Raisonnement

Le raisonnement mathématique le plus courant est l'implication "directe", aussi appelé "raisonnement déductif". On suppose une propriété P vraie et on en déduit une propriété Q vraie, ce qu'on note souvent $P \Longrightarrow Q$.

Certaines démonstrations utilisent des variantes très utiles du raisonnement déductif.

1 Différents types de raisonnements

1.1 Par disjonction des cas

Pour démontrer une propriété, il est parfois nécessaire d'étudier cas par cas.

On peut par exemple étudier 2 cas : $x = 0$ et $x \neq 0$.

Ce raisonnement est appelé "disjonction des cas".

Pour démontrer $P \Longrightarrow Q$, on décompose en n sous-cas et on démontre $P_1 \Longrightarrow Q$, $P_2 \Longrightarrow Q, \ldots,$ $P_n \Longrightarrow Q$.

Exemple : démontrer que $n(2n+1)(7n+1)$ est divisible par 2 et 3.

Pour démontrer que $n(2n+1)(7n+1)$ est divisible par 2, on considère deux cas : n est pair et n est impair.

Si n est pair, alors $n(2n+1)(7n+1)$ est divisible par 2.

Si n est impair, alors $7n$ est impair et $7n+1$ est pair, donc $n(2n+1)(7n+1)$ est divisible par 2.

On a bien démontré en deux temps : $P_1 \Longrightarrow Q$, $P_2 \Longrightarrow Q$.

De même, on peut démontrer que $n(2n+1)(7n+1)$ est divisible par 3 en considérant 3 cas : n congru à $0, 1$ ou 2 modulo 3.

1.2 Par élimination des cas

Il est parfois utile, quand le nombre de cas est fini, d'étudier toutes les possibilités et de ne retenir que celles qui conviennent. Ce raisonnement très courant en arithmétique, qui est une variante de la "disjonction des cas", est "l'élimination des cas".

Exemple : résoudre dans $\mathbb{Z}$: $xy = 1$ et $3x + y = -4$.

Dans $\mathbb{Z}$, $3x + y = -4$ revient à étudier une infinité de cas : on ne peut pas faire un raisonnement par "élimination des cas". Par contre, dans $\mathbb{Z}$, $xy = 1$ revient à étudier 2 cas : le cas : $x = 1$, $y = 1$ et le cas : $x = -1$, $y = -1$.

On peut donc faire ici un raisonnement par "élimination des cas". Le premier donne dans la deuxième équation $4 = -4$. Il n'est pas solution. Le deuxième est solution. L'équation a donc une solution $(x; y) = (-1; -1)$.

1.3 Par contraposée

Il est parfois plus pratique de démontrer $nonQ \Longrightarrow nonP$ plutôt que $P \Longrightarrow Q$.

Les deux implications sont équivalentes (nous l'admettrons ici) et l'utilisation de la première s'appelle le "raisonnement par contraposée".

Exemple : démontrer que si $2^n - 1$ est premier alors n est premier.

Il est équivalent de démontrer la contraposée : "si n n'est pas premier alors $2^n - 1$ n'est pas premier".

Si n n'est pas premier, il possède un diviseur d différent de 1 et de n. On peut écrire $n = kd$.

Alors $2^n - 1 = (2^d - 1)(2^{(k-1)d} + 2^{(k-2)d} + \ldots + 1)$ et $2^n - 1$ admet un diviseur $2^d - 1$ autre que 1 et lui-même, donc $2^n - 1$ n'est pas premier.

1.4 Par l'absurde

Pour démontrer qu'une proposition P est vraie, on peut supposer que P est fausse et on cherche une contradiction.

Exemple : le théorème d'Euclide qui affirme que l'ensemble des nombres premiers est infini. (Voir en fin de document d'autres démonstrations).

Quand on veut démontrer que l'implication $P \implies Q$ est vraie, on suppose que cette implication est fausse.

Ceci est logiquement équivalent (et nous l'admettrons ici) à supposer que P est vraie et Q est fausse. Ensuite, on cherche à aboutir à une contradiction. Ce raisonnement est appelé le "raisonnement par l'absurde".

Exemple :, démontrer que si x et y sont des nombres premiers tels que $x^2 - y^2 = pq$ avec p et q premiers supérieurs à 2, alors $y = 2$.

Supposons que P est vraie : x et y sont des nombres premiers tels que : $x^2 - y^2 = pq$ avec p et q premiers supérieurs à 2

et Q est fausse : l'égalité " $y = 2$ " fausse signifie que y est un nombre premier impair.

Donc y^2 est aussi impair et comme x est un nombre premier plus grand que y (sinon $x^2 - y^2$ serait négatif, ce qui est impossible), alors x est aussi impair de même que x^2. Par conséquent, $x^2 - y^2$ est pair.

Or p et q sont des nombres premiers supérieurs à 2, donc p et q sont impairs, et $pq = x^2 - y^2$ est impair.

On a une contradiction. On peut donc conclure que la propriété demandée est démontrée.

1.5 Par récurrence

Le "raisonnement par récurrence" est un raisonnement très spécifique. Soit une assertion $P(n)$: le raisonnement par récurrence sert à démontrer que, sous certaines conditions, $P(n)$ est vraie pour tout entier n supérieur ou égal à n_0.

Les conditions sont les suivantes :

1. $P(n_0)$ est vraie
2. Si $P(n)$ est vraie alors $P(n+1)$ est vraie.

Exemple : démontrer que $2^n > 5(n+1)$ pour n entier supérieur ou égal à 5.

La propriété $P(n)$ est " $2^n > 5(n+1)$ ".

1. $n_0 = 5$: $P(5)$ est vrai car $2^5 > 5(5+1)$.
2. Si $P(n)$ est vraie, alors en multipliant par 2 : $2(2^n) > 2[5(n+1)]$.
   Or 2.$[5(n+1)] = 10n + 2$ et $10n + 2 > 5(n+2)$ est équivalente à $n > 8/5$. Ceci est donc vrai pour tout $n \geq 5$.
   Donc $2^{n+1} > 5(n+2)$, soit $P(n+1)$ est vraie.

Conclusion : pour tout $n \geq 5$, $P(n)$ est vraie.

1.6 Recheche de conjecture

Certaines questions sont données "ouvertes". On ne sait pas si la propriété est vraie ou fausse. Il s'agit de se faire une opinion sur des exemples.

Si on pense que la propriété est fausse, il suffira de trouver un exemple qui le prouve, appelé "contre exemple".

Si, après avoir traité de nombreux exemples, on pense que la propriété est vraie, on va la poser comme "conjecture". Il restera à la démontrer.

Exemple 1 : pour tout entier n non multiple de 5, le nombre $6n + 5$ est-il premier ?

Pour se forger une opinion, on prend des exemples : pour $n = 1, 2, 3, 4, 6$, le nombre $6n + 5$ est premier.

Si on pose comme conjecture que la propriété est vraie, il faut la démontrer.

Si on pense qu'elle peut être fausse, il suffit de trouver un contre exemple.

Avec un peu de persévérance, on trouve pour $n = 12$, quad $6n + 5 = 77 = 7 \times 11$.

On a donc démontré que la propriété est fausse.

Exemple 2 : déterminer tous les entiers n tels que $n, n + 2, n + 6, n + 8, n + 12, n + 14$ soient premiers.

Pour se forger une opinion on prend des exemples :

n	$n+2$	$n+6$	$n+8$	$n+12$	$n+14$	solution
2	4	8	10	14	16	non
3	5	9	11	15	17	non
5	7	11	13	17	19	oui
7	9	13	15	19	21	non
11	13	17	19	23	25	non
13	15	19	21	25	27	non

Il y a une solution pour $n = 5$. Que peut-on conjecturer pour $n > 13$? On peut émettre la conjecture que 5 est la seule solution. Mais comment le prouver ? L'observation des non solutions (en dehors de 2 qui est pair) fait apparaître des multiples de 3 et de 5 (pour $n = 13, 7, 3$). Cependant pour $n = 11$, on a seulement un multiple de 5.

L'idée, ici, est de conjecturer que "au moins un des nombres de la suite est multiple de 5".

La démonstration se fait facilement avec les congruences modulo 5 : $n + 6$ congru à $n + 1$, $n + 8$ congru à $n + 3$, $n + 2$ et $n + 12$ congrus à $n + 2$, $n + 14$ congru à $n + 4$). Donc un des cinq nombres $n, n + 2, n + 6, n + 8, n + 12, n + 14$ est multiple de 5.

2 Quelques idées et méthodes

Avant de choisir quel type de raisonnement peut convenir, il s'agit de savoir ce que l'on veut démontrer et pour cela il est souvent utile de "traduire" les questions posées. De même les définitions et les propriétés du cours peuvent être formulées différemment pour donner des idées ou des méthodes utiles à résoudre des exercices.

En voici quelques exemples :

– Dans la division euclidienne de a par b (b entier naturel non nul), le reste est toujours positif ou nul et ne peut être que l'une des b valeurs distinctes : $0, 1, 2, ..., b - 1$.
  Donc : si $b = 5$, tout entier s'écrit $5q$ ou $5q + 1$ ou $5q + 2$ ou $5q + 3$ ou $5q + 4$.
  si $b = 2$, tout entier s'écrit $2q$ ou $2q + 1$: un entier est pair ou impair.

– Si a divise b et si b divise c alors a divise c.
Donc : le pgcd de a et b divise le ppcm de a et b.

– Si d divise a et b alors d divise tout nombre de la forme $au + bv$.
Exemple : si $c = 5u + 15$ alors 5 divise c.

– Penser à traduire une relation de divisibilité par une égalité : si b divise a alors $a = bq$.

– ppcm$(a, b)\times$ pgcd$(a, b) = ab$. Donc le ppcm divise ab.

– Pour démontrer que deux naturels sont premiers entre eux :
• on peut démontrer que tout diviseur commun à a et b est 1.
• on peut supposer qu'ils ont en commun un diviseur premier et en déduire une contradiction.

– Si un nombre est divisible par des nombres premiers entre eux alors il est divisible par leur produit.
Donc : pour démontrer que n est divisible par 6, on peut démontrer que n est divisible par 3 et par 2.

– Si p est premier et n quelconque, alors ou bien p est premier avec n ou bien p divise n. Donc, d'après le théorème de Gauss, si p premier divise un produit de facteurs, alors il divise au moins l'un d'eux.
Attention ! Ceci n'est pas toujours vrai si p n'est pas premier : par exemple, 6 divise 4×15 et 6 ne divise ni 4 ni 15.

3 Appendice : une infinité de nombres premiers

Le raisonnement par l'absurde est utilisé dans la plupart des démonstrations du théorème : "il existe une infinité de nombres premiers".

Pour illustrer ce fait, voici cinq démonstrations de ce théorème :

3.1 La démonstration d'Euclide

Elle est bien connue et utilise le raisonnement par l'absurde.

3.2 La démonstration de Kummer (1978)

C'est une variante de celle d'Euclide

On suppose qu'il existe seulement un nombre fini de nombres premiers $p_1, p_2, ..., p_n$ et soit $N = p_1 \times p_2 \times ... \times p_n - 1$.

N admet au moins un diviseur premier p et p doit être l'un des nombres $p_1, p_2, ..., p_n$. On en déduit que p divise $p_1 \times p_2 \times ... \times p_n - N = 1$. Ce qui est absurde.

3.3 La démonstration de Métrod (1917)

On suppose qu'il existe seulement un nombre fini de nombres premiers $p_1, p_2, ..., p_n$.

Soit $N = p_1 \times p_2 \times ... \times p_n$, $Q_i = N/p_i$ pour chaque $i = 1, 2, ..., n$ et $S = Q_1 + Q_2 + ... + Q_n$. Pour tout i, p_i divise chaque Q_j (pour j différent de i) et ne divise pas Q_i, donc ne divise pas S. Si q est un nombre premier divisant S, alors q est un nombre premier différent de p_i pour tout i. Ce qui est absurde.

3.4 La démonstration de Schorn

On commence par une remarque : si n est un entier quelconque, i et d deux entiers tels que $1 \leq i \leq n$ et $1 \leq d < n$ alors pgcd $((n!)i + 1, (n!)d) = 1$.

En effet, chaque nombre premier p qui divise $(n!)d$ est au plus égal à n et donc ne divise pas $(n!)i + 1$.

On obtient alors : si $1 \leq i < j \leq n$, pgcd $((n!)i + 1, (n!)j + 1) = 1$. Il suffit d'écrire $j = i + d$ et d'utiliser pgcd $(a, a + b) =$ pgcd (a, b).

On suppose qu'il existe seulement m nombres premiers ;

en prenant $n = m + 1$, la remarque précédente montre que deux entiers distincts pris parmi les $m + 1$ entiers $(m + 1)!i + 1$, ($1 \leq i \leq m + 1$), sont premiers entre eux.

Il suffit alors de choisir un facteur premier de chacun des nombres $(m+1)!i+1$, ($1 \leq i \leq m+1$), pour obtenir $m + 1$ nombres premiers distincts. Ce qui est absurde.

3.5 La démonstration de Polya (1924)

Un nombre de Fermat est de la forme $F_n = 2^{2^n} + 1$. Deux nombres de Fermat distincts sont premiers entre eux. Les nombres de Fermat forment donc une suite infinie de nombres sans facteur premier commun. Si p_0 est un facteur premier de F_0, p_1 un facteur premier de F_1, . . . ,p_n un facteur premier de $F_n, \ldots$ alors $p_1, p_2, ..., p_n, \ldots$ sont des nombres premiers tous distincts. Et il y en a une infinité. Ici, ce n'est pas une démonstration par l'absurde !