ÉQUATIONS ALGÉBRIQUES

par Léonce LESIEUR

(conférence prononcée en 1976 à la Régionale de LIMOGES)

La théorie des équations algébriques, son historique, ses idées, son développement.

Je voudrais parler de la théorie des équations algébriques, de son histoire, de son développement, de ses méthodes, des problèmes et des découvertes qu'elle a amenés. Le sujet est trop vaste pour être entièrement traité en une fois ; je n'aborderai donc que certains aspects de cette théorie, certains moments de son histoire. Si vous voulez, je vais faire un triple saut dans l'espace. Le premier saut nous conduit au milieu du XVIe siècle à l'époque de la résolution des équations du 3e et du 4e degré ; le deuxième nous propulse trois siècles plus tard avec les beaux résultats de GALOIS sur le groupe défini par une équation ; enfin le troisième nous ramène aux temps présents.

I - LA PREMIERE PERIODE

Les équations suivantes posent et ont posé de nombreux problèmes.

(1) $2x = 3$; (2) $ax = b$

(3) $x^2 = 2$; (4) $x^2 = \Pi$

(5) $x^3 = 2$; (6) $x^3 = 3x + 1$

(7) $x^3 + ax = b$; (8) $x^4 = ax^2 + bx + c$

La première question est de savoir quels sont les *nombres* qu'on peut admettre comme solutions de l'équation. La deuxième est de connaître quelles sont les *opérations* ou lois de composition qui sont définies sur ces nombres.

Même dans le cas de l'équation (1), il faut utiliser les nombres rationnels, et pas seulement les entiers, ainsi que les règles de calcul sur ces nombres. Il semble que les Grecs, et avant eux les Egyptiens et les Babyloniens, en avaient une idée claire, grâce à la notion de grandeurs commensurables. Encore faut-il remarquer que tous leurs exemples sont numériques, et que l'usage de désigner par des lettres les nombres connus ou inconnus qui interviennent dans une équation comme (2) n'est apparue qu'avec VIETE au XVIe siècle. (Pour plus de détails, lire la note historique de Bourbaki [3] p.147).

Quand on considère l'équation (3), les nombres rationnels ne suffisent plus, "et il est possible que ce soit l'échec de

tentatives répétées pour exprimer rationellement $\sqrt{2}$ qui conduisit les mathématiciens de l'école pythagoricienne à démontrer que ce nombre est irrationnel" (Bourbaki [4] p. 192).

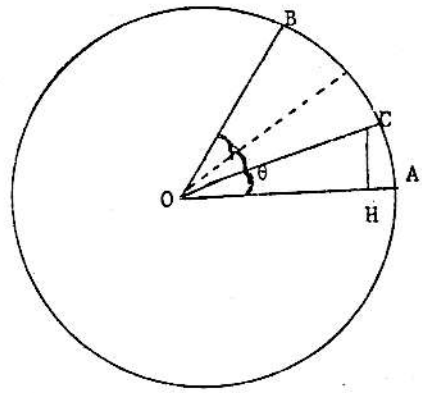
Avec le développement de la géométrie, les grecs et EUCLIDE en particulier, s'ingénièrent à résoudre les problèmes par des constructions géométriques au moyen de la règle et du compas. On pouvait ainsi atteindre toutes les solutions des équations du second degré à coefficients rationnels. Mais ils échouèrent évidemment sur le problème posé par la quadrature du cercle, qui se traduit par l'équation (4) et qui fait intervenir un nombre transcendant. (On ne pourra démontrer rigoureusement que beaucoup plus tard, en 1888, avec LINDEMANN, que π, et par conséquent $\sqrt{\pi}$, est transcendant). Ils échouèrent aussi sur le problème de la duplication du cube : équation (5), et sur celui de la trisection de l'angle de 60° : équation (6), qui ne peuvent pas non plus se résoudre au moyen de constructions avec la règle et le compas.

$\theta = \frac{\pi}{9}$ rad. = 20°

$x = 2 \cos \theta = 2\ OH$

$\cos 3\theta = 4 \cos^3\theta - 3 \cos \theta = \frac{1}{2}$

$x^3 = 3x + 1$



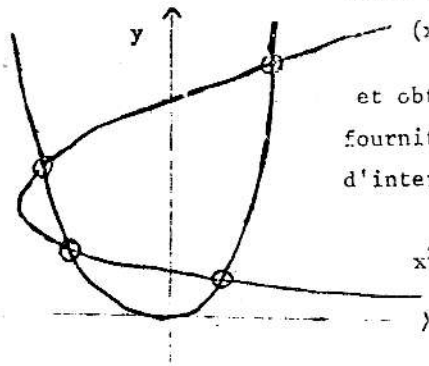
Il fallut ensuite beaucoup de temps, compte tenu du déclin des civilisations et du manque d'intérêt pour les équations algébriques, pour que de nouveaux progrès soient réalisés. Ce fut au Moyen Age, et ils aboutirent enfin à la résolution de l'équation (7) par del FERRO, un mathématicien de l'Ecole Italienne de CARDAN, au moyen de la formule :

$$x = \sqrt[3]{\frac{b}{2} + \sqrt{(\frac{b}{2})^2 + (\frac{a}{3})^3}} + \sqrt[3]{\frac{b}{2} - \sqrt{(\frac{b}{2})^2 + (\frac{a}{3})^2}}$$

L'intérêt de cette formule barbare est d'abord qu'elle exprime les racines par radicaux cubiques et carrés, mais aussi que, même dans le cas où les trois racines sont réelles (les coefficients a, b, c étant supposés réels), les racines carrées sont celles de nombres négatifs. C'est la raison qui a conduit dès cette époque à introduire le symbole $\sqrt{-1}$ et à effectuer des calculs sur ce symbole, calculs qui n'ont été formalisés que plusieurs siècles après pour donner naissance aux nombres complexes. Il n'était pas question à cette époque, sous peine d'être considéré comme un dangereux sorcier, de donner un sens à des racines de l'équation $x^2 + 1 = 0$. Vous remarquerez également que les équations écrites ne font pas en principe intervenir de nombres négatifs, et l'on doit plaindre et admirer en même temps les

mathématiciens de ce temps là qui ne disposaient pas de l'outil élégant consacré seulement par les écrits de DESCARTES.

Enfin, sur la lancée, mais avec un bon temps de retard, FERRARI, un autre élève de CARDAN, résout par radicaux une équation du 4e degré de la forme (8), en 1545. Méthode : écrire l'équation sous la forme :



$$(x^2 + z)^2 = (a + 2z)\,x^2 + b\,x + (c + z^2)$$

et obtenir un carré au second membre en annulant le discriminant qui fournit une résolvante cubique en z. Autre méthode : chercher les points d'intersection des deux paraboles :

$$x^2 = y \quad , \quad y^2 = a\,y + b\,x + c$$

II - LE GROUPE DEFINI PAR UNE EQUATION ALGEBRIQUE

Il était naturel de chercher à résoudre par radicaux les équations de degré $n \geqslant 5$. Mais trois siècles allaient passer avant qu'ABEL et GALOIS ne démontrent l'impossibilité de cette résolution dans le cas d'une équation générale. Je fais une halte à cette nouvelle époque en essayant de dégager la notion de groupe défini par une équation. Je commence par le plus simple des exemples, mais en le traitant complètement avec les moyens et le langage modernes.

1. L'équation du second degré sur un corps k.

Soit k un sous-corps des nombres complexes $\mathbb{C}$, par exemple : $k = \mathbb{Q}$, ou $k = \mathbb{R}$, ou $k = \mathbb{Q}(i)$. On a donc :

$$\mathbb{Q} \subset k \subset \mathbb{C}$$

Considérons l'équation du second degré à coefficients dans k :

(1) $F(x) = x^2 + b\,x + c = 0$, $b, c \in k$

$F(X)$ est un polynôme du second degré de l'anneau $k(x)$

Pour résoudre (1), on met le trinôme sous forme canonique :

$$(x + \frac{b}{2})^2 - \frac{b^2 - 4c}{4} = 0.$$

Posons $\Delta = b^2 - 4c$. On obtient les racines, dans $\mathbb{C}$:

(2) $$x_1 = \frac{b + \sqrt{\Delta}}{2} \quad , \quad x_2 = \frac{-b - \sqrt{\Delta}}{2}$$

Le polynôme $f(X) = X^2 + b\,X + c$ se décompose en facteurs linéaires sous la forme :

(3) $F(X) = (X - x_1)\,(X - x_2)$

et on a les relations entre les racines :

(4) $x_1 + x_2 = -b$, $x_1\,x_2 = c$

Tel est le calcul classique élémentaire. Mais on peut aller un peu plus loin.

Le corps de décomposition K de F(x) sur k

Considérons le corps K engendré dans $\mathbb{C}$ par k et les racines

x_1 et x_2 de l'équation. $K = k(x_1, x_2)$ est constitué par les fractions rationnelles $\frac{f(x_1, x_2)}{g(x_1, x_2)}$ où f et g sont des polynômes de l'anneau $k[X_1, X_2]$ tels que $g(x_1, x_2) \neq 0$. Cette dernière condition implique $g(X_1, X_2) \neq 0$, c'est-à-dire que le polynôme $g(X_1, X_2)$ n'est pas à coefficients tous nuls, mais la réciproque n'est pas vraie : le polynôme $g(X_1, X_2) = X_1 + X_2 + b$ n'est pas nul, alors que le nombre $g(x_1, x_2) = x_1 + x_2 + b$ est nul d'après (4).

Définition 1. Le corps $K = k(x_1, x_2)$ s'appelle le corps de décomposition du polynôme $F(X)$, ou de l'équation (1), sur k. Cette terminologie vient de l'égalité (3) ; on dit également, par abus de langage, corps des racines de l'équation (1) sur k (bien que les racines ne constituent pas à elles-seules un corps).

Etudions ce corps K. En remplaçant x_2 par $-x_1 - b$, d'après (4), il est clair que $K = k(x_1)$ est entièrement engendré par x_1 sur k. De plus, si l'on pose :

(5) $\alpha = \sqrt{\Delta}$, $\Delta = b^2 - 4c$,

on voit immédiatement d'après (2), que $K = k(\alpha)$ est aussi engendré par α sur k.

Deux cas peuvent se présenter :

1°) $\alpha = \sqrt{\Delta} \in k$, ce qui équivaut à :

$\Delta = b^2 - 4c$ est un carré dans k,

ou les racines x_1 et x_2 appartiennent à k, ou : le polynôme $F(x)$ est réductible dans k. Dans ce cas, le corps de décomposition K est égal à k.

2°) $\alpha = \sqrt{\Delta} \notin k$, ce qui équivaut à :

$\Delta = b^2 - 4c$ n'est pas un carré dans k,

ou : les racines x_1 et x_2 n'appartiennent pas à k,

ou : le polynôme $F(x)$ est irréductible sur k.

Dans ce cas, le corps de décomposition K contient strictement k. On l'appelle une *extension quadratique de k.*

Nous allons préciser dans ce deuxième cas la forme des éléments de K. Soit $\xi = \frac{f(\alpha)}{g(\alpha)} \in K$.

En remplaçant α^2 par Δ d'après 5, on met ξ sous la forme homographique $\frac{u + v\alpha}{r + s\alpha}$, $r + s\alpha \neq 0$, les coefficients u, v, r, s appartenant à k.

Démontrons que la condition $r + s\alpha \neq 0$ implique $r - s\alpha \neq 0$. Cela résulte du lemme suivant.

Lemme : *$r + s\alpha = 0$ équivaut à : $r = s = 0$*

($r, s \in k$).

En effet, supposons $r + s\alpha = 0$. La condition $s \neq 0$ entraînerait $\alpha = -\frac{r}{s} \in k$, ce qui est contraire à l'hypothèse $\alpha \notin k$. Il en résulte $s = 0$, d'où $r = 0$. Réciproquement, $r = s = 0 \Rightarrow r + s\alpha = 0$.

Revenons à l'expression $\xi = \frac{u + v\alpha}{r + s\alpha}$, $r + s\alpha \neq 0$.

On a donc en appliquant le lemme à $r - s\alpha$, la condition $r - s\alpha \neq 0$, qui permet de multiplier au numérateur et au dénominateur de ξ par

le nombre $r - s\alpha$. On obtient :

$$\xi = \frac{(u + v\alpha)(r - s\alpha)}{r^2 - s^2 \Delta} = A + B\alpha \quad A, B \in k$$

Cela prouve que 1 et α sont deux générateurs de K considéré comme espace vectoriel sur k . Je dis que $(1, \alpha)$ en est une base : le lemme exprime en effet l'indépendance linéaire de 1 et α sur k.

On a donc démontré le théorème suivant :

théorème 1 . *Dans le cas $\alpha \notin k$, le corps de décomposition K de l'équation $F(x) = o$ sur k est un espace vectoriel sur k de dimension égale à 2, dont une base est constituée par 1 et α .*

Une autre base est constituée par 1 et x_1, ou 1 et x_2, ou même x_1 et x_2 (cette dernière propriété étant laissée comme exercice au lecteur).

Le groupe G défini l'équation $F(x) = o$ sur k.

Quand on a un corps K, il est toujours intéressant de déterminer les automorphismes, c'est-à-dire les bijections σ qui vérifient :

$\forall\, x, y \in K$, $\sigma(x+y) = \sigma(x) + \sigma(y)$, $\sigma(xy) = \sigma(x)\,\sigma(y)$, $\sigma(1) = 1$.

De plus, comme le corps de base k joue un rôle important, on se limite aux automorphismes σ qui laissent fixes tous les éléments de k:

$$\forall\, c \in k\ ,\ \sigma(c) = c.$$

On les appelle des k - automorphismes de K. Ils constituent évidemment un groupe G pour la composition des applications.

Définition 2/ On appelle *groupe de GALOIS de l'équation $F(x) = o$ sur k* , ou du polynôme F sur k, ou de l'extension K du corps k, le groupe multiplicatif des k - automorphismes de K. On le note :

$$G = \mathrm{Gal}(F, k) = \mathrm{Gal}(K, k)$$

Pour déterminer $\sigma \in G$, il suffit de connaître $\sigma(\alpha)$, car $\xi = u + v\alpha$, $u, v, \in k$ donne $\sigma(\xi) = u + v\sigma(\alpha)$.

Mais l'égalité $\alpha^2 = \Delta$ implique $(\sigma(\alpha))^2 = \Delta$, d'où

$\sigma(\alpha) = \pm\sqrt{\Delta} = \pm\alpha$

La condition $\sigma(\alpha) = \alpha$ implique $\sigma = I$ (Identité sur K).

La condition $\sigma(\alpha) = -\alpha$ entraîne $\sigma(u + v\alpha) = u - v\alpha$

qui est effectivement un k - automorphisme de K appelé automorphisme de conjugaison γ . Comme on a $\gamma^2 = I$, le groupe G est isomorphe au groupe cyclique d'ordre 2 constitué par :

$$G = \{I, \gamma\}\ ,\ \gamma^2 = I.$$

Il est clair, par exemple d'après (2), que γ échange les deux racines x_1 et x_2 de l'équation .

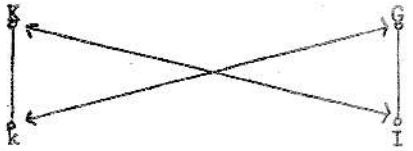
On a donc démontré le théorème suivant :

Théorème 2 . *Le groupe de GALOIS G d'une extension quadratique K de k est isomorphe au groupe cyclique d'ordre 2 constitué par les permutations sur les deux racines x_1 et x_2 de l'équation : la permutation identique et la transposition (x_1, x_2)*

Sous-corps de K contenant k et sous-groupes de G.

Sous-corps de K contenant k est (en particulier) un sous-espace vectoriel sur k contenant un espace vectoriel de dimension (1'espace

k = k.1) et contenu dans un espace vectoreil de dimension 2 (l'espace K). On a donc nécessairement k' = k ou k' = K.



Un sous-groupe G' de $G = \{I, \gamma\}$ est évidemment, soit l'identité, soit G lui-même.

Il en résulte le diagramme ci-contre.

avec les remarques suivantes qui établissent une correspondance binnivoque entre les sous-groupes de G et les sous-corps de K contenant k.

G = Gal (K,k) (définition 2)

k = Fix (K,G) (sous corps F de K constitué par les éléments fixes par tous les k - automorphismes de G. On a évidemment $k \subset F$ et $F \neq K$ puisque γ transforme α en $-\alpha$, d'où F = k)

I = Gal (K, K) car G ne laisse pas fixe α

K = Fix (K, I) évident

Exemples

Equation	Corps k	Racines	Corps K	Groupe G
$x^2 - 2x - 1 = 0$	$\mathbb{Q}$	$1 \pm \sqrt{2}$	$\mathbb{Q}(\sqrt{2})$	$\mathbb{Z}/2\mathbb{Z}$
$x^2 - 2x - 19 = 0$	$\mathbb{Q}$	$1 \pm 2\sqrt{5}$	$\mathbb{Q}(\sqrt{5})$	"
$x^2 + 1 = 0$	$\mathbb{Q}$	$\pm i$	$\mathbb{Q}(i)$	"
$x^2 + 1 = 0$	$\mathbb{R}$	$\pm i$	$\mathbb{R}(i) = \mathbb{C}$	"

Dans l'exemple d'une extension quadratique, le diagramme de la figure 3 est plutôt squelettique. Mais la définition 1 du corps de décomposition K d'une équation F (x) = o sur k, et la définition 2 d'un groupe de GALOIS de F sur k, se généralisent évidemment à un polynôme F quelconque. Voici deux exemples supplémentaires qui donnent lieu à une variété plus grande.

2. Deuxième exemple : L'équation $(x^2+1)(x^2-2) = 0$ sur $\mathbb{Q}$

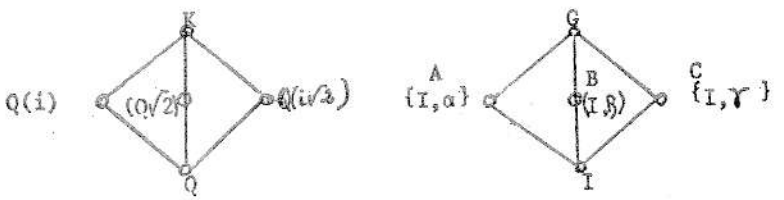
Je donne seulement les résultats, en renvoyant à G. BIRKHOFF et S. MACLANE [2], page 304, pour plus de détails.

$K = \mathbb{Q}(i, \sqrt{2})$ est un espace vectoriel de dimension 4 sur Q, de base $(1, i, \sqrt{2}, i\sqrt{2})$ sur Q.

$G = (I, \alpha, \beta, \gamma)$ est isomorphe au groupe de Klein dont la table de multiplication est ci-contre.

	I	α	β	γ
I	I	α	β	γ
α	α	I	γ	β
β	β	γ	I	α
γ	γ	β	α	I

Le diagramme des sous-corps de K contenant Q et des sous-groupes de G est le suivant :



avec la correspondance binnivoque

Q	Q(i)	Q(√2)	Q(i√2)	K
↕	↕	↕	↕	↕
G	A	B	C	I

qui est telle que : A = Gal (K, Q (i)), Q (i) = Fix (K, A) etc...

3. Troisième exemple . L'équation $x^4 - 3 = o$ sur Q

(vois G. BIRKHOFF et S. MACLANE 2 , page 306)

$K = Q(i, \sqrt[4]{3})$ est un espace vectoriel de dimension 8 sur Q, de base $(1, \alpha, \alpha^2, \alpha^3, i, i\alpha, i\alpha^2, i\alpha^3)$ avec $\alpha = \sqrt[4]{3}$.

G est un groupe non abélien d'ordre 8 isomorphe au groupe diédral du carré, c'est-à-dire au groupe des isométries du plan qui laissent globalement invariants les sommets d'un carré. (On pourra trouver une petite étude de ce groupe dans [7] chap. 9, exercice 10).

De plus, il existe une correspondance binnivoque décroissante entre les sous-corps de K contenant Q et les sous-groupes de G par les applications réciproques :

$$G' = G(k') = Gal(K, k'), \quad k' = Fix(K, G')$$

4. Les exemples précédents suffisent, je crois, pour donner une idée assez claire des résultats obtenus par GALOIS dans la théorie des équations algébriques. Les méthodes qu'il utilisait ne sont pas tout à fait celles qui sont présentées ici. Mais c'est bien à lui, comme le dit E. PICARD dans sa préface aux oeuvres de GALOIS publiées par l'Académie en 1897 et rééditées en 1951 [6], que "la gloire était réservée de montrer que, pour toute équation algébrique, il existe un groupe dans lequel se reflètent les propriétés essentielles de l'équation". Il a pu en outre démontrer, ce qui était le but de ses recherches, qu'une équation est résoluble par radicaux si et seulement si le groupe associé est résoluble (je m'adresse ici à ceux qui connaissent ces notions de pure théorie des groupes ; les autres peuvent faire confiance à GALOIS pour la beauté, la profondeur en même temps que la simplicité des propriétés mises en jeu). Enfin, en prouvant que le groupe associé à l'équation générale de degré n est le groupe symétrique $\mathfrak{S}_n$, et que celui-ci n'est pas résoluble pour $n \geq 5$, il donnait une réponse définitive pour l'impossibilité de la résolution par radicaux d'une équation générale de degré ≥ 5.

J'ajoute encore que la vie de ce génie est aussi intéressante que son oeuvre. (Voir par exemple une conférence que j'avais faite à Poitiers en 1963 et qui est publiée dans le bulletin de l'A.P.M. [8])

III - QUELQUES MOTS SUR LA CONJECTURE DE A. WEIL RESOLUE PAR P. DELIGNE

Avançons d'un siècle et demi pour arriver aux temps modernes et dire quelques mots sur la conjecture de A. WEIL résolue par P. DELIGNE (exposé de JP. SERRE au séminaire Bourbaki, février 1974). Il s'agit encore, comme vous allez voir, de théorie des équations albriques .

Maintenant on considère une équation algébrique sur un corps fini, par exemple le corps $F_p = Z/pZ$ qui a p éléments (p premier) ou plus généralement le corps F_q qui a $q = p^h$ éléments ; on cherche le nombre des solutions $(x_1, \ldots, x_n)$ dans F_q^n de l'équation :

(1) $f(x_1, \ldots, x_n) = 0$

où $f(X_1, \ldots, X_n) \in F_q[X_1, \ldots, X_n]$ est un polynôme à coefficients dans F_q. Des recherches avaient déjà été faites par GAUSS et JACOBI au siècle dernier pour le nombre de solutions de certaines congruences modulo p, au cours de ce siècle, par les arithméticiens HARDY et LITTLEWOOD (1922), DAVENPORT et HASSE (1935). Mais ce sont les méthodes de la géométrie algébrique introduites par A. WEIL (1949) [9] qui ont ouvert des voies nouvelles dans ce domaine. Elles consistent à considérer l'équation (1) comme celle d'une variété algébrique dans l'espace affine sur le corps F_q (ou plutôt sur sa clôture algébrique $\overline{F}_q$), et à chercher les points de cette variété appartenant à F_q^n. WEIL et quelques autres ont trouvé des résultats partiels et proposé des conjectures qui n'ont pu être démontrées que récemment par P. DELIGNE [5]. DELIGNE arrive à traiter non seulement le cas d'une équation, mais celui d'un système d'équations qui définissent dans l'espace projectif une variété algébrique V intersection complète sans point singulier de dimension. La formule donnée pour le nombre N des points dont les coordonnées appartiennent à F_q sur cette variété V, formule qu'il n'est pas question de reproduire ici, a pour conséquence l'inégalité suivante :

$$\left| N - (1 + q + \ldots + q^d \right| < B\, q^{d/2}$$

où B est un nombre de Betti définissant un caractère géométrique de la variété.

Pour terminer sur un exemple infiniment plus simple, on peut chercher les points dans F_q^2 du "cercle"

$$x_1^2 + x_2^2 = 1$$

(cf. E. ARTIN, algèbre géométrique, [1] ou, plus modestement, LESIEUR Géométrie, Cours de C_3 Sciences mathématiques, Orsay). Lorsque $p \neq 2$, On en trouve $q - 1$ dans le cas hyperbolique (c'est-à-dire lorsque (-1) est un carré dans F_q, ce qui équivaut à $q \equiv 1 \pmod 4$ et $q + 1$ dans le cas elliptique (c'est-à-dire lorsque (-1) n'est pas un carré dans F_q, ce qui équivaut à $q \equiv 3 \pmod 4$)

REFERENCES BIBLIOGRAPHIQUES

1. E. ARTIN — Algèbre géométrique Paris, Gauthier-Villars
2. B. BIRKHOFF et S. MACLANE — Algèbre, II, les grands théorèmes, Librairie Gauthier-Villars
3. N. BOURBAKI — Algèbre, Chapitre 1, librairie Hermann
4. N. BOURBAKI — Algèbre, chapitres 4 et 5, librairie Hermann.
5. P. DELIGNE — La conjecture de WEIL, I. Publ. Math. IHES, n° 43, P.U.F., 1974.
6. E. GALOIS — Oeuvres mathématiques, Paris, Gauthier-Villars 1897, nouvelle édition en 1951.
7. L. [illegible] Y. [illegible] J. LEFEBVRE Cl. JOULAIN — Algèbre linéaire et Géométrie, collection U, paraître.
8. L. LESIEUR — Evariste GALOIS, Bulletin de l'A.P.M. octobre 1963, n°232
9. A. WEIL — Number of solutions of équations infinite fields Bull. Amer. Math. Soc., 55 (1949) p. 497-[illegible]