Licence première année
Cours de Logique et Algèbre 1
2018–2019

Luis Paris

1 Logique et raisonnements

1.1 Logique

Définition. Une *assertion* est une phrase soit vraie, soit fausse, mais pas les deux en même temps.

Exemples.

(1) "Il pleut".

(2) "Je suis plus petit que toi".

(3) "$2 + 2 = 4$"

(4) "$2 \times 3 = 7$"

Définition. Soient P et Q deux assertions. Alors l'assertion *"P et Q"* est vraie si P est vraie et Q est vraie. Elle est fausse sinon. On résume ceci dans une *table de vérité* comme suit.

P	V	V	F	F
Q	V	F	V	F
P et Q	V	F	F	F

Exemple. Soient P l'assertion "cette carte est un as" et Q l'assertion "cette carte est un coeur". Alors "P et Q" est vraie si la carte est l'as de coeur et est fausse sinon.

Définition. L'assertion *"P ou Q"* est vraie si l'une (au moins) des deux assertions P ou Q est vraie. Elle est fausse si les deux assertions P et Q sont fausses. On reprend ceci dans la table de vérité suivante.

P	V	V	F	F
Q	V	F	V	F
P ou Q	V	V	V	F

Exemple. Soient P l'assertion "cette carte est un as" et Q l'assertion "cette carte est un coeur". Alors "P ou Q" est vraie si la carte est un as ou bien un coeur. Elle est vraie pour l'as de coeur, mais aussi pour l'as de pique et le 10 de coeur. Elle est fausse pour le 10 de pique.

Définition. Soit P une assertion. L'assertion "non P" est vraie si P est fausse, et fausse si P est vraie. La table de vérité de "non P" est la suivante.

P	V	F
non P	F	V

Définition. Soient P et Q deux assertions. L'assertion "(non P) ou Q" se note "$P \Rightarrow Q$" et se lit *"P implique Q"* ou *"si P est vraie, alors Q est vraie"* ou, simplement, *"si P alors Q"* La table de vérité de cette assertion est la suivante.

P	V	V	F	F
Q	V	F	V	F
non P	F	F	V	V
$P \Rightarrow Q$	V	F	V	V

Exemples.

(1) " $(0 \leq x \leq 25) \Rightarrow (\sqrt{x} \leq 5)$" est vraie.

(2) "$(\sin(\theta) = 0) \Rightarrow (\theta = 0)$" est fausse.

(3) "$(2 + 2 = 5) \Rightarrow (\sqrt{2} = 2)$" est vraie.

Définition. Soient P et Q deux assertions. L'assertion "$(P \Rightarrow Q)$ et $(Q \Rightarrow P)$" se note "$P \Leftrightarrow Q$" et se lit *"P est équivalent à Q"* ou *"P équivaut à Q"* ou *"P si et seulement si Q"*. Cette assertion est vraie lorsque P et Q sont vraies ou lorsque P et Q sont fausses. Sa table de vérité est la suivante.

P	V	V	F	F
Q	V	F	V	F
$P \Leftrightarrow Q$	V	F	F	V

Exemples.

(1) Pour tout $x, y \in \mathbb{R}$ l'assertion "$(x \times y = 0) \Leftrightarrow ((x = 0)$ ou $(y = 0))$" est vraie.

(2) Soit P une assertion. Alors l'assertion "$P \Leftrightarrow$ (non P)" est fausse.

Proposition 1.1. *Soient P, Q, R trois assertions. Alors les assertions suivantes sont toujours vraies.*

(1) "$P \Leftrightarrow$ (non (non P))"

(2) *"(P et Q) ⇔ (Q et P)"*

(3) *"(P ou Q) ⇔ (Q ou P)"*

(4) *"(non (P et Q)) ⇔ ((non P) ou (non Q))"*

(5) *"(non (P ou Q)) ⇔ ((non P) et (non Q))"*

(6) *"(P et (Q ou R)) ⇔ ((P et Q) ou (P et R))"*

(7) *"(P ou (Q et R)) ⇔ ((P ou Q) et (P ou R))"*

(8) *"(P ⇒ Q) ⇔ ((non Q) ⇒ (non P))"*

Démonstration. (1), (2) et (3) sont assez évidentes. On va montrer (4) et (6) et laisser (5), (7) et (8) en exercice. Pour montrer qu'une de ces assertions est vraie, il suffit d'en faire sa table de vérité et constater que l'on a toujours "vraie" quelque soit les conditions initiales. Faisons la table pour l'assertion (4).

P	V	V	F	F
Q	V	F	V	F
P et Q	V	F	F	F
non (P et Q)	F	V	V	V
non P	F	F	V	V
non Q	F	V	F	V
(non P) ou (non Q)	F	V	V	V
(non (P et Q)) ⇔ ((non P) ou (non Q))	V	V	V	V

Donc l'assertion (4) est toujours vraie. Faisons la table de vérité de l'assertion (6).

P	V	V	V	V	F	F	F	F
Q	V	V	F	F	V	V	F	F
R	V	F	V	F	V	F	V	F
Q ou R	V	V	V	F	V	V	V	F
P et (Q ou R)	V	V	V	F	F	F	F	F
P et Q	V	V	F	F	F	F	F	F
P et R	V	F	V	F	F	F	F	F
(P et Q) ou (P et R)	V	V	V	F	F	F	F	F
(P et (Q ou R)) ⇔ ((P et Q) ou (P et R))	V	V	V	V	V	V	V	V

Donc l'assertion (6) est toujours vraie. □

Une assertion P peut dépendre d'un paramètre x. Par exemple l'assertion $P(x)$ donnée par "$x^2 \geq 1$" est vraie ou fausse selon la valeur de x.

Définition. L'assertion "$\forall x \in E$, $P(x)$" est une assertion vraie lorsque les assertions $P(x)$ sont vraies pour tous les éléments x de l'ensemble E. Elle se lit "*pour tout x dans E, $P(x)$*" ou "*pour tout x dans E, $P(x)$ est vraie*".

Exemples.

(1) "$\forall x \in [1, +\infty[,\ x^2 \geq 1$" est vraie.

(2) "$\forall x \in \mathbb{R},\ x^2 \geq 1$" est fausse.

Définition. L'assertion "$\exists x \in E,\ P(x)$" est une assertion vraie lorsque l'on peut trouver au moins un élément x dans E pour lequel $P(x)$ soit vraie. Elle se lit "*il existe x dans E tel que $P(x)$*" ou "*il existe x dans E tel que $P(x)$ soit vraie*".

Exemples.

(1) "$\exists x \in \mathbb{R},\ x(x-1) < 0$" est vraie.

(2) "$\exists x \in \mathbb{R},\ x^2 = -1$" est fausse.

Proposition 1.2.

(1) La négation de "$\forall x \in E,\ P(x)$" est "$\exists x \in E,$ non $P(x)$".

(2) La négation de "$\exists x \in E,\ P(x)$" est "$\forall x \in E,$ non $P(x)$".

Exemples.

(1) La négation de "$\exists z \in \mathbb{C},\ z^2 + z + 1 = 0$" est "$\forall z \in \mathbb{C},\ z^2 + z + 1 \neq 0$".

(2) La négation de "$\forall x \in \mathbb{R},\ x + 1 \in \mathbb{Z}$" est "$\exists x \in \mathbb{R},\ x + 1 \notin \mathbb{Z}$".

(3) La négation de "$\forall x \in \mathbb{R},\ \exists y > 0,\ x + y > 10$" est "$\exists x \in \mathbb{R},\ \forall y > 0, x + y \leq 10$".

1.2 Raisonnements

Définition. Soient P et Q deux assertions. On veut montrer que l'assertion "$P \Rightarrow Q$" est vraie. Pour cela on suppose que P est vraie et on montre directement que Q est vraie. C'est une démonstration par *raisonnement direct*.

Exemple. On veut montrer que, si $a, b \in \mathbb{Q}$, alors $a + b \in \mathbb{Q}$. Ici, P est "$a, b \in \mathbb{Q}$" et Q est "$a + b \in \mathbb{Q}$".

Démonstration. On suppose que $a, b \in \mathbb{Q}$. On peut donc écrire $a = \frac{p}{q}$ et $b = \frac{p'}{q'}$ avec $p, q, p', q' \in \mathbb{Z}$ et $q, q' \neq 0$. On a

$$a + b = \frac{p}{q} + \frac{p'}{q'} = \frac{pq' + qp'}{qq'}\,.$$

Cet élément appartient à $\mathbb{Q}$ car $pq' + qp', qq' \in \mathbb{Z}$ et $qq' \neq 0$. □

Définition. On veut montrer qu'une assertion $P(x)$ est vraie pour tout x dans un ensemble E. On écrit E comme la réunion de deux parties, $E = A \cup B$, et on montre que $P(x)$ est vraie pour tout $x \in A$, puis que $P(x)$ est vraie pour tout $x \in B$. C'est une démonstration *cas par cas*.

Exemple. On veut montrer que $|x-1| \leq x^2 - x + 1$ pour tout $x \in \mathbb{R}$. Ici $P(x)$ est "$|x-1| \leq x^2 - x + 1$", E est $\mathbb{R}$, $A = \{x \in \mathbb{R} \mid x \geq 1\}$ et $B = \{x \in \mathbb{R} \mid x \leq 1\}$.

Démonstration. Cas 1 : $x \geq 1$. Alors $|x-1| = x - 1$, donc

$$x^2 - x + 1 - |x-1| = x^2 - x + 1 - x + 1 = x^2 - 2x + 2 = (x-1)^2 + 1 \geq 0\,,$$

donc $|x-1| \leq x^2 - x + 1$.

Cas 2 : $x \leq 1$. Alors $|x-1| = -x + 1$, donc

$$x^2 - x + 1 - |x-1| = x^2 - x + 1 - (-x + 1) = x^2 \geq 0\,,$$

donc $|x-1| \leq x^2 - x + 1$. □

Définition. Soient P et Q deux assertions. On veut montrer que l'assertion "$P \Rightarrow Q$" est vraie. Rappelons que l'on a l'équivalence

$$(P \Rightarrow Q) \;\Leftrightarrow ((\text{non } Q) \Rightarrow (\text{non } P))$$

(voir la proposition 1.1 (8)). Donc, pour démontrer que "$P \Rightarrow Q$" est vraie on suppose que (non Q) est vraie et on montre que (non P) est vraie. C'est une démonstration par *contraposée*.

Exemple. Soit $n \in \mathbb{N}$. On veut montrer que, si n^2 est pair, alors n est pair. Ici P est "n^2 est pair", Q est "n est pair", (non P) est "n^2 est impair" et (non Q) est "n est impair".

Démonstration. On suppose que n est impair. Alors n s'écrit $n = 2k + 1$, avec $k \in \mathbb{N}$, donc $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ est impair. □

Définition. Soient P, Q deux assertions. Pour montrer que l'implication "$P \Rightarrow Q$" est vraie, on suppose que P et (non Q) sont vraies et on cherche une contradiction. Ainsi, si P est vraie, Q doit aussi être vraie. C'est une démonstration *par l'absurde*.

Exemple. Soient $a, b \geq 0$. On veut montrer que, si $\frac{a}{1+b} = \frac{b}{1+a}$, alors $a = b$. Ici P est "$\frac{a}{1+b} = \frac{b}{1+a}$", Q est "$a = b$" et (non Q) est "$a \neq b$".

Démonstration. On suppose que $\frac{a}{1+b} = \frac{b}{1+a}$ et $a \neq b$.

$$\frac{a}{1+b} = \frac{b}{1+a} \;\Rightarrow\; a(1+a) = b(1+b) \;\Rightarrow a + a^2 = b + b^2$$
$$\Rightarrow\; a^2 - b^2 = b - a \;\Rightarrow\; (a-b)(a+b) = -(a-b)\,.$$

Comme $a \neq b$, on a $a - b \neq 0$, donc on peut diviser la dernière égalité par $a - b$ ce qui donne $a + b = -1 < 0$: absurde. En conclusion, si $\frac{a}{1+b} = \frac{b}{1+a}$, alors $a = b$. □

Définition. Pour démontrer qu'une assertion de la forme "$\forall x \in E,\ P(x)$" est fausse, il faut montrer que sa négation, "$\exists x \in E,$ non $P(x)$" est vraie. En d'autre termes, il faut montrer qu'il existe un $x \in E$ (plus ou moins explicite) tel que $P(x)$ soit fausse. Un tel x s'appelle un *contre-exemple* à l'assertion "$\forall x \in E,\ P(x)$".

Exemple. On veut montrer que l'assertion "toute somme de deux nombres entiers positifs est paire" est fausse. Ici $E = (\mathbb{N} \times \mathbb{N})$, et $P(a, b)$ est "$a + b$ est pair". On doit montrer que "$\exists (a, b) \in (\mathbb{N} \times \mathbb{N}),\ a + b$ est impair". Soit $(a, b) = (1, 2)$. Alors $1 + 2 = 3$ est impair, donc l'assertion "$\exists (a, b) \in (\mathbb{N} \times \mathbb{N}),\ a + b$ est impair" est vraie, donc l'assertion "$\forall (a, b) \in (\mathbb{N} \times \mathbb{N}),\ a + b$ est pair" est fausse.

Théorème (Axiome). *Soit $P(n)$ une assertion dépendant d'un entier $n \in \mathbb{N}$.*

$$(\forall n \in \mathbb{N},\ P(n)) \ \Leftrightarrow\ (P(0) \text{ et } (\forall n \in \mathbb{N},\ (P(n) \Rightarrow P(n+1)))\,.$$

Définition. Pour démontrer qu'une assertion $P(n)$, dépendant d'un entier n, est vraie pour tout $n \in \mathbb{N}$, on procède en trois étapes.

- *Initialisation :* On démontre $P(0)$.
- *Hérédité :* Fixons $n \geq 0$ et supposons que $P(n)$ est vraie. On démontre alors que $P(n + 1)$ est vraie.
- *Conclusion :* On rappelle que, par le principe de récurrence, $P(n)$ est vraie pour tout $n \in \mathbb{N}$.

Une démonstration qui suit ce schéma s'appelle une *démonstration par récurrence.*

Exemple. Montrons que pour tout $n \in \mathbb{N}$, $2^n > n$.

Démonstration. Pour $n \in \mathbb{N}$, notons $P(n)$ l'assertion "$2^n > n$". Nous allons démontrer par récurrence que $P(n)$ est vraie pour tout $n \in \mathbb{N}$.

- *Initialisation :* Pour $n = 0$ nous avons $2^0 = 1 > 0$. Donc $P(0)$ est vraie.
- *Hérédité :* Fixons $n \geq 0$. Supposons que $P(n)$ soit vraie. Nous allons montrer que $P(n + 1)$ est vraie.

  $$\begin{aligned} 2^{n+1} = 2^n + 2^n > n + 2^n \quad & \text{car par } P(n) \text{ nous savons } 2^n > n\,, \\ \geq n + 1 \quad & \text{car } 2^n \geq 1\,. \end{aligned}$$

  Donc $P(n + 1)$ est vraie.
- *Conclusion :* Par le principe de récurrence $P(n)$ est vraie pour tout $n \in \mathbb{N}$.

Remarque. Si on doit démontrer qu'une propriété est vraie pour tout $n \geq n_0$, alors on commence l'initialisation au rang n_0.

2 Ensembles et applications

2.1 Ensembles

Définition. Un *ensemble* est une collection d'éléments. *L'ensemble vide*, noté $\emptyset$, est l'ensemble qui ne contient aucun élément. On note $x \in E$ si x est un élément de E, et $x \notin E$ dans le cas contraire.

Définition. Soit E un ensemble. Une *partie* de E ou *sous-ensemble* de E est un ensemble F tel que tout élément de F appartient à E. L'écriture $F \subset E$ signifie que F est une partie de E. On note $\mathcal{P}(E)$ l'ensemble des parties de E.

Exemple. Soit $E = \{1, 2, 3\}$. $\{1, 2\}$ est une partie de E. Plus généralement, l'ensemble des parties de E est :

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

Définition. Soient E un ensemble et A, B deux parties de E.

- Le *complémentaire* de A dans E est $\complement_E A = \complement A = \{x \in E \mid x \notin A\}$. Deux façon plus générale, on pose $A \setminus B = \{x \in A \mid x \notin B\}$. Remarquer que $A \setminus B = \complement_A(A \cap B)$.
- *L'union* de A et B est $A \cup B = \{x \in E \mid x \in A \text{ ou } x \in B\}$.
- *L'intersection* de A et B est $A \cap B = \{x \in E \mid x \in A \text{ et } x \in B\}$.

Exemple. Soient $E = \{1, 2, 3, 4\}$, $A = \{1, 2\}$ et $B = \{2, 3\}$. Alors $\complement A = \{3, 4\}$, $A \cup B = \{1, 2, 3\}$ et $A \cap B = \{2\}$.

Proposition 2.1. *Soient A, B, C trois parties d'un ensemble E.*

(1) $A \cap B = B \cap A$ *et* $A \cup B = B \cup A$.

(2) $A \cap (B \cap C) = (A \cap B) \cap C$ *et* $A \cup (B \cup C) = (A \cup B) \cup C$.

(3) $A \cap \emptyset = \emptyset$, $A \cap A = A$, $A \cup \emptyset = A$, *et* $A \cup A = A$.

(4) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ *et* $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

(5) $\complement(\complement A) = A$.

(6) $\complement(A \cap B) = \complement A \cup \complement B$ *et* $\complement(A \cup B) = \complement A \cap \complement B$.

Démonstration. On démontre les égalités $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ et $\complement(A \cap B) = \complement A \cup \complement B$. Les égalités $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ et $\complement(A \cup B) = \complement A \cap \complement B$ sont laissées en exercice. Les autres assertions sont assez évidentes.

Soit $x \in E$. Alors

$$x \in A \cap (B \cup C) \;\Leftrightarrow\; (x \in A) \text{ et } (x \in (B \cup C)) \;\Leftrightarrow$$
$$(x \in A) \text{ et } ((x \in B) \text{ ou } (x \in C)) \;\Leftrightarrow\; ((x \in A) \text{ et } (x \in B)) \text{ ou } ((x \in A) \text{ et } (x \in C)) \;\Leftrightarrow$$
$$(x \in A \cap B) \text{ ou } (x \in A \cap C) \;\Leftrightarrow\; x \in (A \cap B) \cup (A \cap C)\,.$$

Donc $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Soit $x \in E$. Alors

$$x \in \complement(A \cap B) \Leftrightarrow x \notin (A \cap B) \Leftrightarrow \text{non } (x \in (A \cap B)) \Leftrightarrow$$
$$\text{non } ((x \in A) \text{ et } (x \in B)) \Leftrightarrow (\text{non } (x \in A)) \text{ ou } (\text{non } (x \in B)) \Leftrightarrow$$
$$(x \notin A) \text{ ou } (x \notin B) \Leftrightarrow (x \in \complement A) \text{ ou } (x \in \complement B) \Leftrightarrow x \in \complement A \cup \complement B\,.$$

Donc $\complement(A \cap B) = \complement A \cup \complement B$. □

Définition. Soient E et F deux ensembles. Le *produit cartésien* de E et F, noté $E \times F$, est l'ensemble des couples (x, y), où $x \in E$ et $y \in F$.

Exemple. Soient $E = \{1, 2, 3\}$ et $F = \{a, b\}$. Alors

$$E \times F = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}\,.$$

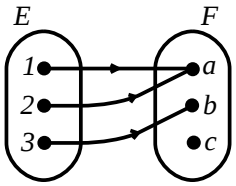
2.2 Applications

Définition. Soient E et F deux ensembles. Une *application* ou *fonction* de E dans F, notée $f : E \to F$, est la donnée pour tout élément $x \in E$ d'un unique élément de F noté $f(x)$.

Exemple. Soient $E = \{1, 2, 3\}$ et $F = \{a, b, c\}$. Soit $f : E \to F$ l'application définie par

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

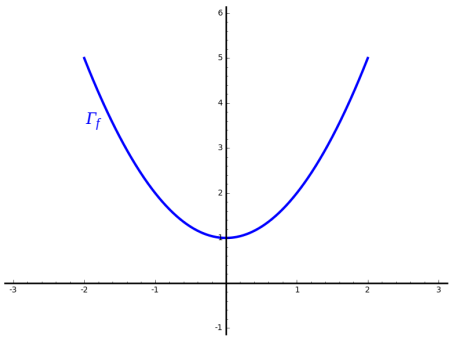
On représente graphiquement cette application comme suit.



Définition. Deux applications $f, g : E \to F$ sont *égales* si l'on a $f(x) = g(x)$ pour tout $x \in E$. On note alors $f = g$.

Définition. Le *graphe* d'une application $f : E \to F$ est $\Gamma_f = \{(x, f(x)) \mid x \in E\} \subset E \times F$.

Exemple. Soit $f : \mathbb{R} \to \mathbb{R}$ l'application définie par $f(x) = x^2 + 1$. Alors le graphe de f est représenté dans la figure ci-dessous.



Définition. Soient $f : E \to F$ et $g : F \to G$ deux applications. La *composition* de f et g est l'application $g \circ f : E \to G$ définie par $(g \circ f)(x) = g(f(x))$.

Exemple. Soient $f :]0, +\infty[\to]0, +\infty[$ et $g :]0, +\infty[\to \mathbb{R}$ les applications définies par

$$f(x) = \frac{1}{x}\,, \quad g(x) = \frac{x-1}{x+1}\,.$$

Alors $g \circ f :]0, +\infty[\to \mathbb{R}$ est donnée par

$$(g \circ f)(x) = g\left(\frac{1}{x}\right) = \frac{\frac{1}{x} - 1}{\frac{1}{x} + 1} = \frac{1-x}{1+x} = -\frac{x-1}{x+1} = -g(x)\,.$$

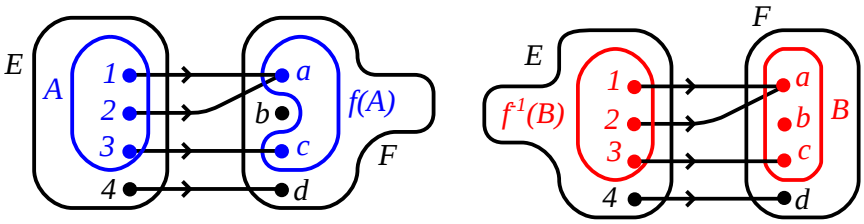
Définition. L'application *identité* d'un ensemble E est l'application $\mathrm{id}_E : E \to E$ qui envoie x sur x pour tout $x \in E$.

Définition. Soient $f : E \to F$ une application, $A \subset E$ et $B \subset F$. *L'image directe* de A par f est $f(A) = \{f(x) \mid x \in A\} \subset F$. *L'image réciproque* de B par f est $f^{-1}(B) = \{x \in E \mid f(x) \in B\} \subset E$.

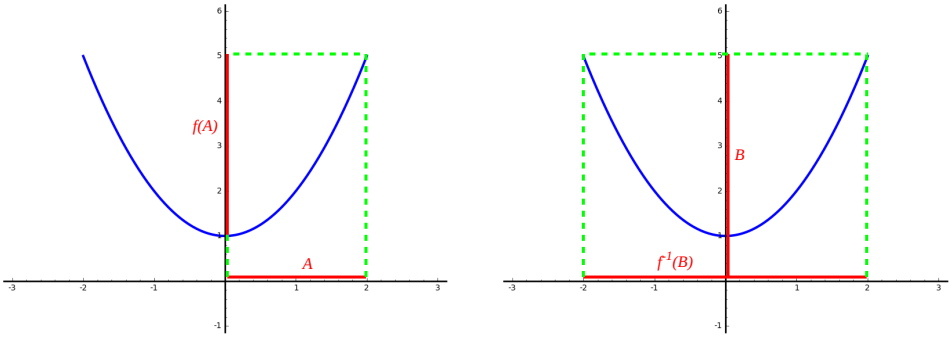
Exemple 1. Soient $E = \{1, 2, 3, 4\}$ et $F = \{a, b, c, d\}$. Soit $f : E \to F$ l'application définie par

$$f(1) = a,\ \ f(2) = a,\ \ f(3) = c,\ \ f(4) = d\,.$$

L'image directe de $A = \{1, 2, 3\}$ et $f(A) = \{a, c\}$. L'image réciproque de $B = \{a, b, c\}$ est $f^{-1}(B) = \{1, 2, 3\}$.



Exemple 2. Soit $f : \mathbb{R} \to \mathbb{R}$ l'application définie par $f(x) = x^2 + 1$. L'image directe de $A = [0, 2]$ est $[1, 5]$. L'image réciproque de $B = [0, 5]$ est $[-2, 2]$.



Définition. Soient $f : E \to F$ une application et $y \in F$. Un *antécédent* de y est un élément $x \in E$ tel que $f(x) = y$. Remarquer que l'ensemble des antécédents de y est $f^{-1}(\{y\})$ (que l'on note simplement $f^{-1}(y)$).

Définition. Soit $f : E \to F$ une application. On dit que f est *injective* si, pour tous $x, x' \in E$, l'égalité $f(x) = f(x')$ implique $x = x'$. En d'autre termes, f est injective si, pour tout $y \in F$, il existe au plus un élément $x \in E$ tel que $f(x) = y$. On dit que f est *surjective* si, pour tout $y \in F$, il existe au moins un élément $x \in E$ tel que $f(x) = y$. On dit que f est *bijective* si elle est à la fois injective et surjective. En d'autres termes, f est bijective si, pour tout $y \in F$, il existe exactement un $x \in E$ tel que $f(x) = y$.

Exemples.

(1) Soient $E = \{1, 2, 3\}$, $F = \{a, b, c, d\}$ et $f : E \to F$ définie par

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

Alors f est injective mais pas bijective.

(2) Soient $E = \{1, 2, 3, 4\}$, $F = \{a, b, c\}$ et $f : E \to F$ définie par

$$f(1) = a,\ f(2) = b,\ f(3) = c,\ f(4) = c.$$

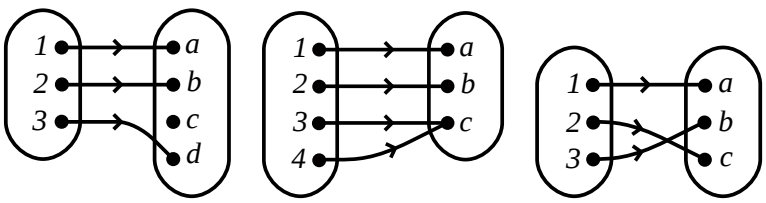
Alors f est surjective mais pas injective

(3) Soient $E = \{1, 2, 3\}$, $F = \{a, b, c\}$ et $f : E \to F$ définie par

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

Alors f est bijective.

Ces trois exemples sont illustrés dans la figure ci-dessous.



Proposition 2.2. *Soient E, F deux ensembles et $f : E \to F$ une application. Alors f est bijective si et seulement s'il existe une application $g : F \to E$ telle que $g \circ f = \mathrm{id}_E$ et $f \circ g = \mathrm{id}_F$. Dans ce cas l'application g est unique.*

Définition. L'application $g : F \to E$ de la proposition 2.2 s'appelle *l'application réciproque* de f et se note f^{-1}. Remarquer que $(f^{-1})^{-1} = f$.

Démonstration. Supposons que f est bijective. Par définition, pour tout $y \in F$, il existe un unique $x \in E$ tel que $f(x) = y$. On pose alors $g(y) = x$. Par définition on a $(f \circ g)(y) = f(x) = y$, pour tout $y \in F$, donc $f \circ g = \mathrm{id}_F$. Soit $x \in E$. On a

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

Comme f est injective, cette égalité implique que $(g \circ f)(x) = x$. On a donc $g \circ f = \mathrm{id}_E$.

Supposons qu'il existe une application $g : F \to E$ telle que $g \circ f = \mathrm{id}_E$ et $f \circ g = \mathrm{id}_F$. Soient $x, x' \in E$ tels que $f(x) = f(x')$. Alors $x = (g \circ f)(x) = (g \circ f)(x') = x'$. Ceci montre que f est injective. Soit $y \in F$. Posons $x = g(y)$. Alors $f(x) = (f \circ g)(y) = y$. Ceci montre que f est surjective.

Supposons qu'il existe deux applications $g, g' : F \to E$ telles que $g \circ f = g' \circ f = \mathrm{id}_E$ et $f \circ g = f \circ g' = \mathrm{id}_F$. Alors $g = \mathrm{id}_E \circ g = (g' \circ f) \circ g = g' \circ (f \circ g) = g' \circ \mathrm{id}_F = g'$. □

Proposition 2.3. *Supposons que $f : E \to F$ et $g : F \to G$ sont deux applications bijectives. Alors $g \circ f : E \to G$ est bijective et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Démonstration. On a

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ \mathrm{id}_F \circ g^{-1} = g \circ g^{-1} = \mathrm{id}_G\,.$$

De même, on a $(f^{-1} \circ g^{-1}) \circ (g \circ f) = \mathrm{id}_E$. Par la proposition 2.2 on en déduit que $g \circ f$ est bijective et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. □

2.3 Ensembles finis

Définition. Un ensemble E est *fini* s'il existe un entier $n \in \mathbb{N}$ et une bijection de E dans $\{1, \ldots, n\}$. Cet entier est unique, s'appelle le *cardinal* de E, et se note $\mathrm{Card}(E)$. Remarquer que $\emptyset$ est fini et $\mathrm{Card}(\emptyset) = 0$.

Lemme 2.4.

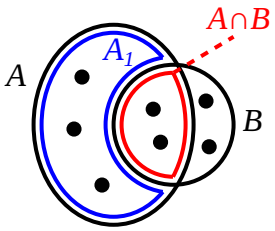
(1) Si A est un ensemble fini et $B \subset A$, alors B est fini et $\mathrm{Card}(B) \leq \mathrm{Card}(A)$.

(2) Si A et B sont deux ensembles finis disjoints (i.e. $A \cap B = \emptyset$), alors $A \cup B$ est fini et $\mathrm{Card}(A \cup B) = \mathrm{Card}(A) + \mathrm{Card}(B)$.

(3) Si A est un ensemble fini et $B \subset A$, alors $\mathrm{Card}(A \setminus B) = \mathrm{Card}(A) - \mathrm{Card}(B)$. En particulier, si $B \subset A$ et $\mathrm{Card}(B) = \mathrm{Card}(A)$, alors $A = B$.

(4) Soient A, B deux parties d'un ensemble fini E. Alors $\mathrm{Card}(A \cup B) = \mathrm{Card}(A) + \mathrm{Card}(B) - \mathrm{Card}(A \cap B)$.

Démonstration. Les assertions (1), (2) et (3) sont assez évidentes. Démontrons l'assertion (4). On pose $A_1 = A \setminus (A \cap B)$. On a $A = A_1 \cup (A \cap B)$ et $A_1 \cap (A \cap B) = \emptyset$, donc $\mathrm{Card}(A) = \mathrm{Card}(A_1) + \mathrm{Card}(A \cap B)$, donc $\mathrm{Card}(A_1) = \mathrm{Card}(A) - \mathrm{Card}(A \cap B)$. On a $A \cup B = A_1 \cup B$ et $A_1 \cap B = \emptyset$, donc $\mathrm{Card}(A \cup B) = \mathrm{Card}(A_1) + \mathrm{Card}(B) = \mathrm{Card}(A) - \mathrm{Card}(A \cap B) + \mathrm{Card}(B)$. □



Proposition 2.5. *Soient E, F deux ensembles finis et $f : E \to F$ une application.*

(1) Si f est injective, alors $\mathrm{Card}(E) \leq \mathrm{Card}(F)$.

(2) Si f est surjective, alors $\mathrm{Card}(E) \geq \mathrm{Card}(F)$.

(3) Si f est bijective, alors $\mathrm{Card}(E) = \mathrm{Card}(F)$.

Démonstration. Supposons que f est bijective. Soit $n = \mathrm{Card}(F)$. On choisit une bijection $g : F \to \{1, \ldots, n\}$. Alors $g \circ f : E \to \{1, \ldots, n\}$ est une bijection, donc $\mathrm{Card}(E) = n = \mathrm{Card}(F)$.

Supposons que f est injective. Soit $F' = f(E) \subset F$. On a une bijection $f' : E \to F'$, $x \mapsto f(x)$, donc $\mathrm{Card}(E) = \mathrm{Card}(F') \leq \mathrm{Card}(F)$.

Supposons que f soit surjective. Pour $y \in F$ on choisit un $x \in E$ tel que $f(x) = y$ et on pose $g(y) = x$. On a ainsi défini une application $g : F \to E$. Cette application est injective, en effet, si $g(y_1) = g(y_2)$, alors, par définition, $y_1 = f(g(y_1)) = f(g(y_2)) = y_2$. Par ce qui précède on en déduit que $\mathrm{Card}(F) \leq \mathrm{Card}(E)$. □

Proposition 2.6. *Soient E, F deux ensembles finis de même cardinal (i.e.* $\mathrm{Card}(E) = \mathrm{Card}(F)$*) et $f : E \to F$ une application. Les assertions suivantes sont équivalentes.*

(i) f est injective.

(ii) f est surjective.

(iii) f est bijective.

Démonstration. Les implications "(iii) ⇒ (i)" et "(iii) ⇒ (ii)" sont évidentes. On va montrer les deux autres implications, "(i) ⇒ (iii)" et "(ii) ⇒ (iii)".

Supposons que f est injective. Posons $F' = f(E) \subset F$. On a vu dans le démonstration de la proposition 2.5 que l'on a une bijection $f' : E \to F'$, $x \mapsto f(x)$. Alors $\mathrm{Card}(F) = \mathrm{Card}(E) = \mathrm{Card}(F')$, donc $F' = f(E) = F$, donc f est surjective. L'application f est injective et surjective, donc est bijective.

Supposons que f est surjective. Pour $y \in F$ on choisit un $x \in E$ tel que $f(x) = y$ et on pose $g(y) = x$. On a vu dans la démonstration de la proposition 2.5 que g est injective. On a aussi, par définition, $y = f(g(y)) = (f \circ g)(y)$ pour tout $y \in F$, c'est-à-dire $f \circ g = \mathrm{id}_F$. Comme $\mathrm{Card}(F) = \mathrm{Card}(E)$, par ce qui précède, g est une bijection. Alors

$$f = f \circ \mathrm{id}_E = f \circ (g \circ g^{-1}) = (f \circ g) \circ g^{-1} = \mathrm{id}_F \circ g^{-1} = g^{-1}$$

donc f est une bijection aussi. □

Proposition 2.7. *Soient E, F deux ensembles finis. Posons $n = \mathrm{Card}(E)$ et $p = \mathrm{Card}(F)$. Alors le nombre d'applications différentes de E dans F est p^n.*

Démonstration. On se fixe F de cardinal p et on montre l'assertion $P(n)$ suivante par récurrence sur n.

$P(n)$ Si E est un ensemble fini de cardinal n, alors le nombre d'applications de E dans F est p^n.

Initialisation. On suppose que $n = 1$. Soit a l'unique élément de E. Un application de E dans F est définie par l'image de a dans F. On a $\mathrm{Card}(F) = p$ choix, donc le nombre d'applications de E dans F est $p = p^1$. Donc $P(1)$ est vraie.

Hérédité. On suppose que $n \geq 1$ et $P(n)$ est vraie. On va montrer $P(n+1)$. Soit E un ensemble à $n+1$ éléments. On choisit $a \in E$ et on pose $E' = E \setminus \{a\}$. Par hypothèse de récurrence on a p^n applications de E' dans F. Chaque application $f' : E' \to F$ peut être prolongée en une application $f : E \to F$ en choisissant $f(a)$. On a p choix possibles pour un tel prolongement, donc, au final, on a $p^n \times p = p^{n+1}$ applications de E dans F.

Conclusion. Par le principe de récurrence $P(n)$ est vraie pour tout $n \geq 1$. □

Exemple. Soient $E = \{1, 2, 3\}$ et $F = \{a, b, c, d\}$. Alors le nombre d'applications de E dans F est $4^3 = 64$.

Proposition 2.8. *Soient E, F deux ensembles finis. On pose $n = \mathrm{Card}(E)$ et $p = \mathrm{Card}(F)$, et on suppose que $p \geq n$. Le nombre d'injections de E dans F est $p(p-1)\cdots(p-n+1)$.*

Remarque. Par la proposition 2.5 le nombre d'injections de E dans F est 0 si $p = \mathrm{Card}(F) < n = \mathrm{Card}(E)$.

Démonstration. On se fixe F de cardinal p et on montre l'assertion $P(n)$ suivante par récurrence sur n.

$P(n)$ Si E est un ensemble fini de cardinal n, alors le nombre d'injections de E dans F est $p(p-1)\cdots(p-n+1)$ si $n \leq p$ et est 0 sinon.

Initialisation. On suppose que $n = 1$. On a évidement $n \leq p$. Soit a l'unique élément de E. Un application de E dans F est définie par l'image de a dans F et cette application est toujours injective. On a $\mathrm{Card}(F) = p$ choix, donc le nombre d'injections de E dans F est p. Donc $P(1)$ est vraie.

Hérédité. On suppose que $n \geq 1$ et $P(n)$ est vraie. On va montrer $P(n+1)$. Soit E un ensemble à $n+1$ éléments. On sait par la proposition 2.5 que le nombre d'injections de E dans F est 0 si $p = \mathrm{Card}(F) < n+1 = \mathrm{Card}(E)$. On peut donc supposer que $n+1 \leq p$, c'est-à-dire $n < p$. On choisit $a \in E$ et on pose $E' = E \setminus \{a\}$. Par hypothèse de récurrence on a $p(p-1)\cdots(p-n+1)$ injections de E' dans F. Chaque injections $f' : E' \to F$ peut être prolongée en une injection $f : E \to F$ en choisissant $f(a) \in F \setminus f(E')$. On a $p-n$ choix possibles pour un tel prolongement, donc, au final, on a $p(p-1)\cdots(p-n+1)(p-n)$ injections de E dans F. Donc $P(n+1)$ est vraie.

Conclusion. Par le principe de récurrence $P(n)$ est vraie pour tout $n \geq 1$. □

Exemple. Soient $E = \{1, 2, 3\}$ et $F = \{a, b, c, d\}$. Alors le nombre d'injections de E dans F est $4 \times 3 \times 2 = 24$. Le nombre d'injections de F dans E est 0.

Définition. Soit n un nombre entier ≥ 1. Alors *factoriel* n est le nombre $n! = 1 \times 2 \times 3 \times \cdots \times (n-1) \times n$. Par convention on pose $0! = 1$.

Exemples. $1! = 1$, $2! = 2$, $3! = 2 \times 3 = 6$, $4! = 2 \times 3 \times 4 = 24$.

Corollaire 2.9. *Le nombre de bijections d'un ensemble E de cardinal n dans lui-même est $n!$.*

Démonstration. Par la proposition 2.6 le nombre de bijections de E dans E est égal au nombre d'injections de E dans E. Par la proposition 2.8 ce nombre est $n!$. □

Proposition 2.10. *Le nombre de sous-ensembles d'un ensemble E de cardinal n est* $\mathrm{Card}(\mathcal{P}(E)) = 2^n$.

Exemple. Soit $E = \{a, b, c\}$. Alors les parties de E sont

- une partie à 0 éléments, $\emptyset$,
- 3 singletons, $\{a\}, \{b\}, \{c\}$,
- 3 paires, $\{a, b\}, \{a, c\}, \{b, c\}$,
- $E = \{a, b, c\}$ lui-même.

Au total on a donc $1 + 3 + 3 + 1 = 8 = 2^3$ parties.

Démonstration. On note $\mathrm{App}(E, \{1, 0\})$ l'ensemble des applications de E dans $\{0, 1\}$. Rappelons que, par la proposition 2.7, on a $\mathrm{Card}(\mathrm{App}(E, \{0, 1\})) = 2^n$. Soit $\Phi : \mathcal{P}(E) \to$

$\mathrm{App}(E, \{0,1\})$ l'application définie comme suit. Soit F une partie de E. Alors $\Phi(F)$ est l'application $f : E \to \{0,1\}$ qui envoie x sur 1 si $x \in F$ et envoie x sur 0 sinon. Soit $\Psi : \mathrm{App}(E, \{0,1\}) \to \mathcal{P}(E)$ l'application qui à f associe le sous-ensemble $\{x \in E \mid f(x) = 1\}$. On a $\Psi \circ \Phi = \mathrm{id}$ et $\Phi \circ \Psi = \mathrm{id}$, donc Φ et Ψ sont des bijections, donc $\mathrm{Card}(\mathcal{P}(E)) = \mathrm{Card}(\mathrm{App}(E, \{0,1\})) = 2^n$. □

Définition. Le nombre de parties à k éléments d'un ensemble à n éléments se note $\binom{n}{k}$ (ou C_n^k).

Exemple. Soit $E = \{a, b, c, d\}$.

- E contient une unique partie à 0 éléments, $\emptyset$, donc $\binom{4}{0} = 1$.
- E contient 4 singletons, $\{a\}, \{b\}, \{c\}, \{d\}$, donc $\binom{4}{1} = 4$.
- E contient 6 paires, $\{a,b\}, \{a,c\}, \{a,d\}, \{b,c\}, \{b,d\}, \{c,d\}$, donc $\binom{4}{2} = 6$.
- E contient 4 parties à 3 éléments, $\{a,b,c\}, \{a,b,d\}, \{a,c,d\}, \{b,c,d\}$, donc $\binom{4}{3} = 4$.
- E contient une unique partie à 4 éléments, E, donc $\binom{4}{4} = 1$.

Proposition 2.11. *Soit $n \in \mathbb{N}^*$.*

(1) $\binom{n}{0} = 1$, $\binom{n}{1} = n$, *et* $\binom{n}{n} = 1$.

(2) On a $\binom{n}{k} = \binom{n}{n-k}$ *pour* $0 \leq k \leq n$.

(3) $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{k} + \cdots + \binom{n}{n} = 2^n$.

Démonstration. On a $\binom{n}{0} = 1$, car E contient une unique partie à 0 éléments, $\emptyset$. On a $\binom{n}{1} = n$, car E contient n singletons. On a $\binom{n}{n} = 1$, car E contient une unique partie à n éléments, E.

Pour $k \in \{0, 1, \ldots, n\}$ on note $\mathcal{P}_k(E)$ l'ensemble des parties de E de cardinal k. On a une bijection $\mathcal{P}_k(E) \to \mathcal{P}_{n-k}(E)$, $F \mapsto \complement F$, donc $\binom{n}{k} = \mathrm{Card}(\mathcal{P}_k(E)) = \mathrm{Card}(\mathcal{P}_{n-k}(E)) = \binom{n}{n-k}$.

L'égalité $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{k} + \cdots + \binom{n}{n} = 2^n$ découle directement du fait que le cardinal de $\mathcal{P}(E)$ est 2^n (voir la proposition 2.10). □

Proposition 2.12. *Soient $n \in \mathbb{N}^*$ et $k \in \{1, \ldots, n-1\}$. Alors* $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$.

Démonstration. Soit E un ensemble à n éléments. On choisit $a \in E$ et on pose $E' = E \setminus \{a\}$. Il y a deux sortes de sous-ensembles de E à k éléments :

(1) Ceux qui ne contiennent pas a. Ce sont donc les parties de E' à k éléments et il y en a $\binom{n-1}{k}$.

(2) Ceux qui contiennent a. Ils sont de la forme $A' \cup \{a\}$ où A' est une partie de E' à $k-1$ éléments. Il y en a donc $\binom{n-1}{k-1}$.

En conclusion, $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$. □

Définition. Le *triangle de Pascal* est un tableau qui donne $\binom{n}{k}$ à la n-ème ligne et k-éme colonne. Le terme à la (n,k)-ème place est la somme de celui qui se trouve à la $(n-1,k-1)$-ème place et celui qui se trouve à la $(n-1,k)$-ème place.

	0	1	2	3	4	5
0	1					
1	1	1				
2	1	2	1			
3	1	3	3	1		
4	1	4	6	4	1	
5	1	5	10	10	5	1

Proposition 2.13. *Soient $n \in \mathbb{N}^*$ et $k \in \{0, 1, \ldots, n\}$. Alors*

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}\,.$$

Démonstration. On démontre par récurrence sur n l'assertion suivante :
$P(n)$ $\forall k \in \{0, 1, \ldots, n\}$, $\binom{n}{k} = \frac{n!}{k!\,(n-k)!}$.

Initialisation. On sait par la proposition 2.11 que $\binom{1}{0} = 1 = \frac{1!}{0!\times 1!}$ et $\binom{1}{1} = \frac{1!}{1!\times 0!}$. Donc $P(1)$ est vraie.

Hérédité. On suppose que $P(n)$ est vraie et on démontre $P(n+1)$. On sait par la proposition 2.11 que $\binom{n+1}{0} = 1 = \frac{(n+1)!}{0!\times(n+1)!}$ et $\binom{n+1}{n+1} = 1 = \frac{(n+1)!}{(n+1)!\times 0!}$. Soit $k \in \{1, \ldots, n\}$. Alors, par la proposition 2.11 et l'hypothèse de récurrence,

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1} = \frac{n!}{k! \times (n-k)!} + \frac{n!}{(k-1)! \times (n-k+1)!} =$$
$$\frac{n!}{(k-1)! \times (n-k)!}\left(\frac{1}{k} + \frac{1}{n-k+1}\right) = \frac{n!}{(k-1)! \times (n-k)!} \times \frac{k+n-k+1}{k \times (n-k+1)} =$$
$$\frac{n! \times (n+1)}{(k-1)! \times k \times (n-k)! \times (n-k+1)} = \frac{(n+1)!}{k! \times (n-k+1)!}$$

Donc $P(n+1)$ est vraie.

Conclusion. Par le principe de récurrence $P(n)$ est vraie pour tout $n \geq 1$. □

Théorème 2.14 (Formule du binôme de Newton). *Soient $a, b \in \mathbb{R}$. Alors*

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

Exemples.

(1) Pour $n = 2$ on a $(a+b)^2 = a^2+2ab+b^2$. Pour $n = 3$ on a $(a+b)^3 = a^3+3a^2b+3ab^2+b^3$.

(2) Si $a = b = 1$, on retrouve la formule $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

Démonstration. On va démontrer par récurrence sur n l'assertion $P(n)$: "$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k$ ".

Initialisation. Pour $n = 1$ on a $(a+b)^1 = a+b = \binom{1}{0}a^1b^0 + \binom{1}{1}a^0b^1$. Donc $P(1)$ est vraie.

Hérédité. On suppose que $P(n)$ est vraie et on démontre $P(n+1)$.

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

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

$$a^{n+1} + \left(\sum_{k=1}^{n}\binom{n}{k}a^{n-k+1}b^k\right) + b^{n+1} + \left(\sum_{l=1}^{n}\binom{n}{l-1}a^{n-l+1}b^l\right) =$$

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

$$\binom{n+1}{0}a^{n+1}b^0 + \left(\sum_{k=1}^{n}\binom{n+1}{k}a^{n-k+1}b^k\right) + \binom{n+1}{n+1}a^0b^{n+1} = \sum_{k=0}^{n+1}\binom{n+1}{k}a^{n-k+1}b^k\,.$$

Donc $P(n+1)$ est vraie.

Conclusion. Par le principe de récurrence $P(n)$ est vraie pour tout $n \geq 1$. □

2.4 Relation d'équivalence

Définition. Soit E un ensemble. Une *relation* sur E est une partie $\mathcal{R} \subset (E \times E)$. La propriété $(x, y) \in \mathcal{R}$ se note $x\mathcal{R}y$.

Définition. Soit $\mathcal{R}$ une relation sur un ensemble E. On dit que $\mathcal{R}$ est *réflexive* si

- $\forall x \in E$, $x\mathcal{R}x$.

On dit que $\mathcal{R}$ est *symétrique* si

- $\forall x, y \in E$, $x\mathcal{R}y \;\Rightarrow\; y\mathcal{R}x$.

On dit que $\mathcal{R}$ est *transitive* si

- $\forall x, y, z \in E$, ($x\mathcal{R}y$ et $y\mathcal{R}z$) $\Rightarrow$ ($x\mathcal{R}z$).

Une *relation d'équivalence* est une relation réflexive, symétrique et transitive.

Exemples.

(1) La relation "être parallèle" est une relation d'équivalence sur l'ensemble des droites affines du plan.

(2) La relation "être perpendiculaire" n'est pas une relation d'équivalence sur l'ensemble des droites du plan, car n'est pas transitive.

(3) La relation $\leq$ dans $\mathbb{R}$ n'est pas symétrique, donc n'est pas une relation d'équivalence.

Définition. Soient $\mathcal{R}$ une relation d'équivalence sur E et x un élément de E. La *classe d'équivalence* de x est $\mathrm{cl}(x) = \{y \in E \mid y\mathcal{R}x\}$. Si C est une classe d'équivalence et $y \in C$, on dit que y est un *représentant* de C.

Définition. Une *partition* d'un ensemble E est une collection $\mathcal{U} \subset \mathcal{P}(E)$ de parties non vides de E telle que $\cup_{U\in\mathcal{U}} U = E$ et $U \cap V = \emptyset$ pour tout $U, V \in \mathcal{U}$, $U \neq V$.

Proposition 2.15. *Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E.*

(1) Pour tous $x, y \in E$ on a $\mathrm{cl}(x) = \mathrm{cl}(y) \Leftrightarrow x\mathcal{R}y$.

(2) Pour tous $x, y \in E$ on a $\mathrm{cl}(x) = \mathrm{cl}(y)$ ou $\mathrm{cl}(x) \cap \mathrm{cl}(y) = \emptyset$.

(3) L'ensemble des classes d'équivalence de $\mathcal{R}$ forme une partition de E.

Lemme 2.16. *Soient $E = \mathbb{Z} \times \mathbb{Z}^*$ et $\mathcal{R}$ la relation sur E définie par*
$(p, q)\mathcal{R}(p', q')$ *si* $pq' = p'q$.
Alors $\mathcal{R}$ est une relation d'équivalence.

Démonstration. Soit $(p, q) \in \mathbb{Z} \times \mathbb{Z}^*$. Comme $pq = pq$, on a $(p, q)\mathcal{R}(p, q)$. Ceci montre que $\mathcal{R}$ est réflexive. Soient $(p_1, q_1), (p_2, q_2) \in \mathbb{Z} \times \mathbb{Z}^*$ tels que $(p_1, q_1)\mathcal{R}(p_2, q_2)$. Alors $p_1q_2 = p_2q_1$, donc $p_2q_1 = p_1q_2$, donc $(p_2, q_2)\mathcal{R}(p_1, q_1)$. Ceci montre que $\mathcal{R}$ est symétrique. Soient $(p_1, q_1), (p_2, q_2), (p_3, q_3) \in \mathbb{Z}\times\mathbb{Z}^*$ tels que $(p_1, q_1)\mathcal{R}(p_2, q_2)$ et $(p_2, q_2)\mathcal{R}(p_3, q_3)$. Alors

$$p_1q_3q_2 = p_1q_2q_3 = p_2q_1q_3 = q_1p_2q_3 = q_1p_3q_2 = p_3q_1q_2\,,$$

donc $p_1q_3 = p_3q_1$, donc $(p_1, q_1)\mathcal{R}(p_3, q_3)$. Ceci montre que $\mathcal{R}$ est transitive. □

Définition. L'ensemble des classes d'équivalence de $\mathcal{R}$ dans $E = \mathbb{Z} \times \mathbb{Z}^*$ se note $\mathbb{Q}$ est s'appelle le *corps des nombres rationnels*. La classe d'équivalence d'une paire (p, q) se note $\frac{p}{q}$.

Lemme 2.17. *Soit $n \geq 2$ un entier fixé. Soit $\mathcal{R}$ la relation sur $E = \mathbb{Z}$ définie par*
$a\mathcal{R}b$ *si n divise $b - a$.*
Alors $\mathcal{R}$ est un relation d'équivalence.

Démonstration. Soit $a \in \mathbb{Z}$. Comme n divise $0 = a - a$ on a $a\mathcal{R}a$. Ceci montre que $\mathcal{R}$ est réflexive. Soient $a, b \in \mathbb{Z}$ tel que $a\mathcal{R}b$. Alors n divise $b - a$, donc n divise $a - b$, donc

$b\mathcal{R}a$. Ceci montre que $\mathcal{R}$ est symétrique. Soient $a, b, c \in \mathbb{Z}$ tels que $a\mathcal{R}b$ et $b\mathcal{R}c$. Alors n divise $b-a$ et $c-b$, donc n divise $(b-a)+(c-b) = c-a$, donc $a\mathcal{R}c$. Ceci montre que $\mathcal{R}$ est transitive. □

Définition. La relation $a\mathcal{R}b$ du lemme 2.17 se note $a \equiv b \pmod{n}$ et se lit "a est congru à b modulo n". La classe d'un entier $a \in \mathbb{Z}$ se note $\bar{a}$ (ou $[a]$). L'ensemble des classes d'équivalence se note $\mathbb{Z}/n\mathbb{Z}$.

Lemme 2.18. *Soit $n \geq 2$ un entier fixé. Alors $\mathbb{Z}/n\mathbb{Z}$ a exactement n éléments $[0], [1], \ldots, [n-1]$.*

Démonstration. Soit $a \in \mathbb{Z}$. Soit $a = qn + r$ la division de a par n. Alors $a - r = qn$ est divisible par n, donc $a \equiv r \pmod{n}$, donc $[a] = [r] \in \{[0], [1], \ldots, [n-1]\}$. Soient $a, b \in \{0, 1, \ldots, n-1\}$ tels que $[a] = [b]$. On peut sans perte de généralité supposer que $b \geq a$. Alors n divise $b-a$ et $0 \leq b-a \leq b < n-1$, donc $b-a = 0$, c'est-à-dire $a = b$. □

3 Nombres complexes

3.1 Définitions et propriétés

Définition. Un *nombre complexe* est un couple $(a, b) \in \mathbb{R}^2$ qui se note $a+ib$. L'ensemble des nombres complexes se note $\mathbb{C}$. Si $z = a + ib$ est un nombre complexe, a s'appelle sa *partie réelle* et se note $a = \mathrm{Re}(z)$ et b s'appelle sa *partie imaginaire* et se note $b = \mathrm{Im}(z)$. On dira que z est *réel* si $b = 0$. En d'autre termes, on suppose que $\mathbb{R}$ est le sous-ensemble de $\mathbb{C}$ des éléments de la forme $a + i\,0$, $a \in \mathbb{R}$. On dit que z est *imaginaire* s'il n'est pas réel, c'est-à-dire si $b \neq 0$. Si $a = 0$ (i.e. $z = ib$), on dit que z est un *imaginaire pur*.

Définition. On définit sur $\mathbb{C}$ deux opérations : *l'addition* par

$$\begin{array}{ccc} \mathbb{C} \times \mathbb{C} & \to & \mathbb{C} \\ (a+ib, a'+ib') & \mapsto & (a+ib)+(a'+ib') = (a+a')+i(b+b') \end{array}$$

et la *multiplication* par

$$\begin{array}{c} \mathbb{C} \times \mathbb{C} \to \mathbb{C} \\ (a+ib, a'+ib') \mapsto (a+ib) \times (a'+ib') = (aa'-bb')+i(ab'+a'b) \end{array}$$

Remarque.

(1) Si $a, a' \in \mathbb{R}$ alors

$$(a + i\,0) + (a' + i\,0) = (a+a') + i\,0\,, \quad (a + i\,0) \times (a' + i\,0) = aa' + i\,0\,,$$

c'est à dire l'addition et la multiplication de a et a' dans $\mathbb{C}$ coïncident avec celles de $\mathbb{R}$.

(2) Plus généralement, si $\lambda \in \mathbb{R}$ et $z = a + ib \in \mathbb{C}$, on a $\lambda \times z = (\lambda a) + i(\lambda b)$.

(3) On a $i^2 = i \times i = -1$.

Théorème 3.1. *L'ensemble $\mathbb{C}$ muni des deux opérations $+$ et $\times$ est un corps, c'est-à-dire qu'il vérifie les propriétés suivantes, où $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.*

(1) On a $z_1 + (z_2 + z_3) = (z_1 + z_2) + z_3$ pour tous $z_1, z_2, z_3 \in \mathbb{C}$.

(2) On a $z_1 + z_2 = z_2 + z_1$ pour tous $z_1, z_2 \in \mathbb{C}$.

(3) On a $z + 0 = z$ pour tout $z \in \mathbb{C}$.

(4) Pour tout $z \in \mathbb{C}$ il existe $z' \in \mathbb{C}$ (noté $z' = -z$) tel que $z + z' = 0$.

(5) On a $z_1 \times (z_2 \times z_3) = (z_1 \times z_2) \times z_3$ pour tous $z_1, z_2, z_3 \in \mathbb{C}$.

(6) On a $z_1 \times z_2 = z_2 \times z_1$ pour tous $z_1, z_2 \in \mathbb{C}$.

(7) On a $z \times 1 = z$ pour tout $z \in \mathbb{C}$.

(8) Pour tout $z \in \mathbb{C}^*$ il existe $z' \in \mathbb{C}^*$ (noté $z' = z^{-1}$) tel que $z \times z' = 1$.

(9) On a $z_1 \times (z_2 + z_3) = (z_1 \times z_2) + (z_1 \times z_3)$ pour tous $z_1, z_2, z_3 \in \mathbb{C}$.

Démonstration. On va montrer les parties (3), (4), (7), (8) et (9). Les parties (1), (2), (5) et (6) se démontrent avec des calculs directs que nous ne ferons pas.

Soit $z = a + ib \in \mathbb{C}$. Alors

$$z + 0 = (a + ib) + (0 + i\,0) = (a + 0) + i(b + 0) = a + ib = z\,.$$

Ceci montre la partie (3). Posons $z' = (-a) + i(-b)(= -z)$. Alors

$$z + z' = (a + ib) + ((-a) + i(-b)) = (a - a) + i(b - b) = 0 + i\,0 = 0\,.$$

Ceci montre la partie (4).

Soit $z = a + ib \in \mathbb{C}$. Alors

$$z \times 1 = (a + ib) \times (1 + i\,0) = (a \times 1 - b \times 0) + i(a \times 0 + 1 \times b) = a + ib = z\,.$$

Ceci montre la partie (7).

Soit $z = a + ib \in \mathbb{C}^*$. Comme $z \neq 0$, on a $a \neq 0$ ou $b \neq 0$, donc $a^2 + b^2 > 0$. On pose $z' = \frac{a}{a^2+b^2} + i\frac{-b}{a^2+b^2}(= z^{-1})$. Alors

$$z \times z' = (a + ib) \times \left(\frac{a}{a^2 + b^2} + i\frac{-b}{a^2 + b^2}\right) =$$

$$\left(a\frac{a}{a^2 + b^2} - b\frac{-b}{a^2 + b^2}\right) + i\left(a\frac{-b}{a^2 + b^2} + b\frac{a}{a^2 + b^2}\right) = \frac{a^2 + b^2}{a^2 + b^2} + i\frac{-ab + ba}{a^2 + b^2} = 1 + i\,0 = 1\,.$$

Ceci montre la partie (8)

Soient $z_1 = a_1 + ib_1, z_2 = a_2 + ib_2, z_3 = a_3 + ib_3 \in \mathbb{C}$. Alors

$$\begin{gathered}
z_1 \times (z_2 + z_3) = (a_1 + ib_1) \times \big((a_2 + ib_2) + (a_3 + ib_3)\big) = \\
(a_1 + ib_1) \times \big((a_2 + a_3) + i(b_2 + b_3)\big) = \\
\big(a_1(a_2 + a_3) - b_1(b_2 + b_3)\big) + i\big(a_1(b_2 + b_3) + b_1(a_2 + a_3)\big) = \\
\big((a_1a_2 - b_1b_2) + (a_1a_3 - b_1b_3)\big) + i\big((a_1b_2 + b_1a_2) + (a_1b_3 + b_1a_3)\big) = \\
\big((a_1a_2 - b_1b_2) + i(a_1b_2 + b_1a_2)\big) + \big((a_1a_3 - b_1b_3) + i(a_1b_3 + b_1a_3)\big) = \\
\big((a_1 + ib_1) \times (a_2 + ib_2)\big) + \big((a_1 + ib_1) \times (a_3 + ib_3)\big) = (z_1 \times z_2) + (z_1 \times z_3)\,.
\end{gathered}$$

□

Notation.

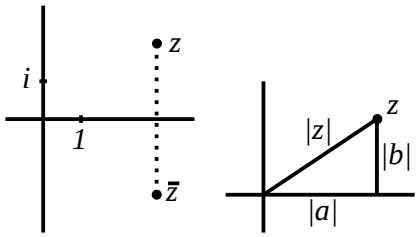
(1) Soient $z, z' \in \mathbb{C}$, $z' \neq 0$. Alors $\frac{z}{z'}$ désigne le nombre complexe $z \times z'^{-1}$. En particulier, $\frac{1}{z'} = z'^{-1}$.

(2) Soient $z \in \mathbb{C}$ et $n \in \mathbb{N}^*$. Alors z^n désigne $z \times z \times z \times \cdots \times z$ (n fois). Par exemple, $z^2 = z \times z$ et $z^3 = z \times z \times z$. Par convention on pose $z^0 = 1$ et $z^{-n} = \frac{1}{z^n} = (z^{-1})^n$. Remarquez que pour tous $n, m \in \mathbb{Z}$ on a $z^n \times z^m = z^{n+m}$.

Lemme 3.2. *Soient $z, z' \in \mathbb{C}$. On a $z\,z' = 0$ si et seulement si $z = 0$ ou $z' = 0$.*

Démonstration. Il est clair que, si $z = 0$ ou $z' = 0$, alors $z\,z' = 0$. Supposons que $z\,z' = 0$ et $z \neq 0$. Alors $z' = z^{-1}\,z\,z' = z^{-1}\,0 = 0$. □

Définition. Le *conjugué* d'un nombre complexe $z = a + ib$ est $\bar{z} = a - ib$. Le *module* de $z = a + ib$ est $|z| = \sqrt{a^2 + b^2}$.



Proposition 3.3.

(1) Soient $z, z' \in \mathbb{C}$. Alors $\overline{z + z'} = \bar{z} + \bar{z}'$, $\bar{\bar{z}} = z$ et $\overline{zz'} = \bar{z}\,\bar{z}'$.

(2) Soit $z \in \mathbb{C}$. On a $z = \bar{z}$ si et seulement si $z \in \mathbb{R}$.

(3) Soient $z, z' \in \mathbb{C}$. Alors $|z|^2 = z\,\bar{z}$, $|\bar{z}| = |z|$ et $|zz'| = |z| \times |z'|$.

(4) Soit $z \in \mathbb{C}$. On a $|z| = 0$ si et seulement si $z = 0$.

Démonstration. **(1)** Les égalités $\overline{z+z'} = \bar{z} + \bar{z}'$ et $\overline{\bar{z}} = z$ sont évidentes. Démontrons l'égalité $\overline{zz'} = \bar{z}\,\bar{z}'$. Posons $z = a + ib$ et $z' = a' + ib'$. Alors

$$\overline{zz'} = \overline{(aa' - bb') + i(ab' + ba')} = (aa' - bb') - i(ab' + ba') =$$
$$(aa' - (-b)(-b')) + i(a(-b') + (-b)a') = (a - ib)\,(a' - ib') = \bar{z}\,\bar{z}'\,.$$

(2) Soit $z = a + ib \in \mathbb{C}$. Alors

$$z = \bar{z} \Leftrightarrow a + ib = a - ib \Leftrightarrow b = -b \Leftrightarrow b = 0 \Leftrightarrow z \in \mathbb{R}\,.$$

(3) L'égalité $|z| = |\bar{z}|$ est assez évidente. On va démontrer les deux autres.

$$z\,\bar{z} = (a + ib)(a - ib) = (a^2 + b^2) + i((-ab) + ab) = a^2 + b^2 = |z|^2\,.$$

Il s'en suit que

$$|z\,z'|^2 = z\,z'\overline{z\,z'} = z\,z'\,\bar{z}\,\bar{z}' = (z\,\bar{z})\,(z'\,\bar{z}') = |z|^2\,|z'|^2\,,$$

donc $|zz'| = |z|\,|z'|$.

(4) Soit $z = a + ib \in \mathbb{C}$. Alors

$$|z| = 0 \Leftrightarrow |z|^2 = a^2 + b^2 = 0 \Leftrightarrow a = b = 0 \Leftrightarrow z = 0\,.$$

□

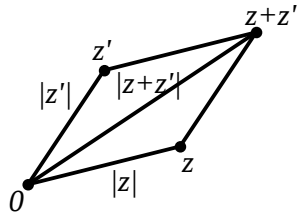
Lemme 3.4. *Soit* $z \in \mathbb{C}$. *Alors* $\mathrm{Re}(z) = \frac{z+\bar{z}}{2}$ *et* $\mathrm{Im}(z) = \frac{z-\bar{z}}{2i}$.

Démonstration. Soit $z = a + ib \in \mathbb{C}$. Alors

$$\frac{z + \bar{z}}{2} = \frac{(a + ib) + (a - ib)}{2} = \frac{2a}{2} = a = \mathrm{Re}(z)\,,$$
$$\frac{z - \bar{z}}{2i} = \frac{(a + ib) - (a - ib)}{2i} = \frac{2ib}{2i} = b = \mathrm{Im}(z)\,.$$

□

Proposition 3.5 (Inégalité triangulaire). *Soient* $z, z' \in \mathbb{C}$. *Alors* $|z + z'| \leq |z| + |z'|$.



Démonstration. On observe d'abord que, si $u = x + iy$, alors $\mathrm{Re}(u) = x \leq |x| \leq \sqrt{x^2 + y^2} = |u|$. Soient $z, z' \in \mathbb{C}$. Alors

$$|z + z'|^2 = (z + z')\,\overline{(z + z')} = (z + z')\,(\bar{z} + \bar{z}') = z\bar{z} + z'\bar{z}' + z\bar{z}' + \bar{z}z' =$$
$$|z|^2 + |z'|^2 + 2\,\mathrm{Re}(z\bar{z}') \leq |z|^2 + |z'|^2 + 2\,|z\bar{z}'| = |z|^2 + |z'|^2 + 2\,|z|\,|\bar{z}'| =$$
$$|z|^2 + |z'|^2 + 2\,|z|\,|z'| = (|z| + |z'|)^2\,.$$

□

3.2 Racines carrées et équations du second degré

Définition. Une *racine carrée* d'un nombre complexe $z \in \mathbb{C}$ est un nombre complexe $\omega \in \mathbb{C}$ tel que $\omega^2 = z$.

Proposition 3.6. *Soit $z \in \mathbb{C}$, $z \neq 0$. Alors z admet deux racines carrées (distinctes), ω et $-\omega$.*

Remarque.

(1) 0 a une unique racine carrée (double), 0.

(2) Contrairement au cas réel, il n'y a pas de façon privilégiée de choisir une racine carrée plutôt que l'autre. En d'autres termes, il n'y a pas de fonction racine carrée.

Démonstration. On pose $z = a + ib$. On cherche $\omega = x + iy \in \mathbb{C}$ tel que $\omega^2 = z$.

$$\omega^2 = z \;\Leftrightarrow\; (x+iy)^2 = a + ib \;\Leftrightarrow\; (x^2 - y^2) + 2ixy = a + ib \;\Leftrightarrow\; \begin{cases} x^2 - y^2 = a \\ 2xy = b \end{cases}$$

Petite astuce ici : nous ajoutons l'égalité

$$|\omega|^2 = |z| \;\Leftrightarrow\; x^2 + y^2 = \sqrt{a^2 + b^2}$$

(qui se déduit de $\omega^2 = z$) au système d'équations précédent. D'où

$$\omega^2 = z \;\Leftrightarrow\; \begin{cases} x^2 - y^2 = a \\ 2xy = b \\ x^2 + y^2 = \sqrt{a^2+b^2} \end{cases} \;\Leftrightarrow\; \begin{cases} 2x^2 = \sqrt{a^2+b^2} + a \\ 2y^2 = \sqrt{a^2+b^2} - a \\ 2xy = b \end{cases} \;\Leftrightarrow$$
$$\begin{cases} x = \pm\frac{1}{\sqrt{2}}\sqrt{\sqrt{a^2+b^2}+a} \\ y = \pm\frac{1}{\sqrt{2}}\sqrt{\sqrt{a^2+b^2}-a} \\ 2xy = b \end{cases}$$

Discutons suivant le signe de b. Supposons que $b > 0$. Alors x et y sont non nuls et de même signe, donc

$$\omega = \pm\frac{1}{\sqrt{2}}\left(\sqrt{\sqrt{a^2+b^2}+a} + i\sqrt{\sqrt{a^2+b^2}-a}\right).$$

Supposons que $b < 0$. Alors x et y sont non nuls et de signes opposés, donc

$$\omega = \pm\frac{1}{\sqrt{2}}\left(\sqrt{\sqrt{a^2+b^2}+a} - i\sqrt{\sqrt{a^2+b^2}-a}\right).$$

Supposons que $b = 0$ (i.e. $z \in \mathbb{R}$). Si $a > 0$, alors $\sqrt{a^2} = a$ donc $\omega = \pm\sqrt{a}$. Si $a < 0$, alors $\sqrt{a^2} = -a$, donc $\omega = \pm i\sqrt{-a} = \pm i\sqrt{|a|}$. □

Exemple. *Les racines carrées de i sont $\frac{\sqrt{2}}{2}(1+i)$ et $-\frac{\sqrt{2}}{2}(1+i)$.*

Démonstration. Soit $\omega = x + iy \in \mathbb{C}$.

$$\omega^2 = i \Leftrightarrow \begin{cases} x^2 - y^2 = 0 \\ 2xy = 1 \\ x^2 + y^2 = 1 \end{cases} \Leftrightarrow \begin{cases} 2x^2 = 1 \\ 2y^2 = 1 \\ 2xy = 1 \end{cases} \Leftrightarrow \begin{cases} x = \pm\frac{1}{\sqrt{2}} \\ y = \pm\frac{1}{\sqrt{2}} \\ 2xy \end{cases}$$

Ici $b > 0$, donc x et y sont non nuls et de même signe, donc

$$\omega = \pm\left(\frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}\right).$$

□

Définition. Une *équation (polynomiale) du second degré* (à coefficients complexes) est une expression de la forme $aZ^2 + bZ + c = 0$, où $a, b, c \in \mathbb{C}$, $a \neq 0$, et Z est un symbole appelé *inconnue*. Une *solution* à cette équation est un nombre complexe $z \in \mathbb{C}$ tel que $az^2 + bz + c = 0$. *Résoudre* cette équation est déterminer l'ensemble de ses solutions. Le *discriminant* de cette équation est $\Delta = b^2 - 4ac$.

Proposition 3.7. *Soient (E) $aZ^2 + bZ + c = 0$ une équation du second degré et $\Delta = b^2 - 4ac$ son discriminant.*

(1) Si $\Delta = 0$ alors (E) a une solution (double) unique $z = \frac{-b}{2a}$.

(2) Supposons que $\Delta \neq 0$. Soient δ et $-\delta$ les deux racines carrées de Δ. Alors (E) a deux solutions, $z_1 = \frac{-b+\delta}{2a}$ et $z_2 = \frac{-b-\delta}{2a}$.

Démonstration. Supposons que $\Delta = 0$. Soit $z \in \mathbb{C}$.

$$az^2 + bz + c = a\left(z^2 + \frac{b}{a}z + \frac{c}{a}\right) = a\left(\left(z + \frac{b}{2a}\right)^2 - \frac{b^2}{4a^2} + \frac{c}{a}\right) =$$

$$a\left(\left(z + \frac{b}{2a}\right)^2 - \frac{b^2 - 4ac}{4a^2}\right) = a\left(z + \frac{b}{2a}\right)^2.$$

Donc

$$az^2 + bz + c = 0 \Leftrightarrow a\left(z + \frac{b}{2a}\right)^2 = 0 \Leftrightarrow z = \frac{-b}{2a}.$$

Supposons que $\Delta \neq 0$. Soient $\delta, -\delta$ les deux racines carrées de Δ. Soit $z \in \mathbb{C}$. Alors

$$az^2 + bz + c = a\left(z^2 + \frac{b}{a}z + \frac{c}{a}\right) = a\left(\left(z + \frac{b}{2a}\right)^2 - \frac{b^2}{4a^2} + \frac{c}{a}\right) =$$

$$a\left(\left(z + \frac{b}{2a}\right)^2 - \frac{b^2 - 4ac}{4a^2}\right) = a\left(\left(z + \frac{b}{2a}\right)^2 - \frac{\Delta}{4a^2}\right) =$$

$$a\left(\left(z + \frac{b}{2a}\right)^2 - \frac{\delta^2}{4a^2}\right) = a\left(z + \frac{b}{2a} + \frac{\delta}{2a}\right)\left(z + \frac{b}{2a} - \frac{\delta}{2a}\right) = a(z - z_1)(z - z_2)$$

où $z_1 = \frac{-b+\delta}{2a}$ et $z_2 = \frac{-b-\delta}{2a}$. D'où

$$az^2 + bz + c = 0 \;\Leftrightarrow\; a(z - z_1)(z - z_2) = 0 \;\Leftrightarrow\; z = z_1 \text{ ou } z = z_2\,.$$

□

Exemple 1. On considère l'équation

$$(E) \quad Z^2 - (2i - 4)Z - 4i + 3 = 0\,.$$

Le discriminant de cette équation est

$$\Delta = (2i - 4)^2 - 4(-4i + 3) = -16i + 12 + 16i - 12 = 0\,,$$

donc (E) a une solution unique $z = \frac{2i-4}{2} = i - 2$.

Exemple 2. On considère l'équation

$$(E) \quad Z^2 - (3i - 1)Z - 3i - 4 = 0\,.$$

Le discriminant de cette équation est

$$\Delta = (3i - 1)^2 - 4(-3i - 4) = -6i - 8 + 12i + 16 = 6i + 8\,.$$

On cherche $\delta = x + iy$ tel que $\delta^2 = \Delta$. On a $|\Delta|^2 = 6^2 + 8^2 = 100$, donc $|\Delta| = 10$.

$$\delta^2 = \Delta \;\Leftrightarrow\; \left\{\begin{array}{l} x^2 - y^2 = 8 \\ 2xy = 6 \\ x^2 + y^2 = 10 \end{array}\right. \;\Leftrightarrow\; \left\{\begin{array}{l} 2x^2 = 18 \\ 2y^2 = 2 \\ 2xy = 6 \end{array}\right. \;\Leftrightarrow\; \left\{\begin{array}{l} x = \pm 3 \\ y = \pm 1 \\ 2xy = 6 \end{array}\right. \;\Leftrightarrow$$

$$\left\{\begin{array}{l} \delta = 3 + i \quad \text{ou} \\ \delta = -3 - i \end{array}\right.$$

On pose $\delta = 3 + i$. Alors les deux solutions de (E) sont

$$z_1 = \frac{(3i - 1) + (i + 3)}{2} = 2i + 1\,, \quad z_2 = \frac{(3i - 1) - (i + 3)}{2} = i - 2\,.$$

Corollaire 3.8. *Soient (E) $aZ^2+bZ+c = 0$ une équation du second degré avec $a, b, c \in \mathbb{R}$ et $\Delta = b^2 - 4ac$ son discriminant.*

(1) Si $\Delta = 0$ alors (E) a une solution (double) unique et réelle $z = \frac{-b}{2a}$.

(2) Si $\Delta > 0$ alors (E) a deux solutions réelles $z_1 = \frac{-b+\sqrt{\Delta}}{2a}$ et $z_2 = \frac{-b-\sqrt{\Delta}}{2a}$.

(3) Si $\Delta < 0$ alors (E) a deux solutions complexes non réelles $z_1 = \frac{-b+i\sqrt{-\Delta}}{2a}$ et $z_1 = \frac{-b-i\sqrt{-\Delta}}{2a}$.

3.3 Théorème fondamental de l'algèbre

Théorème 3.9 (d'Alembert–Gauss). *Soit* $P(Z) = a_n Z^n + a_{n-1}Z^{n-1} + \cdots + a_1 Z + a_0$ *un polynôme de degré* n *à coefficients dans* $\mathbb{C}$. *Alors il existe* $z_1, \ldots, z_n \in \mathbb{C}$ *tels que* $P(Z) = a_n(Z-z_1)(Z-z_2)\cdots(Z-z_n)$. *En particulier, les solutions de l'équation* $P(Z) = 0$ *sont* $z_1, \ldots, z_n$.

Exemple. Soit $P(Z) = aZ^2+bZ+c$, $a \neq 0$, un polynôme de degré 2. Posons $\Delta = b^2-4ac$. Si $\Delta = 0$, alors

$$P(Z) = aZ^2 + bZ + c = a\left(Z + \frac{b}{2a}\right)^2 = a(Z - z_1)(Z - z_2)\,,$$

où $z_1 = z_2 = \frac{-b}{2a}$. Supposons que $\Delta \neq 0$. Soit δ une racine carrée de Δ. Alors

$$P(Z) = aZ^2 + bZ + c = a\left(Z + \frac{b+\delta}{2a}\right)\left(Z + \frac{b-\delta}{2a}\right) = a(Z - z_1)(Z - z_2)\,,$$

où $z_1 = \frac{-b-\delta}{2a}$ et $z_2 = \frac{-b+\delta}{2a}$.

3.4 Arguments et trigonométrie

Rappels. Soit $\alpha \in \mathbb{R}$. Alors

$$\cos^2(\alpha) + \sin^2(\alpha) = 1\,,\ \operatorname{tg}(\alpha) = \frac{\sin(\alpha)}{\cos(\alpha)}\,,\ \operatorname{ctg}(\alpha) = \frac{1}{\operatorname{tg}(\alpha)}\,,$$
$$\frac{1}{cos^2(\alpha)} = 1 + \operatorname{tg}^2(\alpha)\,,\ \frac{1}{\sin^2(\alpha)} = 1 + \operatorname{ctg}^2(\alpha)\,.$$

Soit $\alpha \in \mathbb{R}$. Alors

$$\sin(-\alpha) = -\sin(\alpha)\,,\ \cos(-\alpha) = \cos(\alpha)\,,\ \sin(\pi-\alpha) = \sin(\alpha)\,,\ \cos(\pi-\alpha) = -\cos(\alpha)\,,$$
$$\sin(\pi+\alpha) = -\sin(\alpha)\,,\ \cos(\pi+\alpha) = -\cos(\alpha)\,,$$
$$\sin(\frac{\pi}{2}-\alpha) = \cos(\alpha)\,,\ \cos(\frac{\pi}{2}-\alpha) = \sin(\alpha)\,.$$

Soient $\alpha, \beta \in \mathbb{R}$. Alors

$$\sin(\alpha+\beta) = \sin(\alpha)\,\cos(\beta) + \cos(\alpha)\,\sin(\beta)\,,$$
$$\cos(\alpha+\beta) = \cos(\alpha)\,\cos(\beta) - \sin(\alpha)\,\sin(\beta)\,.$$

Soit $\alpha \in \mathbb{R}$. Alors

$$\sin(2\alpha) = 2\,\sin(\alpha)\cos(\alpha)\,,\ \cos(2\alpha) = \cos^2(\alpha) - \sin^2(\alpha)\,.$$

Soient $\alpha, \beta \in \mathbb{R}$. Alors

$$\sin(\alpha) + \sin(\beta) = 2\,\sin\left(\frac{\alpha+\beta}{2}\right)\,\cos\left(\frac{\alpha-\beta}{2}\right)\,,$$
$$\cos(\alpha) + \cos(\beta) = 2\,\cos\left(\frac{\alpha+\beta}{2}\right)\,\cos\left(\frac{\alpha-\beta}{2}\right)\,.$$

Soient $\alpha, \beta \in \mathbb{R}$. Alors

$$2\,\sin(\alpha)\,\sin(\beta) = -\cos(\alpha+\beta) + \cos(\alpha-\beta)\,,$$
$$2\,\sin(\alpha)\,\cos(\beta) = \sin(\alpha+\beta) + \sin(\alpha-\beta)\,,$$
$$2\,\cos(\alpha)\,\cos(\beta) = \cos(\alpha+\beta) + \cos(\alpha-\beta)\,.$$

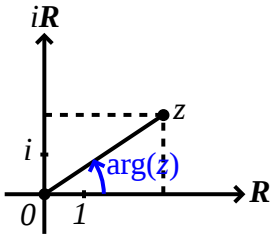
Rappel.

$$\cos(0) = 1\,,\ \sin(0) = 0\,,\ \cos\left(\frac{\pi}{2}\right) = 0\,,\ \sin\left(\frac{\pi}{2}\right) = 1\,,\ \cos\left(\frac{\pi}{6}\right) = \frac{\sqrt{3}}{2}\,,\ \sin\left(\frac{\pi}{6}\right) = \frac{1}{2}\,,$$
$$\cos\left(\frac{\pi}{4}\right) = \frac{\sqrt{2}}{2}\,,\ \sin\left(\frac{\pi}{4}\right) = \frac{\sqrt{2}}{2}\,,\ \cos\left(\frac{\pi}{3}\right) = \frac{1}{2}\,,\ \sin\left(\frac{\pi}{3}\right) = \frac{\sqrt{3}}{2}\,.$$

Définition. Soient $\theta, \theta' \in \mathbb{R}$. On pose $\theta \equiv \theta' \pmod{2\pi}$ s'il existe $k \in \mathbb{Z}$ tel que $\theta' = \theta + 2k\pi$. Remarquez que $\theta \equiv \theta' \pmod{2\pi}$ si et seulement si $\cos(\theta) = \cos(\theta')$ et $\sin(\theta) = \sin(\theta')$. En d'autre termes, on a $\theta \equiv \theta' \pmod{2\pi}$ si et seulement si θ et θ' mesurent le même angle.

Définition. Soit $\omega = x + iy \in \mathbb{C}$ tel que $|\omega| = 1$. On a $x^2 + y^2 = |\omega|^2 = 1$, donc il existe $\theta \in \mathbb{R}$ tel que $x = \cos(\theta)$ et $y = \sin(\theta)$, c'est-à-dire $\omega = \cos(\theta) + i\sin(\theta)$. Un tel nombre θ s'appelle un *argument* de ω. Remarquer qu'un argument n'est pas unique, mais θ' est un autres argument de ω si et seulement si $\theta \equiv \theta' \pmod{2\pi}$. De façon plus générale on a la définition suivante.

Définition. Soit $z \in \mathbb{C} \setminus \{0\}$. Soit $\omega = \frac{z}{|z|}$. On a $|\omega| = \frac{|z|}{|z|} = 1$, donc il existe $\theta \in \mathbb{R}$ tel que $\omega = \cos(\theta) + i\sin(\theta)$. De façon équivalente, $z = |z|(\cos(\theta) + i\sin(\theta))$. Un tel nombre θ s'appelle un *argument* de z et se note $\theta = \arg(z)$. Là encore, il n'est pas unique. Par contre, si θ et θ' sont deux arguments de z, alors $\theta \equiv \theta' \pmod{2\pi}$.



Proposition 3.10. *Soient $z, z' \in \mathbb{C}^* = \mathbb{C} \setminus \{0\}$. Alors*

(1) $\arg(zz') \equiv \arg(z) + \arg(z') \pmod{2\pi}$.

(2) $\arg(z^n) \equiv n \arg(z) \pmod{2\pi}$ *pour tout* $n \in \mathbb{N}$.

(3) $\arg(1/z) \equiv -\arg(z) \pmod{2\pi}$.

(4) $\arg(\bar{z}) \equiv -\arg(z) \pmod{2\pi}$.

Démonstration. On pose $z = |z|\,(\cos(\theta) + i\sin(\theta))$ et $z' = |z'|\,(\cos(\theta') + i\sin(\theta'))$, où $\arg(z) = \theta$ et $\arg(z') = \theta'$.

$$zz' = |z|\,(\cos(\theta) + i\sin(\theta))\,|z'|\,(\cos(\theta') + i\sin(\theta')) =$$
$$|zz'|\big((\cos(\theta)\,\cos(\theta') - \sin(\theta)\,\sin(\theta')) + i(\cos(\theta)\,\sin(\theta') + \sin(\theta)\,\cos(\theta'))\big) =$$
$$|zz'|(\cos(\theta+\theta') + i\sin(\theta+\theta'))\,.$$

Donc

$$arg(zz') = \theta + \theta' \equiv \arg(z) + \arg(z') \pmod{2\pi}\,.$$

On démontre que $\arg(z^n) \equiv n \arg(z) \pmod{2\pi}$ par récurrence sur n. Supposons que $n = 0$. Alors $\arg(z^n) = \arg(1) = 0 \equiv 0 \arg(z) \pmod{2\pi}$. Supposons que $n \geq 0$ et $\arg(z^n) \equiv n \arg(z) \pmod{2\pi}$. Alors, par (1),

$$\arg(z^{n+1}) \equiv \arg(z^n\, z) \equiv \arg(z^n) + \arg(z) \equiv n \arg(z) + \arg(z) \equiv (n+1)\arg(z) \pmod{2\pi}\,.$$

On en conclue que $\arg(z^n) \equiv n \arg(z) \pmod{2\pi}$ pour tout $n \in \mathbb{N}$.

On a $0 \equiv \arg(1) \equiv \arg(zz^{-1}) \equiv \arg(z) + \arg(z^{-1}) \pmod{2\pi}$, donc $\arg(z^{-1}) \equiv -\arg(z) \pmod{2\pi}$. De même, $0 \equiv \arg(|z|^2) \equiv \arg(z\bar{z}) \equiv \arg(z) + \arg(\bar{z}) \pmod{2\pi}$, donc $\arg(\bar{z}) \equiv -\arg(z) \pmod{2\pi}$. □

Corollaire 3.11 (Formule e Moivre). *Soit $\theta \in \mathbb{R}$ et $n \in \mathbb{N}$. Alors* $(\cos(\theta) + i\sin(\theta))^n = \cos(n\,\theta) + i\sin(n\,\theta)$.

Démonstration. Posons $z = \cos(\theta) + i\sin(\theta)$. En particulier, $\arg(z) = \theta$. Alors $\arg(z^n) \equiv n \arg(z) \equiv n\,\theta \pmod{2\pi}$, donc

$$(\cos(\theta) + i\sin(\theta))^n = z^n = |z|^n\,(\cos(n\,\theta) + i\sin(n\,\theta)) = \cos(n\,\theta) + i\sin(n\,\theta)\,.$$

□

Définition. Pour $\theta \in \mathbb{R}$ on pose $e^{i\theta} = \cos(\theta) + i\sin(\theta)$. Soit $z \in \mathbb{C}^*$. On pose $\rho = |z|$ et $\theta = \arg(z)$. Alors $z = |z|(\cos(\theta) + i\sin(\theta)) = \rho e^{i\theta}$. Cette écriture de z s'appelle *l'écriture exponentielle* de z.

La proposition 3.10 en écriture exponentielle s'écrit comme suit.

Proposition 3.12. *Soient $z = \rho e^{i\theta}$ et $z' = \rho' e^{i\theta'}$ deux nombres complexes écrits de façon exponentielle.*

(1) $zz' = \rho\rho' e^{i(\theta+\theta')}$.
(2) $z^n = \rho^n e^{in\theta}$.
(3) $z^{-1} = \rho^{-1} e^{-i\theta}$.
(4) $\bar{z} = \rho e^{-i\theta}$.

Définition. Soient $z \in \mathbb{C}$ et $n \in \mathbb{N}$. Une *racine n-ième* de z est un nombre $\omega \in \mathbb{C}$ tel que $\omega^n = z$.

Proposition 3.13. *Soit n un entier ≥ 2. Soit $z = \rho e^{i\theta}$ un nombre complexe non nul écrit de façon exponentielle. Alors z a n racines n-ièmes, $\omega_0, \omega_1, \ldots, \omega_{n-1}$, où*

$$\omega_k = \rho^{1/n}\, e^{i\frac{\theta+2k\pi}{n}}\,, \quad k = 0, 1, \ldots, n-1\,.$$

Démonstration. Soit $\omega = re^{it}$, où $r > 0$ et $t \in \mathbb{R}$.

$$\omega^n = z \;\Leftrightarrow\; r^n e^{int} = \rho e^{i\theta} \;\Leftrightarrow\; r^n = \rho \text{ et } nt \equiv \theta \pmod{2\pi}$$

Il est clair que $r^n = \rho$ si et seulement si $r = \rho^{1/n}$. On a $nt \equiv \theta \pmod{2\pi}$ si et seulement s'il existe $k \in \mathbb{Z}$ tel que $nt = \theta + 2k\pi$, c'est à dire $t = \frac{\theta+2k\pi}{n}$. Comme $\frac{\theta+2(k+n\ell)\pi}{n} \equiv \frac{\theta+2k\pi}{n} \pmod{2\pi}$ pour tout $\ell \in \mathbb{Z}$, on peut choisir $k \in \{0, 1, \ldots, n-1\}$. Ainsi, ω est une racine n-ième de z si et seulement s'il existe $k \in \{0, 1, \ldots, n-1\}$ tel que $\omega = \omega_k$. □

Lemme 3.14 (Formules d'Euler). *Soit $\theta \in \mathbb{R}$. Alors*

$$\cos(\theta) = \frac{e^{i\theta} + e^{-i\theta}}{2}\,, \quad \sin(\theta) = \frac{e^{i\theta} - e^{-i\theta}}{2i}\,.$$

Démonstration.

$$\frac{1}{2}(e^{i\theta} + e^{-i\theta}) = \frac{1}{2}((\cos(\theta) + i\sin(\theta)) + (\cos(\theta) - i\sin(\theta)) = \frac{2\cos(\theta)}{2} = \cos(\theta)$$
$$\frac{1}{2i}(e^{i\theta} - e^{-i\theta}) = \frac{1}{2i}((\cos(\theta) + i\sin(\theta)) - (\cos(\theta) - i\sin(\theta)) = \frac{2i\sin(\theta)}{2i} = \sin(\theta)$$

□

Application 1. On exprime $\cos(n\theta)$ et $\sin(n\theta)$ en fonction des puissances de $\sin(\theta)$ et $\cos(\theta)$. Pour cela, on utilise la formule de Moivre, $(cos(n\theta) + i\sin(n\theta)) = (\cos(\theta) + i\sin(\theta))^n$, que l'on développe à l'aide de la formule de Newton.

Exemple. On a

$$\cos(3\theta) + i\sin(3\theta) = (\cos(\theta) + i\sin(\theta))^3 =$$
$$\cos^3(\theta) + 3\,\cos^2(\theta)\,i\,\sin(\theta) + 3\,\cos(\theta)\,i^2\,\sin^2(\theta) + i^3\,\sin^3(\theta) =$$
$$\cos^3(\theta) + 3i\,\cos^2(\theta)\,\sin(\theta) - 3\,\cos(\theta)\,\sin^2(\theta) - i\,\sin^3(\theta) =$$
$$\big(\cos^3(\theta) - 3\,\cos(\theta)\,\sin^2(\theta)\big) + i\big(3\,\cos^2(\theta)\,\sin(\theta) - \sin^3(\theta)\big)$$

donc

$$\cos(3\theta) = \cos^3(\theta) - 3\,\cos(\theta)\,\sin^2(\theta) \quad \text{et} \quad \sin(3\theta) = 3\,\cos^2(\theta)\,\sin(\theta) - \sin^3(\theta)\,.$$

Application 2. On exprime $\cos^n(\theta)$ et $\sin^n(\theta)$ en fonction des $\cos(k\theta)$ et $\sin(k\theta)$ avec $k \in \{1, \ldots, n\}$. Pour cela on écrit $\cos^n(\theta) = \left(\frac{e^{i\theta}+e^{-i\theta}}{2}\right)^n$ et $\sin^n(\theta) = \left(\frac{e^{i\theta}-e^{-i\theta}}{2i}\right)^n$, on développe avec la formule de Newton, et on regroupe les termes par paires conjuguées.

Exemple.

$$\cos^3(\theta) = \frac{1}{2^3}(e^{i\theta} + e^{-i\theta})^3 = \frac{1}{8}\left(e^{3i\theta} + 3e^{2i\theta}\,e^{-i\theta} + 3e^{i\theta}\,e^{-2i\theta} + e^{-3i\theta}\right) =$$
$$\frac{1}{8}\left(e^{3i\theta} + 3e^{i\theta} + 3e^{-i\theta} + e^{-3i\theta}\right) = \frac{1}{8}\left((e^{3i\theta} + e^{-3i\theta}) + 3(e^{i\theta} + e^{-i\theta})\right) =$$
$$\frac{1}{8}\left(2\,\cos(3\theta) + 6\cos(\theta)\right) = \frac{1}{4}\left(\cos(3\theta) + 3\cos(\theta)\right).$$

3.5 Nombres complexes et géométrie

Définition. Soit M un point du plan $\mathbb{R}^2$ de coordonnées (x, y). Alors le nombre complexe $z = x + iy$ s'appelle *l'affixe* de M.

Proposition 3.15. *Soit $\mathcal{D}$ une droite affine dans $\mathbb{R}^2$ d'équation (E) $ax + by = c$, où $(a, b) \neq (0, 0)$. Posons $\omega = a + ib \in \mathbb{C}^*$ et $k = 2c$. Soit $M \in \mathbb{R}^2$ d'affixe $z \in \mathbb{C}$. Alors $M \in \mathcal{D}$ si et seulement si z vérifie l'égalité $(E_{\mathbb{C}})$ $\bar{\omega}z + \omega\bar{z} = k$.*

Définition. L'équation ci-dessus $\bar{\omega}z + \omega\bar{z} = k$ s'appelle *l'équation complexe* de la droite $\mathcal{D}$.

Démonstration. Soient M un point de $\mathbb{R}^2$ de coordonnées (x, y) et $z = x + iy$ l'affixe de M. Rappelons que $x = \frac{z+\bar{z}}{2}$ et $y = \frac{z-\bar{z}}{2i}$.

$$M \in \mathcal{D} \;\Leftrightarrow\; ax + by = c \;\Leftrightarrow\; a\frac{z+\bar{z}}{2} + b\frac{z-\bar{z}}{2i} = c \;\Leftrightarrow\; a(z+\bar{z}) - ib(z-\bar{z}) = 2c \;\Leftrightarrow$$
$$(a - ib)z + (a + ib)\bar{z} = k \;\Leftrightarrow\; \bar{\omega}z + \omega\bar{z} = k\,.$$

□

Proposition 3.16. *Soient Ω un point du plan d'affixe ω et r un nombre réel strictement positif. Notons $\mathcal{C}$ le cercle de centre Ω et de rayon r. Soit $M \in \mathbb{R}^2$ d'affixe $z \in \mathbb{C}$. On a $M \in \mathcal{C}$ si et seulement si z vérifie l'égalité $z\bar{z} - \bar{\omega}z - \omega\bar{z} = r^2 - |\omega|^2$.*

Démonstration. Soient M un point de $\mathbb{R}^2$ et z l'affixe de M.

$$M \in \mathcal{C} \Leftrightarrow \Omega M = r \Leftrightarrow |z-\omega| = r \Leftrightarrow |z-\omega|^2 = r^2 \Leftrightarrow (z-\omega)\overline{(z-\omega)} = r^2 \Leftrightarrow$$
$$(z-\omega)(\bar{z}-\bar{\omega}) = r^2 \Leftrightarrow z\bar{z} - \omega\bar{z} - \bar{\omega}z + \omega\bar{\omega} = r^2 \Leftrightarrow z\bar{z} - \omega\bar{z} - \bar{\omega}z = r^2 - |\omega|^2 .$$

□

Définition. L'équation ci-dessus $z\bar{z} - \bar{\omega}z - \omega\bar{z} = r^2 - |\omega|^2$ s'appelle *l'équation complexe* du cercle $\mathcal{C}$.

4 Arithmétique

4.1 Division euclidienne et pgcd

Définition. Soient $a, b \in \mathbb{Z}$. On dit que b *divise* a et on note $b|a$ s'il existe $q \in \mathbb{Z}$ tel que $a = bq$.

On collecte dans le lemme suivant quelques résultats évidents.

Lemme 4.1.

(1) On a $a|0$ et $1|a$ pour tout $a \in \mathbb{Z}$.

(2) On a $a|1$ si et seulement si $a \in \{1, -1\}$.

(3) Si $a|b$ et $b|a$, alors $a = \pm b$.

(4) Si $a|b$ et $b|c$, alors $a|c$.

(5) Si $a|b$ et $a|c$, alors $a|b + c$.

Théorème 4.2. *Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N} \setminus \{0\}$. Il existe des entiers $q, r \in \mathbb{Z}$ tels que $a = bq + r$ et $0 \leq r < b$. De plus, q et r sont uniques.*

Définition. L'expression $a = bq+r$ s'appelle la *division* de a par b. Le nombre q s'appelle le *quotient* et r le *reste* de la division.

Démonstration. *Existence.* On suppose d'abord que $a \geq 0$. Soit $Q = \{n \in \mathbb{N} \mid bn \leq a\}$. On a $0 \in Q$, donc $Q \neq \emptyset$. Par ailleurs, $n \leq nb \leq a$ pour tout $n \in Q$, donc Q est borné, donc Q est fini. Soit q le plus grand élément de Q et $r = a - qb$. On a par définition $a = bq + r$ et $r \geq 0$, car $bq \leq a$. Il reste à montrer que $r < b$. Comme q est maximal, on a $(q + 1) \notin Q$, donc

$$(q+1)b > a \Rightarrow qb + b > a \Rightarrow b > a - qb = r .$$

Supposons que $a < 0$. On choisit $q_1 \in \mathbb{Z}$ tel que $a - q_1 b \geq 0$. Par ce qui précède, il existe $q_2, r \in \mathbb{Z}$ tels que $a - q_1 b = q_2 b + r$ et $0 \leq r < b$. Posons $q = q_1 + q_2$. Alors $a = qb + r$ et $0 \leq r < b$.

Unicité. Soient $q, q', r, r' \in \mathbb{Z}$ tels que $a = qb + r = q'b + r'$ et $0 \leq r, r' < b$. On peut supposer que $r' \geq r$ sans perte de généralité. Alors $0 \leq r' - r \leq r' < b$. On a $b(q - q') = r' - r$ et le seul multiple de b inclus dans $\{0, 1, \ldots, b-1\}$ est 0, donc $b(q - q') = r' - r = 0$, donc $q = q'$ et $r = r'$. □

Remarque. Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N} \setminus \{0\}$. Soit $a = qb + r$ la division de a par b. Alors b divise a si et seulement si $r = 0$.

Définition. Soient $a, b \in \mathbb{Z}$ non tous les deux nuls. Le plus grand entier positif divisant à la fois a et b s'appelle le *plus grand diviseur commun* de a et b et se note $\text{pgcd}(a, b)$.

Exemple. Les diviseurs positifs de 21 sont $1, 3, 7, 21$. Les diviseurs positifs de 14 sont $1, 2, 7, 14$. Les diviseurs positifs communs de 21 et 14 sont $1, 7$. Donc, le plus grand diviseur commun de 14 et 21 est $\text{pgcd}(14, 21) = 7$. On a aussi $\text{pgcd}(-14, 21) = \text{pgcd}(14, -21) = \text{pgcd}(-14, -21) = 7$.

La démonstration du résultat suivant est laissée en exercice.

Lemme 4.3. *On a* $\text{pgcd}(a, ka) = a$ *pour tout* $a \in \mathbb{N}^*$ *et* $k \in \mathbb{Z}$. *En particulier,* $\text{pgcd}(a, 0) = a$ *et* $\text{pgcd}(a, 1) = 1$ *pour tout* $a \in \mathbb{N}$.

Lemme 4.4. *Soient* $a, b \in \mathbb{N}^*$. *Soit* $a = bq + r$ *la division de* a *par* b. *Alors* $\text{pgcd}(a, b) = \text{pgcd}(b, r)$.

Démonstration. Posons $D = \{d \in \mathbb{N} \mid d \text{ divise } a \text{ et } b\}$ et $D' = \{d \in \mathbb{N} \mid d \text{ divise } b \text{ et } r\}$. Soit $d \in \mathbb{N}$. Si $d \in D$, alors d divise a et b, donc d divise b et $a - qb = r$, donc $d \in D'$. Si $d \in D'$, alors d divise b et r, donc d divise b et $a = qb + r$, donc $d \in D$. Ceci montre que $D = D'$, donc $\text{pgcd}(a, b) = \max(D) = \max(D') = \text{pgcd}(b, r)$. □

Algorithme (Algorithme d'Euclide). *L'algorithme d'Euclide* est un algorithme qui, étant donnés $a, b \in \mathbb{N}^*$, calcule $\text{pgcd}(a, b)$. Il se décrit comme suit. On suppose que $a \geq b$.

- On fait la division de a par b : $a = bq_1 + r_1$. Par le lemme 4.4 on a $\text{pgcd}(a, b) = \text{pgcd}(b, r_1)$. Si $r_1 = 0$, alors $\text{pgcd}(a, b) = \text{pgcd}(b, 0) = 0$.
- Supposons que $r_1 \neq 0$. On fait la division de b par r_1 : $b = q_2 r_1 + r_2$. Par le lemme 4.4 on a $\text{pgcd}(a, b) = \text{pgcd}(b, r_1) = \text{pgcd}(r_1, r_2)$. Si $r_2 = 0$, alors on a $\text{pgcd}(a, b) = \text{pgcd}(r_1, 0) = r_1$.
- Supposons que $r_2 \neq 0$. On fait la division de r_1 par r_2 : $r_1 = q_3 r_2 + r_3$. Par le lemme 4.4 on a $\text{pgcd}(a, b) = \text{pgcd}(r_1, r_2) = \text{pgcd}(r_2, r_3)$. Si $r_3 = 0$, alors on a $\text{pgcd}(a, b) = \text{pgcd}(r_2, 0) = r_2$.

- On itère ce procédé. Comme $a \geq b > r_1 > r_2 > \cdots$, celui-ci doit terminer en un reste nul r_{k+1}. Le dernier reste non nul, r_k, est $\mathrm{pgcd}(a, b)$.

Exemple. Calculons $\mathrm{pgcd}(a, b)$, où $a = 600$ et $b = 124$. On effectue les divisions successives

$$\begin{aligned} 600 &= 124 \times 4 + 104 \\ 124 &= 104 \times 1 + 20 \\ 104 &= 20 \times 5 + 4 \\ 20 &= 4 \times 5 + 0 \end{aligned}$$

donc $\mathrm{pgcd}(600, 124) = 4$.

L'algorithme d'Euclide s'exprime formellement comme suit. Nous n'en donnerons pas de démonstration formelle.

Proposition 4.5 (Algorithme d'Euclide). *Soient $a, b \in \mathbb{N}^*$. Pour $n \in \mathbb{N}$ on définit r_n par récurrence sur n comme suit. $r_0 = b$ et r_1 est le reste de la division de a par b. Soit $n \geq 1$. Supposons que r_n est défini. Si $r_n = 0$, alors $r_{n+1} = 0$ et, si $r_n \neq 0$, alors r_{n+1} est le reste de la division de r_{n-1} par r_n. Alors il existe $N \in \mathbb{N}^*$ tel que $r_N \neq 0$ et $r_n = 0$ pour tout $n > N$. Dans ce cas $r_N = \mathrm{pgcd}(a, b)$.*

Définition. On dit que deux nombres $a, b \in \mathbb{Z}\backslash\{0\}$ sont *premiers entre eux* si $\mathrm{pgcd}(a, b) = 1$.

Lemme 4.6. *Soient $a, b \in \mathbb{Z} \setminus \{0\}$ et $d = \mathrm{pgcd}(a, b)$. Soient $a', b' \in \mathbb{Z}$ tels que $a = a'd$ et $b = b'd$. Alors a' et b' sont premiers entre eux.*

Démonstration. Posons $d' = \mathrm{pgcd}(a', b')$, $a' = a_1 d'$ et $b' = b_1 d'$. On a $a = a_1 d' d$ et $b = b_1 d' d$, donc $d' d$ est un diviseur commun à a et b, donc $d' d \leq d$, donc $d' = 1$. □

4.2 Théorème de Bézout

Théorème 4.7 (Théorème de Bézout). *Soient $a, b \in \mathbb{Z} \setminus \{0\}$. Il existe $u, v \in \mathbb{Z}$ tels que $au + bv = \mathrm{pgcd}(a, b)$.*

Définition. Les nombres u, v du théorème 4.7 s'appellent des *coefficients de Bézout* de a et b. Ils ne sont pas uniques.

Démonstration. On suppose d'abord que $a, b > 0$ et $\mathrm{pgcd}(a, b) = 1$. Posons $I = \{au + bv \mid u, v \in \mathbb{Z}\}$. On a $I \cap \mathbb{N}^* \neq \emptyset$ car $a, b \in I \cap \mathbb{N}^*$. Notons d le plus petit élément de $I \cap \mathbb{N}^*$. Soient $u_0, v_0 \in \mathbb{Z}$ tels que $d = au_0 + bv_0$. Soit $a = qd + r$ la division de a par d. On a $r = a - qd = a - q(au_0 + bv_0) = a(1 - qu_0) + b(-qv_0) \in I$. Comme d est le plus petit élément de $I \cap \mathbb{N}^*$ et $0 \leq r < d$, il s'en suit que $r = 0$, donc que d divise a. De même d divise b. Comme $\mathrm{pgcd}(a, b) = 1$, le seul diviseur commun à a et b dans $\mathbb{N}$ est 1, donc $d = 1$.

On suppose maintenant que a et b sont quelconques. Soient $d = \text{pgcd}(a, b)$ et $a', b' \in \mathbb{Z}$ tels que $a = a'd$ et $b = b'd$. Soient $\varepsilon, \mu \in \{\pm 1\}$ tels que $\varepsilon a' > 0$ et $\mu b' > 0$. Par le lemme 4.6 on a $\text{pgcd}(\varepsilon a', \mu b') = \text{pgcd}(a', b') = 1$. Par ce qui précède il existe $u_0, v_0 \in \mathbb{Z}$ tels que $1 = u_0 \varepsilon a' + v_0 \mu b'$. Alors

$$d = (u_0 \varepsilon a' + v_0 \mu b')d = u_0 \varepsilon a' d + v_0 \mu b' d = u_0 \varepsilon a + v_0 \mu b = ua + bv\,,$$

où $u = u_0 \varepsilon$ et $v = v_0 \mu$. □

Observation. Des coefficients de Bézout peuvent se calculer en "remontant" l'algorithme d'Euclide comme dans l'exemple ci-dessous.

Exemple. On cherche des coefficients de Bézout des nombres $a = 600$ et $b = 124$. On effectue d'abord l'algorithme d'Euclide qui calcule le pgcd de ces deux nombres.

$$\begin{aligned} 600 &= 124 \times 4 + 104 \\ 124 &= 104 \times 1 + 20 \\ 104 &= 20 \times 5 + 4 \\ 20 &= 4 \times 5 + 0 \end{aligned}$$

On remonte ces égalités pour obtenir des coefficients de Bézout.

$$\begin{aligned} 4 &= 104 - 20 \times 5 \\ 4 &= 104 - (124 - 104 \times 1) \times 5 \\ &= 124 \times (-5) + 104 \times 6 \\ 4 &= 124 \times (-5) + (600 - 124 \times 4) \times 6 \\ &= 600 \times 6 + 124 \times (-29) \end{aligned}$$

Corollaire 4.8. *Soient a, b, d trois nombres non nuls. Si d divise a et b, alors d divise* $\text{pgcd}(a, b)$.

Démonstration. Par le théorème 4.7 on sait qu'il existe $u, v \in \mathbb{Z}$ tels que $au + bv = \text{pgcd}(a, b)$. Donc, si d divise a et b, alors d divise $au + bv = \text{pgcd}(a, b)$. □

Corollaire 4.9. *Soient a, b deux entiers non nuls. Alors a et b sont premiers entre eux si et seulement s'il existe $u, v \in \mathbb{Z}$ tels que $1 = au + bv$.*

Démonstration. Si a et b sont premiers entre eux, alors, par le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que $1 = au + bv$. Supposons qu'il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$. Soit $d = \text{pgcd}(a, b)$. Alors d divise a et b, donc d divise $1 = au + bv$, donc $d = 1$. D'où a et b sont premiers entre eux. □

Corollaire 4.10 (Lemme de Gauss). *Soient a, b, c trois entiers non nuls. Si a divise bc et* $\text{pgcd}(a, b) = 1$*, alors a divise c.*

Démonstration. Comme $\text{pgcd}(a,b) = 1$, il existe $u, v \in \mathbb{Z}$ tel que $au + bv = 1$, donc $c = cau + cbv$. Mais a divise cau et cbv (car divise bc), donc a divise $c = cau + cbv$. □

Définition. Soient $a, b, c \in \mathbb{Z}$, a et b non nuls. Une *solution* à l'équation entière

$$(E) \quad aX + bY = c$$

est un couple $(x, y) \in \mathbb{Z}^2$ tel que $ax + by = c$. *Résoudre* (E) signifie déterminer l'ensemble de ses solutions.

Lemme 4.11. *Soient $a, b, c \in \mathbb{Z}$, a et b non nuls. Alors l'équation entière $aX + bY = c$ a au moins une solution si et seulement si* $\text{pgcd}(a,b)$ *divise c.*

Démonstration. On pose $d = \text{pgcd}(a,b)$. Supposons que l'équation a une solution (x, y). Alors, comme d divise a et b, d divise $ax + by = c$. Supposons que d divise c. Soit $c_1 \in \mathbb{Z}$ tel que $c = dc_1$. Par le théorème de Bézout il existe $u, v \in \mathbb{Z}$ tels que $d = au + bv$. Alors $c = dc_1 = a(uc_1) + b(vc_1)$, donc (uc_1, vc_1) est une solution de l'équation. □

Remarque 1. Soient $a, b, c \in \mathbb{Z}$, a et b non nuls. On pose $d = \text{pgcd}(a,b)$ et on suppose que d divise c. Soient $a_1, b_1, c_1 \in \mathbb{Z}$ tels que $a = da_1$, $b = db_1$ et $c = dc_1$. Alors

$$ax + by = c \;\Leftrightarrow\; da_1x + db_1y = dc_1 \;\Leftrightarrow\; a_1x + b_1y = c_1\,.$$

Ceci signifie que l'équation (E) "$aX + bY = c$" est *équivalente* à l'équation (E_1) "$a_1X + b_1Y = c_1$", dans le sens que les ensembles de solutions des deux équations sont égaux.

Remarque 2. Soient $a, b, c \in \mathbb{Z}$, a et b non nuls. On suppose que $\text{pgcd}(a,b)$ divise c. Alors on peut trouver une solution particulière de l'équation $aX + bY = c$ en calculant des coefficients de Bézout de a et b à l'aide de l'algorithme d'Euclide.

Exemple. On considère l'équation entière

$$(E) \quad 161X + 368Y = 115\,.$$

On calcule $\text{pgcd}(161, 368)$.

$$\begin{aligned} 368 &= 161 \times 2 + 46 \\ 161 &= 46 \times 3 + 23 \\ 46 &= 23 \times 2 + 0 \end{aligned}$$

donc $\text{pgcd}(161, 368) = 23$. On a $115 = 5 \times 23$, donc (E) a une solution. On a $161 = 7 \times 23$ et $368 = 16 \times 23$, donc (E) est équivalente à

$$(E_1) \quad 7X + 16Y = 5\,.$$

On calcule des coefficients de Bézout de 16 et 7.

$$\begin{aligned} 16 &= 7 \times 2 + 2 \\ 7 &= 2 \times 3 + 1 \end{aligned}$$

donc

$$\begin{aligned} 1 &= 7 + 2 \times (-3) \\ &= 7 + (16 + 7 \times (-2)) \times (-3) \\ &= 7 \times 7 + 16 \times (-3) \\ 5 &= 7 \times 35 + 16 \times (-15) \end{aligned}$$

Donc $(35, -15)$ est une solution de (E_1) et de (E).

Lemme 4.12. *Soient $a, b, c \in \mathbb{Z}$, a et b non nuls. On suppose que* $\text{pgcd}(a, b) = 1$. *Soit (x_0, y_0) une solution (particulière) de l'équation entière*

$$(E) \quad aX + bY = c\,.$$

Alors l'ensemble des solutions de (E) est $\{(x_0 + kb, y_0 - ka) \mid k \in \mathbb{Z}\}$.

Démonstration. Soit $k \in \mathbb{Z}$. Posons $x = x_0 + kb$ et $y = y_0 - ka$. Alors

$$ax + by = a(x_0 + kb) + b(y_0 - ka) = (ax_0 + by_0) + (kab - kab) = c + 0 = c$$

donc (x, y) est une solution de (E). Soit (x, y) une solution de (E). On a

$$a(x - x_0) + b(y - y_0) = c - c = 0$$

donc $a(x - x_0) = b(y_0 - y)$. Comme b divise $a(x - x_0)$ et $\text{pgcd}(a, b) = 1$, b divise $x - x_0$. Il existe donc $k \in \mathbb{Z}$ tel que $x - x_0 = kb$, c'est-à-dire $x = x_0 + kb$. Après $a(x - x_0) = akb = b(y_0 - y)$, donc $y_0 - y = ak$, c'est-à-dire $y = y_0 - ka$. D'où $(x, y) = (x_0 + kb, y_0 - ka)$. □

Exemple. On considère l'équation entière

$$(E) \quad 161X + 368Y = 115\,.$$

On sait que (E) est équivalente à

$$(E_1) \quad 7X + 16Y = 5\,.$$

On sait aussi que $\text{pgcd}(7, 16) = 1$ et $(35, -15)$ est une solution de (E). Donc l'ensemble des solutions de (E) est $\{(35 + 16k, -15 - 7k) \mid k \in \mathbb{Z}\}$.

Définition. Soient $a, b \in \mathbb{Z}$ non tous les deux nuls. Le *plus petit multiple commun* de a et b, noté $\text{ppcm}(a, b)$, est le plus petit entier ≥ 0 divisible par a et b.

Lemme 4.13. *Soient $a, b \in \mathbb{N}^*$. Alors* $\text{pgcd}(a, b) \times \text{ppcm}(a, b) = a \times b$.

Démonstration. Posons $d = \text{pgcd}(a, b)$. Soient $a_1, b_1 \in \mathbb{N}^*$ tels que $a = a_1 d$ et $b = b_1 d$. Posons $m = a_1 b_1 d$. On a $m\,d = a_1 b_1 d^2 = (a_1 d)(b_1 d) = ab$, donc on doit montrer que $m = \text{ppcm}(a, b)$. Remarquer que $m = ab_1 = ba_1$, donc m est un multiple commun de a et b. Reste à montrer qu'il est le plus petit. Soit n un autre multiple commun de a et b. Soit $n_1 \in \mathbb{N}$ tel que $n = an_1$. $b = db_1$ divise $n = an_1 = da_1 n$, donc b_1 divise

$a_1 n_1$. De plus $\text{pgcd}(a_1, b_1) = 1$, donc b_1 divise n_1. Soit $n_2 \in \mathbb{N}$ tel que $n_1 = b_1 n_2$. Alors $n = a n_1 = a_1 d b_1 n_2 = m n_2$, donc m divise n, donc $m \leq n$. □

Lemme 4.14. *Soient $a, b, c \in \mathbb{N}^*$. Si a et b divisent c, alors $\text{ppcm}(a, b)$ divise c.*

Démonstration. Posons $d = \text{pgcd}(a, b)$ et $m = \text{ppcm}(a, b)$. Soient $a_1, b_1 \in \mathbb{N}^*$ tels que $a = a_1 d$ et $b = b_1 d$. Comme $dm = ab = a_1 b_1 d^2$, on a $m = a_1 b_1 d$. Le nombre a divise c, donc il existe $c_1 \in \mathbb{N}^*$ tel que $c = a c_1$. Le nombre $b = b_1 d$ divise $c = a c_1 = a_1 d c_1$, donc b_1 divise $a_1 c_1$. Comme a_1 et b_1 sont premiers entre eux, b_1 divise c_1, donc il existe $c_2 \in \mathbb{N}^*$ tel que $c_1 = b_1 c_2$. Alors $c = a c_1 = a_1 d b_1 c_2 = m c_2$ est divisible par m. □

4.3 Nombres premiers

Définition. Un *nombre premier* est un nombre $p \geq 2$ dont les seuls diviseurs positifs sont 1 et lui-même.

Lemme 4.15. *Tout entier $n \geq 2$ admet un diviseur qui est un nombre premier.*

Démonstration. Soit $D = \{k \geq 2 \mid k \text{ divise } n\}$. On a $D \neq \emptyset$ car $n \in D$. Soit p le plus petit élément de D. Si $q \geq 2$ est un diviseur de p, alors q est un diviseur de n et $2 \leq q \leq p$, donc $q \in D$ et $q \leq p$, donc $q = p$ par la minimalité de p. Ceci montre que les seuls diviseurs positifs de p sont 1 et p, donc que p est premier. De plus, p divise n car $p \in D$. □

Proposition 4.16. *Il existe une infinité de nombres premiers.*

Démonstration. On raisonne par l'absurde. On suppose qu'il existe un nombre fini de nombres premiers, $p_1, p_2, \ldots, p_n$. Posons $N = p_1 p_2 \cdots p_n + 1$. Par le lemme 4.15, N admet un diviseur premier, c'est-à-dire qu'il existe $i \in \{1, \ldots, n\}$ tel que p_i divise N (disons p_1 divise N). Soit $N' \in \mathbb{N}^*$ tel que $N = p_1 N'$. Alors $1 = N - p_1 p_2 \cdots p_n = p_1(N' - p_2 \cdots p_n)$ est divisible par p_1. Ceci est une contradiction donc il existe une infinité de nombres premiers. □

Proposition 4.17. *Soient p un nombre premier et a, b deux entiers relatifs non nuls. Si p divise ab, alors p divise a ou p divise b.*

Démonstration. Supposons que p divise ab et ne divise pas a et montrons que p divise b. Soit $d \geq 1$ un diviseur commun de p et a. Comme p est premier, on a $d = 1$ ou $d = p$. Mais p ne divise pas a, donc $d = 1$, donc p et a sont premiers entre eux. Par le corollaire 4.10 on en conclue que p divise b. □

Théorème 4.18. *Soit $n \geq 2$ un entier. Il existe des nombres premiers $p_1 < p_2 < \cdots < p_r$ et des exposants entiers $\alpha_1, \alpha_2, \ldots, \alpha_r \geq 1$ tels que*

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

De plus les p_i et les α_i sont uniques.

Définition. L'expression $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ du théorème 4.18 s'appelle la *décomposition en facteurs premiers* de n.

Exemple. $24 = 2^3 \times 3$ est la décomposition de 24 en facteurs premiers. $36 = 2^2 \times 9$ n'est pas la décomposition de 36 en facteurs premiers car 9 n'est pas un nombre premier.

Démonstration. *Existence.* On démontre l'existence de la décomposition de $n \geq 2$ par récurrence sur n. Le nombre $n = 2$ est déjà décomposé. On peut supposer que $n \geq 3$ plus l'hypothèse de récurrence. Par le lemme 4.15, n admet un diviseur premier. On note p_1 le plus petit diviseur premier de n et $n' \in \mathbb{N}^*$ tel que $n = p_1 n'$. Si $n' = 1$, alors $n = p_1$ est déjà décomposé. On peut donc supposer que $2 \leq n' < n$. Par hypothèse de récurrence il existe des nombres premiers $p_2 < \cdots < p_r$ et des entiers $\alpha_1' \geq 0$, $\alpha_2, \ldots, \alpha_r \geq 1$, tels que $p_1 < p_2$ et $n' = p_1^{\alpha_1'} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$. Alors

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} ,$$

où $\alpha_1 = \alpha_1' + 1 \geq 1$.

Unicité. On suppose que n admet deux décompositions en facteurs premiers,

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s} .$$

Soit p un diviseur premier de n. Par la proposition 4.17 il existe $i \in \{1, \ldots, r\}$ tel que p divise p_i ce qui implique que $p = p_i$ car p_i est premier. Réciproquement, chaque p_i divise n. On en déduit que les diviseurs premiers de n sont exactement $p_1, p_2, \ldots, p_r$. De même, les diviseurs premiers de n sont $q_1, q_2, \ldots, q_s$. Comme $p_1 < p_2 < \cdots < p_r$ et $q_1 < q_2 < \cdots < q_s$, il s'en suit que $r = s$ et $p_i = q_i$ pour tout $i \in \{1, \ldots, r\}$. On peut supposer sans perte de généralité que $\alpha_1 \geq \beta_1$. Comme $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\alpha_r}$, on a $p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} = p_2^{\beta_2} \cdots p_r^{\beta_r}$. Si on avait $\alpha_1 > \beta_1$, alors p_1 diviserait $p_2^{\beta_2} \cdots p_r^{\beta_r}$. Or les diviseurs premiers de $p_2^{\beta_2} \cdots p_r^{\beta_r}$ sont $p_2, \ldots, p_r$ et ils sont tous différents de p_1. Donc $\alpha_1 = \beta_1$. On montre de la même façon que $\alpha_i = \beta_i$ pour tout $i \in \{2, \ldots, r\}$. □

4.4 Congruences

Définition. Soit $n \geq 2$ un entier. Soient $a, b \in \mathbb{Z}$. On dit que a *est congru à b modulo n* et on note $a \equiv b \pmod{n}$ si n divise $b - a$.

Remarque. n divise a si et seulement si $a \equiv 0 \pmod{n}$.

Proposition 4.19.

(1) La relation "être congru modulo n" est une relation d'équivalence dans $\mathbb{Z}$.

(2) Soient $a, b, c, d \in \mathbb{Z}$ tels que $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$. Alors $(a + c) \equiv (b + d) \pmod{n}$.

(3) Soient $a, b, c, d \in \mathbb{Z}$ tels que $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$. Alors $a\,c \equiv b\,d \pmod{n}$.

(4) Soient $a, b \in \mathbb{Z}$ tels que $a \equiv b \pmod{n}$ et $k \geq 0$. Alors $a^k \equiv b^k \pmod{n}$.

Démonstration. On sait déjà que "être congru modulo n" est une relation d'équivalence (voir le lemme 2.17). Soient $a, b, c, d \in \mathbb{Z}$ tels que $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$. Alors n divise $b - a$ et $d - c$, donc n divise $(b - a) + (d - c) = (b + d) - (a + c)$, donc $(a + c) \equiv (b + d) \pmod{n}$. On a aussi que n divise $b(d - c) + c(b - a) = bd - ac$, donc $ac \equiv bd \pmod{n}$. La partie (4) est une conséquence directe de la partie (3). □

Remarque. Soit $a \in \mathbb{Z}$. Alors il existe un unique $r \in \{0, 1, \ldots, n - 1\}$ tel que $a \equiv r \pmod{n}$. C'est le reste de la division de a par n (voir le lemme 2.18).

Définition. Soient $a, b \in \mathbb{Z}$, $a \neq 0$ et $n \geq 2$. Une solution à l'équation $aX \equiv b \pmod{n}$ est un entier $x \in \mathbb{Z}$ tel que $ax \equiv b \pmod{n}$. *Résoudre cette équation* est déterminer l'ensemble de ses solutions.

Lemme 4.20. *Soient $a, b \in \mathbb{Z}$, $a \neq 0$, et $n \geq 2$. Soit (E) l'équation $aX \equiv b \pmod{n}$.*

(1) L'équation (E) a une solution si et seulement si $\operatorname{pgcd}(a, n)$ divise b.

(2) On pose $d = \operatorname{pgcd}(a, n)$ et on suppose que d divise b. Soit n_1 tel que $n = n_1 d$. Soit x_0 une solution particulière de (E). Alors l'ensemble des solutions de (E) est $\{x_0 + kn_1 \mid k \in \mathbb{Z}\}$.

Démonstration. On considère l'équation entière $(\hat{E})$ $aX - nY = b$. Alors x est solution de (E) si et seulement s'il existe $y \in \mathbb{Z}$ tel que (x, y) est solution de $(\hat{E})$. En effet :

$$ax \equiv b \pmod{n} \;\Leftrightarrow\; \exists y \in \mathbb{Z},\ ax = b + ny \;\Leftrightarrow\; \exists y \in \mathbb{Z},\ ax - ny = b\,.$$

On sait par le lemme 4.11 que $(\hat{E})$ a une solution si et seulement si $\operatorname{pgcd}(a, n)$ divise b, donc (E) a une solution si et seulement si $\operatorname{pgcd}(a, n)$ divise b.

Supposons que d divise b. Soient $a_1, b_1 \in \mathbb{Z}$ tels que $a = a_1 d$ et $b = b_1 d$. Soit x_0 une solution particulière de (E). Il existe $y_0 \in \mathbb{Z}$ tel que (x_0, y_0) est solution de $(\hat{E})$. Par le lemme 4.12 l'ensemble des solutions de $(\hat{E})$ est $\{(x_0 + kn_1, y_0 + ka_1) \mid k \in \mathbb{Z}\}$, donc l'ensemble des solutions de (E) est $\{x_0 + kn_1 \mid k \in \mathbb{Z}\}$. □

Exemple. On considère l'équation

$$(E) \quad 9X \equiv 6 \pmod{24}\,.$$

On a $\operatorname{pgcd}(9, 24) = 3$ et 3 divise 6, donc (E) a une solution. On considère l'équation

$$(\hat{E}) \quad 9X - 24Y = 6\,.$$

Alors $(\hat{E})$ est équivalente à

$$(\hat{E}') \quad 3X - 8Y = 2\,.$$

On a

$$8 = 2 \times 3 + 2 \;\Rightarrow\; 2 = (-2) \times 3 - (-1) \times 8\,,$$

donc $(-2, -1)$ est une solution particulière de $(\hat{E}')$, donc -2 est une solution particulière de (E). Alors l'ensemble des solutions de (E) est $\{-2 + 8k \mid k \in \mathbb{Z}\}$.