nombres premiers

Définition 3.3.1. Soit $a \in \mathbb{Z}$ avec $a \neq -1, 0, 1$. L'entier a est *premier* si les seuls diviseurs de a sont les entiers ± 1 et $\pm a$. De manière équivalente, a est premier si $a = bc$, avec $b, c \in \mathbb{Z}$, implique que $b = \pm 1$ ou $c = \pm 1$.

Exemple 3.3.2. 1. Les entiers 2, 3, 5, 7, et 11 sont des nombres premiers, ainsi que leurs opposées -2, -3, -7, et -11. L'entier 1 n'est pas un nombre premier.

2. Déterminons si 161 est un nombre premier. Le plus grand entier m tel que $m^2 \leq 161$ est l'entier $m = 12$. En effet, $12^2 = 144 \leq 161$ et

$13^2 = 169 > 161$. D'après Proposition 3.1.4, il suffit de vérifier si l'un des entiers $2, 3, 4, \ldots, 12$ divisent 161. Or, 2 ne divise pas 161 car $161 = 80 \times 2 + 1$. L'entier 3 ne divise pas 161 car $161 = 53 \times 3 + 2$. L'entier 4 ne divise pas 161, sinon 2 le diviserait aussi. Comme $161 = 32 \times 5 + 1$, l'entier 5 ne divise pas 161 non plus. L'entier 6 ne divise pas 161, sinon 2 le diviserait aussi. Par contre, $161 = 23 \times 7 + 0$. Donc, 7 divise 161. L'entier 161 n'est donc pas premier.

3. Déterminons si 401 est premier ou pas. D'après Proposition 3.1.4, il suffit de vérifier si l'un des entiers $2, 3, 4, \ldots, 20$ divise 401. En effectuant les division euclidiennes de 401 par $2, 3, 5, 7, 11, 13, 17, 19$ on obtient

$$\begin{aligned} 401 &= 200 \times 2 + 1 \\ 401 &= 133 \times 3 + 2 \\ 401 &= 80 \times 5 + 1 \\ 401 &= 57 \times 7 + 2 \\ 401 &= 36 \times 11 + 5 \\ 401 &= 30 \times 13 + 11 \\ 401 &= 23 \times 17 + 10 \\ 401 &= 21 \times 19 + 2 \end{aligned}$$

et on constate que 401 n'est pas divisible par l'un de ces entiers. Comme les autres entiers de la liste $2, 3, 4, \ldots, 20$ sont multiples de ceux-ci, ils ne divisent pas non plus 401. L'entier 401 est donc bien premier.

3. La crible d'Erastosthène.

Proposition 3.3.3. *Soit $n \in \mathbb{Z}$, $n \neq \pm 1$. Alors, il existe un nombre premier p divisant n.*

Démonstration. L'énoncé est trivialement vrai pour lorsque $n = 0$. Il suffit donc de le démontrer pour des entiers relatifs strictement positifs, i.e., pour tout $n \in \mathbb{N}$ avec $n \geq 2$. On le montre par l'absurde. Soit A le sous ensemble de $\mathbb{N}$ des entiers naturels $n \geq 2$ qui ne sont pas divisibles par un nombre premier. Par hypothèse, A est non vide. Comme $\mathbb{N}$ est bien ordonné, A contient un plus petit élément. Soit $n \in A$ le plus petit élément de A. Comme $n \in A$, l'entier n n'est divisible par aucun nombre premier. En particulier, n n'est pas premier, sinon, n, étant divisible par lui-même, serait divisible par un premier. Comme n n'est pas premier et $n \neq -1, 0, 1$, il existe des entiers relatifs a et b tels que $n = ab$ avec $a \neq \pm 1$ et $b \neq \pm 1$. Comme n est strictement positif, on peut supposer que a et b sont également strictement positifs. Comme $a, b \neq 1$, on a $a, b \geq 2$. Comme $ab = n$ et $b \geq 2$, on a $a < n$. Du coup, $a \notin A$ car n est le plus petit élément de A. Mais comme $a \geq 2$, l'entier a est donc divisible par un nombre premier p. Comme $n = ab$, l'entier n aussi est divisible par le nombre premier p. Contradiction car $n \in A$. □

Grâce à la proposition précédente, on a le critère de primalité suivant.

Proposition 3.3.4. *Soit $a \in \mathbb{Z}$, avec $a \neq -1, 0, 1$. Supposons que tous les nombres premiers p satisfaisant $2 \leq p \leq \lfloor\sqrt{|a|}\rfloor$ ne divisent pas a. Alors a est un nombre premier.*

Démonstration. Supposons que $a = bc$, où $b, c, \in \mathbb{Z}$. On doit montrer que $b = \pm 1$ ou $c = \pm 1$. Supposons, par l'absurde que $b \neq \pm 1$ et $c \neq \pm 1$. D'après Proposition 3.1.4, on a $|b| \leq \lfloor\sqrt{|a|}\rfloor$ ou $|c| \leq \lfloor\sqrt{|a|}\rfloor$. Quitte à échanger b et c si nécessaire, on peut supposer que $|b| \leq \lfloor\sqrt{|a|}\rfloor$. Comme $b \neq \pm 1$. Il existe un nombre premier p divisant b d'après Proposition 3.3.3. On peut supposer que p est positif. Du coup $p \geq 2$. Comme p divise b, on a $p \leq |b|$, d'après Proposition. Par conséquent, $p \leq \lfloor\sqrt{|a|}\rfloor$. Contradiction, car p divise b donc aussi a. □

Exemple 3.3.5. Montrons que 167 est premier. Comme $12^2 = 144 \leq 167$ et $13^2 = 169$, il suffit de vérifier que 167 n'est pas divisible par $2, 3, 5, 7, 11$. En effectuant les divisions euclidiennes de 167 par ces entiers-là on constate que, effectivement, 167 n'est pas divisible par $2, 3, 5, 7, 11$. D'après Proposition 3.3.4, 167 est premier.

Théorème d'Euclide. *Il y a une infinité de nombres premiers dans $\mathbb{Z}$.*

Démonstration. Supposons qu'il n'y avait qu'un nombre fini de nombres premiers $p_1, \ldots, p_n$ dans $\mathbb{Z}$, i.e., tout nombre premier dans $\mathbb{Z}$ est l'un de la liste $p_1, \ldots, p_n$. Soit $N = p_1 \cdots p_n + 1$. Comme $N \neq \pm 1$, il existe un nombre premier p divisant N, d'après Proposition 3.3.3. Comme p est premier, $p = p_i$ pour un certain indice $i \in \{1, \ldots, n\}$. Comme p divise $p_1 \cdots p_n$ et p divise N, p divise la différence $N - p_1 \cdots p_n = 1$. Contradiction. □

Voici la propriété clé d'un nombre premier.

Proposition 3.3.6. *Soient $a, b \in \mathbb{Z}$ et soit $p \in \mathbb{Z}$ un nombre premier. Si p divise ab, alors p divise a ou p divise b.*

Démonstration. Soit c le pgcd de a et p. Comme c divise p et p est premier, $c = \pm 1$ ou $c = \pm p$. Dans le deuxième cas, p divise a. Dans le premier cas, p et a sont premiers entre eux. D'après le Lemme de Gauss, p divise b. □

Comme application, on peut montrer l'énoncé suivant.

Proposition 3.3.7. $\sqrt{2} \notin \mathbb{Q}$.

Démonstration. Par l'absurde, supposons que $\sqrt{2} \in \mathbb{Q}$. D'après Proposition 3.2.11, il existe $a, b \in \mathbb{Z}$, avec $b \neq 0$ et a et b premiers entre eux, tels que $\sqrt{2} = a/b$. En prenant les carrés de deux côtés, on obtient $2 = a^2/b^2$, i.e., $2b^2 = a^2$. En particulier, 2 divise a^2. Comme 2 est premier, 2 divise a d'après Proposition 3.3.6. On peut donc écrire $a = 2a'$ avec $a' \in \mathbb{Z}$. On a $2b^2 = 2a^2 = 2(2a')^2 = 8(a')^2$. D'où $b^2 = 4(a')^2$. En particulier, 2 divise b^2. Et de nouveau, 2 divise b d'après Proposition 3.3.6. Par conséquent, 2 divise a et b. Contradiction car a et b sont premiers entre eux. □

Remarque 3.3.8. Plus généralement, on peut démontrer que $\sqrt{p}$ n'est pas un nombre rationnel pour tout nombre premier $p \in \mathbb{N}$.

3.4 La décomposition en facteurs premiers

Théorème (la décomposition en facteurs premiers). *Soit $a \in \mathbb{Z}$, $a \neq 0$. Il existe un signe $\varepsilon \in \{\pm 1\}$, il existe un entier naturel n, il existe des entiers naturels premiers $p_1, \ldots, p_n$ avec $p_1 < p_2 < \cdots < p_n$, et des entiers naturels non nuls $e_1, \ldots, e_n$ tels que*

$$a = \varepsilon \cdot p_1^{e_1} \cdot \ldots \cdot p_n^{e_n}.$$

De plus, le signe ε et les entiers $n, p_1, \ldots, p_n, e_1, \ldots, e_n$ sont uniquement déterminés par a.

Démonstration. Il suffit de démontrer l'énoncé pour $a \in \mathbb{N}^\star$, i.e., on montre, quel que soit $a \in \mathbb{N}^\star$, qu'il existe un entier naturel n, des entiers naturels premiers $p_1 < p_2 < \cdots < p_n$ et des entiers naturels non nuls $e_1, \ldots, e_n$ tels que

$$a = p_1^{e_1} \cdot \ldots \cdot p_n^{e_n}.$$

De plus, les entiers $n, p_1, \ldots, p_n, e_1, \ldots, e_n$ sont uniquement déterminés par a. On montre cet énoncé par récurrence sur généralisée sur a.

Pour $a = 1$, lénoncé est bien vrai, car a s'écrit comme le produit de 0 facteurs premiers, et cette écriture est bien unique. Supposons, ensuite, que l'énoncé est vrai pour tout entier naturel non nul $b < a$, pour un certain $a \in \mathbb{N}$, avec $a \geq 2$. D'après Proposition 3.3.3, il existe un entier naturel premier p divisant a. L'ensemble de tous les entiers naturels premiers divisant a est donc non vide. Comem $\mathbb{N}$ est bien ordonné, il existe donc un plus petit entier naturel premier divisant a. Soit p_1 cet entier naturel premier. Comme p_1 divise$a$, il existe $b \in \mathbb{N}$ tel que $p_1 b = a$. Comme p_1 est premier, $b < a$. D'après l'hypothèse de récurrence, b s'écrit sous la forme $p_1^{e_1 - 1} \cdot \ldots \cdot p_n^{e_n}$, pour un certain n, où $p_1, \ldots, p_n$ sont des entiers naturels premiers avec $p_1 <$

$p_2 < \cdots < p_n$, et où $e_1, \ldots, e_n \in \mathbb{N}$ avec $e_1 \geq 1$ et $e_2, \ldots, e_n$ non nul. Comme $a = p_1 b$, on a

$$a = p_1^{e_1} \cdot \ldots \cdot p_n^{e_n},$$

où $e_1, \ldots, e_n$ sont des entiers naturels non nuls. Cela montre l'existence au rang a.

Montrons maintenant l'unicité de la décomposition au rang a. Supposons que

$$a = p_1^{e_1} \cdot \ldots \cdot p_n^{e_n} = q_1^{f_1} \cdot \ldots \cdot q_m^{f_m}.$$

Montrons que $n = m$, que $p_i = q_i$ et que $e_i = f_i$, pour $i = 1, \ldots, n$. Soit b l'entier naturel tel que $p_1 b = a$. On a

$$b = \varepsilon \cdot p_1^{e_1 - 1} \cdot \ldots \cdot p_n^{e_n}.$$

Comme p_1 divise a, p_1 divise $q_1^{f_1} \cdots q_m^{f_m}$. Comme p_1 est premier, p_1 divise l'un des facteurs, i.e., p_1 divise q_i, pour un certain i. Comme $p_1 \neq \pm 1$ et q_i est premier, $p_1 = q_i$. De même, il existe j tel que $q_1 = p_j$. Si $i \neq 1$, on aurait $p_1 = q_i > q_1 = p_j$ ce qui contredirait le fait que p_1 est le plus petit nombre premier divisant a. Cela montre que $i = 1$, i.e., que $p_1 = q_1$. Du coup,

$$b = p_1^{e_1 - 1} \cdot \ldots \cdot p_n^{e_n} = q_1^{f_1 - 1} \cdot \ldots \cdot q_m^{f_m}.$$

D'après l'hypothèse de récurrence, $n = m$, et $p_i = q_i$ et $e_i = f_i$, pour $i = 1, \ldots, n$. □

Définition 3.4.1. Soit $a \in \mathbb{Z}^\star$. L'écriture $a = \varepsilon \cdot p_1^{e_1} \cdot \ldots \cdot p_n^{e_n}$ où $\varepsilon \in \{\pm 1\}$, où $p_1, \ldots, p_n$ sont des entiers naturels premiers avec $p_1 < \cdots < p_n$, et où $e_1, \ldots, e_n$ sont des entiers naturels non nuls, est la *décomposition en facteurs premiers* de a.

Exemple 3.4.2. 1. La décomposition de 2004 en facteurs premiers est $2004 = 2^2 \times 3 \times 167$.

2. La décomposition de 2005 en facteurs premiers est $2005 = 5 \times 401$.

Si on dispose de la décomposition en facteurs premiers d'un entier, on dresse très facilement la liste de tous ses diviseurs, c'est le contenu de l'énoncé suivant, conséquence de la décomposition en facteurs premiers.

Proposition 3.4.3. *Soit $a \in \mathbb{Z}^\star$. Soit $a = \varepsilon \cdot p_1^{e_1} \cdot \ldots \cdot p_n^{e_n}$, sa décomposition en facteurs premiers. Les diviseurs de a sont les entiers*

$$\pm p_1^{f_1} \cdot \ldots \cdot p_n^{f_n},$$

où $f_1, \ldots, f_n \in \mathbb{N}$ avec $f_i \leq e_i$ pour tout $i = 1, \ldots, n$. En particulier, le nombre de diviseurs de l'entier a est égal à

$$2(e_1 + 1) \cdots (e_n + 1).$$

La démonstration est laissé en exercice. Si on dispose des décompositions en facteurs premiers de deux entiers, on déterminera très facilement le pgcd de ceux-là.

Corollaire 3.4.4. *Soient $a, b \in \mathbb{Z}^\star$. Soient $p_1, \ldots, p_n$ des nombres premiers tels que*

$$a = \varepsilon \cdot p_1^{e_1} \cdot \ldots \cdot p_n^{e_n} \quad et \quad b = \delta \cdot p_1^{f_1} \cdot \ldots \cdot p_n^{f_n}$$

où $e_1, \ldots, e_n, f_1, \ldots, f_n \in \mathbb{N}$. Alors,

$$\mathrm{pgcd}(a, b) = p_1^{m_1} \cdot \ldots \cdot p_n^{m_n} \quad et \quad \mathrm{ppcm}(a, b) = p_1^{M_1} \cdot \ldots \cdot p_n^{M_n},$$

où $m_i = \min\{e_i, f_i\}$ et $M_i = \max\{e_i, f_i\}$ pour $i = 1, \ldots, n$.

Ce corrolaire est une conséquence du corollaire préc'édent. Une dernière conséquence de la décomposition en facteurs premiers et Propositon 3.2.11 est l'énoncé suivant.

Corollaire 3.4.5. *Soit $x \in \mathbb{Q}$, $x \neq 0$. Il existe un signe $\varepsilon \in \{\pm 1\}$, il existe un entier naturel n, il existe des entiers naturels premiers $p_1 < p_2 < \cdots < p_n$ et des entiers relatifs non nuls $e_1, \ldots, e_n$ tels que*

$$x = \varepsilon \cdot p_1^{e_1} \cdot \ldots \cdot p_n^{e_n}.$$

De plus, le signe ε et les entiers $n, p_1, \ldots, p_n, e_1, \ldots, e_n$ sont uniquement déterminés par x.

3.5 Le plus grand diviseur commun de n entiers

Définition 3.5.1. Soit $n \in \mathbb{N}$ et soient $a_1, \ldots, a_n \in \mathbb{Z}$. Un entier relatif c *diviseur commun* de $a_1, \ldots, a_n$ si c divise chacun des entiers $a_1, \ldots, a_n$. Un entier relatif c est un plus grand diviseur commun de $a_1, \ldots, a_n$ si les condtions suivantes sont vérifiées :

1. c est un diviseur commun de $a_1, \ldots, a_n$, et
2. pour tout diviseur commun d de $a_1, \ldots, a_n$, on a que d divise c.

Un plus grand diviseur commun de $a_1, \ldots, a_n$ est noté par $\mathrm{pgcd}(a_1, \ldots, a_n)$.

Proposition 3.5.2. *Soit $n \in \mathbb{N}$ et soient $a_1, \ldots, a_n \in \mathbb{Z}$. Si $a_1, \ldots, a_n$ admettent un plus grand diviseur commun, alors il est unique à signe près.*

Démonstration. Soient c et c' deux plus grands diviseurs communs des entiers $a_1, \ldots, a_n$. Alors, l'entier c divise c' et l'entier c' divise c, i.e., $c' = \pm c$. □

Proposition 3.5.3. *Soit $n \in \mathbb{N}$ et soient $a_1, \ldots, a_n \in \mathbb{Z}$. Les entiers relatifs $a_1, \ldots, a_n$ admettent un plus grand diviseur commun. De plus,*

$$\text{pgcd}(a_1, \ldots, a_{n-1}, a_n) = \text{pgcd}(\text{pgcd}(a_1 \ldots, a_{n-1}), a_n).$$

Démonstration. Montrons par récurrence que les entiers $a_1, \ldots, a_n$ admettent un plus grand diviseur commun, quel que soit $n \in \mathbb{N}$. La suite vide d'entier relatifs a 0 comme plus grand diviseur commun. Cela montre l'énoncé au rang $n = 0$. La suite a_1 d'un seul entier a comme plus grand diviseur commun a_1. Donc l'énoncé est bien vrai au rang $n = 1$. On a vu au paragraphe 3.2 qu'une suite de deux entiers admet bien un plus grand diviseur commun. L'énoncé est donc également vrai au rang $n = 1$. Supposons maintenant que l'énoncé est vrai au rang $n - 1$, pour un certain $n \in \mathbb{N}$, avec $n \geq 3$. On suppose donc que les entiers relatifs $a_1, \ldots, a_{n-1}$ admettent un plus grand diviseur commun, pour un certain entier naturel n, avec $n \geq 3$. Montrons que les entiers $a_1, \ldots, a_n$ admettent un plus grand diviseur commun. D'après l'hypothèse de récurrence, les entiers naturels $a_1, \ldots, a_{n-1}$ admettent un plus grand diviseur commun c. Soit d un plus grand diviseur commun de c et a_n. Montrons que d est un plus grand diviseur commun de $a_1, \ldots, a_n$.

Comme d divise c et comme c divise les entiers $a_1, \ldots, a_{n-1}$, l'entier d divise $a_1, \ldots, a_{n-1}$. Par conséquent d divise les entiers $a_1, \ldots, a_n$, i.e., d est un diviseur commun de $a_1, \ldots, a_n$.

Soit e un diviseur commun de $a_1, \ldots, a_n$. On montre que e divise d. Comme e divise $a_1, \ldots, a_{n-1}$, l'entier e divise le plus grand diviseur commun c de $a_1, \ldots, a_{n-1}$. Donc e divise c et a_n. Par conséquent, e divise le plus grand diviseur commun d de c et a_n. Cela montre que d est un plus grand diviseur commun de $a_1, \ldots, a_n$. En particulier, les entiers $a_1, \ldots, a_n$ admettent un plus grand diviseur commun. On conclut par récurrence que les entiers $a_1, \ldots, a_n$ admettent un pus grand diviseur commun. De plus, l'argument montre qu'on a bien

$$\text{pgcd}(a_1, \ldots, a_n) = \text{pgcd}(\text{pgcd}(a_1, \ldots, a_{n-1}), a_n).$$

□

Exemple 3.5.4. Déterminons le plus grand diviseur commun des entiers $105, 63, 45$. En effectuant l'algorithme d'Euclide, on trouve $\text{pgcd}(105, 63) = 21$. Puis, $\text{pgcd}(21, 45) = 3$. Donc

$$\text{pgcd}(105, 63, 45) = \text{pgcd}(\text{pgcd}(105, 63), 45) = \text{pgcd}(21, 45) = 3$$

d'après Proposition 3.5.3. Remarquons que les pgcd deux-à-deux sont tous différents de 3. En effet,

$$\text{pgcd}(105, 63) = 21, \quad \text{pgcd}(105, 45) = 15, \quad \text{et} \quad \text{pgcd}(63, 45) = 9.$$

Théorème de Bézout. *Soit $n \in \mathbb{N}$ et soient $a_1, \ldots, a_n \in \mathbb{Z}$. Soit c un diviseur commun de $a_1, \ldots, a_n$. Alors, c est un plus grand diviseur commun de $a_1, \ldots, a_n$ si et seulement s'il existe $u_1, \ldots, u_n$ tels que*

$$u_1 a_1 + \cdots + u_n a_n = c.$$

Démonstration. Supposons qu'il existe $u_1, \ldots, u_n$ comme ci-dessus. Montrons que c est un plus grand diviseur commun de $a_1, \ldots, a_n$. D'après l'hypothèse, c est un diviseur commun de $a_1, \ldots, a_n$. Pour montrer que c est un plus grand diviseur commun, supposons que d est un diviseur commun de $a_1, \ldots, a_n$. Donc, d divise $u_1 a_1, \ldots, u_n a_n$ et aussi leur somme qui est égale à c. Par conséquent, c est un plus grand diviseur commun de $a_1, \ldots, a_n$.

Montrons la réciproque par récurrence, c-à-d, on montre par récurrence que si c est un plus grand diviseur commun de $a_1, \ldots, a_n$, alors il existe $u_1, \ldots, u_n \in \mathbb{Z}$ tels que

$$u_1 a_1 + \cdots + a_n u_n = c,$$

quel que soit $n \in \mathbb{N}$, avec $n \geq 2$.

L'assertion est bien vraie pour $n = 0$ et 1, et pour $n = 2$ d'après le Théorème de Bézout du paragraphe 3.2. Supposons que l'assertion est vraie au rang $n-1$, pour un certain $n \in \mathbb{N}$ avec $n \geq 3$. Montrons-la au rang n. Soit d un plus grand diviseur commun de $a_1, \ldots, a_{n-1}$. Par hypothèse, il existe $v_1, \ldots, v_{n-1} \in \mathbb{Z}$ tels que

$$v_1 a_1 + \cdots + v_{n-1} a_{n-1} = d.$$

D'après la proposition précédente, c est un plus grand diviseur commun de d et a_n. D'après le Théorème de Bézout du paragraphe 3.2, il existe $u, v \in \mathbb{Z}$ tels que $ud + va_n = c$. Du coup,

$$c = ud + va_n = u(v_1 a_1 + \cdots + v_{n-1} a_{n-1}) + va_n = u_1 a_1 + \cdots + u_n a_n,$$

si on pose $u_i = uv_i$, pour $i = 1, \ldots, n-1$, et $u_n = v$. Remarquons qu'on a bien $u_1, \ldots, u_n \in \mathbb{Z}$. □

La démonstration ci-dessus est constructive, i.e., elle nous montre non suelement qu'il existe des entiers $u_1, \ldots, u_n$, mais en plus, elle nous explique comment les trouver.

Exemple 3.5.5. On a vue que $\text{pgcd}(105, 63, 45) = 3$. Déterminons $u, v, w \in \mathbb{Z}$ tels que $105u + 63v + 45w = 3$. Tout d'abord, en effectuant l'algorithme d'Euclide, on trouve que $(-1) \times 105 + 2 \times 63 = \text{pgcd}(105, 63) = 21$. Puis,

on trouve que $(-2) \times 21 + 1 \times 45 = \text{pgcd}(21, 45) = 3$. En substituant , on obtient

$$3 = (-2) \times 21 + 1 \times 45 = (-2) \times ((-1) \times 105 + 2 \times 63) + 1 \times 45 = \\ = 2 \times 105 + (-4) \times 63 + 1 \times 45.$$

Donc, $u = 2$, $v = -4$ et $w = 1$ conviennent.

Définition 3.5.6. Soit $n \in \mathbb{N}$ et soient $a_1, \ldots, a_n \in \mathbb{Z}$. On dit que $a_1, \ldots, a_n$ sont *premiers entre eux* si les seuls diviseurs communs de $a_1, \ldots, a_n$ sont ± 1. De manière équivalente, les entiers $a_1, \ldots, a_n$ sont premiers entre eux si 1 est un plus grand diviseur commun de $a_1, \ldots, a_n$.

Exemple 3.5.7. Les entiers $15, 10, 6$ sont premiers entre eux. En effet,

$$\text{pgcd}(15, 10, 6) = \text{pgcd}(\text{pgcd}(15, 10), 6) = \text{pgcd}(5, 6) = 1.$$

Par contre, les entiers $15, 10, 6$ ne sont pas premiers entre eux deux-à-deux. En fait, $\text{pgcd}(10, 6) = 2$, $\text{pgcd}(15, 6) = 3$ et $\text{pgcd}(15, 10) = 5$. Donc, pour aucun choix de deux entiers a, b parmi les trois entiers $15, 10, 6$, on n'a $\text{pgcd}(a, b) = 1$.

Corollaire 3.5.8. *Soit $n \in \mathbb{N}$ et soient $a_1, \ldots, a_n \in \mathbb{Z}$. Les entiers $a_1, \ldots, a_n$ sont premiers entre eux si et seulement s'il existe $u_1, \ldots, u_n \in \mathbb{Z}$ tels que*

$$u_1 a_1 + \cdots + u_n a_n = 1.$$

Démonstration. S'il existe des entiers $u_1, \ldots, u_n$ tels que $u_1 a_1 + \cdots + u_n a_n = 1$, alors l'entier 1 est un plus grand diviseur commun de $a_1, \ldots, a_n$ d'après le Théorème de Bézout.

Réciproquement, si 1 est un plus grand diviseur commun de $a_1, \ldots, a_n$, alors, d'après le Théorème de Bézout, il existe des entiers $u_1, \ldots, u_n$ tels que $u_1 a_1 + \cdots + u_n a_n = 1$. □

Exemple 3.5.9. On a vue que les entiers $15, 10, 6$ sont premiers entre eux. Déterminons $a, v, w \in \mathbb{Z}$ tels que $15u + 10v + 6w = 1$. Effectuons d'abord l'algorithme d'Euclide étendu sur les entiers $15, 10$. On obtient $1 \times 15 + (-1) \times 10 = \text{pgcd}(15, 10) = 5$. Puis, $(-1) \times 5 + 1 \times 6 = 1$. Donc

$$(-1) \times 15 + 1 \times 10 + 1 \times 6 = 1,$$

i.e., $u = -1$, $v = 1$ et $w = 1$ conviennent.

3.6 Le plus petit multiple commun

Définition 3.6.1. Soient $a, b \in \mathbb{Z}$. Un entier relatif c est un *multiple commun* de a et b si c est multiple de a et b. Un entier relatif c est un plus petit multiple commun de a et b si

1. c est un multiple commun de a et b, et
2. tout multiple commun d de a et b, est un multiple de c.

On écrit $c = \text{ppcm}(a, b)$ si c est un plus petit multiple de a et b.

En général, si un entier relatif c est un multiple commun de deux entiers relatifs a et b, l'entier c n'est pas un multiple du produit ab. L'énoncé suivant nous dit que cette conclusion est bien valide lorsque a et b sont premiers entre eux.

Proposition 3.6.2. *Soient $a, b, c \in \mathbb{Z}$. Supposons que c est multiple commun de a et b. Si a et b sont premiers en eux, alors c est multiple de ab.*

Démonstration. Comme b divise c, il existe $d \in \mathbb{Z}$ tel que $bd = c$. Comme a divise $c = bd$, et comme a et b sont premires entre eux, a divise d, d'après le Lemme de Gauss. Du coup, il existe $e \in \mathbb{Z}$ tel que $ae = d$ et

$$c = bd = b(ae) = (ab)e.$$

Par conséquent, ab divise c, i.e., c est multiple de ab. □

Proposition 3.6.3. *Soient $a, b \in \mathbb{Z}$. Si un plus petit multiple de a et b existe, alors il est unique à signe près.*

Démonstration. Supposons que c et c' sont deux plus petits multiples communs de a et b. On a donc, $c|c'$ et $c'|c$. D'où $c = \pm c'$. □

Théorème 3.6.4. *Soient $a, b \in \mathbb{Z}$. Alors, a et b admettent un plus petit multiple commun. De plus,*

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

En particulier, si a et b sont premiers entre eux, $\text{ppcm}(a, b) = ab$.

Démonstration. Si $a = 0$ ou $b = 0$, tout multiple commun de a et b est égal à 0. L'entier 0 est donc un plus petit multiple commun de a et b, si $a = 0$ ou $b = 0$. De plus, on a bien $\text{pgcd}(a, b)\text{ppcm}(a, b) = ab$, $a = 0$ ou $b = 0$.

On peut donc supposer que $a \neq 0$ et $b \neq 0$, et donc, que $c = \text{pgcd}(a, b) \neq 0$. Comme c divise a et b, on peut écrire $a = ca'$, avec $a' \in \mathbb{Z}$, et $b = cb'$ avec $b' \in \mathbb{Z}$. Soit $d = a'b$. On montre que $d = \text{ppcm}(a, b)$.

Comme $a'b = a'(cb') = (ca')b' = ab'$, il est clair que d est un multiple commun de a et b. Soit e un multiple commun de a et b. On montre que $d|e$. Or, e est divisible par c. Soit $e' \in \mathbb{Z}$ tel que $e = e'c$. L'entier e' est multiple commun de a' et b'. Comme a' et b' sont premier entre eux, e' est multiple de $a'b'$ d'après Proposition 3.6.2. Par conséquent, $e = e'c$ est multiple de $a'b'c = d$. Il s'ensuit que a et b admettent un plus petit multiple commun, et $\text{pgcd}(a, b)\text{ppcm}(a, b) = ab$. □

Soient $a, b \in \mathbb{Z}$. Le théorème de Bézout nous dit que l'équation $ax+by = c$ admet un solution $(x, y) \in \mathbb{Z}^2$ si $c = \text{pgcd}(a, b)$. Grâce aux ppcm, on pourra trouver l'ensemble de toutes les solutions de cette équation pour tout $c \in \mathbb{Z}$.

Théorème 3.6.5. *Soient $a, b, c \in \mathbb{Z}$ avec $a \neq 0$ et $b \neq 0$. Soit $d = \text{pgcd}(a, b)$. Alors, l'équation $ax+by = c$ admet une solution $(x, y) \in \mathbb{Z}\times\mathbb{Z}$ si et seulement si d divise c. De plus, si (x_0, y_0) est une solution particulière, l'ensemble de toutes les solutions de l'équation $ax + by = c$ dans $\mathbb{Z} \times \mathbb{Z}$ est l'ensemble*

$$\{(x_0 + kb', y_0 - ka') \mid k \in \mathbb{Z}\},$$

où $a', b' \in \mathbb{Z}$ sont tels que $a = a'd$ et $b = b'd$.

Démonstration. Supposons que c est divisible par d, et soit $e \in \mathbb{Z}$ tel que $c = de$. D'après le Théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que $ua+vb = d$. Posons $x = ue$ et $y = ve$. On a

$$ax + by = aue + bve = (au + bv)e = de = c.$$

Par conséquent, l'équation $ax + by = c$ admet une solution dans $\mathbb{Z} \times \mathbb{Z}$ lorsque c est un multiple de d.

Réciproquement, supposons que l'équation $ax + by = c$ admet une solution (x, y) dans $\mathbb{Z}\times\mathbb{Z}$. Comme d divise a et b, l'entier d divise ax et by, et donc aussi leur somme $ax + by = c$. D'où d divise c lorsque l'équation $ax + by = c$ admet une solution dans $\mathbb{Z} \times \mathbb{Z}$.

Pour montrer la deuxème assertion du théorème, supposons que d divise c et soit $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ une solution de l'équation $ax + by = c$. Montrons d'abord que tous les couples de la forme $(x_0 + kb', y_0 - ka')$ sont bien des solutions de l'équation $ax + by = c$, quel que soit $k \in \mathbb{Z}$. Effectivement, on a

$$a(x_0 + kb') + b(y_0 - ka') = ax_0 + by_0 + k(ab' - a'b) = c + k \times 0 = c,$$

car $a'b = ab' = \text{ppcm}(a, b)$. Par conséquent, tous les couples de la forme $(x_0 + kb', y_0 - ka')$ sont bien des solutions de l'équation $ax + by = c$, quel que soit $k \in \mathbb{Z}$.

Réciproquement, supposons que $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ est une solution de l'équation $ax + by = c$. On montre qu'il existe $k \in \mathbb{Z}$ tel que $(x, y) = (x_0 + kb', y_0 - ka')$. En effet, on a

$$ax + by = c = ax_0 + by_0.$$

D'où

$$a(x - x_0) = b(y_0 - y).$$

Donc, l'entier $a(x-x_0)$ est divisible par b. C'est donc un multiple commun de a et b. Du coup, $a(x-x_0)$ est un multiple du $\text{ppcm}(a, b) = ab'$. Comme $a \neq 0$, $x - x_0$ est un multiple de b', i.e., il existe $k \in \mathbb{Z}$ tel que $x = x_0 + kb'$. Du coup,

$$b(y_0 - y) = a(x - x_0) = kab' = ka'b.$$

Comme $b \neq 0$, on obtient que $y_0 - y = ka'$ et donc que $y = y_0 - ka'$. Cela montre que $(x, y) = (x_0 + kb', y_0 - ka')$ pour un certain $k \in \mathbb{Z}$. □

Exemple 3.6.6. 1. Soit D la droite dans $\mathbb{R}^2$ définie par l'équation $y = -\frac{2}{3}x + \frac{1}{2}$. Alors, $D \cap \mathbb{Z}^2 = \emptyset$. En effet, puisque la condition $y = -\frac{2}{3}x + \frac{1}{6}$ est équivalente à $4x + 6y = 3$, l'intersection $D \cap \mathbb{Z}^2$ est l'ensemble des solutions dans $\mathbb{Z}^2$ de l'équation $4x + 6y = 3$. D'après le théorème précédent, cet ensemble est vide.

2. Soit D' la droite dans $\mathbb{R}^2$ d'équation $4x + 6y = 10$. Alors

$$D \cap \mathbb{Z}^2 = \{(1 + 3k, 1 - 2k) \mid k \in \mathbb{Z}\}.$$

Définition 3.6.7. Soit $n \in \mathbb{N}$ et soient $a_1, \ldots, a_n \in \mathbb{Z}$. Un entier relatif c est un *multiple commun* de $a_1, \ldots, a_n$ si c est multiple de chacun des entiers $a_1, \ldots, a_n$. Un entier relatif c est un *plus petit multiple commun* de $a_1, \ldots, a_n$ si

1. c est un multiple commun de $a_1, \ldots, a_n$, et
2. tout multiple commun d de $a_1, \ldots, a_n$, est un multiple de c.

On écrit $c = \text{ppcm}(a_1, \ldots, a_n)$ si c est un plus petit multiple de a et b.

Proposition 3.6.8. *Soit $n \in \mathbb{N}$ et soient $a_1, \ldots, a_n \in \mathbb{Z}$. Si un plus petit multiple commun de $a_1, \ldots, a_n$ existe, alors il est unique à signe près.*

Démonstration. Soient c et c' deux plus petits multiples communs des entiers $a_1, \ldots, a_n$. On a $c|c'$ et $c'|c$. D'où $c = \pm c'$. □

On laisse la démonstration de l'énoncé suivant comme exercice.

Proposition 3.6.9. *Soit $n \in \mathbb{N}$ et soient $a_1, \ldots, a_n \in \mathbb{Z}$. Les entiers relatifs admettent un plus petit multiple commun. De plus*

$$\text{ppcm}(a_1, \ldots, a_{n-1}, a_n) = \text{ppcm}(\text{ppcm}(a_1, \ldots, a_{n-1}), a_n).$$

3.7 Inversibles dans $\mathbb{Z}/n\mathbb{Z}$

Proposition 3.7.1. *L'ensemble $\mathbb{Z}/n\mathbb{Z}$ muni des lois $+$ et $\cdot$ est un anneau commutatif.*

Proposition 3.7.2. *Soit $a \in \mathbb{Z}$. L'élément $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si* $\text{pgcd}(a, n) = 1$.

Démonstration. Supposons que $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$. Il existe donc $\overline{u} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\overline{u} \cdot \overline{a} = \overline{1}$. D'où $\overline{ua} = \overline{1}$, i.e., $ua - 1$ est divisible par n. Du coup, il existe $v \in \mathbb{Z}$ tel que $ua - 1 = vn$, i.e., $ua + (-v)n = 1$. Il s'ensuit que $\text{pgcd}(a, n) = 1$.

Réciproquement, supposons que $\text{pgcd}(a, n) = 1$. D'après le Théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que $ua + vn = 1$ dans $\mathbb{Z}$. Prendre les classes modulo n donne

$$\overline{1} = \overline{ua + vn} = \overline{ua} + \overline{vn} = overlineu\overline{a},$$

car $\overline{n} = \overline{0}$. Par conséquent, $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$. □

Corollaire 3.7.3. *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.*

3.8 Décomposition en éléments simples

Théorème 3.8.1. *Soit $a, b \in \mathbb{N}$ avec $b \geq 2$. Alors, il existe un entier naturel n et des entiers naturels $a_0, \ldots, a_n$ tels que*

1. $a = a_n b^n + \cdots + a_1 b^1 + a_0 b^0$, *et*
2. $a_n < b \ldots,\ a_1 < b_1,\ a_0 < b_0$.

De plus, les entiers $n, a_0, \ldots, a_n$ sont uniquement déterminés par a et b.

Démonstration. Montrons l'existence par récurrence sur a. Pour $a = 0$, on prend $n = 0$ et $a_0 = 0$. Supposons que l'existence est démontrée pour tout entier naturel inférieur strict à un entier naturel donné a. Montrons l'existence pour a. D'après la division euclidienne, il existe des entiers q et a_0 tels que $a = qb + a_0$, où $0 \leq a_0 < b$. On a donc $q \in \mathbb{N}$ et $q < a$. D'après l'hyppothèse de récurrence, il existe $n \in \mathbb{N}$ et $a_1, \ldots, a_n \in \mathbb{N}$ avec $a_i < b$ et $q = a_n b^{n-1} + \cdots + a_1 b^0$. Du coup, $a = a_n b^n + \cdots + a_1 b^1 + a_0 b^0$. Cela montre l'existence.

L'unicité se démontre de même par récurrence. □

Théorème 3.8.2. *Soit $\frac{a}{b}$ un nombre rationnel, i.e., $a \in \mathbb{Z}$ et $b \in \mathbb{N}$, avec $b \neq 0$. Soit $b = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ la décomposition de b en facteurs premiers. Alors il existe un entiers relatif q et des entiers naturels r_{ij}, pour $j = 1, \ldots, e_i$ et $i = 1, \ldots, n$, tels que*

$$\frac{a}{b} = q + \frac{r_{11}}{p_1} + \frac{r_{12}}{p_1^2} + \cdots + \frac{r_{1e_1}}{p_1^{e_1}} + \frac{r_{21}}{p_2} + \frac{r_{22}}{p_2^2} + \cdots + \frac{r_{2e_2}}{p_2^{e_2}} + \cdots \\ \cdots + \frac{r_{n1}}{p_n} + \frac{r_{n2}}{p_n^2} + \cdots + \frac{r_{ne_n}}{p_n^{e_n}},$$

où $0 \leq r_{ij} < p_i$ pour tout $j = 1, \ldots, e_i$ et pour tout $i = 1, \ldots, n$. De plus, les entiers q et r_{ij} sont uniquement déterminés par $\frac{a}{b}$.

Démonstration. Montrons d'abord l'existence. Soient

$$b_i = \prod_{j \neq i} p_j^{e_j}$$

pour $i = 1, \ldots, n$. Donc, on a $b = b_i \cdot p_i^{e_i}$, pour tout i. Il est clair que les entiers $b_1, \ldots, b_n$ sont premiers entre eux. Par conséquent, il existe des entiers relatifs $a_1, \ldots, a_n$ tels que

$$a_1 b_1 + \cdots + a_n b_n = a.$$

Soient $q_1, \ldots, q_n$ les quotients de la division euclidienne de a_i par $p_i^{e_i}$, et $r_1, \ldots, r_n$ les restes, pour $i = 1, \ldots, n$. Soit $q = q_1 + \cdots + q_n$. On a

$$qb + r_1 b_1 + \cdots + r_n b_n = qb + (a_1 - q_1 p_1^{e_1}) b_1 + \cdots + (a_n - q_n p_n^{e_n}) b_n = a,$$

où $0 \leq r_i < p_i^{e_i}$ pour tout $i = 1 \ldots, n$. Comme $0 \leq r_i < p_i^{e_i}$, on peut écrire r_i sous la forme

$$r_i = r_{i1} p_i^{e_i - 1} + \cdots + r_{i2} p_i^{e_i - 2} + \cdots + r_{i,e_i - 1} p_i^1 + r_{i,e_i} p_i^0,$$

où chaque $r_i j$ est un entier satisfaisant $0 \leq r_{ij} < p_i$. Par conséquent

$$\frac{a}{b} = \frac{qb + r_1 b_1 + \cdots + r_n b_n}{b} = q + \frac{r_1}{p_1^{e_1}} + \frac{r_2}{p_2^{e_2}} + \cdots + \frac{r_n}{p_n^{e_n}} = \\ = q + \frac{r_{11}}{p_1} + \frac{r_{12}}{p_1^2} + \cdots + \frac{r_{1e_1}}{p_1^{e_1}} + \frac{r_{21}}{p_2} + \frac{r_{22}}{p_2^2} + \cdots + \frac{r_{2e_2}}{p_2^{e_2}} + \cdots \\ \cdots + \frac{r_{n1}}{p_n} + \frac{r_{n2}}{p_n^2} + \cdots + \frac{r_{ne_n}}{p_n^{e_n}},$$

où $q \in \mathbb{Z}$ et r_{ij} sont des entiers satisfaisant $0 \leq r_{ij} < p_i$ pour tout $j = 1, \ldots e_i$ et pour tout $i = 1, \ldots, n$. Cela montre l'existence.

Montrons, ensuite, l'unicité des entiers q et r_{ij}. Supposons que q' et r'_{ij} sont d'autres entiers tels que

$$\frac{a}{b} = q' + \frac{r'_{11}}{p_1} + \frac{r'_{12}}{p_1^2} + \cdots + \frac{r'_{1e_1}}{p_1^{e_1}} + \frac{r'_{21}}{p_2} + \frac{r'_{22}}{p_2^2} + \cdots + \frac{r_{2e'_2}}{p_2^{e_2}} + \cdots \\ \cdots + \frac{r'_{n1}}{p_n} + \frac{r'_{n2}}{p_n^2} + \cdots + \frac{r'_{ne_n}}{p_n^{e_n}},$$

où $0 \leq r'_{ij} < p_i$ pour tout $j = 1, \ldots, e_i$ et pour tout $i = 1, \ldots, n$. On montre que $q = q'$ et que $r_{ij} = r'_{ij}$ quels que soient $j = 1, \ldots, e_i$ et $i = 1, \ldots, n$.

En effet, posons $r'_i = r'_{i,1}p_i^{e_i-1} + \cdots + r_{i,e_i}p_i^0$. pour $i = 1, \ldots, n$. Comme $0 \leq r_{ij} < p_i$, il suffit de montrer que $r_i = r'_i$ quel que soit i. Or, on a

$$q + \frac{r_1}{p_1^{e_1}} + \frac{r_2}{p_2^{e_2}} + \cdots + \frac{r_n}{p_n^{e_n}} = \frac{a}{b} = q' + \frac{r'_1}{p_1^{e_1}} + \frac{r'_2}{p_2^{e_2}} + \cdots + \frac{r'_n}{p_n^{e_n}}.$$

Multiplier l'équation par b donne

$$bq + b_1r_1 + b_2r_2 + \cdots + b_nr_n = bq' + b_1r'_1 + b_2r'_2 + \cdots + b_nr'_n.$$

Prendre les congruences modulo $p_i^{e_i}$ de deux côtés donne

$$b_ir_i \equiv b_ir'_i \pmod{p_i^{e_i}}.$$

pour $i = 1, \ldots, n$. Comme b_i est inversible modulo $p_i^{e_i}$, on en déduit que $r_i \equiv r'_i \pmod{p_i^{e_i}}$. Comme $0 \leq r_i < p_i^{e_i}$ et $0 \leq r'_i < p_i^{e_i}$, on a $r_i = r'_i$ pour $i = 1, \ldots, n$. Du coup, on a aussi $q = q'$. Cela montre l'unicité. □

Exemple 3.8.3. Décomposer le nombre rationnel $\frac{73}{360}$ en éléments simples. La décomposition en facteurs premiers de $b = 360$ est

$$b = 360 = 2^3 \times 3^2 \times 5.$$

Soient donc $n = 3$, $p_1 = 2$, $e_1 = 3$, $p_2 = 3$, $e_2 = 2$, $p_3 = 5$ et $e_3 = 1$. On déroule l'algorithme comme dans la démonstration ci-dessus. On pose $b_1 = 3^2 \times 5 = 45$, $b_2 = 2^3 \times 5 = 40$ et $b_3 = 2^3 \times 3^2 = 72$. On cherche des entiers relatifs a_1, a_2, a_3 tels que $a_1b_1 + a_2b_2 + a_3b_3 = a = 73$.

Pour cela, on cherche d'abord des entiers u_1, u_2, u_3 tels que $u_1b_1 + u_2b_2 + u_3b_3 = 1$. Il en existe car $\text{pgcd}(b_1, b_2, b_3) = 1$. On applique l'Algorithme d'Euclide étendu pour trouver des entiers v_1, v_2 tels que $v_1b_1 + v_2b_2 = \text{pgcd}(b_1, b_2)$. En fait, comme $b_1 = 45$ et $b_2 = 40$ on voit tout de suite que $\text{pgcd}(b_1, b_2) = 5$ et que $v_1 = 1$ et $v_2 = -1$ conviennent. Puis, on cherche des entiers u et v tels que $u \times 5 + v \times b_3 = 1$, en effectuant l'Algorithme d'Euclide étendu.

Cela donne $u = 29$ et $v = -2$. Posons $u_1 = u \times v_1 = 29 \times 1 = 29$, $u_2 = u \times v_2 = 29 \times (-1) = -29$ et $u_3 = v = -2$. Alors, on a

$$u_1 b_1 + u_2 b_2 + u_3 b_3 = 1.$$

Maintenant, on multiplie cette équation par 73 pour trouver que

$$a_1 b_1 + a_2 b_2 + a_3 b_3 = 73,$$

où $a_1 = 73 \times u_1 = 2117$, $a_2 = 73 \times (-29) = -2117$ et $a_3 = 73 \times (-2) = -146$.

On effectue les divisions euclidiennes de a_i par $p_i^{e_i}$ pour $i = 1, 2, 3$. On trouve

$$a_1 = 264 \times p_1^{e_1} + 5, \quad a_2 = -236 \times p_2^{e_2} + 7, \quad \text{et} \quad a_3 = -30 \times p_3^{e_3} + 4.$$

Soient donc $r_1 = 5$, $r_2 = 7$, $r_3 = 4$ et $q = 264 - 236 - 30 = -2$. Ecrire

$$r_1 = 1 \times p_1^2 + 0 \times p_1^1 + 1 \times p_1^0, \quad r_2 = 1 \times p_2^1 + 1 \times p_2^0 \quad \text{et} \quad r_3 = 4 \times p_3^0.$$

La décomposition en éléments simples de $\frac{73}{360}$ est donc

$$\begin{aligned} \frac{73}{360} &= q + \frac{r_1}{p_1^3} + \frac{r_2}{p_2^2} + \frac{r_3}{p_3} = \\ &= q + \frac{1 \times p_1^2 + 0 \times p_1^1 + 1 \times p_1^0}{p_1^3} + \frac{1 \times p_2^1 + 1 \times p_2^0}{p_2^2} + \frac{4 \times p_3^0}{p_3^1} = \\ &= -2 + \frac{1}{2} + \frac{1}{2^3} + \frac{1}{3} + \frac{1}{3^2} + \frac{4}{5}. \end{aligned}$$

Chapitre 4

Arithmétique des polynômes

4.1 La division euclidienne

Soit K un corps, par exemple $K = \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$. Rappelons qu'un polynôme en l'indéterminé X et à coefficients dans K est une expression formelle de la forme $a_n X^n + \cdots + a_0$, où les coefficients $a_0, \ldots, a_n$ sont des éléments de K. Rappelons également que $K[X]$ désigne l'ensemble des polynômes en X à coefficients dans K. L'ensemble $K[X]$ est un anneau commutatif unitaire (voir paragraph 2.2).

Définition 4.1.1. Soit $A \in K[X]$ un polynôme. Donc $A = a_n X^n + \cdots + a_0$, où $a_0, \ldots, a_n \in K$, pour un certain $n \in \mathbb{N}$. Si A est non nul, on peut supposer que $a_n \neq 0$. Le coefficient a_n est alors appelé *coefficient dominant* de A. L'entier natrurel n est appelé *degré* de A, et on note $\deg(A) = n$. Par convention, le *coefficient dominant* du polynôme nul est 0, et le degré du polynôme nul est $-\infty$, i.e., $\deg(0) = -\infty$. Le polynôme A est *constant* s'il est de degré 0 ou $-\infty$.

Le degré d'un polynôme définit donc une application

$$\deg\colon K[X] \longrightarrow \mathbb{N} \cup \{-\infty\}.$$

On étend l'addition sur $\mathbb{N}$ à $\mathbb{N} \cup \{-\infty\}$ en définissant $-\infty + x = -\infty$ et $x + (-\infty) = -\infty$ pour tout $x \in \mathbb{N} \cup \{-\infty\}$. On étend la relation d'ordre $\leq$ sur $\mathbb{N}$ à $\mathbb{N} \cup \{-\infty\}$ en déclarant $-\infty$ strictement plus petit que tout entier naturel. Comme $\mathbb{N}$ est bien orodonné, il est clair que $\mathbb{N} \cup \{-\infty\}$ est bien ordonné par sa relation d'ordre.

Proposition 4.1.2. *Soient $A, B \in K[X]$. On a les règles de calcul suivantes :*

1. $\deg(A + B) \leq \max\{\deg(A), \deg(B)\}$

2. $\deg(AB) = \deg(A) + \deg(B)$

Démonstration. 1. L'énoncé est bien vrai lorsque $A = 0$ et $B = 0$. On peut donc supposer que $A \neq 0$ ou $B \neq 0$. On peut écrire $A = a_n X^n + \cdots + a_0$ et $B = b_n X^n + \cdots + b_0$, où $n \in \mathbb{N}$ et $a_0, \ldots, a_n, b_0, \ldots, b_n \in K$, avec $a_n \neq 0$ ou $b_n \neq 0$. Comme

$$A + B = (a_n + b_n)X^n + \cdots + (a_0 + b_0),$$

on a bien $\deg(A + B) \leq n = \max\{\deg(A), \deg(B)\}$.

2. L'énoncé est bien vrai lorsque $A = 0$ ou $B = 0$. On peut donc supposer que $A \neq 0$ et $B \neq 0$. On peut donc écrire $A = a_n X^n + \cdots + a_0$ et $B = b_m X^m + \cdots + b_0$, où $m, n \in \mathbb{N}$ et $a_0, \ldots, a_n, b_0, \ldots, b_m \in K$, avec $a_n \neq 0$ et $b_m \neq 0$. Du coup,

$$AB = a_n b_m X^{n+m} + \cdots + a_0 b_0.$$

Comme $a_n \neq 0$ et $b_m \neq 0$, $a_n b_m \neq 0$. Il s'ensuit que $\deg(AB) = n + m = \deg(A) + \deg(B)$. □

Remarque 4.1.3. Soient $A, B \in K[X]$. On a l'égalité

$$\deg(A + B) = \max\{\deg(A), \deg(B)\}$$

si et seulement si l'une des deux conditions suivantes est vérifiée :

1. $\deg(A) \neq \deg(B)$, ou
2. $\deg(A) = \deg(B)$ et la somme des coefficients dominants de A et B est non nul dans K.

Corollaire 4.1.4. *L'anneau $K[X]$ est intègre.*

Démonstration. On a bien $K[X] \neq \{0\}$, car $1 \neq 0$ dans K, et donc dans $K[X]$. Soient $A, B \in K[X]$, et supposons que $AB = 0$. Comme $\deg(A) + \deg(B) = \deg(AB) = \deg(0) = -\infty$, on a $\deg(A) = -\infty$ ou $\deg(B) = -\infty$, i.e., $A = 0$ ou $B = 0$. □

Corollaire 4.1.5. *Un polynôme dans $K[X]$ est inversible si et seulement s'il est de degré 0, i.e., $K[X]^\times = K^\star$.*

Démonstration. Soit $P \in K[X]$ un polynôme de degré 0. Dans ce cas $P = a_0$, où $a_0 \in K^\star$. Comme $a_0 \in K^\star$ et K est un corps, il existe $b_0 \in K$ tel que $a_0 b_0 = 1$. Soit Q le polynôme b_0. On a bien $PQ = 1$, i.e. P est inversible dans $K[X]$.

Réciproquement, supposons que $P \in K[X]$ est inversible. Il existe donc $Q \in K[X]$ tel que $PQ = 1$. Du coup, $\deg(P) + \deg(Q) = \deg(PQ) = \deg(1) = 0$. En particulier, $\deg(P) \neq -\infty$ et $\deg(Q) \neq -\infty$. Donc, $\deg(P)$ et $\deg(Q)$ sont des entiers naturels dont la somme est égale à 0. D'où $\deg(P) = 0$. □

Définition 4.1.6. Soient $A, B \in K[X]$. On dit que A *divise* B dans $K[X]$ s'il existe $C \in K[X]$ tel que $CA = B$. On note $A|B$ lorsque A divise B.

Proposition 4.1.7. *Soient $A, B, C \in K[X]$.*

1. *$A|A$.*
2. *Si $A|B$ et $B|A$, alors il existe $\lambda \in K^\star$ tel que $B = \lambda A$.*
3. *Si $A|B$ et $B|C$, alors $A|C$.*
4. *Si $A|B$ et $A|C$,alors, $A|B + C$.*
5. *Si $A|B$, alors $CA|CB$.*
6. *Si $CA|CB$ et $C \neq 0$, alors $A|B$.*
7. *Si $A|B$ et $B \neq 0$, alors $\deg(A) \leq \deg(B)$.*

Démonstration. 1. Comme $1 \cdot A = A$ et $1 \in K[X]$, on a bien $A|A$.

2. Supposons que $A|B$ et $B|A$. Il existe donc $C, D \in K[X]$ tels que $CA = B$ et $DB = A$. Du coup, $A = DB = D(CA) = (DC)A$, et donc $(DC-1)A = 0$. Comme $K[X]$ est intègre, on en déduit que $DC = 1$ ou $A = 0$. Si $A = 0$, on a aussi $B = CA = 0$, et l'énoncé est vrai. Si $DC = 1$, le polynôme C est inversible dans $K[X]$. D'après Corollaire 4.1.5, il existe $\lambda \in K^\star$ tel que $C = \lambda$. Du coup, $B = CA = \lambda A$.

3. Si $A|B$ et $B|C$, il existe $D, E \in K[X]$ tels que $DA = B$ et $EB = C$. Du coup, $(ED)A = E(DA) = EB = C$. Comme $ED \in K[X]$, on a bien $A|C$.

4. Si $A|B$ et $A|C$, il existe $D, E \in K[X]$ tels que $DA = B$ et $EA = C$. Du coup, $(D + E)A = DA + EA = B + C$. Comme $D + E \in K[X]$, on a bien $A|B + C$.

5. Si $A|B$, il existe $D \in K[X]$ tel que $DA = B$. en multipliant par C, on a $D(CA) = CB$. Comme $D \in K[X]$, on a bien $CA|CB$.

6. Si $CA|CB$, il existe $D \in K[X]$ tel que $D(CA) = CB$. D'où $C(DA) = CB$, ou encore $C(DA - B) = 0$. Comme K est intègre et $C \neq 0$, on a $DA - B = 0$, i.e., $DA = B$. Il s'ensuit que A divise B.

7. Si $A|B$, il existe $C \in K[X]$ tel que $CA = B$. En particulier, $\deg(B) = \deg(CA) = \deg(C) + \deg(A)$. Comme $B \neq 0$, on a aussi $C \neq 0$, et donc $\deg(C) \geq 0$. D'où $\deg(B) \geq \deg(A)$. □

Théorème (la division euclidienne). *Soient $A, B \in K[X]$ avec $A \neq 0$. Il existe $Q, R \in K[X]$ tels que $B = QA + R$ et $\deg(R) < \deg(A)$. De plus, Q et R sont uniquement déterminés par ces conditions.*

Démonstration. Soit $\mathcal{R}$ l'ensemble des polynômes de la forme $B - QA$, où $Q \in K[X]$. L'ensemble des degrés des polynômes de $\mathcal{R}$ est le sous-ensemble $\deg(\mathcal{R})$ de $\mathbb{N} \cup \{-\infty\}$. Comme $\mathcal{R} \neq \emptyset$, le sous-ensemble $\deg(\mathcal{R})$ a un plus petit

élément. Soit d le plus petit élément de $\deg(\mathcal{R})$. Il existe $Q \in K[X]$ tel que $\deg(B-QA) = d$. Soit $R = B - QA$, et montrons que $\deg(R) < \deg(A)$.

Supposons, par l'absurde, que $\deg(R) \geq \deg(A)$. Comme $A \neq 0$, A a un coefficient dominant non nul a. Comme $\deg(R) \geq \deg(A)$, le polynôme R est non nul également, et a un coefficient dominant non nul r. Soit $e = \deg(A)$, et $S = R - ra^{-1}X^{d-e}A$. On a bien $S \in K[X]$ et $\deg(S) < \deg(R)$. De plus, $S = B - QA - ra^{-1}X^{d-e}A = B - (Q + ra^{-1}X^{d-e})A$, donc $S \in \mathcal{R}$ et $\deg(S) < \deg(R)$. Contradiction. □

Définition 4.1.8. Soient $A, B \in K[X]$ avec $A \neq 0$, et $Q, R \in K[X]$ tels que $B = QA + R$ avec $\deg(R) < \deg(A)$. Le polynôme Q est le *quotient*, et R est le *reste* dans la division euclidienne de B par A.

Proposition 4.1.9. *Soient $A, B \in K[X]$ avec $A \neq 0$. Soit R le reste dans la division euclidienne de B par A. Le polynôme A divise B dans $K[X]$ si et seulement si $R = 0$.*

Démonstration. Supposons que A divise B dans $K[X]$. Il existe donc $C \in K[X]$ tel que $CA = B$. Par unicité dans la division euclidienne, on a bien $R = 0$.

Réciproquement, supposons que $R = 0$. Soit Q le quotient dans la division euclidienne de B par A. On a donc $B = QA + R = QA$. Comme $Q \in K[X]$, le polynôme A divise bien B dans $K[X]$. □

Corollaire 4.1.10. *Soit L un corps contenant K comme sous-corps. Soient $A, B \in K[X]$. Alors, A divise B dans $K[X]$ si et seulement si A divise B dans $L[X]$.*

Démonstration. Comme l'énoncé est bien vrai lorsque $A = 0$, on peut supposer que $A \neq 0$. Soient Q et R le quotient et le reste, respectivement, dans la division euclidienne de B par A dans $K[X]$. On a donc $Q, R \in K[X]$ et $B = QA + R$, avec $\deg(R) < \deg(A)$. Comme $K \subseteq L$, on a aussi $K[X] \subseteq L[X]$. Le polynômes Q et R sont donc a fortiori des éléments de $L[X]$, et on a $B = QA + R$ dans $L[X]$, où $\deg(R) < \deg(A)$. Il s'ensuit que Q et R sont le quotient et le reste, respectivement, dans la division euclidienne de B par A dans $L[X]$. D'après Proposition 4.1.9, A divise B dans $K[X]$ si et seulement si $R = 0$. D'après cette même proposition, appliquée à A et B comme éléments de $L[X]$, on a $R = 0$ si et seulement si A divise B dans $L[X]$. □

Théorème (le développement de Taylor). *Soit $B \in K[X]$ de degré ≥ 1. Pour tout $A \in K[X]^\star$, il existe $n \in \mathbb{N}$, et $A_0, \ldots, A_n \in K[X]$ tels que*

$$A = A_n B^n + A_{n-1}B^{n-1} + \cdots + A_1 B + A_0$$

où $A_n \neq 0$ et $\deg(A_i) < \deg(B)$ pour $i = 0, \ldots, n$. De plus, l'entier naturel n et les polynômes $A_0, \ldots, A_n$ sont uniquement déterminés par ces conditions. En fait, n est le quotient dans la division euclidienne de $\deg(A)$ par $\deg(B)$.

Démonstration. On démontre l'énoncé par récurrence généralisée sur $\deg(A)$. L'énoncé est bien vrai pour tous les polynômes $A \in K[X]^\star$ avec $\deg(A) < \deg(B)$. Supposons que l'énoncé est vrai pour tous les polynômes dans $K[X]$ de degré $\leq d$, pour un certain $d \in \mathbb{N}$ avec $d \geq \deg(B) - 1$. Montrons qu'il est vrai au rang $d+1$. Soit donc $A \in K[X]$ un polynôme de degré $d+1$. Effectuer la division euclidienne de A par B nous donne des polynômes $Q, A_0 \in K[X]$ tels que $A = QB + A_0$, où $\deg(A_0) < \deg(B)$. Comme $\deg(B) \geq 1$, on a $\deg(Q) < \deg(A) = d + 1$. De plus, $Q \neq 0$ car $\deg(A) = d + 1 \geq \deg(B)$. D'après l'hypothèse de récurrence, il existe $A_1, \ldots, A_n \in K[X]$ tels que $Q = A_n B^{n-1} + \cdots + A_1$, où $\deg(A_i) < \deg(B)$ pour $i = 1, \ldots, n$, et $A_n \neq 0$. Du coup,

$$A = QB + A_0 = (A_n B^{n-1} + \cdots + A_1)B + A_0 = A_n B^n + \cdots + A_1 B + A_0.$$

Cela montre l'existence au rang $d + 1$.

Pour montrer l'unicité au rang $d + 1$, supposons que

$$A = A'_m B^m + \cdots + A'_1 B + A'_0,$$

où $A'_0, \ldots, A'_m \in K[X]$, avec $A_m \neq 0$ et $\deg(A'_i) < \deg(B)$ pour $i = 0, \ldots, m$. Soit $Q' = A'_m B^{m-1} + \cdots + A'_1$. On a $A = Q'B + A'_0$. D'après l'unicité dans la division euclidienne, on a $Q' = Q$ et $A'_0 = A_0$. Par hypothèse de récurrence, $m = n$, et $A'_i = A_i$ pour $i = 1, \ldots, n$. Cela montre l'unicité au rang $d+1$. □

Définition 4.1.11. Soit $A \in K[X]$ et $x \in K$. Soit $n \in \mathbb{N}$ et $a_0, \ldots, a_n \in K$ tels que $A = a_n X^n + \cdots + a_0$. L'*évaluation* de A en x est l'élément $A(x)$ de K défini par

$$A(x) = a_n x^n + \cdots + a_0.$$

On dit que x est *racine* de A si $A(x) = 0$.

Proposition 4.1.12. *Soient $A, B \in K[X]$ et $x \in K$. On a $(A + B)(x) = A(x) + B(x)$ et $(AB)(x) = A(x)B(x)$.*

Démonstration. Exercice. □

Proposition 4.1.13. *L'ensemble des racines de AB est la réunion de l'ensemble des racines de A et de celui de B.*

Démonstration. Soit $x \in K$. D'après Proposition 4.1.12, on a $(AB)(x) = A(x)B(x)$. Il s'ensuit que x est une racine de AB si et seulement si x est une racine de A ou de B. Par conséquent, l'ensemble des racines de AB est égal à la réunion de l'ensemble des racines de A et de celui de B. □

Proposition 4.1.14. *Soit $A \in K[X]$ et $x \in K$. Alors, x est racine de A si et seulement si le polynôme $X - x$ divise A.*

Démonstration. Supposons que le polynôme $X - x$ divise le polynôme A. Il existe donc $B \in K[X]$ tel que $A = (X - x)B$. D'après Proposition 4.1.12, on a $A(x) = (x - x)B(x) = 0$, i.e., x est une racine de A.

Réciproquement, supposons que x est une racine de A. Montrons que le polynôme $X - x$ divise A. Effectuons la division euclidienne de A par $X - x$. Soit Q le quotient et R le reste. On a $A = (X - x)Q + R$ et $\deg(R) < \deg(X - x) = 1$. Le polynôme R est donc un polynôme constant, i.e., $R \in K$ ou encore $R(x) = R$. Comme $A = (X - x)Q + R$ et comme x est une racine de A, on a

$$0 = A(x) = (x - x) \cdot Q(x) + R(x) = 0 \cdot Q(x) + R = R,$$

d'après Proposition 4.1.12. Comme $R = 0$, on a $A = (X - x)Q$ ce qui montre que $X - x$ divise A. □

Définition 4.1.15. Soit $A \in K[X]^\star$ et soit x une racine de A dans K. La *multiplicité* de la racine x de A est le plus grand entier $m \in \mathbb{N}$ tel que $(X-x)^m$ divise A.

Théorème 4.1.16. *Soit d un entier naturel et $A \in K[X]$ de degré d. Alors, le nombre de racines de A dans K, comptées avec leurs multiplicités, est inférieur à d.*

Démonstration. Démonstration par récurrence sur d. Lorsque $d = 0$, A est un polynôme constant non nul. Le polynôme A n'a donc aucune racine dans K. Cela montre bien l'énoncé au rang 0. Montrons l'hérédité ensuite. Supposons donc que l'énoncé est vrai pour tous les polynômes dans $K[X]$ de degré d, pour un certain entier naturel d. Montrons que l'énoncé est vrai au rang $d+1$. Soit donc $A \in K[X]$ de degré $d+1$. On montre que le nombre de racines de A, comptées avec leurs multiplicitées, est inférieur à $d+1$. Si A n'a pas de racine, cette assertion est bien vraie. On peut donc supposer que A admet au moins une racine dans K. Soit x une racine de A dans K. D'après Proposition 4.1.14, il existe un polynôme $B \in K[X]$ tel que $A = (X - x)B$. Comme $\deg(A) = d + 1$, le polynôme B est de degré d. D'après l'hypothèse de récurrence, le nombre de racines de B dans K, comptées avec leurs multiplicitées, est inférieur à d. Il s'ensuit que le nombre de racines de A, comptées avec leurs multiplicitées, est inférieur à $d + 1$. □

4.2 Le plus grand diviseur commun

Définition 4.2.1. Soient $A, B \in K[X]$. Un polynôme C est un *diviseur commun* de A et B si $C|A$ et $C|B$. Un polynôme C est un *plus grand* diviseur commun de A et B si les conditions suivantes sont vérifiées :

1. C est un diviseur commun de A et B, et
2. pour tout diviseur commun D de A et B, on a $D|C$.

On écrit $C = \mathrm{pgcd}(A, B)$ pour dire que C est un plus grand diviseur commun de A et B.

Proposition 4.2.2. *Soient $A, B \in K[X]$. Si A et B admettent un plus grand diviseur commun, alors il est unique à un scalaire non nul près.*

Démonstration. Supposons que C et C' sont plus grands diviseurs communs de A et B. Comme C est un plus grand diviseur commun et comme C' est un diviseur commun de A et B, le polynôme C' divise C. Il existe donc $D \in K[X]$ tel que $DC' = C$. Par symétrie, ou par un même argument, C divise C'. D'où l'existence d'un polynôme $D' \in K[X]$ tel que $D'C = C'$. Il vient que $C = DC' = D(D'C) = (DD')C$. D'où $(DD' - 1)C = 0$ dans $K[X]$. Comme $K[X]$ est intègre, on a $DD' - 1 = 0$ ou $C = 0$. Si $C = 0$, on a aussi $C' = 0$, et l'énoncé est vrai. Supposons donc que $C \neq 0$. Dans ce cas, $DD' = 1$, i.e., $D \in K[X]$ est inversible. D'après Corollaire 4.1.5, D est un scalaire non nul, i.e., $D = \lambda$, où $\lambda \in K^\star$. On a bien $C = \lambda C'$. □

L'énoncé suivant affirme que deux polynômes admettent un plus grand diviseur commun. De plus, il donne un algorithme rapide pour le déterminer.

Théorème (l'Algorithme d'Euclide). *Soient $A, B \in K[X]$ avec $B \neq 0$. On pose $R_{-1} = A$, $R_0 = B$, et, par récurrence, R_i est le reste de la division euclidienne de R_{i-2} par R_{i-1}, pour $i = 1, 2, 3, \ldots$ tant que $R_{i-1} \neq 0$. Soit n l'unique entier naturel tel que $R_{n-1} \neq 0$ et $R_n = 0$. Alors, R_{n-1} est un plus grand diviseur commun de A et B.*

Démonstration. Remarquons qu'il existe bien un entier naturel $n \in \mathbb{N}$ tel que $R_n = 0$, sinon la suite infini des degrés $\deg(R_i)$ serait une suite d'entiers naturels strictement décroissante, ce qui est impossible.

Soit C un polynôme. Soit $i \in \{0, \ldots, n\}$. Par définition de R_i, on a

$$R_{i-2} = Q_i R_{i-1} + R_i,$$

où Q_i est le quotient de la division euclidienne de R_{i-2} par R_{i-1}. On voit que C divise R_{i-2} lorsque C divise R_{i-1} et R_i. On a aussi

$$R_i = R_{i-2} - Q_i R_{i-1}.$$

D'où C divise R_i lorsque C divise R_{i-2} et R_{i-1}. Il s'ensuit que C est un diviseur commun de R_{i-2} et R_{i-1} si et seulement si C est un diviseur commun de R_{i-1} et R_i. On montre alors facilement, par récurrence sur i, que A et B ont les mêmes diviseurs communs que R_{i-1} et R_i, pour $i = 0, \ldots, n$. En particulier, A et B ont les mêmes diviseurs communs que R_{n-1} et R_n. Comme $R_n = 0$, les diviseurs communs de R_{n-1} et R_n sont les diviseurs de R_{n-1}. Donc, R_{n-1} et R_n admettent un plus grand diviseur commun, R_{n-1} par exemple, et de plus, ce plus grand diviseur commun est aussi plus grand diviseur commun de A et B. □

Théorème (l'Algorithme d'Euclide étendu). *Soient $A, B \in K[X]$. On pose $R_{-1} = a$, $R_0 = b$, et, par récurrence, R_i est le reste de la division euclidienne de R_{i-2} par R_{i-1}, pour $i = 1, 2, 3, \ldots$ tant que $R_{i-1} \neq 0$. Soit n l'unique entier naturel tel que $R_{n-1} \neq 0$ et $R_n = 0$. Soit Q_i le quotient de la division euclidienne de R_{i-2} par R_{i-1}, pour $i = 1, \ldots, n$. Soient $U_{-1} = 1$, $U_0 = 0$, $V_{-1} = 0$ et $V_0 = 1$. Définir U_i et V_i par récurrence pour $i = 1. \ldots, n-1$ par*

$$U_i = U_{i-2} - Q_i V_{i-1} \quad et \quad V_i = V_{i-2} - Q_i V_{i-1}.$$

Alors, R_{n-1} est un plus grand diviseur commun de A et B et

$$U_{n-1}A + V_{n-1}B = R_{n-1}.$$

Démonstration. On sait déjà que R_{n-1} est un plus grand diviseur commun de A et B. Montrons, par récurrence, que

$$U_i A + V_i B = R_i,$$

pour $i = -1, 0, 1, \ldots, n-1$. Par définition, c'est vrai pour $i = -1$ et $i = 0$. Supposons que c'est vrai jusqu'au rang $i-1$, pour un certain $i \geq 1$ et $\leq n-1$. Alors,

$$\begin{aligned} U_i A + V_i B &= (U_{i-2} - Q_i U_{i-1})A + (V_{i-2} - Q_i V_{i-1})B = \\ &= (U_{i-2}A + v_{i-2}B) - Q_i(U_{i-1}A + V_{i-1}B) = \\ &= R_{i-2} - Q_i R_{i-1} = R_i. \end{aligned}$$

On en déduit que, pour $i = n-1$, on a $U_{n-1}A + V_{n-1}B = R_{n-1}$. □

Théorème de Bézout. *Soient $A, B \in K[X]$. Soit C un diviseur commun de A et B. Alors, C est un plus grand diviseur commun de A et B si et seulement s'il existe des polynômes U, V tels que*

$$UA + VB = C.$$

Démonstration. Supposons qu'il existe $U, V \in K[X]$ tels que $UA+VB = C$. Montrons que C est un plus grand diviseur commun de A et B. D'après l'hypothèse, C est un diviseur commun de A et B. Montrons que tout autre diviseur commun de A et B divise C. Soit donc D un diviseur commun de A et B. Comme D divise A et B, D divise UA et VB, donc aussi leur somme $UA + VB = C$. Cela montre que C est un plus grand diviseur commun de A et B.

Réciproquement, supposons que C est un plus grand diviseur commun de A et B. D'après l'Algorithme d'Euclide étendu, il existe un plus grand diviseur commun D de A et B et des polynômes U et V tels que $UA + VB = D$. Comme C et D sont plus grands diviseurs communs de A et B, il existe $\lambda \in K^\star$ tel que $C = \lambda D$ d'après Proposition 4.2.2. Par conséquent, quitte à multiplier U et V par λ, il existe des polynômes U et V tels que $UA + VB = C$. □

Proposition 4.2.3. *Soient $A, B, C \in K[X]$. On a*

$$\mathrm{pgcd}(AB, AC) = A \cdot \mathrm{pgcd}(B, C).$$

Démonstration. Soit D le pgcd de B et C. Le produit AD est bien un diviseur commun de AB et AC. D'après le Théorème de Bézout, il existe $U, V \in K[X]$ tel que $UB+VC = D$. Du coup, $U(AB)+V(AC) = AD$. D'après le Théorème de Bézout, $\mathrm{pgcd}(AB, AC) = AD$. □

Définition 4.2.4. Soient $A, B \in K[X]$. On dit que A et B sont *premiers entre eux* si les seuls diviseurs communs de A et B sont les polynômes constants non nuls. De manière équivalente, A et B sont premiers entre eux si le polynôme constant 1 est un plus grand diviseur commun de A et B.

Corollaire 4.2.5. *Soient $A, B \in K[X]$. Les polynômes A et B sont premiers entre eux si et seulement s'il existe des polynômes U et V tels que*

$$UA + VB = 1.$$

Démonstration. Supposons qu'il existe $U, V \in K[X]$ tels que $UA + VB = 1$. Comme 1 est un diviseur commun de A et B, 1 est un plus grand diviseur commun d'après le Théorème de Bézout. Par conséquent, A et B sont premiers entre eux.

Réciproquement, supposons que A et B sont premiers entre eux. Cela veut dire que 1 est un plus grand diviseur commun de A et B. D'après le Théorème de Bézout, il existe $U, V \in K[X]$ tels que $UA + VB = 1$. □

Voici une application importante de Théorème de Bézout, ou plutôt de son corollaire.

Lemme de Gauss. *Soient $A, B, C \in K[X]$ tels que A divise BC. Si A et B sont premiers entre eux, alors A divise C.*

Démonstration. Comme A et B sont premiers entre eux, il existe $U, V \in K[X]$ tels que $UA + VB = 1$. Mulitplier cette équation par C donne $UAC + VBC = C$. Comme A divise UAC et A divise VBC par hypothèse, A divise leur somme qui est égale à C. □

Comme application du plus grand diviseur commun de deux polynômes, on peut démontrer que toute fraction rationnelle s'écrit de manière unique comme *fraction simple*, i.e., de la forme A/B où A et B sont des polynômes premiers entre eux.

Proposition 4.2.6. *Soit $F \in K(X)$. Il existe un unique couple (A, B) où $A \in K[X]$, $B \in K[X]^\star$ de coefficient dominant 1, avec A et B premiers entre eux et $F = A/B$.*

Démonstration. Montrons d'abord l'existence d'un tel couple. Comme F est une fraction rationnelle, il existe $A \in K[X]$ et $B \in K[X]^\star$, avec B de coefficient dominant 1, tels que $F = A/B$. Soit C un plus grand diviseur commun de A et B. On peut supposer que C est à coefficient dominant 1. Ecrire $A = CA'$ et $B = CB'$, où $A' \in K[X]$ et $B' \in K[X]^\star$, avec B' de coefficient dominant 1. On a $F = A'/B'$ et $\mathrm{pgcd}(A', B') = 1$. Cela montre l'existence.

Quand à l'unicité, supposons qu'il existe encore un couple (R, S), où $R \in K[X]$, $S \in K[X]^\star$ de coefficient dominant 1, et R et S premiers entre eux, tels que $F = R/S$. On a donc $A/B = R/S$, i.e., $AS = BR$. En particulier, S divise BR. Comme S et R sont premiers entre eux, S divise B, d'après le Lemme de Gauss. Par la même argument, B divise S. Il existe donc $\lambda \in K^\star$ tel que $B = \lambda S$. Comme les coefficients dominants de B et S sont tous les deux égaux à 1, $\lambda = 1$ et donc $B = S$. Du coup $AS = BR = SR$. Comme $S \neq 0$, on a aussi $A = R$. Cela montre l'unicité. □

4.3 Polynômes irréductibles

Définition 4.3.1. Soit $P \in K[X]$. Le polynôme P est *premier* ou *irréductible* dans $K[X]$ lorsque

1. $\deg(P) \geq 1$, et
2. si $P = AB$, où $A, B \in K[X]$, alors $\deg(A) = 0$ ou $\deg(B) = 0$.

Exemples 4.3.2. 1. Le polynôme $X^2 + 1$ est irréductible dans $\mathbb{R}[X]$. Montrons cela par l'absurde. Supposons que $X^2 + 1$ est réductible dans $\mathbb{R}[X]$.

Il existe donc $A, B \in \mathbb{R}[X]$ tels que $X^2 + 1 = AB$, avec $\deg(A) \neq 0$ et $\deg(B) \neq 0$. Comme $\deg(X^2+1) = 2$, on a forcément $\deg(A) = \deg(B) = 1$. Comme $\deg(A) = 1$, A admet une racine x dans $\mathbb{R}$. Comme $X^2 + 1 = AB$, le nombre réel x est aussi une racine de $X^2 + 1$. Contradiction, car $X^2 + 1$ n'a pas de racine dans $\mathbb{R}$. Cela montre que $X^2 + 1$ est irréductible dans $\mathbb{R}$.

2. Le polynôme $X^2 + 1$ est réductible dans $\mathbb{C}[X]$. En effet, dans $\mathbb{C}[X]$, ce polynôme se décompose comme $(X - i)(X + i)$ et est donc réductible.

3. Le polynôme X^2+1 est irréductible dans $\mathbb{Q}[X]$. En effet, soient $A, B \in \mathbb{Q}[X]$ tels que $X^2 + 1 = AB$. Comme $\mathbb{Q} \subseteq \mathbb{R}$, on a aussi $A, B \in \mathbb{R}[X]$ tels que $X^2+1 = AB$. On a vu ci-dessus, que X^2+1 est irréductible dans $\mathbb{R}[X]$. Donc $\deg(A) = 0$ ou $\deg(B) = 0$. Cela montre que $X^2 + 1$ est iréductible dans $\mathbb{Q}[X]$.

Proposition 4.3.3. *Soit $P \in K[X]$. Si $\deg(P) = 1$, alors P est irréductible dans $K[X]$.*

Démonstration. On a bien $\deg(P) \geq 1$. Supposons que $P = AB$, où $A, B \in K[X]$. On a $\deg(A)+\deg(B) = \deg(AB) = \deg(P) = 1$. Du coup, $\deg(A) = 0$ ou $\deg(B) = 0$. Cela montre que P est irréductible dans $K[X]$. □

Proposition 4.3.4. *Soit $P \in K[X]$ de degré ≥ 2. Si P admet une racine dans K, alors P n'est pas irréductible dans $K[X]$.*

Démonstration. Soit x une racine de P dans K. D'après Proposition 4.1.14, le polynôme $X - x$ divise P. Il existe donc $B \in K[X]$ tel que $P = (X - x)B$. Comme $\deg(P) \geq 2$, $\deg(B) \geq 1$. On a donc $\deg(B) \neq 0$, et bien sûr, $\deg(X - x) \neq 0$. Cela montre que P n'est pas irréductible dans $K[X]$. □

La réciproque de Proposition 4.3.4 est fausse comme montre l'exemple suivant.

Exemple 4.3.5. Le polynôme $X^4 + 1$ est réductible dans $\mathbb{R}[X]$, bien qu'il ne possède pas de racine dans $\mathbb{R}$. En effet, on a la décomposition

$$X^4 + 1 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1).$$

On admettra l'énoncé suivant.

Théorème fondamental de l'algèbre. *Soit $P \in \mathbb{C}[X]$ avec $\deg(P) \geq 1$. Alors, P admet une racine dans $\mathbb{C}$.* □

En général, il est difficile de déterminer les polynômes irréductibles de $K[X]$. Pour $K = \mathbb{R}$ ou $\mathbb{C}$, par contre, on sait caractériser très explicitement les polynômes irréductibles de $K[X]$, grâce au Théorème fondamental de l'algèbre, comme on verra ci-dessous.

Quand $K = \mathbb{C}$, la réciproque de Proposition 4.3.4 est vraie :

Corollaire 4.3.6. *Soit $P \in \mathbb{C}[X]$. Alors, P est irréductible dans $\mathbb{C}[X]$ si et seulement si* $\deg(P) = 1$.

Démonstration. D'après Proposition 4.3.4 et le Théorème fondamental de l'algèbre, les polynômes dans $\mathbb{C}[X]$ de degré ≥ 2 ne sont pas irréductibles. Du coup, si P est irréductible, $\deg(P) = 1$.

Réciproquement, si $\deg(P) = 1$, P est irréductible dans $\mathbb{C}[X]$ d'après Proposition 4.3.3. □

Corollaire 4.3.7. *Soit $P \in \mathbb{R}[X]$. Le polynôme P est irréductible dans $\mathbb{R}[X]$ si et seulement si*

1. $\deg(P) = 1$, *ou*
2. $\deg(P) = 2$ *et le discriminant de P est strictement négatif.*

Démonstration. Montrons d'abord que si l'une des deux conditions ci-dessus est satisfaite, alors P est irréductible dans $\mathbb{R}[X]$. Si $\deg(P) = 1$, c'est une conséquence de la Proposition 4.3.3. On peut donc supposer que $\deg(P) = 2$ et que le discriminant de P est strictment négatif. On montre que P est irréductible dans $\mathbb{R}[X]$. Supposons que $P = AB$ avec $A, B \in \mathbb{R}[X]$. Comme $\deg(P) = 2$, $\deg(A) = 0, 1$ ou 2. Si $\deg(A) = 1$, A admet une racine dans $\mathbb{R}$, et donc P admet une racine dans $\mathbb{R}$. Mais dans ce cas, le discriminant de P serait positif, ce qui est contradictoire à l'hypothèse. par conséquent $\deg(A) = 0$, ou 2. Si $\deg(A) = 2$, $\deg(B) = 0$. On a donc bien montré que $\deg(A) = 0$ ou $\deg(B) = 0$. Par conséquent, P est irréductible.

Réciproquement, montrons que si P est irréductible dans $\mathbb{R}[X]$, alors P saitisfait l'une des deux conditios ci-dessus. Supposons donc que P est irréductible dans $\mathbb{R}[X]$. Par définition, $\deg(P) \geq 1$. Si $\deg(P) = 1$, alors P satisfait la première condition. On peut donc supposer que $\deg(P) \geq 2$. On montre que P satisfait la deuxième condition. Comme $\mathbb{R} \subseteq \mathbb{C}$, on a aussi $P \in \mathbb{C}[X]$. Comme $\deg(P) \geq 1$, P admet une racine dans $\mathbb{C}$ d'après le Théorème fondamental de l'algèbre. Soit α donc une racine de P dans $\mathbb{C}$. D'après Proposition 4.1.14, $X - \alpha$ divise P dans $\mathbb{C}[X]$. Comme $P \in \mathbb{R}[X]$, le conjugé $\overline{\alpha}$ est aussi une racine de P, et $X - \overline{\alpha}$ divise également P dans $\mathbb{C}[X]$. Comme P est irréductible dans $\mathbb{R}[X]$ et comme $\deg(P) \geq 2$, le polynôme P n'a pas de racine dans $\mathbb{R}$ d'après Proposition 4.3.4. En particulier, α n'est pas un nombre réel, i.e., $\overline{\alpha} =\neq \alpha$. Du coup, les polynômes $X - \alpha$ et $X - \overline{\alpha}$ sont premiers entre eux. Comme ils divisent P tous les deux, leur produit divise P. Or, le produit

$$(X - \alpha)(X - \overline{\alpha}) = X^2 - (\alpha + \overline{\alpha})X + \alpha\overline{\alpha} = X^2 - 2\mathrm{Re}(\alpha)X + |\alpha|^2$$

est un polynôme dans $\mathbb{R}[X]$. Soit A ce polynôme. Comme A divise P dans $\mathbb{C}[X]$, et comme $A, P \in \mathbb{R}[X]$, le polynôme A divise aussi P dans $\mathbb{R}[X]$

d'après Corollaire 4.1.10. Comme P est irréductile dans $\mathbb{R}[X]$, $P = \lambda \cdot A$, pour un certain $\lambda \in \mathbb{R}^\star$. Par conséquent, $\deg(P) = 2$. De plus, comme P n'a pas de racine réelle, le discriminant de P est strictement négatif. □

4.4 La décomposition en facteurs irréductibles

Théorème (la décomposition en facteurs irréductibles). *Soit $A \in K[X]^\star$. Alors, il existe $\lambda \in K^\star$, un entier naturel n, des polynômes irréductibles $P_1, \ldots, P_n$, et des entiers naturels non nuls $e_1, \ldots, e_n$ tels que*

$$A = \lambda \cdot P_1^{e_1} \cdot \ldots \cdot P_n^{e_n}.$$

Remarque 4.4.1. Il y a aussi unicité de cette décomposition en polynômes irréductibles, mais sa formulation est un peu technique.

Définition 4.4.2. Soit $A \in K[X]^\star$. L'écriture $A = \lambda \cdot P_1^{e_1} \cdot \ldots \cdot P_n^{e_n}$ où $\lambda \in K^\star$, $P_1, \ldots, P_n$ sont des polynômes irréductibles de $K[X]$, et $e_1, \ldots, e_n$ sont des entiers naturels non nuls, est la *décomposition en facteurs irréductibles* de A.

Démonstration du Théorème de la décomposition en facteurs irréductibles. Montrons l'énoncé par récurrence généralisé sur $\deg(A)$. Si $\deg(A) = 0$, l'énoncé est trivialement vrai. Supposons que l'énoncé est vrai pour tous les polynômes non nuls de $K[X]$ de degré inférieur à d, pour un certain entier naturel d. Montrons que l'énoncé est vrai pour tout les polynômes de $K[X]$ de degré $d+1$. Soit $A \in K[X]$ de degré $d+1$. Si A est irréductible, l'énoncé est bien vrai. On peut donc supposer que A n'est pas irréductible. Comme $\deg(A) = d + 1 \geq 1$, il existe $B, C \in K[X]$ tels que $A = BC$, où $\deg(B) \neq 0$ et $\deg(C) \neq 0$. Du coup, $\deg(B) < \deg(A)$ et $\deg(C) < \deg(A)$. D'après l'hypothèse de récurrence, B et C se décomposent en produit de facteurs irréductibles. Il en est donc de même de $BC = A$. □

Corollaire 4.4.3. *Soit $A \in \mathbb{C}[X]^\star$. Soient $a_0, \ldots, a_d \in \mathbb{C}$, avec $a_d \neq 0$, tels que $A = a_d X^d + \cdots + a_0$. Alors, il existe $n \in \mathbb{N}$, $\alpha_1, \ldots \alpha_n \in \mathbb{C}$ deux-à deux distincts, et $e_1, \ldots, e_n \in \mathbb{N}^\star$ tels que*

$$A = a_d (X - \alpha_1)^{e_1} \cdots (X - \alpha_n)^{e_n}.$$

En particulier, les racines de A sont les nombres complexes $\alpha_1, \ldots, \alpha_n$. De plus, la multiplicité de la racine α_i de A est égale à e_i.

Démonstration. D'après Théorème 4.4, il existe $\lambda \in \mathbb{C}^\star$, $n \in \mathbb{N}$, des polynômes irréductibles $P_1, \ldots, P_n$ de $\mathbb{C}[X]$ et $e_1, \ldots, e_n \in \mathbb{N}^\star$ tels que $A = \lambda P_1^{e_1} \cdots P_n^{e_n}$. D'après Corollaire 4.3.6, les polynômes $P_1, \ldots, P_n$ sont tous de

degré 1. Soit λ_i le coefficient dominant de P_i. Il existe $\alpha_i \in \mathbb{C}$ tel que $\lambda_i^{-1} P_i = X - \alpha_i$. On a

$$A = \lambda P_1^{e_1} \cdots P_n^{e_n} = (\lambda \lambda_1^{e_1} \cdots \lambda_n^{e_n}) \cdot (X - \alpha_1)^{e_1} \cdots (X - \alpha_n)^{e_n}.$$

Comme le coefficient dominant du dernier membre est égal à $\lambda \lambda_1^{e_1} \cdots \lambda_n^{e_n}$, et celui du premier membre est égal à a_d, on a forcément $a_d = \lambda \lambda_1^{e_1} \cdots \lambda_n^{e_n}$. Du coup,

$$A = a_d (X - \alpha_1)^{e_1} \cdots (X - \alpha_n)^{e_n}.$$

En regroupant des facteurs si nécessaire, on peut supposer que les nombres complexes $\alpha_1, \ldots, \alpha_n$ sont deux-à-deux distincts. Cela montre la première assertion. Les autres assertions s'en déduisent facilement. □

4.5 La décomposition en éléments simples d'une fraction rationnelle

Théorème (la décomposition en éléments simples). *Soit F une fraction rationnelle dans $K(X)$, i.e., $F = \frac{A}{B}$, où $A, B \in K[X]$, avec $B \neq 0$. Soit $B = \lambda \cdot P_1^{e_1} P_2^{e_2} \cdots P_n^{e_n}$ la décomposition de B en facteurs irréductible. Alors il existe un polynôme $Q \in K[X]$ et des polynômes $R_{ij} \in K[X]$, pour $j = 1, \ldots, e_i$ et $i = 1, \ldots, n$, tels que*

$$F = Q + \frac{R_{11}}{P_1} + \frac{R_{12}}{P_1^2} + \cdots + \frac{R_{1e_1}}{P_1^{e_1}} + \frac{R_{21}}{P_2} + \frac{R_{22}}{P_2^2} + \cdots + \frac{R_{2e_2}}{P_2^{e_2}} + \cdots \cdots + \frac{R_{n1}}{P_n} + \frac{R_{n2}}{P_n^2} + \cdots + \frac{R_{ne_n}}{P_n^{e_n}},$$

où $\deg(R_{ij}) < \deg(P_i)$ pour tout $j = 1, \ldots, e_i$ et pour tout $i = 1, \ldots, n$. De plus, les polynômes Q et R_{ij} sont uniquement déterminés par ces conditions. En fait, Q est égal au quotient dans la division euclidienne de A par B.

Démonstration. Montrons d'abord l'existence de la décomposition. Quitte à remplacer A par $\lambda^{-1}A$ et B par λ^{-1}B, on peut supposer que $\lambda = 1$. Soient

$$B_i = \prod_{j \neq i} P_j^{e_j}$$

pour $i = 1, \ldots, n$. Donc, on a $B = B_i \cdot P_i^{e_i}$, pour tout i. Il est clair que les polynômes $B_1, \ldots, B_n$ sont premiers entre eux. Par conséquent, il existe des polynômes $A_1, \ldots, A_n$ tels que

$$A_1 B_1 + \cdots + A_n B_n = B.$$

Soit Q_i le quotient de la division euclidienne de A_i par $P_i^{e_i}$, et R_i le reste, pour $i = 1, \ldots, n$. Soit $Q = Q_1 + \cdots + Q_n$. On a

$$QB + R_1B_1 + \cdots + R_nB_n = Qb + (A_1 - Q_1P_1^{e_1})B_1 + \cdots + (A_n - Q_nP_n^{e_n})B_n = A,$$

où $\deg(R_i) < \deg(P_i^{e_i})$ pour tout $i = 1 \ldots, n$. D'après le développement de Taylor, on peut donc écrire R_i sous la forme

$$R_i = R_{i1}P_i^{e_i-1} + \cdots + R_{i2}P_i^{e_i-2} + \cdots + R_{i,e_i-1}P_i + R_{i,e_i},$$

où chaque polynômes R_{ij} satisfait $\deg(R_{ij}) < \deg(P_i)$. Par conséquent

$$\begin{aligned} F = \frac{A}{B} = \frac{QB + R_1B_1 + \cdots + R_nB_n}{B} = Q + \frac{R_1}{P_1^{e_1}} + \frac{R_2}{P_2^{e_2}} + \cdots + \frac{R_n}{P_n^{e_n}} = \\ = Q + \frac{R_{11}}{P_1} + \frac{R_{12}}{P_1^2} + \cdots + \frac{R_{1e_1}}{P_1^{e_1}} + \frac{R_{21}}{P_2} + \frac{R_{22}}{P_2^2} + \cdots + \frac{R_{2e_2}}{P_2^{e_2}} + \cdots \\ \cdots + \frac{R_{n1}}{P_n} + \frac{R_{n2}}{P_n^2} + \cdots + \frac{R_{ne_n}}{P_n^{e_n}}. \end{aligned}$$

Cela montre l'existence.

Montrons, ensuite, l'unicité des polynômes Q et R_{ij}. Supposons que Q' et R'_{ij} sont d'autres polynômes tels que

$$\begin{aligned} F = Q' + \frac{R'_{11}}{P_1} + \frac{R'_{12}}{P_1^2} + \cdots + \frac{R'_{1e_1}}{P_1^{e_1}} + \frac{R'_{21}}{P_2} + \frac{R'_{22}}{P_2^2} + \cdots + \frac{R_{2e'_2}}{P_2^{e_2}} + \cdots \\ \cdots + \frac{R'_{n1}}{P_n} + \frac{R'_{n2}}{P_n^2} + \cdots + \frac{R'_{ne_n}}{P_n^{e_n}}, \end{aligned}$$

où $\deg(R'_{ij}) < \deg(P_i)$ pour $j = 1, \ldots, e_i$ et pour $i = 1, \ldots, n$. On montre que $Q = Q'$ et que $R_{ij} = R'_{ij}$ quels que soient i et j.

Posons $R'_i = R'_{i,1}P_i^{e_i-1} + \cdots + R_{i,e_i}P_i^0$. pour $i = 1, \ldots, n$. Comme on a $\deg(R_{ij}) < \deg(P_i)$, il suffit de montrer que $R_i = R'_i$ quel que soit i, d'après l'unicité du développement de Taylor. Or, on a

$$Q + \frac{R_1}{P_1^{e_1}} + \frac{R_2}{P_2^{e_2}} + \cdots + \frac{R_n}{P_n^{e_n}} = F = Q' + \frac{R'_1}{P_1^{e_1}} + \frac{R'_2}{P_2^{e_2}} + \cdots + \frac{R'_n}{P_n^{e_n}}.$$

Multiplier l'équation par B donne

$$BQ + B_1R_1 + B_2R_2 + \cdots + B_nR_n = BQ' + B_1R'_1 + B_2R'_2 + \cdots + B_nR'_n.$$

Prendre les congruences modulo $P_i^{e_i}$ de deux côtés donne

$$B_iR_i \equiv B_iR'_i \pmod{P_i^{e_i}}.$$

pour $i = 1, \ldots, n$. Comme B_i est inversible modulo $P_i^{e_i}$, on en déduit que $R_i \equiv R_i' \pmod{P_i^{e_i}}$. Comme $\deg(R_i) < \deg(P_i^{e_i})$ et $\deg(R_i') < \deg(P_i^{e_i})$, on a $R_i = R_i'$ pour $i = 1, \ldots, n$. Du coup, on a aussi $Q = Q'$. Cela montre l'unicité.

Il reste à montrer que Q est égal au quotient de la division euclidienne de A par B. Or, on a vu que

$$A = QB + R_1B_1 + \cdots + R_nB_n.$$

Comme $\deg(R_i) < \deg(P_i^{e_i})$ pour $i = 1, \ldots, n$, on a $\deg(R_iB_i) < \deg(B)$ pour tout i. Du coup, $\deg(R_1B_1 + \cdots + R_nB_n) < \deg(B)$. Il s'ensuit que Q est le quotient de la division euclidienne de A par B. □

La démonstration de l'existence de la décomposition en éléments simples d'une fraction rationnelle est constructive. Elle donne un algorithme pour déterminer cette décomposition, qui marche pour toute fraction rationnelle. En pratique, cependant, il y a souvent des méthodes bien plus rapides pour déterminer la décomposition en éléments simples d'une fraction rationnelle.

Définition 4.5.1. Soit $F \in K(X)$ un fraction rationnelle. Ecrire $F = \frac{A}{B}$, où A et B sont premiers entre eux. Un *racine* de F dans K est une racine du polynôme A. Un *pôle* de F dans K est une racine de B. La *multiplicité* d'une racine x de F dans K est la multiplicité de x comme racine de A. La *multiplicité* d'un pôle x de F dans K est la multiplicité de x comme racine de B. Un pôle de F est *simple* s'il est de multiplicité 1.

Les fractions rationnelles à pôles simples dans $\mathbb{C}$ sont particulièrement facile à décomposer en éléments simples comme montre l'exemple suivant.

Exemple 4.5.2. Soient $A = X^4 - 5X^3 + 11X^2 - 17X + 12$ et $B = X^3 - 6X^2 + 11X - 6$. Déterminons la décomposition en élṁents simples de la fraction rationnelle $F = \frac{A}{B}$ dans $\mathbb{Q}(X)$. Comme $\deg(A) \geq \deg(B)$, on effectue la division euclidienne de A par B et on obtient $A = QB + R$, où $Q = (X + 1)$ et $R = 6X^2 - 22X + 18$. Du coup,

$$F = \frac{A}{B} = \frac{QB + R}{B} = Q + \frac{R}{B} = X + 1 + \frac{R}{B}.$$

Décomposons B en facteurs irréductibles. On voit que 1 est une racine de B. Donc $X - 1$ divise B. On trouve $B = (X - 1)(X^2 - 5X + 6)$. Ce dernier facteurs se décompose comme $(X - 2)(X - 3)$. La décomposition en facteurs premiers de B est donc $B = (X - 1)(X - 2)(X - 3)$. Comme toutes les racines de B sont simples, la fraction rationnelle F est à pôles simples. D'après le théorème de la décomposition en éléments simples, on peut écrire

$$\frac{R}{B} = \frac{6X^2 - 22X + 18}{(X - 1)(X - 2)(X - 3)} = \frac{a}{X - 1} + \frac{b}{X - 2} + \frac{c}{X - 3},$$

où $a, b, c \in \mathbb{Q}$. Pour déterminer a, b, c on fait comme ceci. Pour déterminer a, on multiplie l'équation ci-dessus par $X - 1$, on simplifie, et on évalue en 1. On obtient

$$a = \frac{6 - 22 + 18}{(1-2)(1-3)} = 1.$$

De même, on obtient $b = 2$ et $c = 3$. Au final, la décomposition de F en éléments simples est

$$F = X + 1 + \frac{1}{X-1} + \frac{2}{X-2} + \frac{3}{X-3}.$$

Quand une fraction rationnelle a des pôles non simples la méthode ci-dessus ne marche que partiellement. On aura besoin d'un nouveau type de division d'un polynôme par un autre pour décomposer la fraction rationnelle en éléments simples.

Théorème (la division suivant les puissances croissantes). *Soient $A, B \in K[X]$ avec $B(0) \neq 0$. Soit $d \in \mathbb{N}$. Il existe $Q, R \in K[X]$ tels que*

$$A = QB + X^d R,$$

où $\deg(Q) < d$. De plus, Q et R sont uniquement déterminés par ces conditions.

Démonstration. Existence par récurrence sur d. Pou $d = 0$, on prend $Q = 0$ et $R = A$. Supposons qu'il existe $Q, R \in K[X]$ tels que $A = QB + X^d R$, où $\deg(Q) < d$. Ecrire $R = r - NX^n + \cdots + r_0$ et $B = b_m X^m + \cdots + b_0$. Comme $b_0 \neq 0, b_0^{-1} \in K$. On a $R - r_0 b_0^{-1} B = XR'$, pour un certain $R' \in K[X]$. Du coup, et

$$A - (Q + r_0 b_0^{-1} X^d)B = A - QB - r_0 b_0^{-1} X^d B = X^d R - r_0 b_0^{-1} X^d B = X^{d+1} R'.$$

Comme $\deg(Q + r_0 b_0^{-1} X^d) < d + 1$, cela montre l'existence au rang $d + 1$.

Pour l'unicité, supposons que $A = QB + X^d R = Q'B + X^d R'$. On a donc $(Q - Q')B = X^d(R' - R)$. Comme B et X^d sont premiers entre eux, X^d divise $Q - Q'$. Comme $\deg(Q - Q') < d$, on endéduit que $Q - Q' = 0$. D'où $Q = Q'$ et $R = R'$. □

Définition 4.5.3. L'écriture $A = QB + X^d R$ comme ci-dessus est la *division de A par B suivant les puissances croissantes* de X à l'ordre d.

Montrons par un exemple comment la division suivant les puissances croissantes permet de décomposer en éléments simples certaines fractions rationelles à pôles multiples.

Exemple 4.5.4. Soient $A = X^4 + 4X^3 + 6X^2 + 4X + 2$ et $B = (X^2 - 1)X^5$. Soit $F = \frac{A}{B}$. Comme 0 est un pôle de F de multiplicité 5, on effectue la division de A par $X^2 - 1$ selon les puissances croissantes de X à l'ordre 5. On obtient

$$A = -(2 + 4X + 8X^2 + 4X^3 + 8X^4)(X^2 - 1) + X^5(8X + 4).$$

D'où

$$\begin{aligned} F = \frac{A}{B} = \frac{-(2 + 4X + 8X^2 + 4X^3 + 8X^4)(X^2 - 1) + X^5(8X + 4)}{(X^2 - 1)X^5} = \\ = -\frac{(2 + 4X + 8X^2 + 4X^3 + 8X^4)}{X^5} + \frac{8X + 4}{X^2 - 1} = \\ = -\frac{2}{X^5} - \frac{4}{X^4} - \frac{8}{X^3} - \frac{4}{X^2} - \frac{8}{X} + \frac{6}{X - 1} + \frac{2}{X + 1}, \end{aligned}$$

où la décomposition en éléments simples

$$\frac{8X + 4}{X^2 - 1} = \frac{6}{X - 1} + \frac{2}{X + 1}$$

est obtenue par la méthode de l'Exemple 4.5.2.

Index