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 $qq' \neq 0$. $\square$

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 $a \neq b$.

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

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 $n \in \mathbb{N}$.*

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

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

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

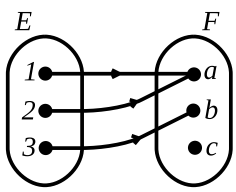
2.2 Applications

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

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

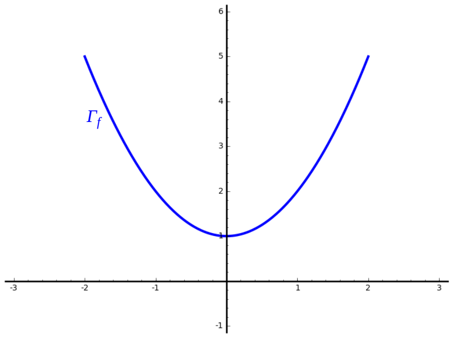
On représente graphiquement cette application comme suit.



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

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

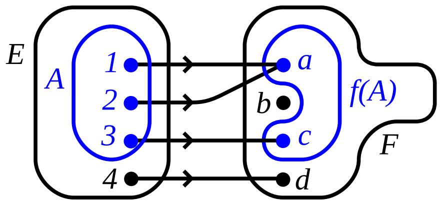
Définition. L'application *identité* d'un ensemble E est l'application $\mathrm{id}_E : E \to E$ qui envoie x sur x pour tout $x \in E$.

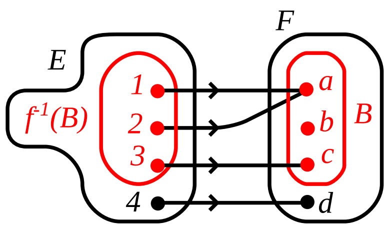
Définition. Soient $f : E \to F$ une application, $A \subset E$ et $B \subset F$. *L'image directe* de A par f est $f(A) = \{f(x) \mid x \in A\} \subset F$. *L'image réciproque* de B par f est $f^{-1}(B) = \{x \in E \mid f(x) \in B\} \subset E$.

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

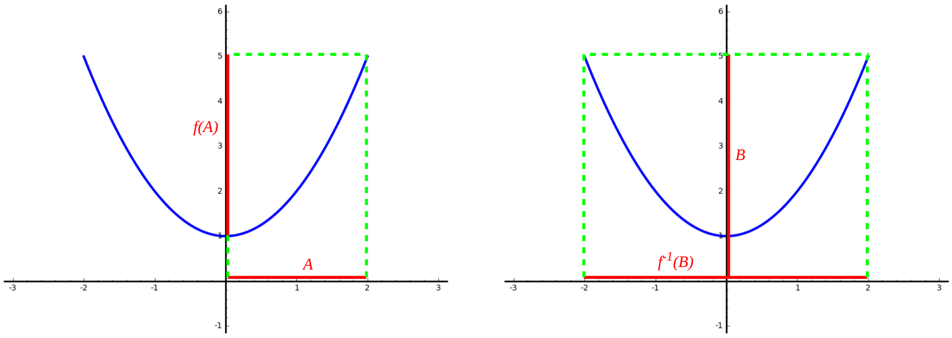
$$f(1) = a, \ f(2) = a, \ f(3) = c, \ f(4) = d.$$

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 $f(x) = y$.

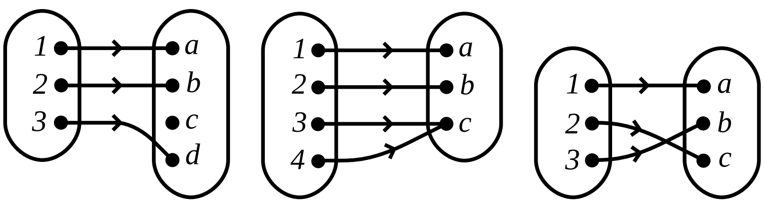
Exemples.

(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.

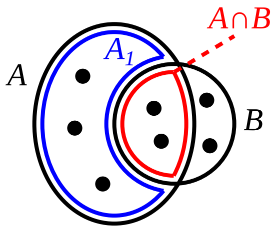
(1) *Si A est un ensemble fini et $B \subset A$, alors B est fini et $\mathrm{Card}(B) \leq \mathrm{Card}(A)$.*

(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) $\Rightarrow$ (i)" et "(iii) $\Rightarrow$ (ii)" sont évidentes. On va montrer les deux autres implications, "(i) $\Rightarrow$ (iii)" et "(ii) $\Rightarrow$ (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. $\square$

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 $n \geq 1$. $\square$

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 $n \geq 1$. $\square$

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 $n!$. $\square$

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 $\mathrm{Card}(\mathcal{P}(E)) = \mathrm{Card}(\mathrm{App}(E,\{0,1\})) = 2^n$. $\square$

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* $0 \le k \le n$.
(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). $\square$

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, $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$. $\square$

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 $k \in \{0,1,\dots,n\}$. Alors*

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

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

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 $k \in \{1,\dots,n\}$. 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 $n \geq 1$. $\square$

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

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

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

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

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

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

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

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*
$$(p, q)\mathcal{R}(p', q') \text{ si } pq' = p'q.$$
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 $\frac{p}{q}$.