Combinatoire

Le cours intitule « Combinatoire » comprend deux parties distinctes, dont les thématiques sont voisines. La première partie consiste en une introduction aux notions de la théorie des ensembles; ces notions sont en principe déjà bien connues, et utilisées régulièrement dans d'autres cours de mathématiques (analyse, algèbre), mais elles sont traitées ici de manière séparée pour mettre l'accent sur les constructions et arguments purement « ensemblistes ». La deuxième partie est un premier aperçu du domaine de combinatoire proprement dit, où on considère notamment certains problèmes et techniques de dénombrement, l'art de déterminer la taille de certains classes d'ensembles finis sans avoir recours à une énumération explicite de leurs éléments.

Objectifs.

Dans les trois parties, l'objectif du cours n'est que de donner une introductions aux domaines considérés; en particulier, on n'a pas l'ambition d'exposer des résultats poussés. En contrepartie, la terminologie, la notation, et les techniques de bases présentées sont (en partie) nouvelles, et il est un objectif important du cours d'obtenir une facilité à les comprendre et utiliser.

Ce type de compétences n'étant pas facile à contrôler en isolation, les contrôles typiquement demandent de les appliquer dans des situations telles que:

- Comparaison de deux expressions ensemblistes, et décision s'il s'agit du même ensemble, si l'un des deux ensembles contient l'autre, ou s'il n'y a pas de telle relation.
- Questions concernant des notions telles que injectivité, surjectivité, image directe et indirect, composition et graphe d'applications, relations d'équivalence et ensembles quotient, et relations d'ordre; tout cela dans des exemples concrets.
- Questions de dénombrement (dont la réponse fait souvent intervenir des coefficients binomiaux, mais pas exclusivement) dans des situations appliquées (donc une compétence importante requise est de savoir modéliser la situation et sélectionner la formule pertinente).

Chapitre 1. Théorie d'ensembles.

Dans les domaines les plus classiques des mathématiques, tels que la géométrie, l'arithmétique, et le calcul différentiel et intégral, on travaille avec des objets et des valeurs atomiques (c'est-à-dire non composés) : points, droites, nombres, fonctions/formules. La notion d'ensemble n'y est donc pas indispensable, bien qu'on voit que certains problèmes ont plusieurs solutions, ou aucune, ce qui permet de concevoir dans ces cas l'ensemble des solutions. Ainsi notion d'ensemble fait une entrée assez timide en mathématiques, mais quand vers la fin du 19^{e} siècle elle est formalisée par la mathématicien allemand Georg Cantor, qui y est amené par l'étude des questions délicates concernant des ensembles infinis, le résultat a un effet fracassant. La théorie d'ensembles transformera les mathématiques profondément, et sera considérée au 20^{e} siècle comme sa théorie fondatrice, à la base de tous les domaines des mathématiques.

Les ensembles figurent en maths sous plusieurs formes. Ils apparaissent naturellement quand on ne veut considérer qu'une partie de toutes les valeurs possibles, par exemple les solutions d'une équation. Ainsi on pourrait définir un cercle comme un ensemble de points du plan qui ont tous une distance donnée r (avec $r > 0$) d'un point C du plan (le centre du cercle), également donné. Mais les ensembles sont aussi utiles pour décrire la totalité des valeurs qu'on veut considérer au départ pour un certain problème, décrivant ainsi le type des valeurs cherchées ; dans l'exemple donné, le plan est l'ensemble de toutes les valeurs (des points) qu'on veut considérer, et cet ensemble figure ainsi comme« type » pour le notion d'un point ; dire qu'une valeur considérée est un point revient ainsi à dire que cette valeur est élément de l'ensemble appelé « le plan ». Il est important de spécifier un tel ensemble de base avant même de parler des équations, car par exemple une même équation peut avoir des solutions différentes si on la considère pour des valeurs dans $\mathbf{Z}$, $\mathbf{R}$ ou $\mathbf{C}$. Dans presque tous les domaines des mathématiques modernes, on commence par désigner l'ensemble (ou les ensembles, si de différents types de valeurs sont considérés en même temps) des valeurs considérées, avant de préciser les propriétés et les relations entre ses valeurs auxquelles on s'intéresse. Ensuite, dans certains domaines la possibilité de formuler des propriétés non pas en termes de valeurs individuelles (les éléments d'un ensemble de base) mais également en termes de certains sous-ensembles de valeurs (intervalles ouverts ou fermés de $\mathbf{R}$ en analyse, par exemple, ou des courbes en géométrie) permet de formuler des propriétés de façon plus efficace et élégante qu'il ne serait possible autrement. Finalement, la possibilité de former de nouveaux ensembles à partir d'autres ensembles (comme sous-ensembles) ou même à partir de rien du tout (comme l'ensemble vide $\emptyset$, mais aussi par exemple l'ensemble $\{\emptyset\}$ ayant $\emptyset$ comme unique élément), permet de construire à l'intérieur de la théorie des ensembles de objets modélisant la valeurs de base d'une théorie (comme les nombres naturels, rationnel ou réels), et de considérer ainsi cette théorie comme fondatrice en mathématiques, fournissant le matériau brut étudié dans des domaines plus spécifique comme l'analyse ou l'algèbre.

Pour ces raisons, la connaissance des notions de base de la théorie d'ensembles est utile dans tous ces domaines. Dans ce cours on propose une première aperçu de cette théorie, avec un accent sur sa terminologie et ses notation. Mais si par sa nature fondatrice cette théorie est souvent présentée en isolation (donc sans supposer d'autres notions, comme celle des nombres naturels, l'idée étant qu'on peut ensuite « construire » ces nombres à l'intérieur de la théorie des ensembles), ce n'est pas notre but, et on se focalisera surtout à l'*utilisation* des ensembles dans divers contextes mathématiques.

1.1. *Notion d'un ensemble, langage ensembliste, parties d'un ensemble.*

Un ensemble est par nature un objet composé : il peut « posséder » certains autres valeurs, ses éléments (ou membres), et un ensemble est déterminé par les éléments qu'il possède. Les

ensembles sont eux-mêmes des valeurs, et peuvent être membre d'autres ensembles. Le plus souvent les éléments d'un ensemble sont tous du même type ; par exemple on peut former d'un côté un ensemble de nombre naturels, comme l'ensemble des nombres premiers, et d'autre côté un ensemble de vecteurs, comme un sous-espace de $\mathbf{R}^3$, mais former un ensemble qui contient à la fois des nombres et des vecteurs est inhabituel. Cependant, il est difficile d'interdire de tels ensembles, car dans la pratique «être du même type» veut dire appartenir à un même ensemble (préalablement établi) comme $\mathbf{N}$ ou $\mathbf{R}^3$, et selon sa formulation une telle interdiction risque d'être soit circulaire, soit trop restrictive pour la construction d'ensembles (si on exigeait par exemple que tous les éléments d'un nouvel ensemble formé appartiennent déjà à un ensemble préexistent). On se contentera donc simplement de se focaliser sur les ensembles dont les éléments sont d'un même type dans un sens informel, ce qui permet déjà des exemples assez compliqués.

Quand on parle d'un ensemble E, deux choses sont importantes: (1) pour tout valeur x (du bon type) il faut qu'il soit clair si v appartient à E (noté $x \in E$), ou non (noté $x \in E$), et (2) si $x \in E$ et $y \in E$, il faut pouvoir dire si $x = y$ ou non (c'est-à-dire $x \neq y$). Ce dernier point peut sembler redondant, car toute affirmation mathématique comme $x = y$ doit en principe être soit vrai soit faux, et cela indépendamment du fait que x et y appartiennent à E. Mais dans la pratique on veut souvent se réserver une troisième possibilité, à savoir dire que l'affirmation «$x = y$» n'a pas de sens, si x et y sont des valeurs de nature différentes (disons un nombre complexe et une application $\mathbf{N} \to \mathbf{N}$), qui ne sont pas comparables. L'acte de former un ensemble qui contient à la fois x et y donne pour ainsi dire à cette comparaison ses lettres de noblesse : si on le fait, on ne peut plus refuser de de se prononcer sur l'égalité entre x et y.

Il y a un autre cas de figure où les points (1) et (2) s'appliquent, quand un veut laisser un certain flou sur la question ce que *sont* les éléments de E, à condition de pouvoir dire quelle information est suffisante pour les décrire, quelle condition cette information doit vérifier (1), et quand deux informations décrivent le même élément (2). On peut penser à une définition de l'ensemble $\mathbf{Q}$ des nombres rationnels comme celui des expressions $\frac{p}{q}$ où (1) $p, q \in \mathbf{Z}$ et $q \neq 0$, et (2) on a $\frac{p}{q} = \frac{r}{s}$ si et seulement si $ps = qr$ dans $\mathbf{Z}$. Ainsi on n'a pas dit ce qu'est exactement une fraction $\frac{p}{q}$, mais la description de $\mathbf{Q}$ est suffisamment précise pour pouvoir travailler avec. Cette méthode de définition est surtout pratique quand l'information nécessaire est contenue dans une expression qu'on peut écrire sur le papier, comme une fraction, polynôme, ou matrice. Pour être cohérent, la condition de (2) doit être un relation d'équivalence ; on reviendra sur cette notion.

La théorie des ensembles parle essentiellement de valeurs d'un seul type, les ensembles, et de deux relations, l'égalité $x = y$ et l'appartenance $x \in A$; leurs négations seront écrites (comme d'habitude) en barrant le symbole de la relation : $x \neq y$ respectivement $x \notin A$. Un ensemble peut appartenir à un autre ensemble, donc dans une relation $x \in A$ non seulement A est un ensemble, mais x aussi peut être un ensemble. Dans la théorie des ensembles pure, on prétend que *toute* valeur est un ensemble, donc en particulier x dans "$x \in A$", mais dans la pratique on admet aussi que x peut être une valeur autre qu'un ensemble, comme un nombre ou une matrice. Pour de telles valeurs l'égalité est toujours définie, mais la notion d'appartenir à une telle valeur n'a pas de sens. La relation "$x \in A$" est prononcée de diverses manières: «x est élément de A» ou «x appartient à A» ou «A possède x». L'expression plus naturel «A contient x» est parfois utilisée, mais est à éviter quand il y a risque d'ambiguïté (quand x est un ensemble) avec la relation d'inclusion d'ensembles dont on parlera dans un instant.

On postule un nombre d'axiomes. La plupart affirme l'existence d'ensembles avec certains propriétés, mais un premier axiome fondamental décrit la relation d'égalité entre ensembles, en exprimant que les ensembles sont caractérisés par leurs éléments.

1.1.1. Axiome. *Si A, B sont des ensembles, alors $A = B$ si pour tout x on a $x \in A \Leftrightarrow x \in B$.*

Donc deux ensembles sont égaux dès qu'ils ont précisément les mêmes éléments. Dans la pratique on vérifie une égalité d'ensembles $A = B$ en montrant que pour chaque $x \in A$ on a aussi $x \in B$, et réciproquement pour chaque $y \in B$ on a aussi $y \in A$. Les deux parties de cette démonstration sont assez distinctes, d'où il est naturel de considérer une relation plus faible que l'égalité où l'on demande seulement l'une des deux parties; c'est la relation d'inclusion:

1.1.2. Définition. *Si A, B sont des ensembles, la relation $A \subseteq B$ veut dire que pour tout $x \in A$ on a $x \in B$; elle est prononcée « A est inclus dans B », ou « A est un sous-ensemble de B ».*

Cette relation s'écrit aussi sous forme renversée $B \supseteq A$. Le terme *partie* est un synonyme de sous-ensemble. On dit aussi « B contient A » pour $B \supseteq A$, mais comme indiqué cela risque l'ambiguïté avec la relation d'appartenance. Parfois on veut exclure $A = B$ de la relation $A \subseteq B$; on parle alors d'inclusion stricte $A \subset B$, qui par définition veut dire $A \subseteq B$ et $B \nsubseteq A$.

L'axiome ci-dessus se traduit en termes d'inclusion, donnant la proposition suivante.

1.1.3. Proposition. *Pour ensembles A, B on a $A = B$ si et seulement si $A \subseteq B$ et $A \supseteq B$.*

Maintenant on donne quelques axiomes qui affirment l'existence de certains ensembles. On ne cherche pas à être exhaustif, notre but étant juste de montrer les principaux ingrédients dans la construction des ensembles. On commence avec un axiome assez modeste (car il n'affirme que l'existence d'un seul ensemble), mais qui a l'avantage d'avoir aucune hypothèse, et qui peut donc servir comme point de départ pour des constructions plus ambitieuses. L'ensemble dont on affirme l'existence est le plus petit ensemble possible, l'ensemble vide.

1.1.4. Axiome [Ensemble vide]. *Il existe un ensemble E tel que pour tout x on ait $x \notin E$.*

Un tel ensemble est dit vide. Un ensemble vide E est une partie de n'importe quel ensemble A, car pour le montrer il faut prouver $x \in A$ pour tout x vérifiant $x \in E$, mais de tels x n'existent pas, donc il n'y a rien à démontrer. Par conséquent il ne peut exister qu'*un seul* ensemble vide, car si E, E' sont des ensembles vides, on a $E \subseteq E'$ et $E' \subseteq E$, donc $E = E'$. Puisqu'un unique ensemble vide existe, on pourra le désigner par un symbole ; on l'écrit $\emptyset$.

L'axiome suivant est beaucoup plus puissant, car il affirme l'existence d'un ensemble correspondant à *chaque propriété* (le terme officiel est « prédicat ») qu'on puisse formuler pour les éléments d'un ensemble donné. Un prédicat n'est pas un objet (ensemble), mais une entité linguistique : si P désigne le prédicat, alors $P(x)$ est une condition qui parle de x, une phrase ou formule qui peut être vraie ou fausse selon la valeur de x.

1.1.5. Axiome [Compréhension]. *Si U est un ensemble et P un prédicat tel que $P(x)$ soit défini pour tout $x \in U$, alors il existe un ensemble A tel que pour tout x, la condition $x \in A$ soit équivalent à "$x \in U$ et $P(x)$". Cet ensemble est unique, et est noté $A = \{\, x \in U \mid P(x) \,\}$.*

Cet axiome permet de former des ensembles tels que celui des nombres premiers, une fois que l'ensemble $\mathbf{N}$ des nombres naturels est disponible : pour cela on prend $U = \mathbf{N}$ et P la propriété d'être un nombre premier (propriété bien définie pour tout nombre naturel, et facile à exprimer formellement), et $A = \{\, n \in \mathbf{N} \mid n \text{ est premier} \,\}$ est l'ensemble des nombre premiers.

Dans l'axiome, l'unicité de A est simple à montrer : si A' était un autre ensemble tel que pour tout x la condition $x \in A'$ soit (aussi) équivalent à "$x \in U$ et $P(x)$", alors $x \in A'$ est équivalent à $x \in A$, ce qui prouve $A' = A$.

Il est clair que $A = \{\, x \in U \mid P(x) \,\}$ vérifie $A \subseteq U$, car "$x \in U$ et $P(x)$" entraîne $x \in U$. L'ensemble U joue donc un rôle limitatif dans la construction de A: on ne considère aucune valeur en dehors de U, et parmi ces valeurs on ne rassemble que celles qui vérifient le prédicat P.

On peut se demander si ce rôle est vraiment nécessaire ; après tout, on peut définir un nouveau prédicat P' où $P'(x)$ veut dire "$x \in U$ et $P(x)$", et dire que A est l'ensemble de toutes les valeurs x vérifiant $P'(x)$. Ne serait il pas possible de généraliser l'axiome en disant que pour tout prédicat P il existe un ensemble A tel que $x \in A$ soit équivalent à $P(x)$, sans restriction *a priori* sur x ?

La réponse est non. Le pionnier allemand Gottlob Frege de la logique mathématique a conçu au 19$^{\text{e}}$ siècle un formalisme dans lequel chaque prédicat définit un ensemble, ce qui correspond à la suggestion qu'on vient d'évoquer. Puis en 1903, le logicien anglais Bertrand Russell a remarqué que ce principe mène à une contradiction, connu depuis comme le paradoxe de Russell. Cet argument est extrêmement simple, et on l'explique brièvement.

Un simple conséquence du principe supposé que *tout* prédicat P corresponde un ensemble A tel que $x \in A \iff P(x)$, est l'existence d'un ensemble Ω pour lequel "$x \in \Omega$" est vrai quel que soit x ; il suffit de prendre un prédicat que est toujours vrai. Cet "ensemble de tout" est à l'opposé de l'ensemble vide $\emptyset$ pour lequel "$x \in \emptyset$" est faux quel que soit x. Mais on va montrer, en utilisant juste l'axiome de compréhension sous sa forme restreinte donnée initialement, que l'existence d'un tel Ω donne une contradiction ; ceci montre que non seulement le principe de compréhension généralisé ne peut pas être admis, on ne peut admettre aucune règle ou principe qui entraîne l'existence d'un "ensemble de tout".

1.1.6. Proposition. *Il n'existe pas de ensemble Ω tel que pour tout x on ait $x \in \Omega$.*

C'est étonnant qu'on puisse *prouver* l'impossibilité d'un tel ensemble, et cela avec seulement les axiomes donnés. La clé de la preuve est d'utiliser le prédicat P donné par $P(x)$ si et seulement si $x \notin x$.

Preuve. Supposons que Ω soit un tel ensemble, on va en tirer une contradiction. D'après l'axiome de compréhension, on peut former l'ensemble $C = \{\, x \in \Omega \mid x \notin x \,\}$, pour lequel par définition de $x \in C$:

$$C \in C \iff C \in \Omega \wedge C \notin C \iff C \notin C$$

(on peut enlever $C \in \Omega$ de la formule, car c'est toujours vrai par hypothèse sur Ω). Mais une condition (ici $C \in C$) ne peut jamais être équivalent à sa propre négation (que la condition soit vérifiée ou non). Notre conclusion est donc une contradiction, et l'hypothèse disant que Ω existe est donc fausse. □

L'axiome de compréhension ne produit que des sous-ensembles d'ensembles existants, donc pour assurer l'existence d'autres ensembles que l'ensemble vide, on a besoin d'autres axiomes. L'axiome suivant produit pour chaque ensemble A un nouvel ensemble $\mathcal{P}(A)$ qui est «plus profond», dans le sens où il possède A comme élément (car on a toujours $A \subseteq A$) :

1.1.7. Axiome [l'Ensemble des parties]. *Pour tout ensemble A il existe un ensemble E pour lequel $B \in E \iff B \subseteq A$. On appelle E l'ensemble des parties de A, noté $E = \mathcal{P}(A)$*

Voici un exemple concret: en prenant $A = \{2, 4, 7\}$, tout ensemble ne possédant par d'autres éléments que ceux de A est une partie de A et donc un élément de $\mathcal{P}(A)$. On peut énumérer ces parties explicitement :

$$\mathcal{P}(\{2, 4, 7\}) = \{\emptyset, \{2\}, \{4\}, \{7\}, \{2, 4\}, \{2, 7\}, \{4, 7\}, \{2, 4, 7\}\}.$$

Bien que aucun élément de $\mathcal{P}(A)$ n'a plus d'éléments que A, on voit que l'ensemble $\mathcal{P}(A)$ lui-même a nettement plus d'éléments que A (et c'est une règle générale): 8 contre 3. On montrera plus tard que si A est un ensemble fini à n éléments, alors $\mathcal{P}(A)$ est un ensemble fini à 2^n éléments.

Pour chaque prédicat P défini sur A, l'ensemble $\mathcal{P}(A)$ possède un élément correspondant $\{\, x \in A \mid P(x) \,\}$. Et réciproquement pour $B \in \mathcal{P}(A)$, c'est-à-dire $B \subseteq A$, on a un prédicat $Q(x)$ défini par $x \in B$ sur A. La partie $\{\, x \in A \mid x \in B \,\}$ correspondant à ce prédicat Q est bien égale à B. On a envie de dire que cela marche aussi dans l'autre sens, mais les prédicats ne sont pas des valeurs, donc on ne parlera pas de leur égalité. Mais on peut définir l'*équivalence* logique de deux prédicats P, Q définis sur un même ensemble A : c'est le cas si l'on a $P(x) \iff Q(x)$ pour tout $x \in A$. La proposition suivante découle alors directement des définitions :

1.1.8. Proposition. *Si P, Q sont deux prédicats définis sur un même ensemble A, alors ils sont logiquement équivalents si et seulement si $\{ x \in A \mid P(x) \} = \{ x \in A \mid Q(x) \}$ dans $\mathcal{P}(A)$.*

Cette correspondance entre prédicats et parties entraîne une correspondance entre des connecteurs logiques tels que «et» et «ou» et des opérations définies sur $\mathcal{P}(A)$. Ainsi, pour deux prédicats P, Q définis sur A, on peut définir un nouveau prédicat par la condition $x \in E$ vérifie à la fois P et Q, noté en formalisme logique comme $P(x) \wedge Q(x)$; la partie de A correspondant à ce nouveau prédicat est par définition l'*intersection* $V \cap V'$ des parties $V = \{ x \in A \mid P(x) \}$ et $V' = \{ x \in A \mid Q(x) \}$ correspondant à P respectivement Q. Autrement dit on définit $V \cap V' = \{ x \in A \mid P(x) \wedge Q(x) \}$; on remarquera la similitude des symboles $\wedge$ du connecteur logique et $\cap$ de l'opération sur $\mathcal{P}(A)$. De façon similaire on définit $P(x) \vee Q(x)$ (prononcé «ou») par la condition que x vérifie l'un au moins de P et Q, et pour opération correspondante sur $\mathcal{P}(A)$ la *réunion* noté $V \cup V'$ et définie par $V \cup V' = \{ x \in A \mid P(x) \vee Q(x) \}$.

Finalement on a la négation (d'une seule condition, par vraiment un "connecteur" donc) noté $\neg$; elle correspond à une opération sur $\mathcal{P}(A)$, mais cette fois-ci sans ressemblance pour les symboles utilisés. La négation de P est vérifié par tout $x \in A$ qui ne vérifie pas P (et seulement par ces x là), et correspond à opération de complémentaire dans A d'une partie V, noté $A \setminus V = \{ x \in A \mid x \notin V \}$ (parfois aussi écrit $A - V$). Si l'ensemble A est fixé dans le contexte, on trouve aussi la notation V^{c} pour ce complémentaire.

Une des première opérations qu'on apprend concernant les ensembles est qu'on peut toujours former une ensemble qui contient un certain nombre de valeurs explicitement données, et rien d'autre ; si par exemple on a trois valeurs a, b, c, cet ensemble est désigné par $\{a, b, c\}$, et est censé d'exister sans aucune condition sur a, b, et c. (En particulier on n'exclut pas une égalité entre deux ou tous valeurs, d'où $\{a, b, c\}$ n'a pas toujours trois éléments, mais parfois 2 ou 1 ; mais c'est une digression.)

1.1.9. Axiome. *Si $a_1, a_2, \ldots, a_n$ est une liste finie de valeurs, il existe une ensemble L tel que*

$$x \in L \iff (x = a_1 \vee x = a_2 \vee \cdots \vee x = a_n)$$

Cet ensemble est unique, et noté $L = \{a_1, a_2, \ldots, a_n\}$.

1.1.10. Axiome. *Si A est un ensemble dont tous les éléments sont des ensembles, alors il existe une ensemble U tel que*

$$x \in U \iff \exists P \in A : x \in P$$

Cet ensemble est unique, et noté $U = \bigcup A$. Dans le cas particulier $A = \{P_1, \ldots, P_n\}$ on note $\bigcup\{P_1, \ldots, P_n\} = P_1 \cup \cdots \cup P_n$.

Cette dernière opération (réunion de tous les éléments de A) peut être visualisée (pour des ensembles finis) comme l'opération qui enlève les accolades directement intérieur aux accolades extérieures). Par exemple

$$\bigcup\{\{1\}, \{\}, \{4, 5\}, \{4, 9, 10, 11\}, \{\{4\}\}\} = \{1,\ 4, 5, 4, 9, 10, 11, \{4\}\} = \{1, 4, 5, 9, 10, 11, \{4\}\}$$

et pour un cas où A est un ensemble infini (avec $\mathbf{N}_{>1}$ une l'abréviation pour $\{ n \in \mathbf{N} \mid n > 1 \}$) :

$$\bigcup \{ \{ ik \mid k \in \mathbf{N}_{>1} \} \mid i \in \mathbf{N}_{>1} \} = \{4, 6, 8, \ldots, 6, 9, 12, \ldots, 8, 12, 16, \ldots, 10, 15 \ldots\}$$

ce qui donne après tri et suppression des doublés l'ensemble $\{4, 6, 8, 9, 10, 12, 14, 15, \ldots\}$ des nombres naturels (multiplicativement) composés (le complément dans $\mathbf{N}_{>1}$ des nombres premiers).

On est finalement arrivé à un point ou on peut construire quelques exemples d'ensembles finis ; on commence par voir ce qu'on obtient en théorie pure des ensembles (donc sans supposer l'existence d'autre chose, comme des nombres). On a déjà vu l'ensemble vide $\emptyset = \{\,\}$. Il est différent que le singleton formé à partir de $\emptyset$, car $\{\emptyset\}$ contient un élément (à savoir $\emptyset$) ce qui n'est pas le case de $\emptyset$. Ce singleton $\{\emptyset\}$ est le même ensemble que celui $\mathcal{P}(\emptyset)$ des parties de l'ensemble vide, car $\emptyset$ n'a qu'un seul sous-ensemble, à savoir $\emptyset$ (pour avoir $A \subseteq \emptyset$, il faut que $x \in A$ entraîne $x \in \emptyset$, mais cette conclusion étant absurde, l'implication ne peut être valable que si l'hypothèse $x \in A$ est aussi absurde, c'est-à-dire si $A = \emptyset$). L'ensemble $\mathcal{P}(\{\emptyset\})$ est parties de $\{\emptyset\}$ possède deux éléments, l'ensemble vide (qui est partie de n'importe quel ensemble) et $\{\emptyset\}$ lui même : $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$. En fait on a $\mathcal{P}(\{a\}) = \{\emptyset, \{a\}\}$, quel que soit a : une partie du singleton $\{a\}$ ne peut avoir aucun élément distinct de a, donc la seul question restante est si elle possède a comme élément ou non, et les deux réponses sont possibles. On peut continuer à prendre l'ensemble des parties de $\mathcal{P}(\{\emptyset\})$, ce qui donne un ensemble à 4 éléments : $\mathcal{P}(\{\emptyset, \{\emptyset\}\}) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$. On voit que cela devient vite grand, et compliqué.

On peut facilement construire une infinité d'ensembles distincts. Par exemple on peut poser $E_0 = \emptyset$, $E_1 = \{\emptyset\}$, et ensuite pour tout $n \in \mathbf{N}$ poser par récurrence $E_{n+1} = E_n \cup \{E_n\}$ (exercice : vérifier que pour $n = 0$ on obtient effectivement $E_1 = \{\emptyset\}$). On a $E_n \subset E_{n+1}$, car d'un côté $E_n \subseteq E_n \cup \{E_n\} = E_{n+1}$, et d'autre côté $E_n \in E_{n+1}$ pendant que $E_n \notin E_n$; il en découle que $E_i \neq E_j$ quand $i \neq j$. Ce qu'on *ne saura pas construire* avec les axiomes donnés est un ensemble qui contient à la fois chacun des E_i ; c'est étonnant, mais essayez le pour vous en convaincre. En fait on ne saura construire aucun ensemble infini. C'est pour cela qu'on a besoin d'un axiome supplémentaire pour assurer l'existence de tels ensembles (on ne le formulera pas ici, car on n'est pas encore prêt à exprimer la propriété d'être un ensemble infini).

On peut visualiser les ensembles (finis, ou avec un peu d'imagination infinis) comme des conteneurs dans lequel sont stockés leurs éléments. La notation $\{a_1, a_2, \ldots, a_n\}$ pour les ensembles finis renforce ce point de vue. Cependant il est important d'observer les point suivants, ou l'image d'un conteneur peut être trompeur : (1) un élément ne peut apparaître dans un ensemble donné qu'une seul fois (une valeur appartient à un ensemble ou non, elle ne peut pas y «appartenir plusieurs fois»), et (2) il n'y a pas d'ordre dans lequel ses éléments apparaissent dans un ensemble. Donc si a, b, c sont des valeurs distinctes, on a par exemple les égalités $\{a, a\} = \{a\}$, $\{a, b, c\} = \{c, a, b\}$, $\{a, b, a\} = \{b, a, b\} = \{a, b\}$, et $\{\{a, b\}\} = \{\{a, b\}, \{b, a\}\}$.

1.2. *Produit cartésien, relations, applications.*

On vient d'indiquer qu'on ne peut pas considérer un ensemble comme un conteneur dans lequel sont rangés différentes valeurs, mais on a souvent besoin de valeurs qui ont bien cette possibilité. Pour combiner deux on plusieurs valeurs en une seule valeur, on peut former un couple ou un n-uplet. La question que c'est exactement un n-uplet est peu importante, et on de donnera pas une réponse exacte ; ce qui importe sont les opérations qu'on peut définir pour ces valeurs. Si l'on a n valeurs quelconques, disons $a_1 \in A_1$, $a_2 \in A_2$, $\ldots$, $a_n \in A_n$ (chaque valeur est élément d'un certain ensemble, pas forcément toutes du même ensemble), alors on peut former leur n-uplet, qui sera noté $(a_1, a_2, \ldots, a_n)$, et pour chaque $i = 1, 2, \ldots, n$ on a une opération qu'on appelle π_i qui récupère la valeur a_i du n-uplet. Tous les n-uplets ainsi formés, avec les ensembles $A_1, A_2, \ldots, A_n$ fixés, forment un ensemble noté $A_1 \times A_2 \times \cdots \times A_n$ et appelé produit cartésien des ensembles A_i. (Il est possible de réaliser les produits cartésiens dans la théorie des ensembles pure, en identifiant les n-uplets à certains ensembles particuliers, et en définissant les opérations π_i de façon convenable Mais on ne détaille pas cela, car on ne parlera jamais des *éléments* d'un n-uplet u ; les valeurs $\pi(u)$ sont les *composantes* du n-uplet.) On exige les

relations évidents $\pi_i((a_1,\ldots,a_n)) = a_i$ pour $i = 1,\ldots,n$, ainsi que $(\pi_1(u),\ldots,\pi_n(u)) = u$ pour tout n-uplet u. On a $(x_1,\ldots,x_n) = (y_1,\ldots,y_n)$ si et seulement si $x_i = y_i$ pour $i = 1,2,\ldots,n$.

On peut visualiser un produit cartésien $A \times B$ par un rectangle, ou les coordonnées horizontale et verticale d'un élément $u \in A \times B$ correspondent aux composantes $a = \pi_1(u) \in A$ et $b = \pi_2(u) \in B$ de $u = (a,b)$. En fait, si A et B sont des intervalles de $\mathbf{R}$ cette image est parfaitement exacte ; pour des ensembles plus généraux on peut toujours imaginer que leurs éléments étiquettent les deux côtés d'un rectangle.

Le produit cartésien de deux ensembles X, Y (où il n'est pas interdit de prendre deux fois le même ensemble, c'est-à-dire $X = Y$) permet de représenter une relation entre membres de X et Y par un ensemble. Une relation (binaire) est comme un prédicat sauf qu'elle parle de deux valeurs x, y au lieu d'une, c'est donc un phrase ou expression qui contient x et y ; on a déjà vu les exemples de l'égalité $x = y$, l'appartenance $x \in y$, l'inclusion $x \subseteq y$ et l'inclusion stricte $x \subset y$, et chaque fois on a aussi leurs négations $x \neq y$, $x \notin y$, etc. Puisque dans la pratique une relation est le plus souvent désigné par un symbole écrit *entre* les valeurs, on écrira $x \mathcal{R} y$ pour désigner une relation $\mathcal{R}$ qui vaut entre x et y.

Une relation entre éléments de X et Y est donc essentiellement un prédicat défini sur $X \times Y$. Tout comme un prédicat P défini sur un ensemble U correspond à la partie $\{\, x \in U \mid P(x) \,\}$ de U, une relation $\mathcal{R}$ entre éléments de X et Y correspond à la partie $G = \{\, (x,y) \in X \times Y \mid x \mathcal{R} y \,\}$ de $X \times Y$. Cet ensemble est appelé le « graphe » de la relation. Par exemple, si $X = Y = [0,1]$, un intervalle de $\mathbf{R}$, alors $I \times I$ est un carré, et la relation $x \mathcal{R} y$ donné par $x \leq y$ a pour graphe un sous-ensemble triangulaire de ce carré : la diagonale principale et tous les points du carré au dessus de celle-ci (avec la convention usuelle pour les coordonnées cartésiennes).

1.2.1. Proposition. *Si $\mathcal{R}, \mathcal{R}'$ sont tous deux des relations entre les ensembles X et Y, alors elles sont logiquement équivalentes (c'est-à-dire $x \mathcal{R} y \iff x \mathcal{R}' y$ pour tout $x \in X$ et $\in Y$) si et seulement si leurs graphes sont égaux (en tant que parties de $X \times Y$).*

Ainsi la notion d'équivalence logique de deux relations devient très concret, en se traduisant en égalité de deux ensembles (leurs graphes). Une autre notion pour laquelle il est important d'avoir une notion concrète d'équivalence est celle des applications (aussi appelées fonctions). Contrairement aux relations, on considère souvent des applications comme étant elles mêmes des *valeurs*, et dans ce cas on considérera deux applications équivalentes $X \to Y$ comme *égales*.

Une application $X \to Y$ donne une règle qui associe à chaque $x \in X$ un élément de Y. La nature de cette règle n'est pas spécifiée. Elle peut consister d'une expression $\mathcal{E}$ qui décrit la valeur associée à x en termes de x, par exemple $\mathcal{E} = x^2 - x$ (dans ce cas l'expression $x \mapsto \mathcal{E}$ désigne l'application ; plus souvent on donne un nom à l'application, disons f, et on écrit $f(x) = \mathcal{E}$). Mais une application peut aussi être donnée par un tableau donnant tous les $x \in X$ avec chaque fois les valeurs associée dans Y (cette méthode s'applique seulement quand X est un ensemble fini). On peut également spécifier une application par un algorithme, pourvu qu'on puisse prouver sa terminaison dans tous les cas, ou encore par d'autre moyens (distinction de cas,...). Quelle que soit la méthode de description, la valeur $f(x) \in Y$ doit être bien défini pour tout $x \in X$, et ne dépendre que de x (donc si $x = x'$ dans X alors $f(x) = f(x')$ dans Y), ce qui justifie la notation $f(x)$. Deux fonctions $f, g : X \to Y$ sont égales si $\forall x \in X : f(x) = g(x)$.

Beaucoup d'objets mathématiques composés sont modélisés par des applications. À titre d'exemple, une suite infinie $(a_0, a_1, a_2, \ldots)$ de nombres réels a_i est modélisée par une application $\mathbf{N} \to \mathbf{R}$ à savoir $i \mapsto a_i$, ou une matrice $n \times m$ à coefficients complexes par une application $\{1,\ldots,n\} \times \{1,\ldots,m\} \to \mathbf{C}$ qui associe à un couple (i,j) d'indices l'entrée $A_{i,j}$.

1.3. *Attributs des applications (domaine, codomaine, graphe, image).*

Quand on parle d'une application, il sera toujours sous-entendu que les ensembles X, Y telle que qu'il s'agisse une application $X \to Y$ sont connus ; on appelle X le domaine de l'application, et Y son codomaine.

Une application $f : X \to Y$ détermine une relation entre X et Y, à savoir « $f(x) = y$ » (qui peut être vrai ou faux selon les values $x \in X$ et $y \in Y$ choisies), et on définit le *graphe de* f comme le graphe de cette relation, soit l'ensemble $\{\, (x, y) \in X \times Y \mid f(x) = y \,\}$, pour lequel on a aussi la notation équivalente $\{\, (x, f(x)) \mid x \in X \,\}$. Deux applications $f, g : X \to Y$ sont égales si et seulement si leurs graphes sont égaux : d'une part si $f(x) = g(x)$ pour tout $x \in X$ alors la relation « $f(x) = y$ » exprime la même condition que « $g(x) = y$ », et leurs deux graphes sont donc les mêmes ; d'autre part si $G \subseteq X \times Y$ est à la fois le graphe de f et de g, alors pour tout $x \in X$ on peut caractériser $f(x)$ comme l'unique $y \in Y$ tel que $(x, y) \in G$, mais c'est aussi une caractérisation de $g(x)$, donc $f(x) = g(x)$.

Contrairement au graphe d'une relation, le graphe d'une application ne peut pas être n'importe quel partie de $X \times Y$. On vient de voir qu'un graphe G d'une application possède la particularité que pour tout $x_0 \in X$ l'ensemble $\{\, y \in Y \mid (x_0, y) \in G \,\}$ est un singleton (si c'est $\{y_0\}$, alors y_0 est l'image par l'application de x_0). De façon équivalente, l'intersection de G avec $\{\, (x_0, y) \mid y \in Y \,\}$ (une « droite verticale » si l'on imagine x et y comme des coordonnées cartésiennes) est toujours un singleton $\{(x_0, y_0)\}$. Par contre on ne saura rien dire des ensembles de la forme $\{\, x \in X \mid (x, y_0) \in G \,\}$ pour un $y_0 \in Y$ fixé (l'intersection de G avec une « droite horizontale ») ; elle peut être n'importe que partie de X, y compris la partie vide. Dire que c'est effectivement la partie vide veut dire qu'il est impossible de trouver $x \in X$ tel que $f(x) = y_0$, et on dit que y_0 n'est pas dans l'image de f. En fait, on définit comme *image* de l'application f, notée $\mathrm{Im}(f)$ l'ensemble $\{\, y \in Y \mid \exists x \in X : f(x) = y \,\}$, une partie de Y.

Cette description de l'image de f parcourt Y, et cherche pour chaque élément y un $x \in X$ pour lequel il s'écrit comme $f(x)$. Il est un peu plus intuitif de parcourir X, et pour chaque tel x calculer $f(x)$ qui appartient à $\mathrm{Im}(f)$; ainsi on trouve (sans mentionner Y) la totalité des éléments de $\mathrm{Im}(f)$, certains éventuellement plusieurs fois. La notation suivante correspond à cette intuition : si $f : X \to Y$, alors

$$\{\, f(x) \mid x \in X \,\} \quad \text{est défini comme l'ensemble} \quad \{\, y \in Y \mid \exists x \in X : f(x) = y \,\}.$$

On a donc $y \in \{\, f(x) \mid x \in X \,\}$ si et seulement si $\exists x \in X : f(x) = y$ (on pourra rajouter la condition $y \in Y$, mais elle est une conséquence de l'autre, c'est-à-dire de $\exists x \in X : f(x) = y$). Il n'est pas nécessaire d'avoir un nom f pour cette transformation, il suffit que $f(x)$ soit une expression désignant une valeur construite à partir de x. On pourra par exemple désigner par $\{\, x^4 - 2x^3 + 4x - 7 \mid x \in \mathbf{R} \,\}$ l'image de l'application $\mathbf{R} \to \mathbf{R}$ donnée par $x \mapsto x^4 - 2x^3 + 4x - 7$.

Comme dit ci-dessus, on considère la connaissance du domaine et du codomaine d'une application une partie intégrante de sa spécification. Ce n'est pas tellement parce qu'on voudrait pouvoir comparer deux applications n'ayant pas le même domaine ou codomaine (c'est rarement voulu, mais si on le faisait il faudrait les considérer d'office distinctes), mais parce qu'on veut pouvoir définir des propriétés d'applications qui font référence au domaine ou codomaine. Mais il est souvent utile d'associer à $f : X \to Y$ certaines applications $f' : X' \to Y'$ avec $X' \subseteq X$ et $Y' \subseteq Y$, où la relation $f'(x) = y$ est *la même* que $f(x) = y$, mais seulement limitée au cas $x \in X'$ et $y \in Y'$ (on ne change donc pas la règle de l'application, juste son domaine et/ou codomaine). Une telle application f', déterminée par f une fois que X' et Y' sont spécifiés, s'appelle une *restriction* de f. Si on ne change pas le codomaine ($Y' = Y$), on peut prendre $X' \subseteq X$

quelconque, et obtient *la restriction* de f à X', notée $f|_{X'}$, dont le graphe est $\{\,(x, f(x) \mid x \in X'\,\}$. Si on garde le domaine ($X' = X$), on n'a pas la liberté de prendre $Y' \subseteq Y$ quelconque, car il faut assurer que $\mathrm{Im}(f) \subseteq Y'$ (sinon certains $f(x)$ tombent en dehors de Y') ; dans ce cas on peut parler d'une «restriction à l'arrivée» de f (mais cette terminologie n'est pas établie). On peut observer que dans ce dernier cas le graphe de la restriction est *le même* que le graphe de f.

1.4. *Surjectivité, injectivité, existence d'application réciproque.*

Pour une relation $\mathcal{R}$ entre ensembles X et Y on peut toujours former une relation $\mathcal{R}'$, dite relation réciproque (ou inverse), entre Y et X qui intervertit simplement les rôles des deux arguments ; autrement dit, on a par définition $y\,\mathcal{R}'\,x \iff x\,\mathcal{R}\,y$. Ainsi par exemple la relation '$\geq$' sur $\mathbf{R}$ est la réciproque de '$\leq$', et la relation '$\in$' entre X et $\mathcal{P}(X)$ (pour un ensemble X quelconque) possède une relation réciproque entre $\mathcal{P}(X)$ et X qui est parfois noté '$\ni$'. Le graphe de la relation réciproque $\mathcal{R}'$ est $\{\,(y, x) \mid (x, y) \in G\,\}$ où G est le graphe de $\mathcal{R}$ (c'est le transposé ${}^{\top}G$ du graphe G).

Pour une application $f : X \to Y$, les choses sont pas aussi simples. On a vu que le graphe G de f vérifie une condition qui n'est pas symétrique en x et y, donc son transposé ${}^{\top}G$ n'est pas forcément le graphe d'une application $Y \to X$. Si toutefois c'est le cas, disons que ${}^{\top}G$ est le graphe de $g : Y \to X$, alors on appellera g «application réciproque» de f. Considérons les conditions pour qu'une telle application réciproque existe.

Le graphe ${}^{\top}G$ est bien le graphe d'une *relation* entre Y et X, à savoir $y = f(x)$. Pour que cette relation soit une application $Y \to X$, il faut que pour tout $y \in Y$ il existe un et un seul $x \in X$ tel que $y = f(x)$. On appelle un tel x un *antécédent* de y pour f. Il s'avère utile de séparer les conditions, pour tout $y \in Y$, de l'existence et de l'unicité d'un antécédent, donnant lieu aux définitions suivantes

1.4.1. Définition. *Une application $f : X \to Y$ est surjective si tout $y \in Y$ possède (au moins) un antécédent pour f, ou de façon équivalente, si l'image* $\mathrm{Im}(f)$ *est égal au codomaine Y de f.*

On observe que la condition pour être surjectif dépend explicitement du codomaine Y de f. Une restriction à l'arrivée peut «rendre surjective» une application qui ne l'est pas ; en effet, la restriction à $Y' = \mathrm{Im}(f)$ à l'arrivée (la plus petite possibilité) est par construction surjective.

1.4.2. Définition. *Une application $f : X \to Y$ est injective si tout $y \in Y$ possède au plus un antécédent pour f, c'est à dire si $f(x) = f(x')$ avec $x, x' \in X$ entraîne $x = x'$.*

La reformulation de la condition ne mentionne pas $y \in Y$, car si x, x' sont deux antécédents d'un même y, on aura $y = f(x) = f(x')$. De façon informelle, f est injectif s'il n'y a pas de «collisions» entre $x \neq x'$ dans X avec $f(x) = f(x')$. Puisque le codomaine n'est pas mentionné, une restriction à l'arrivée de change pas l'injectivité ou non d'une application. Par contre, une restriction de X (donc au départ) peut rendre injective une application qui ne l'est pas.

1.4.3. Définition. *Une application $f : X \to Y$ est bijective si elle est injective et surjective.*

Une application bijective $f : X \to Y$ est telle que le transposé ${}^{\top}G$ de son graphe vérifie la condition pour être graphe d'une application $g : Y \to X$. Or ${}^{\top}G$ est le graphe de la relation $y = f(x)$, et on aura donc $g(y) = x \iff y = f(x)$. Puisque f et g sont des applications, chacune des valeurs x, y détermine dans cette situation l'autre ; g vérifie donc la défintion suivante.

1.4.4. Définition. *Pour $f : X \to Y$, une application $g : Y \to X$ est réciproque de f si $g(f(x)) = x$ pour tout $x \in X$, et $f(g(y)) = y$ pour tout $y \in Y$.*

Clairement f est aussi application réciproque de g si g est application réciproque de f.

1.4.5. Proposition. *Une application $f : X \to Y$ possède une application réciproque $g : Y \to X$ si et seulement si f est bijective. Dans ce cas cette réciproque est unique, et notée $g = f^{-1}$.*

1.5. *Relations d'équivalence, partitions, ensemble quotient.*

On étudiera certains types particuliers de relations entre deux éléments d'un même ensemble. Voici un nombre d'attributs que peut avoir une telle relation.

1.5.1. Définition. *Une relation $\mathcal{R}$ entre éléments de X est appelée*

- *Réflexive si $\forall x \in X : x \mathcal{R} x$;*
- *Irréflexive si $\forall x \in X : \neg(x \mathcal{R} x)$;*
- *Symétrique si elle est sa propre réciproque: $\forall x, y \in X : (x \mathcal{R} y \iff y \mathcal{R} x)$;*
- *Antisymétrique si $\forall x, y \in X : (x \mathcal{R} y \wedge y \mathcal{R} x \Rightarrow x = y)$;*
- *Transitive si $\forall x, y, z \in X : (x \mathcal{R} y \wedge y \mathcal{R} z \Rightarrow x \mathcal{R} z)$.*

Une relation $\mathcal{R}$ entre éléments de X définit un prédicat (ne dépendant donc que d'une seule valeur x) $x \mathcal{R} x$ sur X, mais pour des relations intéressantes ce sera toujours soit le prédicat toujours vrai (cas d'une relation réflexive telle que '$\leq$' ou '$\geq$') soit le prédicat toujours faux (cas d'une relation irréflexive telle que '$<$' ou '$>$'). En plus on passe de l'un à l'autre en enlevant/rajoutant la possibilité de l'égalité, donc c'est une question de goût quel type on préfère ; on penchera plutôt pour les relations réflexives. Parmi les trois attributs restants, le dernier (la transitivité) est le plus important ; les cas qui nous intéresseront sont ceux où la transitivité est combinée avec soit la symétrie, soit avec l'antisymétrie.

La transitivité veut dire que si une chaîne de relations est donnée, comme $x_0 \mathcal{R} x_1$, $x_1 \mathcal{R} x_2$, $\ldots$, $x_{n-1} \mathcal{R} x_n$ (aussi écrit $a_0 \mathcal{R} a_1 \mathcal{R} \cdots \mathcal{R} a_n$), alors on peut «passer à travers» et conclure $a_0 \mathcal{R} a_n$ (on prouve ceci facilement par récurrence sur n).

1.5.2. Définition. *Une relation d'équivalence sur X est une relation qui est à la fois réflexive, symétrique et transitive.*

Sur chaque ensemble X le relation d'égalité est une relation d'équivalence, mais cet exemple est peu intéressant (et à l'autre extrême, la relation qui est toujours vraie en est une aussi). Les exemples types de relations d'équivalence sont celles définies par la condition d'avoir un certain caractéristique ou attribut en commun. Par exemple sur $\mathbf{Z}$ la relation «avoir la même parité» est une relation d'équivalence ; sur l'ensemble des droites dans un plan géométrique la relation d'être parallèles (ou confondues) en est une aussi, tout comme celle d'être proportionnels (collinéaires) sur l'ensemble des vecteurs non nuls dans un espace vectoriel donné. En fait on peut dire qu'en général une relation $\mathcal{R}$ d'équivalence découpe X en morceaux, les *classes d'équivalence*, tels que $x \mathcal{R} y$ exprime simplement le fait que x et y appartiennent à une même classe. Voyons pourquoi.

Considérons la propriété suivante, qu'une partie C de X peut avoir ou non : on a $x \mathcal{R} y$ pour *tout couple* $x, y \in C$. Alors, pour chaque $x_0 \in X$, la transitivité assure que la partie $C = \{ x \in X \mid x_0 \mathcal{R} x \}$ possède cette propriété. En fait C est la plus grande partie avec cette propriété qui contient x_0, car $x_0 \mathcal{R} x$ est condition nécessaire pour que x appartienne à une telle partie. Puis en variant les choix de x_0, on trouvera de la même manière parfois la même partie de X, parfois une autre. Considérons l'ensemble de toutes les parties ainsi obtenues,

c'est-à-dire $\mathcal{Q} = \{\, \{\, x \in X \mid x_0 \,\mathcal{R}\, x \,\} \mid x_0 \in X \,\}$. Il s'agit d'un ensemble de parties de X (et donc $\mathcal{Q} \in \mathcal{P}(\mathcal{P}(X))$). Attention, bien que chaque choix $x_0 \in X$ contribue un élément (une partie de X) à $\mathcal{Q}$, cela peut donner la même partie plusieurs fois, donc $\mathcal{Q}$ peut avoir moins d'éléments que X ; par exemple pour $X = \mathbf{Z}$ avec $\mathcal{R}$ la relation d'avoir la même parité, $\mathcal{Q}$ n'a que deux éléments : l'ensemble des entiers pairs et celui des entiers impairs.

Avant de caractériser la forme que peut avoir $\mathcal{Q}$, notons une opération définie pour $\mathcal{Q}$ en tant qu'ensemble de parties de X (donc élément de $\mathcal{P}(\mathcal{P}(X))$, introduisons une nouvelle notation : on désignera par $\bigcup \mathcal{Q}$ la réunion de toutes les parties appartenant à $\mathcal{Q}$, qui est définie par

$$\bigcup \mathcal{Q} = \bigcup_{C \in \mathcal{Q}} C = \{\, x \mid \exists C \in \mathcal{Q} : x \in C \,\},$$

ce qui généralise l'opération de réunion de deux ou plusieurs parties (car si $\mathcal{Q} = \{U, V\}$ alors $\bigcup \mathcal{Q} = U \cup V$, et si $\mathcal{Q} = \{U_1, \ldots, U_n\}$ alors $\bigcup \mathcal{Q} = U_1 \cup \cdots \cup U_n$, mais $\mathcal{Q}$ peut aussi être infini).

1.5.3. Définition. *Une partition d'un ensemble X est une collection $\mathcal{Q} \subseteq \mathcal{P}(X)$, telle que*

- *la partie vide n'appartient pas à $\mathcal{Q}$, en formule $\emptyset \notin \mathcal{Q}$;*
- *la réunion des parties appartenant à $\mathcal{Q}$ est X, en formule $\bigcup \mathcal{Q} = X$;*
- *les parties appartenant à $\mathcal{Q}$ sont deux à deux disjointes : $\forall U, V \in \mathcal{Q} : U \neq V \to U \cap V = \emptyset$.*

1.5.4. Proposition [correspondance entre relations d'équivalence et partitions].

(1) Si $\mathcal{R}$ est une relation d'équivalence sur X, alors $\mathcal{Q} = \{\, \{\, x \in X \mid x_0 \,\mathcal{R}\, x \,\} \mid x_0 \in X \,\}$ est une partition de X.

(2) Si $\mathcal{Q}$ est une partition de X, alors $\mathcal{R}$ définie par $x \,\mathcal{R}\, y \iff \exists C \in \mathcal{Q} : x \in C \wedge y \in C$ est une relation d'équivalence sur X.

(3) Ces deux correspondances sont réciproques l'une de l'autre.

Le dernier point veut simplement dire qu'en enchaînant les deux correspondances, dans un sens ou dans l'autre, on retombe toujours sur la relation respectivement partition du départ.

La preuve de cette proposition est un exercice instructif. Pour (1), la condition que les membres de $\mathcal{Q}$ sont deux à deux disjoints se reformule $(U, V \in \mathcal{Q} \wedge x \in U, x \in V) \to U = V$, et on peut montrer d'abord $(x_0 \in U \in \mathcal{Q}) \to U = \{\, x \mid x_0 \,\mathcal{R}\, x \,\}$ pour l'établir. Pour montrer la transitivité dans (2), les hypothèses $x \,\mathcal{R}\, y$ et $y \,\mathcal{R}\, z$ parlent de l'existence de deux classes à priori distinctes de $\mathcal{Q}$, mais le fait que y appartient aux deux permet de les montrer identiques.

Souvent on introduit une relation d'équivalence $\mathcal{R}$ sur un ensemble X avec le but de former un nouvel ensemble X' qui contient un élément pour chaque classe d'équivalence pour $\mathcal{R}$. Par exemple on peut former un ensemble $X' = \{\mathit{pair}, \mathit{impair}\}$, dont chaque élément représente l'une des deux classes d'équivalence dans $\mathbf{Z}$ pour la parité. Un exemple plus compliqué mais bien connu est la formation des nombres rationnels à partir de $\mathbf{Z}$. Pour obtenir les fractions nécessaires, on commence à former l'ensemble $F = \{\, (n, d) \in \mathbf{Z} \times \mathbf{Z} \mid d > 0 \,\}$ où (n, d) représente la fraction $\frac{n}{d}$. Mais cela donne trop d'éléments, car il est nécessaire d'associer multiples fractions au même nombre rationnel, comme on l'a évoqué auparavant. On définit donc $(p, q) \,\mathcal{R}\, (r, s) \iff ps = qr$, ce qui est une relation d'équivalence sur F (exercice), dont les classes d'équivalence correspondent aux nombres rationnels.

Dans une telle situation, on peut prendre pour X', par manque d'imagination, l'ensemble $\mathcal{Q}$ des classes d'équivalence lui-même. Dans ce rôle on appelle $\mathcal{Q}$ l'*ensemble quotient* de X par la relation $\mathcal{R}$, noté $X/\mathcal{R}$. Ces éléments sont des ensembles (de parties de X), ce qui n'est aucun problème d'un point de vue mathématique, mais un peu encombrant si on veut les manipuler. Et si la relation $\mathcal{R}$ est fixé, il n'est pas nécessaire de mentionner la totalité d'une classe pour

spécifier un élément de $X/\mathcal{R}$, car si on mentionne un seul élément de la classe, il est clair qu'on vise l'unique classe d'équivalence pour $\mathcal{R}$ qui contient cet élément. Ainsi on identifie toute la classe $C \in X/\mathcal{R}$ par un membre choisi $r \in C$, ce qu'on appelle un *représentant* de la classe. Il sera important de réaliser que, bien que r soit un élément de X, son rôle est de désigner un élément de $X/\mathcal{R}$, et qu'en tant que tel, son remplacement par un autre élément de C ne devait pas faire une différence.

Ce détail est important dans la plupart de situations où l'on veut définir une application ou opération sur $X/\mathcal{R}$. Puisque ses éléments sont des parties de X, ces définitions feront référence aux éléments de X, et le plus souvent c'est fait en *choisissant* d'abord un élément dans chaque valeur de $X/\mathcal{R}$ concernée, en spécifiant le résultat (souvent une classe dans $X/\mathcal{R}$) en termes de ces valeurs, et en montrant finalement que ce résultat ne dépend pas des choix faits. Voici un exemple : on définit la somme de deux nombres rationnels par $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$. En détail cela veut dire qu'on choisit (a, b) et (c, d) pour représenter leur classe dans $F/\mathcal{R}$, on définit la somme de ces classes comme la classe dans $X/\mathcal{R}$ de $(ad + bc, bd)$, et finalement si (a', b') et (c', d') sont d'autres représentants des mêmes classes (donc $ab' = a'b$ et $cd' = c'd$) alors la valeur correspondante $(a'd' + b'c', b'd')$ est dans la même classe : on a $(ad + bc)b'd' = ab'dd' + bb'cd' = a'bdd' + bb'c'd = bd(a'd' + b'c')$. On voit que les choix sont faits *implicitement* simplement en désignant chaque classe par un représentant ; néanmoins la vérification de l'indépendance de ces choix est essentielle pour montrer que la définition est valable.

1.6. *Relations d'ordre (partiel, total), pré-ordre.*

Quand une relation transitive relie des éléments dans un cycle, $x_1 \mathcal{R} x_2 \mathcal{R} \cdots \mathcal{R} x_n \mathcal{R} x_1$, alors $x_i \mathcal{R} x_j$ est forcé pour tout $i, j \in \{1, 2, \ldots, n\}$. C'est ce qui se passe pour une relation d'équivalence dans chacune de ses classes, mais il est intéressant d'étudier aussi les relations transitives où une telle situation ne se produit *jamais* (avec $n > 1$ éléments distincts). Il suffit d'interdire les situations avec $n = 2$, ce qui veut dire exiger une relation anti-symétrique. Cela nous mène à la notion d'un ordre partiel.

1.6.1. Définition. *Une relation d'ordre partiel sur X est une relation qui est à la fois réflexive, anti-symétrique et transitive.*

Un relation d'ordre partiel définit une notion de hiérarchie, où un argument de la relation est considéré comme plus petit que l'autre. Par exemple us un ensemble $\mathcal{P}(X)$ la relation $A \subseteq B$ est un ordre partiel (l'antisymétrie correspond au fait que $A \subseteq B$ et $B \subseteq A$ entraînent $A = B$). Le mot « partiel » met l'accent sur le fait qu'il n'est pas exigé que l'une des relations $x \mathcal{R} y$ et $y \mathcal{R} x$ sont valables pour tout couple x, y ; il est possible que ni l'une ni l'autre sont vraies, et dans ce cas x et y sont dits incomparables pour $\mathcal{R}$. Par exemple dans $\mathcal{P}(\{1, 2, 3, 4\})$, les parties $A = \{2, 4\}$ et $B = \{1, 3, 4\}$ sont incomparables car $2 \in A \setminus B$ et $3 \in B \setminus A$. Si aucun pair d'éléments n'est incomparable, alors on appelle le relation un *ordre total*. Par exemple ' $\leq'$ et ' $\geq'$ sont des ordres totaux sur $\mathbf{R}$, et l'ordre lexicographique (utilisé dans les dictionnaires) est un ordre total sur les mots d'une langue ; en général, un ordre total sur X permet de ranger toute partie finie de X de façon unique en une liste croissante. Un ordre partiel intéressant sur $\mathbf{N}_{>0}$ est celui de la divisibilité, noté $k \mid n$ et défini par la condition $\exists l \in \mathbf{N} : kl = n$.

Les relations d'ordre, partiel ou total, apparaissent dans domaines très divers. Ce n'est pas ici le lieu de développer les propriétés de ces ordres, mais on clora ce chapitre avec une indication comment obtenir une relation d'ordre à partir d'une relation transitive même si elle n'est pas antisymétrique.

1.6.2. Définition. *Un pre-ordre sur X est une relation qui est réflexive et transitive.*

Voici le résultat en question ; on laisse comme exercice de faire des vérifications nécessaires pour justifier la construction indiquée dans son énoncé.

1.6.3. Proposition. *Soit X un ensemble et $\mathcal{R}$ un pre-ordre sur X. On définit une autre relation $\mathcal{S}$ par $x \mathcal{S} y \iff (x \mathcal{R} Y \wedge y \mathcal{R} x)$. Alors $\mathcal{S}$ est une relation d'équivalence sur X, et $\mathcal{R}$ induit un ordre partiel $\overline{\mathcal{R}}$ sur l'ensemble quotient $X/\mathcal{S}$ en posant $\bar{x} \overline{\mathcal{R}} \bar{y}$ si $x \mathcal{R} y$, où $\bar{x} \in X/\mathcal{S}$ désigne la classe de $x \in X$.*

Chapitre 2. Combinatoire énumérative.

Dans cette partie du cours on va s'intéresser au dénombrement de certaines familles d'ensembles finis, un sujet appelé la *combinatoire énumérative*. Dénombrer (mot savant pour "compter") un ensemble fini veut dire déterminer son *cardinal*, qui est un nombre naturel, par définition du terme "fini". Rappelons quelques généralités de la notion de cardinalité.

Deux ensembles X, Y sont dit de même cardinal, ou équipotents, s'il existe une bijection $X \to Y$. Il s'agit d'une relation d'équivalence sur l'univers de tous les ensembles ; une classe d'équivalence correspond à un *cardinal* (en fait on peut choisir un représentant distingué dans chaque classe appelé (ensemble) cardinal, mais ce choix ne nous intéresse pas ici). Une relation plus faible est que le cardinal de X n'excède pas le cardinal de Y, relation définie par l'existence d'une application injective $X \to Y$. Il s'agit d'une pré-ordre dont la relation d'équivalence associée est (d'après le théorème de Cantor-Schröder-Bernstein) celle d'être équipotent, et qui donne donc lieu à une relation d'ordre sur les cardinaux.

Tout cela est défini indifféremment pour les ensembles finis et infinis, mais les questions de cardinalité sont plus fines pour les ensembles finis. La notion de finitude est liée aux nombres naturels comme suit. Pour chaque nombre $n \in \mathbf{N}$ on peut former un ensemble spécifique E_n de cardinal n (en fait il s'agit de *définir* ce qu'est le cardinal n), à savoir $E_n = \{\, i \in \mathbf{N} \mid i < n \,\}$. (Le choix précis de cet ensemble modèle n'a pas beaucoup d'importance. On pourrait aussi prendre l'ensemble E_n défini de façon récurrente dans la section 1.1, qui a le même cardinal ; en fait, dans cette construction là on a $E_n = \{\, E_i \mid i < n \,\}$, ce qui est très proche de ce qu'on a ici. Ceci dit, notre choix $E_n = \{0, 1, \ldots, n-1\}$ s'avérera souvent plus commode que $\{1, \ldots, n\}$.)

Il est clair que si $n \leq m$ on a $E_n \subseteq E_m$, donc le cardinal de E_n n'excède pas celui de E_m. Un fait fondamental (qui se montre par récurrence sur m) est que E_n et E_m ne sont équipotents que si $n = m$. Un ensemble X est *fini* s'il existe $n \in \mathbf{N}$ pour lequel X est équipotent avec E_n, et dans ce cas n est unique, et appelé le cardinal de X, ce qu'on écrira en formule comme $\#X = n$. Une application injective $X \to Y$ entre ensembles finis *existe* si et seulement si $\#X \leq \#Y$, et, chose spécifique pour les ensembles finis, si $\#X = \#Y$ alors toute application $X \to Y$ qui est injective est automatiquement surjective (donc bijective) et aussi réciproquement (surjectif entraîne injectif, toujours en supposant que $\#X = \#Y$ est fini).

Parfois on veut transformer une condition (expression logique, qui est fausse ou vraie) en une valeur 0 ou 1. Pour cela on mettre des crochets autour de la condition, en convenant $[\![\,\text{faux}\,]\!] = 0$ et $[\![\,\text{vrai}\,]\!] = 1$. (Ces « crochets d'Iverson » généralisent le « symbole de Kronecker », la notation $\delta_{i,j}$ qui vaut 1 si $i = j$ et 0 sinon, car on a $\delta_{i,j} = [\![\, i = j \,]\!]$.) Pour une partie $A \subseteq X$, on définie sa *fonction caractéristique* (ou indicatrice) $\chi_A : X \to E_2 = \{0, 1\}$ par $\chi_A(x) = [\![\, x \in A \,]\!]$.

2.1. *Principes de dénombrement.*

Dans la combinatoire énumérative, on essaye de trouver pour certaines familles d'ensembles finis

leurs cardinaux. Le plus souvent la famille est indicé par un entier naturel, et donne donc lieu à une suite de nombres naturels qui décrit les cardinaux des membres de la famille.

2.1.1. Proposition. *Si A, B sont deux ensembles finis et disjoints, alors $\#(A \cup B) = \#A + \#B$.*

Si $A \subseteq B$, alors A et son complémentaire $B \setminus A$ dans B sont toujours disjoints. En appliquant la proposition à ces deux ensembles, on déduit une formule permettant de trouver le cardinal d'une partie d'un ensemble fini B en termes de celles de B et du complémentaire :

2.1.2. Corollaire. *Si B est fini et $A \subseteq B$, alors $\#A = \#B - \#(B \setminus A)$.*

La proposition se généralise sans problèmes aux réunions U de collections $\{ A_i \mid i \in I \}$ de plusieurs ensembles qui sont deux à deux disjoints. (Une telle collection forme essentiellement une partition de U, sauf qu'on peut permettre à certains A_i d'être vide, ce qui est interdit pour une partition.) Une telle collection définit une application $f : U \to I$ qui associe à $x \in U$ l'unique $i \in I$ tel que $x \in A_i$, et réciproquement toute application $U \to I$ définit une collection de parties $A_i = f^{-1}(\{i\})$ qui sont disjointes et dont U est la réunion. On appelle ces parties (les ensembles d'antécédents d'un seul éléments du codomaine) les *fibres* de l'application f.

2.1.3. Proposition. *Si X est fini, $f : X \to Y$ une application, alors $\#X = \sum_{y \in Y} \#f^{-1}(\{y\})$.*

(On n'a pas exigé que Y soit fini, mais l'image $f(X)$ est forcément fini, et les $y \in Y$ qui ne sont pas dans cette image de X ne contribuent que des termes égaux à 0 à la somme ; celle-ci ne change donc pas si on la restreint à une somme sur $y \in f(X)$ qui est une somme finie. La somme est donc «essentiellement finie».) On appelle cette manière de déterminer $\#X$ l'énumération selon l'attribut $f(x)$, car les $x \in X$ avec la même valeur de $f(x)$ sont regroupés dans une même fibre. Si toutes les fibres ont le même nombre d'éléments, on peut utiliser une multiplication :

2.1.4. Proposition. *Si X est fini, et $f : X \to Y$ est une application dont toutes les fibres $f^{-1}(\{y\})$ ont le même cardinal, alors $\#X = \#f^{-1}(\{y_0\}) \times \#Y$ pour $y_0 \in Y$ quelconque.*

Que les fibres ont toutes le même cardinal peut être assuré de différentes manières. Le plus simple est si toutes les fibres sont naturellement en bijection avec un ensemble fixe par exemple, dans la projection $\pi_2 : A \times B \to B$ d'un produit cartésien sur son second facteur, chaque fibre $\pi_1^{-1}(b) = A \times \{b\}$ est en bijection avec A (par la projection sur le premier facteur), d'où :

2.1.5. Fait. *Pour un produit cartésien d'ensembles finis on a $\#(A \times B) = \#A \times \#B$.*

Un ensemble de fonctions $\{ f \mid f : X \to Y \}$ peut être vue comme un produit cartésien répété de $\#X$ facteurs tous égaux à Y, d'où la notation Y^X pour cet ensemble. En effet, si $X = A \cup B$ avec A et B disjoints, l'ensemble Y^X est en bijection avec $Y^A \times Y^B$, les projections sur les deux facteurs étant $f \mapsto f|_A$ et $f \mapsto f|_B$. Avec en plus $Y^{\{x\}}$ étant en bijection avec Y via $f \mapsto f(x)$, on montre sans difficulté par récurrence sur $\#X$ la formule suivante :

2.1.6. Fait. *Pour l'ensemble Y^X des toutes les application $X \to Y$, on a $\#(Y^X) = \#Y^{\#X}$.*

L'association à chaque partie $A \subseteq X$ de sa fonction caractéristique χ_A définit une application $\mathcal{P}(X) \to {E_2}^X$, dont $f \mapsto \{ x \in X \mid f(x) = 1 \}$ est la réciproque, est qui est donc une bijection. Par conséquent on obtient une formule pour le cardinal de $\mathcal{P}(X)$ quand X est fini :

2.1.7. Fait. *Pour l'ensemble $\mathcal{P}(X)$ des parties d'un ensemble fini X, on a $\#\mathcal{P}(X) = 2^{\#X}$.*

La proposition 2.1.4 peut être appliquée dans des situation bien plus compliquées que celle d'un produit cartésien : il suffit qu'on puisse montrer l'égalité des cardinaux des fibres, ce qui revient à montrer *l'existence* d'une bijection entre chaque paire de fibres, sans forcément avoir une bijection naturelle. Par exemple, si l'on enlève du produit cartésien $X \times X$ la diagonale, pour obtenir $C = \{\, (x, x') \in X \times X \mid x \neq x' \,\}$, alors les fibres de l'application $C \to X : (x, x') \mapsto x$ sont toutes de cardinal $n - 1$ si $n = \#X$ (corollaire 2.1.2), et on en déduit que $\#C = (n-1)n$.

Comme pour le principe additif (proposition 2.1.1), la proposition 2.1.4 peut être appliqué dans deux sens, pour donner lieu à une multiplication ou à une division de cardinaux selon le cas. Comme exemple de ce dernier cas de figure, considérons l'ensemble $P = \{\, A \in \mathcal{P}(X) \mid \#A = 2 \,\}$ de paires d'éléments de X (qu'ont notera bientôt $P = \binom{X}{2}$). Avec C l'ensemble décrit ci-dessus, on a une application $C \to P : (x, y) \mapsto \{x, y\}$ dont toutes les fibres sont de cardinal 2 (celle au dessus de $\{x, y\}$ est $\{(x, y), (y, x)\}$). La formule $\#C = 2 \times \#P$ donne alors $\#P = \frac{\#C}{2} = \frac{(n-1)n}{2}$.

2.2. *Arrangements, permutations, et combinaisons.*

La généralisation de la formule qu'on vient de donner, pour compter les parties d'un cardinal fixé l (l'exemple étant le cas $l = 2$) dans un ensemble X de cardinal n est un problème classique de la combinatoire énumérative. Les nombres $\binom{n}{l}$ qui sont la solution de ce problème seront appelé *coefficients binomiaux*, et ils sont très riche en propriétés particulières.

• *Définition des coefficients binomiaux, formule du binôme, récurrence de Pascal.*

2.2.1. Définition. *Si X est un ensemble et $m \in \mathbf{N}$, on pose $\binom{X}{m} = \{\, A \in \mathcal{P}(X) \mid \#A = m \,\}$.*

2.2.2. Définition. *Pour $n, l \in \mathbf{N}$, le coefficient binomial $\binom{n}{l}$ est le cardinal de l'ensemble $\binom{E_n}{l}$.*

Il est clair qu'on a $\#\binom{X}{l} = \binom{\#X}{l}$ pour tout ensemble fini X et tout $l \in \mathbf{N}$. Comme une partie de X ne peut pas avoir plus d'éléments que X lui-même, on a $\binom{n}{l} = 0$ quand $l > n$. Le tableau des valeurs $\binom{n}{l}$ pour $n \in \mathbf{N}$ et $0 \leq l \leq n$ est appelé le «triangle de Pascal». En général on l'affiche avec n numérotant les lignes de haut en bas (commençant avec $n = 0$) et l la position à l'intérieur de la ligne (en commençant à gauche avec $l = 0$), où ce début de ligne recule d'une demi-place vers la gauche par rapport à la ligne précédente, pour maintenir la symétrie :

$$
\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
 & 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 & \\
 & & 1 & & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & & 1 \\
 & 1 & & 8 & & 28 & & 56 & & 70 & & 56 & & 28 & & 8 & & 1 & \\
1 & & 9 & & 36 & & 84 & & 126 & & 126 & & 84 & & 39 & & 9 & & 1
\end{array}
$$

La symétrie de ce tableau s'exprime par l'identité

$$\binom{n}{l} = \binom{n}{n-l} \qquad \text{pour } 0 \leq l \leq n,$$

et s'explique parle fait que si $\#X = n$ et $A \in \binom{X}{l}$, alors son complémentaire $A^c = X \setminus A$ dans X vérifie $A^c \in \binom{X}{n-l}$, et l'opération $A \mapsto A^c$ sur $\mathcal{P}(X)$ est inversible, car elle est sa propre inverse.

Le nom des coefficients binomiaux vient de leur occurrence dans la formule du binôme.

2.2.3. Proposition. *Pour toutes valeurs de x et y (avec $xy = yx$), et tout $n \in \mathbf{N}$, on a*

$$(x+y)^n = \sum_{l=0}^{n} \binom{n}{l} x^{n-l} y^l, \qquad \textit{qui s'écrit aussi} \qquad (x+y)^n = \sum_{\substack{k,l \in \mathbf{N} \\ k+l=n}} \binom{n}{l} x^k y^l.$$

Cette formule se démontre en utilisant juste la définition 2.2.2. En effet, si l'on fait l'expansion de $(x+y)^n$ en utilisant distributivité de la multiplication mais sans permuter les facteurs x et y qui sont multipliés pour former chaque terme, on obtient la somme sur les 2^n « mots » de longueur n qu'on peut former avec les lettres x et y, le terme étant le produit des lettres dans le mot. Ensuite, en appliquant $xy = yx$, on peut transformer chaque terme en un monôme de la forme $x^k y^l$ avec $k + l = n$, et il reste à compter combien de ces mots contribuent à un monôme donné. Chaque mot est caractérisé par l'ensemble $A \in \mathcal{P}(E_n)$ des positions où la lettre est y, et contribue à $x^{n-l}y^l$ avec $l = \#A$; le nombre de mots cherché est donc $\binom{n}{l}$.

La proposition ne spécifie volontairement pas la nature des valeurs x, y, car elle s'applique dans beaucoup de situations différentes. Un cas est particulièrement utile, où x et y sont des polynômes en X, à savoir $x = 1$ (polynôme constant) et $y = X$; on obtient alors

$$(1+X)^n = \sum_{l=0}^{n} \binom{n}{l} X^l,$$

qui permet d'identifier les coefficients binomiaux dans un ligne du triangle de Pascal comme les coefficients de ce polynôme. Cette formule permet d'obtenir facilement des identités qui relient les coefficients binomiaux. Notamment, puisque $(1+X)^{n+1} = (1+X)^n(1+X)$ et en général $(\sum_{i=0}^{n} c_i X^i)(1+X) = c_0 + \sum_{i=1}^{n}(c_i + c_{i-1})X^i + c_n X^{n+1}$, comparaison des coefficients donne :

2.2.4. Proposition. *On a $\binom{n}{0} = 1 = \binom{n}{n}$ pour $n \in \mathbf{N}$, et $\binom{n+1}{i} = \binom{n}{i} + \binom{n}{i-1}$ pour $0 < i \leq n$.*

Ceci se voit aussi en utilisant directement de la définition 2.2.2 : $\binom{E_n}{0} = \{\emptyset\}$ et $\binom{E_n}{n} = \{E_n\}$, et comme $E_{n+1} = E_n \dot\cup \{n\}$ on a pour $i > 0$ que $\binom{E_{n+1}}{i} = \binom{E_n}{i} \dot\cup \{\, A \dot\cup \{n\} \mid A \in \binom{E_n}{i-1} \,\}$ (où on a partitionné l'ensemble $\binom{E_{n+1}}{i}$ en ses éléments $B \subseteq E_{n+1}$ avec $n \notin B$ et celles avec $n \in B$).

La relation dans la proposition s'appelle la récurrence de Pascal. La proposition permet de calculer rapidement les valeurs dans le triangle de Pascal, par lignes successives, car elle dit que chaque valeur intérieure est la somme des deux valeurs placées directement au-dessus d'elle.

• *Arrangements et combinaisons; formules pour leur dénombrement.*

La proposition 2.2.4 détermine les valeurs de tous les coefficients binomiaux implicitement, mais il existe une formule qui décrit ces coefficients individuels plus explicitement. Pour l'obtenir on généralise le procédé qu'on a appliqué ci-dessus pour trouver $\binom{n}{2} = \frac{(n-1)n}{2}$.

2.3. *Problèmes d'énumération dont la réponse est un coefficient binomial.*

Une particularité des coefficients binomiaux $\binom{n}{l}$ est qu'ils comptent non seulement les parties de cardinal l d'un ensemble de cardinal n (ce qui est leur définition), mais qu'il apparaissent aussi de la réponse à de nombreux autres problèmes d'énumération, qui au fond sont équivalents, mais néanmoins parfois d'une apparence assez différente. Ce type de problèmes se résout donc

principalement par reconnaissance : on voit que le problème donné est équivalent à un autre dont on sait que la réponse est donnée par un coefficient binomial. On présentera ici un nombre de tels problèmes. Parfois les différences antre ces problèmes sont peu signifiantes, et les variations sont données juste pour indiquer des formes diverses auxquelles on peut s'attendre. Dans d'autre cas les différences sont plus importantes, et nécessitent une transformation des valeurs dans l'énoncé du problème avant l'insertion dans un coefficient binomial.

Dans notre présentation, on va présenter ces "interprétations combinatoires" de $\binom{n}{l}$ comme des façons différentes de décrire les membres d'un ensemble déterminé par n et l, mais pour point de départ on ne prendra pas pour cela l'ensemble des parties de cardinal l d'une ensemble E_n modèle à n éléments, mais un ensemble d'objets plus compliqués, à savoir les chemins de réseau passant de l'origine $(0,0)$ de $\mathbf{N}^2$ au point de coordonnées $(n-l,l)$. Un chemin de réseau est défini par une succession de pas, où chaque pas avance l'une des deux coordonnées d'une unité. Pour fixer les idées, on place l'origine en haut à gauche (comme en informatique plutôt qu'en coordonnées cartésiennes), avec la première coordonnée avançant vers le bas et la second vers la droite. Un chemin menant de $(0,0)$ à $(n-l,l)$ compte donc n pas, dont $n-l$ pas verticaux (vers le bas) et l pas horizontaux. Il sera parfois plus naturel de spécifier le rectangle traversé par le chemin en utilisant d'autres nombres que la longueur n du chemin et le nombre l de ses pas horizontaux ; on utilisera notamment le nombre $k = n-l$ de ses pas verticaux, le nombre $n' = n+1$ de points du réseau visités (appelés les *sommets* du chemin), ou le nombre $m = k+1$ de lignes horizontales distinctes sur lesquels sont situés ces sommets.

D'abord on remarque la symétrie entre k et l par l'opération de "transposition" du rectangle (réflection par la diagonale principale) qui nous donne $\binom{n}{k} = \binom{n}{n-l} = \binom{n}{l}$, qui fait que pour chaque interprétation on peut en déduire un autre ; parfois on mentionnera les deux.

2.3.1. Fait. *Les chemins de réseau menant de* $(0,0)$ *à* (k,l) *sont de nombre* $\binom{k+l}{k} = \binom{k+l}{l}$.

On peut décrire la forme du chemin en enregistrant pour les $k+l$ pas successivement la direction, par exemple avec A pour un pas vertical et B pour un pas horizontal; le résultat est un mot de longueur $k+l$ avec en total k lettres A et l lettres B.

2.3.2. Fait. *Les "mots" formés de* k *lettres* A *et* l *lettres* B *sont de nombre* $\binom{k+l}{k} = \binom{k+l}{l}$.

On peut aussi utiliser le nombre 0 pour les pas verticaux et 1 pour les pas horizontaux ; dans ce cas le nombre l de ces derniers est aussi la somme des nombres, d'où la reformulation :

2.3.3. Fait. *Les* n*-uplets* $v \in \{0,1\}^n$ *avec* $v_0 + \cdots + v_{n-1} = l$ *sont de nombre* $\binom{n}{l}$.

Un tel n-uplet $v = (v_i)_{i \in E_n}$ est en correspondance avec la partie $P = \{\, i \in E_n \mid v_i = 1 \,\}$ de E_n, qui est de cardinal l, d'où on obtient l'interprétation classique du coefficient binomial :

2.3.4. Fait. *Les parties* $P \subseteq E_n$ *avec* $\#P = l$ *sont de nombre* $\binom{n}{l}$.

Les éléments de P correspondent aux pas horizontaux du chemin, et en donnent leurs positions parmi les n pas en total. La liste de ces positions pris dans l'ordre du chemin donne un l-uplet strictement croissant d'éléments de E_n, et tous ces l-uplets sont possibles :

2.3.5. Fait. *Les* l*-uplets* $(a_0, \ldots, a_{l-1}) \in E_n^l$ *avec* $a_0 < \cdots < a_{l-1}$, *sont de nombre* $\binom{n}{l}$.

Au lieu des positions des pas horizontaux, on peut aussi faire la liste de leurs *premières coordonnées* (celle qui ne change pas dans un pas horizontal). Cet l-uplet sera croissant au sens large, et ses coefficients son dans l'ensemble $\{0,1,\ldots,k\} = E_m$ (on rappelle que $m = k+1$). En plus tous ces l-uplets sont possibles (pour un l-uplet $b_0 \leq \cdots \leq b_{l-1}$, le pas horizontal correspondant à b_j est $(b_j, j) \to (b_j, j+1)$, en position $b_j + j = a_j$ dans le chemin), donc :

2.3.6. Fait. *Les l-uplets* $(b_0, \dots, b_{l-1}) \in E_m^l$ *avec* $b_0 \leq \cdots \leq b_{l-1}$ *sont de nombre* $\binom{m-1+l}{l}$.

Au lieu de noter pour chaque $j \in E_l$ la première coordonnée $i = b_j \in E_m$ du pas horizontal $(i, j) \to (i, j+1)$, on peut noter pour chaque $i \in E_m$ le *nombre* c_i de pas horizontaux avec i comme première coordonnée ($c_i = \#\{\, j \in E_l \mid b_j = i \,\}$), pour obtenir un m-uplet $(c_0, \dots, c_k) \in \mathbf{N}^m$ avec $c_0 + \cdots + c_k = l$. On obtient l'interprétation suivante, qui est à comparer avec celle de 2.3.3:

2.3.7. Fait. *Les m-uplets* $(c_0, \dots, c_{m-1}) \in \mathbf{N}^m$ *de somme l sont de nombre* $\binom{m-1+l}{l} = \binom{m-1+l}{m-1}$.

Cette interprétation se présente souvent sous une forme où on compte le nombre de possibilités de distribuer l unités parmi m candidats (les nombres c_i), où les unités ne sont pas distinguées, mais où l'on distingue les candidats. Par exemple l boules sont placées dans m urnes numérotées, ou l votes sont exprimés sur m candidats, ou l sélections faites parmi m options proposées (une même option pouvant être choisie plusieurs fois). Les variations sont nombreuses, par exemple le nombre de monômes en $x_0, \dots, x_k$ de degré total l est encore un problème du même type (un tel monôme étant de la forme $x_0^{c_0} \dots x_k^{c_k}$ avec $c_0 + \cdots + c_k = l$).

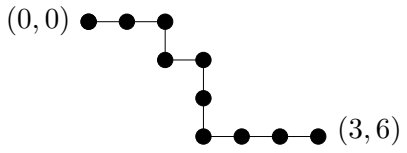
Puisque $\binom{m-1+l}{l} = \binom{m-1+l}{m-1}$, la symétrie dans cette formule est celle entre l et $m-1$, et non pas entre l et m. Quand on reconnaît un problème où cette interprétation s'applique, on doit donc bien identifier qui est l (à utiliser tel quel) et qui est m (à diminuer de 1). Pour aider à le faire, on peut noter que $k = m - 1$ est le nombre de *séparations* (entre candidats, urnes,...), à insérer *entre* les l unités ; c'est le nombre d'opérateurs '+' dans l'expression $c_0 + \cdots + c_{m-1} = l$.

Finalement, on peut aussi noter pour chaque niveau horizontal i le nombre p_i de *sommets* du chemin au niveau i ; par rapport à l'interprétation précédente on a $p_j = c_j + 1$ pour $j \in E_l$ (en particulier on a toujours $p_j > 0$), et la somme $p_0 + \cdots + p_{m-1}$ est le nombre total $n' = n+1$ de sommets. En effet $p_0 + \cdots + p_{m-1} = (c_0 + \cdots + c_k) + m = l + k + 1 = n + 1$. On a donc :

2.3.8. Fait. *Les m-uplets* $(p_0, \dots, p_{m-1}) \in \mathbf{N}_{>0}^m$ *de somme* n' *sont de nombre* $\binom{n'-1}{n'-m} = \binom{n'-1}{m-1}$.

La formule étant relativement simple ici, il existe une façon directe à la trouver : pour séparer l'ensemble des n' unités en m parts *non vides*, on les met sur une ligne, et on «coupe» en $m-1$ endroits *distincts*, qui sont à choisir parmi les $n'-1$ intervalles disponibles.

Pour illustrer ces différentes formes, considérons les chemin suivant, dont les sommets sont $(0,0) \underset{0}{-} (0,1) \underset{1}{-} (0,2) \underset{2}{-} (1,2) \underset{3}{-} (1,3) \underset{4}{-} (2,3) \underset{5}{-} (3,3) \underset{6}{-} (3,4) \underset{7}{-} (3,5) \underset{8}{-} (3,6)$; en voici le dessin :



Le nombre de pas est $n = 9$, dont $k = 3$ horizontaux et $l = 6$ verticaux, on a $m = k + 1 = 4$ niveaux horizontaux (0, 1, 2, et 3), et $n' = 9 + 1 = 10$ sommets sur le chemin; le nombre de chemins avec les mêmes paramètres est $\binom{9}{3} = \binom{9}{6} = 84$. Les descriptions de ce chemin selon les méthodes ci-dessus sont les suivantes.

- (2.3.2) comme mot avec $k = 3$ lettres A et $l = 6$ lettres B : BBABAABBB.
- (2.3.3) comme $(n = 9)$-uplet $v \in \{0,1\}^9$ avec somme 6 : $(v_0, \dots, v_8) = (1, 1, 0, 1, 0, 0, 1, 1, 1)$.
- (2.3.4) comme partie $P \subseteq E_9 = \{0, 1, 2, 3, \dots, 8\}$ avec $\#P = 6$: $P = \{0, 1, 3, 6, 7, 8\}$.
- (2.3.5) comme 6-uplet strictement croissant d'éléments de E_9 : $(a_0, \dots, a_5) = (0, 1, 3, 6, 7, 8)$.
- (2.3.6) comme 6-uplet faiblement croissant d'éléments de E_4 : $(b_0, \dots, b_5) = (0, 0, 1, 3, 3, 3)$.
- (2.3.7) comme $(m = 3 + 1 = 4)$-uplet dans $\mathbf{N}^4$ de somme 6 : $(c_0, \dots, c_3) = (2, 1, 0, 3)$.
- (2.3.8) comme 4-uplet dans $\mathbf{N}_{>0}^4$ de somme $n' = 9 + 1 = 10$: $(p_0, \dots, p_3) = (3, 2, 1, 4)$.

Table de matières.

1 Théorie d'ensembles 2
1.1 Notion d'un ensemble, langage ensembliste, parties d'un ensemble 2
1.2 Produit cartésien, relations, applications 7
1.3 Attributs des applications (domaine, codomaine, graphe, image) 9
1.4 Surjectivité, injectivité, existence d'application réciproque 10
1.5 Relations d'équivalence, partitions, ensemble quotient 11
1.6 Relations d'ordre (partiel, total), pré-ordre 13
2 Combinatoire énumérative 14
2.1 Principes de dénombrement 14
2.2 Arrangements, permutations, et combinaisons 16
Définition des coefficients binomiaux, formule du binôme, récurrence de Pascal 16
Arrangements et combinaisons; formules pour leur dénombrement 17
2.3 Problèmes d'énumération dont la réponse est un coefficient binomial 17