INFORMATION MATHEMATIQUE

7

IREM
MARSEILLE

IREM marseille
institut de recherche
sur l'enseignement des **mathématiques**

70, route léon lachamp
13009 marseille luminy

Tél. **41.39.40 - 41.15.40**

INFORMATION

MATHEMATIQUE

Publication de l'I.R.E.M. de Marseille

RESPONSABLE DE LA PUBLICATION

J.C. Beniamino

INSTITUT DE RECHERCHE
SUR L'ENSEIGNEMENT DES MATHEMATIQUES

I. R. E. M.
70, Route Léon Lachamp
13009 - MARSEILLE

(Tél. 41.15.40 poste 32.10 / 41.39.40)

INFORMATION MATHEMATIQUE

N° 7

SEPTEMBRE 1975

SOMMAIRE

E D I T O R I A L

GROUPE DE TRAVAIL MATHEMATIQUE-PHYSIQUE

Une soixantaine de Professeurs des deux disciplines travailleront dès la rentrée scolaire 1975-1976, sur tous les problèmes relatifs à la coordination, au développement et à l'actualisation de ces deux enseignements

Il est prévu de faire fonctionner trois Centres : DIGNE, AIX EN PROVENCE, MARSEILLE . Dans chaque Centre une équipe d'animation s'efforcera de coordonner les diverses activités et de donner les impulsions nécessaires à la bonne marche du travail .

Ont été retenus les thèmes suivants :

- Lois linéaires .
- Forces, Vecteurs .
- Grandeur repérable, grandeur mesurable .
- Orientation de l'espace .
- Propagation et fonctions périodiques .
- Automatisme et Algèbre de Boole .
- Dérivation .

La première séance a été prévue le 24 Septembre 1975 , au LYCEE SAINT CHARLES, 45 Bd.Camille Flammarion, MARSEILLE à 14 h.30 .

Nous souhaitons à tous une bonne rentrée et une fructueuse année scolaire .

J.C. BENIAMINO

QUELQUES REFLEXIONS INSPIREES PAR LE COLLOQUE DE MONTPELLIER SUR L'ENSEIGNEMENT DES MATHEMATIQUES DANS LES C.E.T.

* * *

Robert ROLLAND - Directeur de l'I.R.E.M. de Marseille

Les 10, 11, 12 Avril 1975 a eu lieu à MONTPELLIER un colloque inter-IREM sur l'enseignement des mathématiques dans les C.E.T. Cette rencontre, organisée par l'I.R.E.M. de MONTPELLIER regroupait en majorité des Professeurs de C.E.T. (enseignement général et enseignement professionnel), mais aussi des Professeurs de Lycées classiques et techniques, et de l'enseignement supérieur .

Il ne m'est pas possible de citer tous les problèmes qui ont été soulevés lors de ces journées ; je voudrais simplement en reprendre quelques uns qui me semblent importants et qui pourraient être éventuellement objet d'études et d'expériences pour les groupes C.E.T. qui vont fonctionner cette année à l'I.R.E.M.

Un des problèmes les plus importants est le suivant : dans l'état actuel des choses, les élèves ressentent l'orientation vers un C.E.T. comme un échec ; d'autre part, on leur propose au C.E.T. un enseignement de type très proche de celui dans lequel ils n'ont pas réussi au Lycée ou au C.E.S. Il s'en suit un désintéressement quasi général pour les activités scolaires, même souvent en ce qui concerne l'enseignement professionnel .

Bien entendu si on peut résoudre un tel problème, ce ne peut être que par une modification profonde du système éducatif ; néanmoins on peut sans doute améliorer la situation par l'emploi de moyens techniques bien choisis : machines à calculer de toutes sortes, mini-ordinateurs, magnétoscopes, rétroprojecteurs etc ... et bien sûr tout gadget que l'on pourra imaginer .

Certaines de ces techniques demandent une formation préalable solide des professeurs : je pense ici par exemple à l'usage des mini-ordinateurs ou des magnétoscopes . Ce sera une des activités de l'I.R.E.M. que de fournir

cette formation . Une autre activité sera évidemment de mettre au point diverses manières d'utiliser ces techniques avec les élèves .

Les contenus de l'enseignement des mathématiques et les façons de les exposer posent aussi des problèmes très délicats, d'autant qu'il faut en outre concilier des tendances qui semblent parfois contradictoires, surtout quand on ne dispose que d'un horaire réduit : le point de vue culturel et le point de vue utilitaire (utilisation des mathématiques comme outil dans l'enseignement professionnel) . A ce propos j'ai constaté, et cela me semble assez grave, que dans l'esprit de beaucoup d'enseignants il existe les deux types de mathématiques suivants : "Mathématiques traditionnelles" , "Mathématiques modernes" . Cette idée est d'ailleurs entretenue par les sujets d'examens puisque certains sujets de C.A.P. ou de B.E.P. comportent deux épreuves au choix : l'une de mathématiques dites "traditionnelles", l'autre de mathématiques dites "modernisées" . Il y a là, à mon avis, une grande confusion entre le fond et la forme ; pour le fond on peut dire que l'évolution continuelle des mathématiques apporte parfois plus qu'un simple ajout à l'échaffaudage existant des mathématiques ; souvent en effet cette évolution bouleverse et restructure les rapports entre les divers concepts . Or chaque notion n'est vraiment bien saisie que par les différents liens par lesquels on peut la relier à l'échaffaudage général des mathématiques . Il ne faut donc pas s'étonner que certaines notions qui étaient à l'honneur s'avèrent dans l'état actuel des mathématiques de peu de portée, tandis que d'autres (tout aussi anciennes) prennent une dimension nouvelle et apparaissent comme des rouages importants . Quant à la forme, (c'est à dire le langage), c'est sans doute elle qui pose le problème le plus délicat à résoudrre . Souvent dans la résolution d'un problème de mathématiques, une bonne part du travail consiste à trouver un langage adapté ; il n'est donc pas étonnant que le langage ait évolué de la façon que nous connaissons . Mais ce langage qui s'est élaboré au contact de problèmes
élémentaire de nos classes . (J'ai vu des corrigés de problèmes de C.A.P. rendus incompréhensibles par un abus de formalisation au niveau du langage) . Il faut donc trouver un juste milieu et cela pourrait constituer une part du travail de certains groupes I.R.E.M.

Une dernière remarque enfin : l'évolution que l'on connait, n'a jamais impliqué la disparition de l'intuition que l'on voit dans certains manuels scolaires et par voie de conséquence dans certains cours

(absence de figures, d'exemples concrets, etc...) , ni celle de certaines techniques actuellement indispensables .

Comme on le voit, ne serait ce que sur les quelques problèmes que l'on a posés, il y a beaucoup de travail à faire ; je pense qu'une véritable formation des maîtres passe par un tel travail et pas seulement par un recyclage des connaissances mathématiques .

HISTOIRE DE LA RESOLUTION DES EQUATIONS ALGEBRIQUES

* * *

Madame C.BLANCHARD - Faculté des Sciences Saint-Charles

Nous exposerons essentiellement l'historique des deux théories achevées : résolution des systèmes d'équations linéaires et résolution par radicaux des équations algébriques à une variable de degré > 1 .

I - EQUATIONS LINEAIRES .

Leur calcul a été abordé dès l'Antiquité la plus reculée : on résout des équations linéaires dès qu'on fait des divisions, et elles sont à l'origine de l'introduction des fractions . Des règles pratiques de calcul linéaire, telles que "règle de trois" ou "règle de fausse position" se retrouvent dans les manuels d'arithmétique depuis les papyrus égyptiens en passant par les mathématiciens hindous, arabes ou européens du Moyen-Age .

Les Babyloniens savaient déjà résoudre de façon élégante les systèmes d'équations du premier degré . Jusqu'au XVIIIème siècle , cependant, les théories de résolution des sytèmes linéaires se ramènent à l'énoncé de règles, déjà connues de DIOPHANTE d'Alexandrie au IVème siècle, sur le passage des termes d'un membre dans un autre, et l'élimination des inconnues pour n'en avoir plus qu'une . On ne considère que des systèmes a autant d'équations que d'inconnues, les premiers membres étant implicitement supposés linéairement indépendants : le problème est considéré comme mal posé s'il n'en est pas ainsi, c'est à dire si l'élimination se fait mal .

Les progrès dûs aux Mathématiciens du XVIIIème siècle et du début du XIXème consistent essentiellement en l'adoption d'une notation qui permet d'écrire les systèmes de n équations à n inconnues, et en l'introduction des déterminants, progrès déjà amorcés, mais seulement ébauchés et non publiés, par LEIBNIZ (1646-1716) .

C'est l'étude des formes quadratiques et bilinéaires qui va conduire au XIXème siècle à la résolution générale des systèmes d'équations linéaires, problème que n'avait pu élucider JACOBI (1804-1851), faute d'avoir perçu la notion de rang. Le problème, tout en ayant des motivations géométriques, est abordé par voie arithmétique, avec la résolution en nombres entiers des systèmes linéaires à coefficients entiers. Ce problème est résolu dans un cas particulier par HERMITE (1822-1901) ; puis dans sa généralité par H J SMITH vers 1860. Cependant, KRONECKER (1823-1891) avait institué à l'Université de Berlin un vaste programme de recherches, auquel participait également WEIERSTRASS, visant à reconstruire toutes les Mathématiques à partir des calculs sur les nombres entiers. Dans le cadre de ce programme FROBENIUS retrouva en 1878 les résultats de SMITH, puis KRONECKER donna leur forme définitive aux théorèmes sur les systèmes linéaires à coefficients réels ou complexes, mais laissa à ses disciples le soin de formuler ces résultats. C'est FROBENIUS qui introduit le mot rang. Ces résultats étaient élucidés à la même époque par LEWIS CARROLL.

La notion de déterminant utilisée pour la résolution des systèmes linéaires avait pris corps, d'une manière d'abord empirique, à propos du problème linéaire posé par la recherche d'une courbe de forme donnée passant par des points donnés, avec CRAMER (1750) et BEZOUT (1779). Elle fut définitivement mise au point, et ses propriétés furent développées, par CAUCHY (1789-1857) et JACOBI, tandis que GRASSMANN en développait le calcul, KRONECKER et WEIERSTRASS en donnaient finalement la définition axiomatique utilisée aujourd'hui.

II - EQUATIONS ALGEBRIQUES DE DEGRE >1 A UNE VARIABLE.

La difficulté à résoudre une équation de degré >1, provenant du fait que les calculs ne sont plus rationnels, a été perçue depuis l'Antiquité. Déjà les Babyloniens ont su ramener à la seule extraction de racines carrées la résolution d'équations quadratiques et bicarrées. Les Grecs se borneront à retrouver leurs formules en termes géométriques. On n'en retrouve trace sous forme algébrique qu'avec HERON (100 ap. J.C) et DIOPHANTE.

1/ - La Résolution par radicaux.

La théorie des équations quadratiques et bicarrées se perfectionna durant tout le Moyen-Age et on s'orienta alors vers une recherche

de résolution par radicaux des équations de degré ≥ 3 . EUCLIDE (IIIème siècle av. J.C) avait étudié un certain nombre d'expressions faisant intervenir des radicaux carrés . LEONARD DE PISE (1170-1230) reconnut que ces expressions ne pouvaient suffire à résoudre l'équation du 3ème degré et s'essaya à des calculs analogues sur les racines cubiques .

Ce sont les mathématiciens hindous et arabes, dont LEONARD DE PISE introduisit les travaux en Occident, qui avaient doté les radicaux de symboles de plus en plus maniables, considérant leur calcul comme aussi fondamental que celui des autres opérations algébriques .

On sait que c'est seulement au début du XVIème siècle que SCIPION DEL FERRO donna une formule de résolution par radicaux de $x^3 + ax = b$, formule qui amena CARDAN (1501-1576) et ses élèves à calculer sur les racines carrées de nombres négatifs, alors que les nombres négatifs eux-mêmes étaient encore regardés avec méfiance par beaucoup de mathématiciens. C'est BOMBELLI, élève de CARDAN qui, le premier, donna explicitement des règles de calcul sur les nombres complexes . FERRARI, autre élève de CARDAN, avait donné en 1545 un procédé pour résoudre par radicaux l'équation générale du 4ème degré à l'aide d'une équation auxiliaire du 3ème degré .

Jusqu'au XVIIIème siècle, on ne fait guère que développer les idées précédentes avec plus ou moins de bonheur . Ainsi, un ami de LEIBNIZ crut avoir résolu par radicaux l'équation générale du 5ème degré, grâce à des réductions faisant disparaître les termes de degré intermédiaire . Seule faille, vite perçue par LEIBNIZ, ces réductions font intervenir des équations de degré > 5 .

2/ - Le Théorème fondamental de l'algèbre .

Cependant VIETE (1540-1603) avait exprimé les relations entre les coefficients et les racines d'une équation algébrique, du moins quand les racines sont toutes positives . En 1620, A.GIRARD affirme sans démonstration qu'une équation de degré n a exactement n racines en comptant les "racines impossibles" et chacune avec son ordre de multiplicité , notion que l'on commence à percevoir, ces racines satisfaisant aux relations trouvées par VIETE . Il est aussi le premier à donner les "formules de NEWTON" donnant les sommes de puissances semblables des racines, jusqu'à l'exposant 4 .

L'intégration des fractions rationnelles, effectuée par LEIBNIZ et JOHANN BERNOULLI (1667-1748), ranime l'intérêt porté à la possibilité de décomposer un polynôme en facteurs du premier degré annoncée par GIRARD, qui devient bientôt le "théorème fondamental de l'algèbre".

Le calcul sur les nombres complexes est encore assez balbutiant LEIBNIZ semble considérer qu'on ne peut décomposer $x^4 + 1$ en produit de deux facteurs du 2^{nd} degré à coefficients réels ! Cependant, dès le début du XVIIIème siècle, MOIVRE, ayant ramené la résolution de $x^n - 1 = 0$ à la division du cercle en n parties égales, se restreint ainsi au cas où n est premier impair, et constate pour les petites valeurs de n qu'on peut se ramener, en posant $y = x + \frac{1}{x}$, à la résolution "par radicaux" d'une équation de degré $\frac{n-1}{2}$.

Mais des tentatives (par EULER en particulier) de résolution générale par radicaux des équations algébriques ayant échoué, on commence à chercher des démonstrations a priori du théorème fondamental. Les idées, fort peu rigoureusement justifiées au départ, qui président à ces dernières recherches sont celles qui conduiront par la suite à la notion d'adjonction formelle de racines : on part du principe (sans doute déjà sous-jacent chez GIRARD) qu'un polynôme de degré n à n "racines idéales" sur lesquelles on peut raisonner comme sur des nombres en particulier quant à leurs relations avec les coefficients du polynôme ; le problème est alors de montrer que l'une au moins de ces racines est un nombre complexe. Reprenant les idées encore très vagues émises par EULER (1707-1783) dans ce sens, LAGRANGE (1736-1813) donne enfin en 1772 une démonstration satisfaisante du "théorème fondamental". Cependant GAUSS (1777-1855) critiqua cette démonstration, trouvant en l'adjonction de racines une notion fructueuse peut-être mais encore trop peu clairement explicitée, et finit par donner en 1797 une démonstration remarquablement claire et concise, où la seule propriété "topologique" des nombres réels qu'on utilise (propriété plutôt liée à la structure ordonnée comme on le remarqua vite) est le fait qu'un polynôme réel de degré impair a au moins une racine réelle.

Cependant d'ALEMBERT (1717-1783) avait attaché son nom au théorème pour avoir en 1746 donné la première amorce de démonstration rigoureuse, fondée sur d'autres considérations. Il utilise la représentation

géométrique des nombres complexes à laquelle GAUSS donnera toute sa rigueur et toute son importance, mais que l'on cherchait à utiliser depuis la fin du XVIIème siècle : remarquant que les points (a,b) du plan tels que $a + ib$ soit racine de $P(X + iY) = A(X,Y) + iB(X,Y)$, sont les points d'intersection éventuels des courbes $A(X,Y) = 0$ et $B(X,Y) = 0$, il étudie cette intersection par des considérations topologiques évidemment très intuitives .

3/ - La théorie de Galois .

En 1770, s'amorcent par deux mémoires, l'un de LAGRANGE, l'autre de VANDERMONDE, les recherches qui aboutiront à la théorie de Galois . Ils parlent tous deux de l'ambiguïté qu'introduit la pluralité des déterminations de radicaux dans les formules de résolution des équations de degré 3 ou 4 . EULER avait déjà montré comment associer entre elles les déterminations des différents radicaux dans la formule de SCIPION DEL FERRO de façon à n'obtenir que 3 racines distinctes . Reprenant les formules de résolution des équations de degré 3 ou 4, LAGRANGE met en évidence des fonctions des racines qui ne prennent qu'un petit nombre de valeurs distinctes quand on permute les racines de façon quelconque : par exemple, si x_1, x_2, x_3 sont les trois racines d'une équation du 3ème degré, et si w est une racine cubique de 1 dans $\mathbb{C}$, $(x_1 + w x_2 + w^2 x_3)^3$ ne peut prendre que 2 valeurs distinctes pour toute permutation des racines, ce qui permet de voir le véritable principe de la résolution de l'équation du 3ème degré . Cela le conduit à étudier en général, pour un polynôme de degré n, le nombre de valeurs que peut prendre une fonction rationnelle des n racines quand on permute ces racines et à trouver à ce sujet des résultats fragmentaires de ce qui sera la théorie de Galois . Cherchant toujours les formules générales pour la résolution des équations algébriques, il introduit les "résolvantes de LAGRANGE" qui permettent de systématiser la résolution de l'équation du 4ème degré, mais n'ont guère d'intérêt pratique général au-delà .

VANDERMONDE avait mené parallèlement des recherches analogues, avec des résultats sensiblement moins clairs et moins généraux, mais avait été plus loin dans l'application des résolvantes de LAGRANGE, considérant l'équation $X^n - 1 = 0$ pour n premier impair et affirmant, malheureusement sans le démontrer de façon générale, que les résolvantes sont racines $m^{\text{ièmes}}$ de rationnels pour $m = \frac{n-1}{2}$. C'est GAUSS qui vers 1800 élucide complètement la résolution par radicaux des polynômes

"cyclotomiques" $\varphi_n(X) = \frac{X^n - 1}{X - 1}$ pour n premier impair, montrant en particulier la possibilité de construire "à la règle et au compas", le polygone régulier à n côtés, si n est premier de la forme $2^{2^k} + 1$. Signalons aussi que c'est à cette époque qu'un élève de LAGRANGE montre enfin, par des raisonnements d'ailleurs obscurs et incomplets sur les groupes de Galois avant la lettre, l'impossibilité de résoudre par radicaux l'équation générale du 5ème degré .

C'est GALOIS (1811-1832) qui met en 1832 un point final à la théorie dont ABEL, interrompu par la mort en 1829, avait sans doute perçu bien des aspects . C'est d'abord GALOIS qui précise clairement les notions d'appartenance d'une quantité à un corps donné (sans d'ailleurs se préoccuper de la structure abstraite de corps), d'adjonction d'éléments à un corps, et de polynôme irréductible sur un corps donné, le vague de ces notions ayant beaucoup nui jusque là à la clarté des énoncés, et même des idées . Après avoir démontré que le corps de décomposition L d'un polynôme F sans racines multiples à coefficients dans K peut être engendré sur K par adjonction d'un seul élément α dont les racines $x_1, \ldots, x_n$ de F sont fonctions rationnelles (il s'agit évidemment de caractéristique 0) , il définit le "groupe de Galois" Γ de L sur K , ou de F, comme l'ensemble des permutations des x_i obtenues en substituant, dans leurs expressions, à α l'un de ses conjugués . Il montre ensuite que si L contient un corps intermédiaire L_1 , corps de décomposition sur K d'un autre polynôme, le groupe de Galois de L sur L_1 est un sous-groupe distingué de Γ , notion qu'il introduit à cette occasion . Cela le conduit au critère général de résolubilité d'une équation par radicaux : $F(X) = 0$ est résoluble par radicaux si et seulement si le groupe de Galois Γ de F est résoluble, c'est à dire si et seulement s'il existe une chaîne de sous-groupes : $\Gamma_0 = \Gamma \supset \Gamma_1 \supset \ldots \supset \Gamma_k = \{e\}$ où chaque Γ_i est sous-groupe distingué de Γ_{i-1} , et ou chaque quotient Γ_{i-1}/Γ_i est cyclique . La démonstration de la partie réciproque est effectuée par GALOIS au moyen des résolvantes de LAGRANGE .

III - EQUATIONS ALGEBRIQUES GENERALE .

L'étude des systèmes d'équations algébriques de degré quelconque à plusieurs variables est à la base de la géométrie algébrique . Les grecs déjà ramenaient souvent la résolution de problèmes algébriques à l'intersectic

de deux courbes planes auxiliaires convenablement choisies, méthode encore utilisée par d'ALEMBERT dans sa tentative pour démontrer le théorème fondamental .

Rappelons que c'est à FERMAT avant DESCARTES, que revient l'idée de la classification des courbes suivant leur degré . Cela permet de supposer que FERMAT avait perçu l'invariance du degré des courbes par changement de coordonnées, invariance qui ne fut clairement mise en relief que par EULER .

Nous n'entreprendrons pas ici l'histoire de la géométrie algébrique branche des mathématiques qui n'a connu son plein épanouissement qu'au XXème siècle et qui est encore aujourd'hui en pleine effervescence .

Comme exemple de résultat historique, mentionnons le fameux théorème de BEZOUT (1730-1783) : deux courbes algébriques planes sans composante commune de degrés respectifs n et p ont au plus n.p points d'intersection (c'est à dire que le système formé par deux équations algébriques à deux variables de degrés respectifs n et p a au plus n.p solutions). Ainsi formulé, le théorème est valable sur n'importe quel corps commutatif . On peut remplacer le "ou plus" par "exactement" à condition de remplacer le plan affine par le plan projectif, d'exiger que le corps de base soit algébriquement clos, et de compter chaque point "avec sa multiplicité" (notion qui n'a été complètement élucidée en termes algébriques qu'assez récemment) .

Nous donnerons davantage de détails historiques sur la résolution des systèmes généraux d'équations algébriques, dans le cas particulier où les équations sont à coefficients entiers et où on en cherche des solutions entières.

IV - EQUATIONS DIOPHANTIENNES .

La recherche des solutions en nombres entiers des systèmes d'équations algébriques à coefficients entiers est appelée résolution d'équations diophantiennes . Les solutions cherchées n'existent en général que dans le cas de systèmes indéterminés sur $\mathbb{Q}$, systèmes auxquels s'est précisément intéressé DIOPHANTE . On lui doit en particulier la résolution en nombres entiers de l'équation $X^2 + Y^2 = Z^2$.

Cependant les chinois du haut Moyen-Age, sans doute motivés par la confection des calendriers, ont donné une règle de résolution de congruences linéaires simultanées (la formulation actuelle de telles règles est toujours appelée théorème chinois d'approximation) . Vers la même époque, les hindous, également motivés par des problèmes astronomiques, savaient traiter méthodiquement les systèmes d'équations diophantiennes linéaires à un nombre quelconque d'inconnues par application de l'algorithme d'EUCLIDE , tandis qu'ils avaient été les premiers, vers 400 avant J.C. , à aborder des équations du 2ème degré du type qui sera dit " de PELL-FERMAT" : $Y^2 - N X^2 = 1$, avec N entier positif .

L'étude de cette équation, sujet d'un problème posé par FERMAT, appelée "De PELL" par suite d'une erreur d'EULER, et de ses généralisations, a occupé assez longtemps les mathématiciens, et stimulé l'étude des approximations rationnelles des irrationnelles algébriques . La solution générale de l'équation $Y^2 - N X^2 = 1$ a été donnée par DIRICHLET en 1854 .

On ne peut dresser ici un tableau systématique des équations diophantiennes ayant fait l'objet de recherches plus ou moins célèbres . La plupart conduisent à des problèmes encore ouverts aujourd'hui (c'est le cas des généralisations de l'équation de PELL-FERMAT) et on ne peut guère dégager de méthodes générales de résolution .

A titre d'exemple particulièrement illustre, rappelons brièvement l'histoire de l'équation de FERMAT $X^n + Y^n = Z^n$, dont on doute fort que FERMAT ait réellement prouvé la non-résolubilité en nombres entiers pour $n > 2$. Rappelons que les solutions pour $n = 2$ étaient déjà connues de DIOPHANTE . FERMAT lui-même a prouvé l'impossibilité pour $n = 4$, tandis qu'EULER l'a prouvé pour $n = 3$. Ce dernier croyait avoir trouvé une démonstration générale de l'impossibilité, au prix d'une erreur dont l'analyse allait se révéler très fructueuse pour le développement de l'algèbre, puisqu'elle aboutissait à l'introduction par KUMMER de la notion d'idéal vers 1850 . Vers cette époque l'Académie des Sciences offrit un prix de 300 francs-or à qui montrerait l'impossibilité de résoudre $X^n + Y^n + Z^n = 0$ en nombres entiers relatifs pour n premier impair (énoncé équivalent à l'hypothèse de FERMAT) . Personne n'y étant arrivé, c'est KUMMER qui eut le prix, pour avoir fourni la contribution la plus décisive par un critère prouvant que l'équation de FERMAT n'a pas de solutions entières si n ne divise le numérateur d'aucun des $\frac{n-3}{2}$

premiers nombres de BERNOULLI (pour $n < 100$, seuls 37, 59 et 67 échappent à ce critère) .

Aucune étape décisive n'a été franchie depuis, malgré un certain nombre de démonstrations fausses données chaque année, et aussi des contributions non négligeables à la résolution du problème, en particulier des preuves de l'impossibilité pour un grand nombre d'exposant . On ignore en particulier si les différents critères connus de non-résolubilité s'appliquent à une infinité de nombres premiers . Certains mathématiciens se demandent si la réponse au problème de l'Académie des Sciences n'est pas logiquement indécidable .

Mettant en jeu plusieurs variables, les équations diophantiennes se rattachent naturellement à la géométrie algébrique dont elles ont contribué à stimuler le renouveau, et sont maintenant étudiées sous l'angle " recherche de points rationnels sur des courbes algébriques". On doit aussi au mathématicien anglais WORDELL des théorèmes fondamentaux sur les points rationnels sur les courbes du genre 1 (dont l'exemple le plus simple est constitué par les cubiques sans point multiple) .

ETUDE GENERALE DU GROUPE LINEAIRE DE V

J.C.BENIAMINO - I.R.E.M. d'Aix-Marseille

1. GENERALITES SUR LES HYPER-PLANS :

dim $V = n$ sur un corps k commutatif .
$GL_n(k)$ est l'ensemble des applications linéaires de V dans lui-même qui sont bijectives - $\sigma \in GL_n(k) \Leftrightarrow \ker \sigma = \{0\}$.

On appelle hyper-plan dans V un sous-espace vectoriel de V de dimention $n-1$. On désigne par $\hat{V}$ le dual de V (l'ensemble des formes linéaires) $\hat{V}$ est un espace vectoriel de dimension n .

Soit φ $\varphi \in \hat{V}$ $\ker \varphi = \{x, x \in V, \varphi(x) = 0\}$
$\ker \varphi$ est un sous-espace vectoriel de dimension $(n-1)$ dans V .

Inversement, soit H un hyper-plan quelconque et B un vecteur $B \in V-H$ on peut noter que $V = B \oplus H$ et soit φ définie par les conditions : φ est linéaire et $\varphi(B) = 1$; $\forall X$, $X \in V$ $X = \lambda B + Y$ où $Y \in H$. $\varphi(X) = \lambda \varphi(B) = \lambda$. φ définie de cette manière est une forme linéaire dont le noyau est l'hyper-plan H . On constate donc qu'il est possible de définir une infinité de telles formes φ ce qui nous amène à étudier le problème suivant : étant donné deux formes φ et ψ qui ont le même noyau, quelle relation existe-t-il entre φ et ψ .

Soit H ce noyau et $B \in V-H$ on peut toujours écrire $\varphi(B) = 1$ et $\psi(B) = c$ $(c \in k)$ $\forall X$, $X \in V$ $X = \lambda B + Y$ car $V = B \oplus H$.

On a donc $\varphi(X) = \lambda$ et $\psi(X) = \lambda c$

Soit le résultat $\forall X$, $X \in V$ $\psi(X) = c\,\varphi(X)$
ou encore $\psi = c\,\varphi$.

2. DEFINITION DES TRANSVECTIONS .

H un hyper-plan et $\varphi \in \hat{V}$ tel que $\ker \varphi = H$.
Cherchons les applications linéaires de V dans lui-même laissant H invariant vecteur à vecteur et telles que $\varphi \circ \sigma = \varphi$ $(\sigma \in GL_n(k))$.

Soit $B \in V-H$ tel que $\varphi(B) = a \neq 0$.
le vecteur $X - a^{-1} \varphi(X) B$ est un vecteur de H quel que soit X dans V
Si donc σ est l'une des applications ci-dessus, on a :

$$\sigma(X) - a^{-1} \varphi(X) \sigma(B) = X - a^{-1} \varphi(X) B$$

Soit $\sigma(X) = X + a^{-1} \varphi(X) (\sigma(B) - B)$
le vecteur $\sigma(B) - B$ est un vecteur de H grâce à la condition $\varphi \circ \sigma = \varphi$.
on pose

$$A = a^{-1} (\sigma(B) - B) \qquad A \text{ vecteur fixe de } H$$

d'où $\sigma(X) = X + \varphi(X) A \qquad \forall X , X \in V \qquad (1)$.

Inversement, considérons une application σ définie par une relation du type (1) , σ est évidemment linéaire et on la note τ_A .
Un calcul simple du noyau montre que σ_A est une injection, donc un élément de $GL_n(k)$.
$\ker \sigma_A = \{X, X \in V / X + \varphi(X) A = 0\}$ en distinguant deux cas $X \in H$ et $X \notin H$ on établit que $\ker \sigma_A = \{0\}$.

On a les propriétés :

1/ $\forall X , X \in H \qquad \sigma_A (X) = X$

2/ $\sigma_A \circ \sigma_B = \sigma_{A+B}$ quand A et B sont deux vecteurs du même hyper-plan H .

3. RAPPELS D'ALGEBRE .

G étant un groupe quelconque, on dit que deux éléments a et b sont conjugués dans G . S'il existe g, $g \in G$ tel que $a = g\, b\, g^{-1}$ $(b = g^{-1} a\, g)$. Ceci n'a évidemment d'intérêt que dans un groupe qui n'est pas commutatif .

Cette relation entre éléments de G est une relation d'équivalence dont les classes sont appelées : classes de conjugaison .

Commutateur de deux éléments a,b est l'élément $ab\,a^{-1}\,b^{-1}$ dans G . Soit H un sous groupe de G contenant les commutateurs, alors on peut écrire :

$$\forall x\ ,\ x \in G\ ,\ \forall h\ ,\ h \in H \qquad xh = xh\,x^{-1}\,h^{-1}\,hx \quad .$$

Soit donc $xh \in Hx$ et encore $xH \subset Hx$ et de même bien sûr $xH \supset Hx$ on a donc pour un tel sous groupe $xH\,x^{-1} = H$ on dit que H est distingué .

On peut alors munir l'ensemble quotient $G/_H$ d'une structure de groupe et l'application canonique $G \longrightarrow G/_H$ qui est un homomorphisme de groupe a pour noyau H .

$G/_H$ est alors un groupe abélien .

En effet, le produit $xH\ yH = xy\ H$ de deux classes s'écrit aussi :
$\forall\ h\ ,\ h \in H \qquad xyh = yx\ (x^{-1}\ y^{-1}\ xyh)$ et $h' = x^{-1}\ y^{-1}\ xyh \in H$
d'où $xy\ H \subset yx\ H$ et vice versa d'où $xy\ H = yx\ H$.

On appelle groupe des commutateurs dans G , le plus petit sous groupe de G contenant tous les commutateurs (ou encore le groupe engendré par les commutateurs, c'est à dire l'ensemble des produits finis de commutateur) . Si G' désigne ce sous groupe, $G/_{G'}$ est un groupe abélien .

A étant une partie de G , on appelle centralisateur de A l'ensemble des éléments de G, tels que $\forall\ x\ ,\ x \in A$ $gx = xg$ on le note C_A . Si $A = G$, on note C_G et on appelle ceci le centre de G .

C_A et C_G sont des sous groupes de G . C_G est commutatif et distingué .

4. ETUDE DES TRANSFORMATIONS LINEAIRES DE DETERMINANT 1 .

V est ramené à une base $(E_1 \ldots E_n)$ quelconque et la valeur du déterminant d'une application Φ ($\Phi \in GL_n(k)$) ne dépend pas du choix de la base .

On désigne par $B_{ij}(\lambda)$ la matrice déduite de la matrice unité, en écrivant λ à la place de zéro en position (i,j) avec $i \neq j$. Il est facile de constater que $B_{ij}(\lambda)$ est la matrice d'une transvection par rapport à l'hyper-plan $(E_1 \dots E_{j-1}\ E_{j+1} \dots E_n)$ déterminé par la forme φ définie par :

$$\varphi(x) = x_j \quad \text{si} \quad x = x_1 E_1 + \dots + x_n E_n \quad \text{et de direction} \quad \lambda E i .$$

A désignant une matrice quelconque $A.B_{ij}(\lambda)$ revient à remplacer A par une matrice dont la $j^{ème}$ colonne est la somme de la $j^{ème}$ colonne de A et de la $i^{ème}$ colonne de A multipliée par λ. De la même manière, $B_{ij}(\lambda).A$ revient à remplacer A par une matrice dont le $i^{ème}$ ligne est la somme de la $i^{ème}$ ligne de A et de sa $j^{ème}$ ligne multipliée par λ.

Soit donc A avec $\det A = 1$ et A diagonale.
$a_{11} \dots a_{nn} = 1$.

$$\begin{pmatrix} a_{11} & 0 & \cdots \\ 0 & a_{22} & 0 \cdots \\ | & & \end{pmatrix} \xrightarrow{①} \begin{pmatrix} a_{11} & \cdots \\ a_{11} & a_{22} \cdots \\ | & | \end{pmatrix} \xrightarrow{②} \begin{pmatrix} 1 & (a_{11}^{-1} - 1)\, a_{22} \cdots \\ a_{11} & a_{22} \cdots \\ | & | \end{pmatrix}$$

$$\xrightarrow{③} \begin{pmatrix} 1 & (a_{11}^{-1} - 1)\, a_{22} \cdots \\ 0 & a_{22} - (1 - a_{11})\, a_{22} \cdots \\ | & | \end{pmatrix} = \begin{pmatrix} 1 & (a_{11}^{-1} - 1)\, a_{22} \cdots \\ 0 & a_{11}\ a_{22} \cdots \\ | & \end{pmatrix} = \begin{pmatrix} 1 & \alpha_{12} \cdots \\ | & \alpha_{22} \cdots \\ | & \alpha_{nn} \end{pmatrix}$$

① on ajoute la première ligne à la seconde ;

② on ajoute à la première ligne le produit par $(a_{11}^{-1} - 1)$ de la seconde ;

③ on ajoute à la seconde ligne le produit par a_{11} de la première.

①, ②, ③ sont des opérations du type $B_{ij}(\lambda)$ la matrice finale obtenue

contient 1 et des zéros en première colonne , seuls sont non nuls les éléments diagonaux et l'élément en position (2,1) si $a_{11} \neq 1$.

Si α_{12} n'est pas nul on multiplie la première colonne par α_{12}^{-1} et on l'ajoute à la seconde colonne, ce qui fournit une matrice

$$\begin{pmatrix} 1 & & \\ & \alpha_{22} & \\ & & \alpha_{nn} \end{pmatrix}$$

diagonale, dont le premier terme est égal à 1 .

On peut donc poursuivre ce procédé jusqu'à l'obtention de la matrice unité .

Théorème : Si A est tel que $\det A = 1$ A étant diagonale , A est le produit de matrices du type $B_{ij}(\lambda)$.

Considérons une application g bijective de V sur V qui transforme la base $E_1 \ldots E_n$ en une nouvelle base $B_1 \ldots B_n$.

On peut écrire $B_1 = \alpha_1 E_1 + \ldots + \alpha_n E_n$ si $\alpha_1 \neq 0$ on peut écrire $E_1 - \lambda_1 B_1$ est un élément de l'hyper-plan $E_2 \ldots E_n$. On considère alors la transvection définie par cet hyper-plan, de direction $E_1 - \lambda_1 B_1$, et de forme φ déterminée par la condition $\varphi(E_1) = -1$

$$\tau(X) = X + \varphi(X)\,(E_1 - \lambda_1 B_1)$$

$$\tau(E_1) = E_1 - (E - \lambda_1 B_1) = \lambda_1 B_1$$

τ est donc une bijection qui transforme la base $(E_1 \ldots E_n)$ en la base $(\lambda_1 B_1, E_2, \ldots, E_n)$. On peut écrire alors :

$B_2 = \alpha_1 (\lambda_1 B_1) + \alpha_2 E_2 + \ldots + \alpha_n E_n$ avec un α_i $i \geq 2$ non nul .

On peut dire par exemple que $E_2 - \lambda_2 B_2$ est un élément de l'hyper-plan $(B_1, E_3, \ldots E_n)$ défini par la forme φ $\varphi(E_2) = -1$.

$\tau(X) = X + \varphi(X)\,(E_2 - \lambda_2 B_2)$ transforme E_2 en $\lambda_2 B_2$ etc...

On peut trouver une suite de transvections qui transforment la base

$E_1 \ldots E_n$ en la base $(\lambda_1 B_1 \ldots \lambda_n B_n)$ $\quad T_1 \ldots T_n = \sigma$ étant le produit de ces transvections, on peut noter :

$$\begin{array}{ccc} (E_1 \ldots E_n) & \xrightarrow{\ \sigma\ } & (\lambda_1 B_1 ; \ldots ; \lambda_n B_n) \\ & \searrow^{g} \quad \nearrow_{\varphi} & \\ & (B_1 ; \ldots ; B_n) & \end{array}$$

φ étant une transformation bijective de matrice diagonale dans la base $(B_1 \ldots B_n)$. Comme $\det \sigma = 1$, si $\det g = 1$ Il vient $\det \varphi = 1$ Si A est la matrice de φ dans la base $(B_1 \ldots B_n)$ A se ramène à l'identité après multiplication par des matrices $B_{ij}(\lambda)$ qui sont des matrices de transvection .

Théorème : Si g est une transformation linéaire telle que $\det g = 1$, g peut s'écrire sous forme d'un produit de transvections .

5. GROUPE DES COMMUTATEURS DE $GL_n(k)$.

On désigne par $T_n(k)$ l'ensemble des transvections et par $SL_n(k)$ le sous groupe de $GL_n(k)$ engendré par $T_n(k)$.

Soit $\sigma_A \in T_n(k)$ et $\tau \in GL_n(k)$ H étant l'hyper-plan de la transvection σ_A , l'étude de $\tau^{-1} \sigma_A \tau$ conduit à :

$$\forall X, X \in V \qquad \tau^{-1} \sigma_A \tau(X) = X + \varphi(\tau(X))\, \tau^{-1}(A) .$$

Si H' est l'hyper-plan $\tau^{-1}(H)$ d'équation $\varphi(\tau(X)) = 0$

$\tau^{-1} \circ \sigma_A \circ \tau$ est la transvection d'hyper-plan H' , de direction $B = \tau^{-1}(A)$.

Inversement, étant donné deux transvections σ_A et σ_B d'hyper-plan H_1 et H_2 , on peut trouver de plusieurs manières un automorphisme τ tel que $\tau(H_1) = H_2$ et $\tau(A) = B$. On peut même en plus avoir $\det \tau = 1$. Dans ce dernier cas on peut écrire $\sigma_A = \tau^{-1} \circ \sigma_B \circ \tau$.

On peut donc conclure que l'ensemble $T_n(k)$ est contenu dans une seule classe de conjugaison par rapport au groupe $SL_n(k)$.

Si $n = 2$ l'hyper-plan et la direction de la transvection coïncident ; l'ensemble des transvections de direction D et l'ensemble des transvections de direction D' sont alors conjugués dans $SL_2(k)$.

C désigne le groupe des commutateurs de $GL_n(k)$.

Considérons l'application $\varphi \; GL_n(k) \longrightarrow GL_n(k)/_C$.
σ_1 et σ_2 étant deux transvections, il vient $\sigma_1 = \tau^{-1} \sigma_2 \tau$
$\varphi(\sigma_1) = \varphi(\tau)^{-1} \; \varphi(\sigma_2) \; \varphi(\tau) = \varphi(\sigma_2)$ car $GL_n(k)/_C$ est commutatif .
toutes les transvections ont donc même image par φ .

Comme $\varphi(\sigma^2) = \varphi(\sigma^2) = \varphi(\sigma)$ quand σ est une transvection on a $\varphi(\sigma) = 1$. Donc les transvections $T_n(k)$ forment une partie de C ou encore $SL_n(k) \subset C$.

Considérons l'application $\Delta : GL_n(k) \longrightarrow k^*$ $\Delta(\sigma) = \det \sigma$.
on désigne par $\Delta^{-1}(\{1\})$ le noyau de cet homomorphisme de groupe .
On a l'inclusion $C \subset \Delta^{-1}(\{1\}$ car l'image par Δ d'un commutateur est l'élément unité .

$$\text{donc} \quad SL_n(k) \subset C \subset \Delta^{-1}(\{1\}) .$$

Comme on a montré plus haut que $\Delta^{-1}(\{1\}) \subset SL_n(k)$

$$\text{on a donc} \quad SL_n(k) = C = \Delta^{-1}(\{1\}) .$$

ce qui permet une double caractérisation du groupe des commutateurs de $GL_n(k)$.

Théorème : Le groupe des commutateurs de $GL_n(k)$ est le noyau de l'application déterminant, c'est aussi le groupe engendré par les transvections $T_n(k)$.

6. CENTRE DE $GL_n(k)$.

Le centraliseur de $SL_n(k)$ est l'ensemble des éléments de $GL_n(k)$ qui commutent avec tous les éléments de $SL_n(k)$, donc en particulier tous ceux de $T_n(k)$.

Soit donc g un élément du centralisateur et σ_A une transvection quelconque

$$g \circ \sigma_A = \sigma_A \circ g \qquad \text{d'où} \quad g(A) = \sigma_A(g(A)) \ .$$

Si φ désigne la forme linéaire associée à σ_A on a $\varphi(g(A)) = 0$ et donc $g(A)$ est dans l'hyper-plan servant à la définition de σ_A . Toujours avec le même vecteur A on peut envisager H' avec $H \cap H' = D_A$ et σ'_A la nouvelle transvection ; $g(A)$ sera dans l'hyper-plan H' et donc $g(A) \in H \cap H'$ ou encore $g(D_A) = D_A$ un élément du centralisateur laisse donc globalement invariantes les droites vectorielles .

Désignons par $(e_1 \ldots . e_n)$ une base de V

$g(e_1) = \lambda_1 e_1 \ldots . g(e_n) = \lambda_n e_n$.

$$g(e_1 + e_2) = k e_1 + k e_2 = \lambda_1 e_1 + \lambda_2 e_2 \qquad \lambda_1 = \lambda_2 = k$$

g est donc une homothétie de $GL_n(k)$.

L'inverse étant vrai : une homothétie laisse les droites vectorielles globalement invariantes .

Désignons par $\mathcal{H}_n(k)$ le groupe des homothéties dont on rappelle qu'il est commutatif et inclu dans le centre du groupe $GL_n(k)$.

Z étant le centre de $GL_n(k)$ on a donc $\mathcal{H}_n(k) \subset Z$ et aussi

$Z \subset$ centralisateur de $SL_n(k) \subset \mathcal{H}_n(k)$.

On a donc $\mathcal{H}_n(k)$ = Centralisateur de $SL_n(k)$ dans $GL_n(k)$.

$\mathcal{H}_n(k)$ étant le centre de $GL_n(k)$.

Le centre de $SL_n(k)$ est donc formé des homothéties vectorielles de rapport λ tel que $\lambda^n = 1$.

Théorème . Le groupe des homothéties $\mathcal{Z}_n(k)$ est le centre de $GL_n(k)$ c'est aussi le centralisateur dans $GL_n(k)$ de $SL_n(k)$.

INITIATION A L'ETUDE DES RELATIONS SUR UN ENSEMBLE FINI

Jean MARION - I.R.E.M. d'Aix-Marseille

INTRODUCTION

La modestie du titre de cet article n'est qu'apparente . Aussi bien les problèmes de recherche opérationnelle que la cybernétique, en passant par la sociométrie et les arts décoratifs, relèvent du traitement, de l'analyse de relations sur un ensemble fini ; si nous nous plaçons du point de vue, non plus de l'utilisateur mais du formateur, de l'enseignant, le fait d'évoluer sur des ensembles finis permet une expérimentation immédiatement accessible ; cette expérimentation favorise l'intuition, la recherche du contre-exemple, l'analyse de la cause de non-validité d'une solution initialement prévue au problème posé, etc .

C'est pourquoi cet aspect des "mathématiques du fini" , qui consiste en l'analyse des systèmes relationnels sur un ensemble fini, a un pouvoir formateur essentiel .

Paradoxalement, dans nos enseignements, seul l'aspect combinatoire des "mathématiques du fini" est abordé .

Cet exposé se veut tout d'abord une initiation à quelques outils de traitement des relations binaires sur ensemble fini, et ensuite voudrait être un facteur déclenchant des réflexions sur ce que l'on pourrait faire dans ce domaine, en suscitant des groupes de travail qui mettraient au point des projets qui seraient expérimentés dans des classes et qui analyseraient ensuite les résultats obtenus .

§1 - DE LA DEFINITION D'UNE RELATION

Soit S un ensemble fini non vide ; une définition qui donne toute satisfaction aux mathématiciens est la suivante : se donner une relation R sur S, c'est se donner un sous-ensemble G de SxS, R étant définie à partir de G par : $xRy \Leftrightarrow (x,y) \in G$.

Pratiquement, une relation sur S n'apparaît jamais comme cela, y compris dans des modèles abstraits.

1er exemple :

Soit S = {Marseille, Paris, Montélimar, Lille, Lyon}.
Pour 2 villes x et y de S, décidons que "x a une expansion démographique comparable à celle de y si le taux d'augmentation de population de x et le taux d'augmentation de population de y diffèrent de moins de 1 % en 1974".

Sous réserve que la notion de taux d'expansion ait été définie et évaluée, on peut décider sans ambiguïté si oui ou non Paris R Marseille, R étant représentée par le groupe verbal : " a une expansion démographique comparable à celle de".

Nous avons là une relation, définie par un groupe verbal, qui définit une structure que nous appellerons objective sur S.

2ème exemple :

Soit S un ensemble d'individus que l'on doit répartir en plusieurs équipes de commandos. Afin de constituer des équipes solidement cohérentes, on pose à chaque $x \in S$ la question : "avez-vous confiance en y ?" (y étant un autre élément de S), et convenons de noter xRy si et seulement si x a répondu qu'il avait confiance en y.

Nous avons là un exemple d'une relation déterminant une structure empirique. Alors que dans le 1er exemple, on peut affirmer à priori que si xRy alors yRx, il n'en est plus de même dans le 2ème exemple.

Toutefois, diverses expériences montrent que les individus attribuent aux relations définies par des groupes verbaux tels que : "a confiance en", "trouve sympathique", la propriété de symétrie.

Les relations de choix, de préférence, mettent en évidence un phénomène curieux, comme le montre le 3ème exemple ci-après.

3ème exemple :

Monsieur X décide de se marier ; 3 filles : F_1, F_2, F_3 sont candidates, mais M. X, qui connaît bien ces 3 filles est embarassé pour choisir celle qu'il préfère. Pour décider de son choix, il considère 5 critères pour chacune des filles : le degré de beauté, le degré d'intelligence, le degré de fortune, le degré de qualités sportives, le degré de qualités amoureuses.
Il décide qu'il préfèrera la fille F à la fille F', si F est supérieure à F' en au moins 3 des 5 critères. Or, il trouve que :

F_1 $\begin{bmatrix}\text{plus belle}\\ \text{plus intelligente}\\ \text{plus fortunée}\end{bmatrix}$ que F_2, que :

F_2 est $\begin{bmatrix}\text{plus amoureuse}\\ \text{plus sportive}\\ \text{plus belle}\end{bmatrix}$ que F_3, et que :

F_3 est $\begin{bmatrix}\text{plus amoureuse}\\ \text{plus intelligente}\\ \text{plus fortunée}\end{bmatrix}$ que F_1.

Il préfère donc F_1 à F_2, F_2 à F_3 et F_3 à F_1 !

Laissons notre candidat au mariage se débattre dans son problème ; ses ennuis résultent du fait qu'aux relations associées à un groupe verbal du type "est préférée à" on attribue en général la propriété de transitivité, ce qui risque de ne pas se produire si les critères du choix sont multiples ; notre candidat au mariage a fait connaissance avec ce que l'on appelle un triangle d'intransitivité : $F_1 R F_2$, $F_2 R F_3$ et $F_3 R F_1$, connu par les sociologues sous le nom de "phénomène Condorcet".

4ème exemple :

Reprenons l'ensemble S = {Paris, Marseille, Montélimar, Lille, Lyon} de l'exemple 1, et soit R la relation sur S définie par le groupe verbal : "a même initiale que".

Nous avons, comme en 1, une relation définie à partir d'une structure objective. Toutefois l'expérience montre que si l'on demande à quelqu'un, possédant la langue française, mais non habitué aux manuels de 6ème, 5ème, etc. de nos lycées, quels sont les éléments de S qui sont en relation avec Lille (par la relation R) il répondra "il n'y a que l'élément Lyon". Autrement dit la réflexivité n'est pas perçue dans la formulation de la relation.

Il semble bien que la réflexivité :

a) a peu d'importance pratique ;
b) n'est en général pas perçue ;
c) est ajoutée pour des commodités mathématiques ;

elle est perçue par exemple dans la relation "divise" sur un ensemble d'entiers naturels, elle n'est pas perçue dans une relation associée à un groupe verbal du type : "a même ... que".

De tout ceci retenons que :

1) En général, le groupe verbal utilisé pour "définir" une relation doit être accompagné d'un environnement (consensus, ou conventions précisés) lorsque cette relation est introduite à priori (structures objectives) de manière à ce que toute propriété de cette relation puisse être détectée.

2) Lorsqu'il s'agit d'une relation existante dans un socius donné, le contenu intuitif de la formulation de cette relation n'est pas nécessairement reflété dans l'observation des résultats (cf. : effet d'intransitivité de l'exemple 3).

Nous supposerons dans tout ce qui suit le problème de la définition d'une relation résolu, pour nous attacher au problème de la description et de l'analyse d'une relation. Nous laisserons de côté la description "graphique" d'une relation, qui est celle traditionnellement utilisée, pour utiliser la description matricielle.

§2 - REPRESENTATION MATRICIELLE D'UNE RELATION

A - L'ALGEBRE $Z_2^{[n]}$

Notons Z_2 l'ensemble des entiers modulo 2, qui est un corps pour l'addition définie par la table :

$Z_2 = \{0, 1\}$

+	0	1
0	0	1
1	1	0

et pour la multiplication définie par la table :

×	0	1
0	0	0
1	0	1

Soit $n \geq 1$ un entier naturel et soit $Z_2^{[n]}$ l'ensemble des tableaux à n lignes et n colonnes d'éléments de Z_2. Si $M \in Z_2^{[n]}$ on note $m_{i,j}$ l'élément situé à la $i^{ème}$ ligne et à la $j^{ième}$ colonne.

Soit M de terme général $m_{i,j}$, M' de terme général $m'_{i,j}$, on note $M + M'$ le tableau de terme général $(m_{i,j} + m'_{i,j})$ et $M \times M'$ le tableau de terme général $\mu_{i,j} = \sum_{s=1}^{s=n} m_{i,s}\, m'_{s,j}$.

Proposition 1 : $(Z_2^{[n]}, +, \times)$ est un anneau dit : anneau des matrices booléennes d'ordre n.

Preuve : facile, nous en laissons le soin à nos lecteurs. c. q. f. d.

Les lois + et × ne sont peut être pas celles qui ont le plus d'intérêt pour étudier les relations :

Soit $M = (m_{i,j})$ et $M' = (m_{i,j})$ deux matrices booléennes ; on note $M * M'$ la matrice booléenne de terme général $\mu_{i,j}$ telle que :

$\mu_{i,j} = 1 \Leftrightarrow \exists m'_{i,k} = 1$ et $m'_{k,j} = 1$, et 0 sinon.

Exercice 1 :

a) la loi * est-elle commutative ?

b) la loi * est-elle associative ?

c) la loi * admet-elle un élément neutre ?

d) tout élément de $Z_2^{[n]}$ a-t-il un inverse pour cette loi ?

Enfin, pour $M = (m_{i,j})$ et $M'(m'_{i,j})$ notons MVM' la matrice de terme général $(\mu_{i,j})$ telle que :

$$\mu_{i,j} = 1 \Leftrightarrow m_{i,j} = 1 \quad \text{ou} \quad m'_{i,j} = 1$$
$$= 0 \Leftrightarrow m_{i,j} = m'_{i,j} = 0$$

V est également une loi de composition interne sur $Z_2^{[n]}$

Exercice 2 : a) la loi V est-elle : 1) commutative ?
2) associative ?
b) V a-t-elle un élément neutre ?
c) la loi $*$ est-elle distributive par rapport à la loi V ?

B - BASE POUR UN ENSEMBLE FINI

Soit S un ensemble fini non vide, de cardinal n, et soit $I_n = \{1, 2, 3, \ldots, n\}$. Si σ est une bijection de I_n sur S le n-uplet $b = (\sigma_1, \sigma_2, \ldots, \sigma_n)$ où $\sigma_i = \sigma(i)$ $(1 \leq i \leq n)$ est appelé une base de S.

Remarquons qu'il y a donc autant de bases de S que de permutations sur S, c'est-à-dire $n!$.

Soit alors R(S) l'ensemble des relations binaires sur S, $b = (\sigma_1, \sigma_2, \ldots, \sigma_n)$ une base de S et soit $\mathcal{R} \in R(S)$; on associe à $\mathcal{R}$ la matrice $m_b(\mathcal{R})$ de terme général $m_{i,j}$, définie de la manière suivante :

$$m_{i,j} = \begin{cases} 1 \Leftrightarrow \sigma_i \mathcal{R} \sigma_j, \\ 0 \text{ sinon.} \end{cases}$$

Proposition 2 : L'application $m_b : R(S) \to Z_2^{[n]}$ qui à $\mathcal{R} \in R(S)$ fait correspondre $m_b(\mathcal{R})$ est une bijection.

Preuve : La participation active du lecteur à cet article ne peut être mieux réalisée, qu'en laissant au dit lecteur le soin d'établir la démonstration. c.q.f.d.

5ème exemple :

Soit $S = \{2, 4, 7, 11, 14, 28\}$ et $\mathcal{R}$ la relation sur S définie par par le groupe verbal : "est un multiple de". Prenons $b = (2, 4, 7, 11, 14, 28)$ comme base ; on a :

$$m_b(\mathcal{R}) = \begin{bmatrix} 1&0&0&0&0&0 \\ 1&1&0&0&0&0 \\ 0&0&1&0&0&0 \\ 0&0&0&1&0&0 \\ 1&0&1&0&1&0 \\ 1&1&1&0&1&1 \end{bmatrix}$$

C - REPRESENTATION MATRICIELLE D'UNE RELATION

Définition : Soit $\mathcal{R} \in R(S)$, b une base de S, alors $m_b(\mathcal{R})$ est appelée la représentation matricielle de $\mathcal{R}$ dans la base b.

Cela étant pour chaque indice i $(1 \leq i \leq n)$ notons $\Gamma_i = \{\sigma_j \in S / \sigma_i \mathcal{R} \sigma_j\}$; alors il est clair que :

Proposition 3 : Soit $m_{i,j}$ le terme général de $M = m_b(\mathcal{R})$ alors $\sigma_j \in \Gamma_i \Leftrightarrow m_{i,j} = 1$.

Cela étant, soit $m_i = (m_{i,1}, m_{i,2}, \ldots, m_{i,n})$ la $i^{ème}$ ligne de M et faisons la agir sur b de la manière suivante : on considère le "produit scalaire" :

$$(m_{i,1}, m_{i,2}, \ldots, m_{i,n}) \begin{pmatrix} \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_n \end{pmatrix} = (m_{i,1}.\sigma_1, m_{i,2}.\sigma_2, \ldots, m_{i,n}.\sigma_n)$$

puis on supprime les termes $m_{i,j}.\sigma_j$ pour lesquels $m_{i,j} = 0$ et si $m_{i,j} = 1$ on note $m_{i,j}.\sigma_j = \sigma_j$; l'action de m_i sur b donne donc les σ_j tels que $m_{i,j} = 1$, c'est-à-dire exactement Γ_i. Faisant cela pour chaque indice i, on voit que M opère sur la base b pour donner chacun des Γ_i, opération qui

se traduit formellement comme l'action de la matrice d'un endomorphisme d'un espace vectoriel sur un vecteur de cet espace vectoriel, par :

$$\begin{bmatrix} m_{1,1}, m_{1,2}, \ldots, m_{1,n} \\ m_{2,1}, m_{2,2}, \ldots, m_{2,n} \\ \vdots \\ m_{i,1}, m_{i,2}, \ldots, m_{i,n} \\ \vdots \\ m_{n,1}, m_{n,2}, \ldots, m_{n,n} \end{bmatrix} \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_i \\ \vdots \\ \sigma_n \end{bmatrix} = \begin{bmatrix} \Gamma_1 \\ \Gamma_2 \\ \vdots \\ \Gamma_i \\ \vdots \\ \Gamma_n \end{bmatrix}$$

Reprenant les données de l'exemple 5, on obtient ainsi :

$$\begin{bmatrix} 1\,0\,0\,0\,0\,0 \\ 1\,1\,0\,0\,0\,0 \\ 0\,0\,1\,0\,0\,0 \\ 0\,0\,0\,1\,0\,0 \\ 1\,0\,1\,0\,1\,0 \\ 1\,1\,1\,0\,1\,1 \end{bmatrix} \begin{bmatrix} 2 \\ 4 \\ 7 \\ 11 \\ 14 \\ 28 \end{bmatrix} = \begin{bmatrix} \{2\} \\ \{2,4\} \\ \{7\} \\ \{11\} \\ \{2,7,14\} \\ \{2,4,7,14,28\} \end{bmatrix}$$

Ici Γ_i est l'ensemble des éléments de S dont σ_i est multiple.

Nous faisons encore appel à la participation active du lecteur pour établir la :

Proposition 4 :

Soit $b = (\sigma_1, \sigma_2, \ldots, \sigma_n)$ une base de S, $\mathcal{R}$ une relation sur S. Alors, si $(m_{i,j})$ est la matrice de $\mathcal{R}$ dans b :

(a) $\mathcal{R}$ est réflexive $\Leftrightarrow m_{i,i}=1 \quad \forall i = 1, 2, \ldots, n.$

(b) $\mathcal{R}$ est symétrique $\Leftrightarrow m_{i,j}=m_{j,i} \quad (1 \leq i, j \leq n)$

(c) $\mathcal{R}$ est antisymétrique $\Leftrightarrow [m_{i,j} \times m_{j,i}=1 \Rightarrow i=j]$

(d) $\mathcal{R}$ est transitive $\Leftrightarrow [m_{i,j} \times m_{j,k}=1 \Rightarrow m_{i,k}=1]$

et la :

Proposition 5 :

Soit $b=(\sigma_1, \sigma_2, \ldots, \sigma_n)$ une base de S ;

$\mathcal{R}$ est une valeur d'équivalence $\Leftrightarrow$

a) $\forall i \quad \sigma_i \in \Gamma_i$

b) $\Gamma_1 \cup \Gamma_2 \cup \ldots \cup \Gamma_n = S$

c) $\Gamma_i \cap \Gamma_j \neq \emptyset \Rightarrow \Gamma_i = \Gamma_j$

Remarquons que Γ_i est alors précisément la classe d'équivalence de σ_i.

§3 - MATRICE D'UNE APPLICATION

Soit $b = (\sigma_1, \sigma_2, \ldots, \sigma_n)$ une base de S, $\mathcal{R}$ une relation sur S ; $\mathcal{R}$ est une application de S dans S $\Leftrightarrow$ $\forall \sigma_i \in S$ il existe un élément et un seul σ_j, qu'on note $\mathcal{R}(\sigma_i)$ tel que $\sigma_i \mathcal{R} \sigma_j$ $\Leftrightarrow$ pour chaque i $(1 \leq i \leq n)$ il existe un seul j $(1 \leq j \leq n)$ tel que $m_{i,j}=1$. On a alors $\Gamma(\sigma_i) = \{\sigma_j\} = \mathcal{R}(\sigma_i)$.

Proposition 6 :

1) $\mathcal{R}$ est une application $\Leftrightarrow$ $m(\mathcal{R})$ a un seul élément non nul dans chaque ligne.

2) si $\mathcal{R}$ est une application $\Leftrightarrow$ $\Gamma_i = \mathcal{R}(\sigma_i)$

Considérons alors le cas plus particulier des applications bijectives f de S sur S, qu'on appelle permutations de S.

Soit f injective : si $\sigma_j = f(\sigma_i) = f(\sigma_{i'})$ alors $\sigma_i = \sigma_{i'}$ et donc $i = i'$; la traduction matricielle en est :

$$m_{i,j} = m_{i',j} = 1 \quad \Rightarrow \quad i = i' ;$$

Il y a donc un seul 1 par colonne; comme il y a un seul 1 par ligne et par colonne, soit alors $\sigma_k \in S$, il existe un seul 1 dans la $k^{ième}$ colonne ; soit i le rang de l'unique ligne dont le 1 se trouve dans la $k^{ième}$ colonne : $m_{i,k} = 1$ donc $\sigma_k = f(\sigma_i)$ et σ_i est unique, donc f est surjective et injective. On a finalement démontré que :

Proposition 7 :

Soit f une relation sur S fini ; alors f est une bijection $\Leftrightarrow$ f injective $\Leftrightarrow$ f surjective $\Leftrightarrow$ la matrice de f dans une base quelconque de S a un seul 1 par ligne et par colonne.

5ème exemple :

Soit $S = \{1, 2, 3, 4\}$ et $M = \begin{bmatrix} 0&1&0&0 \\ 1&0&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \end{bmatrix}$ matrice d'une permutation de S dans la base (1, 2, 3, 4) ; on a :

$$\begin{bmatrix} 0&1&0&0 \\ 1&0&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \\ 4 \\ 3 \end{bmatrix}$$

donc M est la matrice de la permutation $\downarrow \begin{matrix} 1&2&3&4 \\ 2&1&4&3 \end{matrix}$ qui permute 1 et 2, et 3 et 4, donc c'est le produit de transpositions: (1,2)(3, 4).

Exercice 3 : Soit $b = (1, 2, \ldots, n)$ une base de $S = \{1, 2, \ldots, n\}$;

a) Ecrire dans la base b la matrice de la transposition (i, j).

b) Ecrire la matrice de la permutation circulaire $i \to i+1$ $(1 \leq i \leq n-1)$ et $n \to 1$.

§4 - MATRICE DE LA COMPOSEE DE 2 RELATIONS

Soient $\mathcal{R}$ et $\mathcal{R}'$ deux relations binaires sur S ; on appelle composée de $\mathcal{R}$ par $\mathcal{R}'$ la relation binaire notée $\mathcal{R}.\mathcal{R}'$ définie de la manière suivante :

$x \mathcal{R}.\mathcal{R}' y \Leftrightarrow \exists z \in S$ tel que $x \mathcal{R}' z$ et $z \mathcal{R} y$.

Soit alors $b = (\sigma_1, \sigma_2, \ldots, \sigma_n)$ une base de S, $(m_{i,j})$ la matrice $m_b(\mathcal{R})$, $(m'_{i,j})$ la matrice $m_b(\mathcal{R}')$ et $(\mu_{i,j})$ la matrice $m_b(\mathcal{R}.\mathcal{R}')$; par définition de $\mathcal{R}.\mathcal{R}'$ on a :

$\mu_{i,j} = 1 \Leftrightarrow \sigma_i \mathcal{R}.\mathcal{R}' \sigma_j \Leftrightarrow \exists \sigma_k$ tel que $\sigma_i \mathcal{R}' \sigma_k$ et $\sigma_k \mathcal{R} \sigma_j$.

$\Leftrightarrow \exists k$ tel que $m'_{i,k} = 1$ et $m_{k,j} = 1$.

$\Leftrightarrow m_b(\mathcal{R}.\mathcal{R}') = m_b(\mathcal{R}) * m_b(\mathcal{R}')$.

On a donc démontré la :

Proposition 8 : $m_b(\mathcal{R} \circ \mathcal{R}') = m_b(\mathcal{R}) * m_b(\mathcal{R}')$.

On peut se poser la question de savoir quand le produit ordinaire de matrices coïncide avec la loi $*$.

Proposition 9 : Soit f une application de S dans S, $\mathcal{R}$ une relation sur S ; alors :

$$m_b(f \circ \mathcal{R}) = m_b(f).\, m_b(\mathcal{R}).$$

Preuve : Les lignes de $m_b(f)$ n'ont qu'un seul élément non nul ; soit alors $\mu_{i,j}$ l'élément situé à $i^{ème}$ ligne et la $j^{ième}$ colonne de $m_b(f \circ \mathcal{R}) = m_b(f) * m_b(\mathcal{R})$; on a $\mu_{i,j} = 1 \Leftrightarrow \exists \sigma_k$ tel que $\sigma_k = f(\sigma_i)$ et $\sigma_k \mathcal{R} \sigma_j \Leftrightarrow (m_b(f))_{i,k} = 1$ (et c'est le seul élément de la $i^{ème}$ ligne de $m_b(f)$ non nul) et $(m_b(\mathcal{R}))_{k,j} = 1$

$$\Leftrightarrow \sum_{s=1}^{s<n} m_b(f)_{i,s} \cdot m_b(\mathcal{R})_{s,j} = 1 \Leftrightarrow m_b(f)_{i,k} \cdot m_b(\mathcal{R})_{k,j} = 1$$

$\Leftrightarrow m_b(f \circ \mathcal{R})$ est le produit de $m_b(f)$ par $m_b(\mathcal{R})$. c.q.f.d.

Proposition 10 : Soit $\mathcal{R}$ une relation sur S, f une permutation de S, alors :

$$m_b(\mathcal{R} \circ f) = m_b(\mathcal{R}).\, m_b(f).$$

Preuve : Soit $\mu_{i,j}$ le terme général de $m_b(\mathcal{R} \circ f) = m_b(\mathcal{R}) * m_b(f)$, $f_{i,j}$ le terme général de $m_b(f)$, $r_{i,j}$ le terme général de $m_b(\mathcal{R})$. On a $\mu_{i,j} = 1 \Leftrightarrow \exists k$ tel que $r_{i,k} = 1 = f_{k,j}$; f étant bijective il n'y a qu'un seul élément non nul par colonne (dans la $j^{ième}$ colonne ce ne peut donc être que $f_{k,j}$ et par suite :

$$\sum_{s=1}^{s<n} r_{i,s} \cdot f_{s,j} = r_{i,k} \cdot f_{k,j} = 1,$$ qui n'est autre que le terme général $m_{i,j}$ de $m_b(\mathcal{R}).m_b(f)$. c.q.f.d.

Corollaire

Soit $\mathcal{R}$ une relation sur S, f une permutation de S. Alors, pour toute base b de S :

$$m_b(f) * m_b(\mathcal{R}) * m_b(f^{-1}) = m_b(f) . m_b(\mathcal{R}) . m_b(f^{-1}).$$

Preuve : Conséquence immédiate des propositions 9 et 10.

Exercice 4 : Soit b et b' deux bases de S, f la permutation de S transformant b en b' et $\mathcal{R}$ une relation sur S. Calculer $m_{b'}(\mathcal{R})$ en fonction de $m_b(\mathcal{R})$ et $m_b(f)$.

§5 - CHEMINS ASSOCIES A UNE RELATION BINAIRE

Soit S un ensemble fini non vide, $\mathcal{R}$ une relation binaire sur S.

Définition : On appelle chemin (relativement à $\mathcal{R}$) toute suite $\gamma = (x_0, x_1, \ldots, x_p)$ de points de S telle que

$x_i \mathcal{R} x_{i+1} \quad \forall i = 0, 1, 2, \ldots, p-1.$

- L'entier p est dit alors longueur du chemin.
- x_0 et x_p sont dites les extrémités, respectivement initiale et terminale du chemin.
- Les éléments $x_0, x_1, x_2, \ldots, x_{p-1}, x_p$ sont dits les maillons du chemin.
- On dira que le chemin $\gamma = (x_0, x_1, \ldots, x_p)$ est injectif si ses maillons sont distincts 2 à 2.
- Soit x et y, 2 éléments de S ; on dira qu'il existe un chemin reliant x à y s'il existe un chemin dont x et y sont les extrémités respectivement initiale et terminale.

Exercice 5 : Montrer que s'il existe des chemins reliant x à y il en existe qui sont injectifs.

- Les points de S sont les chemins de longueur 0.
- On dira que le chemin γ est minimal s'il n'existe pas de chemin ayant les mêmes extrémités et de longueur strictement inférieure.

Exercice 6 : a) Montrer que $\mathcal{R}$ est réflexive $\rightarrow \forall x \in S$, (x, x) est un chemin (de longueur 1).

b) Montrer que si $\mathcal{R}$ est transitive, tout chemin minimal est de longueur ≤ 1. Réciproque ?

Soit $\gamma = (x_0, x_1, \ldots, x_p)$ un chemin ; alors $\forall i, j$ tel que $0 \leq i < j \leq p$, $\gamma' = (x_i, x_{i+1}, \ldots, x_j)$ est un chemin. On dit que j' est un sous-chemin de γ.

Notons, pour tout entier k : C^k = ensemble des chemins de longueur k.

On a donc $C^0 = S$, C^1 = ensemble des chemins de longueur 1 = graphe de $\mathcal{R}$.

On note $C(x, y)$ = ensemble des chemins reliant x à y.

Deux problèmes fondamentaux sont liés à la notion de chemin :

1er problème : Reconnaître si $C(x, y) \neq \emptyset$

2ème problème : En supposant $C(x, y) \neq \emptyset$, déterminer un chemin minimal reliant x à y.

- Le 1er problème : APPLICATION A LA FORMULATION DU CRITERE DE DEDUCTIBILITE

Ce premier problème contient comme cas particulier le problème fondamental universel du logicien, à savoir :

" Soit S un ensemble de propositions, $\mathcal{R}$ la relation d'implication, p et q " deux éléments de S ; le théorème $p \Rightarrow q$ est-il exact ?

Il revient au même de se poser la question : existe-t-il un chemin $(p = p_0, p_1, p_2, \ldots, p_n = q)$ pour la relation $\mathcal{R}$? (on dit "chemin déductif").

Essayons de préciser cette relation dite d'implication ou de déductibilité.

En logique mathématique on utilise une langue particulière, formée de formules qui se présentent comme des mots formés avec des lettres d'un certain alphabet, contenant à côté des signes usuels des mathématiques, comme par exemple des lettres, des parenthèses, d'autres signes spéciaux représentant des opérations logiques telles que $\vee, \wedge, \Gamma$ (négation), etc. Toute proposition se présente donc comme un mot de cet alphabet. Soit S l'ensemble des mots de cet alphabet. Choisir une logique, c'est se donner un ensemble $\mathcal{L}$ dit de substitutions permises ; par exemple, dans notre logique classique,

on a la substitution qui consiste à remplacer dans un mot $p \wedge p$ par p, $a \wedge \neg a$ par le symbole de l'assertion fausse (principe de non-contradiction), $a \vee \neg a$ par le symbole de l'assertion vraie (principe de tiers exclu) etc.

Identifiant une proposition et un mot qui l'exprime dans le langage de la logique formelle, la relation de déductibilité peut se formuler de la manière suivante :

$p \mathcal{R} q \Leftrightarrow q$ se déduit de $p \Leftrightarrow$ il existe un chemin $(p = p_0, p_1, p_2, \ldots, p_n = q)$ tel que l'on passe du mot p_i au mot p_{i+1} par une substitution permise $(0 \leq i \leq n-1)$.

On peut alors annoncer : "$p \Rightarrow q$' est un théorème", ou encore, q est déductible de p.

On voit donc que le problème de la "décision de déductibilité" se formule de la manière suivante :

" Pour deux mots p et q donnés, existe-t-il un chemin de déductibilité de " p à q ?

Jusqu'à présent, les obstacles liés à la résolution de ce problème universel sont restés insurmontables. Cela résulte du fait que l'ensemble S des mots est infini et que, peut-être, il faille envisager des chemins infinis. Mais le problème peut se résoudre dans des cas particuliers, par exemple si S est fini.

Quoiqu'il en soit, il nous a paru intéressant de formuler de manière rigoureuse ce qu'on appelle en général un "raisonnement déductif". Le langage relationnel nous en a fourni l'occasion.

§7 - LE TRAITEMENT DU DEUXIEME PROBLEME

Soit $\mathcal{R}$ relation binaire sur S, $b = (\sigma_1, \sigma_2, \ldots, \sigma_n)$ une base de S et soit $M = m_b(\mathcal{R})$ la matrice de $\mathcal{R}$ dans la base b.

Considérons la relation $\mathcal{R}^2 = \mathcal{R} \circ \mathcal{R}$; sa matrice représentative dans la base b sera $M^{(2)} = M * M$.

Plus général, soit $p \geq 1$ entier, on définit $\mathcal{R}^p = \mathcal{R}^{p-1} \circ \mathcal{R}$; sa matrice représentative sera $M^{(p)} = M^{(p-1)} * M$; notons $m^p_{i,j}$ le terme situé à la $i^{ème}$ ligne et à la $j^{ième}$ colonne de $M^{(p)}$.

D'après la définition de * nous savons que :

$m^2_{i,j} = 1$ ⇔ $\exists k$ $(1 \leq k \leq n)$ tel que $m^1_{i,k} = 1$ et $m^1_{k,j} = 1$

⇔ $\sigma_i \mathcal{R} \sigma_k$ et $\sigma_k \mathcal{R} \sigma_j$

⇔ Il existe un chemin $(\sigma_i, \sigma_j, \sigma_k)$ de longueur 2 reliant σ_i à σ_j.

Si nous faisons l'hypothèse d'induction : $m^{p-1}_{i,j} = 1$ ⇔ il existe un chemin de longueur p-1 reliant σ_i à σ_j ; alors $m^p_{i,j} = 1$ ⇔ $\exists k$ $(1 \leq k \leq n)$ tel que $m^{p-1}_{i,k} = 1$ et $m_{k,j} = 1$ ⇔ il existe un chemin $(\sigma_i, \ldots, \sigma_k)$ de longueur p-1 et un chemin (σ_k, σ_j) de longueur 1 ⇔ il existe un chemin $(\sigma_i, \ldots, \sigma_j)$ de longueur p reliant σ_i à σ_j. Donc :

Proposition 11 : Il existe un chemin de longueur p reliant σ_i à σ_j ⇔ $m^p_{i,j} = 1$.

Remarquons que si card (S) = n il ne peut y avoir de chemin de longueur supérieure à n sans répétition de sommets. Or si un élément x_i figure deux fois dans un chemin, on peut supprimer le sous-chemin d'extrémités x_i :

si $\gamma = (x_o, x_1, \ldots, x_k, x_i, \ldots, x_i, x_j, \ldots x_p)$ alors

$\gamma' = (x_o, x_1, \ldots, x_k, x_i, \ldots, x_j \ldots x_p)$ est aussi un chemin

reliant x_o à x_p. Par suite, il existe un chemin reliant x_o à x_p, si et seulement si il existe un chemin de longueur $k \leq n$ reliant x_o à x_p.

Compte tenu de la proposition 11, pour savoir s'il existe un chemin reliant x_o à x_p il suffit de calculer les "puissances" $M^{(k)}$ successives, la longueur d'un chemin minimal reliant σ_i à σ_j (s'il existe des chemins reliant x_i à σ_j) sera le plus petit entier p tel que $m^p_{i,j} = 1$, et il suffit de calculer $M^{(p)}$ $\forall p \leq n$.

Pour compléter cette étude nous allons introduire la notion de matrice de fermeture transitive de la relation $\mathcal{R}$.

Notons $\Gamma^1 = \{\sigma_j \in S / \exists \sigma_i \in S$ avec $\sigma_i \mathcal{R} \sigma_j\}$ = ensemble des extrémités terminales des chemins de longueur 1, et $\Gamma^1(\sigma_i) = \{\sigma_j \in S / \sigma_i \mathcal{R} \sigma_j\}$ = ensemble des extrémités terminales des chemins de longueur 1 issus de σ_i $(1 \leq i \leq n)$. De même, par récurrence, pour p entier, $p > 1$; soit $\Gamma^p = \{\sigma_j \in S / \exists \sigma_k \in \Gamma^{p-1}$ avec $\sigma_k \mathcal{R} \sigma_j\}$ = ensemble des extrémités terminales des chemins de longueur p, et $\Gamma^p(\sigma_i) = \{\sigma_j \in S / \exists \sigma_k \in \Gamma^{p-1}(\sigma_i)$ avec $\sigma_k \mathcal{R} \sigma_j\}$ = ensemble des extrémités terminales des chemins de longueur p issus de σ_i.

On a évidemment $\Gamma^p = \bigcup_{i=1}^{i=n} \Gamma^p(\sigma_i) \qquad \forall p \geq 1.$

Considérons alors la relation $\mathcal{R}_p$ définie sur S par $x \mathcal{R}_p y \Leftrightarrow y \in \Gamma^p(x)$ et soit $\tilde{\mathcal{R}}$ la relation définie par :

$$x \tilde{\mathcal{R}} y \Leftrightarrow \exists p \quad (0 \leq p \leq n) \text{ tel que } x \mathcal{R}_p y$$

soit : $\sigma_i \tilde{\mathcal{R}} \sigma_j \Leftrightarrow \exists p \quad (0 \leq p \leq n)$ tel que $\sigma_j \in \Gamma^p(\sigma_i)$

Or, si M est la matrice représentative de $\mathcal{R}$ dans $b = (\sigma_1, \sigma_2, \ldots \sigma_n)$ on a $m^p_{i,j} = 1 \Leftrightarrow \sigma_j \in \Gamma^p(\sigma_i)$, donc si $\mu_{i,j}$ est le terme situé à la $i^{ème}$ ligne et la $j^{ième}$ colonne de $\tilde{M} = m_b(\tilde{\mathcal{R}})$; on a :

$$\mu_{i,j} = 1 \Leftrightarrow \sigma_i = \sigma_j \text{ ou } m_{i,j} = 1 \text{ ou } m^2_{i,j} = 1 \ldots \text{ou } m^p_{i,j} = 1 \text{ ou} \ldots m^n_{i,j} = 1$$

donc $\tilde{M} = I_n \vee M \vee M^{(2)} \vee M^{(3)} \vee \ldots \vee M^{(n)}$, I_n étant la matrice de l'égalité = matrice unité d'ordre n . D'où :

<u>Proposition 12</u> :

> Soit S de cardinal S, $b = (\sigma_1, \ldots, \sigma_n)$ une base de S, $\mathcal{R}$ une relation sur S, M la matrice de $\mathcal{R}$ dans b ; alors il existe un chemin de σ_i à σ_j $\Leftrightarrow$ le terme général situé à la $i^{ème}$ ligne et la $j^{ième}$ colonne de la matrice : $\tilde{M} = I_n \vee M \vee M^{(2)} \vee M^{(3)} \vee \ldots \vee M^{(n)}$ est égal à 1.

La relation $\tilde{\mathcal{R}}$ s'appelle la fermeture transitive de $\mathcal{R}$.

Exemple :

Soit $S = \{a, b, c, d, e\}$, $\mathcal{R}$ la relation sur S définie par $a\mathcal{R}b$, $b\mathcal{R}c$, $d\mathcal{R}a$, $e\mathcal{R}d$, $a\mathcal{R}e$, $d\mathcal{R}c$, $e\mathcal{R}b$ et $e\mathcal{R}d$.

Dans la base (a, b, c, d, e) $\mathcal{R}$ a pour matrice :

$$M = \begin{bmatrix} 0&1&0&0&1 \\ 0&0&1&0&0 \\ 0&0&0&0&0 \\ 1&0&1&0&0 \\ 0&1&0&1&0 \end{bmatrix}$$; un calcul immédiat montre que :

$$M^{(2)} = \begin{bmatrix} 0&1&0&0&1 \\ 0&0&0&0&0 \\ 0&0&0&0&0 \\ 1&0&1&0&0 \\ 0&1&1&1&0 \end{bmatrix} \qquad M^{(3)} = \begin{bmatrix} 1&0&1&0&0 \\ 0&0&0&0&0 \\ 0&0&0&0&0 \\ 0&1&1&1&0 \\ 0&1&0&0&1 \end{bmatrix}$$

$$M^{(4)} = \begin{bmatrix} 0&1&0&0&1 \\ 0&0&0&0&0 \\ 0&0&0&0&0 \\ 1&0&1&0&0 \\ 0&1&1&1&0 \end{bmatrix} \qquad M^{(5)} = \begin{bmatrix} 0&1&1&1&0 \\ 0&0&0&0&0 \\ 0&0&0&0&0 \\ 0&1&0&0&1 \\ 1&0&1&0&0 \end{bmatrix}$$

d'où $M = \begin{bmatrix} 1&1&1&1&1 \\ 0&1&1&0&0 \\ 0&0&1&0&0 \\ 1&1&1&1&1 \\ 1&1&1&1&1 \end{bmatrix}$

Il n'y a donc pas de chemin reliant : b à a , b à d
b à e
c à a
c à b
c à d
c à e

Exercice 7 : Résoudre le problème dit de la chèvre, du chou et du loup.
Soit $\mathcal{E} = \{s, c, l, b\}$: s = chou, c = chèvre, l = loup, b = berger, et S = ensemble des parties de $\mathcal{E}$; on considère la relation Rdéfinie sur S par :

$XRY \rightarrow X \cup Y = \mathcal{E}$, $X \cap Y = \emptyset$, avec de plus la condition : si $b \in X$, alors les éléments Y ne se mangent pas entre eux et si $b \in Y$, alors les éléments de X ne se mangent pas entre eux.

Montrons que trouver une solution au problème posé consiste à trouver un chemin (pour R), d'extrémité centrale $(\mathcal{E}, \emptyset)$ et pour extrémité terminale $(\emptyset, \mathcal{E})$

Exercice 8 : En suivant une démarche analogue, résoudre le problème suivant, qui fit les délices des soirées de l'époque coloniale :

3 blancs, b_1, b_2, b_3 et 3 noirs N, n_1, n_2 doivent traverser un fleuve infesté de crocodiles.
Le seul moyen est un canot à moteur que seuls les 3 blancs et le noir N savent conduire. Ce canot ne peut contenir que 2 personnes au maximum. Les 3 noirs sont anthropophages : dès qu'en un même lieu le nombre des noirs est strictement supérieur à celui des blancs les noirs mangent les blancs.
Comment s'y prendre pour effectuer la traversée des 6 hommes sans qu'aucun acte de cannibalisme ne vienne endeuiller l'expédition ?

I - MODELES STRUCTURAUX POUR L'ETUDE D'UN "SOCIUS"

Appelons socius tout ensemble d'éléments entre lesquels existent des systèmes relationnels (phénomènes d'organisation, de circulation, d'information, etc.) que le sociologue du moment prétend déceler.

Ces structures concrètes pouvant être décelées (groupes de personnes, hiérarchie, réseaux d'information, ensemble de croyances ou d'opinion,

classes culturelles, etc.) ; si entre des éléments peuvent être mis en évidence des systèmes relationnels, on pourra dégager de là une relation dont les propriétés pourront, par analogie avec une relation abstraite, introduire des concepts nouveaux du point de vue du sociologue. Le problème est de déterminer les éléments concrets, et, quels concepts de théorie sociologique peuvent être mis en bijection avec respectivement un ensemble S et un sous-ensemble de S x S de manière à obtenir une relation binaire sur S. Les possibilités sont très nombreuses : on peut prendre pour S aussi bien par exemple l'ensemble des étudiants participant à un cours, l'ensemble des emplacements de bureaux d'une organisation, l'ensemble des solutions d'un problème de décision. La relation concrète étant définie par un groupe verbal V, il sera nécessaire qu'une analyse sociométrique soit suffisamment élaborée pour pouvoir décider si la proposition xVy est une assertion vraie ou fausse. Moyennant quoi le sociologue, après avoir inventorié $\mathcal{R}$ en détectant $\{(x, y) \in S/x \mathcal{R} y\}$, voudra :

a) interpréter la relation pour décrire les faits.
b) interpréter la relation pour prévoir des faits.

Les paragraphes précédents ont eu pour but de donner un outil : la représentation matricielle, pour tenter de répondre aux objectifs a) et b). Un premier point consiste à "situer" chaque élément de S par rapport à une relation $\mathcal{R}$ donnée sur S. Nous appellerons cela : $\mathcal{R}$-analyse d'un élément.

§9 - $\mathcal{R}$-ANALYSE D'UN ELEMENT

Soit $b = (\sigma_1, \sigma_2, \ldots, \sigma_n)$ une base de S, $\mathcal{R}$ une relation sur S, $M = (m_{i,j})$ la représentation matricielle de $\mathcal{R}$ dans b.

Définition 1 : On appelle demi-degré extérieur de σ_i, et on note d_i^+ le nombre d'éléments σ_j tels que $\sigma_i \mathcal{R} \sigma_j$, c'est-à-dire le nombre des éléments qui sont extrémités terminales de chemins de longueur 1 ayant σ_i comme extrémité initiale.

Il résulte de la définition de $\Gamma^1(\sigma_i)$ que $d_i^+ = \text{card}(\Gamma^1(\sigma_i))$ et donc que d_i^+ est le nombre de $m_{i,j}$ non nuls, d'où :

Proposition 13 : $d_i^+ = \sum_{j=1}^{j=n} m_{i,j}$ (la somme étant prise au sens de N)

Définition 2 : On appelle demi-degré intérieur de σ_i, et on note d_i^- le nombre d'éléments σ_j tels que $\sigma_j \mathcal{R} \sigma_i$.

Il résulte immédiatement de là que :

Proposition 20 : $d_i^- = \sum_{j=1}^{j=n} m_{j,i}$ (la somme étant prise au sens de n)

Il est clair que $\sum_{i=1}^{i=n} d_i^+ = \sum_{i=1}^{i=n} \sum_{j=1}^{j=n} m_{i,j} = \sum_{i=1}^{i=n} \sum_{j=1}^{j=n} m_{j,i} = \sum_{i=1}^{i=n} d_i^-$, d'où :

Proposition 21 : La somme des demi-degrés intérieurs de tous les éléments est égale à la somme des demi-degrés extérieurs de tous les éléments.

La valeur commune $\mu = \sum_{i=1}^{i=n} \sum_{j=1}^{j=n} m_{i,j}$ n'est autre que la somme des tous les éléments de la matrice M ; il est clair que cette somme ne dépend pas du choix de la base.

On appelle demi-degré moyen le nombre $d = \frac{\mu}{n}$.

Définition 3 : $\sigma_i \in S$ est dit isolé $\Leftrightarrow d_i^+ = d_i^- = 0$.

Définition 4: $\sigma_i \in S$ est dit une source $\Leftrightarrow d_i^+ > 0$ et $d_i^- = 0$

Définition 5 : $\sigma_i \in S$ est dit un puits $\Leftrightarrow d_i^+ = 0$ et $d_i^- > 0$

Définition 6 : $\sigma_i \in S$ est dit un transmetteur $\Leftrightarrow d_i^+ = d_i^- = 1$

Tout autre élément de S est considéré comme élément ordinaire.

Exercice 9 : Soit $b = (\sigma_1, \sigma_2, \ldots, \sigma_n)$ une base de S, $\mathcal{R}$ une relation sur S telle que pour aucun σ_i on a $\sigma_i \mathcal{R} \sigma_i$ et telle que $\forall \sigma_i, \sigma_j$ avec $\sigma_i \neq \sigma_j$ alors $\sigma_i \mathcal{R} \sigma_j$ ou $\sigma_j \mathcal{R} \sigma_i$, $M = (m_{i,j})$ la matrice de $\mathcal{R}$ dans la base b. On dit que $\sigma_i, \sigma_j, \sigma_k$ $(i \neq j \neq k)$ forment un triangle d'intransitivité si $\sigma_i \mathcal{R} \sigma_j$, $\sigma_j \mathcal{R} \sigma_k$ et $\sigma_k \mathcal{R} \sigma_i$. Démontrer que le nombre de triangles d'intransitivité est :

$$n_i = \left[\frac{n}{3}\right] - \sum_{j=1}^{j=n} \frac{d_j^+ (d_j^+ - 1)}{2} .$$

Démontrer que si n = 6 le nombre maximal possible de triangles d'intransitivité est 8.

§10 - SUR LES CHEMINS MINIMAUX

Soit $b = (\sigma_1, \sigma_2, \ldots, \sigma_n)$ une base de S, $\mathcal{R}$ une relation sur S ; un chemin minimal, s'il existe, reliant σ_i à σ_j, est un chemin reliant σ_i à σ_j de longueur minimale.

On note alors $d(\sigma_i, \sigma_j)$ la longueur d'un chemin minimal reliant σ_i à σ_j.

On a déjà vu que, si $C(\sigma_i, \sigma_j)$ désigne l'ensemble des chemins reliant σ_i à σ_j, alors $C(\sigma_i, \sigma_j) \neq \emptyset \Leftrightarrow$ il existe un chemin minimal reliant σ_i à σ_j, et alors $d(\sigma_i, \sigma_j)$ est le plus petit entier $p \leq n$ tel que $m^p_{i,j} = 1$.

Proposition 22 : Si $C(\sigma_i, \sigma_j) \neq \emptyset$ et $C(\sigma_j, \sigma_k) \neq \emptyset$ alors $C(\sigma_i, \sigma_k) \neq \emptyset$ et $d(\sigma_i, \sigma_k) \leq d(\sigma_i, \sigma_j) + d(\sigma_j, \sigma_k)$.

Preuve Soit $(\sigma_i, \ldots, \sigma_j) \in C(\sigma_i, \sigma_j)$ et $(\sigma_j, \ldots, \sigma_k) \in C(\sigma_j, \sigma_k)$, alors $(\sigma_i, \ldots, \sigma_j, \ldots, \sigma_k) \in C(\sigma_i, \sigma_k)$ et longueur de $(\sigma_i, \ldots, \sigma_j, \ldots, \sigma_k)$ = longueur $(\sigma_i, \ldots, \sigma_j)$ + longueur $(\sigma_j, \ldots, \sigma_k)$ en particulier si longueur $(\sigma_i, \ldots, \sigma_j) = d(\sigma_i, \sigma_j)$ et longueur $(\sigma_j, \sigma_k) = d(\sigma_j, \sigma_k)$.

c. q. f. d.

Il est clair que tout sous-chemin d'un chemin minimal est lui-même minimal.

- LA RELATION "DEFINIE" PAR << EST UN DESCENDANT DE >>

Soit sur $S=\{\sigma_1,\sigma_2,\ldots,\sigma_n\}$ une relation $\mathcal{R}$, et $\tilde{\mathcal{R}}$ la relation dite fermeture transitive de $\mathcal{R}$, définie par :

$\sigma_i \tilde{\mathcal{R}} \sigma_j$ ⇔ il existe un chemin allant de σ_i à σ_j ; on a :

Proposition 23 : La relation $\tilde{\mathcal{R}}$, qu'on peut traduire par "est un descendant de" est réflexive et transitive.

Preuve : Nous en laissons le soin au lecteur.

Rappelons que les relations réflexives et transitives sont dites des relations de préordre. Ces relations apparaissent fréquemment dans la nature. Etudions, par exemple, comment se communiquent les informations à l'intérieur d'un groupe de personnes ; on prend pour S l'ensemble des personnes du groupe et pour relation $\mathcal{R}$ la relation : $x\mathcal{R}y$ ⇔ x communique directement avec y.

Pour pouvoir tirer des conclusions au sujet du flot des informations circulant dans ce réseau on suppose que :

(i_1) Une personne ne possède des informations que dans les 2 cas suivants :
- elle est à l'origine de l'information ;
- l'information lui est transmise par une autre personne du réseau.

(i_2) Si une personne σ_i possède une information, elle la transmet à toutes les personnes avec qui elle peut communiquer directement.

On voit alors immédiatement que si σ_i possède une information, et s'il existe un chemin reliant σ_i à σ_j l'information sera transmise à σ_j.

§12 - BASES D'UNE RELATION

Soit donc $S = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$, $\mathcal{R}$ une relation sur S,

la relation : $\sigma_i \mathcal{R} \sigma_j \Leftrightarrow$ il existe un chemin allant de σ_i à σ_j.

Pour chaque σ_i notons $\Gamma(\sigma_i) = \{\sigma_j \in S / \sigma_i \tilde{\mathcal{R}} \sigma_j\} = \bigcup_{0 \le p \le n} \Gamma^p(\sigma_i)$. D'après la proposition 12, si $b = (\sigma_1, \sigma_2, \ldots, \sigma_n)$ est une base de S, et $M = (\mu_{i,j})$ la matrice de fermeture transitive de $\mathcal{R}$: alors $(\Gamma(\sigma_i)) = \sum_{j=1}^{j=n} \mu_{i,j}$ la somme étant prise dans N.

De manière plus générale soit $A \subset S$, on notera :

$\Gamma(A) = \{\sigma_j \in S / \exists \sigma_i \in A$ tel que $\sigma_i \tilde{\mathcal{R}} \sigma_j\}$.

Il est clair que si $A = \{\sigma_{i_1}, \sigma_{i_2}, \ldots, \sigma_{i_k}\}$ alors $\Gamma(A) = \Gamma(\sigma_{i_1}) \cup \Gamma(\sigma_{i_2}) \ldots \cup \Gamma(\sigma_{i_k})$.

Définition : Soit $B \subset S$; on dira que B est une base pour $\mathcal{R}$ si

B_1) $\Gamma(B) = S$

B_2) $B' \subset B \Rightarrow \Gamma(B') \subset S$, l'inclusion étant stricte.

Proposition 24 :

$B \subset S$ est une base si et seulement si :

(a) $\Gamma(B) = S$

(b) $\nexists \sigma_j \in B$ tel que $\exists \sigma_i \in B$ avec $\sigma_i \tilde{\mathcal{R}} \sigma_j$

Preuve : Il suffit d'établir que si B vérifie B_1, alors (b) $\Leftrightarrow B_2$

. Soit alors B vérifiant a) et b), $\forall \sigma_j \in B$, $B - \{\sigma_j\}$ ne contient pas de sommet dont σ_j soit un descendant $\Rightarrow \Gamma(B - \{\sigma_j\})$ ne contient pas σ_j donc strictement plus petit que S ; donc B vérifie B_2.

. Inversement, s'il existait $\sigma_j \in B$ avec $\sigma_i \in B$ et $\sigma_i \mathcal{R} \sigma_j$, alors $B - \{\sigma_j\}$ vérifierait $\Gamma(B - \{\sigma_j\}) = \Gamma(B) = S$ et B ne serait pas une base.

Proposition 25 : Toute relation $\mathcal{R}$ sur S fini possède une base.

Preuve : Soit $\mathcal{U} = \{A \subset S / \Gamma(A) = S\}$; alors $\mathcal{U}$ est un sous-ensemble de l'ensemble des parties de S qui est fini ; donc $\mathcal{U}$ est fini ; $\mathcal{U}$ est non vide car évidemment $\Gamma(S) = S$ et donc $S \in \mathcal{U}$; a donc des éléments minimaux. Ce sont précisément les bases.

c.q.f.d.

Exercice 10: Démontrer que pour une relation $\mathcal{R}$ donnée sur S, toute les bases de $\mathcal{R}$ ont même nombre d'éléments.

Exercice 11 : Les réseaux INTOX.

Lorsqu'un réseau d'espionnage est découvert par un service de contre-espionnage, il est souvent plus intéressant, au lieu de le démanteler, de l'"intoxiquer", c'est-à-dire de faire passer dans ce réseau des informations fausses ; c'est une opération délicate : ces informations ne doivent pas tomber dans le domaine public de façon à conserver le plus longtemps possible un maximum de crédibilité. Par ailleurs, en général, un réseau n'accepte comme valable une information que si tous ses membres arrivent à la connaître, (recoupements).

A la suite d'une longue et discrète enquête, les services du contre-espionnage ont pu savoir comment circulaient les informations secrètes entre les 17 membres (numérotés de 1 à 17) du réseau découvert : le tableau suivant résume les liaisons entre informateurs et informés dont on est absolument sûr:

1 informe 2, 4 et 5	2 informe 3	3 informe 1, 4 et 8
4 n'informe personne	5 informe 1, 6 et 14	6 informe 7
7 n'informe personne	8 informe 3	9 informe 10 et 15
10 informe 9 et 14	11 informe 12	12 informe 13 et 17
13 informe 11, 16 et 17	14 informe 5, 15 et 17	15 informe 5 et 6
16 informe 2, 4 et 8	17 informe 2 et 14	17 informe 2 et 14

Compte tenu de ces données, et compte tenu des difficultés, disons techniques, le service de contre-espionnage doit "informer" au départ, le plus petit nombre possible de membres du réseau.

A qui devra-t-on s'arranger pour donner des "informations" pour atteindre les objectifs souhaités ?