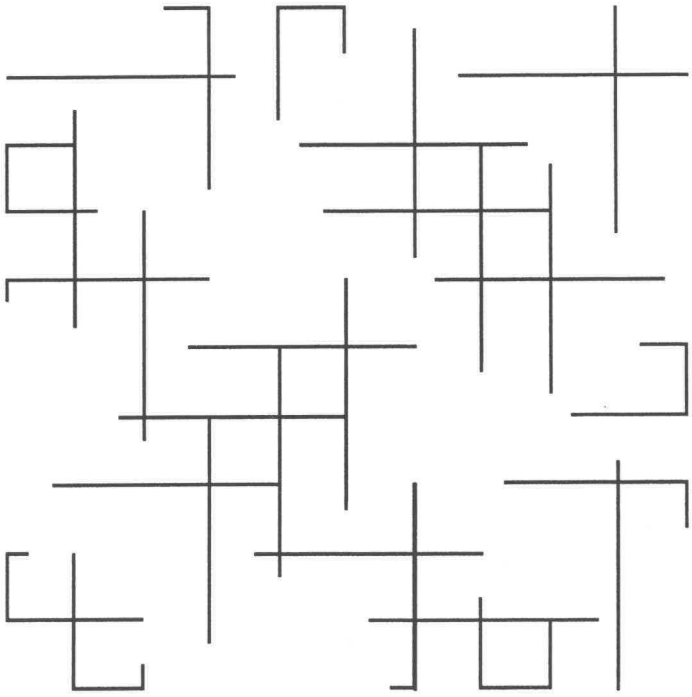
UNIVERSITE DE NANTES

FACULTE DES SCIENCES ET DES TECHNIQUES

Licence pluridisciplinaire de sciences et de technologies

ULP1 – Algèbre et géométrie

Algèbre



B. Truffault

Graphisme d'après Michel Jouët : "Vingt centimètres noir, vingt centimètres rien"

Algèbre

Chapitre I. Les nombres naturels

Chapitre II. Constructions ensemblistes de base

Chapitre III. Les ensembles finis

Chapitre IV . Les nombres entiers relatifs

Chapitre V. Groupes

Chapitre I. Les nombres naturels

§ 1. Les axiomes de Peano

* L'ensemble N

La construction formelle de l'ensemble des *entiers naturels* :

$$\mathbf{N} = \{0, 1, 2, 3, \ldots\}.$$

se fonde sur les *axiomes de Peano* (1), dont une version accessible, se formule comme suit.

Les entiers naturels forment un ensemble **N**, dans lequel on distingue un élément noté 0 et il existe une application σ, de **N** dans lui-même, telle que :

(1) σ est injective,

(2) $0 \notin \sigma(\mathbf{N})$,

(3) Pour toute partie U, de **N**, on a :

$$[[0 \in U] \text{ ET } [n \in U \Rightarrow \sigma(n) \in U]] \Rightarrow [U = \mathbf{N}]].$$

On regarde évidemment σ comme l'application "*suivant*", c'est-à-dire :

$$\sigma : n \mapsto n + 1.$$

En itérant σ, à partir de 0, on entame l'énumération des premiers entiers :

$$\sigma(0) = 1, \sigma(1) = 2, \sigma(2) = 3, \ldots$$

Notant n un élément ainsi engendré, il appartient à **N**, il a donc un suivant dans **N**, l'axiome 3 décide que ce procédé passe en revue tous les éléments de **N**.

Un travail purement formel permet de définir l'addition et la multiplication de **N**, possédant les propriétés qu'on connaît.

(1-1) Rappel des règles de calcul

Pour tous entiers a, b, c, on a :

(4)	$(a+b)+c = (a+b)+c$	associativité
(5)	$a+b = b+a$	commutativité
(6)	$a+0 = a$	0 est élément neutre
(7)	$(a \times b) \times c = (a \times b) \times c$	associativité
(8)	$a \times b = b \times a$	commutativité
(9)	$a \times 1 = a$	1 est élément neutre
(10)	$a \times (b+c) = a \times b + a \times c$	distributivité

Remarques : concernant (10)

1) Plus explicitement on dit que la *multiplication est distributive par rapport à l'addition.*

2) A priori on devrait écrire $a \times (b+c) = (a \times b) + (a \times c)$ mais la *règle de priorité* usuelle permet de supprimer les parenthèses du seond membre sans inconvénient.

---

1 Giuseppe PÉANO : (1858-1932) Logicien et mathématicien italien – propose, entre 1891 et 1908, un exposé axiomatique qui va ses entiers naturels à la théorie générale des ensembles en passant par la géométrie projective. Il est aussi l'inventeur de la courbe qui porte son nom : il s'agit d'un arc paramétré continu qui passe par tous les points de l'intérieur d'un carré. – c'est le premier exemple de ce qu'on nomme aujourd'hui les fractales.

Remarque : on sait prouver que ces axiomes définissent un seul ensemble, *"à isomorphisme près"*, dans un sens qui resterait à préciser mais qui, intuitivement, nous paraît évident. Il existe aussi d'autres façons de fonder cet ensemble, elles aboutissent au même résultat.

*** Le principe de récurrence**

Notons que l'axiome (3) est utilisé couramment sous l'appellation de *principe de récurrence.*

On retiendra que, pour sa mise en œuvre dans les démonstrations ou constructions dites *par récurrence*, l'ensemble U est formé des entiers n tels qu'une certaine propriété P(n) soit vraie (cf. les TD).

*** Le rôle particulier de zéro**

(1-2) Proposition

(11) $$a \times 0 = 0,$$

(12) $$a \times b = 0 \Rightarrow a = 0 \text{ ou } b = 0$$

*** Le bon ordre**

L'ordre de **N** est donné par construction, car si m et n sont deux entiers distincts, l'un d'eux précède l'autre dans l'énumération des entiers. Il s'agit évidemment d'un ordre total qui se caractérise comme suit :

$$m \leq n \Leftrightarrow [\exists x \in \mathbf{N},\ n = m + x].$$

On a, de façon immédiate :

- si $m \leq n$, alors $m + k \leq n + k$, pour tout k ;
- si $m \leq n$, alors $m \times k \leq n \times k$, pour tout k ;

De plus l'ordre vérifie la propriété essentielle qui suit.

(1-2) Théorème 1 : l'ensemble **N** est *bien ordonné* – on entend par là :
toute partie non vide de **N** contient un plus petit élément.

Démonstration : on considère une partie P de **N**, n'ayant pas de plus petit élément. Si 0 appartenait à P, il en serait le plus petit élément, on a donc :

$$0 \notin \mathrm{P}.$$

On considère l'ensemble suivant :

$$\mathrm{U} = \{x \in \mathbf{N} \mid \forall n \in \mathrm{P}\ x < n\}.$$

Il est établi que :

$$0 \in \mathrm{U}.$$

Soit n un élément de U, il est clair qu'aucun aucun des entiers :

$$0, 1, \ldots, n$$

n'appartient à P. Si $n+1$ appartenait à P, ce nombre en serait le plus petit élément, ce qui est contraire à l'hypothèse posée et justifie que :

$$n + 1 \in \mathrm{U}.$$

On en conclut que U = **N**. Autrement dit, si n appartient à P :

$$\forall x \in \mathbf{N}\ \ x < n.$$

Ce qui entraîne en particulier :

$$\forall x \in \mathbf{N}\ n \neq x.$$

et comme P est une partie de **N**, P est l'ensemble vide. ◁

§ 2. La division euclidienne

(2-1) Théorème : étant donnés deux entiers naturels a et b, si $b \neq 0$, il existe un couple (q, r) d'entiers naturels, et un seul, tels que :

$$a = bq + r \text{ et } r < b.$$

Définition : dans ces conditions, on dit que q est le *quotient* et r le *reste* de la *division* de a par b.

Démonstration : commençons par régler la question de l'existence. On note :

A(a) : pour tout entier n, tel que $0 \leq n \leq a$ et pour tout entier $b \neq 0$, il existe q et r, tel que :

$$n = bq + r \text{ et } 0 \leq r < b.$$

A(0) est évidemment vraie car, quel que soit b, on a :

$$0 = b\,0 + 0.$$

Soit a, $a > 0$, on suppose que A(a) soit vraie pour tout entier k, tel que $0 \leq k \leq a-1$. Si b est un entier non nul, on a:

- si $a < b$, $a = b\,0 + a$
- si $a \geq b$, alors $a > a - b$, l'hypothèse de récurrence se traduit : il existe q_1 et r_1, tels que :

$$a - b = bq_1 + r_i \text{ et } r_1 < b.$$

Ceci s'écrit encore :

$$a = bq + r_1 \text{ et } r_1 < b,$$

où $q = q_1 + 1$.

Ce qui démontre l'existence d'un couple (q, r) quels que soient a et b. Il reste à en justifier l'unicité.

On considère deux couples (q, r) et (q', r'), tels que :

$$(a = bq + r \text{ et } r < b) \text{ et } (a = bq' + r' \text{ et } r' < b).$$

On peut, quitte à échanger les rôles de deux couples, supposer que $q \geq q'$. Il s'ensuit que $bq > bq'$ et comme :

$$bq + r = bq' + r',$$

on en déduit que :

$$r' \geq r.$$

Il est donc possible se soustraire $bq' + r$ des deux membres de l'égalité, ce qui donne :

$$b(q - q') = r' - r.$$

Dans ces conditions, on a :

$$r' - r \leq r' < b,$$

Ce qui entraîne que :

$$b(q - q') < b,$$

ce qui n'est possible que si $q - q' = 0$ [1], c'est-à-dire si $q = q'$, ce qui entraîne aussi $r = r'$. On en conclut qu'un tel couple est unique. ◁

1 On retrouve ici l'exigence $b \neq 0$.

*** Le point sur "les quatre opérations"**

L'apprentissage du calcul porte, au début, sur les entiers et met progressivement en œuvre ce qu'on appelle traditionnellement :

"les quatre opérations"

à savoir :

l'addition , la soustration , la multiplication , la division

présentées et mises en œuvre comme autant de modes opératoires indissociables la façon dont on représente les nombres, c'est-à-dire de la numération.

Il s'agit là d'une confusion inéluctable dans la phase d'apprentissage, où il est inconcevable de chercher à dissocier le nombre de la façon dont on l'écrit et des réalités concrètes qu'il permet d'appréhender. Sortir progressivement de cette situation, afin de parvenir au point de vue qui est, ici, le notre, est l'un des enjeux majeurs de l'enseignement mathématique. Précisons le point de vue en question.

L'addition et la multiplication sont ici de même nature, il s'agit de lois de composition internes.

La soustraction et la division sont liées aux deux équations :

$$a+x=b \text{ et } ax=b,$$

La première n'admet de solution que si $b \geq a$ et, dans ce cas, celle-ci est unique, on la note symboliquement :

$$b-a$$

et son calcul pratique est la soustraction de a à b.

Pour la seconde deux cas se présentent :

- si $a=0$, il n'existe pas de solution si $b \neq 0$ et tout nombre est solution de $0x=0$ (1) ;
- si $a \neq 0$, alors la division euclidenne de a par b fournit le quotient et le reste,
  - si le reste est différent de 0, l'équation est sans solution ;
  - si le reste est nul, l'équation admet le quotient pour seule solution.

  Provisoirement, c'est uniquement dans ce cas que, qu'on note :

$$q=a:b \text{ ou } q=\frac{a}{b} .$$

1 C'est la seule façon de percevoir clairement l'inconsistance de l'assemblage "$\frac{a}{0}$".

§ 3. Arithmétique de base

*** Diviseurs d'un nombre**

Définition : on dit que b est un *diviseur* de a – ou que b *divise* a – si le reste de la division de a par b est nul.

Conventions : si b divise a, on dit aussi que a est un *multiple* de b.
En abrégé, on écrira $b \mid a$ pour b divise a.

(3-1) Lemme : tout diviseur commun d'un nombre divise aussi leur somme et leur différence – si celle-ci existe.

Démonstration : immédiate. ◁

*** L'algorithme d'Euclide**

Étant donnés deux entiers a et b, tels que $a > b > 0$, on définit la suite (r_n), par récurrence, comme suit :

- $r_0 = a, r_1 = b$;
- si ($n \geq 1$ et $r_n \neq 0$), r_{n+1} est le reste de la division de r_{n-1} par r_n, autrement dit :

$$r_{n-1} = r_n q_n + r_{n+1} \text{ et } r_{n+1} < r_n$$

La suite d'entiers (r_n) est strictement décroissante. Il existe donc un entier N, tel que :

$$r_N > 0 \text{ et } r_{N+1} = 0.$$

Le procédé se schématise donc comme suit :

$$\left|\begin{array}{ll} a = bq_1 + r_2 & \text{et } r_2 < b \\ b = r_2 q_2 + r_3 & \text{et } r_3 < r_2 \\ r_2 = r_3 q_3 + r_4 & \text{et } r_4 < r_3 \\ \quad \cdots\cdots\cdots\cdots & \\ r_{N-2} = r_{N-1} q_{N-1} + r_N & \text{et } r_N < r_{N-1} \\ r_{N-1} = r_N q_N + 0 & (r_{N+1} = 0) \end{array}\right.$$

1) r_N est un diviseur commun de a et b.

Par construction, r_N divise r_{N-1}. Soit k un entier compris entre 1 et N, on suppose que :

$$r_N \text{ divise } r_{N-1}, \ldots, r_{N-k},$$

Comme :

$$r_{n-(k+1)} = r_{N-k} q_n + r_{N-(k-1)}$$

r_N divise aussi $r_{n-(k+1)}$. On en conclut que r_N divise tous les termes de la suite, en particulier, c'est bien un diviseur commun à a et b.

2) Tout diviseur commun à a et b divise r_N.

Soit d un diviseur commun à a et b, d divise r_0 et r_1. Soit k un entier compris entre 1 et N – 1, on suppose que d divise aussi $r_2, \ldots, r_k$. Comme :

$$r_{k+1} = r_{k-1} - r_k q_k$$

d divise aussi r_{k+1}. Ce qui justifie que d divise tous les les termes de la suite et prouve, en particulier d divise r_N.

En résumé ce commentaire de l'algorithme d'Euclide justifie l'assertion qui suit, où D désigne r_N.

(3-2) Lemme : étant donnés deux nombres a et b, non nuls :

- il existe un diviseur commun D à a et b,
- tel que tout diviseur commun à a et b divise D.

Définition : dans les conditions ci-dessus, D est appelé le *plus grand diviseur commun* – en bref pgcd – de a et b,

On note habituellement $D = \text{pgcd}(a, b)$.

On retient.

(3-3) Proposition : tout diviseur commun de deux nombres divise leur pgcd.

Exemple : calcul du pgcd de 4 290 et 798. On a successivement :

$$\begin{aligned} 4\,290 &= 798\times 5 + 300 \\ 798 &= 300\times 2 + 198 \\ 300 &= 198\times 1 + 102 \\ 198 &= 102\times 1 + 96 \\ 102 &= 96\times 1 + 6 \\ 96 &= 6\times 16 + 0 \end{aligned}$$

Ce qui donne :

$$\text{pgcd}(4\,290, 798) = 6.$$

(3-4) Proposition

1) Si on multiplie deux entiers par un même troisième, non nul, leur pgcd est multiplié par ce même nombre.

2) Le pgcd des quotients de deux nombres par un diviseur commun est le quotient de leur pgcd par ce même nombre.

Démonstration

On se reporte à l'algorithme d'Euclide, tel qu'il est décrit plus haut. On note que si m est un entier non nul, la suite $(mr_n)_{0\le n\le N+1}$ est celle des restes de l'algorithme d'Euclide pour ma et mb. Ce qui montre que :

$$\text{pgcd}(ma, mb) = m\times\text{pgcd}(a, b)$$

et démontre le point 1. Le point 2 en est l'application aux quotients. ◁

*** Nombres premiers entre eux**

Définition : deux nombres sont dit premiers entre eux si leur pgcd est égal à 1.

Remarque : $\text{pgcd}(a, b) = 1$ signifie concrètement que 1 est le seul diviseur commun à a et b.

(3-5) Proposition en divisant deux entiers par leur pgcd, on obtient deux nombres premiers entre eux.

Démonstration : soit d le pgcd de a et b, on note :

$$a' = \frac{a}{d}\ ,\ b' = \frac{b}{d} \quad \text{et} \quad \delta = \text{pgcd}(a', b'),$$

Soit δ un diviseur commun à a' et b', on pose :

$$a'' = \frac{a'}{\delta}\ ,\ b' = \frac{b'}{\delta}\ .$$

Il vient :

$$a = a'd, b = b'd$$

Ce qui donne :

$$a = a'd = a'da''\delta \text{ et } b = b'db''\delta$$
$$a = (a'a'')(d\delta) \text{ et } b = (b'b'')(d\delta)$$

Ce qui montre que $d\delta$ est un diviseur commun de a et b et, ainsi que $d\delta$ divise d, ce qui entraîne $\delta = 1$ – comme attendu. ◁

Remarque (naïve !) : si a et b sont premiers entre eux et si d divise a, d et b sont premiers entre eux.

(3-5) Théorème de Gauss

Si un entier divise le produit de deux autres et s'il est premier avec l'un, il divise l'autre.

Démonstration : a, b et c étant des entiers non nuls, si :

$$bc = ad \text{ et } \text{pgcd}(a, b) = 1$$

On note que :

$$\text{pgcd}(ad, bd) = d$$

Ainsi :

$$b \text{ divise } ad = bc \text{ et } b \text{ divise } bc$$

donc :

$$b \text{ divise leur pgcd } d$$

autrement dit :

$$d = d'b$$
$$bc = ad = ad'b$$
$$c = ad'.$$

a divise c. ◁

(3-6) Corollaire : si un entier est premier avec deux autres, il est premier avec leur produit.

Démonstration : soit a, b, c des éléments de $\mathbf{N}^*$, tels que :

$$\text{pgcd}(a, b) = 1 \text{ et } \text{pgcd}(a, c) = 1$$

premier à bc.

Plus généralement :

si a est premier à $b_1, \ldots, b_n$, a est premier au produit $b_1 \ldots b_n$.

Démonstration : soit $d = \text{pgcd}(a, bc)$, comme a et b sont premiers entre eux, d est premier à b (cf. remarque "naïve). Le théorème de Gauss montre que d divise c et comme a et c sont premiers entre eux, $d = 1$. La généralisation s'effectue au moyen d'une récurrence banale. ◁

(3-7) Corollaire : si un entier est divisible par deux nombres premiers entre eux, il est divisible par leur produit.

Démonstration : soit a, b, c des éléments de $\mathbf{N}^*$, tels que :

$$a = bp \ , \ a = cq \text{ et } \text{pgcd}(b, c) = 1.$$

où p et q sont évidemment des entiers. Comme alors :

$$bp = cq,$$

il découle du théorème de Gauss que c divise p, on pose donc $p = cp'$. ce qui donne :

$$a = bp = bcp'.$$

Ainsi, bc divise a. ◁

*** Plus petit multiple commun**

Considérons deux entiers a et b, non nuls, soit d leur pgcd. on pose :

$$a' = \frac{a}{d} \ , \ b' = \frac{b}{d} \ \text{ et } \ m = \frac{ab}{d} = a'b'd.$$

1) Il est clair que :

$$m = ab' \ \text{ et } \ m = a'b$$

m est donc un multiple commun de a et b.

2) Soit M un multiple commun quelconque de a et b, on pose :

$$\mathrm{M} = pa \ \text{ et } \ \mathrm{M} = qb.$$

Il vient :

$$pa'd = pa = \mathrm{M} = qb = qb'd,$$

puis :

$$pa' = qb'$$

Comme a' et b' sont premiers entre eux (cf 6-5), le théorème de Gauss montre que a' divise q. On note alors $q = a'r$. ce qi donne :

$$\mathrm{M} = qb = a'rb'd = ra'b'd = rm.$$

Ce qui montre que tout multiple commun de a et b est un multiple de m.

Définition : l'entier m ainsi défini, est appelé le *plus petit multiple commun* de a et b, en bref *ppcm*

On retient ce qui suit.

(3-8) Lemme : étant donnés deux entiers a et b, non nuls, il existe un entier m, et un seul, tel que que :

- m soit un multiple commun de a et b,
- m divise tout multiple commun de a et b.

Ce nombre est donné par la formule :

$$m = \frac{ab}{\mathrm{pgcd}(a,b)}.$$

*** Les nombres premiers**

Définition : un entier naturel est dit *premier*, s'il est supérieur à 1 et n'admet pas d'autre diviseur que 1 et lui même.

Exemple : 2, 3, 5, 7, ... , 1999, ... , $2^{11213}-1$ sont des nombres premiers.

Chacun pourra se convaincre par lui même qu'un nombre premier se caractérise comme suit.

(3-9) Proposition : un nombre n est premier si, pour tout entier a, on a :

$$\mathrm{pgcd}(p,a) = 1 \ \text{ ou } \ p \text{ divise } a.$$

(3-10) Lemme : tout entier $n > 1$ est divisible par un nombre premier.

Démonstration

a) Si n n'est pas premier il est divisible par un entier n_1, $1 < n_1 < n$. Si n_1 n'est pas premier, il est divisible par un entier n_2, tel que $1 < n_2 < n_1$, ...

On construit ainsi une suite d'entiers :

$$n > n_1 > n_2 > n_3 > \ldots > 1.$$

Comme il existe qu'un nombre fini d'entiers entre 1 et n, cette suite se termine par un certain n_k qui est nécessairement premier. ◁

(3-11) Théorème – Euclide

Il existe une infinité de nombres premiers.

Démonstration : supposons qu'il n'existe qu'un nombre fini de nombres premiers. Notons les $p_1, p_2, \ldots, p_k$ et considérons leur produit, augmenté de 1 :

$$n = p_1 p_2 \ldots p_k + 1.$$

Si p_1 divisait n il diviserait $n - p_1 p_2 \ldots p_k$ qui est égal à 1. Ceci vaut aussi pour $p_2, \ldots$ et p_k, en contradiction avec le lemme précédent. ◁

(3--12) Théorème : tout entier supérieur ou égal à 2 se décompose, de façon unique, en un produit de nombres premiers – à l'ordre des facteurs près.

Démonstration : on considère un entier n, $n \geq 2$.

1) On définit la suite :

$$n_0, n_1, n_2$$

par récurrence :

- on pose $n_0 = n$
- si k est un entier tel que $k \geq 1$ et le terme n_{k-1} est défini, on est devant l'alternative suivante :
  - soit n_{k-1} est un nombre premier, ce terme n'a pas de suivant, on pose alors $p_k = n_{k-1}$
  - soit n_{k-1} n'est pas premier, il admet un diviseur premier qu'on note p_k et l'on pose :

$$n_k = \frac{n_{k-1}}{p_k}$$

On a donc

$$n_{k-1} > n_k \text{ et } n_{k-1} = p_k n_k.$$

La suite d'entiers, ainsi définie, étant strictement décroissante, elle est finie. Ce qui entraîne qu'il existe un entier K, tel que p_K soit un nombre premier. Ce qui justifie que :

$$n = p_1 n_1 = p_1 p_2 n_2 = \ldots = p_1 p_2 \ldots p_{K-1} n_{K-1},$$
$$n = p_1 p_2 \ldots p_{K-1} p_K.$$

2) Il reste à prouver l'unicité. Nous procédons par récurrence.

Cette condition est évidemment vérifiée pour $n = 2$. Soit n, $n \geq 2$, on suppose qu'elle s'applique à tout entier compris entre 2 et n.

On considère deux décompositions de $n+1$ en facteurs premiers :

$$n + 1 = p_1 p_2 \ldots p_r \text{ et } n + 1 = q_1 q_2 \ldots q_s.$$

Comme p_1 divise $q_1 q_2 \ldots q_s$, p_1 divise l'un des q_i (cf. 3-5), et alors, $p_1 = q_i$ car ces deux nombres sont premiers. Il s'ensuit que :

$$p_2 \ldots p_r = q_1 \ldots q_{i} q_{i+1} \ldots q_s.$$

L'hypothèse de récurrence entraîne que les entiers $q_1, \ldots q_i, q_{i+1}, \ldots, q_s$. sont les mêmes, à l'ordre près, que $p_2, \ldots, p_r$.

Comme $p_1 = q_i$, la démonstration est terminée. ◁

Remarque : on convient généralement de regouper les facteurs premiers égaux. Ainsi, la décomposition de l'entier n prend la forme :

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

où les α_i sont des entiers positifs. Cette forme d'écriture est unique si l'on convient de ranger les p_i par ordre croissant – ou décroissant.

Exemple : décomposition en facteurs premiers de 111 111.

Ce nombre est clairement divisible par 11 ([1]).

$$\frac{111\,111}{11} = 10\,101.$$

10 101 est divisible par 3 et :

$$\frac{10\,101}{3} = 3\,367.$$

Appliqués à 3 367 les caractères de divisbilité usuels ne donnant rien, il est naturel de tenter la division par 7 :

$$\frac{3\,367}{7} = 481,$$

puis d'essayer la division par 13 :

$$\frac{81}{13} = 37$$

et comme 37 est un nombre premier, on obtient :

$$111\,111 = 3\times 7\times 11\times 13\times 37.$$

Remarque : si n n'est pas premier, il possède un diviseur d tel que $d^2 \le n$. En effet, si :

$$n = dd' \text{ , } d^2 > n \text{ et } d'^2 > n$$

alors :

$$n^2 = (dd')^2 > n^2.$$

Ce qui contradictoire;

Cette remarque permet de limiter, de façon notable, le nombre des essais lors la recherche des facteurs premiers d'un nombre entier donné.

*** Retour sur le pgcd et le ppcm**

1) Étant donnés deux entiers a et b, notant $p_1, p_2, \dots, p_s$ les facteurs premiers communs aux décompositions de a et de b. et α_i l'exposant minimum de p_i dans les deux décompositons en question. On a :

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s} a' \text{ et } b = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s} b'.$$

où $(a', b') = 1$. On a donc :

$$\text{pgcd}(a, b) = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}.$$

2) Si m et n sont deux entiers, il est toujours possible d'écrire leur décompositions en facteurs premiers sour la forme :

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_r} \text{ et } n = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_r}.$$

Où certains exposants sont éventuellement nuls. Il est alors facile de voir que :

$$\text{pgcd}(m, n) = p_1^{\mu_1} p_2^{\mu_2} \dots p_s^{\mu_s} \text{ où } \mu_i = \min(\alpha_i, \beta_i) \text{ pour } i = 1, \dots, r.$$

$$\text{ppcm}(m, n) = p_1^{\mu_1} p_2^{\nu_2} \dots p_s^{\nu_s} \text{ où } \nu_i = \max(\alpha_i, \beta_i) \text{ pour } i = 1, \dots, r.$$

Exemple :

$$40 = 2^3\times 5 \text{ et } 60 = 2^2\times 3\times 5$$

$$\text{pgcd}(40, 60) = 2^2\times 5 = 20 \text{ et } \text{ppcm}(40, 60) = 2^3\times 3\times 5 = 120.$$

---

1 Si tel n'est pas le cas, ce devrait l'être après lecture de la secton intitulée "Congruences".

Chapitre II. Constructions ensemblistes de base

§ 4. Le vocabulaire ensembliste

Nous irons directement à l'essentiel en pariant que les règles d'usage courant emmergeront de la pratique. Dans ces conditions, la clarté du discours repose sur un minimum de complicté entre le locuteur et l'auditeur. Cette complicité n'est pas donnée a priori, elle est le fruit d'une volonté commune de se comprendre qui, concrètement, exige une écoute mutuelle.

§ 5. Relations d'équivalence – ensemble quotient

* Relation d'équivalence

Définition : on appelle *équivalence* toute relation binaire $\mathfrak{R}$, d'un ensemble E, qui vérifie les trois conditions suivantes :

(1) elle est *réflexive*, i.e. :

$$\forall x \in \mathrm{E} \quad x \mathfrak{R} x ;$$

(2) elle est *symétrique*, i.e. :

$$x \mathfrak{R} y \Rightarrow y \ \mathfrak{R} x ;$$

(2) elle est *transitive*, i.e. :

$$(x \mathfrak{R} y \ \mathrm{ET} \ y \mathfrak{R} z) \Rightarrow x \mathfrak{R} z.$$

Exemples

La relation d'égalité induit sur tout ensemble une relation d'équivalence.

Dans le plan ou l'espace, noté $\mathscr{E}$, l'égalité des distances est une relation d'équivalence de $\mathscr{E}^2$.

Le parallélisme est une relation d'équivalence entre les droites du plan ou de l'espace.

...

* Ensemble quotient

Définition : si $\mathfrak{R}$ est une relation d'équivalence de E et si x appartient à E, on appelle *classe d'équivalence* x – on précise au besoin *suivant* $\mathfrak{R}$ – et l'on note, selon les cas, C_x ou $\bar{x}$ l'ensemble formé des éléments de E équivalents à x – c'est-à-dire qu'on a :

$$C_x = \{y \in \mathrm{E} \mid y \mathfrak{R} x\}.$$

L'ensemble des classes d'équivalence est appelé *quotient* de E *par* $\mathfrak{R}$ et noté $\mathrm{E}/\mathfrak{R}$, c'est-à-dire que :

$$\mathrm{E}/\mathfrak{R} = \{C_x \mid x \in \mathrm{E}\}.$$

L'application :

$$\begin{array}{rccc} p : & \mathrm{E} & \longrightarrow & \mathrm{E}/\mathfrak{R} \\ & x & \mapsto & C_x \end{array}$$

est appelée *la surjection canonique* de $\mathfrak{R}$ [1].

---

1 La reflexivité assure la surjectivité.

La propriété qui suit peut paraître banale, il n'empêche que c'est elle qui conditionne toute la suite.

(5-1) Lemme : si $\mathfrak{R}$ est une relation d'équivalence, on a :

$$x \mathfrak{R} y \Leftrightarrow C_x = C_y.$$

Démonstration

1) ($\Leftarrow$) Si $C_x = C_y$, la réflexivité garantit que x appartient à C_x et donc à C_y, ce qui donne, par définition $x \mathfrak{R} y$.

2) ($\Rightarrow$) Si $x \mathfrak{R} y$, soit z un élément de C_y, on a :

$$x \mathfrak{R} y \text{ ET } y \mathfrak{R} x.$$

La transitivité garantit que $x \mathfrak{R} z$, puis la symétrie entraîne $z \mathfrak{R} x$, ce qui donne :

$$z \in C_x, \text{ puis } C_y \subseteq C_x.$$

La symétrie permettant d'échanger les rôles de x et y, on a démontré aussi l'inclusion réciproque. Ce qui justifie l'égalité $C_x = C_y$. ◁

(5-2) Théorème

1) Si $\mathfrak{R}$ est une équivalence de E, les classes de E suivant $\mathfrak{R}$ constituent une partition de E.

2) Toute partition de E est formée des classes d'une équivalence.

Démonstration

1) Il résulte de la réflexivité que :

$$x \in C_x,$$

on en déduit immédiatement que :

$$E \subseteq \bigcup_{x \in E} C_x,$$

puis l'égalité.

Considérons deux classes C_x et C_y, si elles ne sont pas disjointes, c'est qu'il existe un élément z de E, tel que :

$$z \mathfrak{R} x \text{ ET } z \mathfrak{R} y.$$

Il découle alors du lemme que :

$$C_x = C_z = C_y.$$

Ce qui montre que deux classes d'équivalence sont égales ou disjointes et justifie que l'ensemble $\{C_x \mid x \in E\}$ est une partition de E.

2) Considérons une partition $\{A_i \mid i \in I\}$ de E, on convient que $x \mathfrak{R} y$ représente :

$$\exists i \in I \ (x \in A_i \text{ ET } y \in A_i).$$

Comme E est la réunion des A_i, si x appartient à E, il appartient à l'un des A_i. On a donc :

$$\forall x \in E \ \exists i \in I \ (x \in A_i \text{ ET } x \in A_i),$$

autrement dit :

$$\forall x \in E \ x \mathfrak{R} x.$$

La symétrie de $\mathfrak{R}$ est évidente.

Soit x, y et z des éléments de E, tels que :

$$(x \mathfrak{R} y \text{ ET } y \mathfrak{R} z),$$

cette condition se traduit :

$$[\exists i \in I \ (x \in A_i \text{ ET } y \in A_i)] \text{ ET } [\exists j \in I \ (y \in A_j \text{ ET } z \in A_j)]$$

Alors $y \in A_i \cap A_j$, il s'ensuit que $A_i = A_j$, on a donc $x \mathfrak{R} z$. Ce qui établit que $\mathfrak{R}$ est ausssi transitive. Il s'agit donc bien d'une relation d'équivalence, comme il était attendu. ◁

§ 6. Décomposition canonique d'une application

On peut considérer comme évident que les notions de partition et d'équivalence soient deux façons d'exprimer un même concept. En revanche, il est plus surprenant que les surjections canoniques des équivalences constituent un modèle de toutes les applications – comme on va le voir maintenant.

(6-1) Lemme : toute application définit une relation d'équivalence sur son ensemble de définition.

Démonstration : soit f une application de E dans F, on note $x \mathfrak{R} y$ la relation :

$$f(x) = f(y).$$

Elle est effectivement bien définie pour tous x et y appartenant à E.

La réflexivité et la symétrie de cette relation sont évidentes. On en vérifie la transitivité.

Soit x, y et z des éléments de E, la proposition :

$$(x \mathfrak{R} y \text{ ET } y \mathfrak{R} z)$$

se traduit :

$$f(x) = f(y) \text{ ET } f(y) = f(z).$$

Elle implique :

$$f(x) = f(z).$$

Ce qui s'exprime :

$$x \mathfrak{R} z,$$

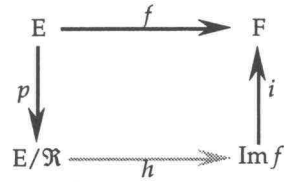
comme attendu. ◁

(6-2) Théorème : toute application f, de E dans F, se factorise, de façon unique, sous la forme :

$$f = i \circ h \circ p$$

où, désignant par $\mathfrak{R}$ l'équivalence qui lui est associée :

- p est la surjection canonique de $\mathfrak{R}$,
- h est une bijection de $E/\mathfrak{R}$ sur $\mathrm{Im} f$.
- i est l'injection canonique de $\mathrm{Im} f$ dans F,



Démonstration : si une telle décomposition existe et si C_x est un élément quelconque de $E/\mathfrak{R}$, on a :

$$f(x) = (i \circ h \circ p)(x) = i \circ h(C_x) = h(C_x).$$

Ce qui montre que $h(C_x) = f(x)$. Cette relation détermine f, pour autant qu'elle soit cohérente. Ce que nous vérifions maintenant.

Soit x et y deux éléments de E, le lemme a établi que $C_x = C_y$, est équivalent à $f(x) = f(y)$. Ainsi, en posant $h(C_x) = f(x)$, pour toute classe de $E/\mathfrak{R}$, on définit bien une application de $E/\mathfrak{R}$ dans $\mathrm{Im} f$. Elle vérifie la condition attendue et c'est effectivement la seule possible. Il reste à s'assurer qu'elle est bijective.

Si deux classes C_x et C_y sont distinctes, la définition de $\mathfrak{R}$ exige que $f(x) \neq f(y)$, h est donc injective. Si y est un élément de $\mathrm{Im} f$, il existe un élément x de E, tel que $y = f(x)$ – c'est-à-dire que $y = h(C_x)$ – h est donc surjective. L'application h est bien une bijection. Ce qui achève la démonstration. ◁

Illustration : l'exponentielle complexe et la mesure des angles orientés.

Chapitre III. Les ensembles finis

§7. Les ensembles finis

Il est naturel d'admettre que, lorsqu'on compte des objets bien déterminés, le résultat est indépendant de la façon dont on opère, cependant on peut ne pas se satisfaire de ce point de vue et désirer justifier ce fait de façon formelle.

Convention : soit n un entier naturel, on note :

$$[1,n]=\begin{cases}\{x\in \mathbf{N} \mid 1\leq x\leq n\} \text{ si } n>0\\ \varnothing \text{ si } n=0\end{cases}$$

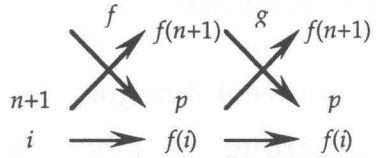
(7-1) Lemme : soit n et p deux entiers naturels, s'il existe une bijection de $[1,n]$ sur $[1,p]$, alors $n=p$.

Démonstration : on procède par récurrence sur n.

Si $n=0$, une bijection f de $\varnothing$ sur $[1,p]$ est telle que $[1,p]=f(\varnothing)=\varnothing$ et alors $p=0$.

Étant donné un entier n, on suppose que la propriété à démontrer est vraie pour n. Soit p un entier tel qu'il existe une bijection f de $[1,n+1]$ sur $[1,p]$. On définit l'application g de $[1,p]$ dans lui-même, telle que :

$$\begin{cases} g(f(n+1))=p,\\ g(p)=f(n+1),\\ g(i)=i \text{ si } i\neq p \text{ et } i\neq f(n+1).\end{cases}$$



Par construction, g est bijective. L'application $g\circ f$ est donc bijective et vérifie :

$$(g\circ f)(n+1)=p.$$

Comme $n+1\geq 1$, on peut considérer l'application suivante induite par $g\circ f$:

$$\begin{aligned} h : [1,n] &\longrightarrow [1,p-1]\\ i &\mapsto g\circ f(i)\end{aligned}$$

elle est aussi bijective. L'hypothèse de récurrence entraîne que $n=p-1$ et par conséquent que $n+1=p$. Le lemme est alors démontré. ◁

Il découle immédiatement de cette propriété que, si E est un ensemble donné, s'il existe un entier n et une bijection entre E et $[1,n]$, n est unique. Ce qui permet de poser la définition qui suit.

Définition : un ensemble E est *fini* s'il existe un entier naturel n et une bijection de E sur $[1,n]$. Dans ces conditions, n est, naturellement, le *nombre des éléments* de E on l'appelle aussi le *cardinal* de E, on le note card E ou $|E|$.

On en déduit immédiatement la proposition qui suit.

(7-2) Proposition : deux ensembles finis E et F ont même cardinal si, et seulement si, il existe une bijection de E sur F.

Nous laissons à chacun le soin de démontrer la proposition qui suit.

(7-3) Théorème : si E et F sont deux ensembles disjoints, alors :

$$|E\cup F|=|E|+|F|.$$

Une récurrence banale permet de généraliser la proposition précédente à un nombre quelconque d'ensembles pouvu qu'ils soient deux à deux disjoints.

(7-4) Proposition : soit E un ensemble fini, si E_1, E_2, ... , E_p est une partition de E on a :

$$|E| = |E_1| + |E_2| + \ldots + |E_p|.$$

(7-5) Théorème : soit E et F deux ensembles finis de même cardinal et f une application de E dans F :

f est injective si, et seulement si, f est surjective.

Démonstration : si f est injective, on pose :

$$E' = f(E) \text{ et } E'' = F - E'.$$

Comme E' et E" sont disjoints, on a :

$$|F| = |E'| + |E''|.$$

Ce qui entraîne que $|E''| = 0$. On a donc $E'' = \varnothing$. Par conséquent $F = E'$, f est alors surjective.

Réciproquement, si f est surjective, notons :

$$F = \{y_1, \ldots, y_n\}$$

on sait que $\{f^{-1}(y_i) \mid \in [1, n]\}$ est une partition de E, on a donc :

$$n = |E| = \sum_{i=1}^{n} |f^{-1}(y_i)|$$

comme f est surjective, on a :

$$|f^{-1}(y_i)| \geq 1, \text{ pour } i = 1, \ldots, n.$$

Il s'ensuit que :

$$|f^{-1}(y_i)| = 1, \text{ pour } i = 1, \ldots, n.$$

Ce qui veut dire que f est bijective. ◁

Remarque : on pourra trouver que c'est là beaucoup d'efforts pour prouver une vérité intuitivement évidente. Cependant, ce résultat n'est banal qu'en apparence. En effet :

- il caractérise les ensembles finis ;
- il justifie un procédé de démonstration fort utile : *le principe des tiroirs* qui généralise un fait bien connu. A savoir que, si cinq objets, au moins, sont répartis dans les quatre tiroirs d'une commode, il existe un tiroir qui en contient au moins deux ;
- il est essentiel pour la compréhension de l'algèbre linéaire en dimension finie.

*** Le principe des bergers**

(7-6) Proposition : *principe des bergers.*

Soit E et F deux ensembles finis, s'il existe une application f de E dans F telle que le cardinal de $f^{-1}(x)$ soit indépendant de x et égal à p, alors :

$$|E| = p\,|F|.$$

Démonstration : ceci est vrai si E est l'ensemble vide, dans le cas contraire, nous savons que les $f^{-1}(x)$ forment une partition de E. ◁

Remarque : on pourrait tenir pour absurde de voir un berger compter les pattes de ses moutons pour en déduire l'effectif du troupeau. Il n'empêche qu'en maintes circonstances, c'est de cette façon qu'on appliquera la relation précédente – souvent implicitement.

§ 8. Dénombrement.

On s'intéresse à quelques ensembles qui serviront de référence dans la résolution des problèmes de dénombrement

* Cardinal d'un produit cartésien

(8-1) Proposition : si E et F sont deux ensembles finis, on a :

$$|E \times F| = |E| \times |F|.$$

Démonstration : soit p la projection sur E, cette application est surjective et il est clair que pour tout x appartenant à E, on a $p^{-1}(x) = \{x\} \times F$ et donc $|p^{-1}(x)| = |F|$. Pour conclure, on applique le principe des bergers. ◁

Une récurrence banale permet de généraliser ce résultat à nombre quelconque de facteurs.

(8-2) Corollaire

1) Si $E_1, E_2, \ldots, E_n$ sont des ensembles finis, on a :

$$|E_1 \times E_2 \times \ldots \times E_n| = |E_1| \times |E_2| \times \ldots \times |E_n|.$$

2) Si E est un ensemble fini et p un entier, on a :

$$|E^n| = |E|^n.$$

(8-3) Corollaire : le nombre des applications d'un ensemble à p éléments dans un ensemble à n éléments est n^p.

Démonstration : on considère des ensembles E et F, ayant respectivement p et n éléments. On peut toujours présenter E sous la forme :

$$E = \{x_1, \ldots, x_n\}.$$

La relation qui lie l'application f de E dans F à l'élément $(y_1, y_2, \ldots, y_p)$ de E^p, tel que :

$$f(x_1) = y_1, f(x_2) = y_2, \ldots, f(x_p) = y_p,$$

est une application bijective. On applique le corollaire précédent. ◁

(8-4) Corollaire : le nombre des parties d'un ensemble à n éléments est 2^n.

Démonstration : soit E un ensemble à n éléments, à tout sous-ensemble A de E, on associe l'application χ_A de E dans $\{0,1\}$ définie par :

$$\chi_A(x) = \begin{cases} 1, \text{ si } x \in A \\ 0, \text{ si } x \notin A \end{cases}$$

(*application caractéristique* de A)

On vérifie immédiatement qu'on est en présence d'une application bijective de l'ensemble $\mathcal{P}(E)$ sur l'ensemble des applications de E dans $\{0,1\}$. On applique le corollaire précédent. ◁

* Arrangements

Définition : on appelle *arrangements* de p éléments d'un ensemble E les suites **sans répétition** de p éléments de E.

Remarque : lorsque p est le nombre des éléments de E, un tel arrangement est une *permutation* de E.

N.B. Insistons bien clairement sur un point :

s'il y a suite, il y a ordre.

Exemple : le palmarès d'un concours est un arrangement de l'ensemble des candidats alors que le classement est une permutation de l'ensemble des candidats ayant composé. Un tiercé dans l'ordre est un arrangement des chevaux ayant pris part à la course concernée.

De façon générale, toute injection de $[1, p] = \{1, 2, \ldots, p\}$ dans un ensemble définit un arrangement de p de ses éléménts.

(8-5) Théorème : notons A_p^n le nombre des arrangements de p éléments d'un ensemble de n éléments. Pour tous entiers n et p tels que $1 \leq p \leq n$, on a :

$$\mathbf{A_0^n = 1} \text{ et si } p \geq 1, \mathbf{A_p^n = n(n-1) \ldots (n-p+1).}$$

Exemple : pour compter le nombres de tiercés possibles lors dune course comportant 20 concurents, on procède comme suit :

- il existe 20 premiers possibles ;
- pour chacun d'eux, il existe 19 deuxièmes possibles, ce qui ouvre 20×19 possibilités ;
- pour chacune d'elles, il existe 18 troisièmes possibles. ce qui ouvre $20 \times 19 \times 18$ possibilités ;
- et il n'y a aucune raison d'en rester là.

On voit donc que, dans le cas général, le résultat sera le produit de p facteurs allant en décroissant de 1 à partir de n.

Démonstration : soit E l'ensemble en question, n le nombre des ses éléments, on procède par récurrence sur p. On a de façon évidente $A_n^0 = 1$ et $A_n^1 = n$. Soit p un entier tel que $1 \leq p < n$, on suppose que $A_p^n = n(n-1) \ldots (n-p+1)$. À chaque arrangement de p éléments de E :

$$a = (a_1, a_2, \ldots, a_p),$$

on associe l'ensemble E_a des arrangements :

$$a_1, a_2, \ldots, a_p, a_{p+1}$$

de $p+1$ éléments de E qui prolongent a. L'élément a_{p+1} pouvant être l'un quelconque des éléments de $E - \{a_1, a_2, \ldots, a_p\}$, on a :

$$\text{card}(E_a) = n - p.$$

On définit ainsi une partition de l'ensemble des arrangements de $p+1$ éléments de E en A_p^n classes de $n-p$ éléments. Il résulte alors du principe des bergers que :

$$A_n^{p+1} = A_n^p \times (n-p) = n(n-1) \ldots (n-p+1)(n-p).$$

Ce résultat est celui qu'on obtient en substituant $p+1$ à p dans l'expression avancée. Il est alors prouvé qu'il vaut pour $p = 1, 2, \ldots, n$. ◁

N.B. On notera que ce nombre prend aussi la forme :

$$A_n^p = \frac{n!}{(n-p)!}.$$

qui vaut encore pour $n = 0$, avec la convention habituelle qui veut que $0! = 1$.

*** Permutations**

La propriété précédente s'applique dans le cas où $p = n$ et le théorème (3-5) justifie l'énoncé qui suit.

(8-6) Théorème : le nombre des permutations d'un ensemble de n éléments est égal à $n!$

Remarque : il est facile de voir que ce nombre est aussi celui des bijections entre deux ensembles à n éléments.

*** Combinaisons**

(8-7) Théorème : soit n et p deux entiers tels que $n \geq p$. Le nombre de parties à p éléments d'un ensemble à n éléments est égal à :

$$\frac{A_n^p}{p!} = \frac{n!}{p!(n-p)!}.$$

Démonstration : soit E un ensemble à n éléments, on note P l'ensemble des ses parties à p éléments. On considère un ensemble F à p éléments et l'ensemble I des applications injectives de F dans E. Comme l'image d'une telle application est une partie à p éléments de E, on peut considérer l'application suivante :

$$\begin{aligned} \varphi : I &\longrightarrow P \\ f &\mapsto f(F) \end{aligned}$$

Soit A une partie à p éléments de E. Toute application f injective, telle que $f(F) = A$ induit une bijection de F sur A. Réciproquement toute bijection de F sur A s'étend de façon unique en une injection de F dans E. On a donc :

$$\operatorname{card} \varphi^{-1}(A) = p!$$

et par suite :

$$A_n^p = \operatorname{card} I = p! \times \operatorname{card} P.$$

Ce qui est bien le résultat avancé. ◁

Remarque : on parle de *combinaison* de p éléments de E pour désigner une partie de E contenant p éléments (1). Ce qui explique la notation usuelle :

$$C_n^p = \frac{n!}{p!(n-p)!}.$$

Pour les calculs pratiques, on retiendra l'expression suivante :

$$C_n^p = \frac{n(n-1) \ldots (n-p+1)}{p!}.$$

Elle vaut pour $p > 0$. On retiendra aussi la formule de récurrence :

$$C_n^p = C_n^{p-1} \frac{n-p+1}{p}.$$

C'est elle qu'on utilisera pour concevoir un programme de calcul de ces nombres.

---

1 La persistance de cet usage témoigne du fait que les préoccupations relatives au dénombrement sont bien antérieures à l'emploi systématique des concepts ensemblistes.

§ 9. Les coefficients du binôme

L'intérêt des nombres notés C_n^p dépassant largement le cadre des seuls problèmes de dénombrement, il nous faut en dire un peu plus à leur sujet.

Tout d'abord, il découle de l'expression :

$$C_n^p = \frac{n!}{p!(n-p)!}.$$

la propriété suivante.

(9-1) *Symétrie* des C_n^p : pour tous entier naturels n et p tels que $p \leq n$, on a :

$$C_n^p = C_n^{n-p}.$$

*** Le triangle de Pascal**

(9-2) Proposition : pour tous entiers naturels n et p tels que $1 \leq p \leq n-1$, on a :

$$C_n^p = C_{n-1}^{p-1} + C_{n-1}^p.$$

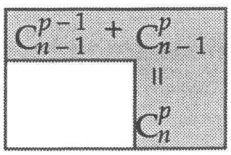
Remarque : il est facile de vérifier cette formule à partir de l'expression trouvée mais plus intéressant d'en donner une démonstration directe à partir de la définition.

Démonstration : on considère un ensemble E de n éléments. On en distingue un élément qu'on note a. Les parties de E formées de p éléments sont au nombre de C_n^p. Elles se répartissent en deux classes :

- celles qui contiennent a, on les obtient en ajoutant a aux parties à $p-1$ éléments de $E-\{a\}$, leur nombre est donc C_{n-1}^{p-1} ;
- celles qui ne contiennent pas a, ce sont aussi les parties à p éléments de $E-\{a\}$, leur nombre est donc C_{n-1}^p.

Il est clair que ces deux ensembles forment une partition de P, ce qui donne bien la relation avancée. ◁

On en déduit un moyen rapide de dresser un tableau de ces nombres, appelé *triangle de Pascal*. Le calcul s'effectue suivant le schéma ci dessous sachant que la première colonne et la diagonale ne comportent que le chiffre 1.



$p \rightarrow$ \ $n \downarrow$	0	1	2	3	4	5	6	7	...
0	1								
1	1	1							
2	1	2	1						
3	1	3	3	1					
4	1	4	6	4	1				
5	1	5	10	10	5	1			
6	1	6	15	20	15	6	1		
7	1	7	21	35	35	21	7	1	
⋮									

*** La formule du binôme de Newton** (1)

(9-3) Théorème : pour tous nombres réels ou complexes, x et y, pour tout entier naturel n, non nul, on a :

$$(x+y^n = \sum_{p=1}^{n} C_n^p x^p y^{n-p} = x^n + nx^{n-1}y + \ldots + C_n^p x^p y^{n-p} + \ldots + nxy^{n-1} + y^n.$$

Démonstration : on procède par récurrence sur n. La propriété est évidemment vérifiée pour $n=1$ car $C_1^0 = C_1^1 = 1$. Soit $n \geq 0$, on suppose que :

$$(x+y)^n = x^n + nx^{n-1}y + \ldots + C_p^n x^{n-p}y^p + \ldots + nxy^{n-1} + y^n.$$

Il s'ensuit que :

$$\begin{aligned}(x+y)^{n+1} &= (x+y)^n(x+y)\\ &= (x^n + nx^{n-1}y + \ldots + C_n^p x^{n-p}y^p + \ldots + nxy^{n-1} + y^n)(x+y)\\ &= x^{n+1} + nx^n y + \ldots + C_n^p x^{n-p+1}y^p + \ldots + xy^n\\ &\qquad + x^n y + nx^{n-1}y + \ldots + C_n^{p-1} x^{n-p+1}y^p + \ldots + nxy^n + y^{n+1}\\ &= x^{n+1} + (n+1)x^n y + \ldots + (C_n^{p-1} + C_n^p)x^{n-p}y^p + \ldots + (n+1)xy^n + y^{n+1}\end{aligned}$$

On applique la proposition 4-2, on obtient :

$$(x+y)^{n+1} = x^{n+1} + (n+1)x^n y + \ldots + C_{n+1}^p x^{n-p}y^p + \ldots + (n+1)xy^n + y^{n+1}$$

Ce qui montre que la propriété est vraie pour $n+1$. On en conclut qu'elle est vraie pour tout $n \geq 1$. ◁

Remarque : on peut aussi démontrer ce résultat en s'appuyant sur la définition. Si l'on développe $(x+y)^n$ sans tenir compte de la commutativité de la multiplication, on fait apparaître tous les 2^n monômes de degré n possibles. Dans chacun d'eux, la position des y est associée à une partie de $\{1, 2, \ldots, n\}$ et cette correspondance est bijective. Le nombre des monômes de degré p en y est donc égal au nombre des parties à p éléments de $\{1, 2, \ldots, n\}$. Il donne le coefficient du terme en $x^{n-p}y^p$.

En substituant 1 à x et y dans la formule du binôme on obtient :

$$2^n = \sum_{p=0}^{n} C_n^p = 1 + n + \ldots + C_n^p + \ldots + n + 1.$$

On retrouve ainsi que le nombre des parties d'un ensemble de n éléments est 2^n.

Remarque : la démonstration classique de la formule du binôme, par récurrence, masque l'explication réelle. Si l'on développe de $(x+y)^n$ sans tenir compte de la commutativité de la multiplication, on fait apparaître tous les 2^n monômes de degré n possibles, en x et y. Dans chacun d'eux, la position des x est associée à une partie de $[1, n]$ et cette correspondance est bijective. Le nombre des monômes de degré p en x est donc égal au nombre des parties à p éléments de $[1, n]$.

---

1 Isaac Newton (1642 - 1727) mathématicien, phycisien, astronome et penseur anglais, s'est illustré dans des domaines aussi divers que le calcul différentiel, l'optique et la mécanique céleste. Sa loi de l'attraction universelle reste, aujourd'hui encore, l'un des fondements de la vision du monde.

*** Nombre des injections croissantes de $[1,p]$ dans $[1,n]$**

L'image d'une telle injection est une partie à p éléments de $[1,n]$.

Réciproquement, p éléments de $[1,n]$ étant donnés, il existe une seule façon de les ranger par ordre croissant. On définit ainsi une injection croissante de $[1,p]$ dans $[1,n]$.

Le nombre cherché est donc exactement le nombre des parties à p éléments de l'ensemble à n éléments $[1,n]$, c'est-à-dire C_n^p.

*** Nombre des applications croissantes de $[1,n]$ dans $[1,p]$**

Une application croissante de $[1,n]$ **dans** $[0,p]$ est une suite finie :

$$u_1, u_2, \dots, u_n \text{ telle que } 1 \le u_1 \le u_2 \le \dots \le u_n \le p.$$

On a donc :

$$1 \le u_1 < u_2 + 1 < u_3 + 2 < \dots < u_n + n - 1 \le p + n - 1.$$

On en déduit une application strictement croissante de $[1,n]$ dans $[0,p+n-1]$.

Réciproquement, toute application strictement croissante de l'ensemble $[1,n]$ dans $[1,p+n-1]$, est une suite $y_1, y_2, \dots, y_n$ telle que :

$$1 \le y_1 < y_2 < \dots < y_n \le p + n - 1.$$

On en déduit les inégalités suivantes :

$$1 \le y_1 \le y_2 - 1 \le y_3 - 2 \le \dots \le y_n - n + 1 \le p.$$

Puis une application croissante (au sens large) et une seule, de $[1,n]$ dans $[1,p]$.

Il y a donc bijection entre les deux ensembles suivants :

- les applications croissantes de $[1,n]$ **dans** $[1,p]$.
- les applications **strictement** croissantes de $[1,n]$ **dans** $[0,p+n-1]$.

Le résultat précédent montre que le nombre cherché est C_{n+p-1}^p.

*** Nombre des solutions entières de l'inéquation $x_1 + x_2 + \dots + x_n \le p$**

En posant :

$$f(1) = x_1 \ , \ f(2) = x_1 + x_2 \ , \ \dots \ , \ f(n) = x_1 + x_2 + \dots + x_n,$$

on définit une application croissante f, de $[1,n]$ dans $[0,p]$. On vérifie immédiatement que la correspondance entre l'élément $(x_1, x_2, \dots, x_n)$ et f est une bijection entre l'ensemble étudié et l'ensemble des applications croissantes de $[1,n]$ dans $[0,p]$.

Le nombre cherché est donc C_{n+p+1}^p.

*** Nombre des solutions entières de l'équation $x_1 + x_2 + \dots + x_n = p$**

Il suffit de retrancher des éléments $(x_1, x_2, \dots, x_n)$ de $\mathbf{N}^n$, tels que :

$$x_1 + x_2 + \dots + x_n \le p,$$

ceux pour lesquels on a :

$$x_1 + x_2 + \dots + x_n \le p - 1.$$

Le nombre cherché est donc :

$$C_{n+p}^p - C_{n+p-1}^{p-1} = C_{n+p-1}^p$$

*** Combinaisons avec répétitions**

On peut retrouver le résultat précédent en remarquant qu'il représente aussi le nombre de façons de répartir n objets indistincts dans des classes numérotées de 1 à p. Une telle répartition peut se schématiser par une suite écrite au moyen de deux symboles, par exemple 0 et de 1, les zéros symbolisant les objets et les 1 des séparations. Ainsi la suite :

$$0\,0\,0\,1\,0\,0\,1\,1\,0\,0\,0\,1\,0\,0\,1$$

représente la répartition suivante de 10 objets dans 6 cases :

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

De façon générale, on est conduit à dénombrer les suites formées de n zéros représentant les objets et de $p-1$ séparateurs. Une telle suite est bien définie, de façon unique, par la donnée des places des zéros.

$$0\,0\,0\,|\;0\,0\;|\;\;|\;0\,0\,0\,|\;0\,0\;|$$

c'est-à-dire par la donnée de n éléments de $[1, n+p-1]$. Le nombre cherché est donc :

$$C_{n+p-1}^{p}.$$

Ce type de préoccupations conduit à parler de *combinaison avec répétitions* de *taille p* des éléments d'un ensemble à n éléments : $E = \{a_1, a_2, \ldots, a_n\}$. On entend par là les applications δ, de E dans **N**, telles que :

$$\delta(a_1) + \delta(a_2) + \ldots + \delta(a_n) = p.$$

*** Permutations avec répétitions**

On voit couramment poser des exercices où il est demandé de compter des anagrammes, par exemple : combien de mots peut-on former avec les lettres du mot :

MATHEMATIQUES ?

Il s'agit en fait d'attribuer un numéro d'ordre à chacune des lettres utilisées. Au départ il y a 13 places à occuper et donc C_{13}^{2} façons de placer deux fois la lettre M. Il reste alors 11 places libres et C_{11}^{2} façons de placer deux fois la lettre A et ainsi de suite ...

Le nombre cherché s'exprime donc comme suit :

C_{13}^{2}	C_{11}^{2}	C_{9}^{2}	C_{7}^{1}	C_{6}^{2}	C_{4}^{1}	C_{3}^{1}	C_{2}^{1}	C_{1}^{1}
M	A	T	H	E	I	Q	U	S

Ce qui donne :

$$\frac{13\times12}{1\times2}\times\frac{11\times10}{1\times2}\times\frac{8\times8}{1\times2}\times\frac{7}{1}\times\frac{6\times5}{1\times2}\times\frac{4}{1}\times\frac{3}{1}\times\frac{2}{1}\times\frac{1}{1}=\frac{13!}{8}=778\,377\,600$$

De façon générale, ce problème peut se poser dans les termes suivants. Étant donnés un ensemble de n éléments : $E = \{a_1, a_2, \ldots, a_n\}$ et n nombres : $p_1, p_2, \ldots, p_n$ de somme p. Étudier les aplications γ de $[1, p]$ dans E telles que :

$$\gamma^{-1}(a_1) = p_1,\ \gamma^{-1}(a_2) = p_2,\ \ldots,\ \gamma^{-1}(a_n) = p_n.$$

On peut parler de *permutations avec répétitions* de $a_1, a_2, \ldots, a_n$ – bien que cet usage soit peu en accord avec celui habituel du terme permutation.

Une telle application est bien définie par le choix des ensembles :

$$\gamma^{-1}(a_1), \gamma^{-1}(a_2), \ldots, \gamma^{-1}(a_n).$$

Définir $\gamma^{-1}(a_1)$, c'est choisir une partie à p_1 éléments de $[1, p]$. Il existe donc C_p^{p-1} possibilités. Définir $\gamma^{-1}(a_2)$ c'est choisir une partie à p_2 éléments de $[1, p] - \gamma^{-1}(a_2)$. Il y a donc $C_{p-p_1}^{p_2}$ possibilités et ainsi de suite ... jusqu'à ce qu'il n'y ait plus qu'une possibilité de choisir les éléments de $\gamma^{-1}(a_n)$ parmi les p_n éléments de E restant.

Le nombre total de choix possibles est égal au produit :

$$C_p^{p_1} C_{p-p_1}^{p_2} C_{p-p_1-p_2}^{p_3} \ldots C_{p_n}^{p_n}.$$

Ce qui donne :

$$\frac{p!}{p_1!\ p_2! \ldots p_n!}.$$

Notons qu'on retrouve bien les symétries du problème dans la forme du résultat.

Chapitre IV. Les nombres entiers relatifs

§ 10. L'anneau des entiers relatifs

On donne un résultat aux soustractions impossibles sans aucune considération a priori sur les nombres négatifs. Ce qui dispense de l'intermédiaire laborieux qui s'impose aux collégiens sous le nom de *"somme algébrique"*.

* Construction de l'anneau Z

On considère la relation, définie sur $\mathbf{N}\times\mathbf{N}$, en convenant que :

$$(m,n)\sim(m',n')$$

représente l'égalité suivante :

$$m+n'=m'+n.$$

On vérifie facilement que $\sim$ est une relation d'équivalence. On considère alors l'ensemble quotient :

$$\mathbf{Z}=(\mathbf{N}\times\mathbf{N})/\sim.$$

Provisoirement, il est commode, de noter les éléments de $\mathbf{Z}$, $[m-n]$ plutôt que $C_{(m,n)}$. De sorte que si m, n, m', n' sont des éléments de $\mathbf{N}$, on a :

$$[m-n]=[m'-n'] \Leftrightarrow m+n'=m'+n.$$

Le point essentiel est de vérifier que l'addition et la multiplication de $\mathbf{N}$ sont compatibles avec le quotient. On entend par là que si :

$$[m-n]=[m'-n'] \text{ et } [p-q]=[p'-q'],$$

alors on a les deux égalités suivantes (1) :

(1) $$[(m+p)-(n+q)]=[(m'+p')-(n'+q')]$$

(2) $$[(m\times p+nq)-(m\times q+n+p)]=[(m'\times p'+n'\times q')-(m'\times q'+n'+p')]$$

Il est alors cohérent de poser :

$$(m-n)+(p-q)=(m+p)-(n+q)$$

$$(m-n)\times(p-q)=(m\times p+n\times q)-(m\times q+n+p)$$

L'ensemble $\mathbf{Z}$ est alors doté de deux lois de composition internes qu'on note aussi :

$$+ \text{ et } \times.$$

La vérification que $\mathbf{Z}$ est un anneau commutatif n'est qu'une formalité fastidieuse dont nous nous dispensons.

---

1 Il n'y a là rien de mystérieux, en effet, le but de l'opération est disposer d'un nouvel ensemble où $[m-n]$ représente le résultat de la soustraction de n à m dans $\mathbf{N}$, si celle-ci est possible et, dans le cas contraire, un nouveau nombre. On cherche donc à étendre la validité des égalités :

$$(m-n)+(p-q)=(m+p)-(n+q)$$

$$(m-n)\times(p-q)=(m\times p+n\times q)-(m\times q+n\times p)$$

*** Z contient N**

Il est naturel de considérer l'application suivante :

$$j : \mathbf{N} \longrightarrow \mathbf{Z}$$
$$n \mapsto [n-0]$$

et de constater que :

(1) $j(n+p) = [(n+p)-0] = [n-0] + [p-0] = j(n) + j(p)$,

(2) $j(n \times p) = [(n \times p)-0] = [n-0] \times [p-0] = j(n) \times j(p)$,

(3) $[n-0] \neq [p-0] \Rightarrow n \neq p$.

On en conclut que les deux lois sont stables par j et que cette application est injective. Elle permet donc d'identifier $j(\mathbf{N})$ à $\mathbf{N}$, ce qui, concrètement, revient à noter :

$$[n-0] = n.$$

Dans ces conditions, si l'on considère un élément quelconque $z = [m-n]$ de $\mathbf{Z}$, on est devant l'alternative suivante :

- $m \geq n$ et alors $[m-n] = [(m-n)-0] = m-n$,
- $m < n$ et alors $[0-(n-m)] = -[(n-m)-0] = -(n-m)$.

Ce qui signifie que :

$$z \in \mathrm{N} \text{ OU } -z \in \mathbf{N}.$$

On peut alors légitimement baptiser $\mathbf{Z}$:

"l'anneau des nombres entiers relatifs".

Il se compose, en effet, des éléments de $\mathbf{N}$, auxquels viennent s'ajouter leur opposés pour une nouvelle addition qui étend celle de $\mathbf{N}$.

*** L'ordre de N s'étend à Z**

On étend la relation d'ordre de $\mathbf{N}$ à $\mathbf{Z}$, en notant $z \leq z'$ la relation définie sur $\mathbf{Z}$, par :

$$z' - z \in \mathbf{N}.$$

Conventions : on convient qu'un entier naturel, **différent de zéro**, est :

- *positif*, s'il appartient à $\mathbf{N}$,
- *négatif*, dans le cas contraire.

Étant entendu que :

0 n'est ni positif, ni négatif [1].

On définit la *valeur absolue* d'un entier relatif z comme suit :

$$|z| = \begin{cases} z, \text{ si } z \geq 0 \\ -z, \text{ si } z < 0 \end{cases}.$$

---

1 Contrairement à un usage couramment répandu qui voudrait que plus grand signifie plus grand ou égal. Ce qui est en désaccord avec l'usage habituel et ne serait pas grave, s'il n'existait, par ailleurs, de sérieuses raisons, d'ordre purement mathématique, de regretter cet état de fait.

*** La division euclidienne**

L'extension de la division euclidienne aux entiers relatifs est une opération essentiellement formelle. Elle se traduit comme suit.

(10-1) Théorème : étant donnés deux entiers relatifs a et b, si b est non nul, il existe un couple $(q, r) \in \mathbf{Z} \times \mathbf{N}$, et un seul, tel que :

$$a = bq + r \text{ et } 0 \leq r < |b|.$$

Démonstration : on part de la division portant sur les valeurs absolues :

$$|a| = |b|q_1 + |r| \text{ et } 0 \leq r < |b|$$

On ajuste la valeur du quotient selon les signes de a et b, sans modifier le reste. ◅

*** Le point sur "les quatre opérations"**

Dans **Z**, l'équation :

$$a + x = b,$$

où a et b sont des entiers relatifs, admet toujours pour solution :

$$x = b - a.$$

L'opération "soustraire b de a" est devenue "ajouter l'opposé de b à a".

On note alors que si a et b sont deux nombres entiers relatifs et si $b \neq 0$, l'équation :

$$a = bx$$

n'admet de solution que si l'équation correspondante dans **N** :

$$|a| = |b|x$$

admet une solution.

§ 11. Le théorème de Bézout

* Diviseurs et multiples

La terminologie introduite pour **N**, vaut pour **Z**, à ceci près que :

$$(a \text{ divise } b \text{ ET } b \text{ divise } a) \Rightarrow |a| = |b|.$$

* Les sous-groupes de Z

Rappel : un sous-groupe additif de **Z**, est une partie non vide G de **Z**, telle que :

- pour tous éléments a et b de G, $a+b$ est dans G,
- pour tout élément a de G, $-a$ est dans G.

Exemple : soit n un entier relatif, on note $n\mathbf{Z}$ l'ensemble des multiples de n, autrement dit :

$$n\mathbf{Z} = \{nz \mid z \in \mathbf{Z}\}.$$

C'est un sous-groupe de **Z**. En effet, si a et b sont deux éléments de $n\mathbf{Z}$, il existe deux éléments z et z' de **Z**, tels que

$$a = n\,z \text{ et } b = n\,z'$$

et alors :

$$a + b = n(z + z')$$

est un élément de $n\mathbf{Z}$. Si a est dans $n\mathbf{Z}$, alors :

$$-a = -nz = n(-z)$$

est dans $n\mathbf{Z}$.

C'est un point essentiel pour la suite que tout sous-groupe de **Z** soit de cette forme, ce que nous montrons maintenant.

(11-1) Théorème : tout sous-groupe G de **Z** est de la forme :

$$G = n\mathbf{Z} \text{ où } n \in \mathbf{Z}.$$

Démonstration : comme il est clair que $\{0\} = 0\,\mathbf{Z}$, la question est réglée si $G = \{0\}$. On suppose donc désormais que $G \neq \{0\}$. On note $G^+ = \{x \in G \mid x > 0\}$. Comme $G \neq \{0\}$, G contient un élément $x \neq 0$ et alors soit $x \in G^+$, soit $-x \in G^+$. On est donc assuré que $G^+ \neq \varnothing$. Il s'ensuit que G^+ contient un plus petit élément qu'on note n_0.

Il est clair que G contient tous les multiples de n_0, on a donc :

$$n_0\mathbf{Z} \subseteq G.$$

Réciproquement, soit n un élément de G^+, on a $n > n_0$. La division euclidienne de a par n nous donne :

$$n = n_0 q + r \text{ et } 0 \leq r < n_0,$$

Ce qui se traduit :

$$0 \leq n - n_0 q = rr < n_0.$$

Or, n et $n_0 q$ sont deux éléments de G, r appartient donc à G. Ainsi, on a à la fois :

$$r \in G \text{ et } 0 \leq r < n_0.$$

On en conclut que $r = 0$. Autrement dit $n \in n_0\mathbf{Z}$, ce qui prouve que :

$$G \subseteq n_0\mathbf{Z}.$$

Il est alors établi que $G = n_0\mathbf{Z}$. ◁

Convention : si $G = n\mathbf{Z}$, on dit que n est un générateur de G. Si $n\mathbf{Z} = m\mathbf{Z}$, il est clair que n et m étant diviseurs l'un de l'autre on a $m = n$ ou $m = -n$. Ainsi tout sous-groupe de **Z**, autre que trivial – i.e. $\{0\}$ – possède deux générateurs qui sont opposés.

(11-2) Lemme : a et b désignant deux entiers relatifs, non tous deux nuls, l'ensemble

$$G = \{au + bv \mid u \in \mathbf{Z} \text{ et } v \in \mathbf{Z}\}$$

est toujours un sous-groupe de **Z**.

Démonstration : exercice facile. ◁.

Convention : G est appelé le *sous-groupe* de **Z** *engendré* par a et b et on le note $[a, b]$.

(11-3) Lemme : étant donnés deux entiers relatifs a et b, soit d, tel que :

$$[a, b] = d\mathbf{Z}.$$

- d est un diviseur commun de a et b,
- tout diviseur commun de a et b divise d.

Démonstration : a et b sont deux éléments de $d\mathbf{Z}$, ils sont donc des multiples de d.

Soit D un diviseur commun à a et b, on a $a = Du$ et $b = Dv$. Il s'ensuit que :

$$a \in D\mathbf{Z} \text{ et } a \in D\mathbf{Z}.$$

Puis :

$$d\mathbf{Z} \subseteq D\mathbf{Z} \ , \ d \in D\mathbf{Z}.$$

Ce qui montre que D divise d. ◁

Commentaire : nous retrouvons ici le concept de pgcd qui nous est familier dans **N**, à ceci près que désormais d est défini au signe près. Dans ces conditions d devrait, en principe, être appelé **un** pgcd de a et b En pratique, nous éviterons les contorsions byzantines en convenant que, sauf mention explicite du contraire, **le** pgcd de a et b est celui des deux qui est positif – c'est notamment le cas lorsqu'on utilise la notation :

$$\text{pgcd}(a, b).$$

On retient en particulier

(11-4) Corollaire : si d est le pgcd de a et b, il existe deux entiers relatifs u et v , tels que :

$$au + bv = d.$$

(11-5) Théorème Bézout [1]

Deux entiers a et b sont premiers entre eux si, et seulement si, il existe deux entiers relatifs u et v, tels que :

$$au + bv = 1.$$

Démonstration : s'il existe u et v tels que $au + bv = 1$ et si D est un diviseur commun à a et b, alors D divise 1 donc $D = \pm 1$.

Réciproquement, si a et b sont premiers entre eux, le corollaire précédent s'applique avec $d = 1$. ◁

---

1 Étienne BÉZOUT(1730-1783) : mathématicien Français, examinateur des gardes de la marine, est l'auteur d'une "Théorie générale des équations algébriques" (1779). Son nom reste attaché à la démonstration que deux courbes algébriques de degrés m et n ont mn points communs (réels ou imaginaires, distincts ou confondues, à distance finie ou à l'infini, à moins qu'elles n'admettent une partie commune).
C'est vraisemblablement par association d'idées que son nom se trouve attaché au théorème ci-dessus.

(11-6) Théorème d'Euler [1]

Deux entiers a et b ne sont pas premiers entre eux si, et seulement si, il existe deux entiers relatifs u et v, tels que :

$$au+bv=0 \ , \ 0<|u|<|b| \ \text{ et } \ 0<|v|<|a|.$$

Démonstration : soit d un diviseur commun à a et b, on pose :

$$a'=\frac{a}{d} \ \text{ et } \ b'=\frac{b}{d}.$$

On a donc :

$$ab'=a'b'd=ba'$$

et ainsi :

$$b'a-a'b=0.$$

Si $d>1$, on a effectivement :

$$u=b' \ , v=-a' \ \text{ et } \ |u|<|b| \ , \ |v|<|a|.$$

Réciproquement, si :

$$au+bv=0 \ , \ 0<|u|<|b| \ \text{ et } \ 0<|v|<|a|,$$

alors :

$$au=b(-v)$$

Si a et b étaient premiers entre eux, le théorème de Gauss exigerait que a divise v, en contradiction avec $|v|<|a|$.

La démonstration est alors complète. ◁

*** Le ppcm dans Z**

(11-7) Lemme : étant donnés deux entiers relatifs a et b, soit m, tel que :

$$a\mathbf{Z}\cap b\mathbf{Z}=m\mathbf{Z}.$$

- m est un multiple commun de a et b,
- tout multiple commun de a et b est un multiple de m.

Démonstration : la première propriété est immédiate car m étant à la fois dans $a\mathbf{Z}$ et $b\mathbf{Z}$, c'est un multiple de a et de b..

Soit D un multiple commun de a et b, on a $M=au$ et $M=bv$. Il s'ensuit que :

$$M\in a\mathbf{Z} \ \text{ et } \ M\in b\mathbf{Z},$$

autrement dit :

$$M\in a\mathbf{Z}\cap b\mathbf{Z}=m\mathbf{Z},$$

Ce qui montre que M est un multiple de m. ◁

Remarque : les règles d'usage valant pour le pgcd s'appliquent, mutatis mutandi, au ppcm.

---

1 Leonhard EULER (1707-1783) : mathématicien d'origine suisse, a une laissé une œuvre qui embrasse toutes les sciences exactes de son temps et ne peut raisonnablement se résumer en quelques mots. On retrouve son nom attaché à des termes aussi divers que : "droite d'Euler", "angles d'Euler", "constante d'Euler", diverses "formule d'Euler", "intégrales eulériennes", "parcours eulériens", ...

§ 12. Les classes résiduelles modulo un entier

* Le groupe $\mathbf{Z}/n\mathbf{Z}$

Étant donné un entier n, on convient de noter $\mathfrak{R}$ la relation suivante :

$$x - y \in n\mathbf{Z}$$

qui est bien définie $\mathbf{Z}$. En d'autre termes :

$$x \mathfrak{R} y \Leftrightarrow \exists k \in \mathbf{Z},\ x - y = kn.$$

Il s'agit d'une équivalence, en effet, on a toujours :

- $x - x = 0 \in n\mathbf{Z}$,
- si $x - y = kn$, alors $y - x = (-k)n$,
- si $x - y = kn$ et $y - z = ln$, alors $x - z = (k + l)n$.

La classe de x est de la forme :

$$C_x = x + n\mathbf{Z} = \{x + kn \mid k \in \mathbf{Z}\}.$$

Convention : il est habituel de noter :

- $\overline{x}$ la classe de x, en précisant au besoin $\overline{x}_n$;
- $x \equiv y \pmod{n}$ plutôt que $x \mathfrak{R} y$, ou simplement $x = y \pmod{n}$ – ce qui se lit *"x congru à y modulo n"* ;
- $\mathbf{Z}/n\mathbf{Z}$ ou $\mathbf{Z}_n$, l'ensemble quotient de $\mathbf{Z}$ par $\mathfrak{R}$.

(12-1) Proposition : $|\mathbf{Z}/n\mathbf{Z}| = n$.

Démonstration : comme toute classe $\overline{x}$ contient le reste de la division de x par n, on a :

$$\mathbf{Z}/n\mathbf{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}.$$

et il est immédiat que les n classes ci-dessus sont distinctes. ◁

Remarque : les classes d'entiers modulo n, sont encore appellées *classes résiduelles, modulo n*. Elles sont, en effet, formées de tous les entiers dont la division par n donne le même reste

(12-2) Lemme : la surjection canonique induit une structure de groupe sur l'ensemble quotient $\mathbf{Z}/n\mathbf{Z}$.

Démonstration : si tel est bien le cas, on doit avoir :

$$\overline{(x+y)} = \overline{x} + \overline{y}$$

Il suffit de vérifier la cohérence de cette expression. C'est-à-dire que cette égalité est indépendante des représentants choisis dans chacune des classes. Soit x, x', y et y' tels que :

$$x \equiv x' \pmod{n} \text{ et } y \equiv y' \pmod{n},$$

il existe deux entiers h et l, tels que :

$$x - x' = kn \text{ et } y - y' = ln.$$

L'addition membre à membre de ces deux égalités donne :

$$(x + y) - (x' + y') = (k + l)n.$$

Ce qui montre que :

$$x + y \equiv x' + y' \pmod{n}.$$

Ainsi, la relation :

$$\overline{x} + \overline{y} = \overline{(x+y)}$$

définit effectivement une loi de composition interne sur $\mathbf{Z}/n\mathbf{Z}$ qui rend la surjection canonique additive. Une vérification banale permet de conclure. (1) ◁

Exemples de tables d'addition

mod 2

+	0	1
0	0	1
1	1	0

mod 3

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

mod 4

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Remarque : on note que, de façon générale, pour tout entier naturel m, on a :

$$m = 1 + 1 + \ldots + 1 \ (m \text{ termes}).$$

Ce qui précède montre que :

$$\overline{m} = \overline{1} + \overline{1} + \ldots + \overline{1} \ (m \text{ termes})$$

ce qui se note :

$$\overline{m} = m\,\overline{1}.$$

*** Les sous-groupes de Z/nZ**

Nous savons que les sous-groupes de **Z** sont constitués des multiples d'un élément. Cette propriété se transfère aux quotients $\mathbf{Z}/n\mathbf{Z}$ – avec quelques complications liées au fait que ces groupes sont finis.

Dans la suite, n désigne un entier donné et on note p la surjection canonique de **Z** sur $\mathbf{Z}/n\mathbf{Z}$. Rappelons que $n\mathbf{Z} = p^{-1}(0)$ est le noyau de p.

(12-3) Proposition : si d est un entier l'ensemble :

$$H = \{z\,\overline{d} \mid z \in \mathbf{Z}\}$$

est un sous-groupe de $\mathbf{Z}/n\mathbf{Z}$. Si, de plus, d divise n, alors :

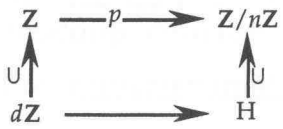
$$H = \{0, \overline{d}, 2\overline{d}, \ldots, (m-1)\overline{d}\} \text{ où } m = \tfrac{n}{d}.$$

Démonstration : de façon générale, on a :

$$H = p(d\mathbf{Z})$$

et comme $d\mathbf{Z}$ est un sous-groupe de **Z**, H est un sous-groupe de $\mathbf{Z}/n\mathbf{Z}$. Si $n = dm$, on a $m\,\overline{d} = \overline{0}$. On en déduit immédiatement que :

$$H = \{0, \overline{d}, 2\overline{d}, \ldots, (m-1)\overline{d}\}.$$ ◁



Définition : $H = \{z\,\overline{d} \mid z \in \mathbf{Z}\}$ est appelé le sous-groupe *engendré par* $\overline{d}$.

Vocabulaire : de façon énérale, un tel groupe est dit *cyclique*.

Remarque : l est clair que $\overline{1}$ engendre $\mathbf{Z}/n\mathbf{Z}$. Les autres générateurs de ce groupe seront caractérisés plus loin (cf. 12-5).

1 On retrouvera plus loin la généralisation de ce fait (cf. lemme 13-13).

(12-4) Lemme : tout sous-groupe, de $\mathbf{Z}/n\mathbf{Z}$ est cyclique.

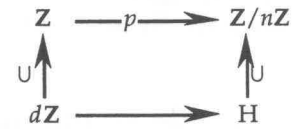
Démonstration : soit H un sous-groupe de $\mathbf{Z}/n\mathbf{Z}$, si $H=\{\bar{0}\}$, il est effectivement cyclique engendré par son seul élément. On écarte ce cas, l'image inverse de H par p est alors un sous-groupe de $\mathbf{Z}$, autre que $\{0\}$, il existe donc un entier x, tel que :

$$x\neq 0 \text{ et } p^{-1}(H)=x\mathbf{Z}.$$

et comme p est surjective, on a :

$$H=p(x\mathbf{Z}).$$

comme annoncé. ◁



(12-5) Lemme : soit x un entier non nul, le sous-groupe cyclique de $\mathbf{Z}/n\mathbf{Z}$, engendré, dans par $\bar{x}$, est le même que celui engendré par la classe du pgcd de x et de n.

Autrement dit :

$$\{k\bar{x} \mid k\in \mathbf{Z}\}=\{0,\bar{d},2\bar{d},\ldots,(m-1)\bar{d}\} \text{ où } d=\text{pgcd}(x,n) \text{ et } m=\tfrac{x}{d}.$$

Démonstration :d et m étant définis ci-dessus, on note H et K les sous-groupes de $\mathbf{Z}/n\mathbf{Z}$ engendrés respectivement par $\bar{x}$ et $\bar{d}$. C'est-à-dire qu'on a :

$$H=\{z\bar{x} \mid z\in \mathbf{Z}\} \text{ et } K=\{0,\bar{d},2\bar{d},\ldots,(m-1)\bar{d}\}.$$

Il est immédiat que :

$$\bar{x}=m\bar{d},$$

ce qui entraîne que :

$$H\subseteq K.$$

Réciproquement il découle du corollaire 11-4 qu'il existe deux entiers relatifs u et v, tels que :

$$xu+nv=d$$

et comme $\bar{n}=\bar{0}$, il existe u, tel que :

$$\bar{d}=u\bar{x}.$$

Ce qui justifie que :

$$K\subseteq H$$

et donne bien l'égalité attendue. ◁

Remarque : on obtient une illustration frappante de ce fait en joignant des sommets d'un polygone régulier de façon à obtenir un polygone régulier étoilé ... de toutes les façons possibles.

*** Les anneaux Z/*n*Z**

(12-5) Lemme : la surjection canonique de **z** sur $\mathbf{Z}/n\mathbf{Z}$ induit une structure d'anneau sur l'ensemble quotient.

Démonstration : il nous reste à justifier que la multiplication de **Z** se transfère sur le quotient. Si tel est bien le cas, on doit avoir :

$$\overline{(x \times y)} = \overline{x} \times \overline{y}.$$

Il suffit de vérifier la cohérence de cette expression, c'est-à-dire que cette égalité est indépendante des représentants choisis dans chacune des classes. Soit x, x', y et y' tels que :

$$x \equiv x' \pmod{n} \text{ et } y \equiv y' \pmod{n}.$$

Il existe deux entiers h et l, tels que :

$$x - x' = kn \text{ et } y - y' = ln.$$

On a donc :

$$x = x' + kn \text{ et } y = y' + ln.$$

La multiplication membre à membre de ces deux égalités donne :

$$xy = x'y' + (x'l + y'k + kl)n.$$

Ce qui montre que :

$$x \times y \equiv x' \times y' \pmod{n}.$$

On est alors assuré que la relation :

$$\overline{x} \times \overline{y} = \overline{(x \times y)}$$

définit effectivement une loi de composition interne sur $\mathbf{Z}/n\mathbf{Z}$ qui rend la surjection canonique multiplicative. Le reste suit. ◁

Exemples de tables de multiplication

mod 2

×	0	1
0	0	0
1	0	1

mod 3

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

mod 4

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

mod 5

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

(12-7) Théorème : la classe $\overline{m}$ de $\mathbf{Z}_n$ est inversible si, et seulement si, m est premier avec n.

Démonstration : les conditions suivantes sont équivalentes :

(1) $\overline{m}$ est un élément inversible $\mathbf{Z}_n$,

(2) $\exists u \in \mathbf{Z},\ \overline{u}\,\overline{m} = \overline{1}$,

(3) $\exists u \in \mathbf{Z}, \exists v \in \mathbf{Z},\ um + vn = 1$

(4) $\operatorname{pgcd}(m, n) = 1$

En effet, les équivalences entre (1), (2) et (3) résultent d'un jeu de traduction. L'équivalence entre (3) et (4) est celle du théorème de Bézout. ◁

Remarque : il est commode de retenir que m est inversible modulo n si, et seulement si, toute équation de la forme :

$$mx = b, \text{ où } b \in \mathbf{Z},$$

admet une solution modulo n, et une seule.

Si m est inversible $\overline{m}^{-1}b$ est la solution en question. Réciproquement, l'existence d'une solution, en particulier si $b = 1$, entraîne que $\overline{m}$ est inversible.

Convention : les éléments inversibles d'un anneau (pour la multiplication) sont couramment appelés ses *unités*.

(12-8) Corollaire : $\mathbf{Z}/n\mathbf{Z}$ est un corps si, et seulement si, n est un nombre premier.

Démonstration : $\mathbf{Z}_n$ est un corps si tout élément de $\mathbf{Z}_n^*$ est une unité. Le théorème précédent montre que cette condition est remplie si, et seulement si, n est premier avec tous les entiers m, tels que $1 \leq m < n$. Cette propriété caractérise le fait que n est premier. ◁

Exemple : considérons la table de multiplication $\mathbf{Z}_7^*$:

×	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	3	2
6	6	5	4	3	2	1

on y lit que :

- 2 et 4 sont mutuellement inverses : $2^{-1} = 4 \pmod 7$ et $4^{-1} = 2 \pmod 7$,
- de même que 3 et 5 : $3^{-1} = 5 \pmod 7$ et $5^{-1} = 3 \pmod 7$,
- 6 est son propre inverse : $6^{-1} = 6 \pmod 7$

Exemple : constater sur la table de multiplication de $\mathbf{Z}_4^*$ que l'équation $2x = 3 \pmod 4$ n'admet pas de solution.

§13. Applications arithmétiques

*** Les restes chinois**

(13-1) Théorème des restes chinois

Si les entiers m et n sont **premiers entre eux**, le système d'équations :

$$\begin{cases} x = a \pmod{m} \\ x = b \pmod{n} \end{cases}$$

admet une solution qui est unique modulo mn.

Démonstration : comme m et n sont premiers entre eux, le théorème 12-7 montre qu'il existe h, tel que :

$$mh = b - a \pmod{n}$$

Posons $x = a + hm$, il est clair que :

$$a + hm = b \pmod{n} \text{ et } a + hm = a \pmod{m}.$$

Ce qui montre que h est une solution. Il nous reste à justifier son unicité moulo mn.

Si x et y sont deux solutions, on a :

$$x - y = 0 \pmod{m} \text{ et } x - y = 0 \pmod{m},$$

$x - y$ est donc un multiple commun de m et de n et comme m et n sont premiers entre eux, c'est un multiple de mn. Autremet dit : $x - y = 0 \pmod{mn}$. ◁

Remarque : le théorème précédent se généralise par récurrence.

(13-1 bis) Théorème : si $n_1, n_2, , \ldots, n_k$ sont des entiers naturels premiers entre eux **deux à deux**, le système d'équations :

$$\begin{cases} x = a_1 \pmod{n_1} \\ x = a_2 \pmod{n_2} \\ \cdots\cdots\cdots \\ x = a_k \pmod{n_k} \end{cases}$$

admet une solution, et une seule, modulo le produit $n_1 n_2 \ldots n_k$.

Exemple : résoudre le système de congruences suivant :

$$\begin{cases} x = 2 \pmod{3} \\ x = 4 \pmod{5} \\ x = 6 \pmod{7} \end{cases}$$

On a successivement :

(1) $x = 3k + 2$
$3k + 2 = 4 \pmod{5}$
$3k = 2 \pmod{5}$
$k = 4 \pmod{5}$

(2) $k = 4 + 5l$

(2) $x = 3(4 + 5l) + 2 = 14 + 15l$
$14 + 15l = 6 \pmod{7}$
$l = 6 \pmod{7}$

(3) $l = 6 + 7m$

Reprenant (1), (2) et (3), on trouve :

$$x = 3[4 + 5(6 + 7m)] + 2,\ m \in \mathbf{Z}.$$
$$x = 104 + 105m,\ m \in \mathbf{Z}.$$

*** Le théorème de Fermat** [1]

La démonstration du théorème de Fermat, s'appuie sur le lemme qui suit.

(13-2) Lemme : si p un nombre premier, pour tout entier k, $1 \leq k < p$, le coefficient du binôme C_p^k est divisible par p.

Démonstration : nous savons que :

$$C_p^k = \frac{p(p-1) \ldots (p-k+1)}{k!}$$

est un entier. Comme $1 \leq k < p$, pn'est pas un diviseur du dénominateur, le facteur p subsistera au numérateur après simplification. Cet entier est donc divisible par p. ◁

(13-3) Théorème de Fermat

Si p est un nombre premier, alors, pour tout entier a :

$$a^p = a \pmod{p}.$$

Démonstration : on procède par récurrence. On a effectivement :

$$0^p = 0 \pmod{p}.$$

Soit a un entier, on suppose que :

$$a^p = a \pmod{p}.$$

On a donc :

$$(a+1)^p = a^p + pa^{p-1} + \ldots + C_p^k a^{p-k} + \ldots + pa + 1.$$

Le lemme montre que :

$$(a+1)^p = a^p + 1$$

Tenant compte de l'hypothèse de récurrence il vient :

$$(a+1)^p = a + 1 \pmod{p}.$$

Ce qui justifie la validité pour tout a. ◁

(13-4) Corollaire : si p est un nombre premier, pour tout entier a, premier à p, on a :

$$a^{p-1} = 1 \pmod{p}.$$

Démonstration : comme a est premier à p, ce nombre est inversible modulo p. il existe donc b, tel que $ba = 1 \pmod{p}$. En multipliant les deux membres de l'égalité du théorème de Fermat par ce nombre, on obtient celle avancée. ◁

Exemple : effectuer la division de 314^{151} par 7 serait une tâche impossible, ce qui n'interdit pas d'en connaître le reste. On note que :

$$314^6 = 1 \pmod{7} \text{ et } 151 = 6 \times 25 + 1,$$

on obtient immédiatement :

$$314^{151} = (314^6)^{25} \times 314 = 314 = 6 \pmod{7}.$$

---

1 Piere de FERMAT (1601-1665) : mathématicien français, est considéré comme le coinventeur, avec Pascal, du calcul des probabilités. Son nom est attaché à un principe d'optique qui se généralise en mécanique sous le nom de *principe de moindre action*. Il est considéré comme l'inventeur de la théorie des nombres. Le théorème démontré ici est aussi appelé *"petit théorème de Fermat"* par opposition au *"grand théorème de Fermat"* resté sans démonstration jusqu'en 1993, date à laquelle l'anglais Andrew Wiles a mis un terme à ce qui fut considéré comme la "quête du Graal des mathématiques", tant cette recherche a mobilisé d'énergie et surtout hanté les rêves de générations de mathématiciens.

Chapitre V. Groupes

§ 14. Les concepts de base

Définition : on appelle *groupe* tout ensemble muni d'une loi de composition interne associative, dotée d'un élément neutre et telle que tout élément soit inversible. Autrement dit, G est un groupe s'il existe une application :

$$\begin{array}{ccc} G\times G & \longrightarrow & G \\ (x,y) & \mapsto & xy \end{array}$$

telle que :

(1) $\forall x\in G\ \forall y\in G\ \forall z\in G\ (xy)z=x(yz)$ — associativité

(2) $e\in G$ et $\forall x\in G\ xe=ex$ — élément neutre

(3) $\forall x\in G\ \exists x'\in G\ xx'=x'x.$ — élément inverse

Si de, plus, on a :

(4) $\forall x\in G\ \forall y\in G\ xy=yx,$

on dit que le groupe est *commutatif* ou encore *abélien*[1].

(14-1) Proposition : dans tout groupe, l'élément neutre est unique et tout élément admet un inverse, et un seul.

Démonstration : si deux éléments e et e' vérifient (2), on a en particulier :

$$e'=e'e=e.$$

Soit x un élément d'un groupe si x' et x'' vérifient (3), alors :

$$x''=x''e=x''xx'=ex'=x'.$$

L'assertion avancée est donc toujours vérifiée. ◁

Convention : ces propriétés d'unicité permettent de noter systématiquement :

- 1 l'élément neutre,
- x^{-1} l'inverse de x.

Remarque : lorsqu'on traite spécifiquement des groupes abéliens l'usage veut qu'on adopte plutôt une notation additive. Dans ces conditions, l'élément neutre est noté 0, on parle d'élément *opposé* plutôt que d'inverse et l'on note $-x$ l'opposé de x.

(14-2) Proposition : dans tout groupe, tout élément est simplifiabe à gauche comme à droite.

Autrement dit, si x, y et z sont des éléments d'un groupe, on a :

$$xy=xz\ \Rightarrow\ y=z \text{ et } xy=zy\ \Rightarrow\ x=z.$$

Démonstration : soit G un groupe et x, y, z trois de ses éléments, si $xy=xz$, on a toujours :

$$y=1y=x^{-1}xy=x^{-1}xz=1z=z$$

et ainsi $y=z$. On procède façon analogue pour la simplification à droite. ◁

---

1 Niels Henrik ABEL (1802-1829) : mathématicien norvégien, a démontré l'impossibilité de résoudre au moyen de radicaux l'équation générale de degré au moins cinq. Son nom reste attaché au critère de semi convergence des séries et à un certain type d'intégrales.

(14-3) Proposition : dans tout groupe, toute équation de la forme :

$$ax = b \text{ (resp. } xa = b),$$

où a et b sont donnés, admet une solution, et une seule.

Démonstration : soit G un groupe, considérons deux de ses éléments a et b. Notons :

$$c = a^{-1}b \text{ et } d = ba^{-1}.$$

On a :

$$ac = aa^{-1}b = 1b = b \text{ et } ca = ba^{-1}a = b1 = b.$$

Ainsi une solution existe, dans G, pour toute équation de ce type. L'unicité découle de la règle de simplification . ◁

(14-4) Proposition : si x et y sont deux éléments d'un groupe, alors :

$$(xy)^{-1} = y^{-1}x^{-1}.$$

Plus généralement, on a :

$$(x_1 \dots x_n)^{-1} = x_n^{-1} \dots x_1^{-1}.$$

Démonstration : exercice. ◁

*** Sous-groupe**

Définition : soit G un groupe, on appelle *sous-groupe* de G, toute partie H de G sur laquelle la loi de G induit une structure de groupe. On note alors $H \leq G$.

(14-5) Théorème : une partie H d'un groupe G est un sous-groupe si, et seulement si :

(1) $H \neq \emptyset$,

(2) $\forall x \in H \ \forall y \in H, xy \in H$,

(3) $\forall x \in H \ x^{-1} \in H$.

Démonstration : ces conditions sont évidemment nécessaires. Montrons qu'elles sont suffisantes.

- La condition (2) assure que la loi de G induit une loi de composition interne de H.
- L'associativité de cette loi sur H découle de celle sur G.
- Comme H est non vide, il existe x appartenant à H et les conditions (3) et (2) assurent que :

  $$x^{-1} \in H \text{ et } 1 = x.x^{-1} \in H,$$

  1 est alors élément neutre de la loi de H.
- (3) complète les conditions requises pour que H soit un groupe. ◁

Dans la pratique, il est généralement avantageux d'effectuer simultanément la vérification de (2) et (3). C'est ce que permet la proposition qui suit.

(14-5 bis) Corollaire : une partie H d'un groupe G est un sous-groupe si, et seulement si :

(1) $H \neq \emptyset$,

(2') $\forall x \in H \ \forall y \in H \ xy^{-1} \in H$,

Démonstration : exercice. ◁

Remarque : G et {1} sont toujours des sous-groupes de G, {1} est appelé le sous-groupe *trivial* et noté simplement 1.

(14-6) Proposition : l'intersection de toute famille de sous-groupes est un sous-groupe.

Démonstration : c'est immédiat. ◁

* Exemples.

- Groupes abéliens additifs :

$$\mathbf{Z} < \mathbf{Q} < \mathbf{R} \leq \mathbf{C}.$$

- Groupes abéliens multiplicatifs :

$$\begin{array}{ccc} \mathbf{Q}^* & < & \mathbf{R}^* < \mathbf{C}^* \\ \vee & & \vee \\ \mathbf{Q}^+ & < & \mathbf{C}^+ \end{array}$$

- Groupes non abéliens : penser à la géométrie.

*** Morphismes de groupes**

Définition : étant donnés deux groupes G et G', on appelle *morphisme* de G dans G' ou *homomorphisme*, toute application f, de G dans G', telle que :

$$\forall x \in G \ \forall y \in G \ f(xy) = f(x)f(y).$$

(14-7) Proposition : Si f est un homorphisme de G dans G', on a :

(1) $f(1) = 1$,

(2) $\forall x \in G \ f(x^{-1}) = (f(x))^{-1}$.

Démonstration : on a toujours :

$$f(1)f(1) = f(11) = f(1) = 1f(1).$$

La règle de simplification dans G' assure que $f(1) = 1$. Si x appartient à G, alors on a toujours :

$$f(x)f(x^{-1}) = f(xx^{-1}) = f(1) = 1$$

et donc $f(x^{-1}) = [f(x)]^{-1}$. ◁

(14-8) Proposition : si f est un morphisme de groupes de G dans G', on a :

1) si H est un sous-groupe de G, f(H) est un sous-groupe de G',

2) si H' est un sous-groupe de G', f^{-1}(H') est un sous-groupe de G.

Démonstration : exercice. ◁

On en déduit en particulier la proposition qui suit.

(14-9) Proposition : si f est un morphisme de groupes de G dans G', alors :

1) f(G) est un sous–groupe de G',

2) $f^{-1}(1)$ est un sous–groupe de G.

Définitions : si f est un morphisme de groupes de G dans G' :

- f(G) est appelé l'*image* de f et noté : Imf,
- $f^{-1}(0)$ est appelé le *noyau* de f et noté Ker$f$ [1].

(14-10) Proposition : un morphisme de groupes est injectif si, et seulement si, son noyau est le sous groupe trivial.

Démonstration : la condition est évidemment nécessaire, elle aussi est suffisante car si $f(x) = f(y)$ alors :

$$f(xy^{-1}) = f(x)f(y)^{-1} = 1$$

et xy^{-1} appartient au noyau. Il s'ensuit que si Ker$f = \{1\}$, $x = y$. ◁

---

1 "Ker" comme *kernel* ou *Kern*.

(14-11) Proposition

1) La composition de deux morphismes de groupes donne un morphisme de groupes.

2) Si un morphisme de groupes est bijectif, son application inverse est un morphisme de groupes.

Démonstration : exercice. ◁

Vocabulaire : on dit :

- *isomorphisme* pour morphisme bijectif,
- *endomorphisme* pour morphisme d'un groupe dans lui-même,
- *automorphisme* si les deux conditions précédentes sont remplies.

(14-12) Proposition : l'ensemble des automorphismes d'un groupe G est un groupe. On le note Aut G.

Démonstration : les propositions (14-11) et (14-5) montrent que c'est un sous-groupe de S_G, l'ensemble des permutations de G. ◁

*** Structure de groupe induite**

(14-13) Lemme : étant donné un groupe G et un ensemble E, muni d'une loi de compositon interne, si une application f, de G dans E est **surjective** et telle que :

$$\forall x \in G \ \forall y \in G \ f(xy) = f(x)f(y),$$

elle induit une structure de groupe sur E.

Démonstration : soit x', y' et z' des éléments de E, comme f est surjective, il existe x, y et z appartenant à G tels que :

$$f(x) = x' \ , \ f(y) = y' \ \text{et} \ f(z) = z'.$$

On a toujours :

- $(x'y')z' = (f(x)f(y))f(z) = f(xy)f(z) = f((xy)z)$
  $= f(x(yz)) = f(x)f(yz) = f(x)(f(y)f(z)) = x'(y'z')$
  la loi de E est donc associative ;
- $x'f(1) = f(x)f(1) = f(x1) = f(x) = x'$,
  $f(1)$ est donc élément neutre ;
- $x'f(x^{-1}) = f(x)f(x^{-1}) = f(xx^{-1}) = f(1)$ et de même $f(x^{-1})x' = f(1)$,
  x' admet donc toujours un inverse $f(x^{-1})$.

L'ensemble E est bien un groupe. ◁

§ 15. Générateurs – groupes cycliques

*** Sous-groupe cyclique**

Dans la suite G désignant un groupe quelconque, sa loi est notée multiplicativement.

(15-2) Lemme : soit G et groupe et a l'un de ses éléments, il existe un morphisme α, et un seul, de $\mathbf{Z}$ dans G, tel que :

$$\alpha(1) = a.$$

Démonstration : si un tel morphisme existe, on a :

- si $x \geq 0$, alors $\alpha(x) = \alpha(1 + \ldots + 1) = (\alpha(1))^x = a^x$,
- si $x < 0$, alors $\alpha(x) = \alpha(-(1 + \ldots + 1)) = (a^x)^{-1}$, on note a^{-x}.

Ainsi, α est entièrement déterminé par la donnée de a.

L'application ainsi définie : $x \mapsto a^x$ est effectivement un morphisme si, pour tous entiers x et y, on a :

$$a^{x+y} = a^x a^y.$$

Cette généralisation de la règle de calcul familière, sur les exposants entiers relatifs, se justifie dans les mêmes termes que ceux utilisés pour les nombres. Il n'y a donc pas lieu d'y revenir. ◁

(15-3) Corollaire : si a est un élément du groupe G, l'ensemble :

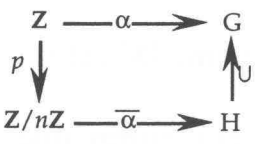
$$H = \{a^k \mid k \in \mathbf{Z}\}$$

est un sous-groupe de G et l'on est devant l'alternative suivante :

- $H \sim \mathbf{Z}$,
- il existe un entier naturel n, tel que : $H = \{1, a, a^2, \ldots, a^{n-1}\}$ et $H \sim \mathbf{Z}/n\mathbf{Z}$.

Démonstration : $H = \{a^k \mid k \in \mathbf{Z}\}$ étant l'image du morphisme α du lemme précédent c'est bien un sous-groupe de G.

- Si $\operatorname{Ker}\alpha = \{0\}$, α est injectif, il induit un isomorphisme entre $\mathbf{Z}$ et son image H.
- Dans le cas contraire il existe un entier n, tel que $\operatorname{Ker}\alpha = n\mathbf{Z}$. On vérifie alors que la bijection canonique de α est un isomorphime. En effet, on sait que pour tout x de $\mathbf{Z}$, on a :



$$\bar{\alpha}(\bar{x}) = \alpha(x) = a.$$

Ainsi, on a toujours :

$$\bar{\alpha}(\overline{x+y}) = \alpha(x+y) = a^{x+y} = a^x a^y = \alpha(x)\,\alpha(y) = \bar{\alpha}(\bar{x})\,\bar{\alpha}(\bar{y}),$$

$\bar{\alpha}$ est donc bien un morphisme bijectif de $\mathbf{Z}_n$ sur H ◁

Définitions : dans les conditions ci-dessus, on dit que H est le *sous-groupe cyclique* de G *engendré* par a, on note alors $H = [a]$. On dit encore que :

- a est d'*ordre infini*, si $[a] \sim \mathbf{Z}$,
- a est d'*ordre n*, si $[a] \sim Z_n$.

N.B. L'ordre de a se caractérise commme le plus petit entier positif n – s'il existe – tel que $a^n = 1$.

Vocabulaire : de façon générale, si G est un groupe fini, on appelle *ordre* de G, le nombre de ses éléments – on le note $|G|$.

*** Groupes cycliques**

Définition : on dit qu'un groupe est *cyclique* ou *monogène*, s'il est engendré par l'un de ses éléments.

Exemples :

- $\mathbf{Z}$ est cyclique engendré par 1 ou –1,
- $\mathbf{Z}/n\mathbf{Z}$ est cyclique engendré par toute classe $\overline{m}$, telle que $\text{pgcd}(m,n)=1$,
- les racines $n^{\text{èmes}}$ complexes de l'unité forment un groupe G qui est cyclique engendré par $e^{i\frac{2\pi}{n}}$.

(15-4) Théorème : tout sous-groupe d'un groupe cyclique est cyclique.

Démonstration : si G est un groupe cyclique, ous avons vu que :

$$G \sim \mathbf{Z} \text{ ou } G \sim \mathbf{Z}/n\mathbf{Z}.$$

On applique les théorème 11-1 et 12-4. ◁

*** Génération d'un sous-groupe**

De façon plus générale, on considère un groupe G et un sous-ensemble X de G. Soit $\mathscr{G}$ l'ensemble des sous-groupes de G qui contiennent X, comme G appartient à $\mathscr{P}$, cet ensemble est non vide. On note :

$$[X]=\bigcap_{H\in\mathscr{G}} H$$

cet ensemble est un sous-groupe de G, il contient X. Il apparaît donc comme étant le plus petit sous-groupe de G qui contient X (1).

Définition : le sous-groupe [X], ainsi défini, est dit *engendré par* X – en précisant au besoin dans G.

(15-5) Proposition :

$$[X]=\{g\in G \mid \exists n\in\mathbf{Z}\ \exists x_1,\dots,x_n\in X\ \exists \alpha_1,\dots,\alpha_n\in\mathbf{Z}\ g=x_1^{\alpha_1}\dots x_n^{\alpha_n}\}.$$

Démonstration : on note provisoirement :

$$H=\{g\in G \mid \exists n\in\mathbf{Z}\ \exists x_1,\dots,x_n\in X\ \exists \alpha_1,\dots,\alpha_n\in\mathbf{Z}\}.$$

Comme [X] est un sous-groupe, il est immédiat que :

$$g=x_1^{\alpha_1}\dots x_n^{\alpha_n}\in[X],$$

ce qui montre que :

$$H\subseteq[X].$$

On vérifie facilement que H est un sous-groupe de G et comme il contient X, on a, par définition :

$$[X]\leq H.$$

L'égalité avancée est alors justifiée. ◁

1 Pour la relation d'inclusion.

§ 16. Actions de groupes

Définition : étant donnés un ensemble E et un groupe G, on dit que G *opère*, ou *agit*, sur E (*à gauche*) s'il existe une loi de composition externe :

$$\begin{array}{ccc} G\times E & \longrightarrow & E \\ (g,x) & \mapsto & gx \end{array}$$

telle que :

(1) $\forall x\in E \;\; 1x=x,$

(2) $\forall g\in G \;\forall h\in G \;\forall x\in E \;\; (hg)x=h(gx).$

(16-1) Proposition : la donnée d'une action de G sur E équivaut à celle d'un morphisme de G dans S_E – le groupe des permutations de E.

Démonstration : une action de G sur E étant donnée, on convient de poser :

$$\forall g\in G \;\; \forall x\in E \;\; f_g(x)=gx.$$

On définit ainsi une application:

$$\begin{array}{ccc} f: G & \longrightarrow & E^E \\ g & \mapsto & f_g \end{array}$$

Si g et h sont deux éléments de G, on a toujours :

$$f_{hg}(x)=(hg)x=h(gx)=(f_h\circ f_g)(x).$$

Il s'ensuit que :

$$\forall g\in G \;\; \forall h\in G \;\; f_{hg}(x)=f_h\circ f_g$$

et comme il est clair que $f_1=\mathrm{Id}_E$, on a :

$$f_{g^{-1}}\circ f_g=\mathrm{Id}_E=f_g\circ f_g^{-1}.$$

Les f_g sont donc toujours des applications bijectives et $g\mapsto f_g$ est un morphisme de G dans S_E.

Réciproquement, considérant un tel morphisme, on pose :

$$gx=f_g(x),$$

alors, on a toujours :

$$1x=f_1(x)=\mathrm{Id}_E(x)=x.$$

et :

$$(hg)x=f_{hg}(x)=(f_h\circ f_g)(x)=h(gx).$$

On a donc bien une action de groupe. ◁

Exemples : les groupes géométriques agissent sur le plan.

(16-2) Proposition : étant donnée une action d'un groupe G sur un ensemble E, la relation définie sur E par :

$$x\,\mathfrak{R}\,y \;\Leftrightarrow\; \exists g\in G \;\; y=gx,$$

est une équivalence.

Démonstration : soit x, y et z des éléments de E, on a toujours :

1) $1x=x$ et donc $x\,\mathfrak{R}\,x$;

2) si $x\,\mathfrak{R}\,y$, il existe un élément g de G tel que $y=gx$ et alors :

$$x=1x=g^{-1}gx=g^{-1}y,$$

on a donc $y\,\mathfrak{R}\,x$;

3) si $x\,\mathfrak{R}\,y$ et $y\,\mathfrak{R}\,z$, il existe des éléments g et h de G tels que $y=gx$ et $z=hy$ et alors :

$$z=hy=hgx=(hg)x,$$

on a donc $x\,\mathfrak{R}\,z$.

Cette relation est symétrique, réflexive et transtive. Il s'agit donc bien une équivalence. ◁

Définitions : dans les conditions ci-dessus, les classes de E suivant $\mathfrak{R}$ sont appelées les *orbites* de E sous l'action de G. Il est commode de noter :

$$Gx = \{y \in E \mid \exists g \in G,\ y = gx\}$$

l'orbite de l'élément x de E, à condition que cette façon de faire ne crée pas d'ambiguité.

(16-3) Théorème : on considère l'action d'un groupe G sur un ensemble fini E. On choisit une famille :

$$x_1, \ldots, x_n$$

de représentants des orbites de E sous l'action de G, alors on a :

$$|E| = |Gx_1| + \ldots + |Gx_n|.$$

Démonstration : cette propriété est immédiate du fait que les classes de l'équivalence $\mathfrak{R}$ forment une partition de E. ◁

*** Génération de S_n**

Soit n un entier, on note S_n le groupe des permutations de $\{1, \ldots, n\}$.

Exemple : une permutation σ est habituellement donnée sous la forme suivante qui parle d'elle même :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 6 & 8 & 2 & 1 & 4 & 7 & 5 & 10 & 9 \end{pmatrix}.$$

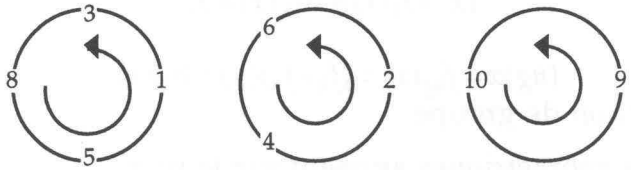
On peut énumérer les images successives d'un même élément on obtient :

$$1 \mapsto 3 \mapsto 8 \mapsto 5 \mapsto 1\ ,\ 2 \mapsto 6 \mapsto 4 \mapsto 2\ ,\ 9 \mapsto 10 \mapsto 9.$$

On constate qu'à chaque fois on retombe sur l'élément de départ et que les éléments $1, \ldots, 10$ se répartissent en quatre sous-ensembles deux à deux disjoints :

$$\{1,3,8,5\}\ ,\ \{2,6,4\}\ ,\ \{7\}\ ,\ \{9,10\},$$

ordonnés de telle sorte que la permutation considérée transforme chaque élément en son suivant – ceci dans un sens élargi où le suivant du dernier est le premier :



Ainsi, on voit σ apparaître comme produit des permutations suivantes :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 2 & 8 & 4 & 1 & 6 & 7 & 5 & 9 & 10 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 6 & 3 & 2 & 5 & 4 & 7 & 8 & 9 & 10 \end{pmatrix}, \cdots$$

qu'il est plus raisonnable – et clair – de présenter sous la forme :

$$(1\,3\,8\,5)\ ,\ (2\,6\,4)\ ,\ (9\,10)\ ,\ (7).$$

La permutation σ s'exprime alors :

$$\sigma = (1\,3\,8\,5)(2\,6\,4)(9\,10).$$

Il est possible d'aller plus loin, en notant que :

$$(1\,3\,8\,5) = (1\,3)(3\,8)(8\,5)$$
$$(2\,6\,4) = (2\,6)(6\,4).$$

Ainsi, on exprime σ comme produit de cyles échangeant deux éléments ou *transpositions* :

$$\sigma = (1\,3)(3\,8)(8\,5)(2\,6)(6\,4)(9\,10).$$

On peut encore ne faire intervenir que des transpositions échangeant deux entiers consécutifs. On a en effet :

- $(1\ 3)=(2\ 3)(1\ 2)(2\ 3)$
- $(3\ 8)=(7\ 8)(6\ 7)(5\ 6)(4\ 5)(3\ 4)(4\ 5)(5\ 6)(6\ 7)(7\ 8)$
- ...

Montrons que ce phénomène a une portée tout à fait générale.

Soit n un entier naturel, on considère le groupe S_n des permutations de $[1,n]$. Soit σ un élément de S_n, la restriction à $\{\sigma\}\times[1,n]$ de l'action de S_n sur $[1,n]$ définit une partition de S_n en orbites. Considérons l'une d'elles qu'on note Ω.

- Si $|\Omega|=1$, alors $\Omega=\{i\}$ et $\sigma(i)=i$;
- Si $|\Omega|=p>1$, alors $\Omega=\{i,\sigma(i),\sigma^2(i),\dots,\sigma^{p-1}(i)\}$ et $\sigma^p(i)=i$.

En effet, dans ce dernier cas, on arrête l'énumération à la première répétition. Si on avait $\sigma^p(i)=\sigma^l(i)$ et $1\le l<p$, ceci entraînerait $\sigma^{p-l}(i)=i$, puis :

$$\Omega=\{i,\sigma(i),\sigma^2(i),\dots,\sigma^{p-l}(i)\},$$

en contradiction avec $|\Omega|=p$.

Posons :

$$i=i_1,\ \sigma(i)=i_2,\ \dots,\ \sigma^{p-1}(i)=i_p.$$

La restriction de σ à Ω est la permutation circulaire :

$$(i_1\ i_2\ \dots\ i_p)$$

qu'il toujours possible considérer comme un élément de S_n en posant :

$$(i_1\ i_2\ \dots\ i_p)=\begin{pmatrix} i_1 & i_2 & \dots & i_{p-1} & i_p & j_1 & j_2 & \dots & j_{n-p} \\ i_2 & i_3 & \dots & i_p & i_1 & j_1 & j_2 & \dots & j_{n-p} \end{pmatrix}$$

Définition : une telle permutation de S_n est appelée *cycle* de support $\{i_1,i_2,\dots,i_p\}$.

À chaque orbite on associe un tel cycle. On définit ainsi :

$$\gamma_1,\gamma_2,\dots,\gamma_r.$$

Pour tout i de $[1,n]$, il existe un cycle γ_j, et un seul, dont le support contient i. Il est tel que :

$$\gamma_j(i)=\sigma(i)\ \text{ et }\ \gamma_k(i)=i\ \text{ si } k\neq j.$$

Ce qui prouve que :

$$\sigma=\gamma_1\gamma_2\dots\gamma_r.$$

Comme ces cycles sont associés aux orbites de l'action du groupe cyclique $[\sigma]$ sur $[1,n]$, il sont définis de façon unique. Leurs supports étant deux à deux disjoints, ils sont permutables. On a donc démontré le théorème qui suit.

(16-4) Théorème : toute permutation de S_n se décompose, de façon unique, en un produit de cycles dont les supports sont deux à deux disjoints. Cette décomposition est unique à l'ordre des facteurs près.

Considérons le cycle $\gamma=(1\ 2\ \dots\ p)$, il est clair que :

$$\gamma=(1\ 2)(2\ 3)\dots(p-1\ p)$$

et plus généralement, que :

$$(i_1\ i_2\ \dots\ i_p)=(i_1\ i_2)(i_2\ i_3)\dots(i_{p-1}\ i_p).$$

Ainsi, toute permutation est un produit de cycles échangeant deux entiers – ou *transpositions*. Résultat qu'on peut énoncer comme suit.

(16-5) Théorème : le groupe S_n est engendré par les transpositions.

Considérons la transposition $\tau = (i\ j)$, en supposant que $i<j$. Il vient :

$$\tau = (j\ \ j-1) \dots (i+2\ \ i+1)(i\ \ i+1)(i+1\ \ i+2) \dots (j-1\ \ j)$$

De façon schématique, on peut décrire les transformations successives d'un même entier par les transpositions de ce produit :

$$\left| \begin{array}{l} i \mapsto i+1 \mapsto i+2 \mapsto \dots \mapsto j-1 \mapsto j \\ j \mapsto j-1 \mapsto j-2 \mapsto \dots \mapsto i+1 \mapsto i \\ k \mapsto k+1 \mapsto k \quad \text{si } i<k<j \end{array} \right.$$

Les autres entiers restant invariants. On a donc démontré l'assertion qui suit.

(16-6) Théorème : le groupe S_n est engendré par les transpositions qui échangent deux entiers consécutifs.

§17. Classes suivant un sous-groupe, groupe quotient

Soit G un groupe et H un de ses sous-groupes, la loi de G se restreint à H×G :

$$\begin{array}{ccc} H \times G & \longrightarrow & G \\ (h, x) & \mapsto & hx \end{array}$$

On définit ainsi une action de H sur G. Les orbites associées sont alors les parties de G de la forme :

$$Hx = \{hx \mid h \in H\}.$$

La relation d'équivalence associée se caractérise alors comme suit :

$$x \,\mathfrak{R}\, y \Leftrightarrow xy^{-1} \in H.$$

Définition : ces orbites sont appelées les *classes* (*à droite*) de G suivant H. Leur ensemble est appelé le *quotient* (*à droite*) de G par H et noté G/H.

Remarque : l'action à droite de H sur G définit les classes à gauche :

$$xH = \{xh \mid h \in H\}$$

et le *quotient à gauche* noté H\G. C'est une notion rarement utilisée.

Définition : si G/H est un ensemble fini, |G/H| est appelé *l'indice* de H *dans* G.

*** Application aux groupes finis**

(17-1) Théorème : si G est un groupe fini et H un sous-groupe de G, alors on a :

$$|G| = |H| \,.\, |G/H|.$$

Démonstration : il est clair que l'application :

$$\begin{array}{ccc} H & \longrightarrow & Hx \\ h & \mapsto & hx \end{array}$$

est bijective. Si H est fini, toutes les classes de G/H ont le même nombre d'éléments que H. Comme elles forment une partition de G, on a bien :

$$|G| = |H| \,.\, |G/H|. \qquad \lhd$$

(17-2) Corollaire : si G est un groupe fini, l'ordre de tout sous-groupe de G divise |G|. En particulier, l'ordre de tout élément de G divise |G|.

Remarque : la dernière affirmation s'utilise couramment sous la forme suivante /

$$a \in G \text{ et } |G| = n \Rightarrow a^n = I.$$

(17-3) Corollaire : tout groupe d'ordre premier est cyclique.

Démonstration : soit G est un groupe d'ordre premier, si a appartient à G, on a :

$$|[a]| = |G| \text{ OU } |[a]| = 1.$$

Ainsi, tout élément de G, autre que 1, engendre G. $\lhd$

*** Groupe quotient**

(17-3)Proposition : soit f un morphisme de groupes de G dans G', de noyau H, on a :

$$\forall g \in G \ \ \forall x \in H \ \ gxg^{-1} \in H.$$

Démonstration : si g et x appartiennent respectivement à G et H, comme H est le noyau de f, on a :

$$f(gxg^{-1}) = f(g)f(x)f(g^{-1}) = f(g)f(x)f(g)^{-1} = f(g)1f(g)^{-1} = 1.$$

On a donc bien $gxg^{-1} \in H$. ◁

Vocabulaire : gxg^{-1} s'appelle le *conjugué* de h par g.

Définition : soit G un groupe et H un de ses sous-groupes, on dit que H est *normal* ou *distingué* dans G si :

$$\forall g \in G \ \ \forall x \in H \ \ gxg^{-1} \in H.$$

Exercice : vérifier que cette condition est équivalente à $G/H = H\backslash G$, c'est-à-dire :

$$\forall g \in G \ \ Hg = gH.$$

Question : soit G un groupe et H un de ses sous-groupes, à quelle condition la surjection canonique p, de G sur G/H induit-elle une structure de groupe sur le quotient G/H ?

Si tel est le cas, p est un morphisme de groupes et l'on doit avoir :

$$1 = p(1) = H1 = H,$$

de sorte que :

$$\mathrm{Ker}\, p = p^{-1}(1) = p^{-1}(H) = H.$$

Une condition nécessaire est donc que H soit un sous-groupe normal de G.

Réciproquement, considérons un sous-groupe normal H de G, soit x, x', y, y' des éléments de G. Si l'on a :

$$p(x) = p(x') \ \text{ et } \ p(y) = p(y'),$$

alors :

$$x'x^{-1} \in H \ \text{ et } \ y'y^{-1} \in H$$

et comme H est normal dans G, il vient :

$$x'y'(xy)^{-1} = x'y'y^{-1}x^{-1} = x'x^{-1}(x(y'y^{-1})x^{-1}) \in H.$$

On a donc :

$$p(x'y') = p(xy).$$

La surjection canonique p induit donc une loi de composition interne sur G/H :

$$(xH)(yH) = (xyH).$$

Nous avons vérifié (cf. 14-13) que G/H est alors un groupe.

(16-4) Théorème : soit G un groupe, si H est un sous-groupe normal de G, G/H est un groupe pour la loi définie par la relation :

$$(xH)(yH) = (xy)H.$$

*** Le théorème d'homomorphisme**

Soit f un morphisme de groupes, de G dans G', la relation $\mathfrak{R}$ associée à f est telle que :

$$x \mathfrak{R} y \Leftrightarrow f(x)=f(y) \Leftrightarrow f(xy^{-1})=1 \Leftrightarrow xy^{-1} \in \ker f.$$

Cette relation donc celle qui définit les classes suivant le noyau de f. La surjection canonique s'exprime donc

$$\begin{array}{rccc} p : & G & \longrightarrow & G/\mathrm{Ker}f \\ & x & \mapsto & (\mathrm{Ker}f)x \end{array}$$

Comme le noyau de f est un sous-groupe normal dans G, nous savons que p est un morphisme de groupes. Comme l'image de f est un sous-groupe de G', l'injection canonique est aussi un morphisme de groupes. Il reste à examiner le cas de la bijection canonique.

Soit $\bar{f}$ cette application, si x et y sont des éléments de G, on a toujours :

$$\bar{f}[(x\mathrm{H})(y\mathrm{H})] = \bar{f}(xy\mathrm{H}) = f(xy) = f(x)f(y) = \bar{f}(x\mathrm{H})\,\bar{f}(y\mathrm{H}),$$

$\bar{f}$ est donc effectivement un morphisme de groupes. Nous avons donc prouvé le théorème qui suit.

(17-5) Théorème d'homorphisme

Si f est un morphisme de groupes défini sur G, on a toujours :

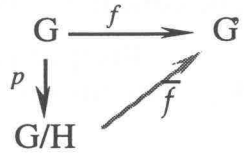
$$\mathrm{Im}f \sim G/\mathrm{Ker}f.$$

*** Morphisme induit sur un quotient**

(17-6) Théorème : soit f un morphisme de groupes de G dans G', H un sous-groupe normal de G ; si $H \subseteq \ker f$, il existe un morphisme, $\bar{f}$ et un seul, de G/H dans G', tel que :

$$\bar{f} \circ p = f,$$

où p désigne le morphisme canonique de G sur G/H.



Démonstration : soit $\bar{f}$ une telle application, si x est un élément de G, on doit avoir :

$$\bar{f}(x\mathrm{H}) = \bar{f} \circ p(x) = f(x).$$

Cette relation détermine $\bar{f}$, il reste à vérifier qu'elle définit bien un morphisme.

Soit x et y appartenant à G, comme :

$$(p(x)=p(y) \Leftrightarrow xy^{-1} \in \mathrm{H}) \text{ et } (\mathrm{H} \subseteq \ker f),$$

alors :

$$p(x)=p(y) \Rightarrow f(x)=f(y).$$

La relation précédente :

$$\bar{f}(x\mathrm{H}) = \bar{f} \circ p(x) = f(x)$$

définit bien une application. De plus, on a :

$$\bar{f}((x\mathrm{H})(y\mathrm{H})) = \bar{f}(xy\mathrm{H}) = f(xy) = f(x)f(y) = \bar{f}(x\mathrm{H})\,\bar{f}(y\mathrm{H}),$$

$\bar{f}$ est donc le morphisme annoncé. ◁