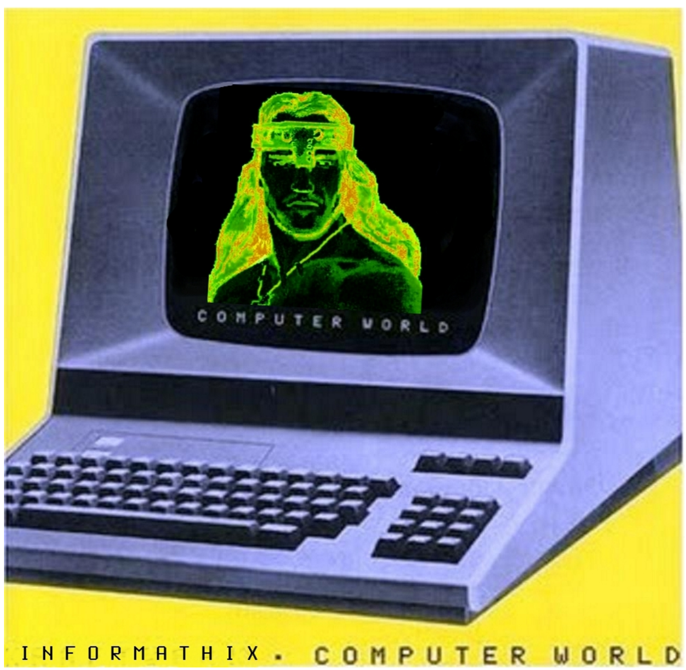
Mathématiques

IUT INFO1 / 2011-2012

IUT d'informatique de Nantes 1ère année



Guillaume CONNAN et Thierry BRUGÈRE

IUT NANTES

UNIVERSITÉ DE NANTES

TABLE DES MATIÈRES

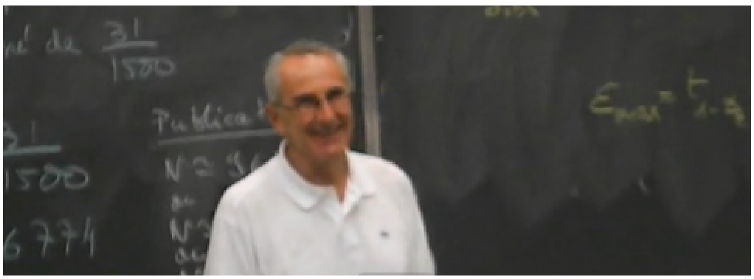
1 Timide introduction aux mathématiques discrètes **6**

1.1 Prouver ou ne pas prouver ?... 7
1.2 Comment raisonner ?... 8
1.2.1 Récurrence, récursion, récursivité, induction & Co. 8
1.2.2 Théorèmes 14
1.3 Théorie naïve des ensembles 17
1.3.1 Éléments 17
1.3.2 Ensembles égaux 20
1.3.3 Inclusion 21
1.3.4 Parties d'un ensemble 22
1.3.5 Opérations 23
1.3.6 Fonction caractéristique 28
1.3.7 Partition d'un ensemble 32
1.3.8 Produit cartésien 33
1.3.9 Notion de cardinal 36
1.4 Calcul booléen 38
1.4.1 Présentation 38
1.4.2 Algèbre de Boole 38
1.4.3 Fonctions booléennes 43
1.4.4 Portes logiques 46
1.4.5 Minimisation de circuits 47
1.5 Un peu de calcul matriciel 50
1.5.1 Produit de matrices 50
1.5.2 Matrices et Python : approche naïve 51
1.6 Relations binaires 53
1.6.1 Au CE1 53
1.6.2 Généalogie 53
1.6.3 À l'IUT 54
1.6.4 Domaine, codomaine 56
1.6.5 Représentation d'une relation 56
1.6.6 Relation réciproque 59
1.6.7 Image, contre image, image réciproque d'une partie 60
1.6.8 Égalité de deux relations 61
1.6.9 Restriction, prolongement 62
1.6.10 Négation, inclusion, union, intersection 64
1.6.11 Composition de relations 68
1.6.12 Fonctions, applications 71
1.7 Relations binaires sur un ensemble 79
1.7.1 Au CE1 79
1.7.2 Définition 80
1.7.3 Représentations 81
1.7.4 Inclusion, union, intersection et négation 82
1.7.5 Composition 83

1.7.6 Fermeture d'une relation : du concret . . . 87
1.7.7 Chemin . . . 87
1.7.8 Propriétés particulières . . . 88
1.7.9 Fermeture transitive et chemin . . . 92
1.8 Relations d'équivalence . . . 95
1.9 Structures d'ordre . . . 97
1.9.1 Relation d'ordre . . . 97
1.9.2 Ensembles ordonnés . . . 97
1.9.3 Ordre lexicographique . . . 98
1.9.4 Diagramme de HASSE . . . 98
1.9.5 Éléments remarquables . . . 99
1.9.6 Ensemble bien ordonné . . . 101
1.10 Un peu de dénombrement . . . 102
1.10.1 Détour historique . . . 102
1.10.2 Quelques résultats sur les cardinaux . . . 106
1.10.3 Dénombrement . . . 108
1.10.4 Triangle de Pascal - Binôme de Newton . . . 111
1.10.5 Combinaisons avec répétitions. . . . 112
1.11 EXERCICES . . . 114
1.11.1 Raisonnements . . . 114
1.11.2 Ensembles . . . 118
1.11.3 Calcul booléen . . . 120
1.11.4 Relations binaires . . . 123
1.11.5 Relations binaires sur un ensemble . . . 127
1.11.6 Relations d'équivalence . . . 128
1.11.7 Ordre . . . 129
1.11.8 Dénombrement . . . 130

HOMMAGE

Pendant 30 ans, les mathématiques à l'IUT d'informatique furent passionnément enseignées par Thierry BRUGÈRE :



Le cours qui vous sera proposé cette année lui doit beaucoup et on le retrouvera souvent désigné comme « Le Maître »...

Des maths en info ?!

Mathémator : Bonjour Hihutix ! Votre formation de Mathaïe va pouvoir commencer. J'espère que la force sera avec vous.

Hihutix: Bonjour Maître Mathémator, mais sans vouloir vous offenser, je suis étudiant à l'IUT d'informatique, pas de mathématiques. J'ai assez souffert au lycée. Je ferai peut-être un effort pour avoir mon DUT dans deux ans mais, bon...

Mathémator : Ah, fougueuse jeunesse...N'oubliez pas que ce sont des mathématiciens qui ont initié l'informatique en tant que science. De plus, vous découvrirez au cours de vos études et de votre carrière que l'usage d'un raisonnement mathématique vous aidera à appréhender vos problèmes informatiques. Les mathématiques sont donc en amont de l'informatique mais aussi en aval car « l'outil » mathématique est fort utile en informatique pour étudier un réseau d'ordinateurs, comprendre un langage, mettre au point un compilateur, faire de jolis dessins en infographie, étudier l'efficacité d'un algorithme, exploiter une base de données, et j'en passe, et des meilleures.

Durant les deux années à venir, nous étudierons des mathématiques « CON-CRÈTES » : ce petit jeu de mot est dû à Donald KNUTH [a] qui intitula ainsi son cours à l'Université de Stanford : un savant mélange de mathématiques CONtinues et de mathématiques disRÈTES [b].
Pour vous donner une idée de la distinction continue/discret, je vais vous donner un exemple concret.
Considérez une montre mécanique et une montre à cristaux liquides : sur l'une, le temps semble s'écouler de manière **continue**, les aiguilles faisant le tour du cadran en passant par toutes les positions possibles. Un informaticien parle de système **analogique**.
Au contraire, avec une montre à cristaux liquides, on n'affiche qu'un ensemble **discret** de valeurs du temps : on ne pourra pas afficher par exemple une valeur intermédiaire entre 10.53.12 et 10.53.13 Un informaticien parle de système **digital** [c].
L'informaticien est bien sûr très concerné par les mathématiques discrètes car le fonctionnement même de l'ordinateur est basé sur un système digital. Cela va nécessiter un apprentissage mathématique en béton...
Le monde qui entoure l'ingénieur, l'informaticien, l'industriel, est en effet le plus souvent discret. On raisonne souvent en nombres entiers : nombre de personnes, d'octets, de machines à licencier, etc.
Beaucoup de problèmes sont *combinatoires* : problèmes d'ordonnancement, d'organisation de réseaux, etc.
Quand il faut prendre une décision, il faut répondre par oui ou par non...
Quand on réfléchit, on utilise des schémas du type :« si je fais ça, alors il se passera peut-être ça ou bien ci, etc. », comme un cheminement sur un graphe...

a. Un des plus grands informaticiens (et mathématiciens) auteur du célébrissime *The Art of Computer Programming* et père du logiciel TEX.
b. Le mot « concrete » désigne aussi le béton en anglais : KNUTH prévenait ainsi ses étudiants qu'il allait enseigner des maths dures...
c. *digit* en anglais ?

CHAPITRE

1

Timide introduction aux mathématiques discrètes

Pour initier nos aventures, nous allons débuter par quelques révisions de l'école primaire puis tenter de les développer un peu afin d'avoir un minimum d'outils pour comprendre les mathématiques pour l'informatique. Mais tout d'abord, il faudra apprendre à raisonner...

1 Prouver ou ne pas prouver ?...

Mathémator : Qu'y a-t-il de plus beau qu'une belle preuve mathématique ? Elle a ceci d'extraordinaire qu'elle permet d'être totalement sûr d'un résultat, aussi compliqué soit-il...pour peu qu'on ne se soit pas trompé dans la preuve. Il est parfois très difficile d'arriver à prouver qu'une preuve est correcte. Par exemple, avant de valider la fameuse preuve d'Andrew WILES du fameux théorème de FERMAT proposée en 1993, trois siècles après l'énoncé du théorème par FERMAT, il a fallu des mois de vérification minutieuse par les plus grands mathématiciens.

Hihutix: Moi j'aime pas les preuves. De toute façon on connaît le résultat. Et puis j'en aurai pas besoin en quittant l'IUT.

Mathémator : Vous avez pourtant choisi de vous lancer dans des études dans le domaine de l'informatique, qui est une science aussi exigeante que les mathématiques. Habituer son esprit à acquérir clarté, précision, à développer ses facultés d'abstraction et de modélisation sans laisser de côté intuition et imagination est une bonne formation pour des informaticiens qui souhaitent éviter de créer des logiciels se bloquant à chaque manipulation.

Hihutix: Dans IUT, il y a T, donc faudrait peut-être pas confondre les étudiants d'ici avec des doctorants en mathématique.

Mathémator : Certes, et c'est pourquoi nous essaierons le plus possible de découvrir les notions nouvelles à partir d'exemples et de les illustrer à partir de situations informatiques concrètes. Nous explorerons également de fausses pistes, des raisonnements maladroits car il est aisé de passer à côté d'un problème et d'aboutir ainsi à une impasse ou un « bug ». Par exemple, dans un langage quelconque, on effectue un test du style « tant que $x < 0,3$ faire bla bla bla ». Ça bug. Pourtant le programme semble parfait. Mais observez plutôt :

– avec OCAML

```
# 3.*.0.1-.0.3;;
- : float = 5.5511151231257827e-17
```

– avec Python :

```
>>> 3*0.1-0.3
5.551115123125783e-17
```

– avec GP/Pari :

```
? 0.3-3*0.1
%1 = 1.4693679385278593850 E-39
```

Il semblerait que $3 \cdot 0,1$ ne soit pas égal à $0,3$...

Hihutix: !!!!

Mathémator : Avec un peu d'informathique, nous apprendrons par exemple à expliquer et à éviter ce genre d'erreur.

2 Comment raisonner ?...

Hihutix (à part): *Ding ! Dong !* **(tout haut)** Voici un problème passionnant mais qui aurait plutôt sa place dans ces merveilleux cours de philosophie que j'ai suivi avec ardeur l'an passé en terminale.

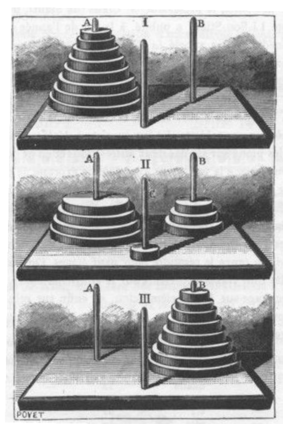
Mathémator : Évidemment, le problème est vaste et demanderait plusieurs décennies de réflexion. Nous nous contenterons d'aborder quelques types de raisonnements utiles que nous développerons plus tard de manière beaucoup plus rigoureuse, notamment lorsque nous étudierons la logique. Il y a quelques années, il aurait été inutile de faire les rappels qui vont suivre, mais que voulez-vous, on n'apprend plus rien à l'école.

Hihutix (à part): *Quel vieux xxx ! Il va pas commencer l'année à nous faire le coup du « ah, d'mon temps, c'était aut'chose ». Il a pas l'air si gâteux pourtant. C'est sûrement la déformation professionnelle. Un prof devient tôt ou tard un vieux xxx.* **(tout haut)** Ah, comme vous avez raison ! Heureusement, vous allez combler cette terrible lacune dans ma formation intellectuelle.

Mathémator : Votre enthousiasme me ravit. Commençons donc par un problème classique qui ravira l'informaticien en herbe que vous êtes.

2 1 Récurrence, récursion, récursivité, induction & Co.

Mathémator : Commençons notre année par un petit jeu :



Ce casse-tête a été posé par le mathématicien français Édouard LUCAS en 1883.
Le jeu consiste en une plaquette de bois où sont plantés trois piquets. Au début du jeu, 8 disques de diamètres croissant de bas en haut sont placés sur le piquet de gauche. Le but du jeu est de mettre ces disques dans le même ordre sur le piquet de droite en respectant les règles suivantes :

– on ne déplace qu'un disque à la fois ;
– on ne peut poser un disque que sur un disque de diamètre supérieur.

Essayez d'abord avec 2 puis 3 disques.

Hihutix: Bon, avec deux, je mets le disque là puis l'autre là-bas et ensuite celui-ci ici. Ça marche. Avec trois, je bouge celui-là, et puis l'autre, celui-ci ici, l'autre là, puis celui-là là et l'autre là puis le dernier ici. Ah, c'est pas le bon piquet mais ça marche à peu près. Facile votre jeu.

Mathémator : Alors essayez avec quatre, cinq, autant de disques que vous voulez.

Quelques minutes plus tard

Hihutix: Pénible votre jeu !

Mathémator : Les choses se compliquent. Il est temps de parler de la légende rapportée par LUCAS dans ses « *récréations mathématiques* » :

> *N. Claus de Siam a vu, dans ses voyages pour la publication des écrits de l'illustre Fer-Fer-Tam-Tam, dans le grand temple de Bénarès, au-dessous du dôme qui marque le centre du monde, trois aiguilles de diamant, plantées dans une dalle d'airain, hautes d'une coudée et grosses comme le corps d'une abeille. Sur une de ces aiguilles, Dieu enfila au commencement des siècles, 64 disques d'or pur, le plus large reposant sur l'airain, et les autres, de plus en plus étroits, superposés jusqu'au sommet. C'est la tour sacrée du Brahmâ. Nuit et jour, les prêtres se succèdent sur les marches de l'autel, occupés à transporter la tour de la première aiguille sur la troisième, sans s'écarter des règles fixes que nous venons d'indiquer, et qui ont été imposées par Brahma. Quand tout sera fini, la tour et les brahmes tomberont, et ce sera la fin des mondes !*

C'est un problème posé par un mathématicien mais nous allons l'étudier en *informathicien*. Nous voudrions répondre à plusieurs questions :

- peut-on résoudre le problème des 64 disques ?
- si oui, en combien de mouvements ?
- peut-on trouver une tactique la plus efficace possible ?
- est-ce que la fin du monde est pour bientôt ?

Au lieu d'étudier des cas séparés, nous allons généraliser un peu et considérer une tour avec n disques, n étant un entier naturel non nul.

Hihutix: Cela va compliquer les choses. Pourquoi ne pas s'en tenir à un cas précis ? C'est une perversion de mathématicien.

Mathémator : Détrompez-vous ! Au lieu d'étudier un à un des cas isolés, il est bon pour un informaticien aussi de voir qu'un programme plus général pourra traiter tous les cas. Cependant, il sera utile d'étudier des cas simples d'abord pour se donner une idée.
Après une rapide exploration avec papier et crayon, il est temps pour un *informathicien* d'introduire des notations adéquates.
Notons M_n le nombre minimum de mouvements pour transférer n disques. Pouvez-vous donner les premières valeurs de M_n ?

Hihutix: Bon, s'il n'y a qu'un disque, on ne pourra pas faire mieux qu'un déplacement : $\mathrm{M}_1 = 1$. Avec deux disques, hop, hop, hop : trois mouvements ; $\mathrm{M}_2 = 3$. Pour trois, j'avais trouvé sept déplacements mais je ne suis pas sûr que ça soit la meilleure solution.

Mathémator : C'est ce que nous allons prouver mais tout d'abord, en bon mathématicien, rajoutons un cas extrême : s'il y a zéro disque, il faudra zéro mouvement.

Hihutix: C'est un peu tiré par les cheveux.

Mathémator : Mais considérer les cas les plus triviaux permet souvent de simplifier le cas général. Il est temps d'ailleurs de voir grand mais il nous faudrait une idée. Essayons de trouver des points communs aux déplacements de deux et trois disques respectivement.

Hihutix: Ben, je mets le petit sur le piquet du milieu, le grand sur celui d'arrivée puis le petit sur ce même piquet d'arrivée.

Mathémator : Pour trois c'est pareil : je mets les deux petits sur celui du milieu, le grand sur celui d'arrivée puis les deux petits par dessus le grand.

Hihutix: Vous trichez ! Vous avez bougé deux disques en même temps.

Mathémator : En fait, j'ai vu que je savais bougé deux disques d'un piquet vers un autre. Cela me demande trois étapes qui se cachent derrière le « *je mets les deux petits sur celui du milieu* ».
Cela nous donne en fait la solution : avec $n+1$ disques, je bouge les n plus petits sur le piquet du milieu (M_n mouvements), je bouge le plus grand sur le piquet d'arrivée (1 mouvement) puis je redéplace les n petits sur le grand (M_n mouvements). Ainsi :

$$M_{n+1} \leqslant 2M_n + 1$$

Hihutix: Pourquoi avoir utilisé $\leqslant$ et non pas $=$? Et puis, on ne connaît pas M_n.

Mathémator : Vous touchez du doigt deux problèmes essentiels qui vont guider bon nombre de nos raisonnements.
Pour le $\leqslant$, il est essentiel de comprendre que nous avons prouvé que $2M_n + 1$ mouvements étaient **suffisants** mais nous ne savons toujours pas si ces $2M_n + 1$ mouvements sont **nécessaires**. C'est très important de comprendre la différence.
Par exemple, pour acheter un chocolat chaud à la cafétéria et l'offrir à son professeur adoré, il est **suffisant** d'avoir 10 euros dans sa poche mais ce n'est pas nécessaire. Inversement, il est **nécessaire** d'avoir au moins 20 centimes mais ce n'est malheureusement pas suffisant.
Nous étudierons cela en détail dans le prochain chapitre sur la logique mais nous pouvons nous contenter pour le moment d'une approche intuitive.

À retenir

On considère P et Q deux propositions (des énoncés, des faits, des formules).

- Q est une **condition nécessaire** pour avoir P si, dès que P est vraie, alors nécessairement, forcément, obligatoirement, Q est vraie. On note souvent $P \Longrightarrow Q$.
- Q est une **condition suffisante** pour avoir P s'il suffit que Q soit vraie pour que P soit vraie. On note souvent $P \Longleftarrow Q$.
- Lorsque P est à la fois condition nécessaire et condition suffisante de Q, on dit que P est une **condition nécessaire et suffisante** de Q ou encore que P est vraie **si, et seulement si,** Q est vraie. On note souvent $P \Longleftrightarrow Q$.

Lorsque qu'une « affirmation » du type $P \Longrightarrow Q$ ou $P \Longleftrightarrow Q$ est vraie, on dit que c'est un **théorème**.

Nous développerons des méthodes de preuve dans la section suivante.
Revenons tout d'abord à nos disques. Peut-on faire mieux que la solution proposée ?
À un moment donné, il *faut* bien bouger le plus grand disque puisqu'il est sur le mauvais piquet. Il *faut* donc qu'il soit tout seul et il *faut* donc avoir bougé auparavant les n autres disques plus petits. Cela *nécessite au minimum* M_n mouvements. Après cela, on peut bouger le grand disque autant de fois qu'on le désire mais à un moment donné, il *faudra* le placer sur le piquet d'arrivée et déplacer les n autres disques sur le piquet d'arrivée ce qui *nécessite* à nouveau M_n mouvements.
Ainsi, il *faudra au minimum* effectuer $2M_n + 1$ mouvements.
On a donc prouvé que :

$$M_{n+1} \geqslant 2M_n + 1$$

Il est donc **nécessaire** d'effectuer $2M_n + 1$ mouvements pour déplacer les $n + 1$ disques. Or nous avons montré auparavant que ces $2M_n + 1$ mouvements étaient **suffisants**. On en déduit donc que :

$$\begin{cases} M_0 = 0 \\ M_n = 2M_{n-1} + 1 \text{ pour tout } n > 0 \end{cases}$$

Est-ce que cette formule marche bien avec nos premiers exemples ?

Hihutix: $M_1 = 2 \cdot 0 + 1 = 1$: OK. $M_2 = 2 \cdot 1 + 1 = 3$: OK. $M_3 = 2 \cdot 3 + 1 = 7$: OK.

Mathémator : Ça ne prouve pas grand chose mais ça nous rassure. De toute façon, nous avons prouvé que cette formule est bonne. Que vaut M_{64} ?

Hihutix: Ben $M_{64} = 2M_{63} + 1$. Le problème, c'est qu'on ne connaît pas M_{63}.

Mathémator : Et oui : on définit la *suite* **M** à partir d'elle-même, ce qui n'est pas très pratique. On dit qu'on a définit la suite par **récurrence**. Vous verrez cette année en informatique que ce mode de calcul n'est pas réservé aux suites que vous avez peut-être étudiées au lycée. Par exemple, en langage formel, on travaille avec les lettres d'un alphabet. On peut alors définir un mot comme étant soit une lettre, soit une lettre suivi d'un mot.

Hihutix: C'est un peu idiot : en fait, vous me dites que pour savoir si un truc est un mot, faut déjà savoir si c'est un mot.

Mathémator : Vous n'êtes pas assez précis. Prenons notre alphabet et la chaîne de caractères « math ». C'est la lettre « m » suivie de la chaîne « ath » qui est la lettre « a » suivie de la chaîne « th » qui est la lettre « t » suivie de la lettre « h » qui est un mot puisque c'est une lettre. En remontant, on obtient que « th » est un mot puis que « ath » aussi et enfin « math » est donc un mot.

Hihutix (à part): *Ben on le savait avant. Si c'est ça c'qu'on apprend à l'IUT d'info, il est peut-être encore temps de m'inscrire ailleurs.* **(tout haut)** Fabuleux ! Math est un mot ! J'aurais pas cru, comme ça, a priori.

Mathémator : Ah, comme quoi ce que nous faisons est utile.

Hihutix (à part): *Complètement gâteux le gars* **(tout haut)** Je n'en doute pas.

Mathémator : Et la fin du monde dans tout ça ? Pour connaître M_{64}, il semblerait qu'il faille connaître tous les M_k précédents.
Voyons voir, calculez jusqu'à M_6.

Hihutix: Si vous voulez :

- $M_3 = 2 \cdot 3 + 1 = 7$;
- $M_4 = 2 \cdot 7 + 1 = 15$;
- $M_5 = 2 \cdot 15 + 1 = 31$;
- $M_6 = 2 \cdot 31 + 1 = 63$;

Ouais, bof. Je ne vois pas trop où ça nous mène.

Mathémator : « *Ils ont des yeux et ils ne voient pas* ». Et pourtant, quand j'étais jeune, un enfant de six ans aurait reconnu la suite :

$$2^3 - 1,\ 2^4 - 1,\ 2^5 - 1,\ 2^6 - 1, \ldots$$

Hihutix (à part): *Ben tiens ! Les puissances à 6 ans et pourquoi pas les logarithmes à 7.*

Mathémator : Vous dites ?

Hihutix: Je réfléchissais.

Mathémator : Ah. Alors, vous avez sûrement envie de dire que tout prête à croire que :

$$M_n = 2^n - 1,\ \text{pour tout entier strictement positif } n$$

Hihutix: Ben oui, c'est vrai au début donc y a pas de raison pour que ça s'arrête.

Mathémator : Encore faudrait-il le prouver. Par exemple, est-ce que la proposition suivante est un théorème :

Les entiers impairs supérieurs à 3 sont tous des nombres premiers.

Hihutix: 3 est premier, 5 est premier, 7 est premier...

Mathémator : ...donc c'est vrai !

Hihutix: Ben non. 9 est impair mais n'est pas premier...Ouais, OK, j'ai compris.

Mathémator : « Vrai pour les premiers, vrai pour tous » n'est pas un théorème ! Vous retiendrez également que...

À retenir

> Pour prouver qu'une proposition n'est pas un théorème, il suffit d'exhiber un **contre-exemple**.

Nous en reparlerons plus loin. Revenons à notre récurrence ou induction.

À retenir

> Pour prouver qu'une propriété $\mathcal{P}_n$ dépendant uniquement d'un paramètre n est vraie pour tout $n \geqslant n_0$, il faut vérifier que :
>
> – $\mathcal{P}_{n_0}$ est vraie (on parle parfois d'initialisation) ;
>
> – pour tout $n \geqslant n_0$, $\mathcal{P}_n \Longrightarrow \mathcal{P}_{n+1}$ (on parle parfois d'hérédité).

Cela peut par exemple se prouver en *raisonnant par l'absurde* comme nous le verrons en exercice mais nous en reparlerons plus tard.
Ici, pour tout entier naturel non nul n, notons $\mathcal{P}_n$ la proposition : $\mathrm{M}_n = 2^n - 1$.
Cette proposition est vraie pour $n = 1$ puisque $\mathrm{M}_1 = 1 = 2^1 - 1$.
Il existe donc au moins un entier naturel non nul k tel que $\mathcal{P}_k$ soit vraie.
Alors $\mathrm{M}_{k+1} = 2\mathrm{M}_k + 1 = 2(2^k - 1) + 1 = 2 \cdot 2^k - 2 + 1 = 2^{k+1} - 1$.
Ainsi $\mathcal{P}_k \Longrightarrow \mathcal{P}_{k+1}$ pour tout entier naturel non nul k.
Le tour est joué. On peut donc affirmer que $\mathrm{M}_n = 2^n - 1$ pour tout entier naturel non nul n.

Hihutix: Donc $\mathrm{M}_{64} = 2^{64} - 1$. Je prends ma calculatrice...$\mathrm{M}_{64} = 18\,446\,744\,073\,709\,551\,615$. Ça ne m'arrange pas tellement pour connaître la date de la fin du monde.

Mathémator : C'est pourtant simple. Disons que les moines sont très bien entraînés et se relaient efficacement. Ils déplacent alors un disque par seconde. Cela nous donne une durée de jeu de...

Hihutix: Ah, ça je sais : $18\,446\,744\,073\,709\,551\,615/3600/24/365,25/100$ ce qui fait en gros 5.8 milliards de siècles...

Mathémator : Et comme l'Univers a grosso modo 140 millions de siècles d'existence, cela nous laisse de la marge et nous pouvons espérer passer des vacances de Noël 2012 assez tranquilles.

Hihutix: Ouf ! Mais cela ne nous indique pas comment déplacer les huit disques du jeu initial. On sait juste qu'en étant aussi efficaces que les moines, cela nous prendra $\mathrm{M}_8 = 2^8 - 1 = 255$ secondes.

Mathémator : Je vous laisse donc cinq minutes pour le faire.

Cinq minutes plus tard

Hihutix: Il faut se rendre à l'évidence : je ne suis pas fait pour être moine. Faut le faire pour chaque n jusqu'à 8 en fait et noter comment on a fait. Pfff... C'est pénible.

Mathémator : Et quand un informathicien a bien réfléchi sur le papier, il peut laisser faire le sale boulot à la machine. On a en effet une méthode qu'on sait être correcte. Mais il est très difficile de l'appliquer pour un grand n donné. On sait que ça marche mais on ne sait pas vraiment comment ça marche. Et c'est là qu'une programmation bien pensée devient merveilleusement efficace. Si on a à notre disposition un langage sachant traiter la récursion, il va suffire de lui donner un minimum d'instruction.

Rappelons ici notre méthode : avec $n+1$ disques, je bouge les n plus petits sur le piquet du milieu (M_n mouvements), je bouge le plus grand sur le piquet d'arrivée (1 mouvement) puis je redéplace les n petits sur le grand (M_n mouvements).

Illustrons notre propos avec le langage OCAML qui aime les récursions :

On commence par créer une fonction qui affichera le mouvement effectué :

```
let mvt depart arrivee=
print_string
("Déplace un disque de la tige "^depart^" vers la tige "^arrivee);
print_newline();;
```

mouvement élémentaire

Le programme proprement dit :

```
let rec hanoi a b c= function
   | 0 -> ()  (*0 disque : on ne fait rien*)
   | n -> hanoi a c b (n-1); (*n-1 disques sont déplacés de a vers b*)
          mvt a c; (*on déplace le disque restant en a vers c*)
          hanoi b a c (n-1) (*n-1 disques sont déplacés de b vers c*);;
```

résolution récursive du problème des tours de Hanoï

Les phrases entre `(*` et `*)` sont des commentaires.

Par exemple, dans le cas de 4 disques, on obtient instantanément :

```
# hanoi "A" "B" "C" 4;;
Déplace un disque de la tige A vers la tige B
Déplace un disque de la tige A vers la tige C
Déplace un disque de la tige B vers la tige C
Déplace un disque de la tige A vers la tige B
Déplace un disque de la tige C vers la tige A
Déplace un disque de la tige C vers la tige B
Déplace un disque de la tige A vers la tige B
Déplace un disque de la tige A vers la tige C
Déplace un disque de la tige B vers la tige C
Déplace un disque de la tige B vers la tige A
Déplace un disque de la tige C vers la tige A
Déplace un disque de la tige B vers la tige C
Déplace un disque de la tige A vers la tige B
Déplace un disque de la tige A vers la tige C
Déplace un disque de la tige B vers la tige C
- : unit = ()
```

Hihutix: Waouh ! Ça je préfère.

Mathémator : Je n'en doute pas, mais pour y arriver, il faudra passer par le stade « réflexion mathématiquement assistée avec papier-crayon »

Pour aller plus loin

En 1889, l'Italien Guiseppe PEANO, liguiste et mathématicien italien, propose une construction axiomatique de l'ensemble des nombres naturels.
Un axiome, c'est quelque chose qu'on tient pour vrai sans preuve. Pour construire l'ensemble des entiers naturels, PEANO a posé cinq axiomes :

1. l'élément appelé zéro et noté 0, est un entier naturel.
2. Tout entier naturel n a un unique successeur, noté $s(n)$ ou S_n.
3. Aucun entier naturel n'a 0 pour successeur.
4. Deux entiers naturels ayant même successeur sont égaux.
5. Si un ensemble d'entiers naturels contient 0 et contient le successeur de chacun de ses éléments, alors cet ensemble est égal à $\mathbb{N}$.

Le dernier axiome est à la base de la preuve par récurrence que nous venons de voir. En fait, on peut montrer que cet axiome peut être remplacé par un autre qui lui est équivalent : « *tout ensemble d'entiers naturels non vide possède un plus petit élément* ». Le principe de récurrence devient une conséquence de ce nouvel axiome. On le montre par une démonstration par l'absurde.
Considérons l'ensemble

$$\mathrm{U} = \{k \in \mathbb{N} \mid k \geqslant n_0 \text{ et } \mathrm{P}(k) \text{ est faux}\}$$

Supposons que U soit non vide (nous sommes en train de faire une démonstration par l'absurde...), il admet donc un plus petit élément$n \in \mathbb{N}$, $n \geqslant n_0 + 1$ (puisque $\mathrm{P}(n_0)$ est vrai par hypothèse) et $\mathrm{P}(n)$ faux. Par conséquent $n-1 \geqslant n_0$ et $\mathrm{P}(n-1)$ est vrai ce qui prouve que $\mathrm{P}(n)$ est vrai ce qui donne la contradiction attendue.
Ce raisonnement est souvent utilisé pour remplacer la récurrence.

2 2 Théorèmes

Mathemator et Hihutix sont sortis prendre un chocolat chaud : profitons-en pour avancer un peu plus vite, sachant que cette partie sera traitée plus rigoureusement dans le prochain chapitre.

En mathématiques, mais aussi dans toute science, on est amené à énoncer « des vérités » ou des conséquences logiques. On commence par « planter le décor », i.e. [a] on précise les objets qui entrent en jeu et un théorème s'énonce alors le plus souvent sous la forme :

si on a P alors on a **forcément** Q
ou bien
si P est vraie alors Q est **forcément** vraie

où P et Q désignent des affirmations (des énoncés) ou des faits ou des formules .... Ces « vérités » portent le nom de théorèmes et **se notent**

$$\mathrm{P} \Rightarrow \mathrm{Q}$$

qu'il faut **absolument** lire : « si P est vraie alors Q est **forcément** vraie » ou bien « si on a P

a. id est = c'est à dire

alors on a forcément Q » ou, **à la rigueur**, « P implique (ou entraîne) Q ».

Exemple 1.1

f est une fonction numérique de variable réelle définie sur l'intervalle $\mathrm{I} = [a, b]$ avec $a < b$ et $x_0 \in \mathrm{I}$. On vient de « planter le décor », c'est obligatoire. Maintenant nous énonçons une « vérité » que vous connaissez tous :

si f est dérivable en x_0 alors f est forcément continue en x_0

C'est un théorème ! La paresse aidant, on se permet de l'écrire sous la forme :

$$f \text{ dérivable en } x_0 \Rightarrow f \text{ continue en } x_0$$

mais il faut absolument lire cette formule « si f est dérivable en x_0 alors f est forcément continue en x_0 ».

Exemple 1.2

Considérons l'énoncé

Si $x^2 = 4$ alors forcément on a $x = 2$

Est-ce un théorème ou, si vous préférez, cette affirmation est-elle vraie ? J'imagine que beaucoup d'entre vous seraient tentés de dire oui ! Malheureusement c'est faux, on n'a pas forcément $x = 2$, x peut aussi être égal à -2. Par contre, si on nous dit que *les* x avec lesquels on travaille sont < 0 alors

Si $x^2 = 4$ alors forcément on a $x = -2$

est un théorème que l'on écrit

Si $x^2 = 4$ et $x < 0$ alors forcément on a $x = -2$

Pour démontrer un théorème P ⇒ Q, P est l'hypothèse et Q est la conclusion, on utilise évidemment l'hypothèse P mais aussi des « vérités » connues (démontrées) ou admises (axiomes) pour arriver à prouver Q. Cette démarche porte le nom de démonstration. Ce n'est pas la seule façon de raisonner, en effet, considérons donc le théorème

si on a P alors on a forcément Q

Cet énoncé nous dit qu'il suffit de savoir que P est vraie (ou vérifiée) pour que Q le soit. Pour cela on dit que P est une **Condition Suffisante** de Q. Si Q est fausse, il est impossible que P soit vraie car, si P était vraie, le théorème P ⇒ Q nous affirme que Q serait forcément vraie. En conséquence pour que P soit vraie, il faut d'abord que Q le soit. Pour cela on dit que Q est une **Condition Nécessaire** de P. Nous venons de prouver ou de démontrer que si P ⇒ Q est un théorème alors nous avons aussi le théorème

si Q est fausse alors P est forcément fausse

qui s'écrit « non Q ⇒ non P » ou, en utilisant un symbole de la logique des propositions, $\neg Q \Rightarrow \neg P$. Inversement si $\neg Q \Rightarrow \neg P$ est un théorème, si P est vraie, cela équivaut à dire que « non P » est fausse, il est alors impossible que Q soit fausse, en conséquence P ⇒ Q est un théorème. La conclusion de ce qui précède est la suivante :

- Démontrer $P \Rightarrow Q$, c'est aussi démontrer $\neg Q \Rightarrow \neg P$.

– Démontrer $\neg Q \Rightarrow \neg P$, c'est aussi démontrer $P \Rightarrow Q$.

Nous avons dit que, si $P \Rightarrow Q$ est un théorème, Q est une condition nécessaire de P, cela se traduit par le fait qu'il est impossible d'avoir simultanémant P vraie et Q fausse et donc que si on suppose simultanément P vraie et Q fausse, un raisonnemnt doit nous amener obligatoirement à contredire au moins une vérité connue.

À retenir

En conclusion, pour démontrer un théorème $P \Rightarrow Q$ on peut utiliser les techniques suivantes :

- Supposer que P est vraie et, en utilisant des résultats prouvés ou définitions ou .... , arriver à prouver que Q est vraie. C'est ce qu'on appelle une démonstration directe.
- Supposer que Q est fausse et, en utilisant des résultats prouvés ou définitions ou des calculs ou ...., arriver à prouver que P est fausse. Ce type de raisonnement est un **raisonnement ou démonstration par contraposition**.
- Supposer simultanément que P est vraie et Q fausse et, en utilisant des résultats prouvés ou définitions ou des calculs ou ...., arriver à une contradiction flagrante ou un résultat manifestement impossible qui peut être $2 = -2$ dans $\mathbb{R}$ ou $x \in A$ et $x \notin A$ ou .... Ce type de raisonnement est un **raisonnement ou démonstration par l'absurde**.

Remarque 1

Il est bien évident que dans toute démonstration on se sert de la transitivité de l'implication

« si on a P alors on a R » et « si on a R alors on a Q »
nous donnent « si on a P alors on a Q »

c'est le « modus barbara », littéralement « la manière étrangère ». Le « modus ponens », littéralement « la manière en posant », traduit que si l'implication $(P \Rightarrow Q)$ est vraie et si P est vraie alors Q est vraie. Pour sa part, le « modus tollens », littéralement « la manière en ôtant », traduit que si $(P \Rightarrow Q)$ est vraie et que Q est fausse alors P est fausse.

Remarque 2

Les théorèmes qui s'énoncent sous la forme

$$P \Leftrightarrow Q$$

traduisent que P est une condition nécessaire et suffisante de Q (ou inversement), cela traduit que P est vraie si, et seulement si, Q est vraie. Pour le démontrer il est conseillé de démontrer les deux théorèmes $P \Rightarrow Q$ et $Q \Rightarrow P$ plutôt que de vouloir à tout prix procéder par équivalences.

3 Théorie naïve des ensembles

3 1 Éléments

Mathémator : Pour cette partie du cours, je m'inspirerai grandement d'un livre de Jean et Suzanne DANIAU publié en 1975 aux éditions CEDIC sous le titre « *Activités mathématiques des enfants de cinq à six ans. Suggestions à l'usage des maîtres* »

Hihutix (à part): *Il cherche vraiment à m'humilier. C'est bien un prof!* **(tout haut)** J'espère avoir le niveau CP.

Mathémator : Les concepteurs des programmes de la maternelle des années 1970 ont peut-être été un peu trop ambitieux mais je vous ai signalé cette petite information pour dédramatiser le cours et vous mettre en confiance.

Hihutix: Quel pédagogue ! J'ai vraiment de la chance de suivre votre enseignement.

Mathémator : Tout petit, donc, on apprend à regrouper des collections d'objets selon certains critères : les copains, les boulets, les cours à ne pas rater, les joueurs dans une équipe, les équipes dans un championnat, les championnats selon le sport, etc. En mathématiques, on est assez collectivistes : on s'intéresse aux propriétés partagées par tous les membres d'une tribu et peu à celles vérifiées par quelques individus [b].
Par exemple, je voudrais collectionner les nombres entiers strictement supérieurs à 1 et qui ne sont divisibles que par 1 et eux-mêmes : comment faire ?

Hihutix: C'est les nombres premiers.

Mathémator : Certes, et l'étude de ces nombres particuliers occupe les esprits depuis des siècles. Vous savez peut-être que le nombre de nombres premiers est infini [c] mais on a envie de se référer à cette collection de nombres. De ce genre d'envie est née la notion d'*ensemble* qui n'a été pleinement développée qu'à partir du début du XXe siècle. Je préfère à présent laisser la parole au Maître :

En mathématiques, pour utiliser correctement un concept, il est nécessaire que ce dernier soit parfaitement défini et qu'on puisse en apprécier les contours. C'est ce que nous allons essayer de faire pour le concept d'**ensemble** et ce n'est pas si facile car notre langage courant peut très bien utiliser le terme ensemble pour dénoter des objets qui ne sont pas des ensembles « mathématiquement parlant ».
Notre ambition, ici, se limite à présenter un cadre strict d'utilisation de la théorie des ensembles et à montrer combien le langage de tous les jours peut être trompeur voire erroné ou dénué de sens lorsque le discours utilise ou définit certains ensembles. N'entend-on pas chaque nouvelle année universitaire qu'une promotion est constituée d'étudiants et nous préciser ensuite qu'une promotion est aussi constituée de groupes. Nous sommes alors en présence d'un ensemble nommé *promotion* et se pose alors la question : « quels sont les éléments de cet ensemble ? ». Sont-ce les étudiants inscrits ? Sont-ce les groupes ? Quel est le sens mathématique du verbe *constituer* ? On ne peut se contenter de réponses approximatives puisque toute spécification informatique se doit d'utiliser des ensembles dont les définitions et les limites sont parfaitement claires.
On considère généralement que les notions d'ensemble, d'appartenance et d'égalité sont des notions *primitives*, en ce sens qu'elles font parties du patrimoine culturel de quiconque comme les notions de point et de droite en géométrie. Néanmoins, nous allons rappeler, voire redéfinir certains mots car la théorie -même « naïve [d] »- des ensembles, la TNE, doit être employée avec un vocabulaire précis et tout n'est pas si simple ....

b. Les dirigeants de la République Populaire de Chine ont le plus souvent suivi une solide formation mathématique : cause ? Conséquence ?...
c. Vous pouvez même le prouver pendant vos temps libres ou en DS, c'est un raisonnement par l'absurde classique...
d. Par opposition à la théorie dite axiomatique.

Hihutix: Le Maître est sage.

Mathémator : Pour vous convaincre qu'une approche trop simpliste et intuitive peut être trompeuse, considérez la situation suivante, connue sous le nom de *paradoxe de* RUSSELL, du nom du célèbre mathématicien britannique et néanmoins prix Nobel de littérature Bertrand RUSSELL :

> Dans une ville, il existe deux types d'hommes : ceux qui se rasent eux-mêmes et les autres. Pour ces derniers, la mairie a désigné un barbier, chargé de tous les raser, et eux seulement : qui rasera le barbier ?...

Hihutix: Moi je me rase tout seul, une fois par mois.

Mathémator : Merci pour cette information pertinente mais je voulais pointer ici le problème de l'existence d'un ensemble de tous les ensembles : pour garantir la validité de la théorie des ensembles, il a fallu postuler que l'ensemble de tous les ensembles...n'en était pas un !

Hihutix: Et vous discutiez de ça en maternelle ?

Mathémator : Je dois avouer que non. Mais trêve de considérations philosophiques. Nous admettrons qu'il existe des ensembles de référence et qu'à partir d'eux on peut en construire d'autres à l'aide d'outils que nous allons découvrir...ensemble.

Hihutix (à part): *Grave drôle sa blague à deux balles.*

Mathémator : N'oublions pas non plus que nous travaillons au département d'informatique et qu'un ordinateur travaille avec des ensembles finis et donc on peut étudier somme toute assez « naïvement » les ensembles sans être confrontés à des paradoxes.

Bon, reprenons. Retenons donc de ce qui précède qu'un ensemble est une collection d'objets (objets matériels ou concepts abstraits) définis sans ambiguïté et que les objets de cet ensemble sont appelés **éléments** de l'ensemble. Nous venons d'utiliser le concept primordial de la théorie des ensembles à savoir celui d'**appartenance** : si E désigne un ensemble [e] et si u est un élément de cet ensemble on écrit

$$u \in \mathrm{E}$$

et $a \notin \mathrm{E}$ pour exprimer que a n'est pas un élément de E. Il faut tout de suite noter que le symbolisme utilisé est tout à fait arbitraire, il n'y a aucune raison sérieuse pour noter les éléments de (l'ensemble) E par des lettres minuscules, il ne faut surtout pas y voir une notion de hiérarchie. Nous verrons ainsi qu'un ensemble peut avoir comme éléments des ensembles.
La relation d'appartenance permet de définir **l'égalité** de deux ensembles, deux ensembles sont égaux si, et seulement si, ils ont les mêmes éléments. Pour exprimer l'égalité des deux ensembles A et B on écrit $\mathrm{A} = \mathrm{B}$ et $\mathrm{A} \neq \mathrm{B}$ exprime que les ensembles A et B ne sont pas égaux, l'un des deux ensembles possédant au moins un élément qui n'appartient pas à l'autre. Cette définition nous amène à dire qu'un ensemble est défini par la liste non ordonnée et sans répétition de ses éléments : **définition en extension.** Nous pouvons alors décider d'une première notation pour les ensembles, une liste (non ordonnée) des éléments de l'ensemble « encadrée » par deux accolades :

$$\text{Chaprot} = \left\{ \text{Papa , Maman , La bonne, Moi} \right\}$$

Papa, Maman, La bonne et Moi sont les quatre éléments de l'ensemble Chaprot.
Il n'y a pas d'ordre dans l'écriture des éléments :

$$\text{Chaprot} = \left\{ \text{Maman , Papa, La bonne, Moi} \right\} = \left\{ \text{Moi, Maman , La bonne, Papa} \right\}$$

e. Nous supposons évidemment l'existence d'au moins un ensemble.

L'ensemble Chaprot peut lui-même appartenir à un ensemble :

$$\text{Familles} = \left\{ \text{Chaprot, Dugland, Du Fermoir de Monsac} \right\}$$

Ainsi, Chaprot est un élément de Familles et Maman est un élément de Chaprot.
Rappelons qu'un ensemble doit être défini sans ambiguïté et qu'en conséquence l'écriture $\{a, a\}$ est incorrecte, elle désigne en fait $\{a\}$. Un ensemble qui ne possède qu'un élément est appelé un singleton et un ensemble qui possède deux éléments est appelé une paire (paire non ordonnée, ne pas confondre avec un couple) ou doublet.
On remarque immédiatement qu'il est impossible de définir un ensemble en extension lorsqu'il a une infinité d'éléments. Un principe majeur de la théorie des ensembles permet dans ce cas, mais aussi dans d'autres, d'identifier les éléments d'un ensemble par l'intermédiaire d'une propriété qu'ils partagent tous. L'axiome en question porte le nom d'axiome de sélection, ou schéma de **compréhension**. De manière simplifiée il s'énonce :

un ensemble A *étant donné ainsi qu'un énoncé ou une propriété* $\mathcal{P}$*, il existe un ensemble* B *dont les éléments sont ceux des éléments de* A *qui satisfont l'énoncé ou la propriété* $\mathcal{P}$*. Cet ensemble* B *est noté indifféremment par :*

$$\begin{aligned}
\mathrm{B} &= \{x \in \mathrm{A} : \mathcal{P}\} = \{x \in \mathrm{A}\,;\mathcal{P}\} = \{x \in \mathrm{A} \mid \mathcal{P}\} = \left\{x \in \mathrm{A} \big/ \mathcal{P}\right\} \text{ ou encore} \\
\mathrm{B} &= \{x : x \in \mathrm{A} \text{ et } \mathcal{P}\} = \{z\,; z \in \mathrm{A} \text{ et } \mathcal{P}\} = \{u \mid u \in \mathrm{A} \text{ et } \mathcal{P}\} = \left\{x \big/ x \in \mathrm{A} \text{ et } \mathcal{P}\right\}
\end{aligned}$$

Cet axiome permet de démontrer qu'il existe un ensemble qui ne possède aucun élément, l'ensemble vide noté $\{\}$ ou $\varnothing$, et que cet ensemble est unique ; pour cela il suffit d'appliquer l'axiome précédent à un ensemble quelconque A et de prendre pour $\mathcal{P}$ l'énoncé $x \neq x$:

$$\mathrm{B} = \{x \in \mathrm{A} \mid x \neq x\} = \{\} = \varnothing$$

Considérons un « autre » ensemble vide, $\mathrm{B}' = \left\{x \in \mathrm{A}' \mid x \neq x\right\}$, nous voulons prouver que $\mathrm{B} = \mathrm{B}'$, pour cela supposons que $\mathrm{B} \neq \mathrm{B}'$, cela signifie que B ou B′ possède au moins un élément qui n'appartient pas à l'autre donc B ou B′ ne serait pas l'ensemble vide ce qui est impossible par hypothèse ; conclusion $\mathrm{B} = \mathrm{B}'$.

Danger

Attention ! L'ensemble $\{\varnothing\}$ est un ensemble ayant l'ensemble vide pour unique élément : il n'est donc pas vide !!! Avec Python :

```
>>> V=[]
# len donne le nombre d'éléments
>>> len(V)
0
>>> W=[V]
>>> len(W)
1
>>> W
[[]]
```

Remarque 3

En Génie Logiciel, on utilise des ensembles « typés » et l'ensemble vide n'est pas unique, il y a autant d'ensembles vides que d'ensembles de base ; « en gros » cela signifie que l'ensemble vide des étudiants est différent de l'ensemble vide des chaises.

Hihutix: Merci pour cette comparaison.

Mathémator : Elle est du Maître. Mais pour me faire pardonner, je vous offre un petit sucre informatique. Le langage Python a l'intéressante particularité de pouvoir définir des listes par compréhension :

```
>>> E=[2,10,12]
>>> F=[k**2 for k in E]
>>> F
[4, 100, 144]
>>> 100 in F
True
```

Remarque 4

Une petite curiosité : la *paire ordonnée* (ou le *couple*) constituée de a et de b dans cet ordre se note (a, b). L'ordre est important et on peut éventuellement avoir $a = b$ ce qui n'est pas le cas pour une paire. En informatique, une manière d'éliminer les doublons dans une liste est de la transformer en ensemble puis à nouveau en liste. Sur Python :

```
>>> A=[1,1,1,2,2,5,6,7,7,7,7,7,7]
>>> E=set(A)
>>> E
set([1, 2, 5, 6, 7])
>>> B=list(E)
>>> B
[1, 2, 5, 6, 7]
# Ou plus rapidement
>>> C=list(set(A))
>>> C
[1, 2, 5, 6, 7]
```

Nous retiendrons de ce paragraphe qu'à chaque fois que sera considéré un ensemble soit il est défini en extension, on indique alors entre deux accolades **dans un ordre quelconque** les différents éléments de cet ensemble, soit il est défini en compréhension et on indique entre deux accolades une propriété caractéristique des éléments de cet ensemble, ces éléments appartenant au préalable à un ensemble bien défini.
Il ne faut surtout pas croire que travailler avec des ensembles soit une chose simple. C'est vrai si l'ensemble A possède des éléments facilement identifiables et en petit nombre, mais si les éléments de A sont des ensembles qui ont eux-mêmes pour éléments des ensembles, on peut avoir beaucoup de mal à se représenter l'ensemble A et à le manipuler.

3 2 Ensembles égaux

Mathémator : La définition de l'égalité de deux ensembles n'est pas vraiment très originale :

Définition 1 - 1

Égalité d'ensembles
Deux ensembles E et F sont égaux si, et seulement si, ils ont les mêmes éléments. On note alors E = F.

Hihutix: Ils sont forts ces mathématiciens ! Où vont-ils trouver ces idées incroyables ?

Mathémator : riez, riez, mais tout ne sera pas toujours aussi simple. Cependant, en grand pédagogue que je suis, je vais essayer de vous mettre en confiance :

Exemple 1.3

On note $\mathrm{E} = \left\{x \in \mathbb{Z} \mid x^2 = 1\right\}$ et $\mathrm{F} = \left\{x \in \mathbb{R} \mid |x| = 1\right\}$. Que pouvez-vous dire de E et F ?

Cependant, démontrer que deux ensembles sont égaux peut devenir fastidieux, voire difficile. Nous verrons plus loin (cf 1.3.6 page 28) comment procéder.

3 3 Inclusion

Un ensemble désigné par B est **contenu** ou **inclus** dans l'ensemble désigné par A ou encore est une **partie** de l'ensemble A si, et seulement si, tout élément de B est aussi un élément de A. On note alors $\mathrm{B} \subseteq \mathrm{A}$ ou $\mathrm{A} \supseteq \mathrm{B}$. On dit aussi que B est **une partie ou un sous ensemble de** A. La définition précédente affirme que $\emptyset$ est inclus dans n'importe quel ensemble A car, si ce n'était pas le cas, l'ensemble vide possèderait au moins un élément qui n'appartient pas à A. On notera aussi que tout ensemble est inclus dans lui même. On retiendra donc que si A désigne un ensemble **on a toujours**

$$\emptyset \subseteq \mathrm{A} \text{ et } \mathrm{A} \subseteq \mathrm{A}$$

Remarque 5

Pratiquement tous les auteurs d'ouvrages mathématiques en langue française utilisent le symbole $\subset$ pour définir l'inclusion (large), nous estimons qu'ils le font à tort. Nous ne nous alignons pas sur une notation anglo-saxonne, nous ne faisons qu'utiliser la notation du système internationnal. Pour nous, le symbole $\subset$ désigne l'inclusion stricte en ce sens que si $\mathrm{B} \subset \mathrm{A}$ on ne peut avoir $\mathrm{B} = \mathrm{A}$ et par conséquent l'énoncé $\mathrm{A} \subset \mathrm{A}$ est faux. Pour éviter les confusions toujours possibles nous utiliserons le symbole $\subsetneq$ ou $\subsetneqq$ pour désigner l'inclusion stricte

$$\mathrm{B} \subsetneq \mathrm{A} \text{ signifie } (\mathrm{B} \subseteq \mathrm{A} \text{ et } \mathrm{B} \neq \mathrm{A})$$

qu'il ne faut pas confondre avec $\mathrm{B} \not\subseteq \mathrm{A}$ qui exprime que B n'est pas inclus dans A. On dit que B est une partie propre de A si, et seulement si, $\mathrm{B} \subseteq \mathrm{A}$ avec $\mathrm{B} \neq \mathrm{A}$ et $\mathrm{B} \neq \emptyset$ (il est nécessaire que A ne soit pas vide et ne soit pas un singleton).

Comme nous l'avons déjà indiqué, un ensemble est toujours inclus dans lui même. Pour tout ensemble A il est correct d'écrire $\mathrm{A} \subseteq \mathrm{A}$. La définition de l'égalité de deux ensembles s'écrit maintenant

$$[\mathrm{A} \subseteq \mathrm{B} \text{ et } \mathrm{B} \subseteq \mathrm{A}] \Leftrightarrow \mathrm{A} = \mathrm{B}$$

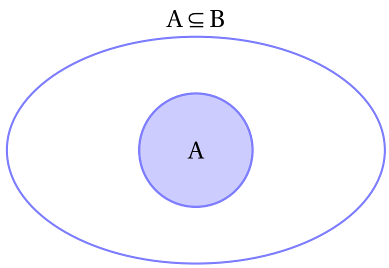
À retenir

Cette propriété est à retenir. Pour démontrer l'égalité de deux ensembles, on n'a pratiquement pas d'autre méthode que de démontrer la double inclusion. Notons aussi le résultat évident

$$[\mathrm{C} \subseteq \mathrm{B} \text{ et } \mathrm{B} \subseteq \mathrm{A}] \Rightarrow \mathrm{C} \subseteq \mathrm{A}$$

Pour guider les raisonnements ou pour « imaginer » les ensembles en présence on est amené à schématiser les ensembles par une ligne fermée sans point double, une « patate » peut très bien faire l'affaire mais un cercle ou un rectangle sont aussi d'excellentes solutions. Ces figures sont appelées diagrammes d'Euler-Venn ou *diagrammes de Venn*. Pour éviter les confusions, il est convenu que les éléments de l'ensemble représenté « sont tous à l'intérieur du dessin et pas sur la frontière ». Pour mettre en exergue un ou plusieurs éléments, on utilise des points ou croix et pour représenter l'ensemble vide, il n'y a aucune bonne solution.

Les patates permettent d'illustrer l'inclusion :



3 4 Parties d'un ensemble

Nous admettons que si E désigne un ensemble alors **l'ensemble des parties de** E est un ensemble (mathématiquement parlant) noté $\mathcal{P}(E)$ mais aussi $\mathbb{P}(E)$. Cet ensemble peut s'écrire en « pseudo-compréhension » par :

$$\mathcal{P}(E) = \left\{X \mid X \subseteq E\right\}$$

nous précisons bien « pseudo-compréhension » car nous ne pouvons indiquer à quel ensemble appartient X puisque nous cherchons à définir cet ensemble. Il faut immédiatement retenir l'équivalence

$$X \in \mathcal{P}(E) \Leftrightarrow X \subseteq E$$

qui seule permet de vérifier que X est bien un élément de $\mathcal{P}(E)$ car il ne faut surtout pas croire que notre esprit soit capable de « maîtriser » un ensemble de parties quasi immédiatement. Pour imaginer un peu plus ce qu'est $\mathcal{P}(E)$ on peut dire que $\mathcal{P}(E)$ est l'**ensemble** des solutions du problème $X \subseteq E$ où X est l'inconnue. On remarque alors que $\varnothing$ et E sont des solutions évidentes et donc que $\mathcal{P}(E)$ ne peut être vide. Si $E = \varnothing$, $\mathcal{P}(E)$ ne contient qu'un seul élément qui est $\varnothing$; $\mathcal{P}(\varnothing) = \{\varnothing\}$ et on se persuadera que $\{\varnothing\}$ n'est pas l'ensemble vide, c'est parfaitement clair, entre les deux accolades « il y a quelque chose » qui existe et qui est l'ensemble vide, $\{\varnothing\}$ est un singleton ! Si $E \neq \varnothing$ alors $\mathcal{P}(E)$ possède au moins deux éléments distincts $\varnothing$ et E :

$$\mathcal{P}(E) = \left\{\varnothing, \ldots, E\right\}$$

Exemple 1.4

Prenons pour ensemble $E = \left\{D, L, M\right\}$ alors

$$\mathcal{P}(E) = \left\{\varnothing, \{D\}, \{L\}, \{M\}, \{D, L\}, \{D, M\} \{L, M\}, E\right\}$$

Que dire de $\mathcal{P}(\mathcal{P}(E))$? Que c'est un ensemble « compliqué », qu'il a 256 éléments dont en voici quelques uns :

$$\mathcal{P}(\mathcal{P}(E)) = \left\{\varnothing, \{\{D\}\}, \cdots, \{\{D\}, \{D, L\}\}, \cdots, \{\{D, L\}, \{D, M\}\}, \cdots\right\}$$

On comprend tout de suite la difficulté d'imaginer l'ensemble des parties d'un ensemble d'autant plus que les diagrammes de Venn ne peuvent nous venir en aide.

Remarque 6

$\mathcal{P}(E)$ est ordonné par la relation $\subseteq$. Nous détaillerons plus loin le concept de relation d'ordre mais indiquons tout de suite les propriétés sous-jacentes :

1. *La relation $\subseteq$ est réflexive, cela signifie que pour toute partie A de E, i.e. pour tout élément A de $\mathcal{P}(E)$, on a $A \subseteq A$.*
2. *La relation $\subseteq$ est antisymétrique, cela signifie que si l'on a simultanément $A \subseteq B$ et $B \subseteq A$ on a forcément $A = B$.*
3. *La relation $\subseteq$ est transitive, cela signifie que si l'on a simultanément $A \subseteq B$ et $B \subseteq C$ alors on a forcément $A \subseteq C$.*

Nous allons maintenant nous intéresser aux « opérations » ensemblistes, on se donne un ensemble de travail appelé E et les ensembles que nous utilisons sont tous des parties[f] de E.

3 5 Opérations

3 5 1 Intersection

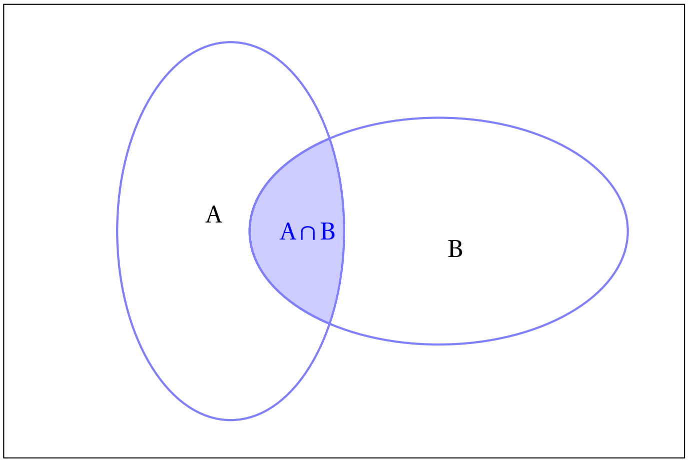
Définition 1 - 2

L'**intersection** des ensembles A et B est l'ensemble $A \cap B$ constitué des éléments communs à A et B. En d'autres termes :

$$A \cap B = \left\{x \in E \mid x \in A \text{ et } x \in B\right\}$$

C'est une partie de E. L'intersection est une *loi de composition* (ou opération) *interne* dans $\mathcal{P}(E)$ qui est *associative, commutative* et qui admet E comme *élément neutre* ($A \cap E = A$), de plus, tout élément est idempotent ($A \cap A = A$). Lorsque $A \cap B = \varnothing$ on dit que les ensembles A et B sont **disjoints**.

f. La théorie axiomatique des ensembles n'exige pas la donnée d'un ensemble E pour définir ce que l'on appelle les opérations usuelles.



Remarque 7

On a l'équivalence $A \cap B = B \Leftrightarrow B \subseteq A$, en effet, supposons en premier que $A \cap B = B$, par définition $A \cap B \subseteq A$ et on obtient tout de suite $B \subseteq A$. Supposons maintenant que $B \subseteq A$, les éléments communs à A et B sont exactement les éléments de B et donc $A \cap B = B$.

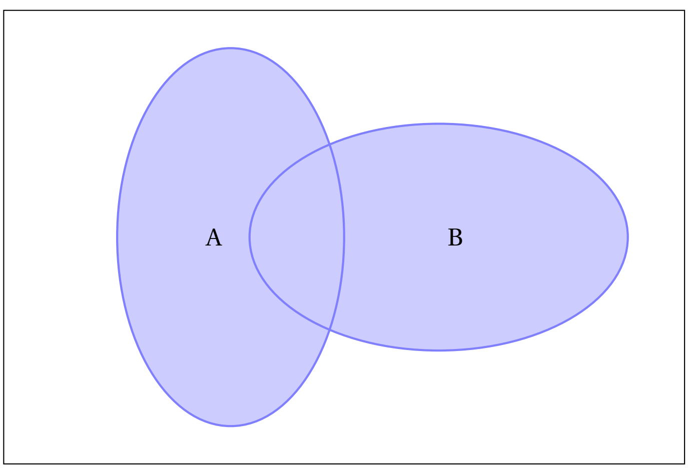
3 5 2 Union

Définition 1 - 3

L'**union** ou la **réunion** des ensembles A et B est l'ensemble :

$$A \cup B = \left\{ x \in E \mid x \in A \text{ ou } x \in B \right\}$$

On doit se persuader que le « ou » intervenant dans cette définition est un « ou non exclusif » et par conséquent on a $A \subseteq (A \cup B)$, $B \subseteq (A \cup B)$ et $(A \cap B) \subseteq (A \cup B)$. L'union est une loi de composition (ou opération) interne dans $\mathcal{P}(E)$ qui est associative, commutative et qui admet $\varnothing$ comme élément neutre ($A \cup \varnothing = A$), de plus tout élément est idempotent ($A \cup A = A$).



$A \cup B$

Remarque 8

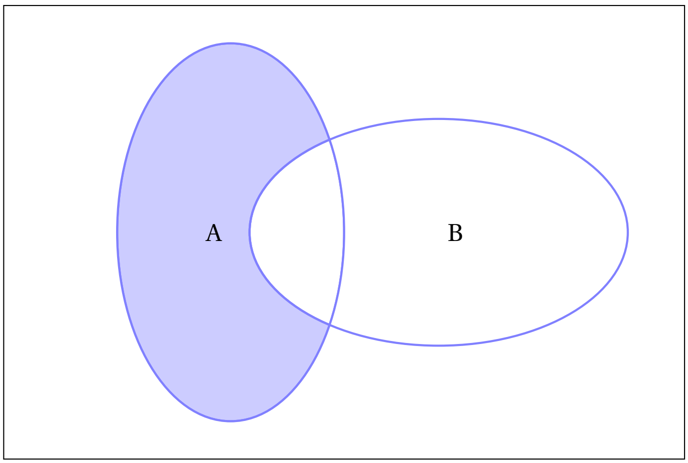
On a l'équivalence $A \cup B = A \Leftrightarrow B \subseteq A$. En effet, si $A \cup B = A$ et comme $B \subseteq (A \cup B)$, on obtient $B \subseteq A$. Si $B \subseteq A$, tout élément de B est aussi un élément de A donc tout élément de $A \cup B$ est aussi un élément de A ; on obtient alors $(A \cup B) \subseteq A$ et comme $A \subseteq (A \cup B)$ on conclut que $A \cup B = A$.

3 5 3 Différence

Définition 1 - 4

La **différence** des ensembles A et B est l'ensemble

$$A - B = \left\{ x \in E \mid x \in A \text{ et } x \notin B \right\}$$



$A - B$

Remarque 9

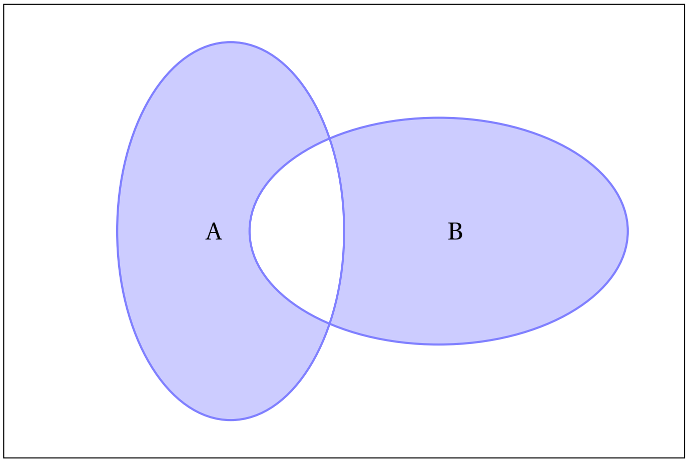
Certains préfèrent utiliser la notation $A \setminus B$ à la place de $A - B$.

3 5 4 Différence symétrique

Définition 1 - 5

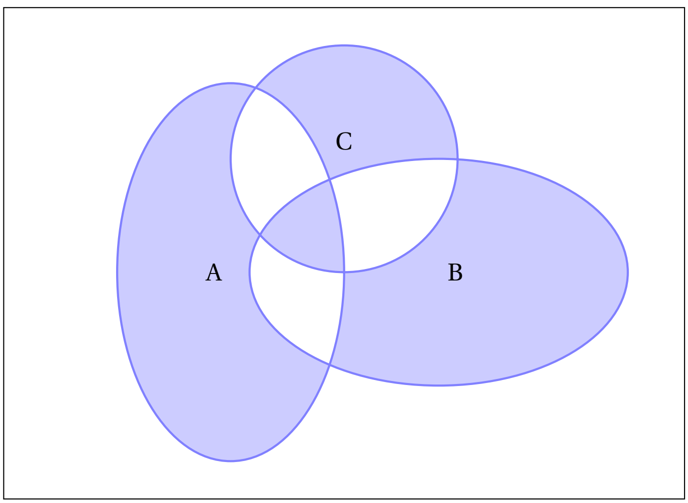
La **différence symétrique** des ensembles A et B est l'ensemble :

$$\begin{aligned} A \bigtriangleup B &= \left\{ x \in E \mid x \in A - B \text{ ou } x \in B - A \right\} = (A - B) \cup (B - A) \\ A \bigtriangleup B &= \left\{ x \in E \mid x \in A \cup B \text{ et } x \notin A \cap B \right\} = (A \cup B) - (A \cap B) \end{aligned}$$



$A \bigtriangleup B$

L'opération $\bigtriangleup$ est associative (nous démontrons cette affirmation plus loin), commutative, admet $\varnothing$ comme élément neutre et tout élément A est son propre symétrique $\left(A \bigtriangleup A = \varnothing\right)$. On résume toutes ces propriétés en disant que $\mathcal{P}(E)$ muni de la loi $\bigtriangleup$ est un groupe[g] commutatif. Vous pourrez vérifier que $A \bigtriangleup B \bigtriangleup C$ peut être représenté par :



$A \bigtriangleup B \bigtriangleup C$

Remarque 10 La différence symétrique correspond au « ou exclusif ».

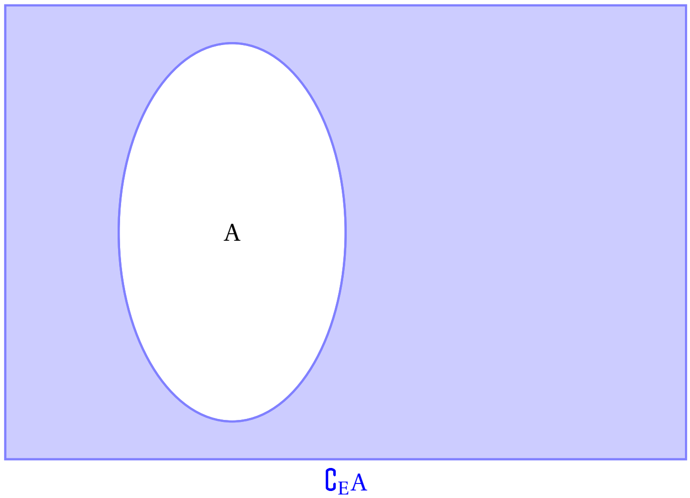
g. Les structures de groupe, anneau et corps doivent devenir pour vous des notions familières mais ne peuvent faire l'objet de questions à un DS.

3 5 5 Complémentaire

Définition 1 - 6

A désignant une partie de E, le **complémentaire** de A par rapport à E ou le complémentaire de A dans E est l'ensemble noté $\complement_{\mathrm{E}}\mathrm{A}$ défini par

$$\complement_{\mathrm{E}}\mathrm{A} = \mathrm{E} - \mathrm{A} = \left\{x \in \mathrm{E} \mid x \notin \mathrm{A}\right\}$$



S'il n'y a pas d'ambiguïté sur le référentiel E, $\complement_{\mathrm{E}}\mathrm{A}$ est noté $\overline{\mathrm{A}}$ et $\overline{\overline{\mathrm{A}}} = \mathrm{A}$.

3 5 6 Lois de De Morgan

Théorème 1 - 1

Lois de DE MORGAN

$$\overline{\left(\bigcup_{i=1}^{n} \mathrm{A}_i\right)} = \bigcap_{i=1}^{n} \overline{\mathrm{A}_i} \qquad \text{et} \qquad \overline{\left(\bigcap_{i=1}^{n} \mathrm{A}_i\right)} = \bigcup_{i=1}^{n} \overline{\mathrm{A}_i}$$

Ceci s'exprime en français courant de la façon suivante :

- Le complémentaire d'une union est égale à l'intersection des complémentaires.
- Le complémentaire d'une intersection est égale à la réunion des complémentaires.

Remarque 11

$\mathrm{A} - \mathrm{B} = \mathrm{A} \cap \overline{\mathrm{B}}$ et $\mathrm{A} \triangle \mathrm{B} = \left(\mathrm{A} \cap \overline{\mathrm{B}}\right) \cup \left(\overline{\mathrm{A}} \cap \mathrm{B}\right)$.

3 6 Fonction caractéristique

Mathémator : Nous avons déjà indiqué quelques propriétés des opérations que nous venons de présenter, le plus souvent sans démonstration car ces dernières sont assez fastidieuses lorsque, pour démontrer l'égalité de deux ensembles, il faut envisager plein de cas. Les diagrammes de Venn peuvent nous aiguiller vers une démonstration mais ne peuvent en aucun cas la remplacer. Nous allons, ici, présenter un outil très efficace qui permet de faire beaucoup de démonstrations sans trop de peine.

Soit E un ensemble. Pour toute partie A de E on définit l'application [h] caractéristique $\mathbb{1}_A$ de A dans E par :

$$\mathbb{1}_A : \begin{array}{rcl} E & \to & \{0;1\} \\ x & \mapsto & \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{si } x \notin A \end{cases} \end{array}$$

Une propriété essentielle de cette notion est donnée par l'équivalence

$$\mathbb{1}_A = \mathbb{1}_B \Longleftrightarrow A = B$$

Hihutix: Je ne vois pas trop où se trouve la simplification !

Mathémator : Un informaticien utilise un « *computer* », c'est-à-dire un calculateur. Nous voudrons donc pouvoir *calculer* avec des ensembles.

Notations

Pour simplifier les écritures, nous utiliserons des opérations sur ces applications caractéristiques :

- $\mathbb{1}_A.\mathbb{1}_B$ ou $\mathbb{1}_A\mathbb{1}_B$ définie pour tout x de E par $(\mathbb{1}_A\mathbb{1}_B)(x) = \mathbb{1}_A(x) \times \mathbb{1}_B(x)$;
- $1 - \mathbb{1}_A$ définie par $(1 - \mathbb{1}_A)(x) = 1 - \mathbb{1}_A(x)$;
- $\mathbb{1}_A + \mathbb{1}_B$ définie par $(\mathbb{1}_A + \mathbb{1}_B)(x) = \mathbb{1}_A(x) + \mathbb{1}_B(x)$.

On voudrait maintenant exprimer $\mathbb{1}_{\overline{A}}$, $\mathbb{1}_{A\cap B}$, $\mathbb{1}_{A-B}$, $\mathbb{1}_{A\cup B}$ et $\mathbb{1}_{A \triangle B}$ à l'aide de $\mathbb{1}_A$ et de $\mathbb{1}_B$.

Je vous donne un coup de main :

- $\mathbb{1}_{\overline{A}} = 1 - \mathbb{1}_A$, c'est évident, ces deux applications coïncident sur E.
- $\mathbb{1}_{A\cap B} = \mathbb{1}_A\mathbb{1}_B$, c'est tout aussi évident, elles coïncident sur E ; on en déduit que $\mathbb{1}_{A\cap A} = \mathbb{1}_A\mathbb{1}_A = \mathbb{1}_A$.
- $\mathbb{1}_{A-B} = \mathbb{1}_A - \mathbb{1}_A\mathbb{1}_B$. On peut le démontrer en vérifiant la coïncidence de ces deux applications sur E mais il est plus judicieux de remarquer que $A - B = A \cap \overline{B}$ et du coup

$$\mathbb{1}_{A-B} = \mathbb{1}_{A\cap\overline{B}} = \mathbb{1}_A\mathbb{1}_{\overline{B}} = \mathbb{1}_A(1 - \mathbb{1}_B) = \mathbb{1}_A - \mathbb{1}_A\mathbb{1}_B$$

h. La définition complète d'une application sera donnée lors de l'étude des relations binaires.

– Concernant $\mathbb{1}_{A\cup B}$, pour trouver une formule similaire aux précédentes, il faut faire preuve d'un peu d'imagination : nous utilisons le résultat[i] $\overline{X\cup Y} = \overline{X}\cap\overline{Y}$ que nous démontrons à l'aide du tableau suivant

$x\in X$	$x\in Y$	$x\in\overline{X\cup Y}$	$x\in\overline{X}\cap\overline{Y}$
non	non	oui	oui
non	oui	non	non
oui	non	non	non
oui	oui	non	non

Ceci étant, $A\cup B = \overline{\overline{A\cup B}} = \overline{\overline{A}\cap\overline{B}}$; on obtient alors

$$\mathbb{1}_{A\cup B} = \mathbb{1}_{\overline{\overline{A}\cap\overline{B}}} = 1 - \mathbb{1}_{\overline{A}\cap\overline{B}}$$

soit $\mathbb{1}_{A\cup B} = 1 - (1-\mathbb{1}_A)(1-\mathbb{1}_B)$ qui se développe en

$$\mathbb{1}_{A\cup B} = \mathbb{1}_A + \mathbb{1}_B - \mathbb{1}_A\mathbb{1}_B$$

– Pour $\mathbb{1}_{A\triangle B}$ je vous laisse prouver que : $\mathbb{1}_{A\triangle B} = \mathbb{1}_A + \mathbb{1}_B - 2\mathbb{1}_A\mathbb{1}_B$.

Recherche

Voici quelques propriétés (en vrac) importantes qu'il faut connaître, certaines sont évidentes et d'autres pas, nous reprenons des résultats déjà énoncés et nous ne donnons que quelques démonstrations, le lecteur étant invité à les reprendre et à en faire d'autres. Il doit être clair que tous les ensembles utilisés sont des parties de l'ensemble E !

– $\cup$ et $\cap$ sont associatives et commutatives. Démontrons l'associativité de l'intersection. Pour cela choisissons trois parties quelconques A, B et C de $\mathcal{P}(E)$. Il nous faut démontrer l'égalité des ensembles $U = A\cap(B\cap C)$ et $V = (A\cap B)\cap C$ et pour cela il suffit de prouver l'égalité des applications caractéristiques de U et V dans E. Allons-y : $\mathbb{1}_U = \mathbb{1}_{A\cap(B\cap C)} = \mathbb{1}_A\mathbb{1}_{B\cap C} = \mathbb{1}_A\mathbb{1}_B\mathbb{1}_C = \mathbb{1}_{A\cap B}\mathbb{1}_C = \mathbb{1}_V$. L'associativité de $\cap$ et $\cup$ permet d'utiliser les notations, lorsque $k\in\mathbb{N}^*$,

$$\bigcup_{i=1}^{k} A_i = A_1\cup A_2\cup\ldots\cup A_n$$
$$\bigcap_{i=1}^{k} A_i = A_1\cap A_2\cap\ldots\cap A_n$$

– $A\subseteq B \Longleftrightarrow A\cup B = B \Longleftrightarrow A\cap B = A \Longleftrightarrow A-B=\varnothing$
– $A\subseteq(A\cup B), (A\cap B)\subseteq A$
– $A-A = A\triangle A = A\cap\varnothing = \varnothing$
– $A\cap A = A\cup A = A\cup\varnothing = A\cap E = A\triangle\varnothing = A$
– $A\cap(A\cup B) = A = A\cup(A\cap B)$
– $\overline{\left(\overline{A}\right)} = A, \overline{A}\cap A = \varnothing, \overline{A}\cup A = E, \complement_E\varnothing = \overline{\varnothing} = E, \complement_E E = \overline{E} = \varnothing$

i. C'est une des formules de De Morgan.

– $\cap$ et $\cup$ sont distributives l'une par rapport à l'autre :

$$\begin{aligned} A\cap(B\cup C) &= (A\cap B)\cup(A\cap C)\\ A\cup(B\cap C) &= (A\cup B)\cap(A\cup C)\end{aligned}$$

La démonstration se fait, soit en vérifiant la double inclusion (c'est un bon exercice), soit en utilisant les applications caractéristiques.

– La différence symétrique est associative et commutative. Démontrons l'associativité toujours à l'aide des applications caractéristiques :

$$\mathbb{1}_{A\triangle(B\triangle C)} = \mathbb{1}_A + \mathbb{1}_{B\triangle C} - 2\mathbb{1}_A\mathbb{1}_{B\triangle C} \text{ avec } \mathbb{1}_{B\triangle C} = \mathbb{1}_B + \mathbb{1}_C - 2\mathbb{1}_B\mathbb{1}_C$$

donne

$$\mathbb{1}_{A\triangle(B\triangle C)} = \mathbb{1}_A + \mathbb{1}_B + \mathbb{1}_C - 2\mathbb{1}_A\mathbb{1}_B - 2\mathbb{1}_A\mathbb{1}_C - 2\mathbb{1}_B\mathbb{1}_C + 4\mathbb{1}_A\mathbb{1}_B\mathbb{1}_C$$

On vérifie que $\mathbb{1}_{(A\triangle B)\triangle C}$ s'exprime de la même façon.

– Rappelons les lois de De Morgan

$$\begin{cases} \overline{\left(\bigcup_{i=1}^{n} A_i\right)} = \bigcap_{i=1}^{n} \overline{A_i}\\ \overline{\left(\bigcap_{i=1}^{n} A_i\right)} = \bigcup_{i=1}^{n} \overline{A_i}\end{cases}$$

Nous avons déjà démontré $\overline{A_1\cup A_2} = \overline{A_1}\cap\overline{A_2}$, pour démontrer

$$\overline{\left(\bigcup_{i=1}^{n} A_i\right)} = \bigcap_{i=1}^{n} \overline{A_i}$$

une récurrence immédiate suffit :

$$\overline{\left(\bigcup_{i=1}^{n+1} A_i\right)} = \overline{\left(\left(\bigcup_{i=1}^{n} A_i\right)\cup A_{n+1}\right)} = \overline{\left(\bigcup_{i=1}^{n} A_i\right)}\cap\overline{A}_{n+1} = \left(\bigcap_{i=1}^{n}\overline{A_i}\right)\cap\overline{A}_{n+1}$$

et l'associativité de l'intersection permet de conclure. Dans la formule

$$\overline{\left(\bigcup_{i=1}^{n} A_i\right)} = \bigcap_{i=1}^{n} \overline{A_i}$$

remplaçons chaque A_i par $\overline{A_i}$:

$$\overline{\left(\bigcup_{i=1}^{n} \overline{A_i}\right)} = \bigcap_{i=1}^{n} \overline{\overline{A_i}} = \bigcap A_i$$

et en écrivant l'égalité des complémentaires de chaque membre il vient

$$\overline{\left(\bigcap_{i=1}^{n} A_i\right)} = \bigcup_{i=1}^{n} \overline{A_i}$$

Fonctions caractéristiques et OCAML

Commentez le listing suivant :

```
# let rec appartient = function
    | (el,[]) -> 0
    | (el,tete::queue) -> if el=tete then 1
                          else appartient(el,queue);;

# let rec carac = function
    |(sous,[]) -> []
    |(sous,tete::queue) -> appartient(tete,sous)::carac(sous,queue);;

# let ens=['a';'b';'c';'d';'e';'f';'g';'h'];;

# let sous_ens_1=['a';'c';'e'];;

# carac(sous_ens_1,ens);;

# let rec op_carac = function
  | (_,[],f) -> []
  | ([],_,f) -> []
  | (tete1::queue1,tete2::queue2,f) -> f(tete1,tete2)::op_carac(queue1,
      queue2,f);;

# let rec carac2ens = function
  | ([],_) -> []
  | (_,[]) -> []
  | (tete::queue,tete_ens::queue_ens) ->
        if tete=0 then carac2ens(queue,queue_ens)
        else tete_ens::carac2ens(queue,queue_ens);;

# let op(a,b,ens,f) =
  carac2ens(op_carac(carac(a,ens),carac(b,ens),f),ens);;

# let sous_ens_2=['a';'d';'f'];;

# let inter(a,b)=a*b;;

# op(sous_ens_1,sous_ens_2,ens,inter);;

# let diff(a,b)=a-a*b;;

# op(sous_ens_1,sous_ens_2,ens,diff);;

# let comp(a,ens)=op(ens,a,ens,diff);;

# comp(sous_ens_1,ens);;

# let union(a,b)=a+b-a*b;;

# op(sous_ens_1,sous_ens_2,ens,union);;
```

```
# let sous_ens_3=['b';'c';'d'];;

# let morg_1=op(op(sous_ens_1,sous_ens_2,ens,inter),op(sous_ens_1,
    sous_ens_3,ens,inter),ens,union);;

# let morg_2=op(sous_ens_1,op(sous_ens_2,sous_ens_3,ens,union),ens,inter);;

# morg_1=morg_2;;
```

3 7 Partition d'un ensemble

Mathémator : E désignant ici un ensemble non vide. Soit P, une partie non vide de $\mathcal{P}(E)$ (on a donc $P \subseteq \mathcal{P}(E)$ et $P \neq \emptyset$) P est un ensemble non vide de parties de E. On dit que P est une **partition** de E si, et seulement si,

1. tout élément de P est non vide,
2. deux éléments distincts quelconques de P sont disjoints,
3. tout élément de E appartient à l'un des éléments de P.

Si E est fini toute partition P de E est du type $P = \{A_1, A_2, \dots, A_k\}$ avec

$$A_i \subseteq E, A_i \neq \emptyset, A_i \cap A_j = \emptyset \text{ si } i \neq j \text{ et } \bigcup_{i=1}^{k} A_i = E$$

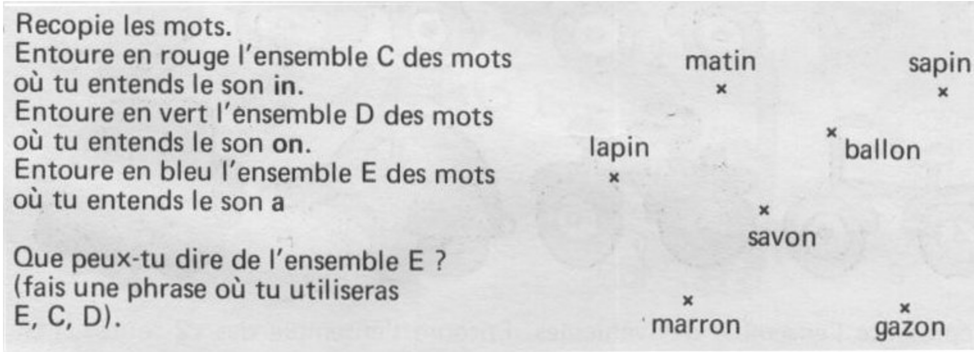
Hihutix: Ouais, bon, pour faire simple, on met les garçons d'un côté et les filles de l'autre. Normalement, on couvre tout le monde et il y a personne à la fois dans les deux groupes.

Mathémator : On peut en effet imaginer une partition de E comme un découpage de E, aucun des morceaux n'étant vide, les morceaux étant tous disjoints deux à deux. Par exemple

$$\{\{\beta\}, \{\alpha, \delta\} \{\varepsilon, \gamma\}\}$$

est une partition de l'ensemble $\{\alpha, \beta, \gamma, \delta, \varepsilon\}$.

Pour vous distraire, voici un exercice extrait de mon livre de CE1 :



Recopie les mots.
Entoure en rouge l'ensemble C des mots où tu entends le son **in**.
Entoure en vert l'ensemble D des mots où tu entends le son **on**.
Entoure en bleu l'ensemble E des mots où tu entends le son a

Que peux-tu dire de l'ensemble E ?
(fais une phrase où tu utiliseras E, C, D).

3 8 Produit cartésien

Mathémator : Dès qu'un mathématicien à un outil à sa disposition comme les ensembles, il a tendance à essayer d'en créer d'autres, plus sophistiqués.

Hihutix: Avouez que les mathématiciens ont l'esprit plutôt tordu.

Mathémator : Ce sont des aventuriers de l'esprit, toujours à la recherche de nouvelles terres vierges à conquérir. Plus prosaïquement, les produits d'ensembles que nous allons explorer sont le point de départ des bases de données.

Par exemple, vous êtes embauché[j] dans un restaurant. Vous disposez de trois ensembles :

– l'ensemble des entrées :

$$\mathrm{E} = \{\text{Cuisses de sauterelles panées, œuf mou, huîtres de l'Erdre}\}$$

– l'ensemble des plats de résistance :

$$\mathrm{P} = \{\text{Turbot à l'huile de ricin, Chien à l'andalouse, Soupe d'orties}\}$$

– l'ensemble des desserts :

$$\mathrm{D} = \{\text{Pomme}, \text{Banane}, \text{Noix}\}$$

Vous avez envie de créer un nouvel ensemble.

Hihutix: celui des menus possibles. Il suffit de regrouper tout le monde en prenant $\mathrm{E}\cup\mathrm{P}\cup\mathrm{D}$.

Mathémator : Je sais bien que la gastronomie n'est pas la principale préoccupation des jeunes au palet perverti par les tristes fastefoudes mais en général on commande UNE entrée SUIVIE D'UN plat de résistance SUIVI D'UN dessert or la simple union que vous avez proposée peut vous faire choisir un menu totalement différent : cinq desserts et vingt entrées, dans n'importe quel ordre, par exemple.

j. Hihutix est donc un garçon...

Nous avons besoin de créer un « objet » ordonné de trois composantes, chacune étant choisie respectivement dans E, P et D.

Par exemple, (œuf mou, chien à l'andalouse, pomme) est un menu. C'est un triplet, à ne pas confondre avec l'ensemble $\{$œuf mou, chien à l'andalouse, pomme$\}$ qui n'est pas ordonné.

Pour aller plus loin

À partir de deux éléments a et b, non nécessairement distincts, on peut construire les deux ensembles suivants :

1. La paire $\{a, b\} = \{b, a\}$ qui se transforme en le singleton $\{a\}$ si $a = b$ (nous avons déjà signalé que l'écriture fautive $\{a, a\}$ désigne le singleton $\{a\}$).
2. La paire $\{\{a\}, \{a, b\}\}$ qui se transforme, si $a = b$, en le singleton

$$\{\{a\}, \{a, a\}\} = \{\{a\}, \{a\}\} = \{\{a\}\}$$

Si $a \neq b$ les deux paires $\{\{a\}, \{a, b\}\}$ et $\{\{b\}, \{a, b\}\}$ sont distinctes, cette écriture permet de définir un ordre car pour chacune de ces paires un seul élément est inclus dans l'autre. Nous décidons de noter une telle paire $\{\{a\}, \{a, b\}\}$ par (a, b) ou $(a; b)$ appelé couple, le couple (a, a) désignant l'ensemble $\{\{a\}\}$. Cette définition compliquée d'un couple permet de s'assurer que l'ensemble de tels couples est bien un ensemble et nous donne les résultats indispensables suivants :

1. Nous avons déjà indiqué que si $a = b$, le couple $(a, b) = (a, a)$ est le singleton $\{\{a\}\}$. Réciproquement si le couple $(a, b) = \{\{a\}, \{a, b\}\}$ est un singleton c'est que $\{a\} = \{a, b\}$ et qu'en conséquence $b \in \{a\}$ soit $b = a$.
2. Pour que les deux couples (a, b) et (c, d) soient égaux, il faut et il suffit que $a = c$ et $b = d$. Démontrons-le : $(a, b) = \{\{a\}, \{a, b\}\}$ et $(c, d) = \{\{c\}, \{c, d\}\}$, si $a = b$ le couple $(a, a) = \{\{a\}\}$ est un sigleton et par conséquent le couple (c, d) aussi ; on en déduit que $c = d$ et $(a, a) = (c, c) = \{\{a\}\} = \{\{c\}\}$ donnent $a = c$. Si $a \neq b$ nécessairement $a = c$ et $\{a, b\} = \{c, d\}$ et comme b ne peut être égal à c sinon on aurait $a = b$, on obtient $b = d$.

On définit le triplet (a, b, c) comme l'ensemble $\{\{a\}\{a, b\}\{a, b, c\}\}$, etc.

Généralisons sans trop entrer dans les détails. La notion de couple se généralise naturellement en notion de triplet, de quadruplet,. . . , de n-uplet, un n-uplet étant noté $\underbrace{(a_1, a_2, \cdots, a_n)}_{n \text{ éléments}}$.

L'égalité de deux n-uplets étant définie par

$$\left(a_1, a_2, \cdots, a_n\right) = \left(a'_1, a'_2, \cdots, a'_n\right) \Leftrightarrow a_i = a'_i \text{ pour tout } i$$

E_1 et E_2 désignant deux ensembles, nous admettons que l'ensemble des couples (a_1, a_2) avec $a_1 \in E_1$ et $a_2 \in E_2$ est bien un ensemble que l'on note $E_1 \times E_2$ appelé **produit cartésien** des ensembles E_1 et E_2, une écriture en pseudo compréhension étant

$$E_1 \times E_2 = \left\{(a_1, a_2) \mid a_1 \in E_1 \text{ et } a_2 \in E_2\right\}$$

On définit de même le produit cartésien des n ensembles ($n \in \mathbb{N}^*$ et $n \geq 2$) $E_{i \in \{1,2,3,\cdots,n\}}$ comme étant l'ensemble :

$$E_1 \times E_2 \times \cdots \times E_n = \prod_{i=1}^{n} E_i = \left\{(a_1, a_2, \cdots, a_n) \mid a_i \in E_i\right\}$$

et lorsque tous les ensembles E_i sont égaux à E on note $E \times E \times \cdots \times E$ par E^n.

Pour se représenter le produit cartésien $E \times F$ avec $E = \{a, b, c\}$ et $F = \{1,2,3,4,5\}$, on peut évidemment l'écrire en extension : il possède $3 \times 5 = 15$ éléments (voir à ce sujet le paragraphe suivant).

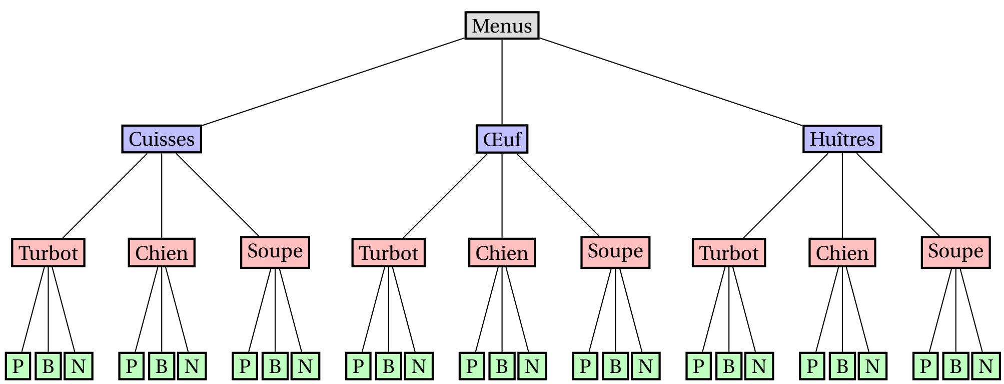
$$E \times F = \left\{(a,1), (a,2), \cdots, (c,5)\right\}$$

mais il est souvent préférable de faire appel à un tableau du type suivant :

$\times$	**1**	**2**	**3**	**4**	**5**
$\boldsymbol{a}$	$(a,1)$	$(a,2)$	$(a,3)$	$(a,4)$	$(a,5)$
$\boldsymbol{b}$	$(b,2)$	$(b,2)$	$(b,3)$	$(b,4)$	$(b,5)$
$\boldsymbol{c}$	$(c,1)$	$(c,2)$	$(c,3)$	$(c,4)$	$(c,5)$

Hihutix: Je ne vois pas trop comment dresser une table avec nos menus du départ. Il faudrait un tableau en 3D.

Mathémator : On utilise plutôt dans ce cas un arbre :



Un menu est donc un triplet élément de $E \times P \times D$. On peut ensuite s'intéresser aux menus végétariens, aux menus sans viande, etc. Nous nous intéresserons par la suite à la manière de les compter.

Hihutix: Là c'est facile : il y a $3 \times 3 \times 3 = 27$ menus possibles. En fait, le $\times$ du produit cartésien marche comme le $\times$ de la multiplication des nombres.

Mathémator : Attention aux conclusions hâtives ! Il ne faut pas se fier aux apparences :

c'est en quoi la rigueur mathématique peut nous éviter certains désagrément, comme par exemple recevoir comme dessert des huîtres au lieu d'un pomme.

En effet, un élément de $E \times F$ en reprenant un exemple précédent est constitué d'une lettre et d'un nombre alors qu'un élément de $F \times E$ est constitué d'un nombre suivi d'une lettre, ce qui n'est pas la même chose.

Cela peut aussi avoir des conséquences fâcheuses en informatique :

```
# let ens=['a';'b';'c'];;
val ens : char list = ['a'; 'b'; 'c']
# let tri=['a','b','c'];;
val tri : (char * char * char) list = [('a', 'b', 'c')]
# tri=ens;;
Characters 4-7:
  tri=ens;;
      ^^^
Error: This expression has type char list
       but an expression was expected of type (char * char * char) list
```

OCAML n'est pas content : `ens` est en effet une liste de caractères contenant trois éléments alors que `tri` est une liste de triplets de trois caractères ne contenant qu'un seul élément. Être trop imprécis sur le type d'objet utilisé peut créer de sérieux problèmes dans vos programmes...

Recherche

Le produit cartésien est-il associatif ?

Remarque 12

Si dans le produit cartésien $E_1 \times E_2 \times \cdots \times E_n$ l'un des ensembles est vide (est l'ensemble vide), le produit cartésien $E_1 \times E_2 \times \cdots \times E_n$ est l'ensemble vide.

3 9 Notion de cardinal

Mathémator : Le cardinal d'un ensemble, c'est en gros le nombre de ses éléments. La notion de cardinal est intimement liée à la notion de fonction et à l'ensemble $\mathbf{N}$ des entiers naturels que nous détaillerons plus tard. Nous nous contenterons dans un premier temps d'une approche intuitive. Le cardinal de E est indifféremment noté :

$$\operatorname{Card}(E) \text{ ou } |E| \text{ ou } \#E$$

Par exemple $|\varnothing| = 0$, cette notation ne devra bien sûr pas être confondue avec la valeur absolue d'un réel ou bien le module d'un nombre complexe. Quoi qu'il en soit, le contexte permettra généralement de lever l'ambiguïté.

Nous admettons les résulats suivants qui ne concernent que des ensembles **finis**[k] :

Propriétés 1 - 1

- Si $A \subseteq B$ alors $|A| \leqslant |B|$. Une conséquence intéressante est celle ci : si $A \subseteq B$ avec $|A| = |B|$ alors $A = B$.
- $|A - B| \leqslant |A|$.
- $|A \cup B| = |A| + |B| - |A \cap B|$
- **Si on a** $E_i \cap E_j = \emptyset$ **lorsque** $i \neq j$, alors $\left|\bigcup\limits_{i=1}^{n} E_i\right| = \sum\limits_{i=1}^{n} |E_i|$.
- $|E_1 \times E_2| = |E_1|.|E_2|$ et

$$\begin{aligned} |E_1 \times E_2 \times \cdots \times E_n| &= |E_1|.|E_2|.\cdots.|E_n| \\ |E^n| &= (|E|)^n \end{aligned}$$

- La formule suivante est absolument à connaître :

$$|\mathcal{P}(E)| = 2^{|E|}$$

  Nous la démontrerons en exercice.

k. Des démonstrations seront proposées à la section 1.10 page 102

4 Calcul booléen

4 1 Présentation

Le Britannique George BOOLE (1815 - 1864) publie en 1854 *An Investigation Into the Laws of Thought, on Which are Founded the Mathematical Theories of Logic and Probabilities* qui, comme son nom l'indique, tente de traduire en équations mathématiques des idées et concepts. Les applications de ses travaux ont été innombrables, tant dans le domaine de l'informatique que dans ceux de l'électronique, de la téléphonie, des probabilités.
Il y a de nombreuses manière d'introduire le calcul booléen. Nous partirons de ce que nous connaissons, à savoir la théorie naïve des ensembles.
Le calcul booléen nous permettra dans un premier temps de calculer avec des ensembles. Nous allons créer une « correspondance » entre $\mathcal{P}(\mathrm{E})$ et un ensemble que nous noterons $\mathcal{B}$.

(En mathématiques, nous parlons d'*isomorphisme*. Puisque vous avez étudié le Grec ancien, vous avez reconnu les racines $\iota\sigma o\varsigma$ qui signifie « le même » et μορφος qui signifie « le corps »...).

4 2 Algèbre de Boole

4 2 1 Correspondance avec les parties d'un ensemble

Donnons nous un ensemble tout à fait quelconque E, mais distinct de l'ensemble vide. Nous allons travailler avec les éléments de $\mathcal{P}(\mathrm{E})$ dont nous distinguons tout de suite deux éléments particuliers $\varnothing$ et E. Nous avons à notre disposition deux opérations binaires qui sont l'union et l'intersection, une opération unaire qui est la complémentation (le complémentaire dans E) ainsi qu'une relation d'ordre qui est l'inclusion (large). Nous résumons ces données par :

$$\left(\mathcal{P}(\mathrm{E}), \cup, \cap, \complement_{\mathrm{E}}, \subseteq, \varnothing, \mathrm{E}\right)$$

Nous décidons maintenant de changer les notations pour qu'elles deviennent plus universelles, plus pratiques et donc plus automatiques.

Voici le dictionnaire des notations qui est en vigueur dans tous les ouvrages et chez tous les utilisateurs de l'algèbre de Boole (les informaticiens, les logiciens, les électriciens et électroniciens, les théoriciens des graphes et des probabilités, etc. Le résultat est appelé algèbre de Boole.

Ainsi $\mathcal{P}$ (E) est noté $\mathcal{B}$; usuellement les éléments de $\mathcal{P}$ (E) sont notés par des lettres majuscules A, B, ..., et les éléments de $\mathcal{B}$ par les lettres minuscules correspondantes (ce n'est pas du tout obligatoire) $a, b, \ldots$.

$\mathcal{P}(\mathrm{E})$	$\mathcal{B}$
A, B, $\cdots$, sont des éléments	a, b, $\cdots$, sont des éléments
$\varnothing$	0
E	1
$\mathrm{A} \cup \mathrm{B}$	$a + b$ (ou $a \vee b$)
$\mathrm{A} \cap \mathrm{B}$	$a.b$ (ou ab ou $a \wedge b$)
$\complement_{\mathrm{E}}\mathrm{A} = \overline{\mathrm{A}}$	$\overline{a}$
$\subseteq$	$\leqslant$

Correspondance entre $\mathcal{P}(\mathrm{E})$ et $\mathcal{B}$

Les propriétés dans $\mathcal{B}$ se déduisent alors sans difficulté en traduisant les résultats connus dans $\mathcal{P}(\mathrm{E})$ à l'aide de ces nouvelles notations. Pour avoir un résultat dans $\mathcal{B}$, il suffit d'écrire une égalité dans $\mathcal{P}(\mathrm{E})$ et de la traduire dans $\mathcal{B}$ à l'aide du dictionnaire. Prenons un exemple : $\mathrm{A} \cup (\mathrm{A} \cap \mathrm{B}) = \mathrm{A}$, c'est un résultat connu. Traduisons-le dans $\mathcal{B}$: $a + (a.b) = a$; ce résultat, qui du premier abord ne paraît pas naturel, peut se vérifier en le « retraduisant » dans $\mathcal{P}(\mathrm{E})$.

Nous allons réécrire un certain nombre de résultats classiques dans $\mathcal{P}(\mathrm{E})$ et les traduire dans $\mathcal{B}$; il faut bien comprendre qu'on ne crée rien de nouveau, on ne fait que changer de notations et, si au début cela peut être perturbant, à l'usage on se rendra compte que ces nouvelles notations sont très pratiques car elles ont des applications concrètes. Si, lors de l'usage d'une propriété dans $\mathcal{B}$ on a le moindre doute, il suffira de la traduire dans $\mathcal{P}(\mathrm{E})$ pour s'assurer ou non de sa validité.

$\mathcal{P}(\mathrm{E})$	$\mathcal{B}$	$\mathcal{P}(\mathrm{E})$	$\mathcal{B}$
$\varnothing \cup \varnothing = \varnothing$	$0 + 0 = 0$	$\varnothing \cap \varnothing = \varnothing$	$0 \cdot 0 = 0$
$\mathrm{E} \cup \mathrm{E} = \mathrm{E}$	$1 + 1 = 1$	$\mathrm{E} \cap \mathrm{E} = \mathrm{E}$	$1 \cdot 1 = 1$
$\mathrm{A} \cup \varnothing = \mathrm{A}$	$a + 0 = a$	$\mathrm{A} \cap \varnothing = \varnothing$	$a \cdot 0 = 0$
$\mathrm{A} \cup \mathrm{E} = \mathrm{E}$	$a + 1 = 1$	$\mathrm{A} \cap \mathrm{E} = \mathrm{A}$	$a \cdot 1 = a$
$\mathrm{A} \cup \mathrm{A} = \mathrm{A}$	$a + a = a$	$\mathrm{A} \cap \mathrm{A} = \mathrm{A}$	$a \cdot a = a$
$\mathrm{A} \cup \overline{\mathrm{A}} = \mathrm{E}$	$a + \overline{a} = 1$	$\mathrm{A} \cap \overline{\mathrm{A}} = \varnothing$	$a \cdot \overline{a} = 0$

Correspondance entre $\mathcal{P}(\mathrm{E})$ et $\mathcal{B}$

$\mathcal{P}(\mathrm{E})$	$\mathcal{B}$
$\cup$ est associative	$+$ est associative
$\cup$ est commutative	$+$ est commutative
$\cap$ est associative	$\cdot$ est associative
$\cap$ est commutative	$\cdot$ est commutative
$\cap$ est distributive pour $\cup$	$\begin{cases} a\cdot(b+c)=(a\cdot b)+(a\cdot c) \\ (b+c)\cdot a=(b\cdot a)+(c\cdot a)\end{cases}$
$\cup$ est distributive pour $\cap$	$\begin{cases} a+(b\cdot c)=(a+b)\cdot(a+c) \\ (b\cdot c)+a=(b+a)\cdot(c+a)\end{cases}$
$\overline{\overline{\mathrm{A}}}=\mathrm{A}$	$\overline{\overline{a}}=a$

Propriétés des calculs booléens et ensemblistes

Les lois de De Morgan se transformant en

$$\begin{cases} \overline{\bigcup_i \mathrm{A}_i}=\bigcap_i \overline{\mathrm{A}_i} \\ \overline{\bigcap_i \mathrm{A}_i}=\bigcup_i \overline{\mathrm{A}_i}\end{cases} \qquad \begin{cases} \overline{\sum_i a_i}=\prod_i \overline{a_i} \\ \overline{\prod_i a_i}=\sum_i \overline{a_i}\end{cases}$$

L'opération « + » est appelée *addition booléenne*, l'opération « · » est appelée *multiplication booléenne* et l'opération unaire qui transforme a en $\overline{a}$ est la *complémentation booléenne*.

Hihutix: Sauf votre respect, vous racontez n'importe quoi : $1+1=1$!!!??? Où vous avez vu ça, vous ?!

Mathémator : Attention en effet à ne pas se laisser piéger par les notations. Nous travaillons sur $\mathcal{B}$ et les symboles + et 1 n'ont pas la même signification que dans $\mathbf{R}$. Pour plus de sûreté, on devrait écrire $+_{\mathcal{B}}$, $1_{\mathcal{B}}$, $+_{\mathbf{R}}$, $+_{\mathbf{N}}$, $1_{\mathbf{R}}$, $1_{\mathbf{N}}$, etc. mais ce serait fastidieux. Il faudra bien faire attention au contexte.

Certains langages forcent à différencier les symboles des différentes opérations selon l'ensemble dans lequel on travaille :

```
# 1 + 1 ;;
- : int = 2
# 1.5 + 2.3 ;;
Characters 0-3:
  1.5+2.3;;
  ^^^
Error: This expression has type float but an expression was expected of
    type
         int
# 1.5 +. 2.3 ;;
```

```
- : float = 3.8
# true + false ;;
Characters 0-4:
  true + false ;;
  ^^^^
Error: This expression has type bool but an expression was expected of type
         int
# true & false ;;
- : bool = false
```

Vous aurez remarqué que le « + » de OCAML est le symbole de l'addition des entiers, que « +. » est le symbole de l'addition des flottants, que « `true` » et « `false` » sont les symboles des éléments « 0 » et « 1 » de $\mathcal{B}$ et que « & » est le symbole de l'addition des booléens.

Mis à part les égalités « naturelles » qui n'ont pas besoin de mémorisation, il est très important de retenir celles qui le sont moins, à savoir :

- $a+a=a$
- $a \cdot a = aa = a$
- $a+1=1$
- $(a+b)\cdot(a+c) = (a+b)(a+c) = a+(bc) = a+bc$ car nous décidons d'utiliser la hiérarchie habituelle de ces opérations.
- $a + a \cdot b = a$ qui correspond à $\mathrm{A} \cup (\mathrm{A} \cap \mathrm{B}) = \mathrm{A}$
- $a \cdot (a+b) = a$ qui correspond à $\mathrm{A} \cap (\mathrm{A} \cup \mathrm{B}) = \mathrm{A}$
- $a \cdot \overline{a} = 0$
- $a + \overline{a} = 1$

N'oublions pas la relation d'ordre, l'inclusion $\subseteq$ dans $\mathcal{P}(\mathrm{E})$ est notée $\leqslant$ dans $\mathcal{B}$:

$$a \leqslant b \iff a+b=b$$

$$a \leqslant b \iff a \cdot b = a$$

$$a \leqslant b \iff \overline{a} + b = 1$$

$$a \leqslant b \iff a \cdot \overline{b} = 0$$

Pour s'en souvenir il suffit de reprendre les propriétés caractéristiques de l'inclusion dans $\mathcal{P}(\mathrm{E})$, à savoir

$$\mathrm{A} \subseteq \mathrm{B} \iff \mathrm{A} \cup \mathrm{B} = \mathrm{B}$$

$$\mathrm{A} \subseteq \mathrm{B} \iff \mathrm{A} \cap \mathrm{B} = \mathrm{A}$$

$$\mathrm{A} \subseteq \mathrm{B} \iff \overline{\mathrm{A}} \cup \mathrm{B} = \mathrm{E}$$

$$\mathrm{A} \subseteq \mathrm{B} \iff \mathrm{A} \cap \overline{\mathrm{B}} = \varnothing$$

et on a toujours

$$0 \leqslant a \cdot b \leqslant a \leqslant a+b \leqslant 1$$

puisque ce n'est autre que la traduction de

$$\emptyset \subseteq \mathrm{A} \cap \mathrm{B} \subseteq \mathrm{A} \subseteq \mathrm{A} \cup \mathrm{B} \subseteq \mathrm{E}$$

Remarque 13

Nous n'avons pas introduit de symbole opératoire booléen pour la différence et la différence symétrique de deux ensembles car ces deux opérations, dans $\mathcal{P}(\mathrm{E})$, s'expriment l'aide de l'union, l'intersection et la complémentation :

$$\begin{aligned}
\mathrm{A} - \mathrm{B} &= \mathrm{A} \cap \overline{\mathrm{B}} \text{ se traduit en } a\overline{b} \\
\mathrm{A} \bigtriangleup \mathrm{B} &= (\mathrm{A} \cup \mathrm{B}) - (\mathrm{A} \cap \mathrm{B}) \text{ se traduit en} \\
(a+b)\cdot\overline{(a\cdot b)} &= (a+b)\cdot\left(\overline{a}+\overline{b}\right) = a\cdot\overline{b}+\overline{a}\cdot b
\end{aligned}$$

Une algèbre de Boole peut être définie algèbriquement à l'aide du système d'axiomes :

Définition 1 - 7

Algèbre de Boole

1. L'ensemble $\mathcal{B}$ est muni de deux opérations internes associatives et commutatives notées + et $\cdot$;
2. les deux lois sont distributives l'une par rapport à l'autre ;
3. $\mathcal{B}$ contient deux éléments 0 et 1, 0 étant élément neutre pour + et 1 étant élément neutre pour $\cdot$;
4. pour tout $a \in \mathcal{B}$ il existe un unique élément $\overline{a} \in \mathcal{B}$ tel que $a + \overline{a} = 1$ et $a \cdot \overline{a} = 0$.

De ces uniques axiomes découlent TOUTES les autres propriétés.

Remarque 14

Si E ne possède qu'un élément alors $\mathcal{P}(\mathrm{E})$ possède exactement deux éléments qui sont $\emptyset$ et E. L'algèbre de Boole associée ne possède donc que les éléments 0 et 1, c'est l'algèbre de Boole la plus utilisée. Elle est notée $\mathcal{B}_2$ et est appelée **algèbre de Boole binaire**.

4 2 2 Table

Pour vérifier ces propriétés, on peut dresser une table. Par exemple :

x	y	z	$y+z$	xy	xz	$x(y+z)$	$xy+xz$
1	1	1	1	1	1	1	1
1	1	0	1	1	0	1	1
1	0	1	1	0	1	1	1
1	0	0	0	0	0	0	0
0	1	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	0	1	1	0	0	0	0
0	0	0	0	0	0	0	0

Cela permet de vérifier que $x(y+z) = xy + xz$.

4 2 3 Dualité

La duale d'une expression booléenne s'obtient en échangeant les opérations $\cdot$ et $+$ ainsi que les nombres 0 et 1.

Par exemple, la duale de $x\cdot(y+0)$ est $x+(y\cdot 1)$.

Il faut retenir qu'une égalité reste vraie lorsqu'on prend les expressions duales des deux termes (pourquoi ?...pensez à $\overline{\cdots}$).

Par exemple, $x\cdot(x+y) = x$ (propriété d'absorption) est équivalente à $x+(x\cdot y) = x$ (également propriété d'absorption).

4 3 Fonctions booléennes

Une **fonction booléenne** de n variables est une **application** de $\mathcal{B}_2^n$ dans $\mathcal{B}_2$. Le cardinal de $\mathcal{A}\left(\mathcal{B}_2^n, \mathcal{B}_2\right)$ étant 2^{2^n}, il existe donc 2^{2^n} fonctions booléennes de n variables. Notons f une fonction booléenne de n variables, f est complètement déterminée par l'ensemble des images des éléments de $\mathcal{B}_2^n$ et on appelle support de f l'ensemble des éléments de $\mathcal{B}_2^n$ qui ont pour image 1. Nous notons $\mathrm{S}_n\left(f\right)$ le support de f :

$$\mathrm{S}_n\left(f\right) = \left\{b \in \mathcal{B}_2^n \mid f(b) = 1\right\}$$

Par exemple, il y a $2^{2^2} = 16$ fonctions booléennes de deux variables. Compléter ce tableau :

x	y	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
0	0											1					
0	1											0					
1	0											1					
1	1											0					

Six de ces fonctions joueront un rôle spécial que nous explorerons au moment d'étudier les portes logiques.

Le support de f_{10} est $S_2(f_{10}) = \{(0,0),(1,0)\}$.

Définition 1 - 8

On appelle **littéral positif** une variable booléenne écrite sous la forme x_i et **littéral négatif** une variable booléenne de la forme $\overline{x_i}$. On appelle **monôme booléen** tout produit de littéraux, un même littéral n'apparaissant pas deux fois.

$\overline{x_1}\cdot\overline{x_2}\cdot x_3$, $x_1\cdot x_2\cdot\overline{x_3}$ et $\overline{x_2}\cdot x_3$ sont des monômes, l'ordre dans lequel sont écrites les variables n'ayant aucune importance. Par contre $x_1\cdot x_2.\overline{x_1}$ n'est pas un monôme, $x_1\cdot\overline{x_1}$ étant égal à 0, nous avons $x_1\cdot x_2\cdot\overline{x_1} = 0$.

Définition 1 - 9

Si m est un monôme, nous dirons que le monôme m_1 est un **diviseur** de m si m peut s'écrire $m = m_1\cdot m_2$, m_2 étant un monôme ou le booléen 1.

$\overline{x_1}\cdot\overline{x_2}$, $\overline{x_1}\cdot x_3$, $\overline{x_2}$ et $\overline{x_1}\cdot\overline{x_2}\cdot x_3$ sont des diviseurs de $\overline{x_1}\cdot\overline{x_2}\cdot x_3$.

Définition 1 - 10

On appelle **polynôme booléen** une somme de monômes.

Par exemple $\overline{x_1}\cdot\overline{x_2}\cdot x_3 + x_1\cdot\overline{x_2}\cdot x_3 + x_1\cdot x_2\cdot\overline{x_3}$ ou $\overline{x_1} + x_2 + x_1\cdot x_3$.

Définition 1 - 11

Dans ce qui suit f est une fonction booléenne de n variables et nous notons f pour $f(x_1, x_2, \cdots, x_n)$. On dit que f est

- Un **p-terme** ou monôme booléen si $f = \prod_{j\in J\subseteq\mathbb{N}_n} y_j$ avec $y_j \in \left\{x_j, \overline{x_j}\right\}$. Un p-terme est **complet** si, et seulement si, $J = \mathbb{N}_n$, cela signifie que toutes les variables figurent dans le monôme. Un p-terme complet est appelé un **minterme**.
- Un **s-terme** ou clause booléenne si $f = \sum_{j\in J\subseteq\mathbb{N}_n} y_j$ avec $y_j \in \left\{x_j, \overline{x_j}\right\}$. Un s-terme est complet si, et seulement si, $J = \mathbb{N}_n$, un **s-terme complet** est appelé un **maxterme.**
- **Disjonctive** si f est une somme de p-termes.
- **Disjonctive canonique** si f est une somme de mintermes.
- **Conjonctive** si f est un produit de s-termes.
- **Conjonctive canonique** si f est un produit de maxtermes.

Des petits exemples avec des fonctions de trois variables pour mettre en pratique :

$f_1 = \overline{x_1}\cdot\overline{x_2} + x_1 + x_2\cdot\overline{x_3}$ est une forme disjonctive,

$f_2 = \overline{x_1}\cdot\overline{x_2}\cdot x_3 + x_1\cdot\overline{x_2}\cdot x_3 + x_1\cdot x_2\cdot\overline{x_3}$ est une forme disjonctive canonique,

$f_3 = \left(\overline{x_1} + \overline{x_2}\right)\cdot(x_3 + x_1)\cdot x_3$ est une forme conjonctive,

$f_4 = \left(\overline{x_1} + \overline{x_2} + x_3\right)\cdot\left(x_1 + \overline{x_2} + x_3\right)$ est une forme conjonctive canonique.

Nous verrons par la suite qu'il sera très important de déterminer les formes canoniques disjonctives et conjonctives.

Il est important de remarquer qu'un minterme vaut 1 pour une combinaison de ses variables et une seulement : il faut que tous les littéraux valent 1 en même temps.

Par exemple, $\overline{x_1}x_2\overline{x_3}x_4x_5$ vaut 1 si, et seulement si, $x_1 = x_3 = 0$ et $x_2 = x_4 = x_5 = 1$.

On peut montrer (mais on peut l'admettre en première lecture) que toute expression booléenne peut s'écrire sous la forme d'une somme de mintermes différents qui ne peuvent donc, d'après la remarque précédente, valoir 1 que dans un seul cas et comme ils sont tous distincts, quand un minterme vaut 1, les autres valent 0.

Comme 1 + n'importe quoi vaut toujours 1, on peut écrire une fonction booléenne sous la forme d'une somme de mintermes.

Un tableau (qu'on appellera table canonique) permet d'obtenir facilement ces mintermes.

Considérons la fonction booléenne de 3 variables : $f = f(x_1, x_2, x_3) = (x_1 + x_2)\,\overline{x_3}$

x_1	x_2	x_3	x_1+x_2	$\overline{x_3}$	$(x_1+x_2)\overline{x_3}$
1	1	1			
1	1	0			
1	0	1			
1	0	0			
0	1	1			
0	1	0			
0	0	1			
0	0	0			

Nous en déduisons que $f(x_1,x_2,x_3) = x_1x_2\overline{x_3} + x_1\overline{x_2x_3} + \overline{x_1}x_2\overline{x_3}$.

On aurait pu y arriver par le calcul :

$$\begin{array}{rcll} f(x_1,x_2,x_3) & = & (x_1+x_2)\overline{x_3} & \\ & = & x_1\overline{x_3}+x_2\overline{x_3} & \text{distributivité} \\ & = & x_1 1\overline{x_3}+x_2 1\overline{x_3} & \\ & = & x_1(x_2+\overline{x_2})\overline{x_3}+(x_1+\overline{x_1})x_2\overline{x_3} & \\ & = & x_1x_2\overline{x_3}+x_1\overline{x_2x_3}+x_1x_2\overline{x_3}+\overline{x_1}x_2\overline{x_3} & \text{distributivité} \\ & = & x_1x_2\overline{x_3}+x_1\overline{x_2x_3}+\overline{x_1}x_2\overline{x_3} & \text{idempotence} \end{array}$$

Pour obtenir la forme canonique conjonctive, on utilise le fait que $\overline{x+y} = \overline{x}\cdot\overline{y}$.

C'est facile car $\overline{f} = 0 \Leftrightarrow f = 1$ et $\overline{f} = 1 \Leftrightarrow f = 0$.

Ainsi $f = x_1x_2x_3 + x_1\overline{x_2}x_3 + \overline{x_1}x_2x_3 + \overline{x_1x_2}x_3 + \overline{x_1} + \overline{x_2} + \overline{x_3}$.

Ensuite, $f = \overline{\overline{f}} = \overline{x_1x_2x_3 + x_1\overline{x_2}x_3 + \overline{x_1}x_2x_3 + \overline{x_1x_2}x_3 + \overline{x_1x_2x_3}}$.

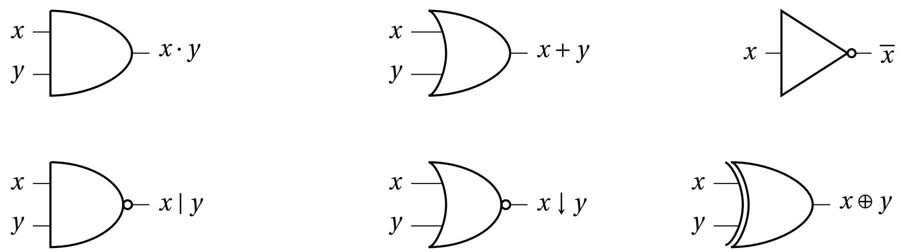
Finalement, $f = \left(\overline{x_1}+\overline{x_2}+\overline{x_3}\right)\left(\overline{x_1}+x_2+\overline{x_3}\right)\left(x_1+\overline{x_2}+\overline{x_3}\right)\left(x_1+x_2+\overline{x_3}\right)(x_1+x_2+x_3)$.

Ces écritures ne sont pas toujours minimales mais nous seront utiles pour étudier les portes logiques.

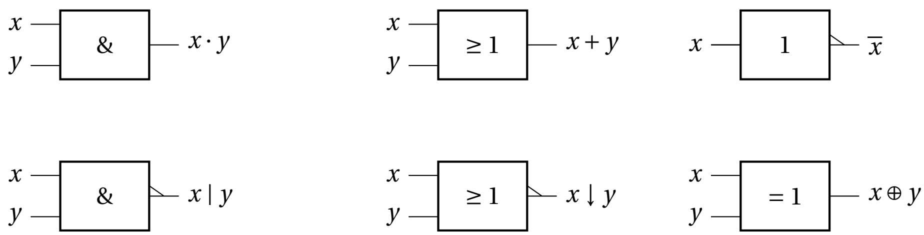
4 4 Portes logiques

L'informatique, concrètement, c'est au départ des circuits électroniques : ça passe ou ça ne passe pas. Les calculs dans une algèbre de Boole sont donc tout à fait adaptés. On trouve dans le commerce des composants électroniques modélisant les fonctions NON, OR, AND et également NOR, NAND, XOR que nous avons étudiées en exercice.

Voici leur représentation à la mode américaine :

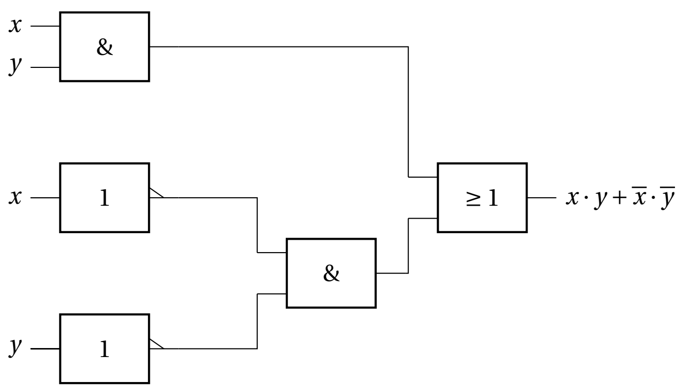


et à la mode européenne :



L'Europe, c'est mieux, alors on adoptera la deuxième série de représentations.

Construisons par exemple un circuit correspondant à la fonction $f(x, y) = x \cdot y + \overline{x} \cdot \overline{y}$:



4 5 Minimisation de circuits

Construisez les circuits correspondant à $xyz + x\overline{y}z$ et xz. Des remarques ?

Pouvoir placer un maximum de circuit sur un même chip est une tâche importante. Pour cela, il faut que les circuit soient les plus petits possibles tout en effectuant les tâches requises.

C'est un problème qui peut devenir compliqué et même actuellement, on a du mal à mettre au point des algorithmes traitant des expressions booléennes dépassant 25 littéraux.

Nous ne verrons que des cas simples avec une méthode graphique : le diagramme de KARNAUGH.

Il existe entre autre la méthode de QUINE-MCCLUSKEY qui permet d'être automatisée sur machine mais dont la complexité est exponentielle.

4 5 1 2 variables

On suppose qu'on dispose d'une fonction de deux variables sous forme disjonctive canonique.

Les quatre littéraux possibles sont regroupés dans un tableau :

f (x \ y)	0	1
0	$\overline{x}\,\overline{y}$	$\overline{x}y$
1	$x\overline{y}$	xy

Ensuite, on met des 1 quand le littéral est présent et un zéro (ou rien) sinon.

Par exemple, pour $xy + \overline{x}y$ on obtient :

f (x \ y)	0	1
0		1
1		1

On repère ensuite les cellules de 1 adjacentes qui vont permettre un regroupement.

Dans le cas présent, $f(x, y) = y\left(\overline{x} + x\right) = y$.

Il est peu utile dans ce cas de recourir à cette méthode.

4 5 2 3 variables

Ça devient plus intéressant à partir de 3 variables. Le but est de recouvrir le plus de 1 avec des blocs les plus grands possibles contenant un nombre de 1 égal à une puissance de 2. Plusieurs blocs peuvent se recouvrir.

Prenons par exemple $f(x,y,z) = x\overline{y}z + x\overline{y}\,\overline{z} + xyz + \overline{x}yz + \overline{x}\,\overline{y}\,\overline{z}$.

	f \ yz	00	01	11	10
x	0	1	0	1	0
	1	1	1	1	0

Alors $f(x,y,z) = \overline{y}\,\overline{z} + x\overline{y} + yz$.

Autre exemple : $f(x,y,z) = x\overline{y}z + x\overline{y}\,\overline{z} + \overline{x}yz + \overline{x}\,\overline{y}\,\overline{z} + \overline{x}\,\overline{y}z$.

	f \ yz	00	01	11	10
x	0	1	1	1	0
	1	1	1	0	0

Cette fois, $f(x,y,z) = \overline{y} + \overline{x}z$.

4.5.3 4 variables

Considérons le tableau suivant (écrivez l'expression booléenne correspondant...).

	f \ x_2x_3	00	01	11	10
x_0x_1	00	1	0	0	1
	01	0	0	1	1
	11	0	0	1	1
	10	1	1	0	1

On obtient $f(x_0,x_1,x_2,x_3) = x_1x_2 + \overline{x_1}\,\overline{x_3} + x_0\overline{x_1}\,\overline{x_2}$

5 Un peu de calcul matriciel

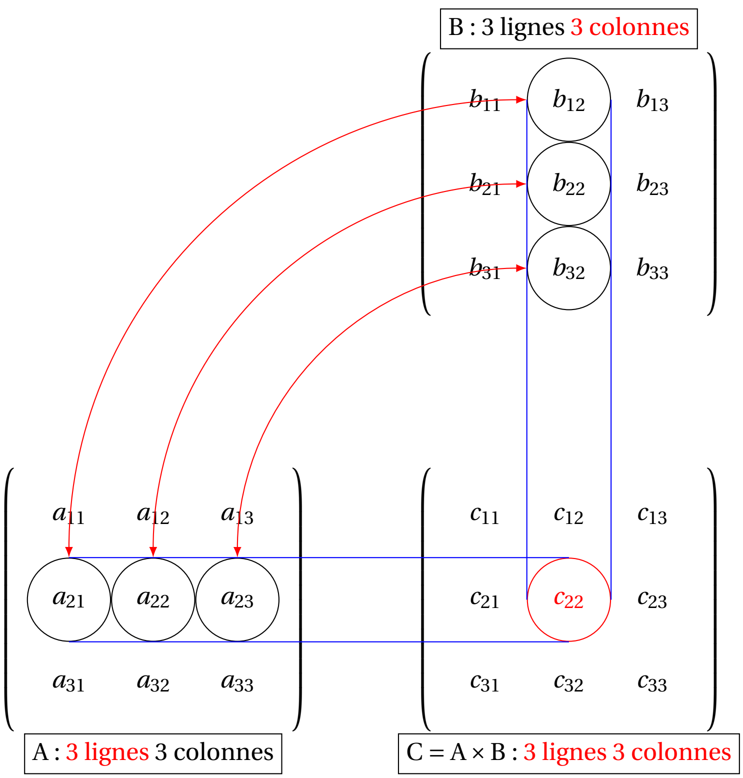
5 1 Produit de matrices

Nous aurons besoin de multiplier des matrices entre elles. Voici une disposition pratique pour effectuer les calculs.

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$$

avec n le nombre de colonnes de A qui doit être égal au nombre de lignes de B.

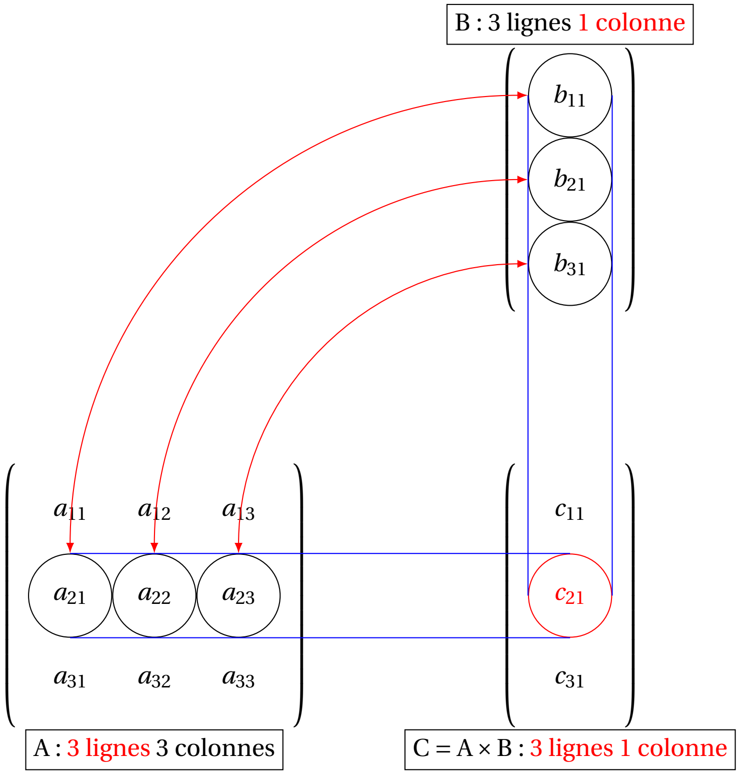
5 1 1 Produit de deux matrices « carré »



Danger

produit de matrice non commutatif
Le produit de deux matrices n'est pas commutatif. Cela signifie qu'en général $A \times B \neq B \times A$.

5 1 2 Produit d'une matrice « carré » et d'une matrice « colonne »



5 2 Matrices et Python : approche naïve

5 2 1 Création d'une matrice

Nous créerons nos matrices comme une liste de listes représentant les lignes.

Par exemple, $\begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}$ sera rentré avec :

```
M=[[1,2],[3,4],[5,6]]
```

Comment faire calculer le nombre de lignes et le nombre de colonnes de **M** à Python ?

5 2 2 Somme de matrices

Créez une procédure qui prend comme arguments deux matrices et renvoie leur somme.
Elle commencera par :

```
def somm(A,B):
   C=[[0 for k in len(A[1])] for k in len(A)]
           ?...?
   return(C);
```

5.2.3 Produit de matrices

Soit $\mathrm{A} = (a_{ij})_{\substack{1\leqslant i\leqslant n\\ 1\leqslant i\leqslant m}}$ et $\mathrm{B} = (b_{ij})_{\substack{1\leqslant i\leqslant m\\ 1\leqslant i\leqslant p}}$.

Alors $\mathrm{A}\times\mathrm{B} = \mathrm{C}$ avec $\mathrm{C} = (c_{ij})_{\substack{1\leqslant i\leqslant n\\ 1\leqslant i\leqslant p}}$ et

$$\forall (i,j)\in \mathbb{N}_n^*\times\mathbb{N}_p^*,\quad c_{ij} = \sum_{k=1}^{m} a_{ik}\cdot b_{kj}$$

Créez alors une procédure qui prend comme arguments deux matrices et renvoie leur produit.

5.2.4 Matrice identité

Créer une procédure `Id(n)` qui crée la matrice identité d'ordre n.

5.2.5 Puissances d'une matrice

Tout est dans le titre...

5.2.6 Trace d'une matrice

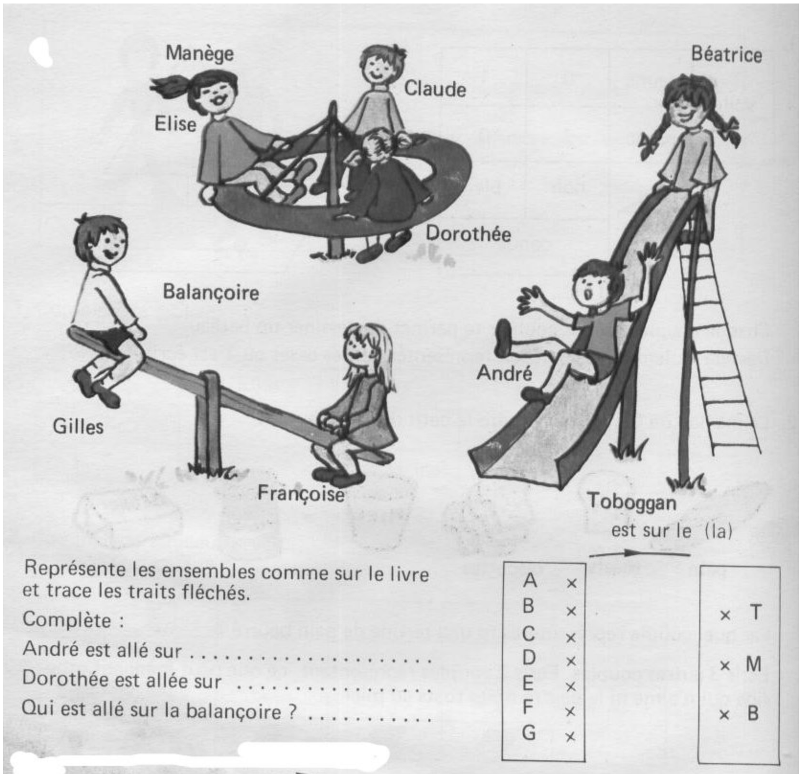
On calcule la somme des éléments diagonaux.

5.2.7 Transposée d'une matrice, matrices orthogonales

On échange lignes et colonnes.

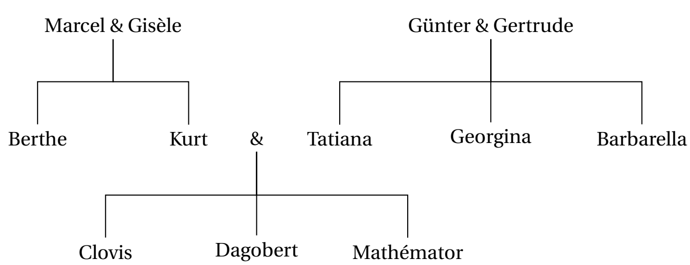
6 Relations binaires

6 1 Au CE1



6 2 Généalogie

Mathémator : Voici mon arbre généalogique :



Formez les couples (x, y) tels que x soit le grand-père de y.

Hihutix: Ben il y a (Marcel,Clovis), (Marcel,Dagobert), (Marcel, Mathémator), (Günter,Clovis), (Günter,Dagobert) et(Günter, Mathémator).

Mathémator : Voici un bel exemple de relation binaire...

6 3 À l'IUT

Mathémator :

Les relations nous entourent : dès que l'on conçoit des objets, objets matériels ou abstraits, on s'intéresse immédiatement aux relations qui peuvent exister entre ces objets, relation ayant, ici, son sens usuel. Nous allons « mathématiser » cette notion. Le vocabulaire et notations utilisés pourront parfois surprendre mais nous estimons que les mauvaises habitudes « françaises » sont sources de confusions et vont à l'encontre de la précision que l'on souhaite obtenir.

La définition d'une relation est excessivement simple :

Définition 1 - 12

Relation binaire
On appelle relation binaire de l'ensemble E vers (ou dans) l'ensemble F tout triplet $(\mathrm{E},\mathrm{F},\mathrm{G}_{\mathcal{R}})$ où $\mathrm{G}_{\mathcal{R}}$ est une partie de $\mathrm{E}\times\mathrm{F}$. Notons $\mathcal{R}$ (ou R ou f ou ...) ce triplet :

$$\mathcal{R} = (\mathrm{E},\mathrm{F},\mathrm{G}_{\mathcal{R}})$$

Hihutix: Ça serait quand même plus simple de dire qu'une relation, c'est un ensemble de couples.

Mathémator : C'est en effet l'idée. Il faut cependant être plus spécifique dans la pratique afin d'effectuer certaines opérations.

E est **l'ensemble de départ**[l] ou domaine[m] de départ de la relation $\mathcal{R}$, F est **l'ensemble d'arrivée** ou but ou cible de la relation $\mathcal{R}$, $\mathrm{G}_{\mathcal{R}}$ est **le graphe** de la relation $\mathcal{R}$ avec, il ne faut surtout pas l'oublier, $\mathrm{G}_{\mathcal{R}}\subseteq\mathrm{E}\times\mathrm{F}$. Les ensembles E et F étant définis, c'est alors $\mathrm{G}_{\mathcal{R}}$ qui détermine la relation $\mathcal{R}$, pour cela, on se permet de confondre, si besoin, la relation $\mathcal{R}$ avec son graphe $\mathrm{G}_{\mathcal{R}}$. La relation $\mathcal{R}$ de E vers F **est alors assimilée à un ensemble : une partie de E × F**.

Il faut bien comprendre que pour définir parfaitement la relation $\mathcal{R}$ il nous faut connaître trois éléments E, F et $\mathrm{G}_{\mathcal{R}}\subseteq\mathrm{E}\times\mathrm{F}$; si au moins l'un de ces trois éléments manque, la relation $\mathcal{R}$ n'est pas définie. Si $\mathrm{G}_{\mathcal{R}}=\emptyset$, $\mathcal{R}$ est la relation vide de E vers F, ce sera forcément le cas si E ou F est vide. L'ensemble des relations binaires de E vers (ou dans) F est noté $\mathrm{E}\longleftrightarrow\mathrm{F}$ ou $\mathrm{E}\leftrightarrow\mathrm{F}$ et est confondu, si besoin, avec $\mathcal{P}(\mathrm{E}\times\mathrm{F})$, l'ensemble des parties de E × F.

l. Aussi appelé source de la relation.
m. Il y a une querelle en France pour l'utilisation de ce mot car un domaine, en topologie, désigne un ensemble compact connexe. Les anglo-saxons utilisent "maximal domain" `pour domaine de départ.`

Les écritures $\mathcal{R} \in E \longleftrightarrow F$ ou $\mathcal{R} : E \longleftrightarrow F$ ou $\mathcal{R} \in \mathcal{P}(E \times F)$ doivent se traduire par « $\mathcal{R}$ est une relation binaire de E vers F ». Si E = F on dit que $\mathcal{R}$ est une relation binaire de E vers E ou de E dans E ou encore une relation binaire **sur** E.

Si $(x, y) \in G_{\mathcal{R}}$, on dit que l'élément x de l'ensemble de départ E est en relation par $\mathcal{R}$ avec l'élément y de l'ensemble d'arrivée F. L'écriture $x\mathcal{R}y$ ou $\mathcal{R}\left(x, y\right)$ [n] est équivalente à $(x, y) \in G_{\mathcal{R}}$ ou $(x, y) \in \mathcal{R}$ puisque l'on se permet de confondre $\mathcal{R}$ et $G_{\mathcal{R}}$:

$$x\mathcal{R}y \Leftrightarrow \mathcal{R}\left(x, y\right) \Leftrightarrow (x, y) \in G_{\mathcal{R}} \Leftrightarrow \left(x, y\right) \in \mathcal{R}$$

et on dit que y est **une** image de x par la relation $\mathcal{R}$ et que x est **un** antécédent de y. Si $(x, y) \notin G_{\mathcal{R}}$, x n'est pas en relation avec y.

Remarque 15 Le couple $\left(x, y\right)$ de $G_{\mathcal{R}}$ est aussi noté $x \mapsto y$, c'est une notation de la méthode B.

Hihutix: Euh...je préfère la présentation CE1...

Mathémator : Revenons-y si vous le désirez.

La relation $\mathcal{R}$ est définie par « est sur le (la) » avec un ensemble de départ qui est en fait l'ensemble des élèves :

$$E = \left\{a, b, c, d, e, f, g\right\}$$

et un ensemble d'arrivée qui est en fait l'ensemble des jeux :

$$J = \left\{T, M, B\right\}$$

Son graphe est :

$$G_{\mathcal{R}} = \left\{(a, T), (b, T), (c, M), (d, M), (e, M), (f, B), (g, B)\right\}$$

Les écritures suivantes sont équivalentes :

$$(a, T) \in G_{\mathcal{R}} \Longleftrightarrow a\,\mathcal{R}\,T \Longleftrightarrow (a, T) \in \mathcal{R}$$

n. Cette notation, $\mathcal{R}\left(x, y\right)$, est appelée « écriture prédicative ».

Remarque 16

Posons-nous la question « combien existe-t-il de relations (binaires) de E vers F » ? Nous venons de dire que, les ensembles E et F étant précisés, la relation est déterminée par son graphe qui est une partie de $E \times F$. Il y a donc autant de relations de E vers F que de parties dans $E \times F$, c'est à dire $2^{|E\times F|}$.
Si, par exemple E a 30 éléments et F a 10 éléments, alors il existe 2^{300} relations de E vers F ($2^{300} \approx 2.10^{90}$ et le nombre d'atomes estimé dans tout l'univers est 10^{77} ! ! !).

6 4 Domaine, codomaine

L'ensemble des éléments de E qui ont au moins une image par $\mathcal{R}$ est l'ensemble de définition ou **domaine** de définition de la relation $\mathcal{R}$ que l'on note le plus souvent par $\mathcal{D}_{\mathcal{R}}$ ou $\mathrm{dom}(\mathcal{R})$. Remarquons que l'on a forcément $\mathrm{dom}(\mathcal{R}) \subseteq E$.

$$\mathrm{dom}(\mathcal{R}) = \left\{x \in E \mid \text{il existe au moins } y \in F \text{ avec } x\mathcal{R}y\right\}$$

Si on est sûr que $\mathrm{dom}(\mathcal{R}) = E$, c'est-à-dire que tout élément de l'ensemble de départ a au moins une image, on dit que la relation $\mathcal{R}$ est **totale** ou partout définie. Dans le cas contraire, on dit qu'elle est non totale et c'est là que les ennuis commencent car on trouve dans la littérature le qualificatif de partiel. Que ce soit clair, si une relation $\mathcal{R}$ est qualifiée de partielle, c'est qu'on ne sait pas, au moment où on cherche à la définir, si elle est totale ou non ou qu'elle n'est pas forcément totale. En conséquence une relation partielle peut très bien être une relation totale et on peut conclure en affirmant que l'adjectif « partiel » ne sert à rien d'autre que de dire qu'on ne sait pas si elle est totale. Pour éviter des confusions fâcheuses, nous conseillons donc, lors de l'utilisation de l'adjectif *partiel,* de bien préciser le sens qu'on lui attribue. Nous retiendrons de ces commentaires que parmi les relations, certaines sont totales et d'autres non !

L'ensemble des éléments de F qui ont au moins un antécédent dans E est appelé l'image de $\mathcal{R}$ ou l'image de E par $\mathcal{R}$ ou le **codomaine** de $\mathcal{R}$. On utilise indifféremment les notations suivantes pour désigner le codomaine de $\mathcal{R}$

$$\mathrm{Im}\,\mathcal{R} \text{ ou } \mathrm{Im}(\mathcal{R}) \text{ ou } \mathrm{Ran}(\mathcal{R}) \text{ ou } \mathrm{codom}(\mathcal{R})$$

$\mathrm{Im}(\mathcal{R})$ se lisant « im de $\mathcal{R}$ » ou « image de $\mathcal{R}$ », la notation $\mathrm{Ran}(\mathcal{R})$ venant de l'anglais « range » (cible en français). Il faut tout de suite remarquer que $\mathrm{Im}(\mathcal{R})$ n'est autre que l'ensemble de toutes les images des éléments de E par la relation $\mathcal{R}$

$$\mathrm{Im}(\mathcal{R}) = \left\{y \in F \mid \text{il exite au moins } x \in E \text{ avec } x\mathcal{R}y\right\}$$

et que l'on a forcément $\mathrm{Im}(\mathcal{R}) \subseteq F$.

6 5 Représentation d'une relation

Lorsque E et F sont finis on a forcément $G_{\mathcal{R}} \subseteq E \times F$ qui est fini et on peut représenter la relation $\mathcal{R}$ ou son graphe $G_{\mathcal{R}}$ de différentes manières. En voici quelques exemples.

6 5 1 Représentation linéaire ensembliste

Prenons pour $\mathrm{E} = \{a, b, c, d, e\}$, $\mathrm{F} = \{\alpha, \beta, \gamma, \delta\}$ et pour graphe :

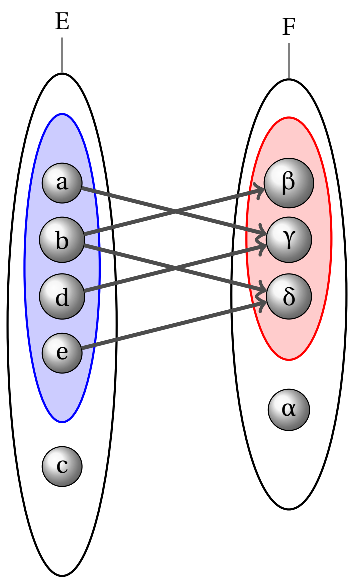
$$\mathrm{G}_{\mathcal{R}} = \{(a, \gamma), (b, \beta), (b, \delta), (d, \gamma), (e, \delta)\}$$

$\mathrm{G}_{\mathcal{R}}$ est aussi noté $\mathrm{G}_{\mathcal{R}} = \{a \mapsto \gamma, b \mapsto \beta, b \mapsto \delta, d \mapsto \gamma, e \mapsto \delta\}$.

Le domaine de $\mathcal{R}$ est $\operatorname{dom}(\mathcal{R}) = \{a, b, d, e\}$, c'est l'ensemble constitué des éléments de E qui ont au moins une image dans F. Le codomaine de $\mathcal{R}$ est $\operatorname{codom}(\mathcal{R}) = \{\beta, \gamma, \delta\}$, c'est l'ensemble constitué des éléments de F qui ont au moins un antécédent ou encore l'ensemble des images des éléments de E par $\mathcal{R}$.

6 5 2 Représentation sagittale

Les ensembles E et F sont représentés par des « patates » et un élément x de E (un point de la patate E) est relié à un élément y de F par une flèche orientée de E vers F si, et seulemnt si, $x\mathcal{R}y$.



Relation non totale

Cette relation n'est pas totale car il y a au moins un élément de l'ensemble de départ E qui n'a pas d'image, en l'occurence c n'a pas d'image.

On visualise immédiatement $\operatorname{dom}(\mathcal{R}) = \{a, b, d, e\}$ et $\operatorname{Im}(\mathcal{R}) = \operatorname{codom}(\mathcal{R}) = \operatorname{Ran}(\mathcal{R}) = \{\beta, \gamma, \delta\}$.

6 5 3 Table relationnelle

C'est la même chose sous forme de tableau :

De	Vers
a	γ
b	β
b	δ
d	γ
e	δ

6 5 4 Dictionnaire

La même chose en plus ramassé :

De	Vers
a	γ
b	β,δ
d	γ
e	δ

6 5 5 Représentation matricielle

Si les ensembles E et F sont définis par :

$$\mathrm{E} = \{x_1, x_2, \cdots, x_n\} \qquad \mathrm{F} = \{y_1, y_2, \cdots, y_p\}$$

alors la relation $\mathcal{R}$ est définie par la matrice [o] $\mathrm{R} = (r_{i,j}) \in \mathfrak{M}_{n,p}$ définie par :

$$\mathrm{R} = \begin{pmatrix} r_{1,1} & \cdots & r_{1,j} & \cdots & \cdots & r_{1,p} \\ \vdots & & \vdots & & & \vdots \\ r_{i,1} & & r_{i,j} & & & r_{i,p} \\ \vdots & & \vdots & & & \vdots \\ r_{n,1} & \cdots & r_{n,j} & \cdots & \cdots & r_{n,p} \end{pmatrix} \text{ avec } r_{i,j} = \begin{cases} 1 \text{ si } x_i \mathcal{R} y_j \\ 0 \text{ sinon} \end{cases}$$

o. Ceux qui ne savent pas encore ce qu'est une matrice (ce doit être le cas de la majorité d'entre vous) le découvriront avec le module Algèbre et Analyse 1, il suffit de savoir ici qu'une matrice est tout simplement un tableau de « nombres ».

$r_{i,j}$ étant l'élément se trouvant sur la $i^{ème}$ ligne et $j^{ème}$ colonne, les lignes étant numérotées du haut vers le bas et les colonnes de la gauche vers la droite. La matrice R est appelée la matrice d'adjacence ou d'incidence de la relation $\mathcal{R}$.

Si l'on reprend l'exemple précédent, il nous faut décider d'ordonner les éléments de E et de F et, pour s'assurer que celui qui va nous lire ne fera pas de confusions, il faut s'obliger à faire figurer les éléments à côté de la matrice d'autant plus que certains utilisateurs peuvent très bien décider d'un autre placement pour les éléments de E et de F puisque les éléments de E et de F ne sont pas indicés :

$\curvearrowright$	α	β	γ	δ
a	**0**	**0**	**1**	**0**
b	**0**	**1**	**0**	**1**
c	**0**	**0**	**0**	**0**
d	**0**	**0**	**1**	**0**
e	**0**	**0**	**0**	**1**

Mais bon, généralement, on place en ligne les élément de départ et en colonne les élément d'arrivée donc on peut se contenter de la matrice :

$$\mathrm{R} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

mais il faut être sûr de ce que l'on fait.

6 6 Relation réciproque

La **relation réciproque** de la relation $\mathcal{R} = (\mathrm{E}, \mathrm{F}, \mathrm{G}_{\mathcal{R}})$ est la relation notée $\mathcal{R}^{-1}$ définie par $\mathcal{R}^{-1} = (\mathrm{F}, \mathrm{E}, \mathrm{G}_{\mathcal{R}^{-1}})$ avec $\mathrm{G}_{\mathcal{R}^{-1}} = \left\{(y,x) \in \mathrm{F}\times\mathrm{E} \mid (x,y) \in \mathrm{G}_{\mathcal{R}}\right\}$, c'est-à-dire $y\mathcal{R}^{-1}x \Leftrightarrow x\mathcal{R}y$.

Pour obtenir la représentation sagittale de $\mathcal{R}^{-1}$, il suffit de modifier le sens des flèches de la représentation sagittale de $\mathcal{R}$.

Pour aller plus loin

Si R est la matrice de $\mathcal{R}$ alors ${}^t\mathrm{R}$, la transposée de R, est la matrice de $\mathcal{R}^{-1}$, c'est-à-dire la matrice obtenue en inversant les lignes et les colonnes, ce qui est assez logique compte tenu de notre définition de la représentation matricielle.
En reprenant l'exemple précédent :

$$\mathrm{R} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad {}^t\mathrm{R} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Les résultats suivants découlent immédiatement de la définition :

- $\mathrm{dom}(\mathcal{R}) = \mathrm{Im}(\mathcal{R}^{-1}) = \mathrm{Ran}(\mathcal{R}^{-1})$
- $\mathrm{dom}\left(\mathcal{R}^{-1}\right) = \mathrm{Im}(\mathcal{R}) = \mathrm{Ran}(\mathcal{R})$
- $\left(\mathcal{R}^{-1}\right)^{-1} = \mathcal{R}$

Hihutix: Tout ceci est bien abstrait !...

Mathémator : Un petit exemple alors...Considérons les ensembles et la relation suivants :

- Étudiants= $\{$Roger, Berthe, Jean-Pierre, Gudrun$\}$;
- Chaînes= $\{$ TF1, Gulli, Zen TV$\}$;
- TV= $\{$Roger $\mapsto$ Gulli, Berthe $\mapsto$ Gulli, Jean-Pierre $\mapsto$ Zen TV, Gudrun $\mapsto$ Gulli$\}$.

Ainsi la relation TV $\in$ Étudiants $\longleftrightarrow$ Chaîne peut s'interpréter en « ... regarde ... ».

Que pensez-vous de la relation réciproque ?

Hihutix: Ben c'est $\mathrm{TV}^{-1} \in$ Chaîne $\longleftrightarrow$ Étudiants qui peut s'interpréter en « ...est regardée par... ».

Ça revient quand même à peu près au même.

Mathémator : « En gros » peut-être mais nous travaillerons plus finement...

6 7 Image, contre image, image réciproque d'une partie

Si U est une partie de E, $\mathcal{R}(\mathrm{U})$ ou $\mathcal{R}\langle\mathrm{U}\rangle$ désigne l'ensemble des images des éléments de U par $\mathcal{R}$. Si U est vide ou si $\mathrm{U} \cap \mathcal{D}_{\mathcal{R}} = \emptyset$, $\mathcal{R}(\mathrm{U})$ est vide et il est clair que $\mathcal{R}(\mathrm{E}) = \mathrm{Im}(\mathcal{R}) = \mathrm{Ran}(\mathcal{R})$.

Remarque 17

Si U n'est pas une partie de E, $\mathcal{R}(\mathrm{U})$ n'a pas de sens ! Ce doit être clair et c'est absolument à retenir.

Si V est une partie de F, la contre image (ou l'image réciproque) de V par $\mathcal{R}$ est l'image de V par $\mathcal{R}^{-1}$. Elle est donc notée $\mathcal{R}^{-1}(\mathrm{V})$ ou bien $\mathcal{R}^{-1}\langle \mathrm{V}\rangle$, elle est vide si V est vide ou si $\mathrm{V}\cap \mathrm{Im}(\mathcal{R}) = \varnothing$. On pourra remarquer que $\mathcal{R}^{-1}(\mathrm{F}) = \mathrm{dom}\,\mathcal{R}$.

La relation $\mathcal{R}$ définie par son diagramme sagittal :

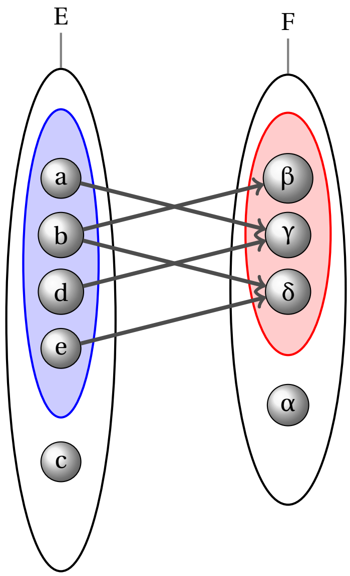


Image et contre-image

Nous avons $\mathcal{R}(\{a,b\}) = \{\beta,\gamma\}, \mathcal{R}(\{c\}) = \{\gamma\}, \mathcal{R}^{-1}(\{\alpha\}) = \varnothing, \mathcal{R}^{-1}(\{\gamma\}) = \{a,c,d\}$ mais aussi $\mathcal{R}(\varnothing) = \varnothing$ et $\mathcal{R}(\{a,\beta\})$ n'a pas de sens car $\{a,\beta\}$ n'est pas une partie de l'ensemble de départ de $\mathcal{R}$.

Mathémator : Allez, vous voulez reprendre un exemple...

Qui regarde Gulli ? Il faut définir $\mathrm{TV}^{-1}(\{\mathrm{Gulli}\})$.

Hihutix: Fastoche : c'est {Roger, Berthe, Gudrun}.

6 8 Égalité de deux relations

Définition 1 - 13

Les relations $\mathcal{R}_1 = (\mathrm{E}_1, \mathrm{F}_1, \mathrm{G}_{\mathcal{R}_1})$ et $\mathcal{R}_2 = (\mathrm{E}_2, \mathrm{F}_2, \mathrm{G}_{\mathcal{R}_2})$ sont égales si, et seulement si, $\mathrm{E}_1 = \mathrm{E}_2$ **et** $\mathrm{F}_1 = \mathrm{F}_2$ **et** $\mathrm{G}_{\mathcal{R}_1} = \mathrm{G}_{\mathcal{R}_2}$.

Vous êtes priés de ne pas modifier cette définition en fonction des circonstances. Il faut comprendre que les relations :

$$\mathcal{R} = (\mathrm{E},\mathrm{F},\mathrm{G}_{\mathcal{R}}) \text{ et } \mathcal{R}_1 = (\mathrm{dom}(\mathcal{R}), \mathrm{Im}(\mathcal{R}), \mathrm{G}_{\mathcal{R}})$$

ne sont pas forcément égales même si on a l'impression que « c'est pareil ». Tout ce que l'on peut dire c'est qu'elles ont le même graphe et c'est déjà beaucoup. Imaginons que E et F soient deux fichiers *informatiques* et que $G_{\mathcal{R}}$ nous donne les couples de fiches correspondant à une certaine requête (relation). Ce n'est pas parce que certaines fiches (éléments des fichiers) ne seront pas utilisées que vous devez les ignorer ou les faire disparaître des fichiers !

6 9 Restriction, prolongement

Définition 1 - 14

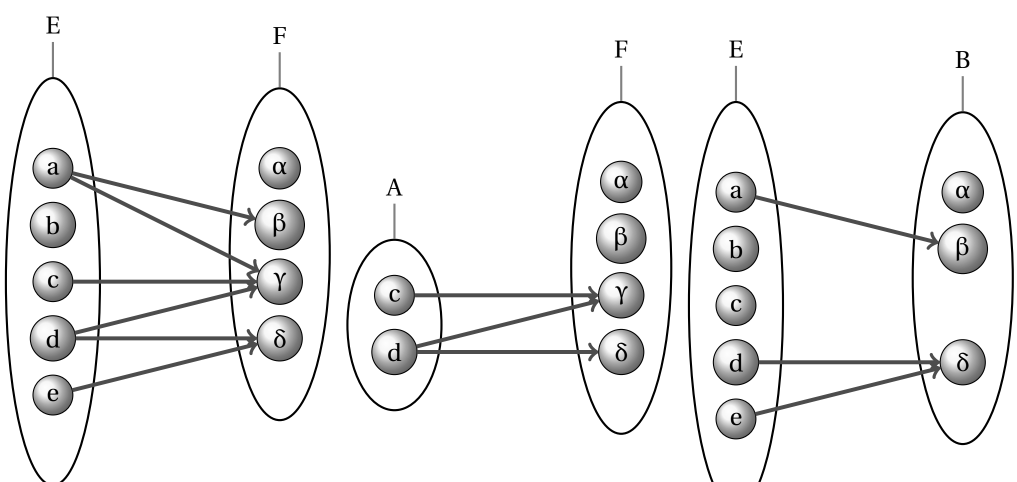
Soit $\mathcal{R} = (E, F, G_{\mathcal{R}})$ une relation de E vers F et A **une partie de** E. La **restriction** de $\mathcal{R}$ à A est la relation notée $\mathcal{R}_{|A}$ définie par $\mathcal{R}_{|A} = \left(A, F, G_{\mathcal{R}} \cap (A \times F)\right)$.
Si $\mathcal{U} = \left(A, F, G_{\mathcal{U}}\right)$ et si $\mathcal{U} = \mathcal{R}_{|A}$ on dit que $\mathcal{R}$ est **un** prolongement de $\mathcal{U}$ à E.

Danger

Nous décidons de noter $\left(\mathcal{R}^{-1}\right)_{|B}$ par $\mathcal{R}^{-1}_{|B}$ qu'il ne faut surtout pas confondre avec $\left(\mathcal{R}_{|B}\right)^{-1}$: $\mathcal{R}^{-1}_{|B}$ est la restriction de $\mathcal{R}^{-1}$ à la partie B (cela n'a de sens que si $B \subseteq F$) et $\left(\mathcal{R}_{|B}\right)^{-1}$ est la relation réciproque de la restriction de $\mathcal{R}$ à la partie B (cela n'a de sens que si $B \subseteq E$)

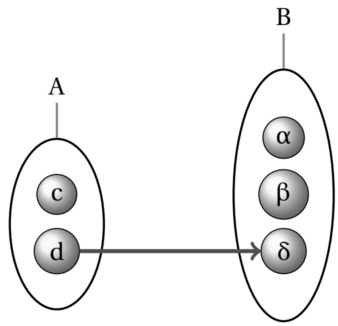
Si B **est une partie de** F, $\left(\mathcal{R}^{-1}_{|B}\right)^{-1}$ est appelée la restriction de $\mathcal{R}$ à la partie B de l'ensemble d'arrivée, c'est la relation $(E, B, G_{\mathcal{R}} \cap (E \times B))$.

Considérons par exemple la relation $\mathcal{R}$ définie par son diagramme sagittal et visualisons quelques restrictions :



$\mathcal{R}$ $\qquad$ $\mathcal{R}_{|A}$ $\qquad$ $\left(\left(\mathcal{R}^{-1}\right)_{|B}\right)^{-1}$

Remarquons enfin que $\left(\mathcal{R}_{|B}^{-1}\right)_{|A}^{-1} = \left(A, B, G_{\mathcal{R}} \cap (A \times B)\right) = \left(\left(\mathcal{R}_{|A}\right)_{|B}^{-1}\right)^{-1}$:



$\left(\mathcal{R}_{|B}^{-1}\right)_{|A}^{-1}$

Hihutix: Ouh la la... $\left(\left(\mathcal{R}^{-1}\right)_{|B}\right)^{-1}$, $\left(\mathcal{R}_{|B}^{-1}\right)_{|A}^{-1}$...Vous avez plus illisible ?

Mathémator : Bon, je suppose qu'il faut rallumer la Télé. Résumons : ici $\mathcal{R} = \text{TV}$, prenons $A = \{\text{Berthe,Gudrun}\}$ et $B = \{\text{Gulli}\}$.

$\left(\mathcal{R}^{-1}\right)_{|B} = \{(\text{Gulli,Roger}), (\text{Gulli,Berthe}), (\text{Gulli,Gudrun})\}$: il s'agit des couples satisfaisant à « Gulli est regardé par... ».

Maintenant, $\left(\left(\mathcal{R}^{-1}\right)_{|B}\right)^{-1}$ est l'ensemble des couples satisfaisant à « ... regarde Gulli ».

Hihutix: $\left(\left(\mathcal{R}^{-1}\right)_{|B}\right)^{-1} = \{(\text{Roger,Gulli}), (\text{Berthe,Gulli}), (\text{Gudrun,Gulli})\}$. On met les couples à l'envers. Ça, ça va.

Mathémator : Bien. Ensuite, point de vue notation, $\mathcal{R}_{|B}^{-1}$ est un diminutif de $\left(\mathcal{R}^{-1}\right)_{|B}$: c'est la même chose.

On a donc toujours $\mathcal{R}_{|B}^{-1} = \{(\text{Gulli,Roger}), (\text{Gulli,Berthe}), (\text{Gulli,Gudrun})\}$.

Alors $\left(\mathcal{R}_{|B}^{-1}\right)_{|A}^{-1}$ est l'ensemble des couples satisfaisant à « ...regarde Gulli » sachant que l'on ne s'occupe que des filles.

Ainsi $\left(\mathcal{R}_{|B}^{-1}\right)_{|A}^{-1} = \{(\text{Berthe,Gulli}), (\text{Gudrun,Gulli})\}$.

C'est bien la même chose que $\left(\left(\mathcal{R}_{|A}\right)_{|B}^{-1}\right)^{-1}$ quand on y pense...

Hihutix: Mouais...

6 10 Négation, inclusion, union, intersection

Une relation $\mathcal{R}$ de E vers F étant assimilée à un ensemble, une partie de $E \times F$, on est naturellement amené à utiliser les opérations ensemblistes élémentaires.

Dans ce qui suit $\mathcal{R}_1 = (E, F, G_{\mathcal{R}_1})$ et $\mathcal{R}_2 = (E, F, G_{\mathcal{R}_2})$ sont deux relations de E vers F et R_1 et R_2 sont, respectivement, leurs matrices[p].

6 10 1 Négation

Définition 1 - 15

La **négation** de $\mathcal{R}_1$ (on dit aussi le complémentaire de $\mathcal{R}_1$) est la relation :

$$\overline{\mathcal{R}_1} = \left(E, F, \complement_{E\times F} G_{\mathcal{R}_1}\right)$$

Cela signifie tout simplement que $x\overline{\mathcal{R}_1}y$ si, et seulement si, $(x, y) \notin G_{\mathcal{R}_1}$ ou encore que x n'est pas en relation avec y par $\mathcal{R}_1$.

La relation $\overline{\mathcal{R}_1}$ est aussi notée $\neg\mathcal{R}_1$.

Mathémator : Par exemple ici, Berthe TV^{-1} TF1 : Berthe ne regarde pas TF1.

Hihutix: Elle a raison.

Pour aller plus loin

Après l'étude du calcul booléen
La matrice booléenne de $\overline{\mathcal{R}_1}$ s'obtient en remplaçant dans la matrice booléenne de $\mathcal{R}_1$ les « 0 » par des « 1 » et les « 1 » par des « 0 ». Cela revient à ajouter 1 à chaque élément de la matrice de $\mathcal{R}_1$, les calculs se faisant modulo 2 (i.e. $1 + 1 = 0$).

6 10 2 Inclusion

Définition 1 - 16

On dit que la relation $\mathcal{R}_1$ est incluse dans la relation $\mathcal{R}_2$ ou que la relation $\mathcal{R}_1$ est une **sous relation** de la relation $\mathcal{R}_2$ si, et seulement si, $G_{\mathcal{R}_1} \subseteq G_{\mathcal{R}_2}$. Cela signifie que

$$x\mathcal{R}_1 y \Rightarrow x\mathcal{R}_2 y$$

et on écrit alors $\mathcal{R}_1 \subseteq \mathcal{R}_2$.

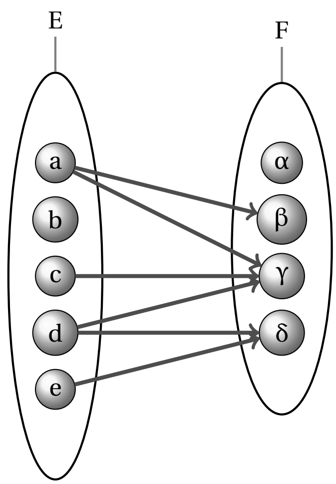
Attention ! Si A est une partie propre de E, la restriction de $\mathcal{R}_1$ à A n'est pas incluse dans $\mathcal{R}_1$ tout simplement parce que$\mathcal{R}_{1|A}$ n'est pas une relation de E vers F mais de A vers F ; par

p. En première lecture, nous laisserons de côté le calcul matriciel qui exige également de connaître dans ce cas précis le calcul booléen et le corps $\mathbf{F}_2$

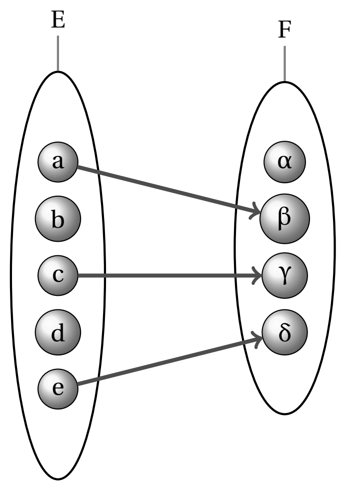
contre, la relation

$$\mathcal{R}_1' = \left(\mathrm{E}, \mathrm{F}, \mathrm{G}_{\mathcal{R}_1'} = \mathrm{G}_{\mathcal{R}_1} \cap (\mathrm{A} \times \mathrm{F})\right)$$

est incluse dans $\mathcal{R}_1$, c'est une sous relation de $\mathcal{R}_1$. Visuellement, une sous relation est obtenue en « supprimant » des flèches :



$\mathcal{R}_1$



$\mathcal{R}_2$ est une sous-relation de $\mathcal{R}_1$

Mathémator : Pour être plus concret, modifions un peu notre exemple télévisuel en supposant qu'on peut maintenant regarder plusieurs chaînes de télévision.

Par exemple, posons à présent TV2= $\{$Roger $\mapsto$ Gulli, Berthe $\mapsto$ Gulli, Berthe $\mapsto$ Zen TV, Jean-Pierre $\mapsto$ Zen TV, Gudrun $\mapsto$ Gulli, Gudrun $\mapsto$ TF1, Gudrun $\mapsto$ Zen TV$\}$.

Alors TV $\subseteq$ TV2.

Pour aller plus loin

Après l'étude du calcul booléen
Matriciellement cela se traduit par le fait que tous les « 1 » de la matrice R_1 sont aussi des « 1 » de la matrice R_2 ce qui donne, en utilisant le calcul booléen $(1+1=1)$:

$$\mathcal{R}_1 \subseteq \mathcal{R}_2 \Leftrightarrow \mathrm{R}_1 + \mathrm{R}_2 = \mathrm{R}_2$$

Notations

Méthode B
Voici les notations utilisées en méthode B, $\mathcal{R}$ désignant une relation de E vers F.
Obligatoirement $A \subseteq E$ **et** $B \subseteq F$.

- *La relation* $\left(E, F, G_{\mathcal{R}} \cap (A \times F)\right)$ *est notée* $A \lhd \mathcal{R}$*, c'est une sous relation de* $\mathcal{R}$ *et les informaticiens parlent de « restriction de domaine ».*
- *La relation* $(E, F, G_{\mathcal{R}} \cap (E \times B))$ *est notée* $\mathcal{R} \rhd B$*, c'est une sous relation de* $\mathcal{R}$*et les informaticiens parlent de « restriction de codomaine ».*
- *La relation* $\left(E, F, G_{\mathcal{R}} \cap (A \times B)\right)$ *est notée* $A \lhd \mathcal{R} \rhd B$*, c'est une sous relation de* $\mathcal{R}$ *et les informaticiens parlent de « restriction de domaine et de codomaine ».*

6 10 3 Réunion et intersection

Définition 1 - 17

La **réunion** de $\mathcal{R}_1$ et de $\mathcal{R}_2$ est la relation $\mathcal{R}_1 \cup \mathcal{R}_2 = \left(E, F, G_{\mathcal{R}_1} \cup G_{\mathcal{R}_2}\right)$.
L'**intersection** de $\mathcal{R}_1$ et de $\mathcal{R}_2$ est la relation $\mathcal{R}_1 \cap \mathcal{R}_2 = \left(E, F, G_{\mathcal{R}_1} \cap G_{\mathcal{R}_2}\right)$.

Cela revient en fait à ajouter ou à enlever des flèches.

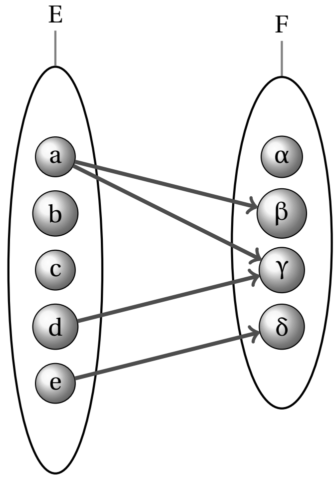
Danger

On notera bien que l'on ne peut comparer ou faire l'union ou l'intersection de deux relations qu'à la condition qu'elles aient le même ensemble de départ et le même ensemble d'arrivée.

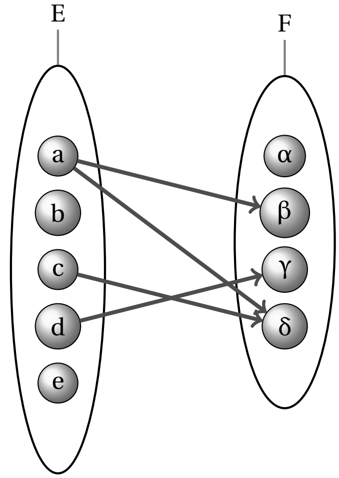
Pour aller plus loin

Après l'étude du calcul booléen
La matrice booléenne de $\mathcal{R}_1 \cup \mathcal{R}_2$ est $R_1 + R_2$.
La matrice booléeen de $\mathcal{R}_1 \cap \mathcal{R}_2$ s'obtient « en ne gardant que les 1 qui ont la même place » dans R_1 et R_2.
Si on veut l'obtenir par le calcul on peut procéder ainsi (c'est tout de même un peu compliqué) : on utilise une des lois de De Morgan, à savoir que le complémentaire d'une union est égale à l'intersection des complémentaires, $\overline{\overline{\mathcal{R}_1} \cup \overline{\mathcal{R}_2}} = \mathcal{R}_1 \cap \mathcal{R}_2$. On rajoute donc **(modulo 2)** 1 à chaque élément des matrices R_1 et R_2, on fait alors la **somme booléenne** des résultats obtenus et on ajoute alors **(modulo 2)** 1 à chaque élément de cette somme.

Rien ne vaut un bon exemple...Considérons deux relations $\mathcal{R}_1$ et $\mathcal{R}_2$:

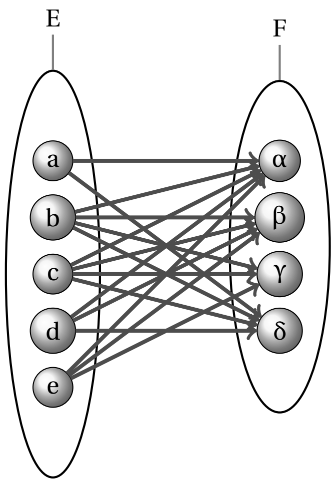


$\mathcal{R}_1$

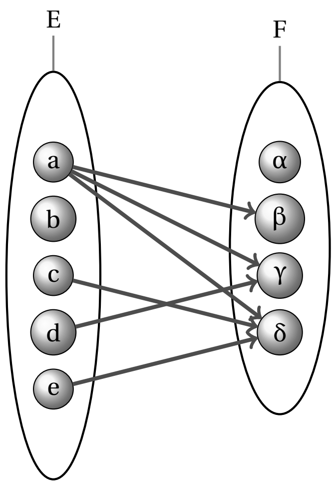


$\mathcal{R}_2$

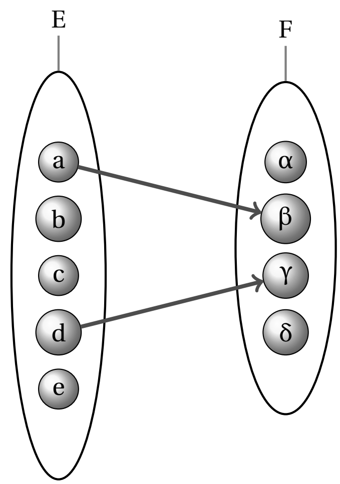
On remarque qu'aucune n'est incluse dans l'autre et on obtient :



$\overline{\mathcal{R}_1}$



$\mathcal{R}_1 \cup \mathcal{R}_2$



$\mathcal{R}_1 \cap \mathcal{R}_2$

Mathémator : Rallumons la télé mais cette fois en distinguant les chaînes regardées le midi de celles regardées le soir :

TVmidi= $\{$Roger $\mapsto$ Gulli, Berthe $\mapsto$ Gulli, Berthe $\mapsto$ Zen TV, Jean-Pierre $\mapsto$ Zen TV, Gudrun $\mapsto$ Gulli, Gudrun $\mapsto$ TF1, Gudrun $\mapsto$ Zen TV$\}$.

TVsoir== $\{$Roger $\mapsto$ TF1, Berthe $\mapsto$ Gulli, Berthe $\mapsto$ TF1, Jean-Pierre $\mapsto$ TF1, Gudrun $\mapsto$ Gulli, Gudrun $\mapsto$ TF1$\}$.

Comment décririez-vous les relations TVmidi ∩ TVsoir et TVmidi ∪ TVsoir ?

Hihutix: Je me souviens de mes cours de probas : ∩ c'est « et » et ∪ c'est « ou » donc :

– TVmidi ∩ TVsoir c'est « ...regarde le midi et le soir ... » ;

– TVmidi ∪ TVsoir c'est « ...regarde le midi ou le soir ... » ;

Mathémator : Parfait. Cela donne :

– TVmidi ∩ TVsoir= $\{$ Berthe $\mapsto$ Gulli, Gudrun $\mapsto$ Gulli, Gudrun $\mapsto$ TF1$\}$;

– TVmidi ∪ TVsoir= $\{$Roger $\mapsto$ Gulli, Berthe $\mapsto$ Gulli,Berthe $\mapsto$ Zen TV, Berthe $\mapsto$ TF1, Jean-Pierre $\mapsto$ Zen TV, Jean-Pierre $\mapsto$ TF1, Gudrun $\mapsto$ Gulli, Gudrun $\mapsto$ TF1, Gudrun $\mapsto$ Zen TV$\}$;

6 11 Composition de relations

Définition 1 - 18

$\mathcal{R} = (\mathrm{E}, \mathrm{F}, \mathrm{G}_{\mathcal{R}})$ et $\mathcal{S} = (\mathrm{U}, \mathrm{V}, \mathrm{G}_{\mathcal{S}})$ sont deux relations. La **composition** (ou la composée) de $\mathcal{R}$ par $\mathcal{S}$ (attention à l'ordre) **ne peut se faire que si** F = U ou, si l'on préfère, que si l'ensemble d'arrivée de $\mathcal{R}$ est égal à l'ensemble de départ de $\mathcal{S}$. Dans ce cas la composée de $\mathcal{R}$ par $\mathcal{S}$ est la relation notée $\mathcal{S} \circ \mathcal{R}$ qui a pour ensemble de départ E (l'ensemble de départ de $\mathcal{R}$), pour ensemble d'arrivée V (l'ensemble d'arrivée de $\mathcal{S}$) et pour graphe $\mathrm{G}_{\mathcal{S}\circ\mathcal{R}}$ qui est l'ensemble des couples (x, z) de E × V tel qu'il existe au moins un $y \in \mathrm{F}$ vérifiant $(x, y) \in \mathrm{G}_{\mathcal{R}}$ **et** $(y, z) \in \mathrm{G}_{\mathcal{S}}$.

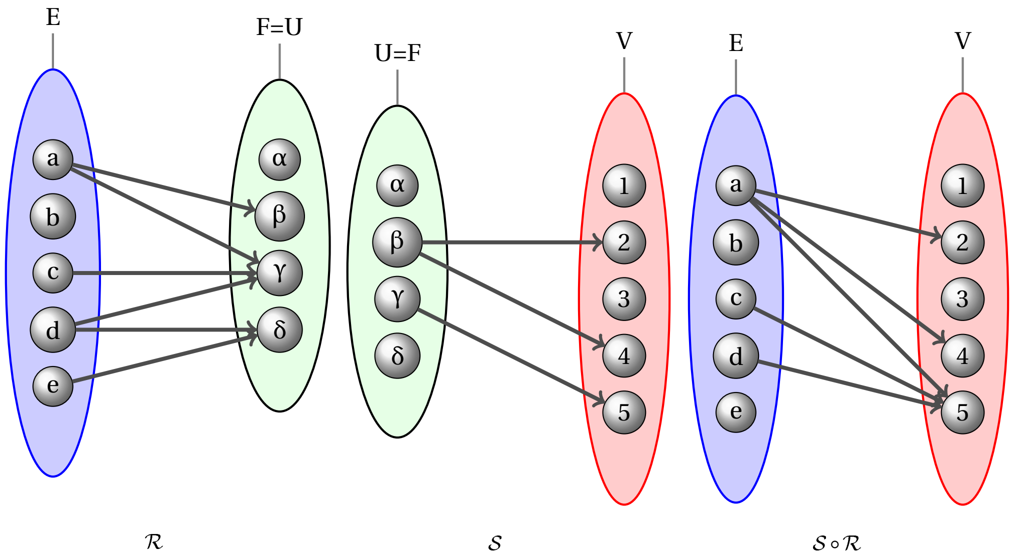
Pour simplifier les choses, $\mathcal{S}\circ\mathcal{R}$ est aussi notée $\mathcal{R}.\mathcal{S}$ ou bien encore $\mathcal{R};\mathcal{S}$ (attention à l'ordre !). En effet, si $x\mathcal{R}y$ et $y\mathcal{S}z$ il est plus « naturel » d'écrire $x\mathcal{R}.\mathcal{S}z$. Sans compter que la paresse amène souvent à noter la relation $\mathcal{R}.\mathcal{S}$ par $\mathcal{R}\mathcal{S}$...

Nous utiliserons plutôt un symbole largement utilisé en informatique : « $\mathcal{R}$ **suivi de** $\mathcal{S}$ » **sera noté** $\mathcal{R} \fatsemi \mathcal{S}$.

Danger

Il est impératif qu'à chaque fois que vous aurez à manipuler la composition de deux relations, vous vous assuriez de son existence ! C'est très clair, pour que $\mathcal{S} \circ \mathcal{R} = \mathcal{R} \fatsemi \mathcal{S}$ existe ou ait un sens il est obligatoire que l'ensemble d'arrivée de $\mathcal{R}$ **coïncide exactement** avec l'ensemble de départ de $\mathcal{S}$; il est vrai que, mathématiquement parlant, on pourrait avoir une définition de la composition moins restrictive, mais l'informatique, qui utilise ces mathématiques, impose la défnition que nous avons donnée.

Le mieux est encore d'analyser un exemple :



Pour aller plus loin

Après l'étude du calcul booléen
Si R est la matrice de $\mathcal{R}$ et S la matrice de $\mathcal{S}$ alors R × S est la matrice de $\mathcal{S}\circ\mathcal{R}$ **(attention à l'ordre)**, les calculs se faisant dans l'algèbre de boole binaire $\mathcal{B}_2$, c'est-à-dire avec « 1 + 1 = 1 ». Le produit R × S est alors qualifié de multiplication booléenne.

Quant à l'exemple précédent, matriciellement nous avons :

$$\mathrm{R} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \mathrm{S} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \mathrm{R}\times\mathrm{S} = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Théorème 1 - 2

Pseudo associativité
On retiendra que si $\mathcal{R} = \left(\mathrm{E},\mathrm{F},\mathrm{G}_{\mathcal{R}}\right), \mathcal{S} = \left(\mathrm{F},\mathrm{V},\mathrm{G}_{\mathcal{S}}\right)$ et $\mathcal{T} = \left(\mathrm{V},\mathrm{W},\mathrm{G}_{\mathcal{T}}\right)$ alors :

$$\mathcal{T}\circ(\mathcal{S}\circ\mathcal{R}) = (\mathcal{T}\circ\mathcal{S})\circ\mathcal{R} \text{ ou } \left(\mathcal{R}\,⨟\,\mathcal{S}\right)⨟\,\mathcal{T} = \mathcal{R}\,⨟\left(\mathcal{S}\,⨟\,\mathcal{T}\right)$$

Cette propriété porte le nom de pseudo associativité car on ne peut considérer la composition des relations comme une loi de composition interne, nous n'avons pas encore fixé « de cadre » pour cette opération.

Recherche

Que pensez de $\mathcal{R}^{-1}\circ\mathcal{R}$ ou de $\mathcal{R}\circ\mathcal{R}^{-1}$? Regardez ce que cela donne avec la relation $\mathcal{R}$ introduite précédemment.
Vérifiez, en deuxième lecture, que la méthode matricielle est efficace dans ce cas.

On notera aussi que la relation réciproque de $\mathcal{S}\circ\mathcal{R}$ est $\mathcal{R}^{-1}\circ\mathcal{S}^{-1}$:

$$(\mathcal{S}\circ\mathcal{R})^{-1}=\mathcal{R}^{-1}\circ\mathcal{S}^{-1} \text{ ou } \left(\mathcal{R}\,\mathring{9}\,\mathcal{S}\right)^{-1}=\mathcal{S}^{-1}\,\mathring{9}\,\mathcal{R}^{-1}$$

Théorème 1 - 3

Lorsque cela a un sens, la composition est distributive par rapport (ou pour) l'union :

$$\begin{cases}\mathcal{R}\circ(\mathcal{S}_1\cup\mathcal{S}_2)=(\mathcal{R}\circ\mathcal{S}_1)\cup(\mathcal{R}\circ\mathcal{S}_2)\\(\mathcal{S}_1\cup\mathcal{S}_2)\circ\mathcal{R}=(\mathcal{S}_1\circ\mathcal{R})\cup(\mathcal{S}_2\circ\mathcal{R})\end{cases}$$

La composition est compatible avec l'inclusion, en ce sens que, si les compositions ont un sens :

$$\begin{cases}\mathcal{R}\subseteq\mathcal{S}\Rightarrow\mathcal{R}\circ\mathcal{T}\subseteq\mathcal{S}\circ\mathcal{T}\\\mathcal{R}\subseteq\mathcal{S}\Rightarrow\mathcal{T}\circ\mathcal{R}\subseteq\mathcal{T}\circ\mathcal{S}\end{cases}$$

Lorsque cela a un sens :

$$\mathcal{R}\subseteq\mathcal{S} \text{ et } \mathcal{T}\subseteq\mathcal{U}\Rightarrow(\mathcal{R}\circ\mathcal{T}\subseteq\mathcal{S}\circ\mathcal{U} \text{ et } \mathcal{T}\circ\mathcal{R}\subseteq\mathcal{U}\circ\mathcal{S})$$

Hihutix: On allume la Télé ?

Mathémator : Allez, on va changer un peu. Cette fois considérons des animaux, leurs petits noms et leurs cris :

- Baptême=$\{$alouette$\mapsto$Josette, alouette$\mapsto$Pépette, albatros$\mapsto$Bernard, bécasse$\mapsto$Germaine$\}$;
- Cri=$\{$Josette$\mapsto$turlute, Josette$\mapsto$grisole, Pépette$\mapsto$turlute, Bernard$\mapsto$piaule, Germaine$\mapsto$croul

Quelle est la tête de Baptême $\mathring{9}$ Cri et comment l'interpréter ?

Hihutix (à part): *Il a une case. D'où il sort des noms pareils ?* **(tout haut)** Fastoche mais vous manquez de rigueur : il faut préciser sur quels ensembles on travaille.

Par exemple, appelons :

- Noms= $\{$Josette, Pépette, Bernard, Germaine$\}$;
- Animaux= $\{$alouette, albatros, bécasse$\}$;
- Bruits= $\{$turlutte, grisole, piaule, croule$\}$.

Alors Baptême $\in$ Animaux $\leftrightarrow$ Noms et Cri $\in$ Noms $\leftrightarrow$ Bruits.

On peut donc bien définir $\text{Baptême} \circ_9 \text{Cri} \in \text{Animaux} \leftrightarrow \text{Bruits}$.

Alors $\text{Baptême} \circ_9 \text{Cri} = \{\text{alouette} \mapsto \text{turlute}, \text{alouette} \mapsto \text{grisole}, \text{albatros} \mapsto \text{piaule}, \text{bécasse} \mapsto \text{croule}\}$.

Ceci nous donne le nom des cris de certains animaux.

Mathémator : Vous progressez à vue d'œil : bravo ! Alors je peux vous poser des petites questions subsidiaires que vous résoudrez pendant vos temps libres...

Recherche

1. Calculez $\{\text{alouette}, \text{albatros}\} \lhd (\text{Baptême} \circ_9 \text{Cri})$;
2. Calculez $(\{\text{alouette}, \text{albatros}\} \lhd \text{Baptême}) \circ_9 \text{Cri}$.

6 12 Fonctions, applications

6 12 1 Définition

Définition 1 - 19

On dit que **la relation** $f = (E, F, G_f)$ est une **fonction** (ou une dépendance fonctionnelle) de E vers (ou dans) F si, et seulement si, tout élément de E a **au plus** (cela veut dire : soit zéro ou une) une image dans F.

Cela signifie aussi que si x est un élément quelconque de E, $f(\{x\})$ est soit l'ensemble vide soit un singleton. Si x a au moins une image, c'est-à-dire s'il existe $y \in F$ tel que $(x, y) \in G_f$, y est forcément unique et est noté $f(x)$. Lorsque la relation $f = (E, F, G_f)$ est une fonction on préfère le plus souvent utiliser la notation :

$$f : \begin{array}{ccc} E & \rightarrow & F \\ x & \mapsto & f(x) = y \end{array}$$

qui se lit « f est une fonction de E dans F qui à x associe $f(x)$ ». On note $\mathcal{F}(E, F)$ ou F^E l'ensemble des fonctions de E dans F.

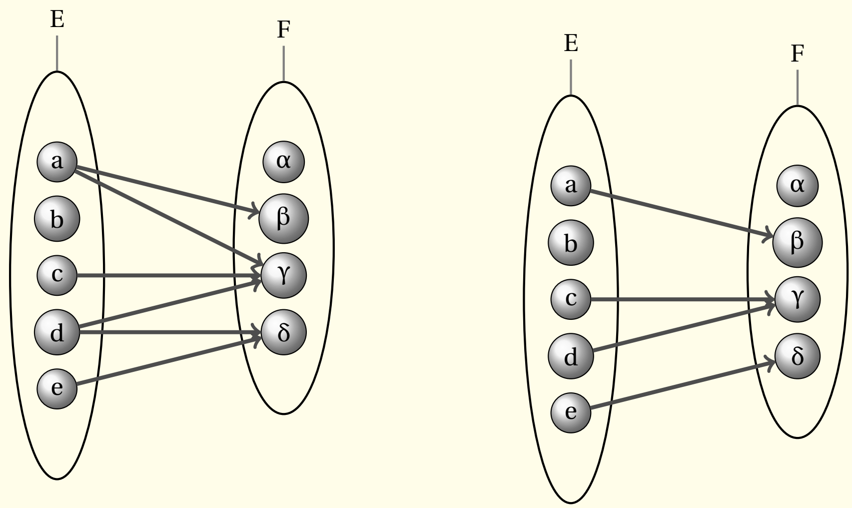
Lorsque E est de la forme $U^n = U \times U \times \ldots \times U$, on dit que la fonction de U^n dans F est une fonction de n variables

$$f : \begin{array}{ccc} U^n & \rightarrow & F \\ (u_1, u_2, ..., u_n) & \mapsto & f(u_1, u_2, ..., u_n) \end{array}$$

et u_i est appelée la $i^{ème}$ variable de f.

Si la fonction $f = (E, F, G)$ vérifie $\text{dom}(f) = E$ on dit que f est une **application** de E dans F ou encore une **fonction totale** de E dans F. Une application est donc une fonction (donc aussi une relation) qui possède la propriété suivante : tout élément de l'ensemble de départ a une et une seule image dans l'ensemble d'arrivée. Si f est une fonction, sa restriction à son domaine (= son ensemble de définition) est une application. C'est pourquoi, en analyse, on confond souvent ces deux notions ; nous vous demandons de ne plus le faire. Il faut aussi reconnaître que la tradition française n'est pas très claire, on entend parler des fonctions polynômes, de la fonction logarithme népérien mais aussi d'applications linéaires et d'applications réciproques sans nous dire pourquoi dans un cas on utilise le mot « fonction » et dans un autre le mot « application ». Il faut bien se rendre compte que les fonctions sont de vulgaires relations qui possèdent tout simplement une propriété intéressante. On note $\mathcal{A}(\mathrm{E},\mathrm{F})$ l'ensemble des fonctions totales (applications) de E vers F.

Recherche



f g

Des commentaires en termes de fonctions ou d'applications ?

Théorème 1 - 4

La composition de fonctions est une fonction et la composition d'applications est une application.

6 12 2 Fonctions particulières

On est très souvent amené à utiliser des mêmes « types » de fonctions, il est alors naturel de fixer un certain vocabulaire pour éviter à chaque fois de redéfinir ces fonctions.

6 12 2 a Projection canonique

La fonction totale (l'application)

$$p_i : \mathrm{E}_1 \times \mathrm{E}_2 \times \ldots \times \mathrm{E}_n \longrightarrow \mathrm{E}_i$$

définie par $p_i(x_1, x_2, \ldots, x_n) = x_i$ est appelée projection canonique de

$$E_1 \times E_2 \times \ldots \times E_n \text{ sur } E_i$$

Si tous les E_i sont égaux au même ensemble E, p_i est appelée la $i^{ème}$ projection.

6 12 2 b Application identique

La fonction totale (l'application) définie sur E par

$$\mathrm{Id}_E : \begin{array}{ccc} E & \to & E \\ x & \mapsto & x \end{array}$$

est l'application identique dans E ou l'application identique de E, on la note aussi id_E ou id si aucune confusion n'est possible.

6 12 2 c Composition réitérée

Si f est une fonction totale de E dans E, on note f^k la composition

$$\underbrace{f \circ f \circ \cdots \circ f}_{k \text{ fois}}$$

si k est un entier naturel non nul et, par convention, $f^0 = id_E$. Si f^{-1} est une fonction on note de même

$$f^{-k} = \underbrace{f^{-1} \circ f^{-1} \circ \cdots \circ f^{-1}}_{k \text{ fois}}$$

et on remarquera que $f^{-k} = \left(f^k\right)^{-1}$.

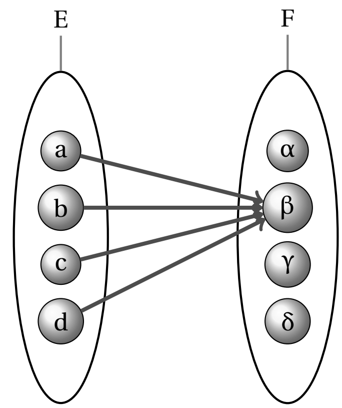
6 12 2 d Application caractéristique

Nous l'avons déjà présentée et utilisée, redonnons la définition : A est une partie de l'ensemble E, l'application caractéristique de A dans E est la fonction totale $\mathbb{1}_A$ définie par

$$\mathbb{1}_A : \begin{array}{ccc} E & \to & \{0,1\} \\ x & \mapsto & \begin{cases} 1 \text{ si } x \in A \\ 0 \text{ si } x \notin A \end{cases} \end{array}$$

6 12 2 e Fonction constante

La fonction totale (application) $f = \left(E, F, G_f\right)$ est dite constante lorsque $\mathbf{Im}\left(f\right)$ est un singleton :



Fonction constante

6 12 2 f Lois de composition

On appelle loi de composition ou opération dans E toute fonction de $A \times E$ dans E. Si $A = E$, on dit que la loi est une loi de composition interne, sinon on parle de loi de composition externe ou loi mixte. Si la loi est une application on dit qu'elle est partout définie. Si f est une telle loi de composition et $(a, x) \in A \times E$, on note $f((a, x))$ par $a \odot x$ ou $a * x$ ou $a \boxplus x$ ou $a \boxdot x$ ou $a + x$ ou ax ou .... On choisit le symbole le mieux adapté aux circonstances ou au contexte.

Exemple 1.5

La multiplication d'un vecteur $\vec{u}$ du plan par un réel λ, $\lambda.\vec{u}$ ou $\lambda\vec{u}$, est une loi de composition externe. E désignant un ensemble, l'union $\cup$ est une loi de composition interne dans $\mathcal{P}(E)$.

6 12 2 g Injection

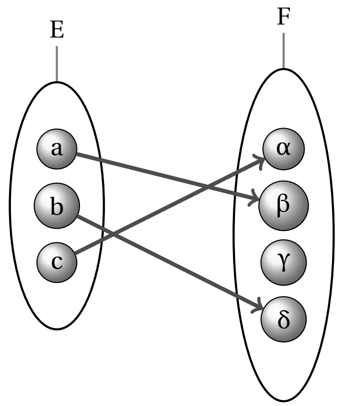
La fonction totale ou application $f : E \longrightarrow F$ (on a donc $\mathrm{dom}\left(f\right) = E$) est **injective** ou est une injection si, et seulement si, tout élément de F a au plus un antécédent. Cette définition équivaut à dire que :

- f^{-1} est une fonction.
- il n'existe pas deux éléments différents de E qui ont la même image dans F. En d'autres termes deux éléments différents ont toujours des images différentes.
- il n'existe pas d'élément de F ayant plus d'un antécédent.

Mathématiquement cela s'écrit :

$$\begin{aligned} f \text{ injective} \quad &\Leftrightarrow \quad \forall (x, x') \in E^2, \left(x \neq x' \Rightarrow f(x) \neq f(x')\right) \\ f \text{ injective} \quad &\Leftrightarrow \quad \forall (x, x') \in E^2, \left(f(x) = f(x') \Rightarrow x = x'\right) \end{aligned}$$

La fonction totale de E dans F :



Injection

est une injection et sa relation réciproque est une fonction (ici, non totale).

Remarque 18

Il est clair que si E a plus d'éléments que F, il est impossible de construire une fonction totale injective de E dans F.

Remarque 19

Si A est une partie non vide de E l'application

$$i : \begin{array}{ccc} A & \longrightarrow & E \\ x & \longmapsto & x \end{array}$$

est appelée injection canonique de A dans E. C'est aussi la restriction de l'application identique de E à A.

Indiquons quelques propriétés :

– La composition d'applications injectives est une injection. La démonstration est élémentaire.
– Si $g \circ f$ est injective, g et f étant des applications, alors f est forcément injective. En effet, si f n'était pas injective, il existerait alors au moins deux éléments distincts x et x' de l'ensemble de départ de f vérifiant $f(x) = f\left(x'\right)$ et du coup on aurait $g \circ f(x) = g \circ f\left(x'\right)$, c'est-à-dire $g \circ f$ non injective.

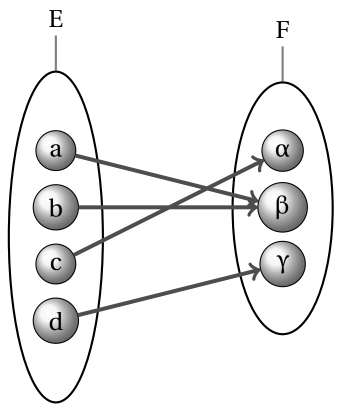
Remarque 20

Peut-on parler de fonction injective ? D'après la définition que nous avons donnée, la réponse est oui si cette fonction est totale. Néanmoins certains usages autorisent le label d'injectif aux fonctions non totales dont la restriction à leur domaine de définition est une application injective.

6 12 2 h Surjection

La fonction totale ou application $f : \mathrm{E} \longrightarrow \mathrm{F}$ (on a donc $\mathrm{dom}\left(f\right) = \mathrm{E}$) est **surjective** ou est une surjection de E dans[q] F si, et seulement si, tout élément de F a au moins un antécédent. Cela équivaut à écrire que $\mathbf{Im}(f) = \mathrm{F}$ ou que $f(\mathrm{E}) = \mathrm{F}$ ou encore que la relation réciproque de f est une relation totale.

L'application ou fonction totale suivante :



Surjection

est une surjection, sa relation réciproque est totale et n'est pas, ici, une fonction.

Remarque 21

L'exemple précédent nous montre que si F a plus d'éléments que E, il est impossible de construire une fonction totale surjective de E dans (ou sur) F.

Indiquons quelques propriétés :

- La composition de surjections est une surjection, la démonstration est évidente.
- Si $g \circ f$ est surjective, g et f étant des applications, alors g est forcément surjective. Supposons que f est une application de E dans F et g une application de F dans G. Il nous faut démontrer que tout élément z de G a au moins un antécédent par g dans F, c'est facile : $g \circ f$ étant surjective, z a au moins un antécédent x dans E , $z = g \circ f(x) = g\left(f(x)\right)$. Notons $y = f(x)$, nous avons $z = g\left(y\right)$ et $y \in \mathrm{F}$.

Remarque 22

Peut-on parler de fonction surjective ? D'après la définition que nous avons donnée, la réponse est oui si cette fonction est totale. Néanmoins certains usages autorisent le label de surjectif aux fonctions non totales dont la restriction à leur domaine de définition est une application surjective.

q. Lorsque f est une fonction totale surjective de E dans ou vers F, on a l'habitude de dire que f est une fonction totale surjective de E **sur** F.

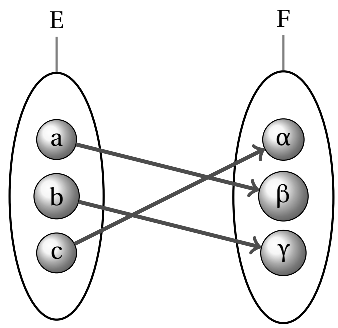
6 12 2 i Bijection

La fonction totale $f : \mathrm{E} \longrightarrow \mathrm{F}$ (on a donc $\mathrm{dom}\left(f\right) = \mathrm{E}$) est **bijective** ou **biunivoque** ou est une bijection si, et seulement si, elle est à la fois injective et surjective. Cela équivaut à écrire que tout élément de F a un et un seul antécédent dans E. On remarque immédiatement que, si E et F sont finis, il ne peut exister de bijection de E sur F qu'à la condition qu'ils aient le même cardinal (le même nombre d'éléments).

Indiquons quelques propriétés :

- La composition de bijections est une bijection..
- Si l'application $f : \mathrm{E} \longrightarrow \mathrm{F}$ est bijective sa relation réciproque, f^{-1}, est une application bijective et $f \circ f^{-1} = \mathrm{I}d_{\mathrm{F}}$ et $f^{-1} \circ f = \mathrm{I}d_{\mathrm{E}}$.

L'application suivante :



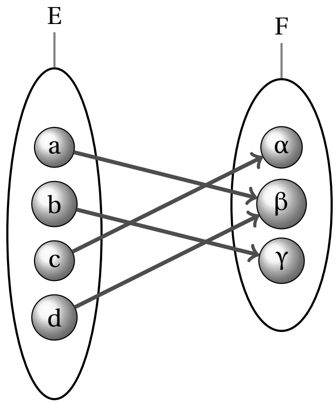
Bijection

est une bijection de E sur F et sa relation réciproque f^{-1} est une application bijective de F sur E.

Remarque 23

La notation $f^{-1}(y)$ n'a de sens que si f^{-1} est une fonction avec $y \in \mathrm{dom}\left(f^{-1}\right)$, c'est forcément le cas si f est bijective et le résultat est l'unique antécédent de y. Vous n'avez pas le droit d'écrire $f^{-1}(y)$ si f^{-1}n'est pas une fonction. Si vous cherchez les antécédents (éventuels) de y, il vous suffit de considérer l'ensemble $f^{-1}\left(\{y\}\right)$ et, dans le cas où f est bijective, vous obtiendrez toujours un singleton. Il vous a été présenté la notion de relation réciproque et si f est une relation quelconque f^{-1} a un sens, c'est la relation réciproque de f, mais ce n'est pas forcément une fonction.

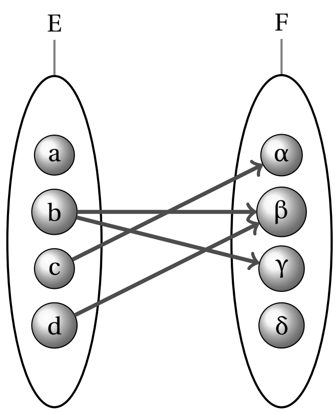
Considérons la relation f :



Application surjective non injective

c'est une fonction totale surjective mais non injective puisque a et e ont la même image. La relation f^{-1} n'est pas une fonction et l'écriture $f^{-1}(\alpha)$ est interdite. Par contre $f^{-1}(\{\alpha\}) = \{b\}$ et $f^{-1}\left(\{\gamma\}\right) = \{a, e\}$.

La relation g :



g n'est pas une fonction mais g^{-1} l'est.

n'est pas une fonction, l'écriture $g(\mathrm{d})$ est interdite mais $g(\{\mathrm{d}\}) = \left\{\beta\right\}$ et $g(\{c\}) = \emptyset$. La relation g^{-1} est une fonction, on a donc $g^{-1}(\alpha) = \mathrm{c}$ mais l'écriture $g^{-1}(\delta)$ est interdite car δ ne fait pas partie de l'ensemble de définition de la fonction g^{-1}. Par contre il est exact que $g^{-1}(\{\delta\}) = \emptyset$.

6 12 2 j Permutation

E étant un ensemble fini, on appelle **permutation** de E toute bijection f de E sur E. Pour représenter une permutation on utilise la notation suivante

$$f = \begin{pmatrix} a & b & c & d & e & f \\ c & a & d & f & e & b \end{pmatrix}$$

pour exprimer que a a pour image c, que b a pour image a, que c a pour image d , etc ....
Une transposition est une permutation qui échange deux éléments et qui laisse invariants tous les autres :

$$\begin{pmatrix} a & \mathbf{b} & c & d & e & \mathbf{f} \\ a & \mathbf{f} & c & d & e & \mathbf{b} \end{pmatrix}$$

Une **permutation circulaire** d'une unité vers la gauche des éléments ordonnés a_1, a_2, ..., a_n (dans cet ordre) est la permutation

$$pcg_1 = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_{n-1} & a_n \\ a_2 & a_3 & a_4 & \cdots & a_n & a_1 \end{pmatrix}$$

et une permutation circulaire de k unités vers la gauche est la bijection pcg_1^k. On définit de même une permutation circulaire de k unités vers la droite. On remarquera que la permutation circulaire de k unités vers la gauche coïncide avec la permutation circulaire de $n-k$ unités vers la droite.

Exemple 1.6

Considérons la suite de bits $s = (0,1,1,0,1,1,0,0)$, notons pcg_k la permutation circulaire de k unités vers la gauche et pcd_k la permutation circulaire de k unités vers la droite. Nous avons :

$$\begin{aligned} pcg_1(s) &= (1,1,0,1,1,0,0,0) \\ pcg_2(s) &= (1,0,1,1,0,0,0,1) = pcg_1\left(pcg_1(s)\right) \\ pcd_3(s) &= (1,0,0,0,1,1,0,1) = pcg_1^5(s) \end{aligned}$$

La suite s comportant 8 éléments, il est clair que $pcg_8(s) = pcd_8(s) = s$.

7 Relations binaires sur un ensemble

7 1 Au CE1

7 2 Définition

Définition 1 - 20

On appelle **relation binaire sur l'ensemble** E tout triplet du type

$$\mathcal{R} = \left(\mathrm{E}, \mathrm{E}, \mathrm{G}_{\mathcal{R}}\right)$$

où $\mathrm{G}_{\mathcal{R}}$ est une partie de $\mathrm{E} \times \mathrm{E}$.

Une relation binaire sur l'ensemble E est donc tout simplement une relation « classique » qui a son ensemble de départ égal à son ensemble d'arrivée Nous allons reprendre rapidement les généralités pour ces relations et développer les particularités.

On confond souvent la relation $\mathcal{R}$ avec $\mathrm{G}_{\mathcal{R}}$ puisque c'est la donnée de $\mathrm{G}_{\mathcal{R}}$ qui définit la relation $\mathcal{R}$. On utilisera les différentes écritures :

$$(x, y) \in \mathrm{G}_{\mathcal{R}} \Leftrightarrow (x, y) \in \mathcal{R} \Leftrightarrow x \mathcal{R} y \Leftrightarrow \mathcal{R}(x, y)$$

pour exprimer que l'élément x de E est en relation avec l'élément y de E. Lors de l'étude des graphes qui correspondent à des relations binaires sur l'ensemble E, les éléments de E sont appelés les sommets du graphe $\mathcal{R}$ et les éléments de $\mathrm{G}_{\mathcal{R}}$ sont appelés des arcs ; si $\left(x, y\right)$ est un arc, c'est à dire si $x\mathcal{R}y$, on utilise le vocabulaire suivant :

- x est l'extrémité initiale de l'arc $\left(x, y\right)$ ou x est un antécédent ou précédent ou prédécesseur de y ;
- y est l'extrémité finale ou terminale de l'arc $\left(x, y\right)$ ou y est un suivant ou successeur de x.

Remarque 24

Comme l'ensemble de départ de la relation $\mathcal{R}$ est égal à l'ensemble d'arrivée, on convient alors de dire que la relation $\mathcal{R}$ est le couple $\left(\mathrm{E}, \mathrm{G}_{\mathcal{R}}\right)$. L'ensemble des relations de E dans E est noté $\mathrm{E} \longleftrightarrow \mathrm{E}$ et cet ensemble peut être confondu avec $\mathcal{P}(\mathrm{E} \times \mathrm{E})$. Le couple $\mathcal{R} = \left(\mathrm{E}, \mathrm{G}_{\mathcal{R}}\right)$ est aussi appelé graphe orienté d'ensemble de sommets E et d'ensemble d'arcs $\mathrm{G}_{\mathcal{R}}$, cette terminologie est utilisée pour les graphes.

Remarque 25

Si $\mathrm{G}_{\mathcal{R}} = \emptyset$, la relation est appelée la relation vide de E ou dans E. Si $\mathrm{G}_{\mathcal{R}} = \mathrm{E} \times \mathrm{E}$, la relation est appelée la relation pleine de E qui est parfois notée Π_{E}. Si $\mathrm{G}_{\mathcal{R}} = \{(x, x) \mid x \in \mathrm{E}\}$ (la diagonale de $\mathrm{E} \times \mathrm{E}$), la relation est la relation identité, ce n'est autre que l'application identique de E notée $\mathrm{I}d_{\mathrm{E}}$ ou id_{E}.

7 3 Représentations

On considère un ensemble fini E : on peut donc représenter la relation $\mathcal{R}$ à l'aide des outils habituels.

Par exemple, considérons la relation $\mathcal{R}$ définie par

$$\mathcal{R} = \left(\mathrm{E} = \{a, b, c, d, e\}, \mathrm{G}_{\mathcal{R}} = \{(a,a), (a,b), (b,a), (d,b), (c,d), (c,e)\}\right)$$

On aurait envie d'utiliser le diagramme sagittal habituel :

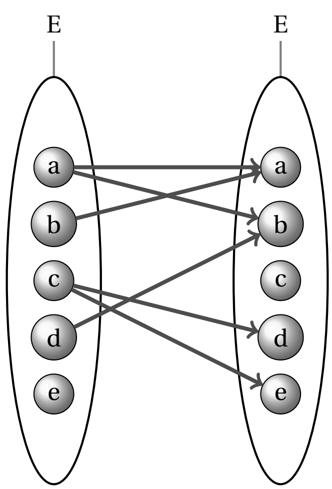


Diagramme sagittal d'une relation sur un ensemble (version 1)

Il est cependant plus « économique » de n'utiliser qu'une « patate » car nous restons dans E. On symbolise alors les relations du type $a \,\mathcal{R}\, a$ à l'aide de *boucles* :

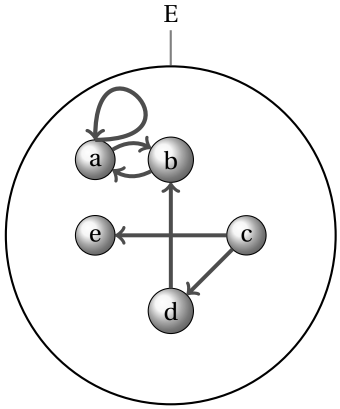


Diagramme sagittal d'une relation sur un ensemble (version 2)

Pour aller plus loin

On peut bien sûr utiliser une matrice carrée d'ordre n.
Si $E = \{x_1, x_2, \cdots, x_n\}$, la matrice :

$$M = (m_{i,j}) \text{ avec } \begin{cases} m_{i,j} = 1 \text{ si } x_i \mathcal{R} x_j \\ m_{i,j} = 0 \text{ si } (x_i, x_j) \notin G_{\mathcal{R}} \end{cases}$$

est appelée la *matrice d'adjacence* de $\mathcal{R}$ ou du graphe $\mathcal{R}$. On dit aussi que M est la *matrice booléenne* de la relation $\mathcal{R}$, dans ce cas, les calculs matriciels utilisent le fait que « $1+1=1$ ».

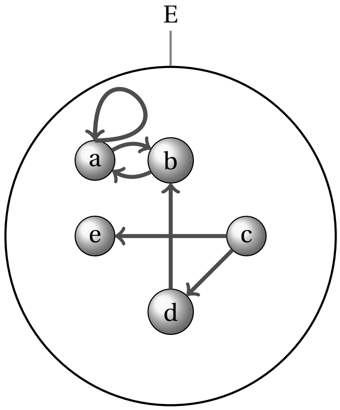
7 4 Inclusion, union, intersection et négation

Nous avons déjà défini ces concepts pour les relations binaires « quelconques » mais il est important de remarquer que la négation, l'union et l'intersection de relations binaires sur E est encore une relation binaire sur E. On dit que ces opérations sont fermées pour l'ensemble des relations binaires sur E ou que l'ensemble des relations binaires sur E est stable pour ces opérations ou encore que ce sont des opérations internes. Si la relation $\mathcal{S}$ est incluse (ou égale) à $\mathcal{R}$, on a donc $\mathcal{S} = \left(E, G_{\mathcal{S}}\right)$, $\mathcal{R} = \left(E, G_{\mathcal{R}}\right)$ avec $G_{\mathcal{S}} \subseteq G_R$, on dit alors que la relation $\mathcal{S}$ est « plus petite » que la relation $\mathcal{R}$ et $x\mathcal{S}y \Rightarrow x\mathcal{R}y$

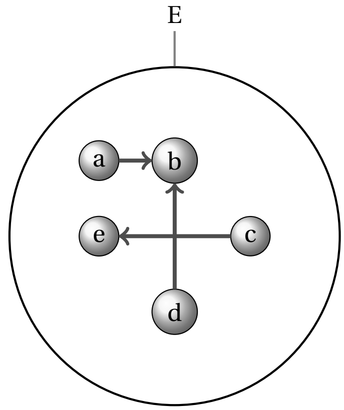
Reprenons la relation $\mathcal{R}$ définie par

$$\mathcal{R} = \left(E = \{a, b, c, d, e\}, G_{\mathcal{R}} = \{(a,a), (a,b), (b,a), (d,b), (c,d), (c,e)\}\right)$$

Pour obtenir une sous-relation, on « supprime » des flèches comme nous l'avons vu précédemment :



La relation $\mathcal{R}$



Une sous-relation de $\mathcal{R}$

Remarque 26

Il ne faut pas confondre une sous relation avec la restriction d'une relation, la restriction d'une relation s'obtient en « supprimant » des éléments de l'ensemble E (ensemble de départ) et une sous relation s'obtient en « supprimant » des flèches.

7 5 Composition

7 5 1 Rappels

Nous avons déjà défini la composition de deux relations binaires $\mathcal{R}$ et $\mathcal{S}$ et nous avons indiqué que le produit $\mathcal{S} \circ \mathcal{R}$ n'avait de sens que si l'ensemble d'arrivée de $\mathcal{R}$ était égal à l'ensemble de départ de $\mathcal{S}$. Si nous travaillons avec des relations sur le même ensemble E, cette condition sera toujours réalisée et la composition (on dit aussi le produit) de deux relations binaires sur E a toujours un sens.

Danger

Nous notons aussi la composition de deux relations binaires $\mathcal{R}$ et $\mathcal{S}$ par $\mathcal{R} \fatsemi \mathcal{S}$ ou $\mathcal{R}\mathcal{S}$.

7 5 2 Quelques propriétés

- La composition ou le produit de relations binaires sur l'ensemble E est une loi de composition interne dans l'ensemble des relations binaires sur E.
- Ce produit est associatif et il a pour élément neutre $\mathrm{I}d_\mathrm{E}$:

$$\mathcal{R} \fatsemi \mathrm{I}d_\mathrm{E} = \mathrm{I}d_\mathrm{E} \fatsemi \mathcal{R} = \mathcal{R}$$

- Si la relation $\mathcal{R}$ n'est pas la relation vide, on pose $\mathcal{R}^0 = \mathrm{I}d_\mathrm{E}$ sinon c'est la relation vide (de E dans E).

– k désignant un entier naturel, une définition récursive de $\mathcal{R}^k$ est la suivante :

$$i \in \mathbb{N}, \mathcal{R}^{i+1} = \mathcal{R}^i \mathbin{;} \mathcal{R} = \mathcal{R} \circ \mathcal{R}^i$$

Détaillons les premières puissances de $\mathcal{R}$:
$\mathcal{R}^2 = \mathcal{R} \mathbin{;} \mathcal{R}, \mathcal{R}^3 = \mathcal{R}^2 \mathbin{;} \mathcal{R} = (\mathcal{R} \mathbin{;} \mathcal{R}) \mathbin{;} \mathcal{R}$. Le produit (la composition) étant associatif, nous obtenons $\mathcal{R}^3 = \mathcal{R} \mathbin{;} (\mathcal{R} \mathbin{;} \mathcal{R})$ mais aussi $\mathcal{R}^3 = \mathcal{R} \mathbin{;} \mathcal{R} \mathbin{;} \mathcal{R}$ puisque l'associativité permet de se passer de parenthèses. De même

$$\mathcal{R}^4 = \mathcal{R}^3 \mathbin{;} \mathcal{R} = (\mathcal{R} \mathbin{;} \mathcal{R}.\mathcal{R}) \mathbin{;} \mathcal{R} = \mathcal{R} \mathbin{;} \mathcal{R} \mathbin{;} \mathcal{R} \mathbin{;} \mathcal{R}$$

etc.... On retiendra donc :

$$\mathcal{R}^k = \underbrace{\mathcal{R} \mathbin{;} \mathcal{R} \mathbin{;} \cdots \mathbin{;} \mathcal{R}}_{k \text{ fois}} = \underbrace{\mathcal{R} \circ \mathcal{R} \circ \cdots \circ \mathcal{R}}_{k \text{ fois}}$$

mais aussi

$$\mathcal{R}^{i+1} = \mathcal{R}^i \mathbin{;} \mathcal{R} = \mathcal{R} \mathbin{;} \mathcal{R}^i \text{ puisque}$$
$$(\mathcal{R} \mathbin{;} \mathcal{R} \mathbin{;} \cdots \mathbin{;} \mathcal{R}) \mathbin{;} \mathcal{R} = \mathcal{R} \mathbin{;} (\mathcal{R} \mathbin{;} \mathcal{R} \mathbin{;} \cdots \mathbin{;} \mathcal{R})$$

ainsi que

$$\mathcal{R}^{i+j} = \mathcal{R}^i \mathbin{;} \mathcal{R}^j = \mathcal{R}^j \mathbin{;} \mathcal{R}^i$$

On convient aussi de noter

$$\mathcal{R}^{-k} = \underbrace{\mathcal{R}^{-1} \circ \mathcal{R}^{-1} \circ \cdots \circ \mathcal{R}^{-1}}_{k \text{ fois}} = \left(\mathcal{R}^{-1}\right)^k$$

et on remarque que $\mathcal{R}^{-k} = \left(\mathcal{R}^{-1}\right)^k = \left(\mathcal{R}^k\right)^{-1}$.

Remarque 27

Il faut bien comprendre que si $x\mathcal{R}^k y$ alors il existe

$$u_1, u_2, \ldots, u_{k-1} \text{ éléments de E}$$

vérifiant

$$x\mathcal{R}u_1 \text{ et } u_1\mathcal{R}u_2 \text{ et } u_{21}\mathcal{R}u_3 \text{ et } \ldots \text{ et } u_{k-1}\mathcal{R}y$$

et l'on dit que y est un descendant de x ou que x est un ascendant de y.

– La composition est distributive pour l'union :

$$\begin{cases} \mathcal{R} \circ (\mathcal{S}_1 \cup \mathcal{S}_2) = (\mathcal{R} \circ \mathcal{S}_1) \cup (\mathcal{R} \circ \mathcal{S}_2) \\ (\mathcal{S}_1 \cup \mathcal{S}_2) \circ \mathcal{R} = (\mathcal{S}_1 \circ \mathcal{R}) \cup (\mathcal{S}_2 \circ \mathcal{R}) \end{cases}$$

– La composition est compatible avec l'inclusion. Si $\mathcal{R}$, $\mathcal{S}$ et $\mathcal{T}$ sont des relations binaires sur E, on a :

$$\mathcal{R} \subseteq \mathcal{S} \Rightarrow \mathcal{R} \circ \mathcal{T} \subseteq \mathcal{S} \circ \mathcal{T}$$
$$\mathcal{R} \subseteq \mathcal{S} \Rightarrow \mathcal{T} \circ \mathcal{R} \subseteq \mathcal{T} \circ \mathcal{S}$$

et

$$\mathcal{R} \subseteq \mathcal{S} \text{ et } \mathcal{T} \subseteq \mathcal{U} \Rightarrow (\mathcal{R} \circ \mathcal{T} \subseteq \mathcal{S} \circ \mathcal{U} \text{ et } \mathcal{T} \circ \mathcal{R} \subseteq \mathcal{U} \circ \mathcal{S})$$

– La relation $\mathcal{R}^+$ est la relation définie par :

$$\mathcal{R}^+ = \mathcal{R}^1 \cup \mathcal{R}^2 \cup \mathcal{R}^3 \cup \cdots$$

soit aussi :

$$\mathcal{R}^+ = \bigcup_{i=1}^{+\infty} \mathcal{R}^i = \bigcup_{i \in \mathbb{N}^*} \mathcal{R}^i$$

$\mathcal{R}^+$ est appelée la **fermeture transitive** de $\mathcal{R}$, nous verrons plus loin pourquoi.

Remarque 28

$x\,\mathcal{R}^+\,y$ équivaut à écrire qu'il existe une suite finie

$$(u_i)_{i \in \{0,1,2,\ldots,k\}}$$

d'éléments de E vérifiant

$$\begin{cases} u_0 = x, u_k = y \\ x\mathcal{R}u_1 \text{ et } u_1\mathcal{R}u_2 \text{ et } u_2\mathcal{R}u_3 \text{ et } \ldots \text{ et } u_{k-1}\mathcal{R}y \end{cases}$$

– La relation $\mathcal{R}^*$ est la relation définie par $\mathcal{R}^* = \mathrm{I}d_{\mathrm{E}} \cup \mathcal{R}^+$, c'est-à-dire

$$\mathcal{R}^* = \bigcup_{i=0}^{+\infty} \mathcal{R}^i = \bigcup_{i \in \mathbb{N}} \mathcal{R}^i$$

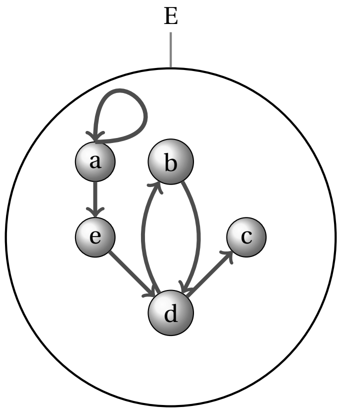
$\mathcal{R}^*$ est appelée la fermeture **réflexive-transitive** de $\mathcal{R}$.

Remarque 29

Si E est fini de cardinal n, le graphe $\mathrm{G}_{\mathcal{R}}$ d'une relation binaire $\mathcal{R}$ sur E est lui aussi fini puisque c'est une partie de $\mathrm{E} \times \mathrm{E}$. En conséquence le graphe $\mathrm{G}_{\mathcal{R}^i}$ de $\mathcal{R}^i$, qui est aussi une partie de $\mathrm{E} \times \mathrm{E}$, est fini. Comme il y a 2^{n^2} parties dans $\mathcal{P}(\mathrm{E} \times \mathrm{E})$, la suite $\left(\mathcal{R}^i\right)$ est forcément périodique à partir d'un certain rang, cela veut dire qu'il existe un entier naturel non nul minimum t et un rang minimum k tel qu'à partir du rang k on a pour tout $i \geq k$ $\mathcal{R}^{i+t} = \mathcal{R}^i$. On obtient alors

$$\mathcal{R}^* = \bigcup_{i=0}^{k+t-1} \mathcal{R}^i$$

Voyons un **exemple**. Considérons la relation $\mathcal{R}$ sur $\mathrm{E} = \{a, b, c, d, e\}$:



On vérifie que $\mathcal{R}^5 = \mathcal{R}^3$ et donc que $\mathcal{R}^3 = \mathcal{R}^5 = \mathcal{R}^7 = \mathcal{R}^9 = \cdots$ et $\mathcal{R}^4 = \mathcal{R}^6 = \mathcal{R}^8 = \mathcal{R}^{10} = \cdots$

Nous venons de définir les relations $\mathcal{R}^k$, $\mathcal{R}^+$ et $\mathcal{R}^*$; il nous faut maintenant expliquer comment on les détermine lorsque E est fini.

Nous admettrons le théorème suivant :

Théorème 1 - 5

Si E a pour cardinal n alors $\mathcal{R}^+ = \bigcup_{i=1}^{n} \mathcal{R}^i$ et $\mathcal{R}^* = \bigcup_{i=0}^{n-1} \mathcal{R}^i$.

Pour aller plus loin

Nous sommes maintenant en mesure de déterminer « facilement » les matrices booléennes de $\mathcal{R}^+$ et de $\mathcal{R}^*$, en effet, il nous suffit de traduire sous forme matricielle les résultats précédents. Si nous appelons M la matrice de $\mathcal{R}$, M est une matrice carrée d'ordre n, alors la matrice de $\mathcal{R}^+ = \bigcup_{i=1}^{n} \mathcal{R}^i$ est $\mathrm{S} = \sum_{i=1}^{n} \mathrm{M}^i$ et la matrice de $\mathcal{R}^*$ est $\mathrm{T} = \sum_{i=0}^{n-1} \mathrm{M}^i$ (rappel $\mathrm{M}^0 = \mathrm{I}_n$). Une méthode « pratique » (mais pénible à la main si n n'est pas petit) est la suivante, on considère la suite matricielle $(\mathrm{S}_i)_{i\in\{1,\ldots,n\}}$ définie par :

$$
\begin{aligned}
\mathrm{S}_1 &= \mathrm{M}\\
\mathrm{S}_2 &= \mathrm{M} + \mathrm{M}^2 = (\mathrm{I}_n + \mathrm{M}) \times \mathrm{M} = (\mathrm{I}_n + \mathrm{S}_1) \times \mathrm{M}\\
\mathrm{S}_3 &= \mathrm{M} + \mathrm{M}^2 + \mathrm{M}^3 = \left(\mathrm{I}_n + \mathrm{M} + \mathrm{M}^2\right) \times \mathrm{M} = (\mathrm{I}_n + \mathrm{S}_2) \times \mathrm{M}\\
&\ldots\\
\mathrm{S}_n &= \sum_{i=1}^{n} \mathrm{M}^i = \left(\sum_{i=0}^{n-1} \mathrm{M}^i\right) \times \mathrm{M} = (\mathrm{I}_n + \mathrm{S}_{n-1}) \times \mathrm{M}
\end{aligned}
$$

S_n donne S et $\mathrm{I}_n + \mathrm{S}_{n-1}$ donne T.

7 6 Fermeture d'une relation : du concret

Disons que vous gérer un réseau informatique avec des centres situés à Vertou, Saint Mars du Désert, Chavagne en Paillé, Guéméné Penfao et des lignes de câbles unidirectionnelles de Vertou vers Saint Mars, de Vertou vers Chavagne, de Chavagne vers Guéméné, de Guéméné vers Saint Mars. Si $\mathcal{R}$ est la relation qui contient le couple (a,b) s'il y a une ligne entre a et b, on voudrait savoir si on peut connecter deux centres donnés. Le chemin de Vertou vers Guéméné existe mais est indirect car il passe par Chavagne : la relation $\mathcal{R}$ n'est donc pas transitive car elle ne contient pas tous les couples pouvant se connecter. La fermeture transitive est en fait la plus petite relation transitive contenant $\mathcal{R}$. C'est concrètement la relation qui comprend tous les couples de centres pouvant être connectés.

On peut dans le même esprit s'occuper des fermetures symétrique, réflexive, réflexive-transitive, etc. Pour les fermetures réflexive et symétrique, c'est assez immédiat. Notre problème sera de trouver des algorithmes pour la fermeture transitive car c'est moins simple.

Exemple 1.7

Essayez de déterminer la fermeture transitive de $\mathcal{R} = \{(1,3),(1,4),(2,1),(3,2)\}$ sur l'ensemble $\mathcal{E} = \{1,2,3,4\}$.

7 7 Chemin

Nous parlerons l'an prochain de graphes directionnels et de chemine sur ces graphes. Grosso modo, un graphe directionnel, c'est des sommets reliés par des flèches et un chemin c'est un parcours en suivant ces flèches.

Nous pouvons reprendre l'idée pour une relation :

Définition 1 - 21

Soit $\mathcal{R}$ une relation. Il existe un **chemin** de a vers b dans $\mathcal{R}$ s'il existe une suite d'éléments $x_1, x_2, x_3, \ldots, x_{n-1}$ telle que $(a,x_1),(x_1,x_2),(x_2,x_3),\ldots,(x_{n-1},b)$ appartiennent à $\mathcal{R}$. Ce chemin est de **longueur** n.

En reprenant la relation représentée sur la figure 1.29 page ci-contre, il existe un chemin (et même plusieurs !) de a vers c, passant par exemple par a, a, a, e, d, b, d, c.

Le théorème suivant nous sera très utile :

Théorème 1 - 6

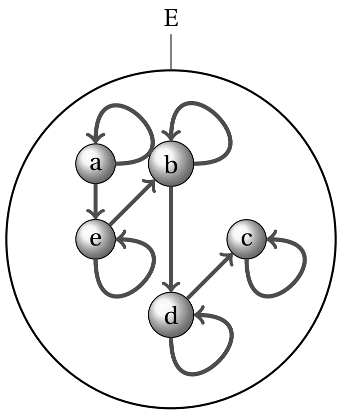
Soit $\mathcal{R}$ une relation sur un ensemble et n un entier naturel. Il existe un chemin de longueur n de a vers b si, et seulement si, $(a,b) \in \mathcal{R}^n$.

La démonstration s'effectue par récurrence...et est laissée au lecteur attentif.

7 8 Propriétés particulières

Soit $\mathcal{R} = (\mathrm{E}, \mathrm{G}_{\mathcal{R}})$ avec $\mathrm{G}_{\mathcal{R}} \neq \emptyset$ et R sa matrice booléenne.

1. $\mathcal{R}$ est dite **totale à gauche** si, et seulement si, pour tout x de E, il existe au moins un y de E vérifiant $x\mathcal{R}y$, une relation totale à gauche est une relation « totale » en ce sens que son domaine est l'ensemble E.
2. $\mathcal{R}$ est dite **totale à droite** si, et seulement si, pour tout x de E, il existe au moins un y de E vérifiant $y\mathcal{R}x$, le codomaine de $\mathcal{R}$ est E.
3. $\mathcal{R}$ est **réflexive** si, et seulement si, pour tout x de E on a $x\mathcal{R}x$. En d'autres termes $\mathcal{R}$ est réflexive si, et seulement si, $\mathrm{G}_{\mathcal{R}}$ contient Δ la diagonale de $\mathrm{E}\times\mathrm{E}$, $\Delta = \{(x,x) \mid x \in \mathrm{E}\}$.



Relation réflexive

Visuellement (diagramme sagittal), une relation est réflexive s'il y a une boucle à chaque élément.

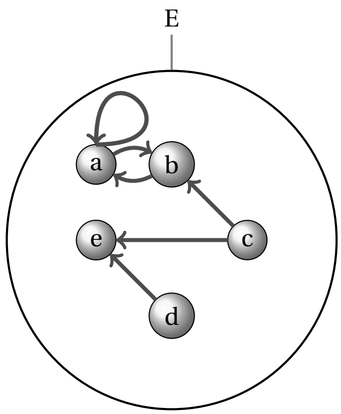
Pour aller plus loin

Matriciellement, $\mathcal{R}$ est réflexive si, et seulement si, les éléments diagonaux de R sont tous égaux à 1 ce qui équivaut à écrire que $\mathrm{I}_n + \mathrm{R} = \mathrm{R}$ et donc $\mathcal{R} \cup \mathrm{Id}_{\mathrm{E}} = \mathcal{R}$.

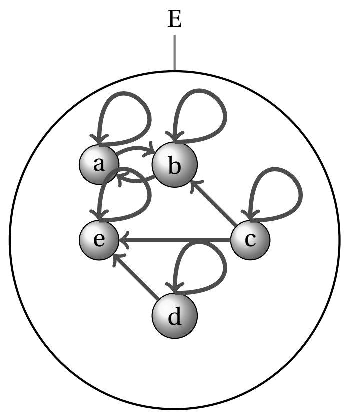
Théorème 1 - 7

Si $\mathcal{R}$ est réflexive alors $\mathcal{R}^k$ est réflexive.

La **fermeture réflexive** d'une relation quelconque $\mathcal{R}$ sur E est la relation dont le graphe est $\mathrm{G}_{\mathcal{R}} \cup \Delta$. C'est la plus petite relation binaire sur E (au sens de l'inclusion) qui contient $\mathcal{R}$. Elle s'obtient très facilement, il suffit de « rajouter » (au sens de l'union) au graphe de $\mathcal{R}$, la diagonale de $\mathrm{E} \times \mathrm{E}$; cela revient à mettre une boucle, s'il n'y en avait pas déjà, à chaque élément du diagramme sagittal et à ajouter I_n, la matrice unité d'ordre n, à la matrice booléenne de $\mathcal{R}$.



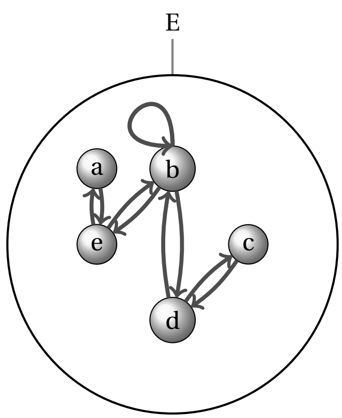
La relation $\mathcal{R}$



La fermeture réflexive de $\mathcal{R}$

4. $\mathcal{R}$ est **irréflexive**[r] si, et seulement si, il n'existe pas $x \in \mathrm{E}$ vérifiant $x\mathcal{R}x$. On peut aussi exprimer cette propriété en écrivant que si on a $x\mathcal{R}y$ alors on a forcément $x \neq y$. Ne pas confondre une relation irréflexive avec une relation non réflexive : une relation n'est pas réflexive dès qu'il existe au moins un x de E ne vérifiant pas $x\mathcal{R}x$ alors que pour une relation irréflexive on n'a jamais $x\mathcal{R}x$.

5. $\mathcal{R}$ est **symétrique** si, et seulement si, à chaque fois que l'on a $x\mathcal{R}y$ on a aussi $y\mathcal{R}x$. Si nous traduisons $x\mathcal{R}y$ par « on peut aller de x à y » alors $\mathcal{R}$ est symétrique si à chaque fois qu'il y a un « aller » de x à y, il y a aussi un « retour ».



Relation symétrique

Recherche

Mathémator : Considérons par exemple la relation :

Train = {(Nantes,Paris),(Paris,Nantes),(Nantes,Vertou),(Vertou,Nantes),
(Paris,Vertou),(Vertou,Paris),(Paris,Sucé),(Sucé,Paris)}

Est-elle symétrique ?

r. On utilise aussi le mot « antiréflexif ».

Pour aller plus loin

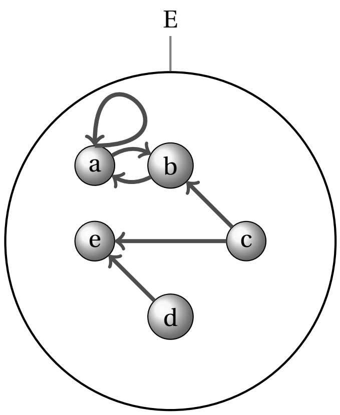
Matriciellement, $\mathcal{R}$ est symétrique si, et seulement si, sa matrice R est symétrique, c'est-à-dire ${}^t\mathrm{R} = \mathrm{R}$.

On peut rajouter quelques théorèmes utiles pour le plaisir :

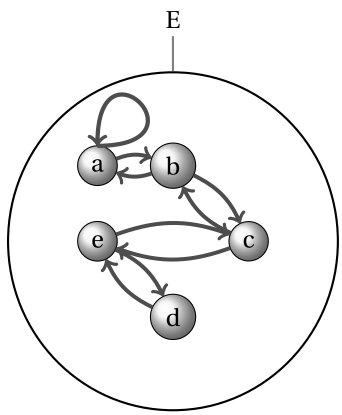
Théorème 1 - 8

- L'union et l'intersection de relations symétriques sont des relations symétriques.
- Si $\mathcal{R}$ est symétrique alors $\mathcal{R}^k$ est symétrique.
- Si $\mathcal{R}$ est une relation quelconque alors $\mathcal{R}\cup\mathcal{R}^{-1}$ est une relation symétrique.

La **fermeture symétrique** de la relation $\mathcal{R} = (\mathrm{E}, \mathrm{G}_{\mathcal{R}})$ est la plus petite relation symétrique dont le graphe contient $\mathrm{G}_{\mathcal{R}}$. Il suffit de « doubler » les flèches du diagramme sagittal.



La relation $\mathcal{R}$



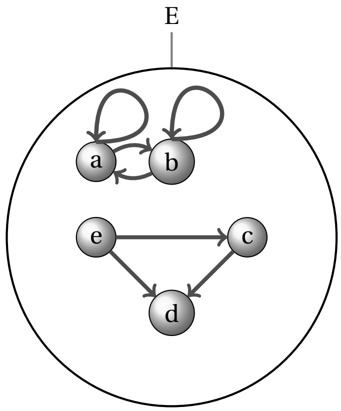
La fermeture symétrique de $\mathcal{R}$

Pour aller plus loin

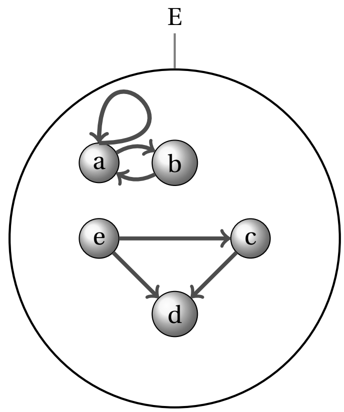
On l'obtient très facilement, si R est la matrice booléenne de $\mathcal{R}$. On « rajoute » le minimum de « 1 » pour que la matrice obtenue soit symétrique. La matrice de la fermeture symérique de $\mathcal{R}$ est donc égale à $\mathrm{R} + {}^t\mathrm{R}$, c'est la matrice de $\mathcal{R}\cup\mathcal{R}^{-1}$.

6. $\mathcal{R}$ est **antisymétrique** si, et seulement si, à chaque fois que l'on a $x\mathcal{R}y$, avec x différent de y, on n'a pas $y\mathcal{R}x$. Cela équivaut à écrire que si on a simultanément $x\mathcal{R}y$ et $y\mathcal{R}x$, on a forcément $x = y$. Le diagramme sagittal ne possède aucun « aller et retour ».

7. $\mathcal{R}$ est **transitive** si, et seulement si, à chaque fois que l'on a $x\mathcal{R}y$ et $y\mathcal{R}z$, on a aussi $x\mathcal{R}z$. Si « on peut aller de x à z en passant par y, on doit pouvoir aller directement de x à z ».



Relation transitive



Relation non transitive

Recherche

Mathémator : Considérons à nouveau la relation :

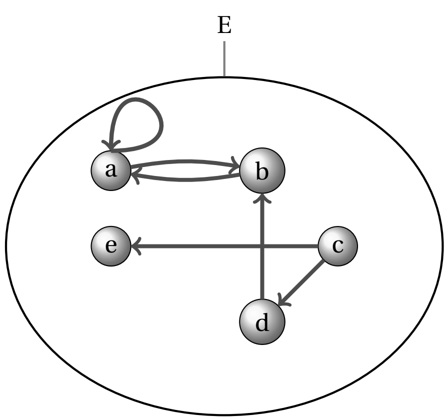
$$\text{Train} = \{(\text{Nantes},\text{Paris}),(\text{Paris},\text{Nantes}),(\text{Nantes},\text{Vertou}),(\text{Vertou},\text{Nantes}),\\ (\text{Paris},\text{Vertou}),(\text{Vertou},\text{Paris}),(\text{Paris},\text{Sucé}),(\text{Sucé},\text{Paris})\}$$

Est-elle transitive ?

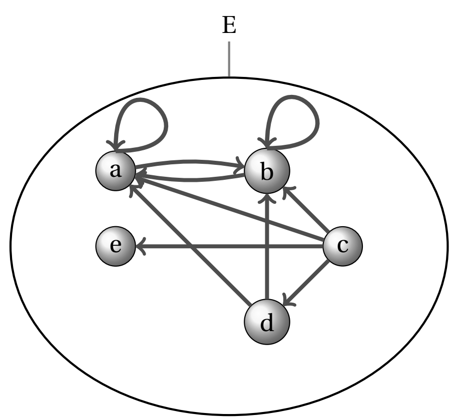
Théorème 1 - 9

- $\mathcal{R}$ transitive $\Leftrightarrow \mathcal{R}^2 \subseteq \mathcal{R}$.
- $\mathcal{R}$ réflexive et transitive $\Rightarrow \mathcal{R}^2 = \mathcal{R}$.
- $\mathcal{R}$ est transitive si, et seulement si, $\mathcal{R}^n \subseteq \mathcal{R}$ pour tout entier naturel non nul n.

La **fermeture transitive** de la relation $\mathcal{R} = (\mathrm{E}, \mathrm{G}_{\mathcal{R}})$, est la plus petite (au sens de l'inclusion) relation transitive sur E dont le graphe contient $\mathrm{G}_{\mathcal{R}}$.



Relation



Fermeture transitive de la relation

7 9 Fermeture transitive et chemin

En fait, trouver la fermeture transitive d'une relation, c'est déterminer les couples reliés par un chemin.

Définition 1 - 22

Soit $\mathcal{R}$ une relation sur un ensemble. La relation de connexion $\mathcal{R}^+$ contient tous les couples (a,b) tels qu'il existe un chemin sur $\mathcal{R}$ de longueur non nulle allant de a vers b.

Maintenant, souvenons-nous que $\mathcal{R}^n$ est formé des couples (a,b) tels qu'il existe un chemin de longueur n de a vers b. Il en découle que $\mathcal{R}^+$ est en fait la réunion de tous les $\mathcal{R}^n$:

Théorème 1 - 10

$$\mathcal{R}^+ = \bigcup_{n\in\mathbb{N}^*} \mathcal{R}^n$$

Recherche

Par exemple, si $\mathcal{R}$ est la relation sur l'ensemble des département français qui contient (a,b) si les départements a et b ont une frontière commune, quelle est $\mathcal{R}^n$? $\mathcal{R}^+$?

Nous en arrivons au théorème important suivant :

Théorème 1 - 11

La fermeture transitive d'une relation $\mathcal{R}$ est égale à $\mathcal{R}^+$.

Pour les curieux, on peut survoler une petite démonstration de ce résultat.

Il est assez simple de montrer que $\mathcal{R}^+$ est transitive (faites-le...) et que $\mathcal{R}^+$ contient $\mathcal{R}$.

Maintenant, il faudrait montrer que n'importe quelle relation $\mathcal{S}$ transitive qui contient $\mathcal{R}$ contient aussi $\mathcal{R}^+$.

Comme $\mathcal{S}$ est transitive, alors $\mathcal{S}^n$ aussi et $\mathcal{S}^n \subseteq \mathcal{S}$.

Or $\mathcal{S}^+ = \bigcup_{n\in\mathbb{N}^*} \mathcal{S}^n$ donc $\mathcal{S}^+ \subseteq \mathcal{S}$. Or $\mathcal{R} \subseteq \mathcal{S}$ donc $\mathcal{R}^+ \subseteq \mathcal{S}^+$.

Finalement $\mathcal{R}^+ \subseteq \mathcal{S}^+ \subseteq \mathcal{S}$ ce qui achève notre démonstration.

Bon, on sait ce que c'est que la fermeture transitive : il reste à savoir comment la déterminer concrètement...

7 9 1 Méthode matricielle pour déterminer la fermeture transitive

La fermeture réflexive-transitive de $\mathcal{R}$ est $\mathcal{R}^* = \mathrm{I}d_{\mathrm{E}} \cup \mathcal{R}^+$ et sa matrice est $\sum_{i=0}^{n-1} \mathrm{M}^i$.

Nous allons présenter une autre méthode pour déterminer la fermeture transitive de la relation $\mathcal{R}$ sur $\mathrm{E} = \{e_1, e_2, ..., e_n\}$, cette méthode utilise le vocabulaire de la théorie de graphes (pour ce qui concerne la démonstration).

L'idée est la suivante : on va prendre les sommets e_i un par un et relier les ascendants de e_i à tous les descendants de e_i s'ils ne l'étaient déjà. Nous notons M_0 la matrice booléenne de $\mathcal{R}$ et θ_i l'opérateur qui consiste à ajouter, au sens de l'addition booléenne, la $i^{ème}$ ligne de M_i à toute ligne de M_i possédant un 1 en colonne numéro i ; le résultat se notant $\mathrm{M}_i = \theta_i\left(\mathrm{M}_{i-1}\right)$. La matrice M_n donne alors la matrice de la fermeture transitive de $\mathcal{R}$.

Reprenons l'exemple de la figure 1.38 page 91.

Sa matrice d'incidence est $\mathrm{M} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$.

Appliquons θ_1, nous allons ajouter (au sens booléen) la ligne numéro 1 sur toute ligne possédant un 1 en colonne numéro 1, seule la deuxième ligne est concernée, on obtient $\mathrm{M}_1 = \theta_1\left(\mathrm{M}\right) = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$. Appliquons maintenant θ_2 à M_1, nous allons ajouter la ligne numéro 2 à toute ligne possédant un 1 en colonne numéro 2, les lignes 1, 2 et 4 sont concernées[s]. Nous obtenons $\theta_2\left(\mathrm{M}_1\right) = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ \mathbf{1} & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$. Aucune ligne n'a de 1 en colonne 3, donc $\theta_3\left(\mathrm{M}_2\right) = \mathrm{M}_3 = \mathrm{M}_2$. La ligne 3 a un 1 en colonne 4, $\theta_4\left(\mathrm{M}_3\right) = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ \mathbf{1} & \mathbf{1} & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} = \mathrm{M}_4$

s. Ajouter (en calcul booléen) la ligne numéro i à la ligne numéro i ne la modifie pas.

et θ_5 ne changeant rien, la matrice de la fermeture transitive est $M_5 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$

qui nous donne le graphe de la figure 1.39 page 91

8 Relations d'équivalence

Tous les étudiants d'Info s'inscrivent pour un camp d'été de maths auprès de leur professeur adoré.

Comme il y a beaucoup d'étudiants, on décide d'inscrire les étudiants dont le nom de famille commence par une lettre comprise entre A et G le lundi, ceux dont le nom commence par une lettre entre H et N le mardi et les autres le mercredi.

Soit $\mathcal{R}$ la relation définie sur l'ensemble $\mathcal{E}$ des étudiants de l'IUT qui contient (x, y) si x et y se sont inscrits le même jour.

On vérifie aisément que cette relation est réflexive, symétrique et transitive.

On remarque surtout que $\mathcal{R}$ divise l'ensemble $\mathcal{E}$ des étudiants en trois classes distinctes. Il suffit de savoir dans quel classe se trouve l'étudiant pour savoir quel jour il s'inscrira, sans avoir besoin de connaître son identité : gain de temps...

Ce genre de relation réflexive, symétrique et transitive s'appelle une **relation d'équivalence**.

Définition 1 - 23

$\mathcal{R} = \left(\mathrm{E}, \mathrm{G}_{\mathcal{R}}\right)$, où E est un ensemble non vide, est une **relation d'équivalence** si, et seulement si, $\mathcal{R}$ est

Réflexive et Symétrique et Transitive (R.S.T.)

x désignant un élément de E, la **classe d'équivalence** de x est l'ensemble

$$cl(x) = \overline{x} = \left\{y \in \mathrm{E} \mid x\mathcal{R}y\right\} = \left\{y \in \mathrm{E} \mid y\mathcal{R}x\right\}$$

Beaucoup d'autres notations sont utilisées : $\overline{x} = cl(x) = \widehat{x} = \widetilde{x} = [x]_{\mathcal{R}}$ ou encore $\mathring{x} = \check{x} = \cdots$.

Propriété 1 - 2

La classe de x, $\overline{x}$, ne peut être un ensemble vide.

En effet, $\mathcal{R}$ étant réflexive, on a pour tout x de E, $x\mathcal{R}x$ et, par conséquent, $\overline{x}$ contient au moins un élément qui est x.

Propriété 1 - 3

$$x\mathcal{R}y \Leftrightarrow \overline{x} = \overline{y}.$$

1. Supposons tout d'abord que $x\mathcal{R}y$ et choisissons un élément $z \in \overline{y}$; nous avons alors $y\mathcal{R}z$ et comme $x\mathcal{R}y$ nous obtenons $x\mathcal{R}z$ qui prouve que $z \in \overline{x}$. Nous venons de démontrer que $\overline{y} \subseteq \overline{x}$. En permutant les rôles de x et y (ne pas oublier que $\mathcal{R}$ est symétrique) on obtient $\overline{x} \subseteq \overline{y}$ et, par conséquent, $\overline{x} = \overline{y}$.

2. Supposons maintenant que $\overline{x} = \overline{y}$, nous savons que $y \in \overline{y}$ et donc que $y \in \overline{x}$; on en déduit que $x\mathcal{R}y$.

Propriété 1 - 4

$\overline{x} \cap \overline{y} = \emptyset \Leftrightarrow x$ n'est pas en relation avec y.

Nous venons d'établir que $x\mathcal{R}y \Leftrightarrow \overline{x} = \overline{y}$. En conséquence, si $x\mathcal{R}y$, il est impossible que $\overline{x} \cap \overline{y} = \emptyset$ puisque $\overline{x} = \overline{y}$ et qu'aucune classe n'est vide. Nous venons de prouver que $\overline{x} \cap \overline{y} = \emptyset \Rightarrow x\overline{\mathcal{R}}y$. Réciproquement, supposons que $\overline{x} \cap \overline{y} \neq \emptyset$. La classe de x et la classe de y ont donc au moins un élément en commun z qui vérifie $x\mathcal{R}z$ et $z\mathcal{R}y$ et, du coup, on a forcément $x\mathcal{R}y$. Nous venons de démontrer que $\overline{x} \cap \overline{y} \neq \emptyset \Rightarrow x\mathcal{R}y$ donc aussi $x\overline{\mathcal{R}}y \Rightarrow \overline{x} \cap \overline{y} = \emptyset$.

Propriété 1 - 5

L'ensemble des classes d'équivalences, noté $\mathrm{E}/\mathcal{R}$, est une partition de E.

Nous n'allons détailler ce résultat que lorsque le nombre de classes est fini : notons $\mathrm{C}_1, \mathrm{C}_2, \ldots, \mathrm{C}_k$ les différentes classes d'équivalence. Nous venons de prouver que $\mathrm{C}_i \cap \mathrm{C}_j = \emptyset$ si $i \neq j$. Maintenant choisissons un élément quelconque $e \in \mathrm{E}$, nous savons que $e \in \overline{e}$ et la classe de e est forcément l'une des classes C_i. Ceci prouve que $\displaystyle\bigcup_{i=1}^{k} \mathrm{C}_i = \mathrm{E}$

Propriété 1 - 6

Toute partition de E définit une relation d'équivalence sur E.

À vous de trouver une démonstration si vous avez un peu compris ce qui se passe...

9 Structures d'ordre

9 1 Relation d'ordre

Définition 1 - 24

La relation $\mathcal{R} = (\mathrm{E}, \mathrm{G})$ est une **relation d'ordre** (ordre large) si, et seulement si, $\mathcal{R}$ est

Réflexive et Antisymétrique et Transitive (R.A.T.)

et on vérifie immédiatement que

$$\mathcal{R} \text{ relation d'ordre} \Leftrightarrow \mathcal{R}^{-1} \text{ relation d'ordre}$$

Une relation d'ordre est dite **totale** si, et seulement si, pour tout couple (x, y) de E on a soit $x\mathcal{R}y$, soit $y\mathcal{R}x$. Cela signifie que deux éléments quelconques sont toujours « comparables ». Si la relation d'ordre n'est pas totale on dit qu'elle est **partielle** et, dans ce cas, il existe au moins deux éléments distincts de E qui ne sont pas comparables.
La relation $\mathcal{R} = (\mathrm{E}, \mathrm{G})$ est une relation d'**ordre strict** si, et seulement si, $\mathcal{R}$ est

Irréflexive et Antisymétrique et Transitive

En général une relation d'ordre (large) est notée par $\leq$ ou par $\preceq$ ou par $\leqslant$ et une relation d'ordre strict est notée par $<$ ou par $\prec$.

La relation réciproque de la relation d'ordre $\leqslant$ est notée $\geqslant$: $x \leqslant y \Leftrightarrow y \geqslant x$ et il est bien entendu que l'on peut utiliser à loisir, l'une ou l'autre.

Théorème 1 - 12

$$\mathcal{R} \text{ est une relation d'ordre} \Leftrightarrow \begin{cases} \mathcal{R} \cap \mathcal{R}^{-1} = \mathrm{I}d_{\mathrm{E}} \\ \mathcal{R} = \mathcal{R}^2 = \mathcal{R}^* \end{cases}$$

Pourquoi ?...

9 2 Ensembles ordonnés

Définition 1 - 25

Un ensemble E est dit ordonné par la relation $\mathcal{R}$ si $\mathcal{R}$ est une relation binaire sur E et si $\mathcal{R}$ est une relation d'ordre. Un **ensemble ordonné** se présente comme le couple $(\mathrm{E}, \mathcal{R})$ où $\mathcal{R}$ est une relation d'ordre sur E. On dit que l'ensemble ordonné $(\mathrm{E}, \mathcal{R})$ est totalement ordonné si $\mathcal{R}$ est une relation d'ordre total.

Attention ! Un même ensemble peut être muni de plusieurs relations d'ordre différentes, si $\leqslant_1$ et $\leqslant_2$ sont deux relations d'ordre différentes alors les ensembles ordonnés $(\mathrm{E}, \leqslant_1)$ et $(\mathrm{E}, \leqslant_2)$ sont des ensembles ordonnés différents.

Exemple 1.8

Montrer par exemple que la relation d'inclusion $\subseteq$ est une relation d'ordre (de quelle nature ?) sur l'ensemble des parties d'un ensemble donné E.
Que pensez-vous de l'ensemble $\mathbb{Z}^+$ muni de la relation « divise » ?

À retenir

En fait, on peut montrer que le principe de récurrence s'applique sur tout ensemble bien ordonné.

9 3 Ordre lexicographique

Comment sont rangés les mots dans un dictionnaire ? C'est une des manière de ranger des éléments d'un produit cartésien (comment le définir ?). Y en a-t-il d'autres possibles ?

9 4 Diagramme de Hasse

Dresser un diagramme sagittal peut s'avérer parfois pénible : il y a trop de flèches dans tous les sens...Nous allons voir un moyen de visualiser plus nettement la situation d'ensembles ordonnés. Nous aurons besoin tout d'abord de préciser les notions de prédécesseur et de successeur.

Définition 1 - 26

On appelle éléments consécutifs de l'ensemble ordonné $(\mathrm{E}, \leq)$ deux éléments a et b qui vérifient

$$\begin{cases} a < b \\ a \leqslant c \leqslant b \Rightarrow a = c \text{ ou } b = c \end{cases}$$

a est un prédécesseur (immédiat) de b ou b est un successeur (immédiat) de a.

Tout ça pour dire que si a et b sont consécutifs, il n'y a personne entre eux, ils sont différents et l'un est plus grand que l'autre.

Revenons à nos ensembles ordonnés : pour ne pas avoir trop de flèches, on convient de ne relier x à y que si x est un prédécesseur de y et on place x sous y. On obtient alors un **diagramme de Hasse**.

En fait, il s'agit d'un diagramme sagittal où on élimine les boucles puisqu'on sait que la relation est réflexive. On élimine aussi les « raccourcis » : s'il y a une flèche de a vers b , de b vers c et de a vers c, on élimine la dernière puisqu'on sait que la relation est transitive. Enfin, on n'a pas besoin de flèches car on « pointe vers le haut ».

Considérons par exemple l'ensemble $\mathcal{E} = \{2, 3, 6, 7, 8, 9, 12, 18\}$ et l'ordre partiel $\{(a, b) \mid a \text{ divise } b\}$.

Le diagramme de HASSE correspondant est :

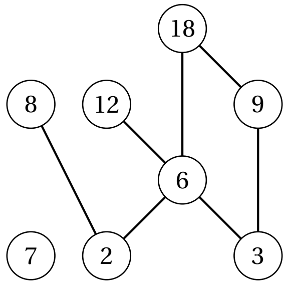


Diagramme de HASSE de $\{\{2,3,6,7,8,9,12,18\},|\}$

Voici un autre exemple pour $\{\mathcal{P}(\{a,b,c\}),\subseteq\}$:

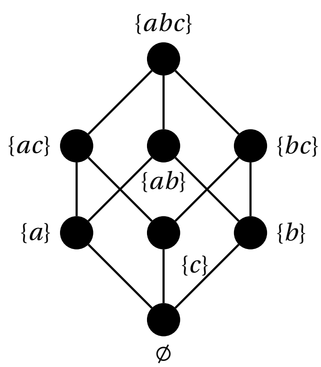


Diagramme de HASSE de $\{\mathcal{P}(\{a,b,c\}),\subseteq\}$

9 5 Éléments remarquables

Dans tout ce qui suit $(\mathrm{E},\leqslant)$ est un ensemble ordonné et A est une partie de E.

Définition 1 - 27

- On dit que la partie A est **majorée** par $u \in \mathrm{E}$ si, et seulement si, on a :

  $$\text{pour tout } x \text{ de A}, x \leqslant u$$

- On dit que la partie A est **minorée** par $v \in \mathrm{E}$ si, et seulement si, on a :

  $$\text{pour tout } x \text{ de A}, v \leqslant x$$

Définition 1 - 28

On dit que g est un **plus grand élément** (ou élément maximum) de A si, et seulement si,

$$g \in \mathrm{A} \text{ et } \forall x \in \mathrm{A}, x \leq g$$

Si g existe, il est unique et on ne doit pas parler d'un plus grand él ément de A mais du plus grand élément de A.

Démontrons ce résultat : pour cela supposons que g et g' sont deux plus grands éléments de A, nous avons alors

$$\begin{aligned} \forall x &\in \mathrm{A}, x \leq g \text{ donc } g' \leq g \\ \forall y &\in \mathrm{A}, y \leq g' \text{ donc } g \leq g' \end{aligned}$$

L'antisymétrie de $\leq$ permet alors de conclure $g = g'$.

Le plus grand élément de A (s'il existe) est noté Max(A) et c'est aussi évidemment le plus petit majorant de A.

Définition 1 - 29

On dit que p est un **plus petit élément** (ou élément minimum) de A si, et seulement si,

$$p \in \mathrm{A} \text{ et } \forall x \in \mathrm{A}, p \leq x$$

Si p existe, il est unique et on ne doit pas parler d'un plus petit élément de A mais du plus petit élément de A.

Le plus petit élément de A (s'il existe) est noté Min(A) et c'est alors le plus grand minorant de A.

Définition 1 - 30

Considérons $\mathcal{G}$ l'ensemble des majorants de A. Si $\mathcal{G}$ admet un plus petit élément s c'est la **borne supérieure** de A.

Bien remarquer que s n'existe pas toujours et que s'il existe, ce n'est pas forcément un élément de A ; par contre si A admet un plus grand élément c'est sa **borne supérieure**. La borne supérieure de A dans E est notée $\mathrm{Sup}_{\mathrm{E}}(\mathrm{A})$ ou Sup(A).

Définition 1 - 31

Considérons $\mathcal{P}$ l'ensemble des minorants de A. Si $\mathcal{P}$ admet un plus grand élément i c'est la **borne inférieure** de A.

Bien remarquer que i n'existe pas toujours et que s'il existe, ce n'est pas forcément un élément de A ; par contre si A admet un plus petit élément c'est sa **borne inférieure**. La borne inférieure de A dans E est notée $\mathrm{Inf}_{\mathrm{E}}(\mathrm{A})$ ou $\mathrm{Inf}(\mathrm{A})$.

Définition 1 - 32

$a \in \mathrm{A}$, a est **maximal** dans A s'il n'existe pas d'élément $x \in \mathrm{A}$ vérifiant $x \neq a$ et $a \leq x$.
$\alpha \in \mathrm{A}$, α est **minimal** dans A s'il n'existe pas d'élément $x \in \mathrm{A}$ vérifiant $x \neq \alpha$ et $x \leq \alpha$.

Si A admet un plus grand élément, ce plus grand élément est maximal et c'est le seul.

Si A admet un plus petit élément, ce plus petit élément est minimal et c'est le seul.

À retenir

Lorsque l'on peut représenter l'ensemble ordonné $(\mathrm{E}, \leq)$ à l'aide d'un diagramme de HASSE, on voit apparaître les éléments minimaux ou maximaux éventuels de E ainsi que les bornes ou é léments extrémaux éventuels de toute partie de E.

Observons par exemple le diagramme de la figure 1.40 page 99. L'ensemble $\mathcal{E}$ ne possède pas de plus grand élément ni de plus petit élément.

Cependant, 8, 12, 18 et 7 sont les éléments maximaux et 2, 3 et 7 sont les éléments minimaux.

La partie $\mathrm{W} = \{8, 12\}$ de E n'admet pas de majorant, il n'y a pas dans E d'élément simultanément « plus grand ou égal » à 8 et 12. Il faut, ici, entendre « plus grand ou égal que » comme « être un multiple de » ! W admet un unique minorant dans E, c'est 2, qui divise simultanément 8 et 12 ; 2 étant le « plus grand » des minorants, c'est la borne inférieure de W.

La partie $\mathrm{V} = \{2, 3, 6\}$ admet 3 majorants dans E, : ce sont 6, 12 et 18 ; 6 est la borne supérieure de V, c'est aussi le plus grand élément de V.

Observons maintenant le diagramme de HASSE de la figure 1.41 page 99.

Le plus petit élément est l'ensemble vide car $\emptyset \subseteq \mathrm{A}$ pour tout partie A de $\mathcal{E} = \{a, b, c\}$.

Le plus grand élément est $\mathcal{E}$ car toute partie A de $\mathcal{E}$ est incluse dans $\mathcal{E}$.

9 6 Ensemble bien ordonné

Définition 1 - 33

$(\mathrm{E}, \leqslant)$ est un **ensemble BIEN ordonné** si $\leqslant$ est un ordre total et si tout sous-ensemble non vide de E contient un plus petit élément.

Est-ce que $(\mathbb{Z}, \leqslant)$ est bien ordonné ?

10 Un peu de dénombrement

Dans cette section, il sera utile de se remémorer ce qu'est le **cardinal** d'un ensemble (cf section 1.3.9 page 36).

10 1 Détour historique

Mathémator : Nous allons être amenés à travailler sur des ensembles dénombrables. Nous étudions pour l'instant les mathématiques *discrètes* avant de survoler un peu de mathématiques *continues*. Nous avons déjà parlé de cette distinction.

Recentrons-nous sur les ensembles : on parle également d'ensembles discrets et continus.

Hihutix: Pouvez-vous être plus explicite ?

Mathémator : Premier cas : l'ensemble contient un nombre fini de valeurs, par exemple $\{0,1\}$.

Deuxième cas : l'ensemble est infini, mais on peut lister ses éléments, leur attribuer un rang. On peut donc écrire ces valeurs sous la forme $v_1, v_2, \cdots, v_n, \cdots$. L'ensemble discret le plus « naturel » est l'ensemble $\mathbb{N}$: $v_1 = 1, v_2 = 2, v_3 = 3\cdots$. En connaissez vous d'autres ?

Hihutix: Tout simplement des parties de $\mathbb{N}$: l'ensemble des entiers pairs, des entiers multiples de 32 etc.

Mathémator : En effet, il y a le premier entier pair, le deuxième, etc. Tiens, pour rigoler : y a-t-il plus d'entiers que de multiples de 32 ?

Hihutix: Oui, évidemment, pourquoi cette question ?

Mathémator : Parce que la réponse n'est pas aussi évidente. En effet, chaque multiple de 32 peut être mis en correspondance avec chacun des éléments de $\mathbb{N}$: $v_1 = 32, v_2 = 64, \cdots, v_n = 32n, \cdots$. Il y aurait donc « autant » d'entiers multiples de 32 que d'entiers tout court ! Plus fort : on peut aussi montrer que l'ensemble $\mathbb{Q}$ est dénombrable, et donc qu'il y a « autant » de rationnels que d'entiers, alors qu'on vous a appris que l'ensemble $\mathbb{N}$ était strictement inclus dans $\mathbb{Q}$! Mais nous abordons des notions extrêmement complexes qui débordent largement notre cours.

Hihutix: Dans ces conditions, je suppose qu'il y a autant de nombres réels que d'entiers et donc tout ensemble est dénombrable : il y a le premier réel, puis le deuxième, etc.

Mathémator : Bon, je suis allé trop vite et de manière trop vague. J'ai précisé qu'on pouvait montrer que $\mathbb{Q}$ était dénombrable. Eh bien allons-y ! L'idée est toute simple : un rationnel peut être représenté par un couple d'entier. Par exemple 2/3 sera représenté par le couple

(2,3). Dans un repère du plan, un rationnel sera donc un point à coordonnées entière et $\mathbb{Q}$ sera représenté par l'ensemble des points à coordonnées entières. Prenez une feuille mon petit Téhessix et représentez quelques-uns de ces points. Et maintenant, un petit jeu qui me rappellera mes folles après-midis à dévorer Pif-gadget : reliez par un trait les points suivants

$$(0,0)-(1,0)-(0,1)-(0,2)-(1,1)-(2,0)-(3,0)-(2,1)-(1,2)-(0,3)-(0,4)-\cdots$$

Nous allons donc pouvoir « numéroter » chaque rationnel (1/2 porte par exemple le dossard 9) en prenant soin de « sauter » le couple $(2,4)$ par exemple car il représente le même rationnel que le couple $(1,2)$. L'ensemble $\mathbb{Q}$ va donc pouvoir être mis en correspondance, terme à terme, avec l'ensemble $\mathbb{N}$, donc il y a « autant » de rationnels que d'entiers ! Faites un petit dessin pour l'illustrer.

Hihutix: Excusez-moi, mais si 1/2 porte déjà le numéro 9, on risque de ne pas avoir assez d'entiers pour les numéroter tous.

Mathémator : N'oubliez pas cher disciple que nous avons une réserve *inépuisable* d'entiers. L'important, c'est d'avoir trouvé une correspondance terme à terme (une bijection) entre les deux ensembles.
Pour illustrer ce propos, le mathématicien HILBERT(1862-1943) imagina un hôtel un peu spécial qui comporterait une infinité de chambres, toutes numérotées avec un entier. Un voyageur arrive et voudrait une chambre.
On lui annonce que l'hôtel est complet mais qu'il va cependant pouvoir prendre la chambre numéro 1 : tous les occupants iront dans la chambre suivant la leur.

Hihutix: ah oui : celui de la chambre 1 va dans la chambre 2, celui de la 3 dans la 4 etc.

Mathémator : et il faut garder en mémoire qu'il n'y a pas de dernière chambre donc il y en aura une pour chacun.

Imaginez maintenant qu'un car d'un million de touristes arrive à l'hôtel.

Hihutix: pas de problème, on se décale d'un million de chambres.

Mathémator : et si un hôtel similaire a des problèmes de plomberie : la direction déécide de reloger ses cleints à l'hôtel Hilbert.

Hihutix: ce n'est plus possible : il faudrait se décaler d'une infinité de chambres.

Mathémator : il existe pourtant de nombreuses possibilités comme par exemple de demander à chaque client d'aller dans la chambre portant le double du numéro de la chambre initiale.

Hihutix: voyons...l'occupant de la 1 va à la 2, celui de la 2 va à la 4, celui de la 3 va à la

6...mmmm....je ne vois pas.

Mathémator : c'est simple : les anciens clients vont dans les chambres de numéros pairs ce qui laisse aux nouveaux les chambres de numéros impairs.

Hihutix: waouh, c'est un peu vertigineux.

Mathémator : un mathématicien contemporain de HILBERT, DEDEKIND(1831-1916), proposa une définition d'un ensemble infini : c'est un ensemble E qui peut être mis en bijection avec un de ses sous-ensembles S, S étant strictement inclus dans E.

Par exemple, il y a autant d'entiers que d'entiers pairs donc $\mathbb{N}$ est infini au sens de DEDEKIND.

Hihutix: Mais tout à l'heure, en comptant les rationnels, vous avez oublié les rationnels négatifs.

Mathémator : Un détail ! Il suffit d'intercaler l'opposé de chaque terme entre deux couples de notre suite :

$$(0,0)-(1,0)-(-1,0)-(0,1)-(0,-1)-(0,2)-(0,-2)-(1,1)-(-1,1)-(2,0)-(-2,0)-\cdots$$

Hihutix: Mais ce n'est qu'un dessin.

Mathémator : Effectivement, il reste à mettre tout ça en forme en introduisant une *bijection* bien choisie, mais le plus dur est fait : c'est CANTOR qui a eu cette intuition à la fin du XIXe siècle.

C'est encore à lui que nous devons une preuve que $\mathbb{R}$ n'est pas dénonbrable grâce au *raisonnement diagonal de ... Cantor*. Notre ami russo-dano-allemand [t] a prouvé que $J = [0,1]$ n'était pas dénombrable de la manière suivante :

Raisonnons par l'absurde et supposons que l'ensemble des points de J soit dénombrable. Il existe alors au moins une suite $(u_n)_{n\in\mathbb{N}}$ de nombres réels vérifiant la propriété suivante : pour tout réel x deJ, il existe un entier n pour lequel $x = u_n$

Explicitons de la sorte la suite $(u_n)_{n\in\mathbb{N}}$:

t. Cantor a ensuite proposé l'hypothèse du continu en 1878 : il y a deux sortes de sous-ensembles infinis de $\mathbb{R}$: ceux qui sont en correspondance terme à terme avec $\mathbb{N}$ et ceux qui sont en correspondance terme à terme avec $\mathbb{R}$: il n'y aurait donc pas « d'infini intermédiaire » entre $\mathbb{N}$ et $\mathbb{R}$. Ce résultat contribua a rendre fou ce génial mathématicien...

$$\begin{aligned}
u_1 &= 0, u_{11}u_{12}u_{13}u_{14}\cdots u_{1n}\cdots \\
u_2 &= 0, u_{21}u_{22}u_{23}u_{24}\cdots u_{2n}\cdots \\
u_3 &= 0, u_{31}u_{32}u_{33}u_{34}\cdots u_{3n}\cdots \\
u_4 &= 0, u_{41}u_{42}u_{43}u_{44}\cdots u_{4n}\cdots \\
\vdots &= \vdots \quad \vdots \quad \vdots \quad \vdots
\end{aligned}$$

La première décimale du premier terme est u_{11}, sa seconde décimale est u_{12}, ... La première décimale du second terme est u_{21}, sa seconde décimale est u_{22}, ... La première décimale du n^{e} terme est u_{n1}, sa seconde décimale est u_{n2}, ...

Considérons alors le réel x de l'intervalle J ainsi défini : $x = 0, x_1x_2x_3\cdots x_n\cdots$ et la décimale x_i de rang i sera 1 si u_{ii} est différent de 1 et 2 dans le cas contraire.

Par conséquent, x ne peut égaler u_1 (il en diffère au moins par u_{11}), x ne peut égaler u_2 (il en diffère au moins par u_{22}), x ne peut égaler u_3 (il en diffère au moins par u_{33}),... : l'égalité $x = u_n$ n'a lieu pour aucun entier n, donc nous avons trouvé un élément de J...qui n'est pas dans J : belle contradiction. Notre supposition de départ est donc fausse et $[0,1]$ n'est pas dénombrable, donc a fortiori $\mathbb{R}$ non plus.

Hihutix: Tout ceci est passionnant, mais qu'est-ce que cela a affaire avec les probabilités ?

Mathémator : Et bien quand une variable prend ses valeurs dans un ensemble continu - $\mathbb{R}$ par exemple - on ne peut plus définir les probabilités comme dans le cas discret.

Hihutix: Je ne vois pas pourquoi.

Mathémator : Supposez que vous disposiez de 100 jetons identiques numérotés de 1 à 100 dans un sac opaque et que vous en tiriez un au hasard. La probabilité de tomber sur le jeton 32 est $1/100$. Pouvez-vous maintenant, même en disposant d'un temps infini, inscrire tous les réels sur des jetons ?

Hihutix: Non, car nous venons de voir qu'on ne peut les numéroter.

Mathémator : Donc il faut procéder autrement. Par exemple, vous voulez mesurer la longueur de votre sabre laser. Même avec le meilleur instrument de mesure imaginable, vous n'obtiendrez qu'un *intervalle* dans lequel se situe le résultat exact (D'ailleurs, la probabilité pour que le résultat exact soit un nombre décimal est nulle (cf l'aparté page suivante)) (au cm près, au µm près, à l'Å près,...). De même, si vous demandez à votre calculatrice de vous donner un nombre réel au hasard dans $[0,1]$, elle se contentera de vous donner un intervalle.

Hihutix: Pourtant un nombre s'affiche.

Mathémator : Oui mais l'événement « obtenir 0.3232 sur l'écran de la calculatrice » est en fait l'événement « obtenir, lors du choix au hasard, un nombre situé dans l'intervalle

$[0,32315\,;0,32325[$ ». De même qu'on peut penser que la « probabilité » (on ne l'a pas encore définie) de rencontrer une personne mesurant *exactement* 1,88m est nulle, et d'ailleurs vous vous en fichez, puisqu'il n'existe aucun moyen de vérifier quelle est exactement sa taille. En fait, la probabilité d'obtenir exactement 32 doit logiquement être nulle.

Hihutix: Ça me fait un peu penser à ce que j'ai entendu dire de la physique quantique : on peut prévoir où se trouve à peu près une particule élémentaire, mais on ne peut pas savoir exactement où elle se trouve à un moment donné.

Mathémator : En effet ! D'ailleurs, les notions mathématiques que nous abordons et les théories physiques que vous évoquez ont été développées presque simultanément. De plus, l'équation quantique par excellence, la fameuse *équation de* SCHRÖDINGER, fait en fait intervenir la densité de probabilité de présence de la particule au point considéré.

Pour aller plus loin

Incroyables réels : quelques quasi-paradoxes
Vous connaissez déjà des nombres réels particuliers : les entiers, les rationnels, les irrationnels. D'autres catégories (pouvant recouper les ensembles habituels) sont utilisées. Ainsi, les nombres racines de polynômes à coefficients entiers sont appelés *nombres algébriques* : c'est le cas de 1 (solution de $x-1=0$), de $1/3$ (solution de $3x-1=0$), de $\sqrt{2}$ (solution de $x^2-2=0$), etc. On connaît des nombres qui ne sont pas algébriques, on les appelle les *nombres transcendants*. C'est le cas par exemple de π et de e. Au premier abord, il semble qu'il y ait beaucoup plus de nombres algébriques que de nombres transcendants (vous n'en connaissez que deux !). Un jour de pur délire, on pourrait même envisager qu'il y ait autant de nombres de chaque catégorie. Or, si on prend un nombre au hasard dans l'intervalle $[0,1]$, vous calculerez peut-être un jour que la probabilité d'obtenir un nombre transcendant vaut ....1 ! ! ! ! En effet, la « mesure » de l'ensemble des nombres algébriques est nulle. Pourtant, demandez à un ordinateur de vous donner un milliard de nombres au hasard entre 0 et 1, l'écran ne vous affichera que des nombres algébriques (décimaux même !). Mathémator a déjà parlé de ce problème. L'ensemble $\mathbb{R}$ recèle bien d'autres résultats étonnants. Il existe une famille de nombres correspondant elle aussi à une probabilité de 1, pourtant, les mathématiciens ne connaissent qu'un seul de ces nombres dont ils ne peuvent calculer que quelques décimales (d'ailleurs ils ne pourront jamais en trouver plus car il est par essence non calculable !). L'étude de l'intervalle $[0,1]$ renvoie donc à des résultats parfois plus philosophiques que techniques...

10 2 Quelques résultats sur les cardinaux

10 2 1 Cardinal de P(E)

Soit $E_2=\{a,b\}$ et $E_3=\{a,b,c\}$. En fait, $E_3=E_2\cup\{c\}$. Les parties de E_3 sont donc les parties de E_2 et ces mêmes parties auxquelles on adjoint c.

En effet, $\mathcal{P}(E_3)=\Big\{\emptyset,\{a\},\{b\},\{a,b\},\emptyset\cup\{c\},\{a\}\cup\{c\},\{b\}\cup\{c\},\{a,b\}\cup\{c\}\Big\}$.

Ainsi $|\mathcal{P}(E_3)|=2\times|\mathcal{P}(E_2)|$.

Notons de manière générale E_n un ensemble à n éléments avec $n \in \mathbb{N}$ et $E_{n+1} = E_n \cup \{\alpha\}$ avec $\alpha \notin E_n$. On montre facilement que $|\mathcal{P}(E_{n+1})| = 2 \times |\mathcal{P}(E_n)|$. Or $\mathcal{P}(E_0) = \{\varnothing\}$ donc $|\mathcal{P}(E_0)| = 1$.

une rapide récurrence permet donc de prouver que :

Théorème 1 - 13

cardinal de $\mathcal{P}(E)$
Si $|E| = n$ alors $|\mathcal{P}(E)| = 2^n$

10 2 2 Cardinal d'une partition

Il est assez immédiat d'obtenir le résultat suivant :

Théorème 1 - 14

cardinal d'une partition
Si la famille $(A_i)_{i \in [\![1,n]\!]}$ de parties non vides d'un ensemble E réalise une **partition** de cet ensemble alors :

$$|E| = \sum_{i=1}^{n} |A_i|$$

[u]

10 2 3 Cardinaux et inclusion

Théorème 1 - 15

$$\forall (A,B) \in \mathcal{P}(E) \times \mathcal{P}(E),\ A \subset B \Longrightarrow |A| \leqslant |B|$$

Pour le prouver, il suffit d'utiliser une petite ruse (bientôt) habituelle : A et $\overline{A} \cap B$ forment une partition de B donc, d'après le théorème 1 - 14, $|A| + \left|\overline{A} \cap B\right| = |B|$, donc $|A| \leqslant |B|$

[v]

u. Pour compter les élèves de la promo, il suffit de compter les élèves de chaque groupe et d'additionner les résultats...
v. Cette application n'est pas une équivalence ! Prenez $A = \{1\}$ et $B = \{3;4\}$

10 2 4 Cardinal d'un produit cartésien

Voici un autre résultat qui sera bien utile :

Théorème 1 - 16

cardinal d'un produit cartésien
Soit $(A_i)_{i\in[\![1,n]\!]}$ des parties d'un ensemble E.

$$\left|\prod_{i=1}^{n} A_i\right| = \prod_{i=1}^{n} |A_i|$$

En effet, pour chaque n-liste $(x_1,\dots,x_n)$, il y a $|A_1|$ choix pour la première composante, $|A_2|$ choix pour la deuxième, etc.

10 2 5 Formule du crible

Nous n'en verrons qu'un cas particulier que vous devez déjà connaître :

Théorème 1 - 17

formule du crible pour deux ensembles
$\forall(A,B)\in\mathcal{P}(E)\times\mathcal{P}(E),\ |A\cup B| = |A|+|B|-|A\cap B|$

Pour le démontrer, nous allons former une partition de $A\cup B$ avec $A\cap\overline{B}$, $\overline{A}\cap B$ et $A\cap B$.

Mais on peut également « partitionner » A avec $A\cap\overline{B}$ et $A\cap B$ puis « partitionner » B avec $B\cap\overline{A}$ et $B\cap A$.

On obtient donc que $|A| = \left|A\cap\overline{B}\right| + |A\cap B|$ puis que $|B| = \left|B\cap\overline{A}\right| + |B\cap A|$.

On en déduit que $|A|+|B| = \left|A\cap\overline{B}\right| + \left|B\cap\overline{A}\right| + |A\cap B| + |B\cap A|$ et enfin que :

$$|A|+|B|-|A\cap B| = \left|A\cap\overline{B}\right| + \left|B\cap\overline{A}\right| + |A\cap B| = |A\cup B|$$

10 3 Dénombrement

Lorsqu'on compte des « objets », on met en « correspondance » des éléments de $\mathbb{N}$ avec des objets : on *dénombre*.

Cela peut parfois être simple : combien y a-t-il d'issues à une expérience de pile ou face ?...

Mais on peut souvent avoir besoin d'outils performants que nous allons présenter à présent.

10 3 1 Permutations

Définition 1 - 34

permutation
Soit E un ensemble de cardinal n. On appelle **permutation** de E toute disposition ordonnée (n-liste) des n éléments de E.

Par exemple, les permutations de $\{a, b, c\}$ sont (a, b, c), (a, c, b), (b, a, c), (b, c, a), (c, a, b), (c, b, a).

Théorème 1 - 18

nombre de permutations
Il y a $n!$ permutations d'un ensemble de n éléments.

La démonstration s'effectue par récurrence. Il y a bien sûr 1 ! façon de permuter 1 élément.

On peut donc supposer qu'il existe au moins un entier k tel qu'il y ait $k!$ permutations d'un ensemble à k éléments.

Considérons un ensemble à $k+1$ éléments. On en choisit 1 : il y a $k+1$ choix possibles. Ensuite, il s'agit d'ordonner les k éléments restant ce qui laisse $k!$ possibilités.

Il y a donc finalement $(k+1) \times k! = (k+1)!$ permutations au total.

On retrouve dans l'exemple précédent qu'il y a $3! = 6$ permutations de $\{a, b, c\}$.

[w]

10 3 2 Combinaisons

Il n'y a pas assez de gagnants au loto. Les règles en sont donc modifiées. Il s'agit maintenant de trouver 3 numéros parmi 5. Combien y a-t-il de grilles (combinaisons) possibles ?

Par exemple, on pourrait dire que j'ai cinq manières de choisir le premier numéro, quatre choix pour le deuxième et trois choix pour le troisième, donc il y a $5 \times 4 \times 3$ grilles différentes mais dans ce cas, je compte des 3-listes ordonnées alors que les 3-listes $(1, 2, 3)$ et $(3, 2, 1)$ correspondent à la même grille ou combinaison $\{1, 2, 3\}$.

Posons une petite définition pour clarifier les débats. Donnons en fait un nom à une grille du loto, c'est à dire à un sous-ensemble (une partie) contenant p éléments d'un plus grand

w. On conviendra que $0! = 1$

ensemble contenant n éléments.

Définition 1 - 35

combinaison sans répétition
Soit n et p deux entiers naturels et E un ensemble contenant n éléments. Un sous-ensemble de E contenant p éléments est appelé une **combinaison** de p éléments de E ou encore une p-**combinaison** d'éléments de E.

Or ce qui nous intéresse, c'est le nombre de ces combinaisons, donc introduisons une notation

Définition 1 - 36

nombre de combinaisons sans répétitions
Le nombre de p-combinaisons d'un ensemble contenant n éléments est noté $\binom{n}{p}$ ou encore C_n^p

Revenons à notre mini-loto. Considérons une grille quelconque (c'est à dire une 3-combinaison de l'ensemble des 5 numéros) : par exemple $\{2,4,5\}$. Nous avons vu dans le paragraphe précédent qu'il y a 3! facons d'ordonner ces nombres. Finalement, il y a $\binom{5}{3} \times 3!$ suites de 3 nombres ordonnées. Or nous en avons comptées $5\times4\times3$ tout à l'heure. Nous en déduisons finalement que

$$\binom{5}{3} = \frac{5\times4\times3}{3!}$$

Il est alors aisé de généraliser la formule suivante :

Propriété 1 - 7

$$\binom{n}{p} = \frac{n(n-1)(n-2)\cdots(n-(p-1))}{p!}$$

Nous pouvons formuler cette propriété plus synthétiquement. En effet

$$\binom{n}{p} = \frac{n(n-1)(n-2)\cdots(n-p+1)}{p!} \times \frac{(n-p)(n-p-1)(n-p-2)\times\cdots\times2\times1}{(n-p)(n-p-1)(n-p-2)\times\cdots\times2\times1} = \frac{n!}{p!(n-p)!}$$

d'où

Théorème 1 - 19

$$\binom{n}{p} = \frac{n!}{p!(n-p)!}$$

Cette formule nous permet un calcul direct des nombres $\binom{n}{p}$ mais il faut s'en méfier car il est difficile de l'utiliser directement dès que n est grand ($70! > 10^{100}$). Il est donc utile de remarquer que

$$\binom{n}{p} = \frac{n}{p}\binom{n-1}{p-1}$$

on a alors un algorithme récursif pour calculer $\binom{n}{p}$.

Théorème 1 - 20

Le nombre de suites strictement croissantes de p éléments de $\mathbb{N}_n$ est $\binom{n}{p}$.

Démonstration : il suffit de remarquer que l'on définit une bijection entre l'ensemble des combinaisons de $\mathbb{N}_n$ à p éléments et l'ensemble des suites strictement croissantes de p éléments de $\mathbb{N}_n$ en associant à toute combinaison $\{i_1, i_2, \cdots, i_p\}$ l'unique suite où $i_1, i_2, \cdots, i_p$ sont rangés par ordre croissant.

10 4 Triangle de Pascal - Binôme de Newton

À l'aide des formules précédentes, on prouve facilement (faites-le !) le résultat suivant :

Propriété 1 - 8

$$\binom{n}{p} = \binom{n}{n-p}$$

On établit ensuite, toujours par le calcul, la relation suivante, dite **Relation de Pascal** même si les mathématiciens chinois l'avaient mise en évidence avant lui :

Théorème 1 - 21

relation de PASCAL

$$\binom{n}{p} = \binom{n-1}{p} + \binom{n-1}{p-1}$$

Il est possible de démontrer cette formule à l'aide d'un raisonnement ensembliste : pour former des groupes de p éléments dans un ensemble en contenant n, on distingue un élément n_0 quelconque :

- soit le groupe le contient et alors il y a $\binom{n-1}{p-1}$ choix des $p-1$ éléments distincts de n_0 parmi les $n-1$ restant ;
- soit le groupe ne le contient pas et il faut donc choisir p éléments parmi les $n-1$ éléments distincts de n_0 : il y a donc cette fois $\binom{n-1}{p}$.

Cette relation permet de démontrer la formule du binôme de NEWTON :

Théorème 1 - 22

formule du binôme de NEWTON

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

Recherche

Pour calculer les nombres $\binom{n}{p}$, on vient de donner trois méthodes (donc 3 algos) tout en sachant que $\binom{n}{p} = 0$ si $n > p$ et $\mathcal{C}_n^0 = 1$

$$\begin{aligned} \binom{n}{p} &= \frac{n!}{p!(n-p)!} \\ \binom{n}{p} &= \frac{n}{p}\binom{n-1}{p-1} \\ \binom{n}{p} &= \binom{n-1}{p-1} + \binom{n-1}{p} \end{aligned}$$

et vous devez créer un programme qui calcule les nombres $\binom{n}{p}$. Donner les avantages et les inconvénients de ces 3 méthodes.

10 5 Combinaisons avec répétitions.

Soit $\mathrm{E} = \{e_1, e_2, e_3, \cdots, e_n\}$ un ensemble ordonné, $e_1 < e_2 < \ldots e_n$. On appelle p-combinaison avec répétitions de E tout p-uplet du type

$$\underbrace{e_1, e_1, \cdots,}_{x_1 \text{ fois}} \underbrace{e_2, e_2, \cdots,}_{x_2 \text{ fois}} \underbrace{e_3, e_3, \cdots,}_{x_3 \text{ fois}} \cdots, \underbrace{e_n, e_n, \ldots}_{x_n \text{ fois}}$$

$$\text{avec } \sum_{k=1}^{n} x_k = p, \text{ des } x_k \text{ pouvant être nuls.}$$

Déterminer le nombre de tels p-uplets c'est déterminer le nombre de p-combinaisons avec répétitions de E et c'est donc déterminer le nombre de n-uplets

$$(x_1, x_2, \cdots, x_n) \in \mathbb{N}^n \text{ vérifiant } \sum_{k=1}^{n} x_k = p$$

Théorème 1 - 23

Le nombre de p-combinaisons avec répétitions dans un ensemble à n éléments est :

$$\Gamma_n^p = \binom{n+p-1}{p}$$

Démonstration : à chaque n-uplet $(x_1, x_2, \cdots, x_n) \in \mathbb{N}^n$ vérifiant $\sum_{k=1}^{n} x_k = p$, associons le mot construit de la façon suivante :

- autant de a que la valeur de x_1 puis un b
- autant de a que la valeur de x_2 puis un b
- $\cdots$
- autant de a que la valeur de x_{n-1} puis un b
- autant de a que la valeur de x_n

Nous obtenons un mot de longueur $n+p-1$ comportant exactement p fois le symbole a, puisque $\sum_{k=1}^{n} x_k = p$, et $n-1$ fois le symbole b. Notons $\mathcal{M}_{p,n-1}$ l'ensemble des mots de ce type. Il est clair que nous venons de définir une bijection entre l'ensemble des n-uplets $(x_1, x_2, \cdots, x_n) \in \mathbb{N}^n$ vérifiant $\sum_{k=1}^{n} x_k = p$ et $\mathcal{M}_{p,n-1}$. Le cardinal de $\mathcal{M}_{p,n-1}$ étant $\binom{n+p-1}{p}$ on obtient bien le résultat attendu.

Théorème 1 - 24

Le nombre de suites croissantes, au sens large, de p éléments de $\mathbb{N}_n$ est égal à Γ_n^p.

Démonstration : considérons une suite croissante de p éléments de $\mathbb{N}_n$:

$$x_1 \leq x_2 \leq x_3 \leq \cdots \leq x_p$$

et considérons l'application φ définie par :

$$y_i = \varphi(x_i) = x_i + i - 1, i \in \{1, 2, 3, \cdots, p\}$$

Il est clair que $y_1 < y_2 < y_3 < \cdots < y_p$. φ définit donc une bijection entre l'ensemble des suites croissantes de p éléments de $\mathbb{N}_n$ et l'ensemble des suites strictement croissantes de p éléments de $\mathbb{N}_{n+p-1}$, or le nombre de suites strictement croissantes de p éléments de $\mathbb{N}_{n+p-1}$ est $\binom{n+p-1}{p} = \Gamma_n^p$.

Exemple 1.9

On doit ranger 10 cahiers dans 5 tiroirs, déterminer le nombre de rangements possibles si

1. les cahiers sont discernables ;
2. les cahiers sont indiscernables

EXERCICES

Raisonnements

Exercice 1 - 1

On note P = « x est un entier naturel » et Q = « $2x$ est un entier naturel pair ».

1. P ⇒ Q est-il un théorème ?
2. Traduire ¬Q ⇒ ¬P.
3. Q ⇒ P est-il un théorème ?
4. ¬P ⇒ ¬Q est-il un théorème ?
5. P ⇔ Q est-il un théorème ?

Exercice 1 - 2

a et b désignent des réels et il est clair que l'affirmation ou l'énoncé P =« $a = b$ »⇒ Q =« $a^2 = b^2$ » est bien un théorème.

1. P est-elle une condition nécessaire de Q ?
2. Q est-elle une condition nécessaire de P ?
3. P est-elle une condition suffisante de Q ?
4. Q est-elle une condition suffisante de P ?
5. Traduire ¬Q ⇒ ¬P.
6. $a \neq b \Rightarrow a^2 \neq b^2$ est-il un théorème ?

Exercice 1 - 3

1. Montrer par une preuve directe que « *n et m sont des entiers pairs* » $\Longrightarrow$ « *n + m est un entier pair* » est un théorème.
2. Montrer par contraposition que « *n^2 est un entier pair* » $\Longrightarrow$ « *n est un entier pair* » est un théorème.
3. Montrer par l'absurde que « *n + m est un entier impair* » $\Longrightarrow$ « *exactement un nombre, parmi n et m est un entier impair* » est un théorème.

Exercice 1 - 4

On considère la suite u définie par

$$\begin{cases} u_0 = 1 \\ n \in \mathbb{N}, u_{n+1} = \dfrac{1}{2+u_n} \end{cases}$$

Démontrer par récurrence que pour tout $n \in \mathbb{N}$ on a $u_n \in [0,1]$.

Exercice 1 - 5

Démontrer par une récurrence simple que

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Exercice 1 - 6

Démontrer directement (pas par récurrence) que

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Exercice 1 - 7 Factorielle

Écrivez un algorithme récursif qui donne $n!$ pour tout entier naturel n.

Exercice 1 - 8 Somme

Écrivez un algorithme récursif qui calcule $\sum_{k=0}^{n} f(k)$ pour une fonction f donnée.

Exercice 1 - 9 Division euclidienne

Déterminer un algorithme récursif qui renvoie le quotient de deux entiers naturels non nuls a et b.

Déterminer un algorithme récursif qui renvoie le reste entier de a et b.

Exercice 1 - 10 Somme de chiffres

Donnez un algorithme récursif qui calcule la somme des chiffres d'un entier naturel n écrit en base 10.

Exercice 1 - 11 Héron

HÉRON d'Alexandrie a trouvé une méthode permettant de déterminer une approximation de la racine carrée d'un nombre positif vingt siècles avant l'apparition des ordinateurs.

Si x_n est une approximation strictement positive par défaut de $\sqrt{a}$, alors a/x_n est une approximation par excès de $\sqrt{a}$ (pourquoi ?) et vice-versa.

La moyenne arithmétique de ces deux approximations est $\frac{1}{2}\left(x_n + \frac{a}{x_n}\right)$ et constitue une meilleure approximation que les deux précédentes.

On peut montrer c'est une approximation par excès (en développant $\left(x_n - \sqrt{a}\right)^2$ par exemple).

On obtient naturellement un algorithme... Donnez une version récursive prenant en argument le nombre dont on cherche la racine carrée, une première approximation x_0 et une précision `eps`.

Exercice 1 - 12 Décimales de e

Posons $e_n = 1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!}$

Alors on a aussi

$$e_n = 1 + 1 + \frac{1}{2}\left(1 + \frac{1}{3}\left(1 + \frac{1}{4}\left(\cdots\left(\frac{1}{n-1}\left(1 + \frac{1}{n}\right)\right)\right)\right)\right)$$

Un exercice classique montre que $e - e_n \leqslant \frac{n+2}{n+1}\frac{1}{(n+1)!}$.

Ainsi, pour $n = 167$, on obtiendra 300 bonnes décimales au moins : trouvez-les !

Exercice 1 - 13 Fractions continues dans Q

– Vous connaissez l'algorithme suivant :

$$\begin{aligned}
172 &= 3 \times 51 + 19 && (1.1)\\
51 &= 2 \times 19 + 13 && (1.2)\\
19 &= 1 \times 13 + 6 && (1.3)\\
13 &= 2 \times 6 + 1 && (1.4)\\
6 &= 6 \times 1 + 0 && (1.5)
\end{aligned}$$

– On peut donc facilement compléter la suite d'égalité suivante :

$$\frac{172}{51} = 3 + \frac{19}{51} = 3 + \frac{1}{\frac{51}{19}} = 3 + \frac{1}{2 + \frac{13}{19}} = \ldots$$

– Quand tous les numérateurs sont égaux à 1, on dit qu'on a développé $\frac{172}{51}$ en fraction continue et pour simplifier l'écriture on note :

$$\frac{172}{51} = [3;2;\ldots]$$

– Par exemple, on peut développer $\frac{453}{54}$ en fraction continue.

– Dans l'autre sens on peut écrire $[2;5;4]$ sous la forme d'une fraction irréductible.

On suppose connus les algorithmes donnant le reste et le quotient d'une division euclidienne.

Écrivez un algorithme donnant le développement en fraction continue d'un rationnel.

Écrivez ensuite un algorithme récursif qui effectue la transformation inverse.

Exercice 1 - 14 Fractions continues dans R

En fait, l'étude précédente correspond à un cas particulier d'une définition plus générale.

Soit x un réel non entier. On construit une suite entière (z_n) de la manière suivante :

$$x = z_0 + \frac{1}{x_1} \qquad z_0 = \lfloor x \rfloor \qquad x_1 = \frac{1}{x - z_0}$$

puis, tant que x_k n'est pas entier :

$$x_k = z_k + \frac{1}{x_{k+1}} \qquad z_k = \lfloor x_k \rfloor \qquad x_{k+1} = \frac{1}{x_k - z_k}$$

Le développement de x en fractions continues est alors donné par $[z_0, z_1, z_2, \dots]$, cette liste pouvant être infinie.

Écrivez un algorithme récursif qui donne n chiffres du développement en fraction continue d'un nombre x donné.

Exercice 1 - 15

On définit deux fonctions `tete` et `queue` qui renvoient respectivement le premier élément d'une liste et la liste privée de sa tête. La syntaxe dépend des langages.

Écrivez à présent une fonction récursive qui renvoie le maximum d'une liste de nombres.

Exercice 1 - 16 Palindrome

Écrivez un algorithme récursif qui vérifie si une liste est un palindrome.

Exercice 1 - 17 Nombres parfaits

Un nombre parfait est un nombre entier n strictement supérieur à 1 qui est égal à la somme de ses diviseurs (sauf n bien sûr !).

1. Il y en a un caché entre 1 et 10 : trouvez-le...
2. Écrivez un algorithme récursif qui donne la liste des diviseurs d'un entier autres que lui-même.
3. Écrivez un algorithme qui calcule la somme des éléments d'une liste.
4. Écrivez un algorithme qui détermine si un nombre entier est parfait.
5. Écrivez un algorithme récursif qui donne la liste des nombres parfaits entre 1 et un nombre n donné.

Exercice 1 - 18 Décomposition en base 2

Une méthode pour obtenir l'écriture en base 2 d'un nombre est d'effectuer des divisions successives. Par exemple pour 11 :

$$\begin{array}{r|l} 1\,1 & 2 \\ \cline{2-2} 1 & 5 \end{array} \qquad \begin{array}{r|l} 5 & 2 \\ \cline{2-2} 1 & 2 \end{array} \qquad \begin{array}{r|l} 2 & 2 \\ \cline{2-2} 0 & 1 \end{array} \qquad \begin{array}{r|l} 1 & 2 \\ \cline{2-2} 1 & 0 \end{array}$$

$$
\begin{aligned}
11 &= \left(2\times 5+1\right)\\
&= \left(2\times\left(2\times 2+1\right)+1\right)\\
&= \left(2\times\left(2\times(2\times 1)+1\right)+1\right)\\
&= \left(2\times(2^2+1)+1\right)\\
&= 2^3+2+1\\
&= 1\times 2^3+0\times 2^2+1\times 2^1+1\times 2^0
\end{aligned}
$$

L'écriture de 11 en base 2 est donc 1011 : c'est la liste des restes obtenus mais dans l'ordre inverse.

La méthode est facilement généralisable.

Écrivez un algorithme récursif qui donne la décomposition d'un entier en base 2 sous forme d'une liste.

Exercice 1 - 19

On définit la partie entière d'un réel x comme étant le plus grand entier inférieur à x.

On part du fait que la partie entière d'un nombre appartenant à $[0;1[$ est nulle.

Commentez l'algorithme suivant :

```
Fonction
partie_entiere(x: flottant) : entier
Début
    Si x>=0 et x<1 Alors
        Retourner 0
    Sinon
        Si x>=0 Alors
            Retourner
1+partie_entiere(x-1)
        Sinon
            Retourner
-1+partie_entiere(x+1)
        FinSi
    FinSi
Fin
```

Exercice 1 - 20

Prouvez par récurrence l'exactitude de l'algorithme suivant :

```
Fonction Carré(n: entier positif) : entier
positif
Début
    sq ← 0
    Pour i variantDe 1 Jusque n Faire
        sq ← sq+2*i-1
    FinPour
    Retourner sq
Fin
```

Exercice 1 - 21

On se propose de démontrer que tous les étudiants en informatique ont le même âge et, pour cela, on note $P(n)$ l'affirmation

« *si on choisit n étudiants en informatique* ($n \in \mathbb{N}^*$), *il est sûr qu'ils ont tous le même âge* »

Il est clair que $P(1)$ est vraie.

Démontrons que $P(n) \Rightarrow P(n+1)$. Pour cela nous supposons que $P(n)$ est vraie (c'est l'hypothèse de récurrence) et nous choisissons un groupe quelconque de $n+1$ étudiants que nous ordonnons par ordre alphabétique (pourquoi pas). D'après l'hypothèse de récurrence, les n premiers de l'ordre alphabétique ont tous le même âge ainsi que les n derniers. Comme ces deux groupes de n étudiants ont au moins un étudiant en commun, on en déduit qu'ils ont tous le même âge.

Nous venons de démontrer que $P(n) \Rightarrow P(n+1)$ pour tout $n \geq 1$ et, comme $P(1)$ est vrai, $P(n)$ est toujours vrai pour tout $n \geq 1$. **Y a-t-il une erreur dans le raisonnement ?**

Ensembles

Exercice 1 - 22

On rappelle qu'une paire ordonnée (ou couple) se note (a, b) et qu'on a

$$(a,b) = (x,y) \Leftrightarrow a = x \text{ et } b = y$$

Montrez que le couple (a, b) peut également être défini par :

$$(a,b) = \{\{a\},\{a,b\}\}$$

Exercice 1 - 23

$E = \{0,1,2,3,4,5,6\}$. Définir en extension les ensembles suivants :

1. $A_1 = \left\{x \in \mathbb{N} \mid x^2 \in E\right\}$
2. $A_2 = \left\{x \in \mathbb{R} \mid x^2 \in E\right\}$
3. $A_3 = \left\{x \in E \mid x^2 \in E\right\}$
4. $A_4 = \left\{x \in E \mid \sqrt{x} \in E\right\}$
5. $A_5 = \{x \in E \mid 2x \in E\}$
6. $A_6 = \left\{x \in E \mid \frac{x}{2} \in E\right\}$

Exercice 1 - 24

$E = \{0,1,2,3,4\}$. Compléter, lorsque c'est possible, par un des symboles (il peut y avoir plusieurs solutions, mais on s'obligera à choisir celle qui donne le plus « de renseignements ») :

$$\in, \ni, \subset, \supset, \subseteq, \supseteq, =, \neq, \subsetneq, \cdots$$

1. $2 \cdots E$, $\{2,3\} \cdots E$, $\{2\} \cdots E$
2. $\{2,3,4\} \cdots \{4,3,2\}$, $\{2,3,4\} \cdots \{4,3,0\}$
3. $\emptyset \cdots E$, $E \cdots E$, $E \cdots \{E\}$, $\emptyset \cdots \{E\}$
4. $E \cdots \{0,1,2,3,\ldots,10\}$, $\{0,1,2,3,4,5\} \cdots E$

Exercice 1 - 25

On définit un opérateur $\divideontimes$ sur les ensembles de la manière suivante :

$$A \divideontimes B = \neg(A \cap B)$$

Démontrer les égalités suivantes :

1. $A \divideontimes A = \neg A$;
2. $(A \divideontimes A) \divideontimes (B \divideontimes B) = A \cup B$;
3. $(A \divideontimes B) \divideontimes (A \divideontimes B) = A \cdots B$.

Exercice 1 - 26

Expliciter $\mathcal{P}(\mathbb{N}_n)$ pour pour $n \in \{1,2,3\}$. On rappelle la notation $\mathbb{N}_n = \{1,2,3,\ldots,n\} = [\![1,n]\!]$.

Exercice 1 - 27

Expliciter $\mathcal{P}(\{a,\{a\}\})$.

Exercice 1 - 28

Expliciter $\mathcal{P}(\emptyset)$, $\mathcal{P}(\mathcal{P}(\emptyset))$.

Exercice 1 - 29

Expliciter $\mathcal{P}(\mathcal{P}(\mathbb{N}_2))$.

Exercice 1 - 30

Donner cinq éléments de $\mathcal{P}(\mathcal{P}(\mathcal{P}(\{a,b,c\})))$.

Exercice 1 - 31

Démontrer par récurrence :

$$\text{E possède } n \text{ éléments} \Rightarrow \mathcal{P}(\mathrm{E}) \text{ possède } 2^n \text{ éléments.}$$

Exercice 1 - 32

Combien d'éléments $\mathcal{P}(\mathcal{P}(\mathcal{P}(\{a,b,c\})))$ contient-il ?

Exercice 1 - 33

Démontrer que $\mathrm{A} \subseteq \mathrm{B} \Rightarrow \mathcal{P}(\mathrm{A}) \subseteq \mathcal{P}(\mathrm{B})$.

Exercice 1 - 34

$\mathrm{E} = \{a,b,c,d\}$, $\mathrm{A} \subset \mathrm{E}, \mathrm{B} \subset \mathrm{E}$

1. *Vrai ou Faux*, $\{\varnothing, \{a\}, \{b,c\}\} \in \mathcal{P}(\mathrm{E})$.
2. *Vrai ou Faux*, $\{\varnothing, \{a\}, \{b,c\}\} \subseteq \mathcal{P}(\mathrm{E})$.
3. *Vrai ou Faux*, $\{\varnothing\} \in \mathcal{P}(\mathrm{E})$.
4. *Vrai ou Faux*, $\varnothing \in \mathcal{P}(\mathrm{E})$.
5. *Vrai ou Faux*, $\{\varnothing\} \subseteq \mathcal{P}(\mathrm{E})$.
6. *Vrai ou Faux*, $\{\varnothing\} \subset \mathcal{P}(\mathrm{E})$.
7. *Quel est le cardinal de* $\mathcal{P}(\mathcal{P}(\mathrm{E}))$.
8. Vrai ou Faux, $\{\mathrm{A},\mathrm{B}\} \in \mathcal{P}(\mathrm{E})$.
9. Vrai ou Faux, $\{\mathrm{A},\mathrm{B}\} \subset \mathcal{P}(\mathrm{E})$.

Exercice 1 - 35

Trouver deux ensembles A et B qui vérifient :

$$\mathrm{A} \in \mathrm{B} \text{ et } \mathrm{A} \subseteq \mathrm{B}$$

On indiquera 5 solutions.

Exercice 1 - 36

A, B et C sont trois parties de l'ensemble E vérifiant $\mathrm{A} \cap \mathrm{B} \cap \mathrm{C} \neq \varnothing$. Représenter à l'aide de « patates » (diagramme de Venn) les ensembles suivants :

1. $\mathrm{A} \cup \mathrm{B}$, $\mathrm{A} \cap \mathrm{C}$, $\mathrm{A} \bigtriangleup \mathrm{C}$, $\complement_{\mathrm{B}}(\mathrm{A} \cap \mathrm{B})$, $\mathrm{A} - \complement_{\mathrm{E}}\mathrm{B}$, $\left(\complement_{\mathrm{E}}\mathrm{B}\right) - \mathrm{A}$
2. $(\mathrm{A} \cap \mathrm{B}) - \mathrm{C}$, $(\mathrm{A} - \mathrm{C}) \cap (\mathrm{B} - \mathrm{C})$
3. $(\mathrm{A} \bigtriangleup \mathrm{B}) \bigtriangleup \mathrm{C}$, $\left((\mathrm{A} \bigtriangleup \mathrm{B}) \bigtriangleup \mathrm{C}\right) - (\mathrm{A} \cup \mathrm{B})$, $\complement_{\mathrm{A}\cup\mathrm{B}}\left(\mathrm{A} \bigtriangleup \mathrm{B}\right)$
4. $\overline{\mathrm{A}} \cup \overline{\mathrm{B}}$, $\overline{\mathrm{A} \cap \mathrm{B}}$, $\overline{\mathrm{A} \cup \mathrm{B}}$, $\overline{\mathrm{A}} \cap \overline{\mathrm{B}}$

Exercice 1 - 37

Démontrer : $[\mathrm{A} \cup \mathrm{B} = \mathrm{B}] \Leftrightarrow [\mathrm{A} \subseteq \mathrm{B}]$

Exercice 1 - 38

Démontrer : $[\mathrm{A} \cap \mathrm{B} = \mathrm{B}] \Leftrightarrow [\mathrm{B} \subseteq \mathrm{A}]$

Exercice 1 - 39

Représenter par des « patates », lorsque c'est possible, deux ensembles A et B vérifiant :

1. $\mathrm{A} \cap \mathrm{B} = \varnothing$
2. $\mathrm{A} \cup \mathrm{B} = \mathrm{A}$
3. $\mathrm{A} \cap \mathrm{B} = \mathrm{B}$
4. $\mathrm{A} \bigtriangleup \mathrm{B} = \mathrm{B}$
5. $\mathrm{A} \bigtriangleup \mathrm{B} = \varnothing$

Exercice 1 - 40

$A = \{a, b\}$ et $E = \{a, b, c, d, e\}$, expliciter tous les ensembles B qui vérifient $A \cup B = E$.

Exercice 1 - 41

A et B sont deux parties de E. Si $A \subseteq B$ que peut-on dire de $\overline{A}$ et $\overline{B}$?

Exercice 1 - 42

Représenter chacun des 4 ensembles $A_{i\in\{1,2,3,4\}}$ par une « patate » sachant que l'intersection d'un nombre quelconque de ces ensembles n'est jamais vide et qu'aucun n'est inclus dans un autre puis représenter

$$A_1 \bigtriangleup A_2 \bigtriangleup A_3 \bigtriangleup A_4$$

On rappelle que l'opération $\bigtriangleup$ est associative et commutative.

Exercice 1 - 43

$A = \{0, 1, 2, 3\}$, $B = \{a, b\}$ et $C = \{1, 2\}$. Donner quelques éléments de :

1. $A \times B$, $(A \times B) \times C$, $A \times B \times C$, $A \times (B \times C)$, $C \times (A \cup B)$, A^5
2. $\mathcal{P}(A) \times \mathcal{P}(B)$
3. $\mathcal{P}(A \times B)$
4. $\emptyset \times A$, $A \times (\emptyset \times B)$, $\{\emptyset\} \times B$

Exercice 1 - 44

A, B et C sont trois ensembles tous différents de l'ensemble vide. Démontrer que

$$(A \cap B) \times C = (A \times C) \cap (B \times C).$$

Exercice 1 - 45

$E = \{a, b, c, d, e\}$

1. *Donner 4 partitions de* E.
2. *Vrai ou Faux* , $\{\emptyset, \{a\}, \{b, c, e\}, \{d\}\}$ *est une partition de* E.
3. *Vrai ou Faux* , $\{\{a\}, \{b, c\}, \{d\}\}$ *est une partition de* E.

Exercice 1 - 46

1. Si $A \cap B = A \cup B$, que peut-on dire de A et B ?
2. Si $A \cap B = A \cap C$ et si $A \cup B = A \cup C$, que peut-on dire de A, B et C ?

Exercice 1 - 47

1. On pose $A = \{a, b\}$ et $B = \{b, c\}$.
   a. Comparer $\mathcal{P}(A) \cap \mathcal{P}(B)$ et $\mathcal{P}(A \cap B)$.
   b. Comparer $\mathcal{P}(A) \cup \mathcal{P}(B)$ et $\mathcal{P}(A \cup B)$.
2. Répondre aux mêmes questions avec A et B des ensembles quelconques.

Calcul booléen

Exercice 1 - 48

Calculer $1 \cdot \overline{0}$, $1 + \overline{1}$, $0 \cdot \overline{0}$ et $\overline{(1 + 0)}$.

Exercice 1 - 49

1. Résoudre dans $\mathcal{B}$ les équations :
   a. $x \cdot 1 = 0$
   b. $x + x = 0$
   c. $x \cdot 1 = 0$
   d. $x \cdot \overline{x} = 1$
2. Résoudre dans $\mathcal{B}^2$ l'équation $xy = x + y$.

Exercice 1 - 50

Dresser les tables canoniques des fonctions suivantes :

1. $f(x,y,z) = \overline{z}$
2. $f(x,y,z) = \overline{x}y + \overline{y}z$
3. $f(x,y,z) = x\overline{y}z + \overline{(xyz)}$
4. $f(x,y,z) = \overline{y}\left(xz + \overline{xz}\right)$

Exercice 1 - 51

L'opérateur booléen $\oplus$ est défini par :

$1 \oplus 1 = 0$, $1 \oplus 0 = 1$, $0 \oplus 1 = 1$ et $0 \oplus 0 = 0$.

1. Simplifier :
   a. $x \oplus 0$
   b. $x \oplus 1$
   c. $x \oplus x$
   d. $x \oplus \overline{x}$
2. Montrer que :
   a. $x \oplus y = (x+y)\,\overline{(xy)}$
   b. $x \oplus y = (x\overline{y}) + (\overline{x}y)$
3. L'opération $\oplus$ est-elle commutative ?
4. Vrai ou faux ?
   a. $x \oplus (y \oplus z) = (x \oplus y) \oplus z$
   b. $x + (y \oplus z) = (x+y) \oplus (x+z)$
   c. $x \oplus (y+z) = (x \oplus y) + (x \oplus z)$

Exercice 1 - 52

$\mathcal{B}$ est une algèbre de Boole et dans ce qui suit on travaille dans $\mathcal{B}$; développer et réduire les expressions :

1. $(a+b)(a+b+c)(c+\overline{d})$
2. $(a+b)(b+c)(c+d)(d+a)$
3. $\overline{(a+b)(b+c)(c+d)(d+a)}$
4. $\overline{(a+\overline{b})}.\overline{(c.b.\overline{d})}.(a.b+c).\overline{(b.c+d)}.\overline{(a.b.\overline{c}+\overline{a}.d)}$
5. $\overline{\overline{(a+\overline{b})}.\overline{(c.b.\overline{d})}.(a.b+c).\overline{(b.c+d)}.\overline{(a.b.\overline{c}+\overline{a}.d)}}$
6. $(a+b)(a+c)(a+d)(a+e)$
7. $\overline{(a+b)(a+c)(a+d)(a+e)}$
8. $(a+b)(a+c)+(a+d)(a+e)+(\overline{a}+b)(\overline{a}+c)+\overline{e}$

Exercice 1 - 53

On considére la fonction booléenne de 4 variables définie par :

$$f = a\overline{b}c + \overline{a}cd + abc\overline{d}$$

1. L'écriture précédente est-elle une écriture disjonctive ? conjonctive ?
2. Mettre f sous forme canonique disjonctive puis sous forme canonique conjonctive.

Exercice 1 - 54

Donner l'écriture canonique disjonctive puis conjonctive de toutes les fonctions booléennes de 2 variables. On remarquera néanmoins que la fonction nulle n'admet pas d'écriture canonique disjonctive.

Exercice 1 - 55

Combien existe-t-il de fonctions booléennes de 3 variables ?

Exercice 1 - 56

On considère la fonction booléenne de 4 variables définie par :

$$f = \overline{\left((\overline{a}+c+d)(b+c+d)(a+b+\overline{c})(a+\overline{c}+\overline{d})(a+\overline{b}+\overline{d})(\overline{b}+c+\overline{d})\right)}$$

1. L'écriture précédente est-elle une écriture disjonctive ? conjonctive ?
2. Mettre f sous forme canonique disjonctive puis sous forme cononique conjonctive.

Exercice 1 - 57

$f = f(a,b,c) = a+b+c$ est une fonction booléenne de 3 variables. Donner la forme canonique disjonctive de

f puis la forme canonique conjonctive de f.

Exercice 1 - 58

On définit deux autres opérateurs :

– l'opérateur $\downarrow$ défini par $1 \downarrow 1 = 1 \downarrow 0 = 0 \downarrow 1 = 0$ et $0 \downarrow 0 = 1$ qu'on appellera « NOR » ;

– l'opérateur $|$ défini par $1 \mid 0 = 0 \mid 1 = 0 \mid 0 = 1$ et $1 \mid 1 = 0$ qu'on appellera « NAND ».

1. Montrer que :

a. $\overline{x} = x \mid x = x \downarrow x$

b. $xy = (x \mid y) \mid (x \mid y)$

c. $x + y = (x \mid x) \mid (y \mid y)$

d. $xy = (x \downarrow y) \downarrow (y \downarrow y)$

e. $x + y = (x \downarrow y) \downarrow (x \downarrow y)$

2. Exprimer chacune des fonctions de l'exercice Exercice 1 - 50 page 120 en utilisant uniquement l'opérateur $|$ puis uniquement l'opérateur $\downarrow$.

Exercice 1 - 59 Machine à voter

Le gouvernement syldave est constitué de trois membres qui prennent toutes les décisions en votant à bulletins secrets. Une proposition est adoptée lorsqu'elle reçoit au moins deux votes sur trois. Leur conseiller technique, ancien étudiant de l'IUT de Nantes, leur propose un petit circuit qui détermine si une décision est adoptée.

On note x, y et z les variables booléennes qui correspondent à chacun des votes du triumvirat. Déterminer une fonction booléenne $f(x, y, z)$ qui réponde au problème et dessiner le circuit correspondant avec les portes NOT, AND et OR.

Exercice 1 - 60 Interrupteur

Le président syldave (il a fait exécuter les deux autres membres du gouvernement grâce à une chaise électrique mise au point par son conseiller technique) a fait construire un palais et désire que dans sa chambre, la lumière soit commandée par deux interrupteurs. En appuyant sur l'un quelconque des interrupteurs, il faut que la lumière s'allume si elle est éteinte et s'éteigne si elle est allumée. Déterminer une fonction booléenne $f(x, y)$ répondant au problème avec x et y correspondant à chacun des interrupteurs. Dessiner le circuit correspondant avec les portes NOT, AND et OR.

Reprendre le problème avec trois interrupteurs.

Exercice 1 - 61 Comparateur

Construire un circuit qui compare deux entiers de deux bits $(x_1x_0)_2$ et $(y_1y_0)_2$ et qui renvoie 1 si le premier est plus grand que le second et 0 sinon.

Exercice 1 - 62 NOR et NAND

Utiliser des portes NOR (puis NAND) pour obtenir les sorties suivantes :

1. $\overline{x}$

2. $x + y$

3. xy

4. $x \oplus y$

Exercice 1 - 63 Demi-additionneur

On veut additionner deux nombres binaires de deux bits. La sortie sera double : une variable u contiendra l'« unité » et une variable r contiendra la « retenue ». Dresser un tableau puis dessiner un circuit ayant deux sorties avec les portes NOT, AND et OR.

Exercice 1 - 64 Recherche : additionneur n-bits

Un peu de recherche : on dispose de demi-additionneurs (qu'on notera 1/2 Add) et de portes NOT, AND et OR.

Imaginez alors un additionneur complet qui prend en entrée un nombre de deux bits et une retenue et renvoie une unité et une retenue. On notera cette porte Add.

Imaginez alors comment, à l'aide de portes Add et 1/2 Add, fabriquer un additionneur n-bits.

Exercice 1 - 65

Dessiner le circuit correspondant aux fonctions suivantes puis simplifier les formules à l'aide d'un diagramme de KARNAUGH et dessiner le nouveau circuit à l'aide de portes NOT, AND et OR.

1. $f(x,y,z) = xy\overline{z} + x\overline{yz} + \overline{x}y\overline{z} + \overline{xyz}$.
2. $f(x,y,z) = \overline{x}yz\left((x+\overline{z}) + (\overline{y}+\overline{z})\right)$

Exercice 1 - 66

Simplifier les expressions suivantes à l'aide d'un diagramme de KARNAUGH.

1. $f(w,x,y,z) = wxyz + wx\overline{y}z + wx\overline{y}z + wx\overline{yz} + w\overline{x}y\overline{z} + w\overline{xy}z$
2. $f(w,x,y,z) = wxyz + wxy\overline{z} + wx\overline{y}z + w\overline{x}yz + w\overline{x}y\overline{z} + \overline{w}xyz + \overline{wx}yz + \overline{wx}y\overline{z} + \overline{wxyz}$

Relations binaires

Exercice 1 - 67

$E_1 = \{a,b,c,d\}, E_2 = \{0,1,2\}, E_3 = \{\alpha,\beta,\gamma,\delta,\epsilon\}$. On considére les relations $\mathcal{R} = (E_1,E_2,G_{\mathcal{R}})$ et $\mathcal{S} = (E_2,E_3,G_{\mathcal{S}})$ avec

$$G_{\mathcal{R}} = \{(a,0),(a,1),(c,1),(d,0)\}$$
$$G_{\mathcal{S}} = \{(1,\beta),(2,\delta),(2,\varepsilon)\}$$

1. Préciser $\operatorname{dom}\mathcal{R}$ et $\operatorname{Im}\mathcal{R}$.
2. $\mathcal{R}$ est-elle totale ?
3. Reprendre les questions précédentes avec $\mathcal{S}$.
4. Déterminer $\mathcal{S}\circ\mathcal{R}$. Préciser $\operatorname{dom}(\mathcal{S}\circ\mathcal{R})$ et $\operatorname{Im}(\mathcal{S}\circ\mathcal{R})$.
5. Déterminer les relations $\mathcal{R}^{-1}$ et $\mathcal{S}^{-1}$.
6. Vrai ou faux ?
   a. $a\mathcal{R}1$
   b. $\mathcal{R}(b,0)$
   c. $(1,c)\in\mathcal{R}^{-1}$
   d. $(a,\beta)\in\mathcal{S}\circ\mathcal{R}$
   e. $(a,\beta)\in\mathcal{R}.\mathcal{S}$
7. $\mathcal{R}^{-1}$ est-elle une fonction ?
8. Déterminer la relation $\mathcal{S}^{-1}.\mathcal{R}^{-1}$.
9. Déterminer $\mathcal{R}\circ\mathcal{S}$.
10. Déterminer les relations suivantes : $\mathcal{R}_{|\{a\}}$, $\mathcal{R}_{|\{b\}}$, $\mathcal{R}_{|\{a,b\}}$, $\mathcal{R}^{-1}_{|\{1\}}$, $\mathcal{R}_{|\{1\}}$.

Exercice 1 - 68

$\mathcal{R} = (E,F,G_{\mathcal{R}})$ et $\mathcal{R}' = (E',F',G_{\mathcal{R}'})$ sont deux relations.

1. Dans quel(s) cas $\mathcal{R}^{-1}$ n'existe pas ?
2. Dans quel(s) cas $\mathcal{R}\circ\mathcal{R}'$ n'existe pas ?
3. Dans quel(s) cas $\mathcal{R}\circ\mathcal{R}'$ et $\mathcal{R}'\circ\mathcal{R}$ existent simultanément ?

Exercice 1 - 69

$\mathcal{R}$ est une relation de E vers F dont le graphe est $G_{\mathcal{R}}$. Cette relation est notée

$$\mathcal{R} = (E,F,G_{\mathcal{R}}) \text{ avec évidemment } G_{\mathcal{R}} \subseteq E\times F$$

Si U est une partie de E, la relation $(U,F,G_{\mathcal{R}}\cap(U\times F))$ est notée $\mathcal{R}_{|U}$, c'est la restriction de la relation $\mathcal{R}$ à la partie U de E. La relation $(E,F,G_{\mathcal{R}}\cap(U\times F))$ est une sous relation de $\mathcal{R}$ qui est notée $U \lhd \mathcal{R}$, c'est une restriction de domaine de $\mathcal{R}$ à U. Sachant que U est une partie de E et V une partie de F, définir les relations suivantes en précisant leur ensemble de départ, leur ensemble d'arrivée et leur graphe

1. $\mathcal{R}_1 = \left(\mathcal{R}^{-1}_{|V}\right)^{-1}$.
2. $\mathcal{R}_2 = \left(\mathcal{R}^{-1}_{|V}\right)^{-1}_{|U}$.
3. $\mathcal{R}3 = \left(\left(\mathcal{R}_{|U}\right)^{-1}_{|V}\right)^{-1}$.
4. $\mathcal{R}_4 = \left(V \lhd \mathcal{R}^{-1}\right)^{-1}$ que l'on note $\mathcal{R} \rhd V$.
5. $\mathcal{R}_5 = U \lhd \left(V \lhd \mathcal{R}^{-1}\right)^{-1}$ que l'on note $U \lhd \mathcal{R} \rhd V$.
6. $\mathcal{R}_6 = \left(\left((U \lhd \mathcal{R} \rhd V)_{|U}\right)^{-1}_{|V}\right)^{-1}$.

Exercice 1 - 70

$E = \{a, b, c, d\}$, $F = \{1, 2, 3, 4, 5\}$, $G_{\mathcal{R}} = \{(a, 1), (a, 2), (c, 4), (d, 2), (d, 5)\}$ et $\mathcal{R}$ est la relation de E vers F qui a pour graphe $G_{\mathcal{R}}$.

1. Combien existe-t-il de relations de E vers F ?
2. Vrai ou faux ? Vous expliquerez votre réponse.
   a. $\mathcal{R} \in E \longleftrightarrow F$
   b. $\mathcal{R} \in \mathcal{P}(E \times F)$
   c. $\mathcal{R} = \left(E, F, G_{\mathcal{R}}\right)$
   d. $a\mathcal{R}1$; $(a, 1) \in \mathcal{R}$; $\mathcal{R}(a, 1)$
   e. $\mathcal{R}$ est une relation totale.
   f. $\mathcal{R}$ est une fonction.
3. Déterminer un ensemble B ayant un maximum d'éléments pour que $\left(\mathcal{R}^{-1}_{|B}\right)^{-1}$ soit une fonction.
4. Déterminer deux ensembles A et B ayant chacun un maximum d'éléments pour que $\left(\left(\mathcal{R}_{|A}\right)^{-1}_{|B}\right)^{-1}$ soit une fonction totale.
5. Déterminer deux ensembles A et B ayant chacun un maximum d'éléments pour que $\left(\left(\mathcal{R}_{|A}\right)^{-1}_{|B}\right)^{-1}$ soit une fonction totale surjective et non injective.
6. Déterminer deux ensembles A et B ayant chacun un maximum d'éléments pour que $\left(\left(\mathcal{R}_{|A}\right)^{-1}_{|B}\right)^{-1}$ soit une fonction totale injective et non surjective.
7. Déterminer deux ensembles A et B ayant chacun un maximum d'éléments pour que $\left(\left(\mathcal{R}_{|A}\right)^{-1}_{|B}\right)^{-1}$ soit une fonction totale bijective.
8. Déterminer un ensemble B ayant un maximum d'éléments pour que $(\mathcal{R} \rhd B)^{-1}$ soit une fonction.
9. Déterminer un ensemble A ayant un maximum d'éléments pour que $(A \lhd \mathcal{R})^{-1}$ soit une fonction.
10. Déterminer un ensemble A et un ensemble B ayant chacun un maximum d'éléments pour que $\left(\left(\left(\mathcal{R}_{|A}\right)^{-1}_{|B}\right)^{-1}\right)^{-1}$ soit une fonction totale.
11. Donner le résultat ou dire que l'écriture n'a pas de sens en expliquant pourquoi :
    a. $\mathcal{R}(c)$, $\mathcal{R}(\{b\})$
    b. $\mathcal{R}^{-1}(5)$, $\mathcal{R}^{-1}(\{d\})$
    c. $\mathcal{R}^2 = \mathcal{R} \circ \mathcal{R}$, $\mathcal{R}^{-1} \circ \mathcal{R}$
    d. $\mathcal{R}^{-1}(\{6\})$
12. Déterminer une relation $\mathcal{R}'$ de E vers F de sorte que $\mathcal{R} \cup \mathcal{R}'$ soit une relation totale.
13. Déterminer une relation $\mathcal{R}'$ de E vers F de sorte que $\mathcal{R} \cap \mathcal{R}'$ soit une fonction.

Exercice 1 - 71

$\mathcal{R}_1 = \left(E, F, G_{\mathcal{R}_1}\right)$ et $\mathcal{R}_2 = \left(E, F, G_{\mathcal{R}_2}\right)$ sont deux relations de l'ensemble E vers (ou dans) l'ensemble F, $G_{\mathcal{R}_i}$ est le graphe de la relation $\mathcal{R}_i$. On considère la relation $\mathcal{R} = \left(E, F, G_{\mathcal{R}}\right)$ dont les éléments (x, y) du graphe vérifient :

$$\text{si } (x, y) \in G_{\mathcal{R}_2} \text{ alors } (x, y) \in G_{\mathcal{R}}$$

$$\text{si } (x, y) \in G_{\mathcal{R}_1} \text{ et pour tout } z \in F, (x, z) \notin G_{\mathcal{R}_2} \text{ alors } (x, y) \in G_{\mathcal{R}}$$

Il vous est demandé d'exprimer le graphe de la relation $\mathcal{R}$ en utilisant les opérations ensemblistes usuelles et des ensembles choisis parmi les ensembles suivants : le domaine de $\mathcal{R}_1$ noté $\operatorname{dom}\mathcal{R}_1$, le domaine de $\mathcal{R}_2$ noté $\operatorname{dom}\mathcal{R}_2$, $G_{\mathcal{R}_1}$, $G_{\mathcal{R}_2}$, E et F.

Exercice 1 - 72

On considère les ensembles $E = \{a, b, c, d\}$ et $F = \{1, 2, 3\}$.

1. Combien existe-t-il de relations de E vers F ?

2. On considère les relations r et s suivantes :

$$\begin{aligned} r &= (\mathrm{E},\mathrm{E},\mathrm{G}_r) \\ \text{avec } \mathrm{G}_r &= \{(a,a),(a,b),(c,a),(b,c),(d,a)\} \\ s &= (\mathrm{E},\mathrm{F},\mathrm{G}_s) \\ \text{avec } \mathrm{G}_s &= \{(b,1),(c,1),(d,3)\} \end{aligned}$$

Pour les diagrammes qui suivent, il est exigé que l'ensemble de départ soit à gauche et l'ensemble d'arrivée à droite, si la question n'a pas de sens, dîtes-le en expliquant pourquoi.

- **a.** Donner un diagramme sagittal de la relation $r \circ r = r^2$
- **b.** Donner un diagramme sagittal de la relation $r.r^{-1}$
- **c.** Donner un diagramme sagittal de la relation $rs = r.s = s \circ r$
- **d.** Donner un diagramme sagittal de la relation $\left(\{1\} \lhd s^{-1}\right).\left(r^{-1} \rhd \{a,c,d\}\right)$
- **e.** Donner un diagramme sagittal de la relation $\left(r^{-1}_{|\{a,c\}}\right)^{-1}_{|\{a,c\}}$

3. Donner le résultat ou dire que l'écriture n'a pas de sens en expliquant pourquoi :

- **a.** $r(d) =$
- **b.** $(r \rhd \{a\})(c) =$
- **c.** $(r \rhd \{a\})(b) =$
- **d.** $r_{|\{a\}}(\{d\}) =$
- **e.** $\left(r_{|\{d\}}\right)(d) =$
- **f.** $\left(s_{|\{a\}}\right)(\{a\}) =$
- **g.** $s^{-1}(\{2\}) =$
- **h.** $(\{d\} \lhd r)(\{a\}) =$
- **i.** $sr(\{1\}) =$
- **j.** $s^{-1}r^{-1}(\{1\}) =$
- **k.** $r^{-1}(\{2\}) =$
- **l.** $(\{a,b\} \lhd s)^{-1}(1) =$

Exercice 1 - 73

$\mathrm{E} = \{12,13,33,51,111,128\}$, $\mathrm{F} = \{2,3,4,5,6,7\}$. On considére la relation $\mathcal{R}$ de E vers (ou dans) F définie par : $x \in \mathrm{E}, y \in \mathrm{F}, x\mathcal{R}y$ ssi la somme des chiffres utilisés dans l'écriture de x (on travaille en base 10) est égale à y.

1. Déterminer le domaine et le codomaine de $\mathcal{R}$, son graphe et donner un diagramme sagittal..
2. $\mathcal{R}$ est-elle une fonction ? L'écriture $\mathcal{R}(33)$ est-elle licite ?
3. $\mathcal{R}$ est-elle une application ?
4. Donner le graphe de $\mathcal{R}^{-1}$, $\mathcal{R}^{-1}$ est-elle une fonction ? L'écriture $\mathcal{R}^{-1}(6)$ est-elle licite ?
5. Calculer, si cela a un sens,
   - **a.** $\mathcal{R}(6)$, $\mathcal{R}(12)$, $\mathcal{R}(\{12\})$, $\mathcal{R}(\mathrm{E})$
   - **b.** $\mathcal{R}^{-1}(\{6\})$, $\mathcal{R}^{-1}(\mathrm{F})$, $\mathcal{R}^{-1}(2)$, $\mathcal{R}^{-1}(\{2\})$
6. Déterminer le graphe de la restriction de $\mathcal{R}$ à $\{33;51\}$
7. $\mathcal{R}_{|\mathrm{E}-\{128\}}$ est-elle une application ? Est-elle injective ? surjective ? bijective ?

Exercice 1 - 74

Donner la représentation sagittale d'une application de l'ensemble fini E dans l'ensemble fini F

1. non injective et non surjective ;
2. non injective mais surjective ;
3. injective mais pas surjective ;
4. bijective.

Exercice 1 - 75

Déterminez si les fonctions de $\mathbb{Z}$ dans $\mathbb{Z}$ suivantes sont injectives ou surjectives ou... ?

1. $f(n) = n - 1$;
2. $f(n) = n^2 + 12$;
3. $f(n) = n^3 + 37$;
4. $f(n) = \lfloor n/2 \rfloor$.

Exercice 1 - 76

Mêmes questions avec les fonctions de $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ suivantes :

1. $f(m,n) = 2m - n$;
2. $f(m,n) = m^2 - n^2$;
3. $f(m,n) = m^2 + n^2$;
4. $f(m,n) = |m| - |n|$;
5. $f(m,n) = m - n$;
6. $f(m,n) = |n|$;
7. $f(m,n) = m$;
8. $f(m,n) = m^2 - 4$.

Exercice 1 - 77

f est une application de E dans F, A et B sont deux parties de E et A' et B' sont deux parties de F. Démontrer :

1. $A \subseteq B \Rightarrow f(A) \subseteq f(B)$
2. $f(A \cup B) = f(A) \cup f(B)$
3. $f(A \cap B) \subseteq f(A) \cap f(B)$, donner un exemple où il n'y a pas égalité.
4. $A \subseteq f^{-1}\left(f(A)\right)$
5. $f^{-1}(A' \cap B') = f^{-1}(A') \cap f^{-1}(B')$
6. $f\left(f^{-1}(B')\right) \subseteq B'$
7. $A' \subseteq B' \Rightarrow f^{-1}(A') \subseteq f^{-1}(B')$
8. $f^{-1}(A' \cap B') = f^{-1}(A') \cap f^{-1}(B')$

Exercice 1 - 78

E, F et G sont 3 ensembles (tous les trois $\neq \emptyset$). $f \in \mathcal{A}(E,F)$, $g \in \mathcal{A}(F,G)$.

1. $g \circ f$ injective $\Rightarrow f$ injective. ?
2. $g \circ f$ surjective $\Rightarrow g$ surjective. ?
3. Si f et $f \circ g$ son injectives (surjectives), est-ce que g est injective (surjective) ?

Exercice 1 - 79

A est une partie non vide de l'ensemble E. Qu'appelle-t-on l'injection canonique de A dans E ?

Exercice 1 - 80

Démontrer que la relation réciproque de la fonction totale $f = (E, F, G_f)$ est une fonction ssi f est injective.

Exercice 1 - 81

$E = \{a, b, c, d\}$ et $F = \{1, 2, 3, 4, 5, 6\}$. Démontrer qu'il est impossible de construire une surjection et, a fortiori une bijection, de E sur F.

Exercice 1 - 82

Donner une bijection de $\mathbb{N}$ sur $\mathbb{Z}$.

Exercice 1 - 83

Lorsqu'on est en présence d'ensembles finis, il est facile de savoir s'il existe des injections ou surjections entre ces ensembles puisque si elles existent on est capable de les construire. Pour des ensembles infinis c'est plus difficile mais on est sûr qu'il n'existe pas de surjection entre un ensemble E et l'ensemble de ses parties $\mathcal{P}(E)$, c'est le théorème de Cantor [x], on va le démontrer :

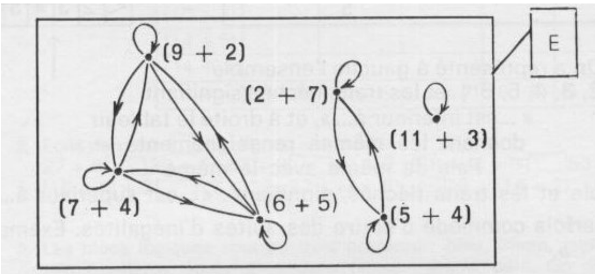
1. $E = \{a, b, c, d\}$ et f est la fonction totale de E dans $\mathcal{P}(E)$ définie par $f(x) = \{x\}$, déterminer
$$A = \left\{x \in E \mid x \notin f(x)\right\}$$
2. $E = \{a, b, c, d\}$ et f est la fonction totale de E dans $\mathcal{P}(E)$ définie par $f(x) = \complement_E \{x\}$, déterminer
$$A = \left\{x \in E \mid x \notin f(x)\right\}$$
3. $E = \{a, b, c, d\}$ et f est la fonction totale de E dans $\mathcal{P}(E)$ définie par $f(a) = \{b, c\}$ et $f(x) = E$ pour $x \neq a$, déterminer
$$A = \left\{x \in E \mid x \notin f(x)\right\}$$
4. E est un ensemble non vide quelconque, fini ou infini, et f est une fonction totale de E dans $\mathcal{P}(E)$; A est la partie de E définie par $A = \left\{x \in E \mid x \notin f(x)\right\}$ et pour prouver que f n'est pas surjective nous allons prouver que A ne peut avoir le moindre antécédent ! Pour cela on suppose que A possède au moins un antécédent u, $f(u) = A$. De deux choses l'une, ou bien $u \in A$ ou bien $u \notin A$; démontrer l'impossibilité de chaque cas et conclure.

x. Ne pas confondre avec le fameux théorème de Cantor-Bernstein (qui n'est pas à votre programme) qui dit que s'il existe une injection de E vers F et une injection de F vers E alors il existe une bijection de E sur F.

Relations binaires sur un ensemble

Exercice 1 - 84

Commentez cet énoncé de CM1 (on progresse...)



Exercice 1 - 85

1. Donner la représentation matricielle des relations suivantes définies sur $\{1,2,3,4\}$:
   - **a.** $\{(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)\}$;
   - **b.** $\{(1,1),(1,4),(2,2),(3,3),(4,1)\}$;
   - **c.** $\{(1,2),(1,3),(1,4),(2,1),(2,3),(2,4),(3,1),(3,2),(3,4),(4,1),(4,2),(4,3)\}$;
   - **d.** $\{(2,4),(3,1),(3,2),(3,4)\}$
2. Quelles sont, parmi ces relations, celles qui sont réflexives ? irrefléxives ? symétriques ? antisymétriques ? transitives ?

Exercice 1 - 86

1. Énumérer les couples des relations sur $\{1,2,3,4\}$ définies par les matrices suivantes :

   a. $\begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$ **c.** $\begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$

   b. $\begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$

2. Quelles sont, parmi ces relations, celles qui sont réflexives ? irrefléxives ? symétriques ? antisymétriques ? transitives ?

Exercice 1 - 87

Combien d'éléments non nuls contient la matrice représentant la relation $\mathcal{R}$ sur l'ensemble $\mathcal{E} = \{1,2,3,\dots,100\}$ si $\mathcal{R}$ est :

1. $\{(a,b) \mid a > b\}$;
2. $\{(a,b) \mid a \neq b\}$;
3. $\{(a,b) \mid a = b+1\}$;
4. $\{(a,b) \mid a = 0\}$;
5. $\{(a,b) \mid ab = 0\}$;
6. $\{(a,b) \mid a+b = 100\}$

Exercice 1 - 88

Soit $\mathcal{R} = \{(a,b) \in \mathbb{Z}^2 \mid a \neq b\}$ Quelle est la fermeture réflexive de $\mathcal{R}$?

Exercice 1 - 89

Soit $\mathcal{R} = \{(a,b) \in \mathbb{N}^2 \mid a \text{ divise } b\}$ Quelle est la fermeture symétrique de $\mathcal{R}$?

Exercice 1 - 90

Soit $\mathcal{E} = \{1,2,3,4,5\}$ et $\mathcal{R}$ une relation sur $\mathcal{E}$ qui contient les couples $(1,3)$, $(2,4)$, $(3,1)$, $(3,5)$, $(4,3)$, $(5,1)$, $(5,2)$ et $(5,4)$. Déterminer :

1. $\mathcal{R}^2$
2. $\mathcal{R}^3$
3. $\mathcal{R}^4$
4. $\mathcal{R}^5$
5. $\mathcal{R}^6$
6. $\mathcal{R}^+$

Exercice 1 - 91

On considère les relations binaires $\mathcal{R}$ et $\mathcal{S}$ sur $E = \{a;b;c;d;e\}$ qui ont pour graphe :

$$\begin{aligned} G_{\mathcal{R}} &= \{(a,a),(a,b),(b,c),(c,b),(e,b)\} \\ G_{\mathcal{S}} &= \{(a,a),(b,a),(b,b),(c,b),(e,b),(e,d)\} \end{aligned}$$

1. Donner une représentation sagittale de $\mathcal{R}$ et de

$\mathcal{S}$.

2. Déterminer le graphe de $\mathcal{R} \cup \mathcal{S}$, de $\mathcal{R} \cap \mathcal{S}$, de $\overline{\mathcal{R}}$, de $\mathcal{S}^{-1}$, de $\mathcal{RS}$ de $\mathcal{SR}$.

3. Déterminer le graphe de $\mathcal{R}^+$ et de $\mathcal{S}^*$.

Exercice 1 - 92

$\mathcal{R}$ est une relation binaire sur l'ensemble E et on suppose que $\mathcal{R}$ n'est pas une relation vide.

1. Rappeler ce qu'est $\mathcal{R}^{k \in \mathbf{N}^*}$.

2. Rappeler ce qu'est $\mathcal{R}^+$.

3. Rappeler ce qu'est $\mathcal{R}^*$.

4. Démontrer que si $x\mathcal{R}^9 z$ et $z\mathcal{R}^{2001} y$ alors $x\mathcal{R}^* y$

5. Traduire correctement $x\mathcal{R}^* y$.

6. Démontrer que $\mathcal{R}^*$ est une relation transitive.

Exercice 1 - 93

$\mathcal{R}$ est une relation binaire sur E

1. Démontrer que $\mathcal{R} \cup \mathcal{R}^{-1}$ et $\mathcal{R} \cap \mathcal{R}^{-1}$ sont symétriques.

2. Démontrer que $\mathcal{R}^+$ est transitive.

3. Démontrer que si $\mathcal{R}$ est transitive alors $\mathcal{R} = \mathcal{R}^+$.

4. Démontrer que si $\mathcal{R}$ est réflexive et transitive alors $\mathcal{R} = \mathcal{R}^*$

Exercice 1 - 94

$\mathcal{R}$ est une relation binaire sur $\mathrm{E} = \{a, b, c, d, e\}$ dont le graphe est

$$\mathrm{G} = \{(a,a), (a,b), (a,c), (b,a), (d,a), (b,e)\}$$

1. Complétez l'écriture : $\mathrm{G} \in$

2. Déterminer le graphe de $\mathcal{R}^2$.

3. Déterminer le graphe de $\mathcal{R}^3$, déterminer le graphe de $\mathcal{R}^{k \geq 2}$.

4. Quel est le graphe de $\mathcal{R}^0$?

5. Quel est le graphe de $\mathcal{R}^+$?

6. Quel est le graphe de $\mathcal{R}^*$?

7. $\mathcal{R}^*$ est-elle transitive ? justifier votre réponse.

8. Déterminer le graphe de $\mathcal{R}^{-1}$, de $\mathcal{R}^{-k}$, $k \in \mathrm{N}^*$.

Relations d'équivalence

Exercice 1 - 95

Dans $\mathbb{Z}$ on considère la relation $x\mathcal{R}y \Leftrightarrow x - y \in 3\mathbb{Z} = \{3k \mid k \in \mathbb{Z}\}$. Démontrer que c'est une relation d'équivalence et déterminer l'ensemble quotient ; vérifier que l'ensemble quotient détermine une partition de $\mathbb{Z}$.

Exercice 1 - 96

E est un ensemble non vide et A est une partie non vide fixée de E. On considére la relation binaire $\mathcal{R}$ sur $\mathcal{P}(\mathrm{E})$ définie par :

$$\mathrm{X}\mathcal{R}\mathrm{Y} \Leftrightarrow \mathrm{X} \cap \mathrm{A} = \mathrm{Y} \cap \mathrm{A}$$

1. *Démontrer que $\mathcal{R}$ est une relation d'équivalence.*

2. *On suppose ici que $\mathrm{E} = \{a, b, c, d\}$ et $\mathrm{A} = \{a, d\}$. Déterminer toutes les classes d'équivalence.*

Exercice 1 - 97

Soit $\mathcal{E}$ l'ensemble des fonctions dérivables de $\mathbb{R}$ dans $\mathbb{R}$.

On considère la relation $\mathcal{R}$ définie sur $\mathcal{E}$ qui contient toutes les couples (f, g) tels que $f'(x) = g'(x)$ pour tout réel x.

1. Est-ce que $\mathcal{R}$ est une relation d'équivalence ?

2. Décrire la classe de $f : x \mapsto x^2$.

Ordre

Exercice 1 - 98

On considère la relation $\preceq$ sur $\mathbb{N}^2$ définie par :

$$(a;b) \preceq (a';b') \Leftrightarrow a \leq a' \text{ et } b \geq b'$$

Est-elle une relation d'ordre ?

Exercice 1 - 99

E est un ensemble totalement ordonné par $\leq$. On considére la relation binaire sur E^2 définie par :

$$(x,y) \preceq (x',y') \Leftrightarrow \begin{cases} x < x' \text{ ou} \\ x = x' \text{ et } y \leq y' \end{cases}$$

Démontrer que c'est une relation d'ordre total. Cet ordre porte le nom d'ordre lexicographique, expliquer pourquoi ?

Exercice 1 - 100

Dans $\mathbb{N}^*$ on considère la relation notée « | » qui est la relation « divise », $a \mid b$ se lit « a divise b » ou encore « b est un multiple de a » ; la définition mathématique de cette relation étant

$$a \mid b \text{ ssi il existe } k \in \mathbb{N}^* \text{ vérifiant } b = ka$$

1. Démontrer que c'est une relation d'ordre sur $\mathbb{N}^*$. Cet ordre est-il total ? Donner des éléments comparables et non comparables.

2. Démontrer que c'est une relation d'ordre sur toute partie A de N^*.

3. On considère la relation divise dans $\mathrm{E} = \{2,4,6,8,10,12\}$.

- **a.** Construire le diagramme sagittal de cette relation.
- **b.** Construire le diagramme de Hasse de cette relation.
- **c.** E admet-il un élément minimum ?
- **d.** E admet-il un élément maximum ?
- **e.** E admet-il des éléments minimaux ?
- **f.** E admet-il des éléments maximaux ?
- **g.** $\mathrm{V} = \{2,4\}$, donner trois majorants de V dans E.
- **h.** $\mathrm{T} = \{8,10\}$ admet-il des majorants dans E ? Donner des majorants de T dans $\mathbb{N}^*$.
- **i.** Donner des minorants de T dans E.
- **j.** Donner tous les minorants de T dans $\mathbb{N}^*$.
- **k.** $\mathrm{U} = \{4,6,8\}$ admet-il une borne supérieure dans E ?
- **l.** $\mathrm{U} = \{4,6,8\}$ admet-il une borne supérieure dans $\mathbb{N}^*$?
- **m.** $\mathrm{U} = \{4,6,8\}$ admet-il une borne inférieure dans E ?
- **n.** $\mathrm{U} = \{4,6,8\}$ admet-il une borne inférieure dans $\mathbb{N}^*$?

Exercice 1 - 101

$(\mathrm{E}, \leq)$ est un ensemble ordonné. Représenter les différents diagrammes de Hasse pour un ensemble E de trois éléments. On précisera, pour chaque diagramme si E est totalement ordonné. Même question pour un ensemble de 4 éléments.

Exercice 1 - 102

$\mathbb{R}$ est muni de sa relation d'ordre habituelle et $\mathbb{R}^2$ est ordonné comme produit direct des ensembles ordonnés $(\mathbb{R}, \leq)$ et $(\mathbb{R}, \leq)$. Le plan P est rapporté à un repère orthonormé $\left(\mathrm{O}, \vec{i}, \vec{j}\right)$ et on pourra confondre tout point M du plan, qui a pour coordonnées x et y dans ce repère, avec le couple (x,y) de $\mathbb{R}^2$. Cela permet d'ordonner P par la relation :

$$\mathrm{M}_1 \preceq \mathrm{M}_2 \Leftrightarrow (x_1,y_1) \leq (x_2,y_2)$$

$\mathcal{C}$ désigne le cercle de centre O et de rayon 1, $\mathcal{D}$ désigne le disque de centre O et de rayon 1.

1. Donner 5 majorants et 5 minorants de $\mathcal{C}$ et de $\mathcal{D}$.

2. $\mathcal{C}$ et $\mathcal{D}$ admettent-ils une borne sup ? une borne inf ? un plus petit élément ? un plus grand élément ?

3. On note $\mathcal{D}^+$ l'ensemble des points de $\mathcal{D}$ qui ont leurs deux coordonnées positives ou nulles, $\mathcal{D}^+$ admet-il un plus petit élément ?

Exercice 1 - 103

Vérifier que $(\mathcal{P}(\mathrm{E}), \subseteq)$ est bien un ensemble ordonné. Soit $\{\mathrm{A}, \mathrm{B}\}$ une partie de $\mathcal{P}(\mathrm{E})$, déterminer sa borne sup et sa borne inf dans $\mathcal{P}(\mathrm{E})$.

Exercice 1 - 104

$\mathbb{N}_{10}$ est ordonné par la relation de divisibilité (rappel : $\mathbb{N}_{10} = \{1, 2, \cdots, 10\}$).

1. Tracer le diagramme sagittal de cette relation puis son diagramme de Hasse.
2. $\mathbb{N}_{10}$ admet-il un plus petit élément, un plus grand élément ?
3. Étudier les éléments remarquables (plus petit élément, majorant, borne sup, $\cdots$) des parties de $\mathbb{N}_{10}$ suivantes :
   a. $\mathrm{A} = \{1, 3, 6\}$
   b. $\mathrm{B} = \{2, 3\}$
   c. $\mathrm{C} = \{2, 3, 4\}$
   d. $\mathrm{D} = \{2, 4\}$

Dénombrement

Exercice 1 - 105

1. Combien existe-t-il de chaînes distinctes de 8 bits ?
2. Combien de chaînes de 10 bits commencent et finissent par 1 ?
3. Combien y a-t-il de chaînes de quatre lettres minuscules de l'alphabet latin contenant la lettre x ?
4. Combien de chaînes de caractères ASCII contiennent le caractère @ au moins une fois ? (il y a 128 caractères ASCII).
5. Combien de chaînes de 10 bits contiennent au moins trois 1 et trois 0 ?
6. Combien de chaînes de six caractères formées à partir de l'alphabet latin contiennent :
   a. exactement une voyelle ?
   b. au moins une voyelle ?
   c. exactement deux voyelles ?
   d. au moins deux voyelles ?
   e. la lettre a ?
   f. les lettres a et b ?