

Boyer Pascal

**DE L'ARITHMÉTIQUE À LA
THÉORIE DES NOMBRES**

Boyer Pascal

DE L'ARITHMÉTIQUE À LA THÉORIE DES NOMBRES

Boyer Pascal

TABLE DES MATIÈRES

I. Arithmétique de \mathbb{Z}	5
I.1. Les entiers relatifs.....	5
I.1.1. Discrétion.....	5
I.1.2. Divisibilité.....	6
I.1.3. Sous-groupes de \mathbb{Z}	7
I.1.4. Plus grand diviseur commun.....	8
I.1.5. Le groupe $\mathbb{Z}/n\mathbb{Z}$: congruences.....	10
I.1.6. L'anneau $\mathbb{Z}/n\mathbb{Z}$: petit théorème de Fermat.....	11
I.2. Quelques preuves de la loi de réciprocité quadratique.....	13
I.2.1. Énoncés.....	13
I.2.2. Preuve d'Eisenstein.....	17
I.2.3. via le symbole de Zolotarev.....	19
I.2.4. en utilisant les résultants.....	21
I.2.5. via une équation diophantienne.....	22
I.2.6. par les sommes de Gauss.....	24
I.2.7. par la théorie de Galois.....	26
II. Nombres premiers	29
II.1. Comment produire des nombres premiers.....	29
II.1.1. Théorème de Dirichlet.....	29
II.1.2. Familles polynomiales.....	31
II.1.3. L'ensemble des nombres premiers n'est pas algébrique.....	32
II.1.4. L'ensemble des nombres premiers est diophantien.....	33
II.1.5. Autour du théorème de Wilson.....	36
II.2. Tests de primalité.....	38
II.2.1. Nombres de Fermat.....	38
II.2.2. Nombres de Mersenne.....	39
II.2.3. Autour du petit théorème de Fermat.....	40
II.2.4. AKS.....	43
II.2.5. Conjectures d'actualité sur les nombres premiers.....	47
III. Théorie des nombres	49
III.1. Théorie des corps.....	49

III.1.1. Généralités sur les extensions.....	49
III.1.2. Extensions algébriques et transcendantes.....	51
III.1.3. Nombres algébriques de degré d	54
III.1.4. Corps de rupture et corps de décomposition.....	56
III.2. Corps finis.....	60
III.2.1. Théorème de Wedderburn.....	61
III.2.2. Propriétés générales.....	63
III.2.3. Existence et unicité des corps finis : preuves constructives.....	64
III.3. Théorie de Galois.....	67
III.3.1. Extensions séparables.....	67
III.3.2. Extensions normales et galoisiennes.....	71
III.3.3. Correspondance de Galois.....	74
III.3.4. Extensions composées.....	76
III.4. Résolubilité par radicaux.....	79
III.4.1. Introduction historique.....	79
III.4.2. Groupe de Galois du polynôme $X^n - a$	80
III.4.3. Extensions résolubles.....	81
III.5. Calculer les groupes de Galois sur \mathbb{Q}	83
III.5.1. quand on voit les racines.....	83
III.5.2. comme sous-groupe de \mathfrak{S}_n	83
III.5.3. par spécialisation.....	84
III.5.4. Résolvantes.....	86
III.5.5. Théorie de Galois inverse.....	87
III.5.6. Cas d'un corps de fonctions en une variable.....	88

CHAPITRE I

ARITHMÉTIQUE DE \mathbb{Z}

I.1. Les entiers relatifs

I.1.1. Discrétion. — Une des premières remarques que l'on peut faire sur l'ensemble \mathbb{Z} des entiers relatifs est que *tout ensemble borné de \mathbb{Z} admet un plus petit et un plus grand élément*. Cette propriété n'est pas aussi anodine qu'il y paraît. Par exemple sur \mathbb{R} , elle n'est pas vraie mais peut être remplacée par la suivante : *tout ensemble borné admet une borne supérieure et une borne inférieure*.⁽¹⁾ En ce qui concerne \mathbb{Q} , l'ensemble des rationnels de valeur absolue inférieure à $\sqrt{2}$ est borné mais n'admet ni borne inférieure ni supérieure ; c'est d'ailleurs à partir de ce phénomène que l'on construit \mathbb{R} . Une deuxième propriété tout aussi simple et utile, est l'implication suivante :

$$0 \leq n < 1 \Rightarrow n = 0.$$

Malheureusement cette propriété ne se généralise pas aux anneaux d'entiers plus généraux, ce qui explique que dans la plupart de ces situations, on essaie de se ramener à \mathbb{Z} .

Remarque : les questions difficiles et subtiles d'arithmétique, et notamment la résolution des équations diophantiennes, consistent le plus souvent à utiliser l'implication précédente. Par exemple la quadrature du cercle qui consiste à montrer qu'on ne peut pas construire à la règle et au compas un carré de même aire qu'un cercle unité, repose sur le fait que *le nombre réel π est transcendant* dont la preuve repose sur la propriété précédente. La démonstration relativement complexe est donnée dans l'exercice ??, en attendant on propose de prouver l'énoncé suivant, dont la preuve est similaire à celle de la transcendance de π .

Proposition I.1.1. — *Le nombre réel π est irrationnel, i.e. $\pi \notin \mathbb{Q}$.*

Démonstration. — Soit D l'opérateur de dérivation sur les polynômes et on pose

$$\Delta = \sum_{k=0}^{+\infty} (-1)^k D^{2k}.$$

Remarquons tout d'abord que la somme est faussement infinie puisque pour tout polynôme P de degré inférieur ou égal à $2n$, on a $\Delta(P)(X) = P(X) - P''(X) + P^{(4)}(X) + \dots + (-1)^n P^{(2n)}(X)$. On remarque alors que pour tout x réel et pour tout polynôme $P(X) \in \mathbb{R}[X]$,

1. Pensez à l'exemple de $[0, 1[$.

on a l'égalité suivante de fonctions réelles :

$$P(x)\sin x = \left(\Delta(P')(x)\sin x - \Delta(P)(x)\cos x \right)'$$

de sorte que par intégration, on obtient la *formule d'Hermite*

$$\int_0^\pi P(x)\sin x dx = \Delta(P)(0) + \Delta(P)(\pi).$$

Supposons $\pi = a/b$ avec $a, b \in \mathbb{N}$ et considérons $P(x) = \frac{1}{n!}x^n(a - bx)^n$. Comme $P(x)\sin x$ est continue positive non identiquement nulle sur $[0, \pi]$, le réel $I_n = \int_0^\pi P(x)\sin x dx$ est strictement positif. Par ailleurs comme $x(a - bx) \leq a^2/4b$ sur $[0, \pi]$, on en déduit que $I_n \leq \frac{1}{n!}\pi\left(\frac{a^2}{4b}\right)^n$ et tend donc vers 0 lorsque n tend vers $+\infty$. Il existe donc un entier N tel que pour tout $n \geq N$, $0 < I_n < 1$ de sorte que I_n ne peut pas être un entier. Or notons que pour tout $0 \leq k < n$, $P^{(k)}(0) = P^{(k)}(\pi) = 0$ (utiliser soit la notion de multiplicité d'une racine d'un polynôme, ou la formule de dérivation de Liebnitz) et pour tout $k \geq n$, $P^{(k)}(0)$ et $P^{(k)}(\pi)$ sont des entiers positifs de sorte que $I_n = \Delta(P)(0) + \Delta(P)(\pi)$ aussi ce qui contredit ce qui précède et donc $\pi \notin \mathbb{Q}$. \square

I.1.2. Divisibilité. — Rappelons qu'un entier m divise un entier n s'il existe un entier q tel que $n = qm$. L'ensemble des diviseurs d'un entier n contient toujours ± 1 et $\pm n$; on peut ainsi distinguer ceux dont l'ensemble des diviseurs est de cardinal 4 ce qui nous conduit à la notion suivante :

Définition I.1.2. — Un entier $p > 1$ est dit premier⁽²⁾ si ses seuls diviseurs sont $\pm 1, \pm p$.

Remarque : dans un cadre plus général, on parle plutôt d'élément irréductible, cf. la définition ??.

Proposition I.1.3. — *Tout entier $n \geq 2$ est divisible par un nombre premier; il peut alors s'écrire comme un produit de nombres premiers.*

Remarque : cette propriété se généralise aux anneaux d'entiers, en revanche l'unicité de l'écriture que nous étudierons plus tard est plus rare.

Démonstration. — On procède par récurrence sur n ; le cas $n = 2$ est vrai car 2 est premier, supposons donc la proposition vérifiée pour tout $k < n$ et montrons qu'elle l'est pour n . Si n est premier c'est clair et sinon il existe un diviseur a de n avec $1 < a < n$ qui, d'après l'hypothèse de récurrence, possède un diviseur premier qui divise n . Le deuxième point se montre exactement de la même manière. \square

Nous noterons alors \mathcal{P} l'ensemble des nombres premiers; la question naturelle est alors de savoir si \mathcal{P} est fini ou pas.

Théorème I.1.4. — (**Euclide**) *L'ensemble \mathcal{P} des nombres premiers est infini.*

Démonstration. — Raisonnons par l'absurde et supposons que $p_1, \dots, p_r = n$ sont les seuls nombres premiers; soit alors $N = n! + 1$, (ou bien $N = (\prod_{p \leq n} p) + 1$). Comme $N > n$ alors N n'est pas premier et possède donc un diviseur premier p qui est donc $\leq n$ de sorte que $p|n!$ et donc aussi $N - n! = 1$ d'où la contradiction. \square

2. Pour ceux qui préfèrent une définition plus imagée, selon Paul Erdős, « un nombre premier est un nombre qui ne se casse pas quand on le laisse tomber par terre »

Remarque : nous verrons par la suite d'autres preuves de ce résultat. On peut par ailleurs se demander s'il l'ensemble des premiers de la forme $n! \pm 1$ est infini : à ce jour le résultat n'est pas connu. De la même façon on peut se demander si les nombres premiers de la forme $(\prod_{p \ni q \leq p} q) \pm 1$ sont en nombre infini : à nouveau la réponse n'est pas connue.

Quand deux entiers n et $m \geq 0$ ne se divisent pas, on peut tout de même leur associer un couple de nombres (q, r) via la notion de *division euclidienne*.

Proposition I.1.5. — *Pour tout $n, m \geq 0$, il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que*

$$n = qm + r \text{ et } 0 \leq r < |m|.$$

L'entier q est le quotient et r le reste de la division euclidienne de n par m .

Démonstration. — Commençons par l'unicité : $mq + r = mq' + r'$ avec $0 \leq r, r' < |m|$ de sorte que $|m| \cdot |q - q'| = |r - r'| < |m|$ et donc $q = q'$ puis $r = r'$. En ce qui concerne l'existence, considérons l'ensemble $A = \{n - km : k \in \mathbb{Z}\} \cap \mathbb{N}$ qui est clairement non vide. Notons $r \geq 0$ son plus petit élément avec $n = mq + r$. Si on avait $r \geq |m|$ alors $0 \leq r - |m| = n - m(q \pm 1) \in A$ ce qui contredit la minimalité de r . \square

Remarque : l'unicité dans la division euclidienne est en général une anomalie et n'a en fait que peu d'intérêt. Signalons tout de même qu'elle permet d'écrire tout entier naturel n de manière unique sous la forme

$$n = \sum_{k=0}^{+\infty} a_k b^k$$

où les a_k sont des entiers positifs $< b$ presque tous nuls. En effet on effectue la division euclidienne de $n = bq_0 + a_0$ par b , puis celle de $q_0 = bq_1 + a_1$ et ainsi de suite ce qui donne l'existence. Pour l'unicité, on reprend la preuve de l'unicité de la division euclidienne.

I.1.3. Sous-groupes de \mathbb{Z} . — Le corollaire suivant nous fournit une manière élégante et plus savante d'utiliser le fait qu'un sous-ensemble minoré de \mathbb{Z} admet un plus petit élément ; il suffit pour cela de considérer des sous-groupes et de prendre son générateur positif comme le justifie l'énoncé suivant.

Corollaire I.1.6. — *Les sous-groupes de \mathbb{Z} sont les $n\mathbb{Z}$.*

Démonstration. — Soit H un sous-groupe de \mathbb{Z} non réduit à $\{0\}$ et notons $A = H \cap \mathbb{N}^*$ qui est donc non vide, car si $h \in H$ alors $-h \in H$. Notons n le plus petit élément de A ; soit $h \in H$; on considère la division euclidienne $h = qn + r$ de h par n avec donc $0 \leq r = h - qn < n$ qui appartient à $H \cap \mathbb{N}$ et est donc nul par minimalité de n . Ainsi donc $H \subset n\mathbb{Z}$ et l'inclusion réciproque est évidente. \square

Lemme I.1.7. — *(d'Euclide) Soit p premier divisant ab ; alors p divise a ou b .*

Démonstration. — Supposons que p ne divise pas a ; soit alors $A = \{n \in \mathbb{Z} : p|an\}$ qui est un sous-groupe de \mathbb{Z} non réduit à $\{0\}$ car $p, b \in A$. D'après le corollaire précédent $A = m\mathbb{Z}$ avec donc $m|p \in A$ et donc $A = p\mathbb{Z}$ de sorte, comme $b \in A$, $p|b$, d'où le résultat. \square

Théorème I.1.8. — *(Factorialité de \mathbb{Z}) Tout entier $n \geq 2$ s'écrit de manière unique sous la forme*

$$n = p_1^{n_1} \cdots p_r^{n_r},$$

où les n_i sont des entiers naturels non nuls, et où les p_i sont des nombres premiers.

Démonstration. — L'existence découle de la proposition I.1.3 en regroupant les facteurs. En ce qui concerne l'unicité supposons que l'on ait $n = p_1^{n_1} \cdots p_r^{n_r} = q_1^{m_1} \cdots q_s^{m_s}$ où les p_i, q_j sont premiers. D'après le lemme d'Euclide q_j est égal à l'un des p_i de sorte que $\{p_1, \dots, p_r\} = \{q_1, \dots, q_s\}$ et donc $r = s$. Supposons $n_1 < m_1$ alors en divisant n par $p_1^{n_1}$, on obtient que p_1 divise $p_2^{n_2} \cdots p_r^{n_r}$ ce qui contredit le lemme d'Euclide, d'où le résultat en raisonnant de même pour les autres indices. \square

Définition I.1.9. — Soit p un nombre premier ; pour $n \in \mathbb{Z}$, la valuation p -adique de n est le plus grand entier k tel que p^k divise n de sorte que

$$n = \prod_{p \in \mathcal{P}} p^{v_p(n)}.$$

Deux entiers n et m sont dits premiers entre eux si pour tout $p \in \mathcal{P}$, $v_p(n) \cdot v_p(m) = 0$.

Remarque : la valuation p -adique permet de définir une norme ultramétrique sur \mathbb{Q} par la formule $|a/b|_p = p^{v_p(b) - v_p(a)}$; comme on a construit \mathbb{R} à partir de \mathbb{Q} et de la valeur absolue, on peut alors construire la complétion \mathbb{Q}_p de \mathbb{Q} pour $|\cdot|_p$.

Lemme I.1.10. — (*de Gauss*) Soient $a, b, c \in \mathbb{Z}$ tels que a divise bc avec a premier avec b ; alors a divise c .

Démonstration. — Il s'agit donc de montrer que pour tout $p \in \mathcal{P}$, $v_p(a) \leq v_p(c)$. Si $v_p(a) = 0$ c'est clair ; supposons donc $v_p(a) \geq 1$ auquel cas $v_p(b) = 0$ et le résultat découle alors du fait que $v_p(a) \leq v_p(bc) = v_p(b) + v_p(c)$. \square

Remarque : si a et b sont premiers entre eux et divisent c alors ab divise c ; en effet on a $c = au$ avec d'après le lemme de Gauss b qui divise u . On notera bien que l'hypothèse est nécessaire puisque $a = b = 2$ divise $c = 2$ mais que 4 ne divise pas 2.

Application : soit p un nombre premier et $1 \leq k \leq p - 1$; alors p divise $\binom{p}{k}$. En effet on a $k! \binom{p}{k} = p(p-1) \cdots (p-k+1)$ et comme p est premier avec $k!$ il divise donc $\binom{p}{k}$.

I.1.4. Plus grand diviseur commun. —

Définition I.1.11. — Pour $a, b \in \mathbb{Z}$, on note

$$a \wedge b = \prod_{p \in \mathcal{P}} p^{\min\{v_p(a), v_p(b)\}}, \quad a \vee b = \prod_{p \in \mathcal{P}} p^{\max\{v_p(a), v_p(b)\}}.$$

Remarque : comme $\min\{v_p(a), v_p(b)\} + \max\{v_p(a), v_p(b)\} = v_p(a) + v_p(b)$, on en déduit que $(a \wedge b) \cdot (a \vee b) = ab$.

Proposition I.1.12. — L'entier $a \wedge b$ (resp. $a \vee b$) est le plus grand diviseur (resp. petit multiple) commun de a et b que l'on appelle encore le pgcd (resp. ppcm) de a et de b .

Démonstration. — Comme pour tout $p \in \mathcal{P}$, $\min\{v_p(a), v_p(b)\} \leq v_p(a), v_p(b)$, on en déduit que $a \wedge b$ est un diviseur de a et de b . Par ailleurs si d divise a et b alors pour tout $p \in \mathcal{P}$, $v_p(d) \leq \min\{v_p(a), v_p(b)\}$ de sorte que d divise $a \wedge b$, d'où le résultat. Le cas du ppcm se montre de la même façon. \square

Remarque : a et b sont premiers entre eux au sens de la définition I.1.9 si et seulement si leur pgcd est égal à 1. Par ailleurs les entiers $\frac{a}{a \wedge b}$ et $\frac{b}{a \wedge b}$ sont premiers entre eux.

On vérifie aisément que $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$; en ce qui concerne $a \wedge b$, on a le résultat suivant qui donne une autre caractérisation du pgcd.

Proposition I.1.13. — *Le sous-groupe de \mathbb{Z} engendré par a et b est $(a \wedge b)\mathbb{Z}$.*

Démonstration. — Notons n l'entier naturel tel que $n\mathbb{Z}$ est le groupe engendré par a et b ; comme a et b appartiennent à $n\mathbb{Z}$, on en déduit que $n|a$ et $n|b$ et donc $n|a \wedge b$. En outre n s'écrit sous la forme $ua + vb$ de sorte que $a \wedge b|ua + vb = n$ d'où le résultat. \square

Remarque : on déduit de la proposition précédente le **théorème de Bézout**, i.e. il existe des entiers relatifs u, v tels que $a \wedge b = ua + vb$.

Que ce soit pour calculer $a \wedge b$ où les coefficients u, v d'une relation de Bézout, il n'est pas nécessaire de calculer la factorisation en facteurs premiers de a et b , on dispose heureusement de l'*algorithme d'Euclide* : on pose $r_0 = a$ et $r_1 = b$. On construit alors par récurrence r_{i+1} comme le reste de la division euclidienne de r_{i-1} par r_i si ce dernier est non nul et sinon $r_{i+1} = 0$. Comme la suite est strictement décroissante et positive, il existe un indice $n \geq 1$ tel que $r_n > 0$ et $r_{n+1} = 0$. On pose par ailleurs

$$u_0 = 1, \quad u_1 = 0 \text{ et } v_0 = 0, \quad v_1 = 1,$$

$$u_{i+1} = u_{i-1} - u_i q_i \text{ et } v_{i+1} = v_{i-1} - v_i q_i$$

où pour tout $i = 1, \dots, n-1$, q_i est le quotient de la division euclidienne de r_{i-1} par r_i .

Proposition I.1.14. — *L'entier r_n est alors le pgcd de a et b avec $r_n = au_n + bv_n$.*

Démonstration. — Comme $r_{i-1} = q_i r_i + r_{i+1}$, alors $r_{i-1} \wedge r_i = r_i \wedge r_{i+1}$ et donc $a \wedge b = r_{n-1} \wedge r_n = r_n$ car $r_{n+1} = 0$. En ce qui concerne la relation de Bézout, il suffit de vérifier que pour tout $i = 1, \dots, n$, on a $r_i = au_i + bv_i$. C'est clairement vrai pour $i = 0, 1$ et supposons que pour $1 \leq k < n$, la relation soit vraie pour tout $i \leq k$. On a alors

$$r_{k+1} = r_{k-1} - q_k r_k = (u_{k-1}a + v_{k-1}b) - q_k(u_k a + v_k b) = au_{k+1} + bv_{k+1}$$

d'où le résultat. \square

Remarque : Lamé a montré que si l'algorithme d'Euclide s'arrête au bout de n pas alors

$$a \geq (a \wedge b)F_{n+2}, \quad b \geq (a \wedge b)F_{n+1}$$

où $F_0 = 0$, $F_1 = 1$ et $F_{n+1} = F_n + F_{n-1}$ est la suite de Fibonacci. Pour le montrer on raisonne par récurrence sur n , le cas $n = 1$ étant trivial; le premier pas transforme (a, b) en $(b, c = a - qb)$ avec donc par hypothèse de récurrence $b \geq a \wedge b F_{n+1}$ et $c \geq a \wedge b F_n$ et donc $a \geq b + c \geq a \wedge b(F_n + F_{n+1}) = a \wedge b F_{n+2}$. On notera en particulier que le cas le pire est pour le couple (F_{n+1}, F_n) .

Résolution de l'équation $ax + by = c$: si c n'est pas divisible par $a \wedge b$ l'équation n'a pas de solution; sinon en divisant cette équation par $a \wedge b$, on se ramène au cas où a et b sont premiers entre eux. Considérons alors une relation de Bézout $au_0 + bv_0 = 1$; si $au + bv = 1$ est une autre relation de Bézout, on a alors $a(u - u_0) = b(v_0 - v)$ de sorte que d'après le lemme de Gauss il existe q tel que $u = u_0 + qb$ et $v = v_0 - qa$. Les solutions (x, y) s'obtiennent alors de la même manière à partir d'une solution particulière $(x_0, y_0) = (cu_0, cv_0)$ et donc $(x, y) = (x_0 + qb, y_0 - qa)$. En ce qui concerne les solutions positives, on renvoie à l'exercice ??.

I.1.5. Le groupe $\mathbb{Z}/n\mathbb{Z}$: congruences. —

Définition I.1.15. — Pour $n \in \mathbb{Z}$, on munit \mathbb{Z} de la relation d'équivalence suivante :

$$x \sim_n y \Leftrightarrow n|x - y$$

et on note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence. On notera \bar{x} la classe associée à $x \in \mathbb{Z}$, i.e. $\bar{x} = \{x + kn : k \in \mathbb{Z}\}$, de sorte que $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$. Deux éléments x, y d'une même classe seront dits congrus modulo n et on le notera sous la forme $x \equiv y \pmod{n}$.

Remarque : l'addition de \mathbb{Z} munit l'ensemble $\mathbb{Z}/n\mathbb{Z}$ d'une structure de groupe; en effet soit \bar{x}, \bar{y} deux classes d'équivalence, on définit alors $\bar{x} + \bar{y} = \overline{x_0 + y_0}$ où x_0 et y_0 sont des éléments quelconques de \bar{x} et \bar{y} respectivement. Le fait, trivial mais primordial, est que le résultat $\overline{x_0 + y_0}$ ne dépend pas du choix de x_0 et y_0 . On notera

$$\varphi : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$$

la surjection dite canonique qui à un entier x associe sa classe d'équivalence \bar{x} .

Remarque : tout groupe cyclique de cardinal n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$; en effet soit $G = \langle g \rangle$ et considérons le morphisme $f : \mathbb{Z} \rightarrow G$ qui à 1 associe g . Par définition le noyau de f est $n\mathbb{Z}$ de sorte que f induit un isomorphisme $\bar{f} : \mathbb{Z}/n\mathbb{Z} \simeq G$.

Proposition I.1.16. — *Tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ est de cardinal d où d est un diviseur de n . Réciproquement pour tout $d|n$, il existe un unique sous-groupe d'ordre d de $\mathbb{Z}/n\mathbb{Z}$ qui est isomorphe à $\mathbb{Z}/d\mathbb{Z}$.*

Démonstration. — Le premier point est un cas particulier du théorème de Lagrange. Réciproquement soit H un sous-groupe de $G = \mathbb{Z}/n\mathbb{Z}$; considérons et $\phi : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \rightarrow G/H$, où G/H est le groupe quotient de G par H . Le noyau de ϕ est un sous-groupe de \mathbb{Z} donc de la forme $d\mathbb{Z}$, contenant $\text{Ker } \varphi = n\mathbb{Z}$, de sorte que d divise n . Ainsi H est cyclique, engendré par la classe de d ; son ordre est n/d . \square

Corollaire I.1.17. — *Le groupe engendré par un élément $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$ est le groupe engendré par $k \wedge n$; il est de cardinal $\frac{n}{n \wedge k}$.*

Démonstration. — Comme k est un multiple de $k \wedge n$, on a l'inclusion $(k) \subset (k \wedge n)$. Réciproquement on écrit une relation de Bezout $uk + vn = n \wedge k$ de sorte que modulo n , $n \wedge k$ appartient au groupe engendré par k et donc $(k \wedge n) \subset (k)$. On en déduit alors que l'ordre de k dans $\mathbb{Z}/n\mathbb{Z}$ qui est par définition le cardinal du groupe engendré par k , est $\frac{n}{n \wedge k}$. \square

Remarque : un élément $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$ est un générateur si et seulement si $k \wedge n = 1$; on notera $\varphi(n)$ le cardinal de l'ensemble des générateurs de $\mathbb{Z}/n\mathbb{Z}$, et donc aussi le cardinal des $1 \leq k \leq n$ premiers avec n .

Corollaire I.1.18. — *L'ensemble des éléments d'ordre $d|n$ (resp. d'ordre divisant d) dans $\mathbb{Z}/n\mathbb{Z}$ est de cardinal $\varphi(d)$ (resp. d). Par ailleurs on a $n = \sum_{d|n} \varphi(d)$.*

Démonstration. — Remarquons tout d'abord que si d ne divise pas n , il n'y a aucun élément d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$. Si d divise n , tous les éléments d'ordre d appartiennent au groupe engendré par $(\frac{n}{d})$ qui est isomorphe, en tant que groupe cyclique d'ordre d , à $\mathbb{Z}/d\mathbb{Z}$. Ainsi les éléments d'ordre d de $\mathbb{Z}/n\mathbb{Z}$ sont en bijection avec les éléments d'ordre d de $\mathbb{Z}/d\mathbb{Z}$ qui sont en nombre $\varphi(d)$.

Cherchons maintenant les éléments d'ordre divisant d dans $\mathbb{Z}/n\mathbb{Z}$ qui sont donc d'ordre divisant $d \wedge n$ et qui appartiennent au groupe engendré par $\frac{n}{n \wedge d}$ isomorphe à $\mathbb{Z}/(n \wedge d)\mathbb{Z}$. Ainsi, comme précédemment, les éléments d'ordre divisant d de $\mathbb{Z}/n\mathbb{Z}$ sont en bijection avec les éléments d'ordre divisant $n \wedge d$ de $\mathbb{Z}/(n \wedge d)\mathbb{Z}$, qui sont en nombre $n \wedge d$.

La dernière égalité découle du dénombrement des éléments de $\mathbb{Z}/n\mathbb{Z}$ selon leur ordre. \square

Théorème I.1.19. — (*chinois*) Soient n et m des entiers premiers entre eux ; l'application $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ qui à un entier k associe sa classe modulo n et m , induit un isomorphisme

$$\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Démonstration. — Considérons tout d'abord un élément k du noyau de sorte que n et m divise k et comme $n \wedge m = 1$, d'après le lemme de Gauss $nm|k$. Ainsi le noyau est contenu dans $nm\mathbb{Z}$, l'inclusion réciproque étant évidente de sorte que l'on a une injection de $\mathbb{Z}/nm\mathbb{Z} \hookrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ qui est un isomorphisme par égalité des cardinaux. \square

Remarque : il peut être utile de savoir déterminer un antécédent d'un couple $(\bar{a}, \bar{b}) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Pour cela on part d'une relation de Bézout $un + vm = 1$ et on pose $k = un\bar{b} + vma$; on vérifie aisément que comme $un \equiv 1 \pmod{m}$ et $vm \equiv 1 \pmod{n}$, on a $k \equiv a \pmod{n}$ et $k \equiv b \pmod{m}$.

Remarque : dans le cas où $n \wedge m = d$, le raisonnement précédant donne que le noyau est $n \vee m\mathbb{Z}$. L'image est clairement contenue dans

$$\{(a, b) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} : d|a - b\}.$$

L'égalité des cardinaux nous que l'image est exactement l'ensemble ci-dessus. Un antécédent explicite se calcule comme précédemment à l'aide d'une relation de Bézout $d = uan + vm$ avec $x = b + \frac{a-b}{d}vm$.

I.1.6. L'anneau $\mathbb{Z}/n\mathbb{Z}$: petit théorème de Fermat. — L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est aussi muni d'une structure d'anneau déduite de celle de \mathbb{Z} ; on note $(\mathbb{Z}/n\mathbb{Z})^\times$ le groupe multiplicatif de $\mathbb{Z}/n\mathbb{Z}$, i.e. l'ensemble des éléments inversibles muni de la multiplication.

Proposition I.1.20. — Un élément $k \in \mathbb{Z}/n\mathbb{Z}$ appartient à $(\mathbb{Z}/n\mathbb{Z})^\times$ si et seulement s'il est un générateur additif de $\mathbb{Z}/n\mathbb{Z}$. En particulier $(\mathbb{Z}/n\mathbb{Z})^\times$ est de cardinal $\varphi(n)$.

Démonstration. — Par définition k est inversible si et seulement s'il existe k' tel que $kk' \equiv 1 \pmod{n}$, i.e. s'il existe $\lambda \in \mathbb{Z}$ tel que $kk' + \lambda n = 1$ ce qui est équivalent à $k \wedge n = 1$ et donc k est un générateur de $\mathbb{Z}/n\mathbb{Z}$. \square

Remarque : comme $\mathbb{Z}/n\mathbb{Z}$ est monogène tout morphisme de source $\mathbb{Z}/n\mathbb{Z}$ est déterminé par l'image de $\bar{1}$ de sorte qu'en particulier le groupe $\text{aut}(\mathbb{Z}/n\mathbb{Z})$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^\times$.

Corollaire I.1.21. — L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si $n = p$ est premier auquel cas on le notera \mathbb{F}_p .

Théorème I.1.22. — (*de Fermat*) Pour tout $n \in \mathbb{Z}$ et $k \wedge n = 1$, on a $k^{\varphi(n)} \equiv 1 \pmod{n}$.

Démonstration. — Nous avons vu que le cardinal de $(\mathbb{Z}/n\mathbb{Z})^\times$ est égal à $\varphi(n)$ et comme l'ordre d'un élément divise le cardinal du groupe, l'ordre de k divise $\varphi(n)$ et donc $k^{\varphi(n)} \equiv 1 \pmod{n}$. \square

Proposition I.1.23. — Pour $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, on a

$$\varphi(n) = \prod_{i=1}^r p_i^{\alpha_i-1} (p_i - 1).$$

Démonstration. — Le théorème chinois donne un isomorphisme

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod_{i=1}^r (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times;$$

le résultat découle alors du fait que le cardinal des $1 \leq k \leq p^\alpha$ divisible par p est de cardinal $p^{\alpha-1}$ et donc $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$. \square

Nous allons à présent étudier la structure de groupe des $(\mathbb{Z}/n\mathbb{Z})^\times$ ce qui, d'après le lemme chinois, revient à décrire les $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$. Commençons par le cas où $\alpha = 1$ qui est un cas particulier du théorème suivant.

Théorème I.1.24. — Soit K un corps commutatif et G un sous-groupe fini de K^\times ; alors G est un groupe cyclique.

Démonstration. — Notons n le cardinal de G et $P(X) = X^n - 1 \in K[X]$; comme K est un corps (commutatif) alors P admet au plus n racines dans K et comme, d'après le théorème de Lagrange, les n éléments de G sont des racines, P est totalement décomposé à racines distinctes dans K . Pour d un diviseur de n , de l'égalité

$$X^n - 1 = (X^d - 1) \left(\sum_{i=0}^{\frac{n}{d}-1} X^{id} \right)$$

on en déduit que $X^d - 1$ est aussi totalement décomposé. Ainsi pour $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ la décomposition en facteurs premiers de n , il existe pour tout $i = 1, \dots, r$ un élément de G d'ordre $p_i^{\alpha_i}$, i.e. une racine de $X^{p_i^{\alpha_i}} - 1$ qui n'est pas racine de $X^{p_i^{\alpha_i-1}} - 1$. Le résultat découle alors du lemme suivant. \square

Remarque : en utilisant la structure de \mathbb{Z} -module de type fini, on peut écrire $G \simeq \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_r\mathbb{Z}$ avec $a_1 | \cdots | a_r$. En particulier tout élément de G est d'ordre divisant a_r de sorte que $X^{a_r} - 1$ aurait $\prod_{i=1}^r a_i$ racines. Comme ce nombre de racines est inférieur à a_r on en déduit que $r = 1$, d'où le résultat.

Lemme I.1.25. — Soient G un groupe commutatif fini, $x, y \in G$ d'ordres respectifs a et b . Si a et b sont premiers entre eux alors xy est d'ordre ab .

Démonstration. — D'après le théorème de Lagrange $H = \langle x \rangle \cap \langle y \rangle$ est d'ordre un diviseur de a et b et donc d'ordre 1. Comme $xy = yx$ on a $(xy)^{ab} = (x^a)^b (y^b)^a = 1$. Réciproquement si $(xy)^n = 1$ alors $x^n = y^{-n} \in H = \{1_G\}$ et donc $a|n$ et $b|n$ soit, comme $a \wedge b = 1$, $ab|n$ ce qui finit de prouver que xy est d'ordre ab . \square

Proposition I.1.26. — (i) Pour p premier impair et $m \geq 1$, $(\mathbb{Z}/p^m\mathbb{Z})^\times$ est cyclique.

(ii) Pour $p = 2$ et $m \geq 2$, on a $(\mathbb{Z}/2^m\mathbb{Z})^\times \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{m-2}\mathbb{Z})$.

Commençons par établir une congruence utile.

Lemme I.1.27. — Soit $k \geq 0$ alors

- (i) si p est un premier impair alors $(1+p)^{p^k} \equiv 1 + p^{k+1} \pmod{p^{k+2}}$;
(ii) $(1+4)^{2^k} \equiv 1 + 2^{k+2} \pmod{2^{k+3}}$.

Démonstration. — Le résultat découle simplement par récurrence de l'observation suivante : les coefficients binomiaux $\binom{p}{i}$ étant divisibles par p pour $0 < i < p$, une congruence $a \equiv b \pmod{p^k}$ implique que $a^p \equiv b^p \pmod{p^{k+1}}$. \square

Démonstration. — (de la proposition)

Le cas (ii) du lemme précédent assure que la classe de 5 est d'ordre 2^{m-2} dans $(\mathbb{Z}/2^m\mathbb{Z})^\times$. Vérifions alors que le morphisme de groupes

$$\mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/2^{m-2}\mathbb{Z}) \longrightarrow (\mathbb{Z}/2^m\mathbb{Z})^\times$$

donné par $(p, q) \mapsto (-1)^p 5^q \pmod{2^m}$ est un isomorphisme ; comme les cardinaux sont égaux il suffit en fait de montrer qu'il est injectif. Si $(-1)^p 5^q \equiv 1 \pmod{2^m}$ alors modulo 4 il vient $p \equiv 0 \pmod{2}$. Ainsi on a $5^q \equiv 1 \pmod{2^m}$ et donc $q \equiv 0 \pmod{2^{m-2}}$, ce qui finit de prouver le cas (ii).

Considérons à présent le cas où p est impair. Le cas (i) du lemme précédent nous fournit que $1+p$ est d'ordre p^{m-1} modulo p^m . Soit alors $a \in \mathbb{Z}$ dont l'image dans $(\mathbb{Z}/p\mathbb{Z})^\times$ soit un générateur, i.e. soit d'ordre $p-1$. Ainsi l'ordre d de a dans $(\mathbb{Z}/p^m\mathbb{Z})^\times$ est divisible par $p-1$ et $b := a^{\frac{d}{p-1}}$ est d'ordre $p-1$ dans $(\mathbb{Z}/p^m\mathbb{Z})^\times$. Comme $(p-1) \wedge p = 1$, il résulte du lemme I.1.25 que $a(1+p)$ est d'ordre $(p-1)p^{m-1}$ et donc que $(\mathbb{Z}/p^m\mathbb{Z})^\times$ est cyclique. \square

Corollaire I.1.28. — Soit p un nombre premier impair et n un entier divisant $p-1$. Alors $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ est une puissance n -ième si et seulement si $a^{\frac{p-1}{n}} = 1$.

Remarque : c'est une sorte de critère d'Euler généralisé.

Démonstration. — Si $a = b^n$ avec $b \in (\mathbb{Z}/p\mathbb{Z})^\times$, alors comme $b^{p-1} = 1$ on obtient bien $a^{\frac{p-1}{n}} = 1$. Réciproquement pour b un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$, on a $a = b^k$ avec $b^{k\frac{p-1}{n}} = 1$ et donc $p-1$ divise $k\frac{p-1}{n}$ soit n divise k et donc $a = (b^{k/n})^n$. \square

Définition I.1.29. — Un entier a dont la classe dans $\mathbb{Z}/n\mathbb{Z}$ engendre $(\mathbb{Z}/n\mathbb{Z})^\times$ est appelée une racine primitive modulo n .

Remarque : si p est un nombre premier de Sophie Germain, i.e. de la forme $p = 2q + 1$ avec q premier alors $a \neq \pm 1$ est un générateur si et seulement si $a^q \neq 1$ et donc égal à -1 .

Remarque : modulo tout nombre premier impair p , il existe des racines primitives modulo p . Une conjecture célèbre due à E. Artin affirme que : *tout entier $a \neq -1$ qui n'est pas un carré, est une racine primitive modulo p pour une infinité de nombres premiers p .*

I.2. Quelques preuves de la loi de réciprocité quadratique

I.2.1. Énoncés. — On dit qu'un élément $a \in \mathbb{F}_p$ est un carré s'il existe $b \in \mathbb{F}_p$ tel que $a = b^2$.

Définition I.2.1. — Pour $p \geq 3$ premier, le symbole de Legendre $\left(\frac{n}{p}\right)$ est défini par :

$$\left(\frac{n}{p}\right) = \begin{cases} 0 & \text{si } p \text{ divise } n \\ +1 & \text{si } n \text{ est un carré dans } \mathbb{F}_p \\ -1 & \text{sinon} \end{cases}$$

Remarque : l'application $x \in \mathbb{F}_p^\times \mapsto x^2 \in \mathbb{F}_p^\times$ est un morphisme de groupe multiplicatif, dont le noyau est $\{-1, 1\}$ et donc de cardinal 2 ; ainsi son image qui est l'ensemble $\mathbb{F}_p^{\times 2}$ des carrés de \mathbb{F}_p^\times est de cardinal $(p-1)/2$. En particulier on interprète la restriction du symbole de Legendre à \mathbb{F}_p^\times au morphisme naturel

$$\mathbb{F}_p^\times \longrightarrow \mathbb{F}_p^\times / \mathbb{F}_p^{\times 2} \simeq \{\pm 1\}.$$

On en déduit alors la multiplicativité du symbole de Legendre, i.e.

$$\forall a, b \in \mathbb{Z}, \quad \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Application : pour tout nombre premier impair p , on a

$$\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) = 0.$$

Lemme I.2.2. — (*Critère d'Euler*) Soit p un nombre premier ; pour tout $n \in \mathbb{Z}$, on a

$$\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \pmod{p}.$$

Démonstration. — Remarquons déjà que la congruence est vraie si p divise n . Supposons donc que p ne divise pas n et donc que l'image de n modulo p appartient à \mathbb{F}_p^\times . D'après le petit théorème de Fermat, pour tout $x \in \mathbb{F}_p^\times$, on a $x^{p-1} = 1$ et donc $x^{(p-1)/2} = \pm 1$ pour tout $x \in \mathbb{F}_p^{\times 2}$. Ainsi si $x \in \mathbb{F}_p^{\times 2}$, x est une solution de l'équation $X^{(p-1)/2} = 1$ laquelle dans \mathbb{F}_p possède au plus $(p-1)/2$ solutions. Ainsi d'après la remarque précédente, $\mathbb{F}_p^{\times 2}$ est exactement égal à l'ensemble des racines de l'équation $X^{(p-1)/2} = 1$ dans \mathbb{F}_p et $\left(\frac{n}{p}\right) \equiv n^{(p-1)/2} \pmod{p}$. \square

Application : pour p un nombre premier impair, on a

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Le calcul explicite des symboles de Legendre se fait alors à partir de l'application précédente, du lemme de Gauss et de la loi de réciprocité quadratique.

Lemme I.2.3. — (*de Gauss*) Pour tout p premier impair on a $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

Démonstration. — Soit A l'anneau quotient $\mathbb{F}_p[X]/(X^4 + 1)$. L'application $\mathbb{F}_p \rightarrow A$ qui à λ associe sa classe dans A , est un morphisme injectif d'anneaux, donc A contient un sous-anneau isomorphe à \mathbb{F}_p . En particulier, A est de caractéristique p , i.e. $p1_A = 0$, et donc le noyau du morphisme $\mathbb{Z} \rightarrow A$ qui à n associe $n1_A$ est $p\mathbb{Z}$.

Soit α la classe de X modulo $(X^4 + 1)$; c'est un élément inversible de A . Posons $y = \alpha + \alpha^{-1} \in A$. On a $\alpha^4 + 1 = 0$, d'où $\alpha^2 + \alpha^{-2} = 0$, puis $y^2 = 2$. Par ailleurs, A étant de caractéristique p , on a

$$y^p = \alpha^p + \alpha^{-p}.$$

Supposons $p \equiv \pm 1 \pmod{8}$. L'égalité $\alpha^8 = 1$ entraîne alors $y^p = y$. Puisque p est impair, 2 est inversible dans A , et l'égalité $y^2 = 2$ entraîne qu'il en est de même de y . On en déduit que l'on a $y^{p-1} = 1$. Par suite, on obtient dans A les égalités

$$2^{\frac{p-1}{2}} = (y^2)^{\frac{p-1}{2}} = y^{p-1} = 1.$$

D'après le critère d'Euler, on a

$$\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \pmod{p},$$

d'où il résulte que l'on a $\left(\frac{2}{p}\right) = 1$.

Supposons $p \equiv \pm 5 \pmod{8}$. Dans ce cas, on a

$$y^p = \alpha^5 + \alpha^{-5} = -(\alpha + \alpha^{-1}) = -y.$$

On a donc $y^{p-1} = -1$, ce qui entraîne par le même argument que celui utilisé ci-dessus, que $\left(\frac{2}{p}\right) = -1$.

L'égalité à démontrer est alors une conséquence de ce qui précède, vu que $p^2 - 1$ est multiple de 16 si et seulement si $p \equiv \pm 1 \pmod{8}$. En particulier, 2 est un carré dans \mathbb{F}_p si et seulement si $p \equiv \pm 1 \pmod{8}$. \square

Théorème I.2.4. — Pour tout p, q premiers impairs, on a

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

Il y a plus de 200 preuves différentes de ce résultat ; Gauss fut le premier à en donner une démonstration, il en donna en fait 6 différentes. Dans le paragraphe suivant nous présenterons quelques unes d'entre elles.

Corollaire I.2.5. — Soient n un entier tel que pour tout p premier sauf éventuellement un nombre fini, n est un carré modulo p . Alors n est un carré dans \mathbb{Z} .

Démonstration. — Soit p_1, \dots, p_n tels que pour tout $p \neq p_i$, n est un carré modulo p . Supposons n sans facteur carré et distinct de $\pm 1, \pm 2$. On écrit $n = hl_1 \cdots l_k$ avec $h \in \{\pm 1, \pm 2\}$ et où les l_i sont premiers impairs distincts ($k \geq 1$). Il existe un entier naturel a tel que :

$$a \equiv 1 \pmod{8p_1 \cdots p_n l_1 \cdots l_{k-1}} \text{ et } a \equiv r \pmod{l_k}$$

D'après la loi de réciprocité quadratique on a

$$\left(\frac{n}{a}\right) = \left(\frac{l_1 \cdots l_k}{a}\right) = \prod_i \left(\frac{a}{l_i}\right) = \left(\frac{1}{l_1}\right) \cdots \left(\frac{1}{l_{k-1}}\right) \left(\frac{r}{l_k}\right) = -1$$

de sorte que a a un diviseur premier p distinct des p_i tel que $\left(\frac{n}{p}\right) = -1$, d'où la contradiction. \square

Corollaire I.2.6. — Soit p un nombre premier impair et soit n le plus petit entier naturel tel que $\left(\frac{n}{p}\right) = -1$. On a alors

$$n < 1 + \sqrt{p}.$$

Démonstration. — Soit m le plus petit entier naturel tel que $mn > p$; puisque p est premier on a donc $n(m-1) < p$ soit $mn - p < n$. D'après le caractère minimal de n , on a

$$1 = \left(\frac{mn-p}{p}\right) = \left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right) \left(\frac{n}{p}\right) = -\left(\frac{m}{p}\right).$$

Par suite on a $m \geq n$ et le résultat découle du fait que

$$(n-1)^2 < n(n-1) \leq n(m-1) < p.$$

\square

Citons à ce propos la conjecture de Vinogradov :

Conjecture I.2.7. — Soit $\epsilon > 0$ un nombre réel; pour tout nombre premier p assez grand, le plus petit entier naturel que ne soit pas un résidu quadratique modulo p est inférieur à p^ϵ .

Par exemple, Hudson et Williams ont démontré en 1979 que si p impair n'est pas congru à 1 modulo 8, le plus petit entier naturel n qui ne soit pas un résidu quadratique modulo p est inférieur à $p^{\frac{2}{5}} + 12p^{\frac{1}{5}} + 33$. On a ainsi $n < 1,54p^{\frac{2}{5}}$ dès que p est plus grand que 10^7 et non congru à 1 modulo 8.

Définition I.2.8. — Soient m et n des entiers avec n impair positif. le symbole de Jacobi $(\frac{m}{n})$ se définit comme suit à partir du symbole de Legendre :

$$\left(\frac{m}{n}\right) = \prod_{i=1}^r \left(\frac{m}{p_i}\right)$$

où $n = p_1 p_2 \cdots p_r$ est la décomposition de n en facteurs premiers (non nécessairement distincts). Par convention on pose aussi $(\frac{m}{1}) = 1$.

Remarque : $(\frac{m}{n})$ ne dépend que de la classe de m modulo n et coïncide avec le symbole de Legendre si n est premier. On notera toutefois que $(\frac{m}{n}) = 1$ n'implique pas en général que m est un carré modulo n comme le montre l'exemple suivant

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1.$$

Son intérêt réside dans la proposition suivante qui fournit un algorithme efficace de $(\frac{m}{n})$.

Proposition I.2.9. — Soient $m, m', n, n' \in \mathbb{Z}$ avec n, n' impairs positifs. On a

$$\left(\frac{mm'}{n}\right) = \left(\frac{m}{n}\right)\left(\frac{m'}{n}\right), \quad \left(\frac{m}{nn'}\right) = \left(\frac{m}{n}\right)\left(\frac{m}{n'}\right),$$

ainsi que

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}, \quad \left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}},$$

et si m est impair positif

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{n-1}{2} \frac{m-1}{2}}.$$

Démonstration. — La première égalité découle de la multiplicativité du symbole de Legendre et la seconde est évidente. Les autres découlent directement des propriétés similaires du symbole de Legendre et des congruences immédiates suivantes, pour $m, n \in \mathbb{Z}$ impairs :

- $\frac{n-1}{2} + \frac{m-1}{2} \equiv \frac{nm-1}{2} \pmod{2}$;
- si $n = \prod_i n_i$ et $m = \prod_j m_j$ alors $\sum_{i,j} \frac{n_i-1}{2} \frac{m_j-1}{2} \equiv \frac{n-1}{2} \frac{m-1}{2} \pmod{2}$;
- $n^2 \equiv 1 \pmod{8}$;
- $\frac{n^2-1}{8} + \frac{m^2-1}{8} \equiv \frac{n^2 m^2 - 1}{8} \pmod{2}$.

□

Ainsi pour calculer $(\frac{m}{n})$ on procède comme suit :

- (i) On cherche $-\frac{n-1}{2} \leq m' < \frac{n-1}{2}$ tel que $m \equiv m' \pmod{n}$; on procède par division euclidienne.
- (ii) On factorise m' sous la forme $\epsilon 2^a \tilde{m}$ avec \tilde{m} impair et $\epsilon = \pm 1$.

(iii) On applique les propriétés du symbole de Jacobi :

$$\left(\frac{m}{n}\right) = \epsilon^{\frac{n-1}{2}} \left(\frac{2}{n}\right)^{\alpha} (-1)^{\frac{n-1}{2} \frac{\tilde{m}-1}{2}} \left(\frac{n}{m'}\right).$$

(iv) Si $\tilde{m} = 1$ c'est terminé sinon on reprend le procédé en notant que $\tilde{m} < n$ et $n \wedge \tilde{m} = 1$. L'avantage de la méthode est qu'il n'est pas nécessaire de factoriser m' , ce qui est à priori impossible dès que m' a plus de 200 chiffres, mais simplement d'en extraire la plus grande puissance de 2 ce qui est très rapide, surtout lorsque m' est écrit en base 2.

Nous avons vu que le symbole de Jacobi n'est pas du tout adapté à la question de savoir déterminer si un entier $n \in \mathbb{Z}$ est un carré modulo m . D'après le théorème chinois, il suffit de savoir traiter le cas où $m = p^\alpha$ avec p premier. On écrit alors $n = p^\beta n'$ avec $n' \wedge p = 1$: évidemment si $\beta \geq \alpha$ alors n est un carré modulo m . Si $\beta < \alpha$ alors n est un carré modulo m si et seulement si $\beta \equiv 0 \pmod{2}$ et n' est un carré modulo $p^{\alpha-\beta}$ ce qui ramène le problème à l'étude des carrés de $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \simeq (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}/p^{\alpha-1}\mathbb{Z}$.

Proposition I.2.10. — Soit \mathcal{P}' la réunion de l'ensemble des nombres premiers impairs et de $\{4, 8\}$. Un élément $n \in (\mathbb{Z}/m\mathbb{Z})^\times$ est un carré si et seulement si son image dans $(\mathbb{Z}/p\mathbb{Z})^\times$ est un carré pour tout $p \in \mathcal{P}'$ divisant m .

Démonstration. — Bien entendu seule la réciproque pose question. D'après le théorème chinois on se ramène au cas où $m = p^\alpha$ avec $\alpha \geq 3$ si $p = 2$. Résonnons alors par récurrence sur α autrement dit par approximations successives. Commençons tout d'abord par le cas où p est impair. Supposons que $u^2 = m + p^\alpha k$ et considérons

$$(u + p^\alpha \delta)^2 \equiv u^2 + 2U\delta p^\alpha \equiv m + (k + 2u\delta)p^\alpha \pmod{p^{\alpha+1}}.$$

Il suffit alors de choisir δ tel que $k + 2u\delta \equiv 0 \pmod{p}$ ce qui est possible puisque, m et donc u sont premiers à p , de sorte que $\delta \equiv k(2u)^{-1} \pmod{p}$ convient, on rappelle que $p \neq 2$.

Traitons alors le cas de $p = 2$ et supposons que $m \in (\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ est un carré modulo 8, i.e. $m \equiv 1 \pmod{8}$. Reprenons l'argument précédent, soit $u^2 = m + 2^\alpha k$ et calculons

$$(u + 2^{\alpha-1} \delta)^2 \equiv u^2 + (k + u\delta)2^\alpha \pmod{2^{\alpha+1}}$$

car $2(\alpha - 1) \geq \alpha + 1$ puisque $\alpha \geq 3$. Comme u est impair, il suffit alors de prendre $\delta \equiv k \pmod{2}$. \square

I.2.2. Preuve d'Eisenstein. — Soit $A = \{2, 4, 6, \dots, p-1\}$; pour tout $a \in A$, on note r_a le reste de la division euclidienne de qa par p .

Lemme I.2.11. — Modulo p , l'ensemble A est égal à $\{(-1)^{r_a} r_a; a \in A\}$.

Démonstration. — Notons tout d'abord que si r_a est pair alors $r_a \in A$ et dans le cas contraire, $-r_a \equiv p - r_a \in A$. Ensuite si on a

$$(-1)^{r_a} r_a = (-1)^{r_{a'}} r_{a'} \pmod{p}$$

alors $qa \equiv \pm qa' \pmod{p}$ et donc $a \equiv \pm a' \pmod{p}$. Ainsi si $a \neq a'$, on a $a + a' \equiv 0 \pmod{p}$ ce qui impose, comme $0 < a + a' < 2p$, $a + a' = p$ ce qui n'est pas puisque p est impair. \square

Lemme I.2.12. — On a

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{a \in A} r_a}.$$

Démonstration. — D'après le lemme précédent, on a

$$\prod_{a \in A} r_a \equiv q^{\frac{p-1}{2}} \prod_{a \in A} a \pmod{p} \text{ et } \prod_{a \in A} (-1)^{\sum_{a \in A} r_a} \prod_{a \in A} r_a \pmod{p}$$

et donc $q^{\frac{p-1}{2}} \equiv (-1)^{\sum_{a \in A} r_a} \pmod{p}$, d'où le résultat. \square

On écrit $qa = p \lfloor \frac{qa}{p} \rfloor + r_a$ de sorte que

$$\sum_{a \in A} r_a \equiv \sum_{a \in A} \lfloor \frac{qa}{p} \rfloor \pmod{2},$$

et donc en particulier

$$\left(\frac{q}{p} \right) = (-1)^{\sum_{a \in A} \lfloor \frac{qa}{p} \rfloor}.$$

Application : pour $q = 2$, on retrouve alors aisément la formule $\left(\frac{2}{p} \right) = (-1)^{\frac{p^2-1}{8}}$.

Lemme I.2.13. — On a $\left(\frac{q}{p} \right) = (-1)^\mu$, où μ désigne le nombre de points entiers dans le triangle AHK de la figure 1.

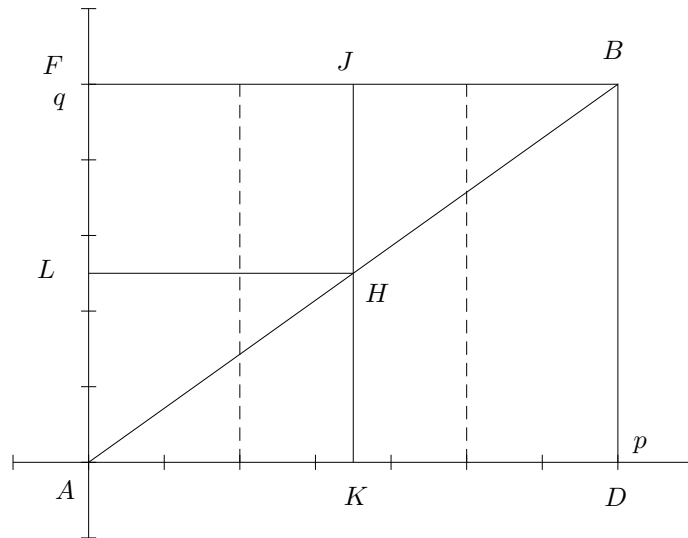


FIGURE 1.

Démonstration. — Avec les notations de la figure 1 ; pour tout $0 \leq a \leq p$, il y a un nombre pair (égal à $q - 1$) de points entiers d'abscisse égale à a dans le rectangle $ADBF$. On note que comme p et q sont premiers entre eux il n'y a aucun points entiers sur le segment $[AB]$ autre que A et B . Pour $a > p/2$ pair, les points entiers de BHJ d'abscisse a sont en bijection

avec ceux de AKH d'abscisse $p - a$. Ainsi le nombre de points de ADB d'abscisse pair a la même parité que l'ensemble des points entiers de AKH , i.e.

$$\sum_{a \in A} \left\lfloor \frac{qa}{p} \right\rfloor \equiv \mu \pmod{2}$$

ce qui donne le résultat. \square

En échangeant les rôles de p et q , on trouve alors que $\left(\frac{p}{q}\right) = (-1)^\nu$ où ν est égal au nombre de points entiers du triangle AHL . Comme le nombre total de points entiers dans le rectangle $AKHL$ est égal à $\frac{p-1}{2} \frac{q-1}{2}$, on obtient

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\mu+\nu} = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}.$$

I.2.3. via le symbole de Zolotarev. — Pour m premier avec n , soit $\binom{m}{n}_Z$ le symbole de Zolotarev défini comme la signature de la permutation $s_n(m)$ correspondant à la multiplication par m dans $\mathbb{Z}/n\mathbb{Z}$.

Lemme I.2.14. — *Le symbole de Zolotarev est multiplicatif en la variable m ,*

$$\binom{mm'}{n}_Z = \binom{m}{n}_Z \binom{m'}{n}_Z.$$

Démonstration. — La multiplicativité du symbole de Zolotarev en la variable m provient du fait que la composition de la multiplication par m avec la multiplication par m' correspond à la multiplication par mm' et que la signature d'une composée est le produit des signatures. \square

Lemme I.2.15. — *Pour p premier et n non divisible par p , le symbole de Zolotarev $\binom{n}{p}_Z$ est égal au symbole de Legendre $\left(\frac{n}{p}\right)$.*

Démonstration. — Le cas $p = 2$ étant évident, on suppose donc p impair. Si $n \equiv a^2 \pmod{p}$, alors $\binom{n}{p}_Z = \left(\frac{a}{p}\right)^2 = \left(\frac{n}{p}\right)$. Supposons donc que n n'est pas un carré modulo p . On considère les involutions de $\mathbb{Z}/p\mathbb{Z}$

$$\alpha : \begin{cases} 0 \mapsto 0 \\ x \mapsto x^{-1} \text{ si } x \neq 0 \end{cases} ; \quad \beta : \begin{cases} 0 \mapsto 0 \\ x \mapsto nx^{-1} \text{ si } x \neq 0. \end{cases}$$

De l'égalité $s_p(n) = \beta \circ \alpha$ on en déduit que $\binom{n}{p}_Z = \epsilon(\beta)\epsilon(\alpha)$. Mais puisque une involution se décompose en produit de transpositions à supports disjoints, la signature d'une involution τ de $\mathbb{Z}/p\mathbb{Z}$ est égale à $(-1)^{p - \#\text{Fix}(\tau)}$ où $\text{Fix}(\tau)$ désigne l'ensemble des points fixes de τ . Or $\text{Fix}(\alpha) = \{0, 1, -1\}$ et $\text{Fix}(\beta) = \{0\}$ car un point fixe $a \neq 0 \pmod{p}$ de β vérifie $n = a^2$ ce qui est exclu. Ainsi $\binom{n}{p}_Z = (-1)^{\frac{p-1}{2}} (-1)^{\frac{p-3}{2}} = -1 = \left(\frac{n}{p}\right)$. \square

Remarque : on peut aussi calculer explicitement la signature. Soit r l'ordre de m dans $(\mathbb{Z}/n\mathbb{Z})^\times$ qui est cyclique si n est premier ; ce groupe se décompose alors sous l'action de m en $(n-1)/r$ orbites chacune de longueur r et sur ces orbites la multiplication par m y induit un cycle de longueur r . On en déduit alors que le symbole de Zolotarev est $(-1)^{(r-1)(n-1)/r}$. Ainsi

- si r est pair on a

$$m^{(n-1)/2} = (m^{r/2})^{(n-1)/r} \equiv (-1)^{(n-1)/r} \pmod{n}$$

car m étant d'ordre r , $m^{r/2}$ est une racine carrée de 1 dans le corps $\mathbb{Z}/n\mathbb{Z}$ distincte de 1 donc égale à -1 ;

- si r est impair, $n-1$ est alors divisible par $2r$ et donc $m^{(n-1)/2} = (m^r)^{(n-1)/2r} \equiv 1 \pmod{n}$ d'où le résultat.

On fixe n et m des entiers impairs premiers entre eux. On range de trois manières différentes les entiers de 0 à $mn-1$ en définissant trois matrices de taille (m, n) notés V , H et D :

- V correspond à un remplissage vertical soit $V = (v_{i,j})$ avec $v_{i,j} = m(j-1) + i - 1$;
- H correspond à un remplissage horizontal soit $H = (h_{i,j})$ avec $h_{i,j} = n(i-1) + j - 1$;
- D correspond à un remplissage diagonal soit $D = (d_{i,j})$ où $d_{i,j}$ est l'unique entier compris entre 0 et $mn-1$ congru à $i-1$ modulo m et $j-1$ modulo n .

Exemple dans le cas $(m, n) = (3, 5)$:

$$V = \begin{pmatrix} 0 & 3 & 6 & 9 & 12 \\ 1 & 4 & 7 & 10 & 13 \\ 2 & 5 & 8 & 11 & 14 \end{pmatrix} \quad H = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 & 9 \\ 10 & 11 & 12 & 13 & 14 \end{pmatrix}$$

$$D = \begin{pmatrix} 0 & 6 & 12 & 3 & 9 \\ 10 & 1 & 7 & 13 & 4 \\ 5 & 11 & 2 & 8 & 14 \end{pmatrix}.$$

On considère les permutations suivantes :

- $\sigma_{D,V} : v_{i,j} \mapsto d_{i,j}$;
- $\sigma_{H,D} : d_{i,j} \mapsto h_{i,j}$;
- $\sigma_{V,H} : h_{i,j} \mapsto v_{i,j}$.

Lemme I.2.16. — On a les propriétés suivantes :

1. $\sigma_{V,H} \circ \sigma_{H,D} \circ \sigma_{D,V} = id$;
2. $\epsilon(\sigma_{D,V}) = \binom{m}{n}_Z$;
3. $\epsilon(\sigma_{H,D}) = \binom{n}{m}_Z$;
4. $\epsilon(\sigma_{V,H}) = (-1)^{\frac{m-1}{2} \frac{n-1}{2}}$.

Démonstration. — a) C'est clair.

b) La permutation $\sigma_{D,V}$ conserve les lignes puisque

$$\{v_{i,j}; j = 1, \dots, n\} = \{0 \leq k \leq mn-1; k \equiv i-1 \pmod{m}\} = \{d_{i,j}, j = 1, \dots, n\}.$$

Ainsi $\sigma_{D,V}$ est le produit de m permutations de n éléments, chacune correspondant à l'action de $\sigma_{D,V}$ sur une ligne. Fixons $1 \leq i \leq m$ et calculons la signature de la permutation ρ_i induit par $\sigma_{D,V}$ sur la i -ème ligne. Grâce au lemme chinois, un élément de la i -ème ligne de D ou de V est uniquement déterminé par sa classe dans $\mathbb{Z}/n\mathbb{Z}$. Ainsi ρ_i^{-1} est la permutation de $\mathbb{Z}/n\mathbb{Z}$ qui envoie $j-1$ sur $m(j-1) + i - 1$, i.e. $\rho_i^{-1} = T_{i-1} \circ s_n(m)$ où T_a désigne la translation $k \in \mathbb{Z}/n\mathbb{Z} \mapsto k + a$. Mais pour tout a , $\epsilon(T_a) = 1$ car $T_a = \underbrace{T_1 \circ \dots \circ T_1}_a$ et $\epsilon(T_1) = 1$ car T_1 est un cycle de longueur impair n . Ainsi $\epsilon(\sigma_{D,V}) = \prod_{i=1}^m \epsilon(\rho_i) = \left(\binom{m}{n}_Z\right)^m = \binom{m}{n}_Z$ puisque m est impair.

c) Même raisonnement que dans b) en remarquant que $\sigma_{H,D}$ conserve les colonnes.

d) Calculons le nombre d'inversions de $\sigma_{V,H}$. On a

$$(v_{i,j} < v_{k,l}) \Leftrightarrow (m(j-1) + i - 1 < m(k-1) + l - 1) \Leftrightarrow (j < l \text{ ou } (j = l \text{ et } i < k)).$$

De même $(h_i, < h_{k,l} \Leftrightarrow (i < k \text{ ou } (i = k \text{ et } j < l))$. On a donc

$$(v_{i,j} < v_{k,l} \text{ et } h_{i,j} > h_{k,l}) \Leftrightarrow (j < l \text{ et } k < i).$$

Ainsi le nombre d'inversion est égal à $\binom{m}{2} \binom{n}{2} = \frac{m(m-1)}{2} \frac{n(n-1)}{2}$, et puisque mn est impair, on a $\epsilon(\sigma_{V,H}) = (-1)^{\frac{m-1}{2} \frac{n-1}{2}}$.

e) Immédiat d'après les questions précédentes. \square

Proposition I.2.17. — *Le symbole de Zolotarev est égal au symbole de Jacobi; la loi de réciprocité quadratique du symbole de Jacobi est vérifiée.*

Démonstration. — La loi de réciprocité contient la multiplicativité en bas du symbole de Zolotarev :

$$\binom{a}{mn}_Z = \binom{a}{m}_Z \binom{a}{n}_Z$$

où m et n sont des entiers impairs et a est premier à mn . En effet si r est un entier congru à 1 modulo 4 et à a modulo mn , on a

$$\binom{a}{mn}_Z = \binom{r}{mn}_Z = (-1)^{\frac{r-1}{2} \frac{mn-1}{2}} \binom{mn}{r}_Z = \binom{m}{r}_Z \binom{n}{r}_Z = \binom{r}{m}_Z \binom{r}{n}_Z = \binom{a}{m}_Z \binom{a}{n}_Z.$$

On en déduit donc que le symbole de Zolotarev est égal au symbole de Jacobi défini pour les couples (m, n) d'entiers premiers entre eux avec n impair comme l'unique symbole multiplicatif en haut et en bas prolongeant le symbole de Legendre. \square

Remarque : pour tout n impair le symbole de Jacobi $\binom{2}{n} = (-1)^{\frac{n^2-1}{8}}$. En effet, comme n est impair, $n \wedge (n-2) = 1$ et donc

$$\begin{aligned} \binom{2}{n} &= \binom{2}{n}_Z = \binom{-(n-2)}{n}_Z = \binom{-1}{n}_Z \binom{n-2}{n}_Z \\ &= (-1)^{\frac{n-1}{2}} (-1)^{\frac{n-1}{2} \frac{n-3}{2}} \binom{n}{n-2}_Z = (-1)^{\frac{n-1}{2}} \binom{2}{n-2}_Z. \end{aligned}$$

En notant $n = 2k + 1$, on a donc $\binom{2}{n}_Z = (-1)^{\frac{k(k+1)}{2}} = \begin{cases} 1 & \text{si } n \equiv \pm 1 \pmod{8} \\ -1 & \text{sinon} \end{cases}$.

I.2.4. en utilisant les résultants. — Rappelons que la loi de réciprocité quadratique est une égalité entre deux signes; l'idée est alors d'utiliser la relation

$$\text{Res}(P, Q) = (-1)^{\deg P \cdot \deg Q} \text{Res}(Q, P)$$

et de choisir des polynômes P et Q de degré respectifs $\frac{p-1}{2}$ et $\frac{q-1}{2}$, où p et q sont des premiers impairs distincts, de sorte que

$$\text{Res}(P, Q) = \left(\frac{p}{q}\right) \text{ et } \text{Res}(Q, P) = \left(\frac{q}{p}\right).$$

Lemme I.2.18. — *Pour tout p premier impair, il existe un polynôme $Q_p \in \mathbb{Z}[X]$ tel que*

$$X^{p-1} + X^{p-2} + \dots + X + 1 = X^{(p-1)/2} Q_p \left(X + \frac{1}{X}\right).$$

En outre modulo p on a

$$Q_p(Y) \equiv (Y - 2)^{\frac{p-1}{2}} \pmod{p}.$$

Démonstration. — En posant $Y = X^{-1}$, le membre de gauche est égal à $X^{(p-1)/2} + \dots + X + 1 + Y + \dots + Y^{(p-1)/2}$, de sorte que d'après le théorème sur les polynômes symétriques, il existe $R \in \mathbb{Z}[X, Y]$ tel que le terme précédent est égal à $R(X + Y, XY)$, d'où le résultat en notant que $XY = 1$. Raisonnons alors modulo p :

$$\begin{aligned} X^{p-1} + \dots + X + 1 &\equiv (X - 1)^{p-1} \\ &\equiv (X^2 - 2X + 1)^{(p-1)/2} \\ &\equiv X^{(p-1)/2} (X + \frac{1}{X} - 2)^{(p-1)/2} \pmod{p}, \end{aligned}$$

de sorte que $Q_p(X + \frac{1}{X}) \equiv (X + \frac{1}{X} - 2)^{(p-1)/2} \pmod{p}$ soit

$$Q_p(X) \equiv (X - 2)^{(p-1)/2}.$$

□

Lemme I.2.19. — Pour $p \neq q$ des nombres premiers impairs, le résultant de Q_p et Q_q est égal à ± 1 .

Démonstration. — Raisonnons par l'absurde et considérons l premier divisant $\text{Res}(Q_p, Q_q)$ de sorte que modulo l , \bar{Q}_p et \bar{Q}_q ont une racine commune $\beta \in \mathbb{F}_l^n$ pour $2n \leq \min\{p-1, q-1\}$. Soit alors $x \in \mathbb{F}_l$ tel que $x^2 - \beta x + 1 = 0$ de sorte que

$$x^{p-1} + \dots + x + 1 = x^{(p-1)/2} \bar{Q}_p(\beta) = 0.$$

En multipliant cette égalité par $x - 1$, on en déduit que $x^p = 1$ dans \mathbb{F}_l . De la même façon on a aussi $x^q = 1$ et comme $p \wedge q = 1$, on en déduit $x = 1$ et donc $p \equiv q \equiv 0 \pmod{l}$ ce qui n'est pas car $p \wedge q = 1$. □

Proposition I.2.20. — Pour $p \neq q$ des nombres premiers distincts, on a

$$\text{Res}(Q_p, Q_q) = \left(\frac{q}{p}\right).$$

Démonstration. — On raisonne modulo p de sorte que d'après le lemme précédent, il suffit de prouver que ce résultant est $\equiv q^{(p-1)/2} \pmod{p}$. Comme $Q_p(X) \equiv (X - 2)^{(p-1)/2} \pmod{p}$, on en déduit que

$$\text{Res}(Q_p, Q_q) \equiv Q_p(2)^{(p-1)/2} \equiv Q_q\left(1 + \frac{1}{1}\right)^{(p-1)/2} \equiv q^{(p-1)/2} \pmod{p},$$

d'où le résultat. □

I.2.5. via une équation diophantienne. — En 1838 V.A. Lebesgue présentait une preuve reposant sur le comptage des points de l'hypersphère $x_1^2 + \dots + x_p^2 = 1$ de \mathbb{F}_q^p . Nous présentons ici une preuve due à Wouter Castryck inspirée de celle de V.A. Lebesgue qui repose sur l'étude, pour $n \equiv 1 \pmod{2}$, du nombre N_n de solutions dans $(\mathbb{Z}/q\mathbb{Z})^n$ de l'équation

$$x_1^2 - x_2^2 + x_3^2 - \dots + x_n^2 = 1.$$

Lemme I.2.21. — Pour tout $n \geq 3$ impair, on a la relation de récurrence

$$N_n = q^{n-2}(q-1) + qN_{n-2}.$$

Démonstration. — Le changement de variable $x_1 \leftarrow x_1 + x_2$ donne alors

$$x_1^2 + x_3^2 - \cdots + x_n^2 - 1 = -2x_1x_2$$

de sorte que pour tout $x_1 \neq 0$ et pour tout x_3, \dots, x_n , il existe un unique x_2 telle que l'équation soit vérifiée. Pour $x_1 = 0$, les solutions correspondent à x_2 quelconque et $x_3^2 - \cdots + x_n^2 = 1$, d'où le résultat. \square

Ainsi on obtient par une récurrence simple

$$N_n = (q-1)(q^{n-2} + q^{n-1} + \cdots + q^{n-k}) + q^k N_{n-2k}$$

de sorte que comme $N_1 = 2$, on obtient

$$N_n = q^{n-1} + q^{\frac{n-1}{2}}.$$

On en déduit alors la congruence suivante

$$N_p \equiv 1 + \left(\frac{q}{p}\right) \pmod{p}.$$

Plus directement, en écrivant l'équation à résoudre sous la forme

$$\sum_{i=1}^n t_i = 1, \quad x_1^2 = t_1, \quad x_2^2 = -t_2, \quad \dots, \quad x_n^2 = t_n$$

on obtient

$$N_p = \sum_{t_1 + \cdots + t_p = 1} \left(1 + \left(\frac{t_1}{q}\right)\right) \left(1 + \left(\frac{-t_2}{q}\right)\right) \left(1 + \left(\frac{t_3}{q}\right)\right) \cdots \left(1 + \left(\frac{t_p}{q}\right)\right).$$

On développe le produit que l'on écrit sous la forme

$$\sum_{t_1 + \cdots + t_n = 1} \sum_I \left(\frac{\epsilon_I \prod_{i \in I} t_i}{q}\right)$$

où I décrit les sous-ensembles de $\{1, \dots, n\}$ et ϵ_I est un signe. Pour I non vide et distinct de $\{1, \dots, n\}$, notons $j_0 \notin I$ de sorte que

$$\sum_{t_1 + \cdots + t_n = 1} \prod_{i \in I} \left(\frac{\prod_{i \in I} t_i}{q}\right) = q^{n-1-\#I} \left(\sum_{t \in \mathbb{Z}/q\mathbb{Z}} \left(\frac{t}{q}\right)\right)^{\#I}$$

puisque en effet on peut laisser les $(t_i)_{i \in I}$ varier arbitrairement dans $(\mathbb{Z}/q\mathbb{Z})^{\#I}$ avec

$$\sum_{(t_i)_{i \in I} \in (\mathbb{Z}/q\mathbb{Z})^{\#I}} \prod_{i \in I} \left(\frac{t_i}{q}\right) = \left(\sum_{t \in \mathbb{Z}/q\mathbb{Z}} \left(\frac{t}{q}\right)\right)^{\#I}$$

on laisse ensuite varier arbitrairement les t_j pour $j \notin I \cup \{j_0\}$ et t_{j_0} est alors défini par $\sum_{i=1}^n t_i = 1$: comme ces t_j n'interviennent pas dans la somme ils donnent le facteur $q^{n-1-\#I}$. De l'égalité $\sum_{t \in \mathbb{Z}/q\mathbb{Z}} \left(\frac{t}{q}\right) = 0$, ne contribue à N_p que $I = \emptyset$ et $I = \{1, \dots, n\}$ ce qui donne

$$N_p = q^{p-1} + \left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right) \sum_{t_1 + \cdots + t_p = 1} \left(\frac{t_1 \cdots t_p}{q}\right).$$

Considérons alors l'action par permutations circulaires, de $\mathbb{Z}/p\mathbb{Z}$ sur $\{(t_1, \dots, t_n) : \sum_{i=1}^n t_i = 1\}$. Les stabilisateurs sont d'après le théorème de Lagrange égaux soit à $\{0\}$ soit à $\mathbb{Z}/p\mathbb{Z}$ de

sorte que les orbites sont toutes de cardinal p sauf celle associée à (p^{-1}, \dots, p^{-1}) qui est de cardinal 1. Pour une telle orbite \mathcal{O} de cardinal p , on a alors

$$\sum_{(t_1, \dots, t_p) \in \mathcal{O}} \left(\frac{t_1 \cdots t_p}{q} \right) \equiv 0 \pmod{p}$$

et donc

$$N_p \equiv 1 + \left(\frac{(-1)^{\frac{p-1}{2}}}{q} \right) \left(\frac{p^{-p}}{q} \right) \equiv 1 + (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{p}{q} \right) \pmod{p}.$$

De ces deux calculs on obtient finalement la congruence suivante :

$$1 + \left(\frac{q}{p} \right) \equiv 1 + (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{p}{q} \right) \pmod{p},$$

ce qui finit de prouver la loi de réciprocité quadratique.

I.2.6. par les sommes de Gauss. — Soit p un nombre premier impair et notons $\zeta = e^{2i\pi/p}$ une racine p -ième primitive de l'unité, dans \mathbb{C} .

Définition I.2.22. — La somme de Gauss relative à p est le nombre complexe

$$G = \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{a}{p} \right) \zeta^a.$$

Proposition I.2.23. — On a $G^2 = (-1)^{\frac{p-1}{2}} p$.

Démonstration. — Par multiplicativité du symbole de Legendre, on a

$$G^2 = \sum_{a, b \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{ab}{p} \right) \zeta^{a+b}.$$

On effectue alors le changement de variable $b = at$ de sorte qu'en utilisant $\left(\frac{a^2 t}{p} \right) = \left(\frac{t}{p} \right)$, G^2 se réécrit :

$$G^2 = \sum_{t \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{t}{p} \right) \left(\sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \zeta^{a(t+1)} \right) = (p-1) \left(\frac{-1}{p} \right) + \sum_{-1 \neq t \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{t}{p} \right) \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \zeta^{a(1+t)}.$$

Pour $t \neq -1$, l'application $a \mapsto (1+t)a$ est une bijection de $(\mathbb{Z}/p\mathbb{Z})^\times$ et donc

$$\sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \zeta^{a(1+t)} = \zeta + \zeta^2 + \dots + \zeta^{p-1} = -1$$

ce qui nous donne

$$G^2 = (p-1) \left(\frac{-1}{p} \right) - \sum_{-1 \neq t \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{t}{p} \right) = p \left(\frac{-1}{p} \right)$$

car $\sum_{t \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{t}{p} \right) = 0$. □

Définition I.2.24. — Pour $p = 2$ on pose $G = \zeta + \zeta^{-1}$ où $\zeta = e^{2i\pi/8} = \frac{1+i}{\sqrt{2}}$ soit $G = \sqrt{2}$ et G^2 vérifie une relation similaire.

Remarque : en fait Gauss a démontré que $G = \sqrt{p}$ pour $p \equiv 1 \pmod{4}$ et $G = i\sqrt{p}$ pour $p \equiv 3 \pmod{4}$; on renvoie à l'exercice ??.

Ainsi G est une racine carré de $(-1)^{\frac{p-1}{2}}p$ dans l'anneau $\mathbb{Z}[\zeta]$, sa réduction modulo $q\mathbb{Z}[\zeta]$ est alors un candidat naturel pour être une racine carrée de $(-1)^{\frac{p-1}{2}}p \pmod{q}$ pourvu que G soit congrue modulo $q\mathbb{Z}[\zeta]$ à un élément de \mathbb{Z} . Une condition nécessaire est que $G^q \equiv G \pmod{q}$ ce qui pousse à s'intéresser à $G \pmod{q\mathbb{Z}[\zeta]}$.

Proposition I.2.25. — On a $G^q \equiv \left(\frac{q}{p}\right)G \pmod{q}$ si $p > 2$ et $G^q \equiv (-1)^{\frac{q^2-1}{8}}G \pmod{q}$ pour $p = 2$.

Démonstration. — Commençons par traiter le cas p impair et calculons $G^q \pmod{q}$ dans $\mathbb{Z}[\zeta]$:

$$G^q \equiv \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{a}{p}\right)^q \zeta^{aq} \pmod{q\mathbb{Z}[\zeta]}.$$

On effectue alors le changement de variable $t = aq$ ce qui, en utilisant les égalités

$$\left(\frac{a}{p}\right)^q = \left(\frac{a}{p}\right) \text{ et } \left(\frac{a}{p}\right) = \left(\frac{q}{p}\right)\left(\frac{qa}{p}\right)$$

donne le résultat.

Le cas $p = 2$ se traite de même en notant que $\zeta^q + \zeta^{-q} = G$ si $q \equiv \pm 1 \pmod{8}$ et $-G$ sinon. \square

Démontrons alors la loi de réciprocité quadratique : le principe est de calculer $G^q \pmod{q\mathbb{Z}[\zeta]}$ en utilisant l'égalité $G^2 = p(-1)^{\frac{p-1}{2}}$. Supposons tout d'abord p impair :

$$G^q = (G^2)^{\frac{q-1}{2}}G = \left((-1)^{\frac{p-1}{2}}p\right)^{\frac{q-1}{2}}G = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}p^{\frac{q-1}{2}}G,$$

l'égalité ayant lieu dans $\mathbb{Z}[\zeta]$. Notons alors que \bar{G}^2 est inversible dans \mathbb{F}_q^\times et donc dans $\mathbb{F}_p[\zeta]$ de sorte que $\bar{G} \in \mathbb{F}_q[\zeta]$ est aussi inversible

soit d'après le critère d'Euler

$$G^q \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}}p^{\frac{q-1}{2}}\left(\frac{p}{q}\right)G \pmod{q\mathbb{Z}[\zeta]}.$$

En comparant avec la proposition précédente, il vient

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}}p^{\frac{q-1}{2}}\left(\frac{p}{q}\right)G \equiv \left(\frac{q}{p}\right)G \pmod{q\mathbb{Z}[\zeta]}$$

soit en multipliant par $(-1)^{\frac{p-1}{2}}G$

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}}p^{\frac{q-1}{2}}\left(\frac{p}{q}\right)p \equiv \left(\frac{q}{p}\right)p \pmod{q\mathbb{Z}}$$

qui est une congruence dans \mathbb{Z} de laquelle on déduit la loi de réciprocité quadratique puisque p est inversible modulo q .

Pour $p = 2$, l'argument précédent et la relation $G^2 = 2$, montrent alors que

$$\left(\frac{2}{p}\right)G \equiv (-1)^{\frac{q^2-1}{8}}G \pmod{q\mathbb{Z}[\zeta]}$$

dont on tire la loi supplémentaire.

Remarque : on peut aussi raisonner dans les corps finis, en considérant cette fois-ci ζ une racine primitive p -ième de l'unité dans une clôture algébrique de \mathbb{F}_q , comme $p \wedge q = 1$ cela ne pose pas de difficulté puisque $X^p - 1$ est un polynôme sans racine multiple : on note

$K = \mathbb{F}_q[\zeta]$ le corps fini associé. Notons alors $\bar{G} \in K$ la somme de Gauss associée. Comme précédemment on a encore $G^2 = (-1)^{\frac{p-1}{2}} p$. Comme K est de caractéristique q , la congruence de la proposition I.2.25 devient une égalité $\bar{G}^{q-1} = \left(\frac{q}{p}\right)$ dans K . On conclut alors comme précédemment

$$\left(\frac{q}{p}\right) = \bar{G}^{q-1} = (\bar{G}^2)^{\frac{q-1}{2}} = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} p^{\frac{q-1}{2}} = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{p}{q}\right).$$

I.2.7. par la théorie de Galois. — On utilise dans ce chapitre certaines notions et résultats du §?? afin de proposer une preuve particulièrement synthétique de la loi de réciprocité quadratique qui permettra en outre d'introduire diverses généralisations.

Soit L/K une extension finie; on note \mathcal{O}_K et \mathcal{O}_L les anneaux d'entiers. Pour \mathfrak{p} un idéal premier non nul de \mathcal{O}_K . On écrit

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{b}_1^{e_1} \cdots \mathfrak{b}_r^{e_r}$$

où les \mathfrak{b}_i sont des idéaux premiers distincts non nuls de \mathcal{O}_L et les e_i des entiers ≥ 1 . On note en outre f_i le degré de l'extension de corps résiduel $\kappa(\mathfrak{b}_i)/\kappa(\mathfrak{p})$. On rappelle que $\sum_i e_i f_i = [L : K] = n$. En outre si l'extension L/K est galoisienne, $e_i = e$ et $f_i = f$ sont constants. Quand $r = 1$ (resp. $r = n$), on dit que \mathfrak{p} est inerte (resp. totalement décomposé). Quand tous les $e_i = 1$, on dit que \mathfrak{p} est non ramifié. On note $\text{Spl}(L/K)$ l'ensemble des idéaux premiers de K totalement décomposés dans L .

Lemme I.2.26. — Soit K un corps quadratique et $a \in \mathbb{Z}$ un entier sans carré tel que $K = \mathbb{Q}[\sqrt{a}]$.

(1) Pour tout premier p , $\mathcal{O}_K/p\mathcal{O}_K \simeq \mathbb{F}_p[X]/(X^2 - a)$.

(2) Pour tout p ne divisant pas $2a$, (p) est non ramifié dans K .

(3) Pour $p \nmid 2a$, (p) est complètement décomposé si et seulement si $\left(\frac{a}{p}\right) = 1$.

Démonstration. — (1) On rappelle que $\mathcal{O}_K = \mathbb{Z}[\omega]$ avec suivant la valeur de a , $\omega = \sqrt{a}$ ou $\omega = \frac{1+\sqrt{a}}{2}$; dans ce dernier cas, pour $\alpha + \beta\omega \in \mathcal{O}_K$ qui n'est pas dans $R = \mathbb{Z}[\sqrt{a}]$, β est impair et donc congru à $\alpha + (\beta + p)\omega \in R$ modulo p . Ainsi dans tous les cas on a

$$\mathcal{O}_K/p\mathcal{O}_K \simeq R/pR \simeq \mathbb{Z}[X]/(X^2 - a, p) \simeq \mathbb{F}_p[X]/(X^2 - a)$$

(2) Si $p\mathcal{O}_K = \mathfrak{b}_1^{e_1} \cdots \mathfrak{b}_r^{e_r}$, le théorème chinois donne

$$\mathcal{O}_K/p\mathcal{O}_K \simeq \bigoplus_{i=1}^r \mathcal{O}_K/\mathfrak{b}_i^{e_i}$$

L'algèbre $\mathbb{F}_p[X]/(X^2 - a)$ étant sans élément nilpotent, (p) est donc non ramifiée dans K et $\mathcal{O}_K/p\mathcal{O}_K$ est la somme de $r = 1, 2$ corps qui sont des extensions de \mathbb{F}_p .

(3) Selon que $X^2 - a$ est irréductible sur \mathbb{F}_p , i.e. selon la valeur de $\left(\frac{a}{p}\right)$, (p) ne se décompose pas ou se décompose complètement dans K . \square

Remarque : d'après la loi de réciprocité quadratique, $\left(\frac{a}{p}\right)$ est déterminé à un signe explicite près, par la classe de p modulo a . Ainsi $\text{Spl}(\mathbb{Q}[\sqrt{a}]/\mathbb{Q})$ est l'ensemble des premiers contenus dans une certaine réunion de classes non nulles modulo $4a$, auquel il faut éventuellement ajouter des diviseurs premiers de $2a$.

Lemme I.2.27. — Soit ζ_n une racine primitive n -ième de l'unité. On pose $K = \mathbb{Q}[\zeta_n]$ d'anneau des entiers $\mathcal{O}_K = \mathbb{Z}[\zeta_n] \simeq \mathbb{Z}[X]/(\Phi_n(X))$.

(1) Pour tout p ne divisant pas n , (p) est non ramifié dans K et se décompose en idéaux premiers de même degré résiduel f égal à l'ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^\times$.

(2) $\text{Spl}(K/\mathbb{Q})$ est l'ensemble des premiers congrus à 1 modulo n .

Démonstration. — (1) On a $\mathcal{O}_K/p\mathcal{O}_K \simeq \mathbb{F}_p[X]/(\overline{\Phi}_n(X))$. On rappelle que $\overline{\Phi}_n(X)$ se décompose en un produit de $\phi(n)/f$ facteurs irréductibles, tous de même degré f qui est égal à l'ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^\times$, d'où le résultat.

(2) p est totalement décomposé si et seulement si $f = 1$ i.e. $p \equiv 1 \pmod{n}$. □

Si \mathfrak{p} un idéal premier non nul de K et soit \mathfrak{b} un idéal de L au dessus de \mathfrak{p} , alors l'ordre du stabilisateur $G_{\mathfrak{b}}$ est égal à ef . Dans le cas où \mathfrak{p} est non ramifié, $e = 1$, $G_{\mathfrak{b}}$ s'identifie au groupe de Galois de l'extension de corps finis $\kappa(\mathfrak{b})/\kappa(\mathfrak{p})$. Ainsi à \mathfrak{b}_i , on associe un élément $\phi_{\mathfrak{b}_i} \in G_{\mathfrak{b}_i}$ qui correspond au morphisme de Frobenius de $\kappa(\mathfrak{b}_i)/\kappa(\mathfrak{p})$. Pour $\sigma \in G$, on a $\phi_{\sigma\mathfrak{b}_i} = \sigma\phi_{\mathfrak{b}_i}\sigma^{-1}$ de sorte que si G est abélien $\phi_{\mathfrak{b}_i}$ ne dépend pas du choix de \mathfrak{b}_i au dessus de \mathfrak{p} : on le note $(\frac{L/K}{\mathfrak{p}})$; c'est le **symbole d'Artin**.

Exemple : pour $K = \mathbb{Q}$, $L = \mathbb{Q}[\zeta_n]$ (resp. $L = \mathbb{Q}[\sqrt{m}]$) et p non ramifié, on a $(\frac{L/K}{\mathfrak{p}})$ est défini par $\zeta_n \mapsto \zeta_n^p$ (resp. par $(\frac{m}{p})$) en identifiant le groupe de Galois à $\{\pm 1\}$.

Lemme I.2.28. — Soit $L = \mathbb{Q}[\zeta_l]$ et $H = (\mathbb{F}_l^\times)^2 \subset \text{Gal}(L/\mathbb{Q})$ et on pose $M = L^H$.

(i) $M = \mathbb{Q}[\sqrt{l^*}]$ avec $l^* = (-1)^{(l-1)/2}$.

(ii) $p \neq l$ est non ramifié dans L et M et la restriction à M de $(\frac{L/\mathbb{Q}}{\mathfrak{p}})$ est $(\frac{M/\mathbb{Q}}{\mathfrak{p}}) = (\frac{p}{l})$.

Démonstration. — (i) On considère la somme de Gauß : $\tau = \sum_{x \in \mathbb{F}_l^\times} (\frac{x}{l})\zeta_l^x$. On rappelle que $\tau^2 = (\frac{-1}{l})l = l^*$, de sorte que $\mathbb{Q}[\tau]/\mathbb{Q}$ est une extension quadratique. Par ailleurs si $\mathbb{Q} \subset K \subset L$ est une extension quadratique alors p est le seul premier qui peut se ramifier ce qui impose $K = \mathbb{Q}[\sqrt{\pm l}]$. Supposons que $\mathbb{Q}[i\sqrt{l^*}]$ soit contenu dans L , on en déduit alors que $i \in L$ ce qui n'est pas car p est impair.

(ii) $(\frac{M/\mathbb{Q}}{\mathfrak{p}})$ est l'identité si et seulement s'il est dans H d'où $(\frac{M/\mathbb{Q}}{\mathfrak{p}}) = (\frac{p}{l})$. □

Remarque : la loi de réciprocité quadratique découle alors des égalités $(\frac{M/\mathbb{Q}}{\mathfrak{p}}) = (\frac{l^*}{\mathfrak{p}}) = (\frac{p}{l})$.

CHAPITRE II

NOMBRES PREMIERS

Commençons par une citation du grand Euler : « Les mathématiciens ont tâché jusqu'ici en vain de découvrir quelque ordre dans la progression des nombres premiers, et l'on a lieu de croire que c'est un mystère auquel l'esprit humain ne saura jamais pénétrer. Pour s'en convaincre, on n'a qu'à jeter les yeux sur les tables des nombres premiers que quelques-uns se sont donné la peine de continuer au-delà de cent mille et l'on s'apercevra d'abord qu'il n'y règne aucun ordre ni règle. » Ne nous décourageons pas pour autant et essayons de voir ce que l'on peut actuellement dire sur le sujet.

II.1. Comment produire des nombres premiers

Une façon naïve de produire tous les nombres premiers plus petit qu'un entier N fixé à l'avance, consiste à mettre en oeuvre le crible d'Ératosthène : on écrit tous les entiers $\leq N$ puis on supprime tous les multiples de 2 qui sont > 2 , puis les multiples de 3 qui sont > 3 et ainsi de suite. À chaque étape, on sélectionne le premier nombre non barré strictement supérieur au nombre premier dont on vient de supprimer tous les multiples : celui-ci est un nombre premier. La liste obtenue est celle de tous les premiers $\leq N$.

Bien entendu l'algorithme proposé n'est pas efficace, on en cherche d'autres. En outre on peut aussi s'intéresser aux problématiques suivantes :

- comment produire de nombreux nombres premiers ?
- comment battre le record du monde du plus grand nombre premier ?

II.1.1. Théorème de Dirichlet. — Considérons un polynôme $P(X) = aX + b$ en une variable de degré 1 avec $a, b \in \mathbb{Z}$. On se demande si un tel polynôme est à même de produire une infinité de nombre premiers. La réponse est donnée par le fameux théorème de Dirichlet.

Définition II.1.1. — Pour a, q des entiers on note

$$P_q(a) = \lim_{n \rightarrow +\infty} \frac{\#\{p \in \mathcal{P} : p \leq n \text{ et } p \equiv a \pmod{q}\}}{\#\{p \in \mathcal{P} : p \leq n\}}.$$

Remarque : évidemment dès que $a \wedge q \neq 1$, il y a soit aucun soit exactement un premier $p \equiv a \pmod{q}$, de sorte que $P_q(a) = 0$. Le théorème de Dirichlet traite le cas intéressant où $a \wedge q = 1$.

Théorème II.1.2. — Pour $a \wedge q = 1$, on a

$$P_q(a) = \frac{1}{\varphi(q)}$$

où φ est l'indicatrice d'Euler.

Remarque : autrement dit, les nombres premiers se répartissent équitablement selon leur congruence modulo q .

Remarque : le cas $a = 1$ est relativement simple à prouver et ne nécessite pas l'utilisation d'argument d'analyse contrairement au cas général, pour l'instant. En utilisant la loi de réciprocité quadratique, on peut montrer quelques cas simples.

Proposition II.1.3. — *Il existe une infinité de nombres premiers p tels que*

- (a) $p \equiv 3 \pmod{4}$; (b) $p \equiv 1 \pmod{4}$;
 (c) $p \equiv 1 \pmod{2^m}$; (d) $p \equiv 5 \pmod{6}$;
 (e) $p \equiv 5 \pmod{8}$; (f) $p \equiv 1 \pmod{6}$;
 (g) $p \equiv -1 \pmod{12}$; (h) $p \equiv -1 \pmod{10}$.

Démonstration. — Le schéma de démonstration sera toujours le même : on raisonne par l'absurde en supposant la finitude de l'ensemble considéré et on construit un entier N qui permet d'aboutir à une contradiction. On note n le plus grand élément de l'ensemble supposé fini. Toute la difficulté revient donc à construire N en fonction de n et de l'ensemble considéré :

(a) $N = n! - 1$; si p divise N alors $p > n$ et donc $p \equiv 1 \pmod{4}$ de sorte que $N \equiv 1 \pmod{4}$ ce qui n'est pas.

(b) $N = (n!)^2 + 1$; si p premier divise N alors -1 est un carré modulo p soit $p \equiv 1 \pmod{4}$ et donc par hypothèse $p \leq n$ soit p divise $n!$ et donc $p|N - (n!)^2 = 1$ d'où la contradiction.

(c) si p divise $a^{2^{m-1}} + b^{2^{m-1}}$ avec p premier avec a , alors $\frac{a}{b}$ est d'ordre divisant 2^m et d'ordre distinct de 2^{m-1} ; il est donc d'ordre 2^m . Or l'ordre de tout élément divise le cardinal du groupe soit $p \equiv 1 \pmod{2^m}$. Soit alors $N = (n!)^{2^{m-1}} + 1$; tout diviseur p premier de N est congru à $1 \pmod{2^n}$ et supérieur à n d'où la contradiction.

(d) $p \equiv 5 \pmod{6}$ est équivalent à $p \equiv 1 \pmod{2}$ et $p \equiv 2 \pmod{3}$ soit $p > 2$ et $p \equiv 2 \pmod{3}$. Soit $N = n! - 1$; pour p premier divisant N , on a $p > n$ et donc $p \equiv 1 \pmod{3}$ de sorte que $N \equiv 1 \pmod{3}$ ce qui n'est pas.

(e) $N = 3^2 5^2 7^2 11^2 \dots n^2 + 2^2$; N est visiblement impair. Soit alors p premier divisant N , p ne divise pas 4, de sorte que $p \equiv 1 \pmod{4}$, soit $p \equiv 1, 5 \pmod{8}$. À nouveau $p \equiv 5 \pmod{8}$ est exclu car sinon p diviserait $4 = N - 3^2 \dots n^2$. On en déduit donc $N \equiv 1 \pmod{8}$. Or si p est premier impair on a $p \equiv 1, 3, 5, 7 \pmod{8}$ et on vérifie aisément que p^2 est alors congru à 1 modulo 8 et donc $N \equiv 5 \pmod{8}$, d'où la contradiction.

(f) $p \equiv 1 \pmod{6}$ est équivalent à $p > 2$ et $p \equiv 1 \pmod{3}$. Or si p divise $a^2 + 3b^2$ et p premier avec b , alors -3 est un carré modulo p et donc $\left(\frac{-3}{p}\right) = 1 = (-1)^{(p-1)(3-1)/4} \left(\frac{p}{3}\right) \left(\frac{-1}{p}\right) = \left(\frac{p}{3}\right)$ et donc -3 est un carré modulo p si et seulement si $p \equiv 1 \pmod{3}$. Soit alors $N = 3(n!)^2 + 1$; tout diviseur premier de N est alors congru à 1 modulo 3 et supérieur à n d'où la contradiction.

(g) si p divise $a^2 - 3b^2$ et p premier avec b alors 3 est un carré modulo p . Or on a $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) (-1)^{(p-1)/2}$ et donc 3 est un carré modulo p dans les deux situations suivantes :

- $\left(\frac{p}{3}\right) = (-1)^{(p-1)/2} = 1$ soit $p \equiv 1 \pmod{3}$ et $p \equiv 1 \pmod{4}$ soit $p \equiv 1 \pmod{12}$;
- $\left(\frac{p}{3}\right) = (-1)^{(p-1)/2} = -1$ soit $p \equiv -1 \pmod{3}$ et $p \equiv -1 \pmod{4}$ soit $p \equiv -1 \pmod{12}$;

Soit alors $N = 3(n!)^2 - 1$; tout diviseur premier p de N est alors congru à ± 1 modulo 12 et supérieur à n de sorte que par hypothèse, $p \equiv 1 \pmod{12}$. On en déduit alors que $N \equiv 1 \pmod{12}$ ce qui n'est pas car $N \equiv -1 \pmod{12}$.

(h) pour p premier $p \equiv -1 \pmod{10}$ si et seulement si $p \equiv -1 \pmod{5}$. Or si p divise $a^2 - 5b^2$ avec p premier avec b alors $\left(\frac{5}{p}\right) = 1 = \left(\frac{p}{5}\right)$ et donc $p \equiv \pm 1 \pmod{5}$. Soit alors

$N = 5(n!)^2 - 1$; tout diviseur premier p de N est strictement supérieur à n et congru à ± 1 mod 5. Par hypothèse il est donc congru à 1 modulo 5 et donc N aussi ce qui n'est pas. \square

Théorème II.1.4. — (*van der Waerden 1927*)

Soient k, r deux entiers positifs ; il existe alors une constante $M(k, r)$ tel que pour toute partition de $\{1, \dots, M(k, r)\}$ en r parties, il en existe au moins une contenant une suite arithmétique de longueur k .

En 1936 Erdős et Turán ont conjecturé que tout sous-ensemble de \mathbb{N} « suffisamment dense » devait contenir des progressions arithmétique de longueur k , résultat prouvé par Szemerédi en 1974.

Théorème II.1.5. — (*Szemerédi 1974*)

Soit k un entier strictement positif et soit $\delta > 0$. Il existe alors un entier $N(k, \delta)$ tel que tout sous ensemble de $\{1, 2, \dots, N(k, \delta)\}$ de cardinal $\geq \delta N$ contient une progression arithmétique de longueur k .

Remarque : considérons l'ensemble de tous les entiers auquel on retire pour tout $n \geq 1$, les segments $\{2^n + 1, \dots, 2^n + n\}$. Visiblement ce sous-ensemble est de densité égal à 1 et ne contient aucune progression arithmétique de longueur infini. En revanche le théorème de Szemerédi, nous dit qu'il contient des progressions arithmétique de longueur k pour tout $k \geq 1$.

Remarque : l'ensemble des nombres premiers est de densité nulle, de sorte que le théorème de Szemerédi ne s'applique pas. Cependant, en réutilisant astucieusement ce résultat, Ben Green et Terence Tao ont réussi le tour de force de montrer que le résultat était encore valable.

Théorème II.1.6. — (*Ben Green et Terence Tao 2004*)

L'ensemble \mathcal{P} des nombres premiers admet des progressions arithmétiques de longueur arbitraire.

Remarque : ainsi pour tout entier k , il existe a et b tels que

$$a, a + b, a + 2b, \dots, a + (k - 1)b \in \mathcal{P}$$

Par exemple pour $k = 10$ le plus petit a est 199 avec $b = 210$ ce qui donne

$$199, 409, 619, 1039, 1249, 1459, 1669, 1879, 2089.$$

Étant donné k on peut noter a_k et b_k les plus petits entiers tels que $a_k + ib_k$ soient premiers pour tout $i = 0, \dots, k - 1$; Green et Tao donne une majoration de la taille de $a_k + (k - 1)b_k$ en fonction de k .

II.1.2. Familles polynomiales. — On cherche des polynômes dont les valeurs sur \mathbb{N} produisent une infinité de nombres premiers.

Conjecture II.1.7. — (*Hardy-Littlewood*)

Soit $P(n)$ le cardinal de l'ensemble des nombres premiers inférieurs à n de la forme $a^2 + 1$; alors

$$P(n) \sim c\sqrt{n} \ln n, \quad c = \prod_{p \geq 3} \left(1 - \frac{\left(\frac{-1}{p}\right)}{p-1}\right) \approx 1,3727.$$

Remarque : Iwaniec a prouvé qu'il y avait une infinité d'entiers n pour lesquels $n^2 + 1$ est le produit d'au plus deux facteurs premiers. Par ailleurs on sait que le plus grand facteur premier de $a^2 + 1$ tend vers l'infini avec a .

On peut bien entendu considérer d'autres polynômes. Ainsi Sierpinski a montré que pour tout $k \geq 1$, il existe b pour lequel $\{a^2 + b : a \in \mathbb{N}\}$ contient au moins k nombres premiers distincts. Toujours avec des polynômes de degré 2, Jacobson nous propose

$$x^2 + x + 3399714628553118047$$

dont il pense qu'il produit encore plus de premiers.

II.1.3. L'ensemble des nombres premiers n'est pas algébrique. — Commençons par une première question très optimiste :

Question : existe-t-il un polynôme P tel que $P(\mathbb{N})$ est l'ensemble \mathcal{P} des nombres premiers ?

Proposition II.1.8. — *Il ne peut pas exister de polynômes de $\mathbb{Z}[X]$ non constant ne prenant sur \mathbb{N} que des valeurs premières.*

Démonstration. — Soit $P(X) = a_n X^n + \dots + a_0$ de sorte qu'en particulier $a_0 \in \mathcal{P}$. Comme $P(n)$ tends vers l'infini quand n tends vers l'infini, il existe une valeur n_0 à partir de laquelle $P(n) > a_0$. Ainsi pour k assez grand, on a $P(ka_0) > a_0$ alors que $P(ka_0)$ est divisible par a_0 . \square

On modifie alors la question initiale en cherchant des polynômes dont les premières valeurs sont premières. Pour des polynômes du second degré, citons les résultats suivant :

- *spirales d'Ulam* : il s'agit des premiers p pour lesquels $n^2 + n + p$ est premier pour $n = 0, \dots, p - 2$: on remarquera en effet que p divise $(p - 1)^2 + (p - 1) + p$, cf. aussi l'exercice ?? . Heegner a montré que les seuls p qui conviennent sont 2, 3, 5, 16 et 41. On conjecture que pour tout A , il existe B tel que $n^2 + n + B$ soit premier pour tout $n = 0, \dots, A$. Pour $A = 41$, B est nécessairement plus grand que 10^{18} et n'est pas connu.
- R. Ruby : $103n^2 - 3945n + 32381$ est premier pour $n = 0, 1, \dots, 42$;
- G. Fung : $47n^2 - 1701n + 10181$ est premier pour $n = 0, 1, \dots, 42$;
- R. Ruby : $36n^2 - 810n + 2753$ est premier pour $n = 0, 1, \dots, 44$.

On peut alors essayer de considérer des polynômes en plusieurs variables mais la situation n'est pas plus favorable.

Proposition II.1.9. — *Un polynôme $P(X_1, \dots, X_k) \in \mathbb{C}[X_1, \dots, X_r]$ qui ne prend que des valeurs premiers sur \mathbb{N}^r , est constant.*

Démonstration. — Soient K un corps de caractéristique nulle et L_0, L_1, \dots, L_n les polynômes de Lagrange pour $\{0, 1, \dots, n\}$. Rappelons alors que pour tout $Q \in K_n[X]$, on a l'égalité

$$Q(X) = \sum_{i=0}^n Q(x_i) L_i(X).$$

Ainsi en raisonnant par récurrence sur r , si $P \in \mathbb{C}[X_1, \dots, X_r]$, vu comme un polynôme en la variable X_r sur le corps des fractions $\mathbb{C}(X_1, \dots, X_{r-1})$, ne prend que des valeurs entières pour tout $(x_1, \dots, x_r) \in \mathbb{N}^r$ alors $P \in \mathbb{Q}[X_1, \dots, X_r]$. Notons l un multiple des dénominateurs des coefficients de P et prenons r minimal tel qu'on puisse considérer P comme un polynôme en

r variables. On suppose $r \geq 1$. Comme par hypothèse $P(1, \dots, 1) = p$ est premier, pour tous $n_1, \dots, n_r \in \mathbb{N}$, on a

$$P(1 + n_1lp, 1 + n_2lp, \dots, 1 + n_rlp) \equiv P(1, \dots, 1) \pmod{p}$$

et donc est égal à p . En particulier

$$Q_r(X_r) = P(1 + n_1lp, \dots, 1 + n_{r-1}lp, X_r) - p$$

qui admet une infinité de racines, est donc constant et donc $P \in \mathbb{Q}[X_1, \dots, X_{r-1}]$ ce qui contredit la minimalité de r et donc $r = 0$ et P est un polynôme constant. \square

Remarque : rappelons qu'une fonction F en les variables X_1, \dots, X_r est dite *algébrique* s'il existe $P \in \mathbb{C}[X, X_1, \dots, X_r]$ telle que

$$P\left(F(X_1, \dots, X_r), X_1, \dots, X_r\right) = 0.$$

On peut montrer qu'une fonction algébrique qui ne prend que des valeurs entières sur \mathbb{N}^r est nécessairement polynomiale de sorte que \mathcal{P} ne peut pas non plus être représenté par une fonction algébrique. On peut alors regarder les fonctions exponentielles, mais à nouveau la conclusion est négative.

Théorème II.1.10. — *Supposons qu'il existe :*

- des entiers $m, n \geq 1$,
- des polynômes $P_i, Q_i \in \mathbb{C}[X_1, \dots, X_n]$ pour $i = 1, \dots, m$,
- des entiers strictement positifs a_1, \dots, a_m

tels que la fonction

$$F(x_1, \dots, x_n) = \sum_{i=1}^m P_i(x_1, \dots, x_n) a_i^{Q_i(x_1, \dots, x_n)}$$

ne prend que des valeurs premières sur \mathbb{N}^r , alors F est constante.

Démonstration. — En raisonnant par récurrence sur n , il suffit comme d'habitude de traiter le cas $n = 1$. Si $F(\mathbb{N})$ est infini, il existe alors x_1 tel que $F(x_1) = p$ est premier avec tous les a_i . D'après le théorème de Fermat, on en déduit que $F(x_1 + kp(p-1)) \equiv p \pmod{p}$ et donc pour tout k

$$F(x_1 + kp(p-1)) = p$$

et donc $F(X) - p$ admet une infinité de racines et est donc nul. Si $F(\mathbb{N})$ est fini, alors il existe p tel que $F(x) - p$ admet une infinité de racines et est donc nul. \square

II.1.4. L'ensemble des nombres premiers est diophantien. —

Définitions II.1.11. — *Un sous-ensemble E de \mathbb{N} est dit :*

- récursivement énumérable s'il existe « un programme » \mathcal{P} tel que $n \in E$ si et seulement si \mathcal{P} appliqué à n répond « oui » en temps fini.
- diophantien s'il existe un entier $n > 0$ et $P \in \mathbb{Z}[T, X_1, \dots, X_n]$ tel que

$$t \in E \Leftrightarrow \exists (x_1, \dots, x_n) \in \mathbb{N}^n : P(t, x_1, \dots, x_n) = 0.$$

Remarque : tant que le programme ne répond pas, on ne peut pas savoir si n appartient ou n'appartient pas à E . En outre si $n \notin E$ alors le programme peut ne jamais répondre. Un ensemble est dit *récuratif* s'il est récursivement énumérable et si en plus $\mathcal{P}(n)$ répond « non » si $n \notin E$. De manière très simple, le lecteur vérifiera qu'un ensemble E est récuratif si et seulement si E et son complémentaire sont récursivement énumérables. Plus subtil en revanche est le fait qu'il existe des ensembles qui sont récursivement énumérables sans être récuratifs.

Remarque : en considérant le polynôme

$$Q(T, X_1, \dots, X_n) := T(1 - P(T, X_1, \dots, X_n)^2),$$

on voit qu'une définition équivalente de la propriété d'être diophantien, est qu'il existe $Q \in \mathbb{Z}[T, X_1, \dots, X_n]$ tel que E est l'ensemble des valeurs strictement positives prises par Q sur \mathbb{N}^{n+1} .

Exemples : les ensembles habituels de l'arithmétique sont récuratifs :

- l'ensemble des carrés de \mathbb{N} est récuratif : le programme consiste par exemple à calculer tous les carrés de manière croissante jusqu'à dépasser n ;
- l'ensemble \mathcal{P} des nombres premiers est récuratif : on peut construire un programme à partir du crible d'Eratostène.

Un ensemble diophantien est clairement récursivement énumérable, un programme consistant simplement à calculer tous $P(t, x_1, \dots, x_n)$ selon, par exemple, $x_1 + \dots + x_n = k$. La réciproque est un théorème remarquable de Matijasevic, initié par Davis, Robinson et Putnam.

Théorème II.1.12. — (Matijasevic)

Tout ensemble récursivement énumérable est diophantien.

Ainsi l'ensemble \mathcal{P} des nombres premiers est diophantien et il existe donc des polynômes dont l'ensemble des valeurs positives est égal à \mathcal{P} .

Théorème II.1.13. — (P. Jones 1976)

L'ensemble des valeurs entières positives prises par le polynôme suivant, de degré 25 en 26 variables, est l'ensemble \mathcal{P} des nombres premiers.

$$\begin{aligned} & (k+2) \left[1 - \left((wz+h+j-q)^2 + (gk+2g+k+1)(h+j)+h-z \right)^2 + (16(k+1)^3(k+2)(n+1)^2+1-f^2)^2 \right. \\ & \quad + (2n+p+q+z-e)^2 + (e^3(e+2)(a+1)^2+1-o^2)^2 + ((a^2-1)y^2+1-x^2)^2 \\ & \quad + (16r^2y^4(a^2-1)+1-u^2)^2 + (((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2)^2 \\ & \quad + ((a^2-1)l^2+1-m^2)^2 + (ai+k+1-l-i)^2 + (n+l+v-y)^2 + (p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m)^2 \\ & \quad \left. + (q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x)^2 + (z+pl(a-p)+t(2ap-p^2-1)-pm)^2 \right] \end{aligned}$$

Schéma de la preuve : on construit d'abord un polynôme $M(k, x_1, \dots, x_n)$ tel que

$$k+2 \in \mathcal{P} \Leftrightarrow \exists x_1, \dots, x_n \in \mathbb{N}^n : M(k, x_1, \dots, x_n) = 0,$$

où M est une somme de carré et donc positif ou nul. Le polynôme P est alors donné par

$$(k+2)(1 - M(k, x_1, \dots, x_n)).$$

La construction de $M(k, x_1, \dots, x_n)$ part du théorème de Wilson, $k + 1$ est premier si et seulement si $k + 1 | k! + 1$. On utilise ensuite la résolution explicite des équations de Pell-Fermat pour traduire une égalité $f = k!$ par l'existence d'entiers positifs j, h, n, p, q, w, z tels que :

$$\begin{aligned} (1) \quad q &= wz + h + j, & (4) \quad p &= (n + 1)^k, \\ (2) \quad z &= f(h + j) + h, & (5) \quad q &= (p + 1)^n, \\ (3) \quad (2k)^3(2k + 2)(n + 1)^2 + 1 & \text{est un carré parfait,} & (6) \quad z &= p^{k+1} \end{aligned}$$

La construction du polynôme découle alors directement de la formulation suivante : $k + 1$ est premier si et seulement s'il existe 26 entiers positifs notés par les 26 lettres de l'alphabet tels que :

$$\begin{aligned} (1) \quad q &= wz + h + j, & (8) \quad (x + cu)^2 &= ((a + u^2(u^2 - a)^2 - 1)(n + 4dy)^2 + 1, \\ (2) \quad z &= (gk + g + k)(h + j) + h, & (9) \quad m^2 &= (a^2 - 1)l^2 + 1, \\ (3) \quad (2k)^3(2k + 2)(n + 1)^2 + 1 &= f^2, & (10) \quad l &= k + i(a - 1), \\ (4) \quad e &= p + q + z + 2n, & (11) \quad n + l + v &= y, \\ (5) \quad e^3(e + 2)(a + 1)^2 + 1 &= o^2, & (12) \quad m &= p + l(a - n - 1) + b(2a(n + 1) - (n + 1)^2 - 1), \\ (6) \quad x^2 &= (a^2 - 1)y^2 + 1, & (13) \quad x &= q + y(a - p - 1) + s(2a(p + 1) - (p + 1)^2 - 1), \\ (7) \quad u^2 &= 16(a^2 - 1)r^2y^4 + 1, & (14) \quad pm &= z + pl(a - p) + t(2ap - p^2 - 1). \end{aligned}$$

Les équations (6), (7), (8) et (11) traduisent le fait que $(x, y) = (x_a(n), y_a(n))$ est la n -ième solution de l'équation de Pell-Fermat

$$X^2 - (a^2 - 1)Y^2 = 1,$$

dont on rappelle qu'elles s'obtiennent via les suites de Lucas :

$$\begin{aligned} x_a(0) &= 1, \quad x_a(1) = a, \quad x_a(n + 2) = 2ax_a(n + 1) - x_a(n), \\ y_a(0) &= 0, \quad y_a(1) = 1, \quad y_a(n + 2) = 2ay_a(n + 1) - y_a(n). \end{aligned}$$

L'équation (9) implique que $(m, l) = (x_a(k'), y_a(k'))$ pour $k' \in \mathbb{N}$ et en utilisant (3), (4) et (5), on montre que $k' = k$. De (12), on déduit que $p = (n + 1)^k$ et de (13) que $q = (p + 1)^n$. Enfin de (14) on obtient $z = p^{k+1}$, de sorte qu'on se ramène aux conditions (1-6) précédentes et donc $k! = f = gk + g + k$ soit $k! + 1 = (g + 1)(k + 1)$ et donc $k + 1$ est premier.

Remarque : le polynôme précédent prend aussi des valeurs négatives, -76 par exemple. Bien entendu un polynôme représentant diophantiennement \mathcal{P} n'est pas unique et on peut demander à minimiser soit le nombre de variables, soit le degré. On ne connaît pas la réponse à ces questions signalons qu'il existe un polynôme de degré 5 et en 42 variables, et un autre en 12 variables dont le degré est très grand.

Remarque : avec les notations précédentes, la fonction $2 + k0^{M(x_1, \dots, x_n)}$ a ses valeurs dans \mathcal{P} sur \mathbb{N}^n . Nous invitons le lecteur à confronter ce résultat avec le théorème II.1.10

Corollaire II.1.14. — Notons p_n le n -ième nombre premier. Il existe alors un polynôme $P(T, X_1, \dots, X_r) \in \mathbb{Z}[T, X_1, \dots, X_r]$ tel que

$$p_n = m \Leftrightarrow \exists (x_1, \dots, x_r) \in \mathbb{N}^r : P(n, x_1, \dots, x_r) = m.$$

Démonstration. — La relation $p_n = m$ étant clairement récursive, elle est diophantienne de sorte qu'il existe un polynôme Q tel que

$$p_n = m \Leftrightarrow \exists x_1, \dots, x_l \in \mathbb{N}^l : Q(n, m, x_1, \dots, x_k) = 0.$$

Il suffit alors de poser $P = x_{l+1} \left(1 - Q^2(n, x_{l+1}, x_1, \dots, x_l) \right)$. □

II.1.5. Autour du théorème de Wilson. — Commençons par rappeler le théorème de Wilson.

Théorème II.1.15. — (de Wilson)

Un entier $n \geq 2$ est premier si et seulement si n divise $(n-1)! + 1$.

Démonstration. — Si p est un diviseur non trivial de n , i.e. $1 < p < n$ alors $p \leq n-1$ et $p|(n-1)!$ de sorte que p ne divise pas $(n-1)! + 1$. Réciproquement si $n = p \geq 3$ est premier alors d'après le petit théorème de Fermat

$$X^{p-1} - 1 = \prod_{a \in \mathbb{F}_p^\times} (X - a)$$

de sorte que dans \mathbb{F}_p , on a

$$-1 = (-1)^{p-1} \prod_{a \in \mathbb{F}_p^\times} a = (p-1)!,$$

d'où le résultat. □

Proposition II.1.16. — La fonction

$$f(n) = 2 + 2(n!) \pmod{n+1}$$

a pour valeurs, l'ensemble des nombres premiers.

Remarque : le lecteur notera cependant qu'elle ne produit que très lentement de nouveaux nombres premiers; en particulier 2 apparaît très souvent.

Démonstration. — Soit p premier alors d'après le théorème de Wilson p divise $1 + (p-1)!$ et donc $2 + 2(p-1)! \equiv 0$ soit $f(p-1) = p$. Si n n'est pas premier alors n divise $(n-1)!$ et donc $f(n-1) = 2$. □

Théorème II.1.17. — (1947 W. Mills)

Il existe une constante A telle que pour tout $n > 1$,

$$\lfloor A^{3^n} \rfloor \in \mathcal{P}.$$

Remarque : la constante A en question se calcule de manière certes approchée 1,306377883863 mais ce calcul nécessite la connaissance de \mathcal{P} ce qui convenons le n'est pas très honnête. L'escroquerie est du même genre que la suivante : posons

$$L = 0,2003000050000007000000011\dots$$

le n -ème nombre premier étant placé en position n^2 , i.e. le chiffre des unités de p_n est placé en position n^2 . On vérifie alors aisément que

$$\lfloor L \times 10^{n^2} \rfloor - \lfloor L \times 10^{(n-1)^2} \rfloor 10^{2n-1}$$

est égal au n -ème nombre premier p_n . On s'interdit désormais d'utiliser des nombres pouvant cacher une infinité d'informations.

Théorème II.1.18. — (Roland Yéléhada)

Pour tout n ,

$$t(n) = 2 + n \lfloor \frac{1}{1 + \sum_{p=2}^{n+1} \lfloor \frac{n+2}{p} - \lfloor \frac{n+1}{p} \rfloor \rfloor} \rfloor$$

est toujours un nombre premier. Plus précisément, si on enlève le nombre 2 dans la suite $(t(n))_{n \in \mathbb{N}}$, on obtient la liste des nombres premiers dans l'ordre croissant.

Démonstration. — Le principe est très élémentaire : si $n+2$ est un multiple de p alors $(n+2)/p$ est un entier q et donc $(n+1)/p = q - 1/p$ et donc $\lfloor \frac{n+2}{p} - \lfloor \frac{n+1}{p} \rfloor \rfloor$ est égal à 1 alors qu'il est nul si p n'est pas un diviseur. Autrement dit la somme compte le nombre de diviseurs de $n+2$ compris entre 2 et $n+1$; ainsi si $n+2$ est premier on obtient $t(n) = n+2$ qui est premier alors que si $n+2$ n'est pas premier on a $t(n) = 2$. \square

Remarque : ainsi la formule ne donne que des nombres premiers mais très lentement, 2 apparaissant très souvent. En utilisant la formule de Wilson, Minac simplifie la formule précédente :

$$t(n) = 2 + n \lfloor \frac{(n+1)! + 1}{n+2} - \lfloor \frac{(n+1)!}{n+2} \rfloor \rfloor$$

laquelle contient moins de symbole et n'a plus de somme, mais requiert de lourds calculs de factoriels.

Théorème II.1.19. — (1995 Minac et Willans)

Soit

$$\pi(m) = \sum_{j=2}^m \frac{\sin^2\left(\frac{\pi}{j}(j-1)!\right)}{\sin^2\left(\frac{\pi}{j}\right)} = \sum_{j=2}^m \lfloor \frac{(j-1)! + 1}{j} - \lfloor \frac{(j-1)!}{j} \rfloor \rfloor$$

alors le n -ème nombre premier p_n est donné par

$$p_n = 1 + \sum_{m=1}^{2^n} \lfloor \lfloor \frac{n}{1 + \pi(m)} \rfloor \rfloor^{1/n}.$$

Remarque : on notera que la formule donnant p_n ne nécessite que 52 symboles et est donc relativement simple.

Théorème II.1.20. — (2000, Ruiz)

On a a

$$p_n = 1 + \sum_{k=1}^{2(\lfloor n \ln n \rfloor + 1)} \left(1 - \lfloor \frac{\psi(k)}{n} \rfloor\right)$$

où $\psi(k) = k - 1 + \sum_{j=2}^k \lfloor \frac{2}{j} \left(1 + \sum_{s=1}^{\lfloor \sqrt{j} \rfloor} \left(\lfloor \frac{j-1}{s} \rfloor - \lfloor \frac{j}{s} \rfloor\right)\right) \rfloor$.

Remarque : très récemment, un étudiant a prouvé le résultat suivant.

Théorème II.1.21. — (Rowland 2008)

Soit a_n la suite définie par récurrence :

$$a_1 = 7 \quad \text{et} \quad a_n = a_{n-1} + n \wedge a_{n-1}.$$

Alors la suite $b_n = a_n - a_{n-1}$ ne prend que ses valeurs que dans $\mathcal{P} \cup \{1\}$.

Remarque : signalons aussi la suite de Perrin définie par

$$u_0 = 3, u_1 = 0, u_2 = 2 \quad u_{n+1} = u_{n-1} + u_{n-2}.$$

Lucas a montré que pour p premier p divise u_p et on conjecture que la réciproque est vraie.

II.2. Tests de primalité

II.2.1. Nombres de Fermat. — Comme -1 est racine du polynôme $X^{2n+1} + 1$ celui-ci est divisible par $X + 1$, le quotient étant égal à $X^{2n} - X^{2n-1} + \dots + 1$. Soit alors $m = 2^n k$ avec k impair ; si $k > 1$, l'égalité

$$2^m + 1 = (2^{2^n})^k + 1 = (2^{2^n} + 1)((2^{2^n})^{k-1} - \dots + 1)$$

montre que $2^{2^n} + 1$ est un diviseur propre de sorte que $2^m + 1$ n'est pas premier. Ainsi si l'on veut trouver des nombres premiers parmi la famille des $2^m + 1$, il faut prendre m de la forme 2^n . On pose alors pour tout $n \in \mathbb{N}$, $F_n = 2^{2^n} + 1$; F_n est le n -ème nombre de Fermat. On calcule $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ et $F_4 = 65537$ et l'on vérifie aisément qu'ils sont tous premiers.

Lemme II.2.1. — Soit p premier divisant F_n , alors $p \equiv 1 \pmod{2^{n+1}}$.

Démonstration. — Pour un tel p , de la congruence $2^{2^n} \equiv -1 \pmod{p}$, on en déduit que 2 est d'ordre 2^{n+1} dans \mathbb{F}_p^\times de sorte que 2^{n+1} divise $p - 1$. \square

Ainsi pour $n = 5$, un diviseur de F_5 doit être de la forme $64k + 1$. Vérifions que le cas $k = 10$ est un bon candidat : déjà 641 est premier et on l'écrit sous la forme $641 = 1 + 5 \cdot 2^7$. Dans le corps $\mathbb{Z}/641\mathbb{Z}$, on a $0 = 641 = 1 + 5 \cdot 2^7$ soit $2^7 = -1/5$. Ainsi $F_5 = 2^{32} + 1 = (2^7)^4 \cdot 2^4 + 1$ car $32 = 7 \cdot 4 + 4$. D'où dans $\mathbb{Z}/641\mathbb{Z}$, on a $F_5 = (-1/5)^4 \cdot 2^4 + 1 = (2^4 + 5^4)/5^4 = 0$.

Remarque : à ce jour on ne connaît pas d'entiers $n \geq 5$ tels que F_n est premier.

Lemme II.2.2. — Pour $n \neq m$, les nombres F_n et F_m sont premiers entre eux.

Démonstration. — Soit $n = m + r$ avec $r > 0$; on a alors

$$2^{2^n} = (((2^{2^m})^{2^m})^{\dots})^{2^m}$$

et dans $\mathbb{Z}/F_m\mathbb{Z}$, on en déduit

$$F_n \equiv (((-1)^{2^m})^{\dots})^{2^m} + 1 = 2 \pmod{F_m}.$$

Ainsi le pgcd de F_m et de F_n divise 2; or 2 ne divise pas F_n d'où le résultat. \square

Remarque : on peut ainsi donner une nouvelle démonstration de la non finitude de l'ensemble \mathcal{P} des nombres premiers positifs. En effet \mathcal{P} contient la réunion disjointe $\coprod_n \mathcal{F}_n$ où \mathcal{F}_n est le sous-ensemble de \mathcal{P} des diviseurs premiers divisant F_n avec \mathcal{F}_n non vide pour tout n puisque $F_n > 1$.

Proposition II.2.3. — (*Critère de Pépin*)

Le nombre de Fermat $p = F_n$ est premier si et seulement si $3^{(p-1)/2} \equiv -1 \pmod{p}$.

Démonstration. — Supposons tout d'abord que $p = F_n \geq 5$ est premier. D'après la loi de réciprocité quadratique, $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = -1$ car $p \equiv (-1)^{2^n} + 1 \equiv 2 \pmod{3}$. D'après le critère d'Euler, on en déduit que $3^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Réciproquement, supposons la congruence vérifiée; $3^{p-1} \equiv 1 \pmod{p}$, de sorte que l'ordre de 3 modulo p est exactement $p-1$ et donc $\mathbb{Z}/p\mathbb{Z}$ est un corps. \square

On peut aussi s'intéresser aux facteurs premiers des nombres de Fermat qui, on l'a vu, sont de la forme $k2^n + 1$. Comme pour les nombres de Fermat, on dispose pour ceux-ci, au moins quand k est relativement petit, de tests de primalité très efficaces qui ont permis de battre des records pour la taille de nombres premiers qui ne sont pas de Mersenne. On conjecture par ailleurs que les nombres de Fermat sont sans facteur carré.

II.2.2. Nombres de Mersenne. — De la factorisation

$$X^{pq} - 1 = (X^p - 1)(X^{p(q-1)} + \dots + X^p + 1),$$

on en déduit que si $2^n - 1$ est premier alors n est un nombre premier.

Définition II.2.4. — Pour p premier, si $M_p = 2^p - 1$ est premier, on le qualifie de nombre premier de Mersenne.

Les premiers exemples sont $3 = 2^2 - 1$, $7 = 2^3 - 1$, $31 = 2^5 - 1$, $127 = 2^7 - 1$ qui sont premiers alors que $2047 = 2^{11} - 1 = 23 \times 89$ ne l'est pas. L'intérêt de ces nombres réside dans le critère de primalité très efficace suivant.

Proposition II.2.5. — (*Critère de Lucas-Lehmer*)

Pour $q \geq 3$, M_q est premier si et seulement si

$$(2 + \sqrt{3})^{2^{q-1}} \equiv -1 \pmod{M_q}.$$

Remarque : si q est un diviseur de M_p alors l'ordre de la classe de 2 dans $\mathbb{Z}/q\mathbb{Z}$ est égale à p qui doit diviser $q-1$ et donc $q \equiv 1 \pmod{p}$ (on a aussi $q \equiv 1 \pmod{2p}$). On en déduit aussi que 2 est un carré modulo q et donc $q \equiv \pm 1 \pmod{8}$.

Démonstration. — Remarquons que 3 est un résidu quadratique modulo $p \neq 2, 3$ si et seulement si $p \equiv \pm 1 \pmod{12}$: en effet d'après la loi de réciprocité quadratique, $\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{(p-1)/2}$ et donc 3 est résidu quadratique modulo p si et seulement si $\left(\frac{p}{3}\right) = (-1)^{(p-1)/2}$. Le seul carré modulo 3 autre que 0 est 1, soit $p \equiv 1 \pmod{3}$ et $p \equiv 1 \pmod{4}$ ou bien $p \equiv 2 \pmod{3}$ et $p \equiv 3 \pmod{4}$, soit en définitive $p \equiv \pm 1 \pmod{12}$.

Lemme II.2.6. — Pour $p > 3$ premier non congru à ± 1 modulo 12, on a le petit théorème de Fermat suivant dans $\mathbb{Z}[\sqrt{3}]$:

$$(x + y\sqrt{3})^p \equiv x - y\sqrt{3} \pmod{p}.$$

Démonstration. — Par hypothèse 3 n'est pas un carré modulo p et par conséquent $\sqrt{3}^p = 3^{(p-1)/2}\sqrt{3} \equiv -\sqrt{3} \pmod{p}$ et donc $(x + y\sqrt{3})^p \equiv x - y\sqrt{3} \pmod{p}$. \square

Supposons alors M_q premier : en remarquant que 2 est un carré modulo M_q , on définit dans $\mathbb{Z}[\sqrt{3}]/(M_q)$: $\tau = \frac{1+\sqrt{3}}{\sqrt{2}}$ et $\bar{\tau} = \frac{1-\sqrt{3}}{\sqrt{2}}$. A partir des relations $\tau^2 = 2 + \sqrt{3}$ et $\tau\bar{\tau} = -1$: $\tau^p = \bar{\tau}$ soit $\tau^{p+1} = -1$ ce qui donne la congruence de l'énoncé $(\tau^2)^{(p+1)/2} \equiv -1 \pmod{p}$ car $\tau^2 = 2 + \sqrt{3}$. \square

Corollaire II.2.7. — (*Test de primalité de Lucas-Lehmer*)

Soit $(L_i)_{i \geq 0}$ la suite de Lucas-Lehmer définie par

$$L_0 = 4 \text{ et } L_{i+1} = L_i^2 - 2 \pmod{M_q}.$$

Alors M_q est premier si et seulement si $L_{q-2} \equiv 0 \pmod{M_q}$.

Démonstration. — Soit $\alpha = 2 + \sqrt{3}$ et $\bar{\alpha} = 2 - \sqrt{3}$, en remarquant que $\alpha\bar{\alpha} = 1$, on montre aisément par récurrence que $L_i = \alpha^{2^i} + \bar{\alpha}^{2^i}$; la congruence $L_i \equiv 0 \pmod{n}$ est ainsi équivalente à $\alpha^{2^{i+1}} \equiv -1 \pmod{n}$, d'où le résultat. \square

Remarque : à ce jour on connaît 45 nombres de Mersenne qui sont premiers; le dernier trouvé possède plus de 10 millions de chiffres et réalise le record du plus grand nombre premier.

II.2.3. Autour du petit théorème de Fermat. —

Définition II.2.8. — Un entier $n \in \mathbb{N}^*$ est dit pseudo-premier de base b si $b^{n-1} \equiv 1 \pmod{n}$.

Par exemple $n = 105 = 3 \cdot 5 \cdot 7$ est pseudo-premier de base 13 : en effet on a $13^{104} = (13^2)^{52} \equiv 1 \pmod{3}$, $13^{104} = (13^4)^{26} \equiv 1 \pmod{5}$ et $13^{104} = (13^6)^{17} \times 13^2 \equiv 1 \pmod{7}$, de sorte que d'après le lemme chinois on a $13^{104} \equiv 1 \pmod{105}$. En revanche on a $2^{104} = (2^6)^{17} \times 2^2 \equiv 4 \pmod{7}$ de sorte que 105 n'est pas pseudo-premier de base 2. Le petit théorème de Fermat dit qu'un nombre premier p est pseudo-premier de base b pour tout b premier à p .

Ce test serait « bon » dans le sens où calculer a^{N-1} requiert, en utilisant l'exponentiation rapide, $O(\log N)$ multiplications; cependant il est « mauvais » à cause des nombres de Carmichael qui vérifient le test sans être premier : le plus petit de ces nombres est $561 = 3 \cdot 11 \cdot 17$ et on sait que l'ensemble de ces nombres est infini. Une amélioration de ce test est donné par le test de *Solovay-Strassen* qui consiste à vérifier les congruences $a^{\frac{N-1}{2}} \equiv (\frac{a}{N}) \pmod{N}$ dont la véracité est assurée par la proposition suivante.

Proposition II.2.9. — Soit $H = \{a \in (\mathbb{Z}/N\mathbb{Z})^\times : a^{\frac{N-1}{2}} \equiv (\frac{a}{N}) \pmod{N}\}$; alors $H = (\mathbb{Z}/N\mathbb{Z})^\times$ si et seulement si N est premier.

Démonstration. — On a déjà vu que si N est premier alors $H = (\mathbb{Z}/N\mathbb{Z})^\times$. Réciproquement si p^2 divise N , il existe alors un élément $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ d'ordre $p(p-1)$ et comme p ne divise pas $N-1$, $a^{N-1} \not\equiv 1 \pmod{N}$. Si $N = pp_2 \cdots p_r$ sans facteurs carrés; par le lemme chinois soit $a \equiv 1 \pmod{p_2 \cdots p_r}$ et a non carré modulo p de sorte que $(\frac{a}{N}) = -1$ mais $a^{(N-1)/2} \equiv 1 \pmod{p_2 \cdots p_r}$ et donc $a^{(N-1)/2} \not\equiv 1 \pmod{N}$. \square

Applications :

- *Test probabiliste :* si N est composé alors comme $[(\mathbb{Z}/N\mathbb{Z})^\times : H] \geq 2$, en prenant a aléatoirement on a au moins une chance sur deux d'avoir $a \notin H$ de sorte que si N passe successivement k tests, on peut dire qu'il est premier avec une probabilité $\geq 1 - 2^{-k}$.
- *Test déterministe sous GRH :* l'hypothèse de Riemann généralisée implique que si N est composé, il existe $a \leq 2(\log N)^2$ qui ne passera pas le test de Solovay-Strassen
- *Test probabiliste de Rabin-Miller :* un entier $n = 1 + 2^k q$ impair, q impair, est dit fortement pseudo-premier de base b si l'une des conditions suivantes est vérifiée :

$$b^q \equiv 1 \pmod{n} \quad \exists 0 \leq j < k, \quad b^{2^j q} \equiv -1 \pmod{n}$$

Si n est premier alors il est fortement pseudo-premier de base b pour tout $1 \leq b < n$: en effet $b^{2^k q} \equiv 1 \pmod{n}$ et soit donc $0 \leq i \leq k$ le plus petit entier tel que $b^{2^i q} \equiv 1 \pmod{n}$.

Si $i = 0$, on a $b^q \equiv 1 \pmod n$ et si $i > 0$ alors $b^{2^{i-1}q} \equiv -1 \pmod n$ car dans un corps $x^2 = 1$ entraîne $x = \pm 1$.

Remarque : si n est fortement pseudo-premier de base b alors il est pseudo-premier de base b : en effet il existe $0 \leq i \leq k$ tel que $b^{2^i q} \equiv 1 \pmod n$; or $2^i q$ divise $n - 1$ de sorte que $b^{n-1} \equiv 1 \pmod n$.

Exemple : $n = 561$ est pseudo-premier de base 13 mais il n'est pas fortement pseudo-premier de base 2 : en effet $n - 1 = 2^4 35$ et $2^{35 2^3} \equiv 1 \pmod{561}$ mais $2^{35 2^2} \equiv 67 \pmod{561}$.

Théorème II.2.10. — (Rabin) Pour n impair soit

$$B_n = \{x \in (\mathbb{Z}/n\mathbb{Z})^\times / n \text{ est fortement pseudo-premier de base } x\}.$$

Alors si n est non premier alors $\frac{|B_n|}{\phi(n)} \leq 1/4$ sauf pour $n = 9$.

Remarque : autrement dit si $|B_n| \geq \phi(n)/4$ alors n est premier. Ainsi si n est fortement pseudo-premier dans m bases tirées au hasard, on peut présumer, avec une probabilité d'erreur inférieure à $1/4^m$, qu'il est premier. Par exemple pour $n = 561$, on obtient $|B_{561}| = 10$ de sorte qu'outre ± 1 , il ne reste plus que 8 entiers qui font croire que 561 est premier et le rapport $\frac{|B_{561}|}{\phi(561)} = 1/32$ est relativement faible. Ce critère est particulièrement adapté à la méthode RSA.

Démonstration. — Soit $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ la décomposition en facteurs premiers de $n = 1 + 2^k q$, q impair ; on écrit $p_i = 1 + 2^{k_i} q_i$ avec q_i impair et $k_1 \leq \cdots \leq k_r$. L'ensemble B_n est la réunion disjointe de $P_n = \{x \in (\mathbb{Z}/n\mathbb{Z})^\times / x^q = 1\}$ et des $Q_n(j) = \{x \in (\mathbb{Z}/n\mathbb{Z})^\times / x^{2^j q} = -1\}$ pour $0 \leq j < k$.

- calcul de $|P_n|$: le théorème chinois donne $P_n \simeq \prod_{i=1}^r P_{p_i^{\alpha_i}}$ avec $|P_{p_i^{\alpha_i}}| = (q, \varphi(p_i^{\alpha_i})) = (q, q_i)$.

- calcul de $|Q_n(j)|$: à nouveau le théorème chinois nous ramène à calculer le cardinal de

$Q_{p_i^{\alpha_i}}(j)$: or ce dernier ensemble est non nul si et seulement si $(-1)^{\frac{\varphi(p_i^{\alpha_i})}{(2^j q, \varphi(p_i^{\alpha_i}))}} = 1$ ce qui est équivalent à $\frac{2^{k_i} q_i}{2^{\inf(j, k_i)} (q, q_i)}$ car $(2^j q, \varphi(p_i^{\alpha_i})) = 2^{\inf(j, k_i)} (q, q_i)$; en effet comme p_i divise n , et que n est premier avec $n - 1 = 2^k q$ alors p_i est premier avec $n - 1$. Ainsi $Q_{p_i^{\alpha_i}}(j)$ est non vide si et seulement si $j < k_i$ et dans ce cas son cardinal est $2^j (q, q_i)$. Finalement si $j \geq k_1$ alors $Q_n(j)$ est vide et si $j < k_1$ alors $|Q_n(j)| = 2^{jr} (q, q_1) \cdots (q, q_r)$. En outre comme $p_i \equiv 1 \pmod{2^{k_i}}$ alors $n \equiv 1 \pmod{2^{k_1}}$ soit $k_1 \leq k$. Ainsi on obtient

$$\sum_{0 \leq j < k} |Q_n(j)| = \sum_{0 \leq j < k_1} |Q_n(j)| = \prod_{i=1}^r (q, q_i) \sum_{0 \leq j < k_1} 2^{jr}$$

ce qui en y ajoutant le calcul du cardinal de P_n , donne

$$|B_n| = (q, q_1) \cdots (q, q_r) \left(1 + \sum_{j=0}^{k_1-1} 2^{jr}\right)$$

et donc $\frac{|B_n|}{\phi(n)} \leq \frac{1 + 2^{k_1 r - 1}}{2^{k_1 r}} K$, avec $K = \prod_{i=1}^r \frac{(q, q_i)}{q_i p_i^{\alpha_i - 1}}$.

Remarque : si tous les k_i ne sont pas tous égaux, on peut améliorer l'inégalité précédente d'un facteur 2.

On obtient ainsi

$$\frac{|B_n|}{\varphi(n)} = \frac{1 + \frac{2^{k_1 r} - 1}{2^r - 1}}{2^{k_1 + \dots + k_r}} K$$

si l'on minore $k_1 + \dots + k_r$ par $r k_1$, on obtient l'inégalité demandée; si en outre tous les k_i ne sont pas égaux k_1 , on peut minorer $k_1 + \dots + k_r$ par $r k_1 + 1$.

Dans le cas où $n = p^\alpha$, on obtient alors $\frac{|B_n|}{\varphi(n)} \leq (q, q_1)/q_1 \leq 1/p_1^{\alpha_1 - 1}$ ce qui donne si $p_1 \geq 5$, $\frac{|B_n|}{\varphi(n)} \leq 1/5$ et si $p_1 = 3$, $\frac{|B_n|}{\varphi(n)} \leq 1/9$ sauf pour $\alpha = 2$, i.e. $n = 9$ auquel cas $B_9 = \{1, -1\}$ et $\varphi(9) = 6$ soit $\frac{|B_9|}{\varphi(9)} = 1/3$.

Dans le cas général, le rapport $\frac{1 + \frac{2^{k_1 r} - 1}{2^r - 1}}{2^{r k_1}}$ qui intervient dans la majoration, est décroissant en k_1 ; on peut donc le remplacer par $1/2^{r-1}$, soit

$$\frac{|B_n|}{\varphi(n)} \leq \frac{1}{2^{r-1}} \prod_{i=1}^r \frac{1}{p_i^{\alpha_i}}$$

Si l'un des α_i est supérieur ou égal à 2, alors $\prod_{i=1}^r \frac{1}{p_i^{\alpha_i - 1}} \leq 1/3$ et donc $\frac{|B_n|}{\varphi(n)} \leq 1/6$. On suppose donc dans la suite que tous les α_i sont égaux à 1 :

cas $r \geq 3$: l'inégalité $\frac{|B_n|}{\varphi(n)} \leq 1/4$ est alors immédiate et l'égalité est obtenue pour $r = 3, k_1 = k_2 = k_3 = 1$ et $q_i | q$ autrement dit si la décomposition primaire de n est $(1 + 2q_1)(1 + 2q_2)(1 + 2q_3)$.

cas $r = 2$ et $k_1 < k_2$ d'après ce qui précède on a la majoration $\frac{|B_n|}{\varphi(n)} \leq \frac{1}{2^2} \prod_{i=1}^2 \frac{(q, q_i)}{q_i} \leq 1/4$, l'égalité étant obtenue si et seulement si $k_1 = 1, k_2 = k_1 + 1 = 2$, q_1 et q_2 divisent q soit $q_1 = q_2$ et la décomposition primaire de n est $(1 + 2q_1)(1 + 4q_1)$, ce qui est le cas étudié plus haut.

cas $r = 2$ et $k_1 = k_2$ on a la majoration $\frac{|B_n|}{\varphi(n)} \leq \frac{1}{2} \prod_{i=1}^2 \frac{(q, q_i)}{q_i}$. Or q_1 et q_2 ne peuvent pas tous deux diviser q ; en effet on a

$$n - 1 = 2^k q = p_1 p_2 - 1 = (1 + 2^{k_1} q_1)(1 + 2^{k_1} q_2) - 1 = 2^{k_1} (q_1 + q_2) + 2^{2k_1} q_1 q_2$$

et si $q_1 | q$ (resp. $q_2 | q$) entraîne $q_1 | q_2$ (resp. $q_2 | q_1$) soit $q_1 = q_2$ puis $p_1 = p_2$ ce qui n'est pas. On en déduit alors $\frac{(q, q_i)}{q_i} \leq 1/3$ pour $i = 1$ ou 2 soit $\frac{|B_n|}{\varphi(n)} \leq 1/6$. □

Remarque : soit $p_1 \equiv 3 \pmod{4}$ premier tel que $p_2 = 2p_1 - 1$ est premier (par exemple $p_1 = 40039, 41011, 42727$). Soit $n = p_1 p_2$: pour $p_1 = 1 + 2q_1$ et $p_2 = 1 + 4q_1$ avec q_1 impair, on écrit $n - 1 = 2q_1(3 + 4q_1) = 2^k q$, soit $k = 1$ et $q = q_1(3 + 4q_1)$. L'ensemble B_n est la réunion disjointe de

$$P_n = \{x \in (\mathbb{Z}/n\mathbb{Z})^\times / x^q = 1\} \quad Q_n = \{x \in (\mathbb{Z}/n\mathbb{Z})^\times / x^q = -1\}$$

Le théorème chinois donne avec des notations évidentes $|P_n| = |P_{p_1}| |P_{p_2}|$ et $|Q_n| = |Q_{p_1}| |Q_{p_2}|$. Or comme $(\mathbb{Z}/p_1\mathbb{Z})^\times$ est cyclique d'ordre $p_1 - 1$, on a $|P_{p_1}| = (q, p_1 - 1) = (q, 2q_1) = (q, q_1) = q_1$. On calcule de même les autres cardinaux et on obtient $|B_n| = 2q_1^2$ et $\phi(n) = 8q_1^2$ et donc finalement $4|B_n| = \phi(n)$.

Remarque : Ainsi si n est fortement pseudo-premier dans m bases tirées au hasard, on peut présumer, avec une probabilité d'erreur inférieure à $1/4^m$, qu'il est premier. Par exemple pour

$n = 561$, on obtient $|B_{561}| = 10$ de sorte qu'outre ± 1 , il ne reste plus que 8 entiers qui font croire que 561 est premier et le rapport $\frac{|B_{561}|}{\varphi(561)} = 1/32$ est relativement faible.

Remarque : en admettant l'hypothèse de Riemann généralisée, dont on peut raisonnablement à la fois penser qu'elle est vérifiée et qu'elle n'est pas prête d'être démontrée, alors si pour tout $2 \leq a \leq 2 \log^2 n$, n est pseudo-premier de base a , nécessairement n est premier. L'algorithme de Rabin-Miller fournit, sous cette hypothèse, une preuve de primalité en $O(\log^4 n)$.

II.2.4. AKS. — En juillet 2002, le professeur Agrawal et deux de ses élèves Kayal et Saxena ont donné le premier test de primalité en temps polynomial. La première version de leur algorithme a été amélioré en 2003 ; nous allons présenter cette dernière version qui ne nécessite au résultat pointu d'algèbre. La complexité de cet algorithme est en revanche beaucoup plus lente que celle de la version conjecturale de l'algorithme de Rabin-Miller.

Proposition II.2.11. — Soient $n \geq 2$ et $a \in \mathbb{Z}$ tels que $a \wedge n = 1$. Alors n est premier si et seulement si

$$(X + a)^n \equiv X^n + a \pmod{n}.$$

Démonstration. — On a déjà vu que pour p premier et pour tout $1 \leq k < p$, le coefficient binomial $\binom{p}{k}$ est divisible par p . Il reste donc à étudier la réciproque. Supposons donc que pour tout $1 \leq i \leq n - 1$, on ait $\binom{n}{i} \equiv 0 \pmod{n}$. Regardons alors les congruences modulo n des $\binom{n-1}{i}$. Pour $i = 1$, on a $\binom{n-1}{1} = n - 1 \equiv -1 \pmod{n}$. De la formule de Pascal

$$\binom{n-1}{i} + \binom{n-1}{i+1} = \binom{n}{i+1}$$

et de l'hypothèse $\binom{n}{i} \equiv 0 \pmod{n}$ pour tout $1 \leq i \leq n - 1$, on en déduit par une récurrence simple que pour tout $1 \leq i \leq n - 1$

$$\binom{n-1}{i} \equiv (-1)^i \pmod{n}.$$

Soit alors d un diviseur strict de n . Rappelons la relation $d \binom{n}{d} = n \binom{n-1}{d-1}$ que l'on interprète combinatoirement comme le nombre de choisir d personnes parmi n et de nommer un chef parmi eux : pour ce faire on peut soit commencer par choisir le groupe puis le chef, ou inversement choisir le chef puis le reste du groupe. D'après ce qui précède on doit donc avoir

$$\binom{n}{d} \equiv 0 \pmod{n} \quad \text{et} \quad \frac{n}{d} \binom{d-1}{n-1} = \frac{n}{d} (-1)^{d-1},$$

soit $\frac{n}{d} (-1)^{d-1} \equiv 0 \pmod{n}$ ce qui n'est possible que pour $d = 1$, i.e. n ne possède qu'un unique diviseur strict et est donc premier. \square

Un premier algorithme élémentaire consisterait ainsi à choisir un entier a premier avec n puis de vérifier si la congruence est satisfaite. Le problème est qu'il faudrait vérifier n coefficients de sorte que la complexité ne pourrait être polynomiale, i.e. en $O(\log^k n)$. Un moyen simple de réduire le nombre de coefficients à calculer est d'évaluer la congruence modulo $X^r - 1$ pour un $r \simeq \ln n$ bien choisi, i.e. de montrer que $(X + a)^n \equiv X^n + a$ est vraie dans $\frac{\mathbb{Z}/n\mathbb{Z}[X]}{(X^r - 1)\mathbb{Z}/n\mathbb{Z}[X]}$.

Comme précédemment, il faut se méfier des nombres de Carmichael. Prenons par exemple $n = 1729 = 7.13.19$ alors pour $a = 5$ et $r = 3$, on a bien

$$(X + 5)^{1729} \equiv X + 5 \pmod{(X^3 - 1)\mathbb{Z}/1729\mathbb{Z}[X]}.$$

En revanche si on prend $r = 5$ alors

$$(X + 5)^{1729} \equiv 1254X^4 + 799X^3 + 556X^2 + 1064X + 1520 \pmod{(X^5 - 1)\mathbb{Z}/1729\mathbb{Z}[X]}.$$

La découverte de AKS est l'existence d'un nombre r tel que la congruence précédente pour plusieurs a déterminés impose la primalité de n . La recherche de r et le nombre de vérifications à accomplir ensuite avec les a déterminés s'effectuent en un temps polynomial en $\log n$. L'algorithme se déroule alors ainsi :

- Si $n = a^b$ avec $b > 1$ alors n n'est pas premier.
- Construire le plus petit entier r tel que l'ordre de n modulo r soit supérieur à $4 \log^2 n$.
- Si $a \wedge n > 1$ pour $a \leq r$ alors n n'est pas premier.
- Si $n \leq r$ alors n est premier.
- Pour $a = 1$ à $\lfloor 2\sqrt{\varphi(r)} \log(n) \rfloor$, si

$$(X + a)^n \not\equiv X^n + a \pmod{(X^r - 1)\mathbb{Z}/n\mathbb{Z}[X]}$$

alors n n'est pas premier.

- Sinon n est premier.

Notons tout d'abord que si n est premier, l'algorithme vous le confirme. Il reste donc à vérifier que l'algorithme annoncera bien la non primalité d'un n composé.

Lemme II.2.12. — Il existe $r \leq \lceil 16 \log^5(n) \rceil$ tel que l'ordre $\omega_r(n)$ de n modulo r est $> 4 \log^2(n)$.

Démonstration. — Notons que pour tout $r > n^{4 \log^2(n)}$, on a $\omega_r(n) > 4 \log^2(n)$ de sorte que l'ensemble $\{r_1 < r_2 < \dots < r_t\}$ des r tels que $\omega_r(n) \leq 4 \log^2(n)$ est fini. Chacun de ces r_i divise le produit

$$\Delta = \prod_{i=1}^{\lfloor 4 \log^2(n) \rfloor} (n^i - 1) < n^{1+2+\dots+\lfloor 4 \log^2(n) \rfloor} < n^{\lfloor 4 \log^2(n) \rfloor^2} < n^{\lfloor 16 \log^4(n) \rfloor}.$$

En écrivant $n = 2^{\log_2(n)}$, on a $\Delta < 2^{\lfloor 16 \log^5(n) \rfloor}$. D'après l'exercice ??, le ppcm des $\lfloor 16 \log^5(n) \rfloor$ premiers entiers est au moins $2^{\lfloor 16 \log^4(n) \rfloor}$. Si tous les nombres $r \leq \lceil 16 \log^5(n) \rceil$ vérifiaient $\omega_r(n) \leq 4 \log^2(n)$ alors ils diviseraient tous Δ et donc leur ppcm serait plus petit que Δ ce qui n'est pas d'après ce que l'on vient de dire, d'où le résultat. \square

Définition II.2.13. — Soient $P \in \mathbb{F}_p[X]$ et $r \geq 1$ un entier. On dit que n est introspectif pour P si $P(X)^n \equiv P(X^n) \pmod{(X^r - 1)\mathbb{F}_p[X]}$.

Remarque : l'ensemble des nombres introspectif pour P est clairement un monoïde multiplicatif :

$$P(X)^{nn'} \equiv P(X^n)^{n'} \pmod{(X^r - 1)\mathbb{F}_p[X]},$$

car n est introspectif. Comme n' est introspectif, on a aussi

$$P(Y)^{n'} \equiv P(Y^{n'}) \pmod{(Y^r - 1)\mathbb{F}_p[X]}.$$

En prenant $Y = X^n$, et en notant que $X^r - 1 \mid X^{nr} - 1$, on obtient alors

$$P(X)^{nn'} \equiv P(X^{nn'}) \pmod{(X^r - 1)\mathbb{F}_p[X]}.$$

Notons aussi que si n est introspectif pour P et Q alors il l'est pour PQ .

Soit alors p un diviseur premier de n que, d'après la troisième étape de l'algorithme, on suppose $> r$. On pose $l := \lfloor 2\sqrt{\varphi(r)} \log(n) \rfloor$ et on suppose donc que pour tout $1 \leq a \leq l$

$$(X + a)^n \equiv X^n + a \pmod{(X^r - 1)\mathbb{Z}/n\mathbb{Z}[X]}$$

soit, comme $p|n$, l'entier n est introspectif pour $X + a$ dans $\mathbb{F}_p[X]$, pour tout $1 \leq a \leq l$. D'après le petit théorème de Fermat, il en est de même pour p . Ainsi d'après la remarque précédente, tout nombre de $\mathcal{I} := \{n^i p^j : i, j \geq 0\}$ est introspectif pour tout polynôme de $\mathcal{A} = \{\prod_{i=1}^l (X + a)^{\lambda_i} : \lambda_i \geq 0\}$.

Notation II.2.14. — Notons G le sous-groupe de $(\mathbb{Z}/r\mathbb{Z})^\times$ engendré par p et n , et soit t son cardinal.

Remarque : par construction de r , on a $t > 4 \log^2(n)$.

Notons ensuite Q un facteur irréductible de du polynôme cyclotomique Φ_r , dans $\mathbb{F}_p[X]$. Rappelons que $\deg Q = \omega_r(p)$ et que $\mathbb{F}_p[X]/(Q)$ s'identifie avec le corps $\mathbb{F}_{p^{\omega_r(p)}}$.

Notation II.2.15. — On note H le sous-groupe de $\mathbb{F}_p[X]/(Q)$ engendré par les images non nulles des $(X + a)$ avec $1 \leq a \leq l$.

Lemme II.2.16. — Le cardinal $\sharp H$ de H est minoré par $\binom{t-1}{t+l-2}$ et si n n'est pas une puissance de p alors il est majoré par $\frac{1}{2}n^{2\sqrt{t}}$.

Démonstration. — Commençons par la minoration. Pour ce faire montrons tout d'abord que si $A \neq B$ sont deux polynômes de \mathcal{A} de degré $< t$ alors les images de A et B dans $\mathbb{F}[X]/(Q)$ sont distinctes. Supposons donc $A \equiv B \pmod{Q}$ ce qui s'exprime en disant que pour ξ une racine de Q alors ξ est aussi racine de $A - B$. Comme tout $m \in \mathcal{I}$ est introspectif pour A et B et que Q divise $X^r - 1$, on en déduit que $A^m \equiv B^m \pmod{Q}$ et donc que ξ^m est aussi racine de $A - B$. Notons que ξ est une racine primitive r -ième de l'unité de sorte que $\{\xi^m : m \in \mathcal{I}\}$ est de cardinal $t = \sharp G$. Or comme A et B sont supposés de degré $< t$, il en est de même pour $A - B$; ainsi $A - B$ possédant t racines distinctes il est nul dans $\mathbb{F}_p[X]$, i.e. $A = B$.

Or notons que comme $l < 2\sqrt{r} \log(n)$ avec $4 \log^2(n) \leq \omega_r(n) < r$, on a bien $l < r < p$ de sorte que, dans $\mathbb{F}_p[X]/(Q)$, les $X + a$, pour $1 \leq a \leq l$, sont tous distincts de sorte qu'il y en a au moins $l - 1$ d'image non nulle. À partir de ces $l - 1$ polynômes de degré 1, on peut en construire $\binom{t-1}{t+l-2}$ de degré $< t$ d'image non nulle dans $\mathbb{F}_p[X]/(Q)$, d'où le résultat.

Passons désormais à la majoration dans le cas où n n'est pas une puissance de p . Considérons pour cela le sous-ensemble de \mathcal{I} défini par $\mathcal{J} = \{n^i p^j : 0 \leq i, j \leq \sqrt{t}\}$. Si n n'est pas une puissance de p alors $\sharp \mathcal{J} = (\lfloor \sqrt{t} \rfloor + 1)^2 > t$ nombres distincts de sorte qu'en vertu du principe des tiroirs, au moins deux éléments $m_1 > m_2$ de \mathcal{J} sont égaux modulo r :

$$X^{m_1} \equiv X^{m_2} \pmod{(X^r - 1)\mathbb{F}_p[X]}.$$

Ainsi pour $P \in \mathcal{A}$, on a

$$P(X)^{m_1} \equiv P(X^{m_1}) \equiv P(X^{m_2}) \equiv P(X)^{m_2} \pmod{(X^r - 1)\mathbb{F}_p[X]}$$

et donc $P(X)^{m_1} = P(X)^{m_2}$ dans $\mathbb{F}_p[X]/(Q)$ et donc $P(X) \in H$ est une racine de $R(Y) = Y^{m_1} - Y^{m_2}$ dans $\mathbb{F}_p[X]/(Q)$. Comme $P(X)$ est un élément arbitraire de H , le polynôme $R(Y)$ possède au moins $\sharp H$ racines distinctes dans $\mathbb{F}_p[X]/(Q)$. Or comme p divise strictement n et donc $p < n/2$, on a

$$\deg R = m_1 \leq \max(\mathcal{J}) = (np)^{\lfloor \sqrt{t} \rfloor} < \frac{1}{2}n^{2\sqrt{t}},$$

et donc $\#H < \frac{1}{2}n^{2\sqrt{t}}$.

□

Supposons à présent que l'algorithme retourne « premier ». D'après le lemme précédent, on a $\#H \geq \binom{t-1}{t+l-2}$ et en utilisant que

$$t > 2\sqrt{t}\log(n) \text{ car } t > 4\log^2(n), \quad l = \lfloor 2\sqrt{\varphi(r)}\log(n) \rfloor \geq \lfloor 2\sqrt{t}\log(n) \rfloor$$

on obtient $\#H \geq \binom{\lfloor 2\sqrt{t}\log(n) \rfloor}{\lfloor 2\sqrt{t}\log(n) \rfloor - 1}$ qui est lui même $\geq 2^{\lfloor 2\sqrt{t}\log(n) \rfloor}$ car $2\sqrt{t}\log(n) \geq 3$ et donc $\#H \geq 2^{\log(n^{2\sqrt{t}})} \geq n^{2\sqrt{t}}$ et donc $\#H \geq \frac{1}{2}n^{2\sqrt{t}}$. D'après le lemme précédent cette inégalité impose que n est de la forme p^k . Mais si $k > 1$, l'algorithme aurait retourné « non premier » à la première étape et donc finalement $n = p$ est premier.

Analyse de la complexité : utilisons la notation $\Omega(\log^k(n)) = O(\log^k(n)) \cdot P(\log(\log(n))) = O(\log^{k+\epsilon}(n))$ pour tout $\epsilon > 0$.

- La première étape de l'algorithme requiert un temps asymptotique en $\Omega(\log^3(n))$.
- Durant la deuxième étape, on cherche r tel que $\omega_r(n) > 4\log^2(n)$. On peut y parvenir en essayant successivement les valeurs de r et en regardant si $n^k \not\equiv 1 \pmod r$ pour tout $k \leq 4\log^2(n)$: au final le temps est de l'ordre $\Omega(\log^2(n)\log(r))$. Or on a vu qu'il suffit de tester $O(\log^5(n))$ différents r , ce qui donne $\Omega(\log^7(n))$.
- La troisième étape consiste en le calcul du pgcd de r nombres. Chacun de ces calculs requiert un temps en $O(\log(n))$ ce qui donne $O(r\log(n)) = O(\log^6(n))$.
- La quatrième étape s'exécute en seulement $O(\log(n))$.
- Lors de la cinquième étape, $\lfloor 2\sqrt{\varphi(r)}\log(n) \rfloor$ congruences sont testées. Chacune requiert $O(\log(n))$ multiplications de polynômes de degré r dont les coefficients sont de taille $O(\log(n))$, donc peut être vérifiée en $\Omega(r\log^2(n))$. Aussi la complexité de cette étape est

$$\Omega(r\sqrt{\varphi(r)}\log^3(n)) = \Omega(r^{3/2}\log^3(n)) = \Omega(\log^{10,5}(n)).$$

Ce terme domine les autres, c'est donc la complexité de l'algorithme.

Remarque : rappelons la conjecture d'Artin.

Conjecture II.2.17. — (**Artin**) Soient $m, n \in \mathbb{N}$ avec n non carré parfait. Alors le nombre de nombres premiers $q \leq m$ pour lesquels $\omega_q(n) = q - 1$ est asymptotiquement $\frac{Am}{\ln(m)}$ où A désigne la constante d'Artin

$$A = \prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p^2 - p}\right) \simeq 0.37.$$

Si la conjecture d'Artin est vraie pour m de l'ordre $O(\log^2(n))$, on a immédiatement l'existence de r de l'ordre de $O(\log^2(n))$ répondant aux propriétés recherchées. Avec un tel r , l'algorithme a une complexité en $O(\log^6(n))$. Notons que Hooley a, en 1967, prouvé cette conjecture à l'aide de l'hypothèse de Riemann généralisée.

Conjecture II.2.18. — Soient $m, n \geq 2$. Le nombre de nombres premiers $m \leq n$ tels que $2m + 1$ soit aussi premier est asymptotiquement

$$\frac{2C_2n}{\ln^2 n} \text{ où } C_2 = \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \simeq 0.66,$$

est la constante des nombres premiers jumeaux.

De tels nombres n sont dits de Sophie Germain. Si cette conjecture est vraie alors r est de l'ordre de $\Omega(\log^2(n))$ et l'algorithme a une complexité en $\Omega(\log^6(n))$.

Remarque : une étude empirique permet de trouver que l'algorithme possède une complexité de l'ordre de $1000 \log^6(n)$ ce qui est en accord avec les deux conjectures précédentes. En outre on notera que la constante est relativement grande, ce qui pour des n pas trop grands est gênant. En revanche si la conjecture suivante est vérifiée alors la complexité serait $\Omega(\log^3(n))$.

Conjecture II.2.19. — Soient $n, r \in \mathbb{N}$ avec r premier ne divisant pas n et

$$(X - 1)^n \equiv X^n - 1 \pmod{(X^r - 1)\mathbb{Z}/n\mathbb{Z}[X]}.$$

Alors n est premier ou $n \equiv 1 \pmod{r}$.

Remarque : cette conjecture a été vérifiée pour $r \leq 100$ et $n \leq 10^{10}$ par Kayal et Sawena. En revanche, de l'observation empirique, la constante du O serait très grande.

II.2.5. Conjectures d'actualité sur les nombres premiers. — Dans ce paragraphe, nous allons mentionner quelques unes des conjectures célèbres sur les nombres premiers qui ont récemment connues des avancées spectaculaires ces dernières années.

Conjecture II.2.20. — (*des nombres premiers jumeaux*) Il existe une infinité de couples $(p, p + 2)$ de nombres premiers.

Remarque : en 1919, Brun a montré que la somme des inverses des nombres premiers jumeaux était convergente ce qui bien entendu ne va pas dans la bonne direction. La question était un peu abandonnée jusqu'au 13 mai 2013 quand Y. Zhang a montré qu'il existait une infinité de paires de nombres premiers dont la différence était inférieure à 70000000. Un projet collaboratif dirigé par T. Tao a rapidement permis de ramener l'écart à 4 680. Ensuite J. Maynard a publié un article permettant de ramener la borne à 600. Depuis les recherches s'activent pour abaisser encore la borne, toutefois il semble que les techniques développées par Zhang ne puissent dépasser 12.

Conjecture II.2.21. — (*Hardy et Littlewood*) Notons $\pi_2(x)$ le nombre de premiers $p \leq x$ tels que $p + 2 \in \mathcal{P}$, alors

$$\pi_2(x) \sim 2C_2 \int_2^x \frac{dt}{(\ln t)^2}, \quad C_2 = \prod_{p \geq 3} \frac{p(p-2)}{(p-1)^2} \simeq 0,66.$$

On dispose de plusieurs généralisations possibles de la conjecture des nombres premiers jumeaux. La plus ancienne date de 1849.

Conjecture II.2.22. — (*de Polignac*) Tout entier naturel pair peut s'écrire comme différence de deux nombres premiers consécutifs et cela d'une infinité de manières.

Plus récemment, soient f_1, \dots, f_k des polynômes de degré 1, irréductibles et vérifiant la propriété que pour tout nombre premier p il y ait au moins un entier n parmi $0, \dots, p - 1$ tel que p ne divise pas le produit des $f_i(n)$. On note $\omega(p)$ le complémentaire à p du nombre de tels entiers. Un tel ensemble de polynômes est dit admissible; on cherche à connaître la proportion d'entiers en lesquels les polynômes prennent simultanément des valeurs premières.

Remarque : se limiter à des ensembles de polynômes admissibles permet d'éviter des cas triviaux comme $f_1(t) = t$, et $f_2(t) = t + 1$.

Conjecture II.2.23. — Le nombre d'entiers $n \leq x$ tels que les valeurs $f_1(n), \dots, f_k(n)$ sont simultanément premières, est pour x assez grand, de l'ordre de :

$$\left(\prod_{p \in \mathcal{P}} \frac{1 - \frac{\omega(p)}{p}}{(1 - \frac{1}{p})^k} \right) \frac{x}{\ln |f_1(x)| \cdots \ln |f_k(x)|}.$$

Remarque : le théorème des nombres premiers correspond au cas $k = 1$ et $f_1 = t$, le théorème de Dirichlet à $k = 1$ et $f_1 = at + b$. Pour $k = 2$, $f_1(t) = t$ et $f_2(t) = t + 2$, on obtient une version quantitative de la conjecture des nombres premiers jumeaux.

Conjecture II.2.24. — (**Conjecture abc**) Pour tout $\epsilon > 0$ il existe une constante K_ϵ telle que pour tous a, b, c entiers relatifs premiers entre eux vérifiant $a + b = c$, on ait

$$\max\{|a|, |b|, |c|\} \leq K_\epsilon N_0(abc)^{1+\epsilon}$$

où $N_0(n)$ est le produit des nombres premiers divisant n .

Remarque : la conjecture abc est une version corps des nombres du théorème de Mason, cf. le §??, pour les corps de fonctions proposée par Oesterlé et Masser en 1985.

Théorème II.2.25. — (sous la conjecture abc) Il existe N qui dépend explicitement de K_ϵ tels que pour tout $n \geq N$, l'équation $x^n + y^n = z^n$ n'a pas de solutions entières.

Démonstration. — Soient x, y, z premiers entre eux solutions de l'équation de Fermat pour n ; sous la conjecture abc, on a

$$|x|^n \leq \max\{|x|^n, |y|^n, |z|^n\} \leq K_\epsilon N_0((xyz)^n)^{1+\epsilon}.$$

Or comme $N_0((xyz)^n) = N_0(xyz)$, en écrivant la relation précédente pour $|y|^n$ et $|z|^n$ et en les multipliant toutes les trois on obtient

$$|xyz|^n \leq K_\epsilon^3 N_0(xyz)^{3(1+\epsilon)}$$

ce qui en utilisant que $N_0(xyz) \leq |xyz|$ implique $|xyz|^{n-3(1+\epsilon)} \leq K_\epsilon^3$. De la minoration $|xyz| \geq 2$, on en déduit $2^{n-3(1+\epsilon)} \leq K_\epsilon^3$ et donc le résultat. \square

Remarque : la conjecture abc implique plusieurs résultats très importants comme la conjecture de Spiro, le théorème de Faltings, l'existence pour $a \geq 2$ fixé, d'une infinité de premiers p tel $a^{p-1} \not\equiv 1 \pmod{p^2}$, la conjecture d'Erdoes-Woods (i.e. il existe une constante $k > 0$ telle que pour tous x, y positifs si $N_0(x+i) = N_0(y+i)$ pour tout $i = 1, 2, \dots, k$ alors $x = y$), et bien d'autres encore. En août 2012, un mathématicien renommé a annoncé avoir démontré cette conjecture dans une série de 4 longs papiers. À cet instant il est difficile de savoir si la preuve est correcte, disons que le sentiment général est plutôt négatif ce qui justifie mon choix de ne pas mentionner le nom de l'auteur.

Conjecture II.2.26. — (**de Goldbach**) Tout entier $n > 2$ est la somme de deux nombres premiers.

Schnizel a montré que la conjecture de Goldbach était équivalente au fait que tout entier $n > 17$ était la somme de trois premiers distincts. Ramaré a montré que tout entier n est la somme d'au plus 6 nombres premiers et en 1966 Chen a montré que tout entier suffisamment grand est la somme d'un nombre premier et d'un entier possédant au plus deux facteurs premiers. En 2012 T. Tao a montré tout entier impair est somme d'au plus 5 nombres premiers et en 2013 H. Helfgott a montré que tout $n > 5$ impair était somme de 3 nombre premiers.

CHAPITRE III

THÉORIE DES NOMBRES

III.1. Théorie des corps

Rappelons qu'un corps est un triplet $(K, +, \times)$ tel que $(K, +)$ est un groupe commutatif d'élément neutre 0_K et où $(K - \{0_K\}, \times)$ est un groupe d'élément neutre 1_K , tel que \times est distributif par rapport à $+$, i.e.

$$\forall(a, b, c) \in K^3 : a \times (b + c) = a \times b + a \times c \text{ et } (b + c) \times a = b \times a + c \times a.$$

Remarque : habituellement le mot corps est réservé à la situation où \times est commutative ; dans le cas contraire on parle d'algèbre à division. C'est en 1843 que W.R. Hamilton, à partir de l'interprétation des nombres complexes comme couple de nombres réels, s'est rendu compte qu'il était impossible de munir \mathbb{R}^3 d'une structure de corps et qu'en dimension 4, on devait autoriser la non commutativité dans la multiplication : il a alors obtenu l'algèbre à division des quaternions \mathbb{H} , i.e. les nombres de la forme $a + bi + cj + dk$ avec $a, b, c, d \in \mathbb{R}$ et

$$i^2 = j^2 = k^2 = ijk = -1.$$

III.1.1. Généralités sur les extensions. — Puisque le seul idéal non nul d'un corps est le corps lui-même, alors un morphisme de corps, $\sigma : k \rightarrow K$ est nécessairement injectif ce qui permet d'identifier k à son image $\sigma(k)$ et donc de le considérer comme un sous-corps de K . Dans cette situation on dit que K est *une extension* du corps k et on note K/k .

Remarque : on dit aussi que K est un sur-corps de k ou que k est un sous-corps de K .

Définition III.1.1. — Soit $k \subset K$ une extension de corps ; la dimension de K en tant que k -espace vectoriel se note $[K : k]$ et s'appelle *le degré* de l'extension K/k . Une extension intermédiaire L de K/k est un corps tel que $k \subset L \subset K$; on dit aussi que L/k est *une sous-extension* de K/k ou un sous-corps de K contenant k .

Remarque : le degré $[K : k]$ peut éventuellement être infini, par exemple $\mathbb{Q} \subset \mathbb{R}$.

Lemme III.1.2. — Soit k un corps et A une k -algèbre de dimension finie sur k ; alors A est un corps.

Démonstration. — Soit $a \in A$ non nul ; la multiplication par a définit une application ϕ_a qui est k -linéaire et injective puisque A est intègre. Comme A est un k -espace vectoriel de dimension finie alors ϕ_a est bijective de sorte qu'il existe b tel que $ab = 1$ et donc a est inversible. \square

Proposition III.1.3. — (théorème de la base télescopique)

Soit $k \subset K \subset L$ des extensions de corps alors

$$[L : k] = [L : K].[K : k].$$

Démonstration. — Soit $(e_i)_{1 \leq i \leq n}$ (resp. $(f_j)_{1 \leq j \leq m}$) une base de K (resp. de L) en tant que k -espace vectoriel (resp. K -espace vectoriel) avec $n = [K : k]$ (resp. $m = [L : K]$). Montrons alors que $(e_i f_j)_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$ est une base de L en tant que k -espace vectoriel. En ce qui concerne la liberté, soit

$$0 = \sum_{i,j} \lambda_{i,j} e_i f_j = \sum_{i=1}^n \left(\sum_{j=1}^m \lambda_{i,j} f_j \right) e_i;$$

la famille $(e_i)_{1 \leq i \leq n}$ étant libre, on en déduit que pour tout $i = 1, \dots, n$, $\sum_{j=1}^m \lambda_{i,j} f_j = 0$. La famille des $(f_j)_{1 \leq j \leq m}$ étant libre, on conclut alors que tous les $\lambda_{i,j}$ sont nuls et donc que la famille $(e_i f_j)_{i,j}$ est libre.

Soit ensuite $l \in L$ que l'on écrit sous la forme $\sum_{j=1}^m a_j f_j$ avec $a_j \in K$; on écrit alors $a_j = \sum_{i=1}^n \lambda_{i,j} e_i$ de sorte que $l = \sum_{i,j} \lambda_{i,j} e_i f_j$ et la famille est génératrice. \square

Définitions III.1.4. — — Soit $S \subset K$ une partie quelconque d'un corps K . L'ensemble des sous-corps de K contenant S étant non vide, l'intersection de tous ces sous-corps est un sous-corps de K , c'est le plus petit sous-corps contenant S appelé le sous-corps engendré par S .

- Si K est une extension de k , la sous-extension $k(S)$ engendrée par S sur k est le sous-corps de K engendré par $S \cup k$. Si $S = \{x_1, \dots, x_n\}$ est fini, on le note aussi $k(x_1, \dots, x_n)$.
- Une extension K/k est dite de type fini si K est engendré comme surcorps de k par un nombre fini d'éléments, i.e. s'il est de la forme $k(x_1, \dots, x_n)$.
- On dit que l'extension K/k est une extension monogène si K est engendré sur k par un élément, i.e. s'il existe $x \in K$ tel que $K = k(x)$.

Remarque : pour I, J deux parties de K , on a $k(I \cup J) = k(I)(J)$; en particulier toute extension de type finie $k \subset k(x_1, \dots, x_n)$ est obtenue comme composée d'extensions monogènes

$$k(x_1, \dots, x_n) = k(x_1)(x_2, \dots, x_n) = k(x_1)(x_2) \cdots (x_n).$$

Définition III.1.5. — Le noyau du morphisme $\mathbb{Z} \rightarrow K$ défini par

$$n \mapsto \overbrace{1_K + \cdots + 1_K}^n$$

est, en tant qu'idéal de l'anneau principal \mathbb{Z} , de la forme $p\mathbb{Z}$ pour $p \geq 0$ appelé la caractéristique de K . On appelle *sous-corps premier* de K , le sous-corps de K engendré par l'image de ce morphisme.

Lemme III.1.6. — La caractéristique p d'un corps est soit nulle soit un nombre premier.

Démonstration. — Écrivons $p = nm$, il s'agit alors de prouver que $p = n$ ou bien $p = m$ ce qui revient à montrer que p divise n ou bien p divise m . On a donc $(n1_K) \times (m1_K) = 0_K$ de sorte que, K étant intègre, $n1_K = 0_K$ ou bien $m1_K = 0_K$. Autrement dit, on a $p|n$ ou bien $p|m$, i.e. $p = n$ ou bien $p = m$. \square

Remarque : si la caractéristique de K est nulle (resp. non nulle) alors son sous-corps premier est \mathbb{Q} (resp. $\mathbb{Z}/p\mathbb{Z}$); il est contenu dans tout sous-corps de K .

III.1.2. Extensions algébriques et transcendentes. —

Définition III.1.7. — Soit $k \subset K$ une extension de corps. Un élément $x \in K$ est dit *algébrique sur k* s'il existe un polynôme $P \in k[X]$ non nul tel que $P(x) = 0$. Dans le cas contraire on dit que x est *transcendant sur k* . L'extension K/k est dit algébrique si tous les éléments de K sont algébriques sur k .

Proposition III.1.8. — *Les points suivants sont équivalents :*

- (i) $x \in K$ est algébrique sur k ;
- (ii) la sous-algèbre $k[x] \subset K$ engendrée par x et k , est de dimension finie sur k ;
- (iii) la sous-algèbre $k[x] \subset K$ est un corps.

Démonstration. — Si x est algébrique sur k , il est annulé par un polynôme de degré $d > 0$ et donc $1, x, \dots, x^{d-1}$ engendrent $k[x]$, prouvant (i) \Rightarrow (ii). L'implication (ii) \Rightarrow (iii) est générale : la multiplication par $z \in k[x]$ non nul, est un endomorphisme du k -espace vectoriel $k[x]$ qui est injective puisque $k[x] \subset K$ est intègre et donc surjective, puisque $k[x]$ est de dimension finie, i.e. 1 est atteint et donc z est inversible.

Enfin pour l'implication (iii) \Rightarrow (i), on écrit x^{-1} sous la forme $P(x)$ pour P un polynôme de $k[X]$ de sorte que l'équation

$$xP(x) - 1 = 0$$

est une relation de liaison entre les x^i pour $i \leq \deg(P) + 1$ et donc $k[x]$ est de dimension finie sur k . \square

Corollaire III.1.9. — *Le sous-ensemble A des éléments algébriques de K sur k est un sous-corps de K .*

Démonstration. — Notons que A contient 0 et 1. Soient alors $x, y \in A$ de sorte que $\{1, x^1, x^2, \dots, x^{n-1}\}$ (resp. $\{1, y, \dots, y^{m-1}\}$) engendrent $k[x]$ (resp. $k[y]$) où $n = [k[x] : k]$ (resp. $m = [k[y] : k]$). On en déduit alors que les $x^i y^j$ pour $1 \leq i \leq n$ et $1 \leq j \leq m$ engendrent $k[x, y]$ qui est donc de dimension finie sur k . Mais comme $k[x - y]$ et $k[xy]$ sont contenus dans $k[x, y]$, ils sont aussi de dimension finie et donc $x - y$ et xy sont aussi dans A . On conclut en notant que si x est annulé par P alors $1/x$ est annulé par le polynôme $X^{\deg(P)} P(1/X)$. \square

Remarque : en particulier si x_1, \dots, x_r sont des éléments algébriques de K/k alors $k[x_1, \dots, x_r] \subset K$ est un corps de dimension $\leq \prod_{i=1}^r [k[x_i] : k]$. Réciproquement le théorème des zéros de Hilbert affirme que $k[x_1, \dots, x_n]$ est un corps si et seulement si il est de dimension finie sur k .

Définition III.1.10. — On appelle *polynôme minimal* d'un élément algébrique x de K/k , le générateur *unitaire* de l'idéal des polynômes de $k[X]$ annihilant x .

Remarque : soient α, β deux nombres algébriques de polynômes minimaux respectifs $\mu_{\alpha, k}$ et $\mu_{\beta, k}$ alors le polynôme minimal de $\alpha + \beta$ est un facteur irréductible du résultant, relativement à la variable Y :

$$R_Y\left(\mu_{\alpha, k}(X - Y), \mu_{\beta, k}(Y)\right) = \prod_{\beta_i} \mu_{\alpha, k}(X - \beta_i) \in k[X]$$

où les β_i sont les racines de $\mu_{\beta,k}$. Par exemple pour $\alpha = \sqrt{2} + \sqrt{3}$ et $\beta = \sqrt{5} + \sqrt{6}$ avec $\mu_{\alpha,\mathbb{Q}}(X) = X^4 - 10X^2 + 1$ et $\mu_{\beta,\mathbb{Q}}(X) = X^4 - 22X^2 + 1$. On calcule alors le résultant ce qui nous donne

$$\begin{aligned} R_Y(\mu_{\alpha,\mathbb{Q}}(X-Y), \mu_{\beta,\mathbb{Q}}(Y)) &= X^{16} - 128X^{14} + 5712X^{12} - 117248X^{10} + 1169248X^8 \\ &\quad - 5289984X^6 + 8195328X^4 - 1990656X^2 + 20736 \\ &= (X^8 - 64X^6 + 96X^5 + 808X^4 - 1152X^3 - 2304X^2 + 1152X + 144) \\ &\quad (X^8 - 64X^6 - 96X^5 + 808X^4 + 1152X^3 - 2304X^2 - 1152X + 144) \end{aligned}$$

et par des calculs approximatifs des racines, on vérifie que le facteur cherché est $X^8 - 64X^6 - 96X^5 + 808X^4 + 1152X^3 - 2304X^2 - 1152X + 144$.

Selon le même principe les résultants $R_Y(\mu_{\alpha,k}(X/Y), \mu_{\beta,k}(Y))$ et $R_Y(\mu_{\alpha,k}(XY), \mu_{\beta,k}(Y))$ fournissent des polynômes annulant respectivement $\alpha\beta$ et α/β .

Proposition III.1.11. — Soit P le polynôme minimal de $x \in K$ algébrique sur k . Alors P est irréductible et $k[x]$ est canoniquement k -isomorphe à $k[X]/(P)$. En particulier $\deg(P) = [k[x] : k]$.

Démonstration. — Par définition le morphisme d'algèbre $k[X] \rightarrow K$ qui envoie X sur x a pour image $k[x]$ et pour noyau l'idéal (P) ce qui fournit, par factorisation, l'isomorphisme $k[X]/(P) \simeq k[x]$. Comme $k[x]$ est un corps, on en déduit que (P) est maximal i.e. P est irréductible. \square

Exemple : soit $K = \mathbb{Q}[\zeta_n]$ où ζ_n est une racine primitive de l'unité dans \mathbb{C} . Alors le n -ième polynôme cyclotomique Φ_n appartient à $\mathbb{Z}[X]$ et donc à $\mathbb{Q}[X]$, est irréductible et annule ζ_n , c'est donc son polynôme minimal sur \mathbb{Q} et

$$[\mathbb{Q}[\zeta_n] : \mathbb{Q}] = \phi(n).$$

L'extension $\mathbb{Q}[\zeta_n]/\mathbb{Q}$ est dite *cyclotomique*.

Proposition III.1.12. — Soit $K = k(x_1, \dots, x_n)$ une extension telle que chaque x_i est algébrique de degré d_i sur k alors $K = k[x_1, \dots, x_n]$ et K/k est algébrique de degré fini $\leq d_1 \cdots d_n$.

Démonstration. — Soit $\phi : k[X_1, \dots, X_n] \rightarrow K$ le morphisme de k -algèbres défini par $\phi(X_i) = x_i$; l'image de ϕ est $A := k[x_1, \dots, x_n]$. Comme chaque monôme x_i^n est combinaison k -linéaire des monômes x_i^r avec $0 \leq r < d_i$, on en déduit que A est engendrée sur k par les monômes $x_1^{r_1} \cdots x_n^{r_n}$ avec $r_i < d_i$ et donc A est une k -algèbre de dimension finie $\leq d_1 \cdots d_n$. De plus A est intègre car contenue dans K . D'après le lemme III.1.2 A est un corps contenant x_1, \dots, x_n et donc K . \square

Remarque : ainsi une extension K/k est de degré fini si et seulement si elle est algébrique et de type fini.

En ce qui concerne les extensions K/k de type fini arbitraires et donc pas nécessairement algébriques, nous allons introduire et étudier la notion de base et degré de transcendance.

Définition III.1.13. — On dit que x_1, \dots, x_n sont *algébriquement indépendants* sur k si le morphisme

$$\phi : k[X_1, \dots, X_n] \rightarrow K, \quad P \mapsto P(x_1, \dots, x_n)$$

est injectif.

Remarque : dans ce cas le morphisme ϕ se prolonge en un isomorphisme de $k(X_1, \dots, X_2)$ sur le sous-corps de K engendré par les x_i . En particulier chacun des x_i est transcendant sur k .

Définition III.1.14. — On dit qu'une partie B de K est une *base de transcendance sur k* si elle vérifie les deux conditions suivantes :

- les éléments de B sont algébriquement indépendants sur k ;
- le corps K est une extension algébrique du sous-corps $k(B)$.

Remarque : cela revient à dire que B est une partie algébriquement indépendante *maximal*.

Lemme III.1.15. — Soit K/k une extension et soit S une partie finie de K telle que K soit algébrique sur $k(S)$. Alors S contient une base de transcendance B de K sur k . De plus le degré $[k(S) : k(B)]$ est fini.

Remarque : en particulier si $K = k(S)$ alors K est de degré fini sur $k(B)$.

Démonstration. — Posons $S = \{x_1, \dots, x_n\}$ avec x_1, \dots, x_r algébriquement indépendants sur k et pour $i > r$, x_i algébrique sur $k(B)$ pour $B = \{x_1, \dots, x_r\}$. Par transitivité des extensions algébriques, K est algébrique sur $k(B)$ et B est bien une base de transcendance de K sur k . \square

Proposition III.1.16. — Soit K/k une extension de corps admettant une base de transcendance sur k qui est finie. Alors toutes les bases de transcendance de K sur k ont le même cardinal.

Démonstration. — Soit B une base de transcendance de cardinal minimal n . Il suffit alors de montrer que si une partie B' est algébriquement indépendante sur k , alors elle est de cardinal $\leq n$. Pour ce faire nous allons raisonner par récurrence sur $s(B, B') := \#B - \#(B \cap B')$ que B' est de Si $s = 0$ alors $B \subset B'$ et donc $B' = B$ par maximalité de B . Supposons alors le résultat acquis jusqu'au rang $s - 1$ avec $s \geq 1$. On écrit $B = \{b_1, \dots, b_n\}$ avec $B \cap B' = \{b_{s+1}, \dots, b_n\}$. Si $B' \subset B$ il n'y a rien à montrer, supposons donc qu'il existe $b' \in B'$ et $b' \notin B$. Alors par maximalité de B , $B \cup \{b'\}$ n'est pas algébriquement indépendante et il existe $P \in k[X_1, \dots, X_n, X_{n+1}]$ non nul tel que $P(b_1, \dots, b_n, b') = 0$ avec en outre $P \notin k[X_{s+1}, \dots, X_{n+1}]$ puisque les éléments de B' sont algébriquement indépendants. Quitte à renuméroter on se ramène au cas où P contient la variable X_1 .

Posons alors $B_1 = \{b_2, \dots, b_n, b'\}$: b_1 est algébrique sur $k(B_1)$ et comme K est algébrique sur $k(B_1)[b_1]$, il est aussi algébrique sur $k(B_1)$. Comme $\#B_1 = n$, la minimalité de n jointe au lemme précédent, implique que B_1 est une base de transcendance de K sur k . De plus on a

$$\#B_1 - \#(B_1 \cap B') = s - 1 \text{ car } B_1 \cap B' = \{b_{s+1}, \dots, b_n, b'\}.$$

Ainsi l'hypothèse de récurrence appliquée à B_1 et B' , nous donne $\#B' \leq \#B_1 = n$. \square

Théorème III.1.17. — Soit $k \subset K$ une extension de corps de type fini.

- Toutes les bases de transcendance de K sur k ont le même cardinal appelé degré de transcendance de K sur k et noté $\text{degr}_k K$. De plus tout ensemble d'éléments algébriquement indépendants est contenu dans une base de transcendance.
- Soit L/k une sous-extension de K/k ; alors L/k est de type fini et son degré de transcendance est inférieur ou égal à celui de K/k .

Démonstration. — On a déjà vu l'existence des bases de transcendance et l'unicité de leur cardinal; on peut ainsi en complétant un ensemble algébriquement indépendants aboutir à une base de transcendance.

En ce qui concerne le deuxième point, comme toute partie de L algébriquement indépendante sur k est aussi une partie de K algébriquement indépendante sur k , on obtient que L possède une base de transcendance fini $B = \{b_1, \dots, b_t\}$ que l'on peut compléter en une bas de transcendance

$$\tilde{B} = B \amalg C = \{b_1, \dots, b_t\} \amalg \{c_1, \dots, c_s\}$$

de K sur k . Il reste alors à vérifier que L/k est de type fini.

Lemme III.1.18. — *L'ensemble C est algébriquement indépendant sur L .*

Démonstration. — Sinon il existerait $P \in L[X_1, \dots, X_s]$ non nul tel que $P(c_1, \dots, c_s) = 0$. Quitte à renuméroter supposons que X_s apparaisse dans P et donc que c_s est algébrique sur $L(c_1, \dots, c_{s-1})$. Comme $L/k(B)$ est algébrique on en déduit que $L(c_1, \dots, c_{s-1})$ est algébrique sur $k(B)(c_1, \dots, c_{s-1})$ et donc c_s est algébrique sur $k(B)(c_1, \dots, c_{s-1})$ ce qui n'est pas. \square

Soient alors l_1, \dots, l_n des éléments de L linéairement indépendants sur $k(B)$ et montrons qu'ils le sont encore sur $k(\tilde{B})$. Soit

$$0 = F_1 l_1 + \dots + F_n l_n$$

une relation linéaire avec $F_i \in k(\tilde{B})$; en chassant les dénominateurs on se ramène à $F_i \in k[\tilde{B}]$ avec

$$F_i = \sum_{\nu \in \mathbb{N}^s} P_{i,\nu}(b_1, \dots, b_t) c_1^{\nu_1} \dots c_s^{\nu_s}.$$

On obtient alors

$$0 = \sum_{\nu \in \mathbb{N}^s} \left(\sum_{i=1}^n P_{i,\nu}(b) l_i \right) c^\nu$$

soit d'après le lemme précédent, $\sum_{i=1}^n P_{i,\nu}(b) l_i = 0$ pour tout $\nu \in \mathbb{N}^s$ et comme les l_i sont linéairement indépendants sur $k(B)$, il vient $P_{i,\nu} = 0$ pour tout i, ν et donc $F_i = 0$ pour $i = 1, \dots, n$. Ainsi l_1, \dots, l_n sont linéairement indépendants sur $k(\tilde{B})$ et donc

$$[L : k(B)] \leq [K : k(\tilde{B})] < \infty$$

et donc L est une extension de degré fini de $k(B)$ et L/k est de type fini. \square

III.1.3. Nombres algébriques de degré d . — L'énoncé suivant justifie l'affirmation selon laquelle les nombres algébriques ne se laissent pas facilement approchés par des rationnels, observation qui a permis à Liouville de construire des nombres transcendants.

Proposition III.1.19. — *Soit α un nombre réel algébrique de degré $d \geq 2$ sur \mathbb{Q} de polynôme minimal $\mu_\alpha \in \mathbb{Z}[X]$ de contenu 1. On pose $c = |P'(\alpha)|$. Pour tout $\epsilon > 0$, il existe un entier q_0 tel que pour tout $p/q \in \mathbb{Q}$ avec $q \geq q_0$, on ait*

$$\left| \alpha - \frac{p}{q} \right| \geq \frac{1}{(c + \epsilon)q^d}.$$

Démonstration. — On écrit $P(X) = a_0 \prod_{i=1}^d (X - \alpha_i)$ avec $a_0 > 0$ et $\alpha = \alpha_1$ de sorte que $P'(\alpha) = a_0 \prod_{i=2}^d (\alpha - \alpha_i)$. Comme P est irréductible de degré ≥ 2 , l'entier $q^d P(p/q) = a_0 q^d \prod_{i=1}^d (p/q - \alpha_i)$ est non nul. Pour tout q , on considère $p = [q\alpha]$ de sorte que $|q\alpha - p| \leq 1/2$ et donc

$$\left| \alpha_i - \frac{p}{q} \right| \leq |\alpha_i - \alpha| + \frac{1}{2q}$$

et donc

$$1 \leq q^d |P(p/q)| \leq q^d a_0 \left| \alpha - \frac{p}{q} \right| \prod_{i=2}^d \left(|\alpha_i - \alpha| + \frac{1}{2q} \right).$$

Pour q suffisamment grand le membre de droite est majoré par $q^d |\alpha - \frac{p}{q}| (|P'(\alpha)| + \epsilon)$, ce qui donne le résultat. \square

Remarque : pour $\epsilon = 1$ et $K = \max\{c + 1, \max_{1 \leq q \leq q_0} \frac{1}{q^{d-1}|q\alpha-p|}\}$, on en déduit que pour tout $p/q \in \mathbb{Q}$ distinct de α , on a

$$\left| \alpha - \frac{p}{q} \right| \geq \frac{1}{Kq^d}.$$

Définition III.1.20. — Un nombre réel α est dit de Liouville si pour tout $k > 0$, il existe $p/q \in \mathbb{Q}$ avec $q \geq 2$ tel que

$$0 < \left| \alpha - \frac{p}{q} \right| \leq \frac{1}{q^k}.$$

D'après la proposition précédente, tout nombre de Liouville est transcendant. Par exemple que pour $g \geq 2$ un entier rationnel et pour $(a_n)_{n \geq 0}$ une suite bornée d'entiers rationnels dont une infinité d'entre eux est non nul, le réel

$$x = \sum_{n \geq 0} a_n g^{-n!}$$

est de Liouville. En effet notons $A = \max_{n \geq 0} |a_n|$ et soit $k > 0$ un nombre réel ; soit alors N un entier suffisamment grand tel que $a_{N+1} \neq 0$ et posons

$$q = g^{N!}, \quad p = \sum_{n=0}^N a_n g^{N!-n!},$$

de sorte que $x - \frac{p}{q} = \frac{a_{N+1}}{g^{(N+1)!}} + \sum_{i \geq 2} \frac{a_{N+i}}{g^{(N+i)!}}$. Pour $i \geq 2$, on a $(N+i)! - (N+1)! \geq N+i$ et donc

$$\sum_{i \geq 2} \frac{a_{N+i}}{g^{(N+i)!}} \leq \frac{A}{g^{(N+1)!}} \sum_{i \geq 2} \frac{1}{g^{N+i}} < \frac{1}{g^{(N+1)!}} \leq \frac{|a_{N+1}|}{g^{(N+1)!}}.$$

On utilise enfin $|a_{N+1}| \leq A$ et $g^{(N+1)!} = q^{N+1}$ d'où

$$0 < \left| x - \frac{p}{q} \right| \leq \frac{2A}{q^{N+1}}.$$

Remarque : Citons le théorème de Thue-Siegel-Dyson-Roth : soit x algébrique de degré d , alors pour tout $\epsilon > 0$, il existe $K(x, \epsilon)$ tel que pour tout p/q on ait

$$\left| x - \frac{p}{q} \right| > \frac{K(x, \epsilon)}{q^{f(d)+\epsilon}}$$

où :

- $f(d) = d/2 + 1$ (Thue) ;
- $f(d) = 2\sqrt{d}$ (Siegel) ;
- $f(d) = \sqrt{2d}$ (Dyson et Gelfond) ;
- $f(d) = 2$ (Roth)

A titre de réflexion, vous pouvez réfléchir à l'argumentaire suivant : soit f une fonction sur \mathbb{N} telle que $f(q) \rightarrow +\infty$ quand $q \rightarrow +\infty$. On note X_f l'ensemble des réels x de $[0, 1]$ admettant une suite d'approximations p_n/q_n avec $|x - p_n/q_n| \leq 1/f(q_n)$, alors

$$X_f = \bigcap_{q_0}^{\infty} \bigcup_{q \geq q_0} \bigcup_{0 \leq p \leq q} \left[\frac{p}{q} - \frac{1}{f(q)}, \frac{p}{q} + \frac{1}{f(q)} \right]$$

L'intersection étant décroissante et les ensembles de mesure finie, il vient

$$\mu(X_f) = \lim_{q_0 \rightarrow \infty} \mu \left(\bigcup_{q \geq q_0} \bigcup_{0 \leq p \leq q} \left[\frac{p}{q} - \frac{1}{f(q)}, \frac{p}{q} + \frac{1}{f(q)} \right] \right) \leq \lim_{q_0 \rightarrow \infty} \sum_{q \geq q_0} \frac{2(q+1)}{f(q)}$$

En particulier si la série $\sum_{q \geq 1} q/f(q)$ converge alors $\mu(X_f) = 0$ ce qui est le cas pour $f(q) = q^\alpha$ avec $\alpha > 2$.

Remarque : en ce qui concerne les résultats d'approximation simultanée des nombres algébrique, on renvoie le lecteur intéressé à [?] chapitre VI.

III.1.4. Corps de rupture et corps de décomposition. — Pour P un polynôme irréductible de $k[X]$, l'idéal (P) est maximal et donc $K := k[X]/(P)$ est un corps contenant k que l'on identifie aux polynômes constants. Notons que dans ce corps la classe x de X vérifie $P(x) = 0$, autrement dit P admet une racine dans K ; en outre on a $K = k[x]$.

Définition III.1.21. — Le corps $L = k[X]/(P)$ est le corps de rupture de P sur k .

Définition III.1.22. — Deux extensions K et K' de k sont dites k -isomorphes s'il existe un isomorphisme $\phi : K \xrightarrow{\sim} K'$ de corps tel que $\phi(\lambda) = \lambda$ pour tout $\lambda \in k$.

Remarque : autrement dit K et K' sont k -isomorphes s'ils le sont en tant que k -algèbres.

Proposition III.1.23. — Soit L/k une extension dans laquelle P admet une racine α ; il existe alors un unique k -morphisme $\psi : K \rightarrow L$ tel que $\psi(x) = \alpha$ d'image le sous-corps $k[\alpha]$ de L .

Démonstration. — Le polynôme minimal $\mu_{k,\alpha}$ de α sur k divise P et donc, P étant irréductible, est de la forme λP pour $\lambda \in k^\times$. Le morphisme de k -algèbres $\phi : k[X] \rightarrow L$ défini par $\phi(X) = \alpha$ induit alors un morphisme $\psi : K := k[X]/(P) \rightarrow L$ tel que $\psi(x) = \alpha$. En outre ce morphisme est unique puisque $K = k[x]$. \square

Remarque : en ce qui concerne l'unicité, il est parfois utile de disposer de la version plus souple suivante. Pour $\tau : k \simeq k'$ un isomorphisme de corps, on note $\phi_\tau : k[X] \simeq k'[X]$ l'isomorphisme d'anneaux qu'il induit :

$$\sum_i a_i X^i \mapsto \sum_i \tau(a_i) X^i.$$

Alors pour tout $P \in k[X]$, ϕ_τ induit un isomorphisme d'anneaux

$$k[X]/(P) \simeq k'[X]/(\tau(P)).$$

Remarque : le corps \mathbb{C} des nombres complexes est le corps de rupture de X^2+1 ou de n'importe quel polynôme irréductible de $\mathbb{R}[X]$. En particulier on notera que des polynômes irréductibles distincts peuvent avoir les mêmes corps de rupture.

Remarque : si $K = k(\alpha)$ est une extension algébrique monogène alors K est un corps de rupture sur k du polynôme minimal de α sur k .

Pour qu'un polynôme de degré supérieur ou égal à 2 soit irréductible sur un corps k , il faut évidemment qu'il n'ait pas de racines dans k . Cette condition nécessaire est aussi suffisante si le polynôme est de degré 2 ou 3. La proposition suivante généralise ce fait aux degrés plus grands :

Proposition III.1.24. — *Soit P un polynôme de $k[X]$ de degré α . Alors P est irréductible si et seulement s'il n'admet de racine dans aucune extension K de k telle que $[K : k] \leq \alpha/2$.*

Démonstration. — Pour P est irréductible, une extension K/k possédant une racine α de P contient nécessairement $k[\alpha]$ qui est un corps de rupture de P sur k et donc $\deg P = [k[\alpha] : k] \leq [K : k]$.

Réciproquement soit Q un facteur irréductible de P : si P n'est pas irréductible on peut choisir Q de degré $\leq \frac{\deg P}{2}$ et P admet une racine dans un corps de rupture de Q lequel est donc de degré $\leq \frac{\deg P}{2}$ d'où le résultat. \square

Remarque : en caractéristique nulle, ce critère est purement théorique puisqu'il y a pour k donné, une infinité d'extension de degré k . En revanche pour les corps finis, la situation est tout autre puisqu'à isomorphisme près, une telle extension est unique.

Corollaire III.1.25. — *Soit $P(X) \in K[X]$ un polynôme irréductible sur K de degré n ; si L est une extension de K de degré m avec $n \wedge m = 1$, alors P est encore irréductible sur L .*

Proposition III.1.26. — *Soit $K = k[\alpha]$ une extension algébrique monogène ; notons $\mu_{\alpha,k}$ le polynôme minimal de α sur k . Pour toute extension L/k , le nombre de k -morphisms $K \rightarrow L$ est égal au nombre de racines de $\mu_{\alpha,k}$ dans L . Par conséquent on a*

$$\# \text{hom}_{k\text{-alg}}(K, L) \leq \deg \mu_{\alpha,k} = [K : k]$$

avec égalité si et seulement si $\mu_{\alpha,k}$ est totalement décomposé dans L .

Remarque : rappelons qu'un polynôme irréductible P de $k[X]$ a des racines simples dans toute extension L/k : en effet sinon le pgcd $P \wedge P' \in K[X]$ ne serait pas égal à 1 puisqu'il aurait une racine dans L , on obtiendrait alors un diviseur non trivial de P ce qui ne se peut pas puisque P est irréductible.

Démonstration. — Pour tout k -morphisme $\phi : K \rightarrow L$, $\phi(\alpha)$ est une racine de $\mu_{\alpha,k}$ dans L . Réciproquement comme $K \simeq k[x]/(\mu_{\alpha,k})$ alors toute racine β de $\mu_{\alpha,k}$ dans L définit un morphisme de k -algèbres $\phi_\beta : K \rightarrow L$ tel que $\phi_\beta(\alpha) = \beta$ et évidemment ces morphismes sont deux à deux distincts. \square

Exemple : pour $k = \mathbb{Q}$ et $P(X) = X^3 - 2$, chacun des sous-corps suivants de \mathbb{C} :

$$\mathbb{Q}[\sqrt[3]{2}], \quad \mathbb{Q}[j\sqrt[3]{2}], \quad \mathbb{Q}[j^2\sqrt[3]{2}]$$

pour $j = e^{2i\pi/3}$, est un corps de rupture de P qui sont \mathbb{Q} -isomorphes et deux à deux distincts. En effet si on avait par exemple, $\mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q}[j\sqrt[3]{2}]$ alors on aurait $j \in \mathbb{Q}[\sqrt[3]{2}]$ ce qui ne se peut pas car $\mathbb{Q}[j]$ est une extension de degré 2 de \mathbb{Q} et que 2 ne divise pas $3 = [\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}]$.

Définition III.1.27. — Soit $P \in k[X]$ un polynôme non constant. On dit qu'une extension K/k est un corps de décomposition de P sur k si elle vérifie les deux conditions suivantes :

- P est scindé dans $K[X]$;
- K est engendré sur k par les racines de P .

Remarque : en particulier un corps de décomposition est une extension de degré fini sur k et donc algébrique.

Proposition III.1.28. — *Tout $P \in k[X]$ non constant admet un corps de décomposition.*

Démonstration. — On raisonne par récurrence sur le degré n de P . Si $n = 1$ alors $P = aX + b$ et donc k est un corps de décomposition de P . Supposons alors le résultat acquis jusqu'au degré $n - 1$ et traitons le cas $\deg P = n$. Soit alors S un facteur irréductible de P et k_1/k un corps de rupture de S sur k . Dans $k_1[X]$, on a $P(X) = (X - \alpha)Q(X)$ avec $Q \in k_1[X]$ de degré $n - 1$. Par hypothèse de récurrence, il existe une extension K/k_1 dans laquelle Q a des racines $\alpha_2, \dots, \alpha_n$ et telle que $K = k_1(\alpha_2, \dots, \alpha_n)$ de sorte que P est scindé sur K avec pour racines $\alpha_1 := \alpha, \alpha_2, \dots, \alpha_n$ et $K = k(\alpha_1, \dots, \alpha_n)$. \square

En ce qui concerne l'unicité, il est plus souple de l'énoncer comme suit.

Théorème III.1.29. — *Soient $\tau : k \simeq k'$ un isomorphisme de corps, $P \in k[X]$ non constant et K (resp. K') un corps de décomposition de P (resp. de $\tau(P)$) sur k (resp. sur k'). Alors τ se prolonge en un isomorphisme $\sigma : K \simeq K'$.*

Démonstration. — On raisonne par récurrence sur le nombre m de racines de P qui sont dans K mais pas dans k ; on se ramène aussi au cas où P est unitaire. Pour $m = 0$ on a clairement $K = k$ et $K' = k'$ et on peut prendre $\sigma = \tau$.

Supposons alors le résultat établi pour tout $m' < m$ et soit $P \in k[X]$ ayant exactement m racines dans $K - k$. On factorise $P = P_1 \cdots P_r$ en facteurs irréductibles dans $k[X]$: comme $m > 0$ l'un au moins de ces facteurs, disons P_1 , est de degré ≥ 2 . Comme P se scinde dans $K[X]$ en facteurs irréductibles de degré 1, P_1 a aussi toutes ses racines dans K ; notons α l'une d'elles et soit

$$\psi : K[X]/(P_1) \simeq k[\alpha] =: k_1.$$

Par application de τ , $\tau(P_1)$ est aussi un diviseur irréductible de $\tau(P)$ scindé dans K' dont on note β une racine :

$$\psi' : k'[X]/(\tau(P_1)) \simeq k'[\beta] =: k'_1.$$

Comme remarqué ci-avant, τ induit un isomorphisme

$$\phi_\tau : k[X]/(P_1) \simeq k'[X]/(\tau(P_1))$$

qui prolonge $\tau : k \simeq k'$ et $\tau_1 := \psi' \circ \phi_\tau \circ \psi^{-1}$ est alors un isomorphisme $k_1 \simeq k'_1$ qui prolonge τ . Désormais K (resp. K') est un corps de décomposition sur k_1 (resp. sur k'_1) de P (resp. $\tau_1(P)$) où le nombre de racines de P dans $K - k_1$ est $< m$. D'après l'hypothèse de récurrence, il existe alors un isomorphisme $\sigma : K \simeq K'$ dont la restriction à k_1 est τ_1 et donc, dont la restriction à k est τ . \square

Définition III.1.30. — On dit que K est une clôture algébrique de k si K/k est une extension algébrique et que K est algébriquement clos, i.e. que les seuls polynômes irréductibles de $K[X]$ sont ceux de degré 1.

Remarque : un corps est algébriquement clos si et seulement si tout polynôme de $K[X]$ est totalement décomposé dans K ou s'il ne possède pas d'autre corps de rupture que lui-même.

Remarque : \mathbb{C} est algébriquement clos mais n'est pas une extension algébrique de \mathbb{Q} : ce n'est donc pas une clôture algébrique de \mathbb{Q} .

Définition III.1.31. — Soit K/k une extension de corps ; nous avons vu que le sous-ensemble $K_{alg/k}$ de ses éléments algébriques est un corps ; on l'appellera *la fermeture algébrique de k dans K* .

Remarque : si x est algébrique sur $K_{alg/k}$ alors, d'après le théorème de la base télescopique, il est algébrique sur k et donc appartient à $K_{alg/k}$: autrement dit $K_{alg/k}$ est égal à sa propre fermeture algébrique. En particulier si K est algébriquement clos alors $K_{alg/k}$ est une clôture algébrique de k : en effet si $P \in K_{alg/k}[X]$ est non constant, une de ses racines quelconques dans K est algébrique sur K' et donc appartient à K' .

Notation III.1.32. — On notera $\overline{\mathbb{Q}}$ l'ensemble des nombres complexes qui sont algébriques sur \mathbb{Q} . D'après ce qui précède c'est une clôture algébrique de \mathbb{Q} .

Théorème III.1.33. — (*Steinitz*)

Tout corps k admet un clôture algébrique unique à k -isomorphisme (non unique) près.

Démonstration. — Désignons par $\{P_\lambda : \lambda \in \Lambda\}$ l'ensemble des polynômes irréductibles unitaires de $k[X]$ et soit A la k -algèbre de polynômes en une infinité de variables X_λ pour $\lambda \in \Lambda$. Pour tout $\lambda \in \Lambda$ soit $P_\lambda(X_\lambda)$ l'image de P_λ dans A par le morphisme $k[X] \rightarrow A$ qui envoie X sur X_λ .

Lemme III.1.34. — L'idéal I de A engendré par les éléments $P_\lambda(X_\lambda)$ pour $\lambda \in \Lambda$ est un idéal propre de A .

Démonstration. — Raisonnons par l'absurde : il existerait alors un sous-ensemble fini $\Lambda_0 = \{\lambda_1, \dots, \lambda_n\}$ de Λ tel que

$$(1) \quad 1 = \sum_{i=1}^n Q_i P_{\lambda_i}(X_{\lambda_i}),$$

avec $Q_i \in A$. Cette égalité a en fait lieu dans un anneau de polynômes $B := k[X_{\lambda_j} : j = 1, \dots, n]$ en un nombre fini de variables : il suffit en effet de rajouter à Λ_0 les X_λ qui apparaissent dans les Q_i .

Considérons alors k_1 un corps de rupture de P_{λ_1} sur k et soit α_1 une de ses racines dans k_1 . De même en considérant un facteur irréductible de P_2 dans $k_1[X]$, on construit une extension k_2/k_1 tel que P_2 ait une racine dans k_2 et ainsi de suite jusqu'à $K = k_n$. Soit alors le morphisme

$$\phi : K[X_{\lambda_j} : j = 1, \dots, n] \longrightarrow K$$

défini par $\phi(X_{\lambda_i}) = \alpha_i$ pour $\lambda_i \in \Lambda_0$ et $\phi(X_j) = 0$ pour les autres. On applique alors ϕ à l'égalité (1) ce qui fournit $1 = 0$ d'où la contradiction. \square

Ainsi puisque I est un idéal propre de A , considérons \mathcal{M} un idéal maximal de A contenant I et posons $K_1 = A/\mathcal{M}$ et $K_0 = k$. Pour tout $\lambda \in \Lambda$, notons x_λ l'image de X_λ dans K_1 : c'est une racine de P_λ . Ainsi tout polynôme irréductible de $k[X]$ admet une racine dans K_1 .

Lemme III.1.35. — L'extension K_1/K_0 est algébrique.

Démonstration. — Soit $y \in K_1$ qui est donc l'image d'un polynôme $Q \in A$ lequel ne fait intervenir qu'un nombre fini de variables X_λ . Ainsi y appartient à la sous-algèbre $C := k[x_{\lambda_1}, \dots, x_{\lambda_s}]$ de K_1 et comme chaque x_{λ_i} est algébrique sur k , puisque racine de P_{λ_i} , y est algébrique sur k . \square

Si K_1 n'est pas algébriquement clos, on peut appliquer à K_1 le même processus : on obtient ainsi une extension algébrique $K_1 \subset K_2$ dans laquelle tout polynôme irréductible de $K_1[X]$ a au moins une racine et telle que K_2/K_0 est algébrique. On construit ainsi une suite croissante d'extensions algébriques

$$k = K_0 \subset K_1 \subset K_2 \subset \dots$$

telle que tout polynôme irréductible $P \in K_i[X]$ a une racine dans K_{i+1} . Posons alors $K = \bigcup_{i \geq 0} K_i$ qui est donc algébrique sur k et algébriquement clos. En effet tout polynôme irréductible $P \in K[X]$ a tous ses coefficients dans un certain K_i et donc une racine dans K_{i+1} et donc K .

Il nous reste à montrer l'unicité à isomorphisme près. Commençons par le lemme suivant.

Lemme III.1.36. — *Soient K/k une extension algébrique, Ω un corps algébriquement clos et $\tau : k \hookrightarrow \Omega$ un morphisme de corps. Alors τ se prolonge à K (de façon non unique en général).*

Démonstration. — Soit \mathcal{E} l'ensemble des couples (k', τ') où k'/k est une sous-extension de K/k et $\tau' : k' \hookrightarrow \Omega$ est un morphisme prolongeant τ . Alors \mathcal{E} est non vide puisqu'il contient (k, τ) , et lorsqu'on le munit de la relation d'ordre

$$(k', \tau') \leq (k'', \tau'') \Leftrightarrow k' \subset k'' \text{ et } \tau'' \text{ prolonge } \tau',$$

\mathcal{E} est un ensemble ordonné inductif. En effet si (k_i, τ_i) est une chaîne totalement ordonnée alors $k' = \bigcup_i k_i$ est un sous-corps de K et on définit τ' par $\tau'(x) = \tau_i(x)$ où i est un indice quelconque tel que $x \in k_i$. Le couple (k', τ') ainsi défini appartient bien à \mathcal{E} et est un majorant de la chaîne considérée. Ainsi d'après le théorème de Zorn, \mathcal{E} possède un élément maximal (k_0, τ_0) .

Montrons que $k_0 = K$; un élément $x \in K$ est algébrique sur k et donc sur k_0 . On note $P \in k_0[X]$ son polynôme minimal sur k_0 . Le polynôme $\tau_0(P)$ admet une racine dans Ω puisque Ω est algébriquement clos. Identifiant k_0 à son image dans Ω via τ_0 , on obtient des isomorphismes

$$k_0[\alpha] \simeq k_0[X]/(P) \simeq k_0[x]$$

et τ_0 se prolonge en un morphisme $k_0[x] \simeq k_0[\alpha] \hookrightarrow \Omega$. Par maximalité de (k_0, τ_0) on en déduit que $k_0 = k_0[x]$ et donc $x \in k_0$. \square

Soient alors Ω et Ω' deux clôtures algébriques de k . D'après le lemme précédent l'injection $\tau : k \hookrightarrow \Omega$ se prolonge en une injection $\tau' : \Omega' \hookrightarrow \Omega$. Soit alors $x \in \Omega$ qui est, par hypothèse, algébrique sur k et donc sur Ω' . Comme Ω' est algébriquement clos, le polynôme minimal de x sur Ω' est de degré 1, i.e. $x \in \Omega'$. Ainsi τ' est un isomorphisme. \square

III.2. Corps finis

Rappelons qu'une algèbre à division est un anneau $(D, +, \times)$ unitaire intègre dont tous les éléments non nuls admettent un inverse à gauche et à droite : en revanche la loi \times n'est pas nécessairement commutative. Avant d'appliquer les propriétés générales de la théorie des

corps, nous allons montrer le fameux théorème de Wedderburn qui affirme que pour une telle algèbre à division D qui est finie alors \times est commutative, autrement dit D est un corps.

III.2.1. Théorème de Wedderburn. —

Théorème III.2.1. — Toute algèbre à division finie est un corps.

Remarque : la question de savoir s'il existait des algèbres à division finie non commutative date du début du vingtième siècle. H.S.M Wedderburn annonça son théorème en 1905 devant ses collègues de l'université de Chicago ; L.E. Dickson qui doutait de la véracité du résultat, en lui cherchant un contre exemple, trouva une preuve qu'il publia en attribuant la paternité du résultat à Wedderburn qui s'inspirant de celle-ci, fournit deux nouvelles preuves. Or il s'avéra par la suite qu'il y avait une faille dans la preuve originale de Wedderburn de sorte que c'est en fait Dickson qui a trouvé la première preuve correcte du théorème.

Nous allons présenter la preuve donnée par Witt en 1930 car elle est considérée comme la plus élégante et c'est celle qui est devenue la preuve classique du théorème de Witt.

Démonstration. — Soit K une algèbre à division finie, pour tout $x \in K$, on note $C_x := \{y \in K : xy = yx\}$ le centralisateur de x dans K qui est clairement une sous-algèbre à division de K . En notant $C = \bigcap_{x \in K} C_x = \{y \in K : \forall x \in K, xy = yx\}$ le centre de K , on obtient un corps commutatif fini et on considère K et C_x comme des C -espaces vectoriels de dimension finie respectives n et n_x ; si q désigne le cardinal de C alors K et C_x sont de cardinal q^n et q^{n_x} . Comme par ailleurs K est un C_x -espace vectoriel de dimension d_x , on a, d'après le théorème de la base télescopique $n = d_x n_x$.

Remarque : pour montrer que $n_x | n$, on peut aussi utiliser que C_x^* est un sous-groupe de cardinal $q^{n_x} - 1$ de K^* lequel est de cardinal $q^n - 1$. D'après le théorème de Lagrange, on a $q^{n_x} - 1 | q^n - 1$ et en notant $n = d_x n_x + r_x$ la division euclidienne de n par n_x , la congruence

$$q^n - 1 \equiv (q^{n_x})^{d_x} q^{r_x} - 1 \equiv q^{r_x} - 1 \pmod{q^{d_x} - 1}$$

et donc $r_x = 0$.

En considérant l'action de $G = K^*$ sur lui-même par conjugaison, l'équation aux classes s'écrit

$$q^n - 1 = q - 1 + \sum_{x \in \mathcal{O}} \frac{q^n - 1}{q^{n_x} - 1}$$

où \mathcal{O} désigne l'ensemble des classes de conjugaisons de cardinal > 1 , et donc n_x est un diviseur strict de n . On va alors montrer que cette équation, ne peut être satisfaite que si $n = 1$ et donc que si K est commutatif.

On rappelle alors que la fonction de Möbius μ est définie par

$$\mu(n) = \begin{cases} (-1)^r & \text{si } n = p_1 \cdots p_r, p_i \neq p_j \forall i \neq j \\ 0 & \text{s'il existe } p^2 | n \end{cases}$$

On a alors $\sum_{d|n} \mu(d) = 0$ pour tout $n > 1$; en effet si n est divisible par r facteurs premiers distincts, alors il y a exactement $\binom{r}{i}$ diviseurs d de n sans facteurs carrés, produit de i facteurs premiers distincts et le résultat découle alors de l'égalité

$$(1 - 1)^r = \sum_{i=0}^r \binom{r}{i} (-1)^i.$$

On considère alors la fraction rationnelle

$$P_n(T) = \prod_{d|n} (T^d - 1)^{\mu(n/d)}$$

de sorte que

$$\prod_{d|n} P_d(T) = \prod_{d|n} \prod_{e|d} (T^e - 1)^{\mu(d/e)} = \prod_{e|n} (T^e - 1)^{\sum_{d|n, e|d} \mu(d/e)} = T^n - 1.$$

Ainsi par récurrence, on obtient que $P_n(T)$ est un polynôme unitaire de $\mathbb{Z}[T]$ vérifiant les propriétés suivantes :

1. $P_n(T) = \frac{T^n - 1}{\prod_{d|n, d \neq n} P_d(T)}$ et donc si d est un diviseur strict de n alors $P_n(T)$ divise $\frac{T^n - 1}{T^d - 1}$;
2. P_n est symétrique, i.e. $P(T) = T^{\deg P} P(T^{-1})$ car $T^n - 1$ l'est, ainsi que $\prod_{d|n, d \neq n} P_d(T)$ par récurrence ;
3. pour $m \wedge p = 1$, on a $P_{p^k m}(T) = P_{p^k m}(T^{p^{k-1}})$ avec $P_{p^k m}(T) = \frac{P_m(T^p)}{P_m(T)}$ et donc $\deg P_n(T) = \phi(n) = \prod_p p^{\alpha_p - 1} (p - 1)$, où $n = \prod_p p^{\alpha_p}$.

Lemme III.2.2. — Pour tout $n \geq 2$, $P_n(q) > q - 1$.

Démonstration. — Posons $P_{\pm} = \left| \prod_{d|n, \mu(\frac{n}{d}) = \pm 1} (q^{-d} - 1) \right|$ de sorte que $|P_n(q^{-1})| = \frac{P_+}{P_-} \geq P_+ \geq \prod_{i=1}^n (1 - q^{-i})$. D'après la formule de binôme,

$$(1 + b^{-1})^b \leq 1 + 1 + 1/2! + \dots + 1/b! \leq 1 + 1 + 1/2 + \dots + 1/2^{b-1} \leq 1 + 2(1 - 2^{-b}) \leq 3.$$

Ainsi $(1 + b^{-1})^{b+1} \leq 6$ et pour $b = q^i - 1$, on obtient $(1 - q^{-i})^{q^i} \geq 1/6$ et donc

$$\prod_{i=1}^n (1 - q^{-i})^{q^n} \geq 6^{-\sum_{i=1}^n q^{n-i}} \geq 6^{-q^n}.$$

De l'égalité $P_n(q) = q^{\phi(n)} P_n(q^{-1})$, on obtient alors $P_n(q) \geq q^{\phi(n)}/6$. On utilise alors que $q^{\phi(n)}/6 \geq q$ sauf pour $n = 1$ ou 2 ou si $(q, \phi(n)) \in \{(2, 2), (2, 3), (3, 2), (5, 2)\}$, i.e. $q = 2, 3, 5$ et $n = 3, 4, 6$. Dans les cas $n \geq 2$, on vérifie alors que $P_n(q) > q - 1$. \square

Ainsi comme $P_n(q)$ divise $q - 1 = q^n - 1 - \sum_{x \in \mathcal{O}} \frac{q^n - 1}{q^{nx} - 1}$, on doit nécessairement avoir $n = 1$. \square

Remarque : les polynômes $P_n(T)$ sont les polynômes cyclotomiques que l'on peut définir plus naturellement en utilisant le corps des nombres complexes. La majoration $|P_n(q)| > q - 1$ est alors élémentaire via la norme euclidienne de \mathbb{R}^2 , cependant le détour suivi dans la preuve précédente est conceptuellement plus élégante car elle n'utilise pas les nombres complexes ou réels et reste donc complètement algébrique.

En 1949, B. L. van der Waerden a proposé une preuve groupiste qui repose sur les deux lemmes suivant dont une preuve du premier sera donnée dans l'exercice ??.

Lemme III.2.3. — Tous les sous-corps maximaux de K sont conjugués, i.e. si F et F' sont deux sous-corps maximaux de K alors il existe un élément $x \in K^*$ tel que $F' = xFx^{-1}$.

Lemme III.2.4. — Soit G un groupe fini et H un sous-groupe propre de G alors $\bigcup_{g \in G} gHg^{-1}$ est strictement contenu dans G .

Démonstration. — Notons tout d'abord que si $g' = gh$ alors $gHg^{-1} = g'H(g')^{-1}$ de sorte qu'il y a au plus $|G/H| = |G|/|H|$ conjugués distincts. Ainsi le cas d'égalité ne peut se produire que si tous les gHg^{-1} sont égaux ou disjoints ce qui n'est pas car l'élément neutre de G est dans tous les gHg^{-1} . \square

Pour tout $x \in K$, $C[x] \subset K$ est un sous-corps commutatif; on choisit alors F_x un sous-corps commutatif maximal de K contenant x ainsi qu'un sous-corps maximal F de K . On a $K = \bigcup_{x \in K} F_x$ et puisque chaque F_x est conjugué à F d'après le premier lemme, on obtient que K^* s'écrit comme la réunion des conjugués de F^* ce qui d'après le lemme précédent implique que $F^* = k^*$ et donc $K = F$ est commutatif.

III.2.2. Propriétés générales. — Rappelons quelques propriétés qui se déduisent de la théorie élémentaire des corps :

- la caractéristique d'un corps fini K est non nulle et donc égale à un nombre premier p ;
- la dimension de K en tant qu'espace vectoriel sur son corps premier \mathbb{F}_p est finie. En particulier le cardinal de K est de la forme p^n où $n = [K : \mathbb{F}_p]$;
- K^\times est un groupe cyclique de cardinal $\#K - 1 = p^n - 1$; si α désigne un générateur alors

$$K = \{0, 1, \alpha, \dots, \alpha^{p^n-2}\}.$$

On en déduit en particulier que tous les éléments de K vérifient l'équation

$$X^{p^n} - X = 0.$$

En utilisant qu'un polynôme de degré k a au plus k -racines sur un corps commutatif, on en déduit que K est l'ensemble des racines de $X^{p^n} - X$, c'est en particulier un corps de décomposition de $X^{p^n} - X$.

- Soit α un générateur du groupe multiplicatif K^\times et soit μ_α le polynôme minimal de α sur \mathbb{F}_p . Comme $K = \mathbb{F}_p[\alpha]$ on en déduit en particulier que K s'obtient comme un corps de rupture $\mathbb{F}_p[X]/(\mu_\alpha)$.
- Si $\mathbb{F}_p \subset k \subset K$ alors $\#K = p^n$ et $\#k = p^d$ pour d un diviseur de n .

Il résulte de l'existence et de l'unicité des corps de décomposition qu'il existe un unique corps de cardinal p^n à isomorphisme près. Rappelons qu'un moyen simple, au moins verbalement, pour faire disparaître l'indétermination « à isomorphisme près », est de fixer une fois pour toute une clôture algébrique $\overline{\mathbb{F}_p}$ et de considérer toutes les extensions comme des sous-corps de $\overline{\mathbb{F}_p}$. Étudions les premiers exemples en caractéristique 2 :

- (i) $\mathbb{F}_2[X]/(X^2 + X + 1)$ est un corps à 4 éléments;
- (ii) $\mathbb{F}_2[X]/(X^3 + X + 1)$ est un corps à 8 éléments;
- (iii) $\mathbb{F}_2[X]/(X^4 + X + 1)$ est un corps à 16 éléments; le sous-corps engendré par $X^2 + X$ est de cardinal 4;
- (iv) $\mathbb{F}_3[X]/(X^2 + X - 1)$ est un corps à 9 éléments.

Démonstration. — (i) On vérifie rapidement que $X^2 + X + 1$ n'a pas de racines dans \mathbb{F}_2 , étant de degré 2 il y est alors irréductible de sorte que $\mathbb{F}_2[X]/(X^2 + X + 1)$ est un corps, une extension de degré 2 de \mathbb{F}_2 et donc isomorphe à \mathbb{F}_4 qui par convention est le corps de cardinal 4 contenu dans une clôture algébrique $\overline{\mathbb{F}_2}$ de \mathbb{F}_2 fixée une fois pour toute. Comme $\mathbb{F}_4^\times \simeq \mathbb{Z}/3\mathbb{Z}$, tout élément autre que 0, 1 est un générateur de \mathbb{F}_4^\times , soit X et $X + 1$.

Remarque : on notera par ailleurs que $X^2 + X + 1$ est le seul polynôme irréductible de degré 2 ce qui permet dès à présent en utilisant la proposition ??, de conclure à l'unicité, à isomorphisme près, d'un corps de cardinal 4.

(ii) De même, on vérifie que $X^3 + X + 1$ n'a pas de racines dans \mathbb{F}_2 ; étant de degré 3 il est alors irréductible sur \mathbb{F}_2 de sorte que $\mathbb{F}_2[X]/(X^3 + X + 1)$ est un corps de cardinal 8 et donc isomorphe à \mathbb{F}_8 . Comme $\mathbb{F}_8^\times \simeq \mathbb{Z}/7\mathbb{Z}$ tout élément autre que 0, 1 est un générateur du groupe des inversibles, par exemple X .

(iii) Encore une fois $X^4 + X + 1$ n'a pas de racines sur \mathbb{F}_2 mais cela ne suffit pas pour conclure à son irréductibilité, en effet il pourrait être le produit de deux polynômes irréductibles de degré 2. Or d'après (i), $X^2 + X + 1$ est l'unique polynôme irréductible de degré 2 sur \mathbb{F}_2 et comme $X^4 + X + 1$ n'a pas de racines multiples, son polynôme dérivée étant égal à 1, il ne peut pas être égal à $(X^2 + X + 1)^2$: évidemment plus simplement on peut calculer $(X^2 + X + 1)^2 = X^4 + X^2 + 1$.

(iv) À nouveau $X^2 + X - 1$ n'a pas de racines dans \mathbb{F}_3 , il y est donc irréductible et $\mathbb{F}_9 \simeq \mathbb{F}_3[X]/(X^2 + X - 1)$. En outre $\mathbb{F}_9^\times \simeq \mathbb{Z}/8\mathbb{Z}$ de sorte qu'il y a $\varphi(8) = 4$ générateurs et donc 4 non-générateurs. On a $X^4 = (X - 1)^2 = X^2 - 2X + 1 = -3X + 2 = -1$ et X est un générateur de \mathbb{F}_9^\times . \square

III.2.3. Existence et unicité des corps finis : preuves constructives. — L'objectif de ce paragraphe est de montrer que pour tout p premier et pour tout $n \geq 1$, il existe un corps de cardinal p^n sans utiliser la théorie générale des corps. Pour ce faire il nous suffit de montrer qu'il existe un polynôme irréductible sur \mathbb{F}_p de degré n .

Lemme III.2.5. — Soit K un corps de caractéristique p et $P(X) \in K[X]$ alors $P(X) \in \mathbb{F}_p[X]$ si et seulement si $P(X^p) = P(X)^p$.

Remarque : on renvoie le lecteur au §?? pour une généralisation de ce résultat via la théorie de Galois.

Démonstration. — Soit $P(X) = \sum_{i=0}^n a_i X^i$ avec $a_i \in K$; si $P(X) \in \mathbb{F}_p[X]$ alors $(\sum_{i=0}^n a_i X^i)^p = \sum_{i=0}^n a_i^p X^{pi} = \sum_{i=0}^n a_i (X^p)^i = P(X^p)$. La réciproque se montre de la même façon en remarquant que l'ensemble des $x \in K$ tels que $X^p = X$ est égal à $\mathbb{F}_p \subset K$: en effet tout élément de \mathbb{F}_p est une racine du polynôme $X^p - X$ lequel a au plus p solutions dans K d'où le résultat. \square

Proposition III.2.6. — Soit P un polynôme irréductible unitaire de $\mathbb{F}_p[X]$ de degré r . Si L est une extension de \mathbb{F}_p possédant une racine α de P alors $P(X) = \prod_{i=0}^{r-1} (X - \alpha^{p^i})$.

Remarque : en général, via la théorie de Galois, le polynôme minimal de α sur k s'explique en fonction de l'action sur α , du groupe de Galois d'une extension K/k contenant α . Dans le cas des corps finis, nous verrons qu'un tel groupe de Galois est connu a priori puisqu'il est engendré par le morphisme de Frobenius; c'est ce fait qui explique la précision et la simplicité de la proposition précédente.

Démonstration. — Notons p^n le cardinal de L ; d'après la proposition ??, on a $\alpha^{p^n} = \alpha$. Par ailleurs l'ensemble des m tels que $\alpha^{q^m} = \alpha$ est un sous-groupe de \mathbb{Z} ; notons s son générateur positif. Comme $P(X) \in \mathbb{F}_p[X]$, d'après le lemme précédent on a $P(X^p) = P(X)^p$ de sorte que les α^{p^i} pour $i = 0, \dots, s-1$ sont des racines de P dans L . Notons

$$Q(X) = \prod_{i=0}^{s-1} (X - \alpha^{p^i})$$

qui est à coefficients dans $\mathbb{F}_p[X]$ car $Q(X^p) = Q(X)^p$ et divise P ; on en déduit donc que $P = Q$ car P est irréductible et donc $s = r$ d'où le résultat. \square

Proposition III.2.7. — Soit p un nombre premier et n un entier ≥ 1 ; on a alors l'égalité

$$X^{p^n} - X = \prod P$$

où P décrit l'ensemble des polynômes irréductibles unitaires de $\mathbb{F}_p[X]$ de degré divisant n .

Démonstration. — Si on suppose que P divise $X^{p^n} - X$ alors $r = \deg P$ divise n ; si réciproquement on suppose que r divise n alors les racines α^{q^i} pour $i = 1, \dots, r$ sont aussi racines de $X^{p^n} - X$ et donc P divise $X^{p^n} - X$. Le résultat découle alors de l'observation évidente que $X^{p^n} - X$ n'a pas de racines multiples puisqu'il est premier avec son polynôme dérivé qui est égal au polynôme constant égal à -1 . \square

Corollaire III.2.8. — Pour tout $n \geq 1$, il existe au moins un polynôme irréductible unitaire de $\mathbb{F}_p[X]$ de degré n .

Démonstration. — Notons $I_n(p)$ le cardinal de l'ensemble des polynômes irréductibles unitaires de degré n sur \mathbb{F}_p ; d'après la proposition précédente on a

$$p^n = \sum_{d|n} I_d(p)d.$$

On va alors montrer par récurrence sur n que $I_n(p) > 0$. Le résultat est clair pour $n = 1$, supposons donc le résultat acquis jusqu'au rang $n - 1$ et traitons le cas de n . On réécrit l'égalité précédente sous la forme

$$p^d = dI_d(p) + \sum_{d'|d, d' < d} I_{d'}(p)d' \quad \forall d < n$$

avec d'après l'hypothèse de récurrence $p^d > dI_d(p)$. Ainsi la formule ci-dessus pour $d = n$ donne les inégalités

$$p^n < nI_n(p) + \sum_{d|n, d \neq n} p^d \leq nI_n(p) + \sum_{k=0}^{n-1} p^k = nI_n(p) + \frac{p^n - 1}{p - 1} < nI_n(p) + p^n$$

et donc $I_n(p) > 0$ d'où le résultat. \square

Corollaire III.2.9. — Pour tout $n \geq 1$ et pour tout nombre premier p , il existe un corps de cardinal p^n .

Démonstration. — Il suffit de considérer $K = \mathbb{F}_p[X]/(P(X))$ pour P un polynôme irréductible sur \mathbb{F}_p et de degré n dont l'existence est assurée par le corollaire précédent. \square

Proposition III.2.10. — Deux corps finis de même cardinal sont isomorphes.

Démonstration. — Soit K un corps fini; son cardinal est de la forme p^n avec p premier. D'après la proposition ?? il existe $\alpha \in K^\times$ d'ordre $p^n - 1$. On considère alors le morphisme $\mathbb{F}_p[X] \rightarrow K$ qui à X associe α ; il est surjectif et son noyau est un idéal de la forme $(P(X))$ pour un polynôme $P(X) \in \mathbb{F}_p[X]$ nécessairement irréductible. Quitte à le diviser par son coefficient dominant, on peut le prendre unitaire de sorte d'après la proposition III.2.7 il divise $X^{p^n} - X = \prod_{a \in K} (X - a)$.

Si L est un corps de cardinal p^n comme tout $a \in L$ vérifie $a^{p^n} = a$, les racines de $X^{p^n} - X$ dans L sont exactement tous ses éléments de sorte que le polynôme $P(X)$ est totalement décomposé dans L . Étant donné une racine a quelconque de P dans L , le morphisme de $\mathbb{F}_p[X] \rightarrow L$ qui à X associe a se factorise pas $\mathbb{F}_p[X]/(P(X))$ et induit un isomorphisme de K sur L . \square

Remarque : pour tout q de la forme p^r , soit $\mathbb{F}_q \ll \text{le} \gg$ corps de cardinal q ; les résultats du paragraphe précédent s'adaptent en remplaçant \mathbb{F}_p par \mathbb{F}_q et donc p par q .

Proposition III.2.11. — *Soit K un corps de cardinal p^n ; si $L \subset K$ est un sous-corps de K son cardinal est alors de la forme p^d pour $d|n$. Réciproquement pour tout diviseur d de n , il existe un sous-corps de K de cardinal p^d .*

Démonstration. — Dans le sens direct, en considérant K comme un L -espace vectoriel on obtient que son cardinal est égal à $p^n = (p^d)^e$ et donc d divise n . Réciproquement si d divise $n = kd$, on a $p^n - 1 = (p^d - 1)N$ avec $N = (p^d)^{k-1} + \dots + 1$ et donc

$$X^{p^n} - X = X(X^{p^{dk}-1} - 1) = X(X^{p^d-1} - 1)(X^{(p^d-1)(N-1)} + \dots + 1)$$

et donc comme K est l'ensemble des racines de $X^{p^n} - X$ dans K , l'ensemble des racines dans K du polynôme $X^{p^d} - X$ forme un corps de cardinal p^d . \square

Construction de $\bar{\mathbb{F}}_p$: considérons par récurrence un corps $\mathbb{F}_{p^{n!}}$ de cardinal $p^{n!}$ comme une extension de degré n de $\mathbb{F}_{p^{(n-1)!}}$ qui existe d'après ce qui précède (unique à isomorphisme près). Notons alors $\bar{\mathbb{F}}_p$ la réunion croissante $\bigcup_{n=1}^{\infty} \mathbb{F}_{p^{n!}}$; c'est un corps. En effet pour $x, y \in k$, il existe n tels que $x, y \in \mathbb{F}_{p^{n!}}$ et $x + y, xy$ sont définis dans $\mathbb{F}_{p^{n!}}$. Il est en outre immédiat que $\bar{\mathbb{F}}_p$ est algébrique sur \mathbb{F}_p car tout $x \in k$ est un élément d'un $\mathbb{F}_{p^{n!}}$ pour n assez grand. Il reste alors à voir que $\bar{\mathbb{F}}_p$ est algébriquement clos; soit donc $P(X) \in k(X)$ irréductible et soit \mathbb{F}_{p^m} une extension contenant les coefficients de P et soit L un corps de rupture de P dans $\bar{\mathbb{F}}_p$ sur \mathbb{F}_{p^m} ; L est alors une extension finie de \mathbb{F}_{p^m} et est donc égale à un certain \mathbb{F}_{p^r} et donc inclus dans $\mathbb{F}_{p^{r!}} \subset k$. Ainsi tout polynôme irréductible sur k est de degré 1 soit k algébriquement clos.

Remarque : étant donné une construction de $\bar{\mathbb{F}}_p$ comme ci-dessus, pour tout $n \geq 1$ on notera \mathbb{F}_{p^n} le corps de cardinal p^n contenu dans $\bar{\mathbb{F}}_p$: il est égal à l'ensemble des racines dans $\bar{\mathbb{F}}_p$ du polynôme $X^{p^n} - X$.

Corollaire III.2.12. — *Les sous-corps de \mathbb{F}_{p^n} sont exactement les \mathbb{F}_{p^r} où r divise n ; en particulier le plus petit sous-corps de $\bar{\mathbb{F}}_p$ contenant \mathbb{F}_{p^n} et \mathbb{F}_{p^m} est $\mathbb{F}_{p^{n \vee m}}$ alors que $\mathbb{F}_{p^n} \cap \mathbb{F}_{p^m} = \mathbb{F}_{p^{n \wedge m}}$.*

Démonstration. — Le premier point découle directement de la proposition III.2.11. En particulier si \mathbb{F}_{p^r} contient \mathbb{F}_{p^n} et \mathbb{F}_{p^m} alors $n|r$ et $m|r$ de sorte que $n \vee m|r$ et $\mathbb{F}_{p^{n \vee m}} \subset \mathbb{F}_{p^r}$; on conclut alors en remarquant que $\mathbb{F}_{p^{n \vee m}}$ contient \mathbb{F}_{p^n} et \mathbb{F}_{p^m} .

De la même façon $\mathbb{F}_{p^n} \cap \mathbb{F}_{p^m}$ est un corps \mathbb{F}_{p^d} tel que \mathbb{F}_{p^n} et \mathbb{F}_{p^m} en sont des extensions. On en déduit donc que d divise n et m et donc d divise $n \wedge m$ et donc $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^{n \wedge m}}$. Réciproquement comme $n \wedge m$ divise n et m , on en déduit que $\mathbb{F}_{p^{n \wedge m}} \subset \mathbb{F}_{p^n} \cap \mathbb{F}_{p^m}$ d'où le résultat. \square

III.3. Théorie de Galois

III.3.1. Extensions séparables. —

Définition III.3.1. — Un polynôme irréductible $P \in k[X]$ est dit *séparable sur k* si ses racines $\alpha_1, \dots, \alpha_n$ dans un corps de décomposition K de P sur k sont deux à deux distinctes. Un polynôme non constant est dit séparable sur k si tous ses facteurs irréductibles dans $k[X]$ le sont.

Remarque : notons que cette notion ne dépend pas du corps de décomposition considéré, puisqu'ils sont tous isomorphes entre eux et que donc si dans un, P possède des racines multiples ce sera le cas pour tous.

Exemple : soit $k = \mathbb{F}_p(T^p) \subset K = \mathbb{F}_p(T)$ et considérons le polynôme $P = X^p - T^p \in k[X]$ qui est un polynôme d'Eisenstein et donc irréductible sur k . Dans $K[X]$ il se factorise en $P(X) = (X - T)^p$ de sorte que P n'est pas un polynôme séparable sur k . En revanche il l'est sur K .

Remarque : si $P \in k[X]$ est séparable sur k et si L est une extension de k alors tout diviseur $Q \in L[X]$ de P est aussi séparable sur L .

Proposition III.3.2. — Soit $P \in k[X]$ non constant ; alors P est séparable si et seulement si P et P' sont premiers entre eux.

Démonstration. — Si P n'est pas séparable sur k , alors il existe une extension finie K/k dans laquelle P admet une racine α d'ordre ≥ 2 , i.e. $P'(\alpha) = 0$ de sorte que le pgcd de P et P' est de degré ≥ 1 puisqu'il admet une racine dans K . Réciproquement si $D = P \wedge P'$ est de degré ≥ 1 alors il admet une racine α dans une extension K/k de degré finie et donc $P(\alpha) = P'(\alpha)$ et donc P n'est pas séparable sur k . \square

Remarque : un polynôme irréductible $P \in k[X]$ est séparable si et seulement si $P' \neq 0$.

Corollaire III.3.3. — En caractéristique nulle, tout polynôme est séparable.

Définition III.3.4. — Soit K/k une extension algébrique. On dit que $\alpha \in K$ est *séparable sur k* si son polynôme minimal sur k l'est. On dit que l'extension K/k est *séparable* si tous ses éléments le sont.

Proposition III.3.5. — Soient $k \subset L \subset K$ des extensions de corps. Si K/k est séparable alors L/k et K/L le sont aussi.

Démonstration. — Le cas de L/k est trivial, étudions alors le cas de K/L . Pour $x \in K$, par hypothèse $\mu_{x,k}$ est séparable et $\mu_{x,L}$ en est un diviseur de sorte que x est séparable sur L . \square

Définition III.3.6. — Soient K/k une extension de corps et $\tau : k \rightarrow L$ un morphisme. On note $\text{hom}_\tau(K, L)$ l'ensemble des morphismes de corps $\phi : K \rightarrow L$ tels que $\phi|_k = \tau$.

Remarque : si on identifie k à son image $\tau(k)$, alors $\text{hom}_\tau(K, L)$ n'est autre que l'ensemble des k -morphisms de K vers L .

Théorème III.3.7. — Soit K/k une extension de degré fini.

1) Pour toute extension L/k , on a l'inégalité

$$\# \text{hom}_{k\text{-alg}}(K, L) \leq [K : k].$$

2) Si K/k est séparable alors l'inégalité de 1) est une égalité lorsque L est algébriquement clos.

3) S'il existe une extension L/k telle que l'égalité ait lieu alors K/k est séparable.

Démonstration. — Par hypothèse K est de la forme $k[x_1, \dots, x_r]$; on va alors montrer 1) et 2) en raisonnant par récurrence sur r . Pour $r = 1$, i.e. $K = k[x]$, d'après la proposition III.1.26, le cardinal de $\text{hom}_{k\text{-alg}}(K, L)$ est égal au nombre de racines distinctes dans L , du polynôme minimal de x sur k et donc $\leq [K : k]$. De plus si x est séparable sur k , l'égalité est obtenue dans 1) si L est un corps de décomposition sur k de P ce qui finit de prouver 1) et 2) dans le cas $r = 1$.

Supposons alors le résultat établi jusqu'au rang $r - 1$. On pose $k_1 = k[x_1] \subset K = k_1[x_2, \dots, x_r]$ et

$$(2) \quad \# \text{hom}_{k\text{-alg}}(k_1, L) \leq [k_1 : k].$$

En outre pour $\tau : k_1 \rightarrow L$ un k -morphisme, par hypothèse de récurrence appliquée à K/k_1 , on a

$$(3) \quad \# \text{hom}_\tau(K, L) = \# \text{hom}_{k_1\text{-alg}}(K, l) \leq [K : k_1].$$

Or si $\phi : K \rightarrow L$ est un k -morphisme sa restriction ϕ_1 à k_1 est un k -morphisme et $\phi \in \text{hom}_{\phi_1}(K, L)$. On a donc

$$(4) \quad \# \text{hom}_{k\text{-alg}}(K, L) \leq \text{hom}_{k\text{-alg}}(k_1, L) \# \text{hom}_{k_1\text{-alg}}(K, L)$$

avec égalité si et seulement si tout k -morphisme $\tau : k_1 \rightarrow L$ se prolonge en un k -morphisme $\phi : K \rightarrow L$. En utilisant la multiplicativité des degrés, les inégalités (2) et (3) donnent

$$(5) \quad \# \text{hom}_{k\text{-alg}}(K, L) \leq [K : k_1] \cdot [k_1 : k] = [K : k]$$

ce qui finit de prouver 1).

Supposons de plus que K/k est séparable et que L est algébriquement clos; d'après le lemme III.1.36, tout k -morphisme $k_1 \rightarrow L$ se prolonge en un k -morphisme $\phi : K \rightarrow L$ et donc (4) est une égalité. De plus (2) et (3) sont des égalités d'après le cas $r = 1$ et l'hypothèse de récurrence et donc (5) est une égalité, ce qui finit de prouver 2).

En ce qui concerne 3), supposons qu'il existe L/k telle que (5) soit une égalité et soit $x \in K$ arbitraire. Prenons dans le raisonnement précédent $k_1 = k[x]$ de sorte que (5) implique que les inégalités (2), (3) et (4) sont des égalités. En particulier on a

$$\# \text{hom}_{k\text{-alg}}(k[x], L) = [k[x] : k],$$

et d'après la proposition III.1.26 ceci implique que x est séparable sur k et puisque x est quelconque que K/k est séparable. \square

Corollaire III.3.8. — Soit K/k une extension de degré fini.

1) Si $x \in K$ est séparable sur k alors $k[x]/k$ est séparable.

2) Soit E/k une extension intermédiaire. Si K/E et E/k sont séparables alors K/k l'est aussi.

3) Si $K = k[x_1, \dots, x_r]$ avec chaque x_i séparable sur k alors K/k est séparable.

Démonstration. — 1) Soit L un corps de décomposition sur k de $\mu_{x,k}$; comme x est séparable sur k alors $\mu_{x,k}$ est scindé à racines simples dans L et donc d'après la proposition III.1.26,

$$\# \text{hom}_{k\text{-alg}}(k[x], L) = [k[x] : k],$$

de sorte que d'après le théorème précédent, $k[x]/k$ est séparable.

2) Soit L une clôture algébrique de K ; puisque E/k et K/E sont séparables alors d'après le théorème précédent on a

$$\# \text{hom}_{k\text{-alg}}(E, L) = [E : k]$$

et tout k -morphisme $\tau : E \rightarrow L$ se prolonge en exactement $[K : E]$ morphismes $K \rightarrow L$. On en déduit que

$$\# \text{hom}_{k\text{-alg}}(K, L) = [K : E].[E : k] = [K : k],$$

et donc, d'après le théorème précédent, K/k est séparable.

Enfin 3) découle de 1) et 2) par récurrence sur r . □

Corollaire III.3.9. — Soit $P \in k[X]$ un polynôme séparable et K un corps de décomposition de P sur k . Alors K/k est séparable.

Démonstration. — Soient x_1, \dots, x_r les racines de P dans $K = k[x_1, \dots, x_r]$. Pour tout $i = 1, \dots, r$, $\mu_{x_i, k}$ est un diviseur irréductible de P et est donc séparable sur k , de sorte que x_i est séparable sur k . Le résultat découle alors du corollaire précédent. □

Théorème III.3.10. — (de l'élément primitif)

Soit K/k une extension séparable de degré fini ; alors K admet un élément primitif ζ sur k , i.e. $K = k[\zeta]$.

Démonstration. — Si k est un corps fini alors K^\times est cyclique et $K = k[\zeta]$ pour tout générateur ζ de K^\times .

Supposons à présent que k est infini et notons $n = [K : k]$. Pour Ω une clôture algébrique de K , K/k étant séparable, il existe des k -isomorphismes $K \rightarrow \Omega$ deux à deux distincts τ_1, \dots, τ_n de sorte que pour tous $i \neq j$, $\text{Ker}(\tau_i - \tau_j)$ est un sous-espace strict de K .

Lemme III.3.11. — Un espace vectoriel V sur un corps infini k n'est pas réunion finie de sous-espaces stricts V_1, \dots, V_t .

Démonstration. — C'est clair pour $t = 1$ et on suppose, par hypothèse de récurrence, que $t \geq 2$ et le résultat établi pour $t-1$. Ainsi il existe $u, v \in V$ tels que $u \notin V_t$ et $v \notin V_1 \cup \dots \cup V_{t-1}$. Si on avait $V = V_1 \cup \dots \cup V_t$ alors $v \in V_t$ et comme l'ensemble des $x_\lambda := u + \lambda v$ pour $\lambda \in k$ est infini, il existe $\lambda \neq \mu$ tels que x_λ et x_μ appartiennent au même V_j . On ne peut avoir $j = t$ car sinon on aurait $u \in V_t$; donc $j < t$ et V_j contient $x_\lambda - x_\mu = (\lambda - \mu)v$ et donc v aussi ce qui n'est pas. □

Ainsi d'après le lemme il existe $x \in K$ n'appartenant à aucun des $\text{Ker}(\tau_i - \tau_j)$ de sorte que les $\tau_i(x)$ sont deux à deux distincts. Comme ce sont des racines dans Ω de $\mu_{x, k}$ de sorte que

$$n \leq [k[x] : k] \leq [K : k] = n$$

et donc $K = k[x]$. □

Remarque : soit K/\mathbb{Q} une extension finie et $\alpha \in K$ un élément primitif de polynôme minimal $\mu_{\alpha, \mathbb{Q}}(X) = \prod_{i=1}^n (X - \alpha_i)$. Les plongements de K dans \mathbb{C} sont en bijection avec les racines α_i de $\mu_{\alpha, \mathbb{Q}}$. À chaque racine réelle (resp. complexe) correspond un plongement réel (resp. complexe), i.e. dont l'image est contenue dans \mathbb{R} (resp. n'est pas contenue dans \mathbb{R}).

Notation III.3.12. — On note r_1 (resp. r_2) le nombre de plongements réels de K : on a $r_1 + 2r_2 = n = [K : \mathbb{Q}]$. Le couple (r_1, r_2) est appelé la signature de K .

Remarque : sous-entendu dans la notation est que ces nombres ne dépendent pas du choix de l'élément primitif α ce qui est clair.

Définition III.3.13. — Soient $\sigma_1, \dots, \sigma_{r_1}$ les plongements réels d'une extension fini K de \mathbb{Q} et soient $\sigma_{r_1+1}, \dots, \sigma_{r_1+r_2}$ des plongements complexes de K tels que $\{\sigma_{r_1+1}, \overline{\sigma_{r_1+1}}, \dots, \sigma_{r_1+r_2}, \overline{\sigma_{r_1+r_2}}\}$ est l'ensemble des plongements complexes de K . Le *plongement canonique* de K est alors l'application \mathbb{Q} -linéaire

$$\begin{cases} \sigma : K & \longrightarrow & \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \\ x & \longmapsto & (\sigma_1(x), \dots, \sigma_{r_1+r_2}(x)). \end{cases}$$

Remarque : le plongement canonique dépend du choix pour chaque $i = 1, \dots, r_2$ entre σ_{r_1+i} et $\overline{\sigma_{r_1+i}}$.

Proposition III.3.14. — Soit K/k une extension de degré fini; les deux points suivants sont alors équivalents

- 1) L'extension K/k admet un élément primitif.
- 2) Le nombre d'extensions intermédiaires de K/k est fini.

Démonstration. — Supposons 1) i.e. qu'il existe ζ tel que $K = k[\zeta]$ et notons $P := \mu_{\zeta, k}$. Pour $k \subset L \subset K$ une extension intermédiaire $Q := \mu_{\zeta, L}$ est un diviseur irréductible de P dans $L[X]$ de degré $[K : L]$ ce qui ne donne qu'un nombre fini de tels Q . Notons $L' \subset L$ le sous-corps de L engendré sur k par les coefficients de Q ; comme Q est encore irréductible sur L' on a donc $[K : L] = \deg Q = [K : L']$ et donc $L = L'$. Autrement dit L est entièrement déterminé par Q et comme il n'y a qu'un nombre fini de tels Q on obtient bien 2).

En ce qui concerne la réciproque, notons que dans le cas où k est fini, les points 1) et 2) sont toujours satisfait de sorte qu'il n'y a rien à montrer. Supposons donc que k est infini et soit $\zeta \in K$ tel que $[k[\zeta] : k]$ soit maximal et montrons que $K = k[\zeta]$. Soit donc $x \in K$ et pour $t \in k$ on note $\zeta_t = \zeta + tx$ ainsi que $L_t = k[\zeta_t]$. Comme il n'y a qu'un nombre fini de corps intermédiaires et que k est supposé infini, il existe $s \neq t$ tels que $L_s = L_t$. Ce corps contient $(s - t)x$ et donc x ainsi que ζ soit

$$k[\zeta] \subset k[\zeta, x] \subset k[\zeta_t].$$

Par maximalité du degré de $k[\zeta]$, on en déduit que ces inclusions sont des égalités et donc en particulier que $x \in k[\zeta]$. \square

Remarque : pour $K = \mathbb{F}_p(X, Y)$ et k le sous-corps engendré par X^p et Y^p on note que $[K : k] = p^2$ et que pour tout $x \in K$, comme $x^p \in k$, on a $[k[x] : k] = 1$ ou p selon que x appartient ou n'appartient pas à k . Ainsi K/k n'est pas monogène et admet donc une infinité de corps intermédiaires.

Définition III.3.15. — Un corps k est dit *parfait* si sa caractéristique est nulle ou s'il est de caractéristique $p > 0$ et que son Frobenius est surjectif.

Remarque : un corps algébriquement clos de caractéristique p est parfait; en particulier un sous-corps d'un corps parfait n'est pas nécessairement parfait. Un corps fini est parfait, en revanche $\mathbb{F}_p(T)$ n'est pas parfait.

Lemme III.3.16. — Soit k un corps parfait et K/k une extension finie. Alors K est parfait.

Démonstration. — Supposons que k est de caractéristique p sinon il n’y a rien à prouver. Le Frobenius f_K de K est bijectif sur k par hypothèse et y admet donc un inverse f_K^{-1} . Alors $f_K(K)$ est un $k = f_K(k)$ -sous-espace vectoriel de K ; plus généralement si les $x_i \in K$ forment une famille libre sur k alors les $f_K(x_i)$ sont aussi libre sur k dans $f_K(K)$ de sorte que $[K : k] \leq [f_K(K) : k]$, l’égalité découlant alors de l’inclusion $f_K(K) \subset K$. \square

L’intérêt des corps parfaits vient du résultat fondamental suivant.

Théorème III.3.17. — *Un corps k est parfait si et seulement si tout polynôme irréductible de $k[X]$ est séparable.*

Démonstration. — Supposons k parfait et soit $P \in k[X]$ irréductible. Alors $P' = 0$ si et seulement si k est de caractéristique p et P est de la forme $P = \sum_n a_{np} X^{np}$. Comme k est parfait on a alors

$$P = \sum_n F^{-1}(a_{np}^p) X^{np} = \left(\sum_n F^{-1}(a_{np}) X^n \right)^p,$$

et P ne serait pas irréductible. Ainsi P' est non nul et $P \wedge P' = 1$, i.e. P est séparable sur k .

Réciproquement supposons que tout polynôme irréductible de $k[X]$ est séparable et supposons k de caractéristique $p > 0$. Soit alors $t \in k$ et supposons que t n’admette pas de racine p -ième de sorte que le polynôme minimal P sur k d’une racine p -ième $t^{1/p}$ de t dans une clôture algébrique de k , est irréductible de degré > 1 . Comme P divise $X^p - t = (X - t^{1/p})^p$ alors $P(X) = (X - t^{1/p})^k$ avec $2 \leq k \leq p$ et P n’est pas séparable, d’où la contradiction. \square

III.3.2. Extensions normales et galoisiennes. —

Définition III.3.18. — Une extension algébrique K/k est dit *normale* si pour tout $\alpha \in K$ le polynôme $\mu_{\alpha,k}$ est décomposé dans K .

Proposition III.3.19. — *Soit K le corps de décomposition sur k d’un polynôme $P \in k[X]$; alors K/k est normale.*

Démonstration. — Soit $\alpha \in K$ et L un corps de décomposition sur K de $\mu_{\alpha,k}$; comme $P\mu_{\alpha,k}$ est scindé dans L et que L est engendré par les racines de $P\mu_{\alpha,k}$, alors L est aussi un corps de décomposition de $P\mu_{\alpha,k}$ sur k . Il s’agit alors de vérifier que $L = K$. Soit β une racine quelconque de $\mu_{\alpha,k}$ et soit $\tau : k[\alpha] \simeq k[\beta]$. D’après le théorème III.1.29, τ se prolonge en un k -automorphisme σ de L . Notons x_1, \dots, x_m les racines distinctes de P ; par définition K est engendré par les x_i et donc $\sigma(K)$ est engendré par les $\sigma(x_i)$. Or, comme $\sigma(P) = P$, σ induit une permutation des x_i et donc $\sigma(K) = K$ de sorte que $\beta = \sigma(\alpha)$ appartient à K . \square

Définition III.3.20. — Pour K/k une extension algébrique, on note

$$\text{aut}(K/k) = \{g \in \text{aut}(K) : g|_k = \text{Id}_k\}.$$

Remarque : si $[K : k]$ est fini alors d’après le théorème III.3.7, $\text{aut}(K/k)$ est un groupe fini. Pour $\alpha \in K$ et $g \in \text{aut}(K/k)$ comme $g(\mu_{\alpha,k}) = \mu_{\alpha,k}$ alors g permute les racines de $\mu_{\alpha,k}$. Ainsi $\mu_{\alpha,k}$ est divisible par $\prod_{\beta \in \mathcal{O}_{K/k}(\alpha)} (X - \beta)$ où $\mathcal{O}_{K/k}(\alpha)$ désigne l’orbite de α sous l’action de $\text{aut}(K/k)$, i.e. $\mathcal{O}_{K/k}(\alpha) := \{g(\alpha) : g \in \text{aut}(K/k)\}$. On se demande alors si cette divisibilité est une égalité, autrement dit si l’action de $\text{aut}(K/k)$ sur l’ensemble des racines de $\mu_{\alpha,k}$ est transitive.

- Évidemment pour qu'on ait une chance que cette égalité ait lieu, il faut pour le moins que K contienne toutes les racines de $\mu_{\alpha,k}$. Par exemple pour $k = \mathbb{Q}$ et $K = \mathbb{Q}(\sqrt[3]{2})$, le groupe $\text{aut}(K/k)$ est réduit à l'identité puisque ni $j\sqrt[3]{2}$ ni $j^2\sqrt[3]{2}$ n'appartiennent à K .
- Notons par ailleurs que $\prod_{\beta \in \mathcal{O}_{K/k}(\alpha)} (X - \beta)$ est un polynôme dont toutes les racines sont deux à deux distinctes. Ainsi s'il devait être égal à $\mu_{\alpha,k}$, α doit être séparable sur k .

Définition III.3.21. — On dit qu'une extension K/k de degré fini est *galoisienne* si $\#\text{aut}(K/k) = [K : k]$. Dans ce cas $\text{aut}(K/k)$ est noté $\text{Gal}(K/k)$ et s'appelle *le groupe de Galois* de K/k .

Théorème III.3.22. — Soit K/k une extension de degré fini. Les conditions suivantes sont équivalentes :

- 1) K/k est galoisienne ;
- 2) K/k est normale et séparable ;
- 3) K est le corps de décomposition sur k d'un polynôme séparable.

Dans ces conditions, pour tout $\alpha \in K$, on a

$$\mu_{\alpha,k}(X) = \prod_{\beta \in \mathcal{O}_{K/k}(\alpha)} (X - \beta).$$

Démonstration. — L'implication 3) \Rightarrow 2) découle de la proposition III.3.19 et du corollaire III.3.9. L'implication 2) \Rightarrow 3) est facile : on écrit $K = k[x_1, \dots, x_n]$ de sorte que K/k étant séparable et normale, $P = \prod_{i=1}^n \mu_{x_i,k}$ est séparable et scindé dans K : K est donc bien un corps de décomposition de P sur k .

Montrons 2) \Rightarrow 1) : soit L une clôture algébrique de K . D'après le théorème III.3.7, il y a exactement $n := [K : k]$ k -morphisms g_1, \dots, g_n de K dans L et donc

$$\#\text{aut}(K/k) \leq n = [K : k].$$

Il s'agit donc de montrer que chacun des g_i appartient à $\text{aut}(K/k)$, i.e. applique K sur lui-même. D'après le théorème de l'élément primitif, il existe $\zeta \in K$ tel que $K = k[\zeta]$ et pour tout $i = 1, \dots, n$, comme $g_i(\mu_{\zeta,k}) = \mu_{\zeta,k}$, $g_i(\zeta)$ est une racine de P et donc appartient à K puisque K/k est normale : on a donc bien $g_i(K) = K$ d'où le résultat.

Montrons enfin que 1) \Rightarrow 2), et donc que $\text{aut}(K/k)$ est de cardinal $[K : k]$. D'après III.3.7, on en déduit que K/k est séparable et il nous reste à prouver que K/k est normale. Soit $\alpha \in K$ et L une clôture algébrique de K : il s'agit alors de montrer que pour toute racine $\beta \in L$ de $\mu_{\alpha,k}$ alors $\beta \in K$. D'après l'unicité à isomorphisme près du corps de rupture de $\mu_{\alpha,k}$ soit $\tau : k[\alpha] \simeq k[\beta]$ avec $\tau(\alpha) = \beta$. D'après le lemme III.1.36, τ se prolonge en un k -morphisme $\sigma : K \rightarrow L$. Ainsi des inégalités

$$[K : k] = \#\text{aut}(K/k) \leq \#\text{hom}_{k\text{-alg}}(K, L) \leq [K : k]$$

on en déduit que $\#\text{hom}_{k\text{-alg}}(K, L) = [K : k]$ et donc que $\sigma \in \text{aut}(K/k)$, soit $\beta = \sigma(\alpha) \in K$ d'où le résultat. \square

Théorème III.3.23. — (**Artin**)

Soient K un corps et G un sous-groupe fini de $\text{aut}(K)$. On note

$$K^G := \{x \in K : g(x) = x, \forall g \in G\}.$$

Alors K^G est un sous-corps de K tel que l'extension K/K^G est galoisienne de groupe de Galois G .

Remarque : en particulier $[K : K^G] = \#G$.

Démonstration. — Il est clair que K^G est un sous-corps de K , montrons que K/K^G est galoisienne. Soit $\alpha \in K$ et notons $\mathcal{O}_G(\alpha)$ son orbite sous G . Considérons alors $P_\alpha(X) := \prod_{\beta \in \mathcal{O}_G(\alpha)} (X - \beta) \in K[X]$. Comme pour tout $g \in G$ on a

$$g(P_\alpha)(X) = \prod_{\beta \in \mathcal{O}_G(\alpha)} (X - g(\beta)) = \prod_{\beta \in \mathcal{O}} (X - \beta) = P_\alpha$$

on en déduit que $P_\alpha \in K^G[X]$. En outre P_α est divisible par μ_{α, K^G} qui est lui-même divisible par $Q(X) := \prod_{\beta \in \mathcal{O}_{K/K^G}(\alpha)} (X - \beta)$. Comme $G \subset \text{aut}(K/K^G)$, alors $\deg Q \geq \#G$ et donc $P_\alpha = \mu_{\alpha, K^G}$ et l'orbite de α sous G est égale à celle sous $\text{aut}(K/K^G)$. Ainsi μ_{α, K^G} est scindé à racines simples dans K et donc, comme le raisonnement est valable pour tout $\alpha \in K$, K/K^G est séparable et normale, i.e. galoisienne. En outre le groupe de Galois $\text{Gal}(K/K^G)$ contient G et donc $\#G \leq [K : K^G]$; pour ζ un élément primitif de K/K^G , d'après ce qui précède

$$[K : K^G] = \deg \mu_{\zeta, K^G} = \#\mathcal{O}_G(\alpha) \leq \#G$$

et donc finalement $G = \text{aut}(K/K^G) = [K : K^G]$. □

Corollaire III.3.24. — Soit K/k une extension galoisienne de groupe de Galois $G = \text{Gal}(K/k)$; alors $K^G = k$.

Démonstration. — Clairement $k \subset K^G$ et puisque K/k est galoisienne, $[K : k] = \#G$. Or d'après le théorème d'Artin, on a $[K : K^G] = \#G$ et le résultat découle du théorème de la base télescopique. □

Définition III.3.25. — On appelle groupe de Galois d'un polynôme P non constant de $k[X]$, le groupe de Galois d'un corps de décomposition de P sur k .

Remarque : dans le cas où k est un corps parfait, le polynôme $\frac{P}{P \wedge P'}$ est séparable et admet les mêmes corps de décomposition ce qui permet de se ramener au cas P séparable. Comme le groupe de Galois laisse k invariant, il permute les racines de P ce qui permet de le considérer comme un sous-groupe de \mathfrak{S}_n où $n = \deg P$.

Proposition III.3.26. — Le polynôme P est irréductible si et seulement si l'action de son groupe de Galois est transitive sur ses racines.

Démonstration. — Supposons P irréductible : ses racines x_i s'identifient aux k -morphisms $k[X]/(P) \rightarrow \Omega$ où Ω est un clôture algébrique de k . Or ces k -morphisms s'identifient aux éléments du groupe de Galois et l'action est donc transitive.

Réciproquement supposons l'action transitive et supposons $P = QR$ avec $Q, R \in k[X]$ et $\deg Q > 0$. Comme précédemment le groupe de Galois permute les racines de Q de sorte que si l'action est transitive les racines de Q sont celles de P et $Q = P$. □

Exemple : reprenons l'exemple de l'extension cyclotomique $\mathbb{Q}[\zeta_n]/\mathbb{Q}$ où ζ_n est une racine primitive n -ième de l'unité dans \mathbb{C} . Un élément σ de $\text{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q})$ est déterminé par $\sigma(\zeta_n)$ qui est de la forme $\zeta_n^{\chi(\sigma)}$ pour $\chi(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^\times$. On définit ainsi un morphisme injectif

$$\chi : \text{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q}) \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times$$

qui est aussi surjectif car les deux groupes ont même cardinal.

Définition III.3.27. — Pour $P \in k[X]$ séparable dont les racines dans une clôture algébrique Ω de k sont x_1, \dots, x_n . Le discriminant de P est défini par

$$\text{Disc}(P) = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j} (x_i - x_j).$$

Proposition III.3.28. — Avec les notations ci-dessus, $\text{Disc}(P)$ est un élément de k^\times et si k n'est pas de caractéristique 2, est un carré de k^\times si et seulement si le groupe de Galois de G est contenu dans le groupe alterné \mathcal{A}_n .

Démonstration. — Visiblement $\text{Disc}(P)$ est non nul et invariant par son groupe de Galois G ; il appartient donc à k^\times . Notons alors $\delta = \prod_{i < j} (x_i - x_j) \in \Omega$, de sorte que $\text{Disc}(P) = \delta^2$. Pour $\sigma \in \mathfrak{S}_n$, par définition de la signature on a $\sigma(\delta) = \epsilon(\sigma)\delta$. Ainsi, en caractéristique différente de 2, $\delta \in k^\times$ si et seulement si $G \subset \mathcal{A}_n$. \square

III.3.3. Correspondance de Galois. — Soit K/k une extension de degré fini galoisienne de groupe de Galois $G = \text{Gal}(K/k)$.

Définition III.3.29. — Pour tout sous-groupe H de G , on note

$$K^H := \{x \in K : h(x) = x, \forall h \in H\},$$

le sous-corps de K fixé par H .

Remarque : on a clairement $k = K^G \subset K^H$ de sorte que K^H est un corps intermédiaire entre k et K .

Théorème III.3.30. — (*Correspondance de Galois*)

- 1) Pour tout sous-groupe H de G , l'extension K/K^H est galoisienne et $\text{Gal}(K/K^H) = H$.
- 2) Réciproquement pour L un corps intermédiaire, K/L est galoisienne et

$$\text{Gal}(K/L) = \{g \in G : g(l) = l, \forall l \in L\}$$

est un sous-groupe H de G et $L = K^H$.

- 3) Les applications

$$H \mapsto K^H \quad \text{et} \quad L \mapsto \text{Gal}(K/L)$$

sont des bijections réciproques entre les deux ensembles

$$\{\text{corps intermédiaires } L \text{ de } K/k\} \leftrightarrow \{\text{sous-groupes } H \text{ de } G\}.$$

Si L et H se correspondent, on a

$$[K : L] = \#H \quad \text{et} \quad [L : k] = \#G/H.$$

Ces deux bijections sont décroissantes, i.e.

$$H \subseteq H' \Leftrightarrow K^H \supseteq K^{H'} \quad \text{et} \quad L \subseteq L' \Leftrightarrow \text{Gal}(K/L) \supseteq \text{Gal}(K/L').$$

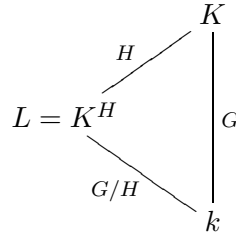
- 4) Si L correspond à H alors, pour tout $g \in G$, $g(L)$ correspond gHg^{-1} .
- 5) Soient L un corps intermédiaire et $H = \text{Gal}(K/L)$; alors L/k est séparable et on a les équivalences

$$L/k \text{ galoisienne} \Leftrightarrow L/k \text{ normale} \Leftrightarrow H \text{ distingué dans } G.$$

Dans ce cas on a $\text{Gal}(L/k) \simeq G/H$.

6) Soient L un corps intermédiaire et $H = \text{Gal}(K/L)$. Alors les bijections de 3) induisent une bijection entre l'ensemble des sous-extensions $k \subseteq L' \subseteq L$ et l'ensemble des sous-groupes H' de G contenant H : en particulier il n'y a qu'un nombre fini de tels L' .

Remarque : visuellement on résume ces résultats par un diagramme



Démonstration. — L'assertion 1) est le théorème d'Artin.

2) Soient L un corps intermédiaire et $x \in K$. Par hypothèse $\mu_{x,k}$ est scindé à racines simples sur K et donc $\mu_{x,L}$ aussi et donc K/L est séparable et normale et donc galoisienne. Son groupe de Galois est clairement un sous-groupe H de G et $L = K^H$ d'après le corollaire III.3.24 ce qui prouve 2). L'assertion 3) résulte alors de 1) et 2) et de la multiplicativité du degré.

4) Si L correspond à H alors pour tout $g \in G$, on a

$$g(L) = \{g(x) : h(x) = x, \forall h \in H\} = \{y = g(x) : ghg^{-1}(y) = y, \forall h \in H\}$$

i.e. $g(L)$ correspond à gHg^{-1} .

5) Soit L un corps intermédiaire de groupe de Galois $H = \text{Gal}(L/K)$ d'après 2). Alors L/k étant séparable, elle est galoisienne si et seulement si elle est normale. Si H est distingué dans G , d'après 4) on a $g(L) = L$ pour tout $g \in G$ de sorte que pour tout $\alpha \in L$, $\mu_{\alpha,k}(X) = \prod_{\beta \in \mathcal{O}_G(\alpha)} (X - \beta)$ a toutes ses racines dans L et donc L/k est normale. Réciproquement si L/k est normale, pour $x \in L$ et $g \in G$, comme $g(x)$ est une racine de $\mu_{x,k}$ alors $g(x) \in L$ et donc $g(L) = L$ pour tout $g \in H$, de sorte que, d'après 4), H est distingué dans G . On a ainsi l'équivalence

$$L/k \text{ galoisienne} \Leftrightarrow H \text{ distingué dans } G.$$

Supposons ces conditions équivalentes vérifiées alors

$$\# \text{Gal}(L/k) = [L : k] = \frac{[K : k]}{[K : L]} = \#G/H.$$

Par ailleurs, L étant stable sous G , l'application de restriction $g \mapsto g|_L$ est un morphisme de groupes dont le noyau est $\text{Gal}(K/L) = H$ ce qui fournit un isomorphisme

$$G/H \xrightarrow{\sim} \text{Gal}(L/k).$$

Enfin 6) est une conséquence immédiate de 3). □

Remarque : la notion d'extension galoisienne est ainsi le cadre dans lequel les sous-extensions sont contrôlées par les sous-groupes de son groupe d'automorphisme. Partant d'une extension quelconque de degré fini, on aimerait ainsi la plonger dans une extension galoisienne. Une condition nécessaire d'après la proposition III.3.5 est que l'on parte d'une extension séparable. La proposition suivante montre que cette condition est suffisante.

Proposition III.3.31. — (Clôture normale)

Soit K/k une extension de degré fini alors K est contenu dans une extension L de degré fini et normale sur k . Par ailleurs il existe à K -isomorphisme près, une unique telle extension

qui est minimale pour cette propriété appelée une clôture normale de K/k . Si en outre K/k est séparable alors L/k est galoisienne et dite une clôture galoisienne de K/k .

Remarque : en particulier si k est de caractéristique nulle, toute extension K/k de degré fini admet une clôture galoisienne.

Démonstration. — Écrivons $K = k[x_1, \dots, x_r]$ et $P = \prod_{i=1}^r \mu_{x_i, k}$. Soit alors L un corps de décomposition de P sur K ; comme L est aussi un corps de décomposition de P sur k , l'extension L/k est finie et normale. Si L' est une extension intermédiaire entre K et L , normale sur k alors L' contient x_1, \dots, x_r et donc toutes les racines des $\mu_{x_i, k}$ et donc L : autrement dit L est minimale.

Soit par ailleurs E une extension de K normale sur k et minimale pour cette propriété; E contient donc un corps de décomposition L' de P sur K et par minimalité $E = L'$. D'après l'unicité du corps de décomposition, il existe un K -isomorphisme $\tau : L \simeq E$.

Enfin si K/k est séparable alors P est séparable sur k ainsi que L le corps de décomposition de P sur k . \square

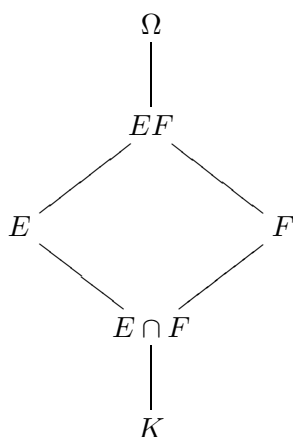
Corollaire III.3.32. — Soit K/k une extension séparable de degré fini. Le nombre d'extensions intermédiaires $k \subseteq L \subseteq K$ est fini.

Démonstration. — Soit E une clôture galoisienne de K/k et G son groupe de Galois qui est donc fini. L'affirmation découle alors du fait que les extensions intermédiaires L de K/k sont en bijection avec l'ensemble des sous-groupes de G contenant $H = \text{Gal}(E/K)$. \square

III.3.4. Extensions composées. — Considérons la situation suivante : K est un corps, Ω une clôture algébrique de K et soient E, F deux extensions de K contenues dans Ω .

Définition III.3.33. — On note EF le sous-corps de Ω engendré par E et F appelé l'extension composée de E et F .

Remarque : en introduisant $E \cap F$, on représente la situation par le diagramme



Lemme III.3.34. — Si E/K est galoisienne alors EF/F est galoisienne. Si en outre F/K est galoisienne alors EF/K et $E \cap F/K$ sont galoisiennes.

Démonstration. — Si E/K est galoisienne alors E est le corps de décomposition sur K d'un polynôme P séparable sur K et donc EF/E est un corps de décomposition sur E de P , i.e. l'extension est galoisienne.

Si en outre F est le corps de décomposition sur K d'un polynôme Q séparable sur K alors EF est le corps de décomposition sur K du polynôme PQ et donc EF/F est galoisienne.

En ce qui concerne $E \cap F/K$, il suffit de vérifier que tout K -morphisme $\sigma : E \cap F \rightarrow \Omega$ stabilise $E \cap F$, i.e. $\sigma(E \cap F) = E \cap F$. D'après le théorème III.3.7, σ s'étend en un K -morphisme $\tau : EF \rightarrow \Omega$: comme E/K (resp. F/K) est galoisienne, alors $\tau(E) = E$ (resp. $\tau(F) = F$) et donc $\tau(E \cap F) = E \cap F$. \square

Étudions à présent ce qui se passe au niveau des groupes de Galois. Supposons donc E/K galoisienne de sorte que EF/F est galoisienne : un élément $\sigma \in \text{Gal}(EF/F)$ est l'identité sur F et donc sur K , i.e. $\sigma \in \text{Gal}(EF/K)$. Comme E/K est galoisienne alors $\sigma(E) = E$ de sorte que σ définit un élément de $\text{Gal}(E/K)$ noté $i(\sigma)$.

Proposition III.3.35. — *L'homomorphisme i ci-dessous obtenu comme le composé*

$$\text{Gal}(EF/F) \hookrightarrow \text{Gal}(EF/K) \twoheadrightarrow \text{Gal}(E/K)$$

est injectif d'image $\text{Gal}(E/E \cap F)$.

Démonstration. — Si $\sigma \in \text{Gal}(EF/F)$ est l'identité sur E alors σ est l'identité sur le corps engendré par E et F , i.e. sur EF , d'où l'injectivité.

Notons H l'image de i et E^H le corps associé avec donc $H = \text{Gal}(E/E^H)$. On a clairement $E \cap F \subset E^H$; réciproquement E^H est l'ensemble des $x \in E$ qui sont fixés par tout $\sigma \in \text{Gal}(EF/F)$ et donc $x \in E \cap F$. \square

Corollaire III.3.36. — *Si E/K est galoisienne alors*

$$[EF : F] = [E : E \cap F].$$

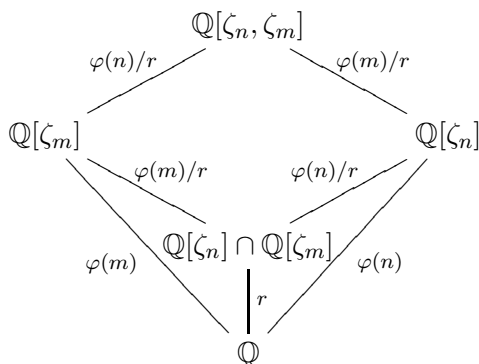
Remarque : en particulier, si E/K est galoisienne, on a $[EF : K] = [E : K].[F : K]$ si et seulement si $K = E \cap F$.

Exemple : considérons le cas où $E = \mathbb{Q}[\zeta_n]$ et $F = \mathbb{Q}[\zeta_m]$ sont deux extensions cyclotomiques. On note $d = n \wedge m$ et $\delta = n \vee m$. Comme $\zeta_n = \zeta_\delta^{\delta/n}$ et $\zeta_m = \zeta_\delta^{\delta/m}$ alors $\mathbb{Q}[\zeta_n, \zeta_m] \subset \mathbb{Q}[\zeta_\delta]$. Inversement d'une relation de Bézout $d = un + vm$ que l'on divise par nm , on en déduit l'égalité $\zeta_\delta = \zeta_m^u \zeta_n^v$ et donc $\mathbb{Q}[\zeta_\delta] \subset \mathbb{Q}[\zeta_n, \zeta_m]$ et finalement

$$\mathbb{Q}[\zeta_n, \zeta_m] = \mathbb{Q}[\zeta_{n \vee m}].$$

En ce qui concerne $\mathbb{Q}[\zeta_n] \cap \mathbb{Q}[\zeta_m]$, des égalités $\zeta_d = \zeta_m^{m/d} = \zeta_n^{n/d}$ on en déduit que $\mathbb{Q}[\zeta_d] \subset \mathbb{Q}[\zeta_n] \cap \mathbb{Q}[\zeta_m]$. Les extensions cyclotomiques étant galoisiennes on a le schéma suivant qui

résume les degrés des différentes extensions :



Comme $\delta d = nm$, l'égalité $[\mathbb{Q}[\zeta_n, \zeta_m] : \mathbb{Q}] = \varphi(\delta)$ dévient alors

$$\varphi(n)\varphi(m) = r\varphi(nm/\delta)$$

de sorte que, comme $\varphi(d)\varphi(nm/d) = \varphi(n)\varphi(m)$, on obtient $r = \varphi(d)$ et donc

$$\mathbb{Q}[\zeta_n] \cap \mathbb{Q}[\zeta_m] = \mathbb{Q}[\zeta_{n \wedge m}].$$

Considérons à présent la situation où E/K et F/K sont toutes deux galoisiennes. Notons

$$j : \text{Gal}(EF/K) \longrightarrow \text{Gal}(E/K) \times \text{Gal}(F/K)$$

le morphisme déduit des morphismes surjectifs $\text{Gal}(EF/K) \twoheadrightarrow \text{Gal}(E/K)$ et $\text{Gal}(EF/K) \twoheadrightarrow \text{Gal}(F/K)$: comme précédemment j est injective.

Remarque : si $E \cap F = K$ alors comme $[EF : K] = [E : K].[F : K]$ on en déduit que j est aussi surjectif. Dans le cas général, les composés π_1 et π_2 de j avec respectivement $\text{Gal}(E/K) \twoheadrightarrow \text{Gal}(E \cap F/K)$ et $\text{Gal}(F/K) \twoheadrightarrow \text{Gal}(E \cap F/K)$, sont clairement égaux à $\text{Gal}(EF/K) \twoheadrightarrow \text{Gal}(E \cap F/K)$ de sorte que l'image de j est contenue dans le sous-groupe

$$G = \{(\sigma_1, \sigma_2) \in \text{Gal}(E/K) \times \text{Gal}(F/K) : \pi_1(\sigma_1) = \pi_2(\sigma_2)\}.$$

Théorème III.3.37. — Soient E/K et F/K deux extensions galoisiennes. L'extension EF/K est alors galoisienne de groupe de Galois G défini ci-dessus.

Démonstration. — Il suffit d'après ce qui précède de montrer que $\sharp G = [EF : K]$. En voyant G comme l'image réciproque de $\text{Gal}(E \cap F/K)$ plongé diagonalement dans $\text{Gal}(E \cap F/K) \times \text{Gal}(E \cap F/K)$ par le morphisme

$$(\pi_1, \pi_2) : \text{Gal}(E/K) \times \text{Gal}(F/K) \longrightarrow \text{Gal}(E \cap F/K) \times \text{Gal}(E \cap F/K)$$

on en déduit que $\sharp G = [E \cap F : K].\sharp \text{Ker } \pi_1.\sharp \text{Ker } \pi_2$ soit

$$\begin{aligned}
 \sharp G &= [E \cap F : K].[E : E \cap F].[F : E \cap F] \\
 &= [F : K].[E : E \cap F] \\
 &= [EF : K].
 \end{aligned}$$

□

Exemple : reprenons la situation où $E = \mathbb{Q}[\zeta_n]$ et $F = \mathbb{Q}[\zeta_m]$ sont deux extensions cyclotomiques. On a vu précédemment que $EF = \mathbb{Q}[\zeta_{n \vee m}]$ et que $E \cap F = \mathbb{Q}[\zeta_{n \wedge m}]$. On vérifie alors que $(\mathbb{Z}/n \vee m \mathbb{Z})^\times$ s'identifie au sous-groupe constitué des éléments $(a, b) \in (\mathbb{Z}/n \mathbb{Z})^\times \times (\mathbb{Z}/m \mathbb{Z})^\times$ tel que les images de a et b modulo d sont égales.

III.4. Résolubilité par radicaux

III.4.1. Introduction historique. — Étant donnée une équation de degré 2, $P(X) = X^2 + aX + b$ ses racines s'expriment selon la formule habituelle

$$x_{\pm} = \frac{-a \pm \sqrt{a^2 - 4b}}{2}.$$

Pour une équation de degré 3, $X^3 + a_1X^2 + a_2X + a_3$, après le changement de variable $Y = X + a_1/3$, l'équation s'écrit $Y^3 + pY + q$. Les formules de Tartaglia-Cardan⁽¹⁾ permettent alors d'exprimer les racines en prenant des racines carrées et des racines cubiques. Par exemple lorsque le discriminant $\Delta = -4p^3 - 27q^2$ est strictement négatif, l'unique racine réelle s'exprime par la formule suivante :

$$x_1 = \frac{\sqrt[3]{\frac{-27q+3\sqrt{-3\Delta}}{2}} + \sqrt[3]{\frac{-27q-3\sqrt{-3\Delta}}{2}}}{3}.$$

Rappelons l'idée originelle de Cardan : on cherche x sous la forme $x = u + v$ avec donc

$$u^3 + v^3 + p(u + v) + q = 0$$

et on impose la relation $3uv + p = 0$ ce qui nous amène à résoudre le système :

$$\begin{cases} u^3 + v^3 = -q \\ u^3v^3 = -(\frac{p}{3})^3 \end{cases}$$

Ainsi u^3 et v^3 sont les solutions de l'équation $X^2 + qX - (\frac{p}{3})^3 = 0$, équation de degré 2 que l'on sait résoudre.

En ce qui concerne l'équation de degré 4, qui après un changement de variable affine se ramène à une équation de la forme $x^4 = px^2 + qx + r$, l'idée de Ferrari, un élève de Cardan, consiste à rajouter un paramètre supplémentaire t en écrivant $x^4 = (x^2 + t)^2 - 2x^2t - t^2$ de sorte que l'équation à résoudre se réécrit

$$(x^2 + t)^2 - 2x^2t - t^2 = px^2 + qx + r \Leftrightarrow (x^2 + t)^2 = (2t + p)x^2 + qx + (t^2 + r).$$

On choisit alors une valeur de t de sorte que $(2t + p)x^2 + qx + (t^2 + r)$ se factorise sous la forme $(ax + b)^2$ ce qui revient à dire que le polynôme a une racine double i.e. que son discriminant $q^2 - 4(2t + p)(t^2 + r)$ est nul. On se ramène ainsi à résoudre une équation de degré 3 en t pour laquelle on dispose des formules de Cardan. On trouve donc t puis a et b qui s'exprime comme des radicaux en fonction de p, q et r . L'équation devient alors $(x^2 + t) = (ax + b)^2$ que l'on résout sous la forme $x^2 + t = \pm(ax + b)$, équations de degré 2 pour laquelle on dispose des formules habituelles.

Plus généralement pour une équation de degré n , on cherche à savoir s'il est possible de l'exprimer à partir de ses coefficients par extraction de racines d'ordre fini, i.e. à l'aide de radicaux. Avant de présenter le point de vue de Galois, mentionnons les réflexions de Lagrange (1771) sur ces questions, qui furent certainement le point de départ du travail de Galois. Lagrange fait la remarque suivante, que l'on traduit en langage moderne : si x_1, \dots, x_n désignent les racines de l'équation de degré n à résoudre, dans un clôture algébrique, alors une quantité $f(x_1, \dots, x_n)$ fonction des racines est d'autant plus simple à calculer qu'elle sera symétrique en les x_i . L'idée de Lagrange est alors de former de telles quantité suffisamment

1. Il semblerait que Tartaglia ait communiqué la méthode à Cardan lui faisant promettre de la garder secrète, mais ce dernier la publia en 1545.

symétriques pour être calculée, mais assez complexes pour que les racines puissent se calculer à partir de ces quantités.

Voyons comment ces idées se mettent en place pour l'équation de degré 3. Notons j une racine cubique primitive de l'unité et considérons

$$u = x_1 + jx_2 + j^2x_3.$$

Regardons alors l'action de \mathfrak{S}_3 : l'orbite de u sous les 3-cycles est donnée

$$\begin{cases} u = x_1 + jx_2 + j^2x_3 \\ u' = x_2 + jx_3 + j^2x_1 \\ u'' = x_3 + jx_1 + j^2x_2 \end{cases}$$

et on note que ces trois quantités ont le même cube. En ce qui concerne les transpositions, elles échangent u, u', u'' avec

$$\begin{cases} v = x_1 + jx_3 + j^2x_2 \\ u' = x_3 + jx_2 + j^2x_1 \\ v'' = x_2 + jx_1 + j^2x_3 \end{cases}$$

qui ont aussi le même cube. Ainsi les quantités u^3v^3 et $u^3 + v^3$ sont symétriques et se calculent donc aisément ; on déterminera ensuite u^3 et v^3 en résolvant l'équation de degré 2 dont ils sont les racines. Enfin pour déterminer x_1, x_2, x_3 , on résout le système linéaire

$$\begin{cases} x_1 + x_2 + x_3 = \sigma_1 \\ x_1 + jx_2 + j^2x_3 = u \\ x_1 + jx_3 + j^2x_2 = v. \end{cases}$$

Pour l'équation de degré 4, on considère la quantité $u = x_1x_2 + x_3x_4$; l'orbite sous \mathfrak{S}_4 est alors de cardinal 3 :

$$\begin{cases} u = x_1x_2 + x_3x_4 \\ v = x_1x_3 + x_2x_4 \\ w = x_1x_4 + x_2x_3. \end{cases}$$

Ainsi les quantités $S = u + v + w$, $T = uv + vw + wu$ et $P = uvw$ sont symétriques et se déterminent aisément. On calcule alors u, v, w en résolvant l'équation

$$X^3 - SX^2 + TX - P = 0.$$

Ensuite pour $p_{12} = x_1x_2$ et $p_{34} = x_3x_4$, de la connaissance de leur produit et de leur somme, on les calcule via la résolution de l'équation de degré 2 associée. Puis pour $s_{12} = x_1 + x_2$ et $s_{34} = s_3 + s_4$, des équations linéaires

$$\begin{cases} s_{12} + s_{34} = \sigma_1 \\ p_{34}s_{12} + p_{12}s_{34} = \alpha \end{cases}$$

on en déduit s_{12} et s_{34} pourvu que l'on puisse calculer α , ce qui est bien le cas puisque α est symétrique. Enfin de la connaissance de s_{12} et p_{12} (resp. s_{34} et p_{34}) on en déduit x_1 et x_2 (resp. x_3 et x_4).

III.4.2. Groupe de Galois du polynôme $X^n - a$. — Si on veut interpréter les calculs précédents en termes de groupe de Galois, la première étape est de comprendre le groupe de Galois quand on prend une racine d'un nombre. Comme Cardan l'aurait dit s'il avait disposé des nombres complexes, il est pratique de disposer dans le corps de départ des racines n -ième de l'unité ce que l'on supposera à présent. En particulier, pour $a \in k^\times$, le corps de rupture $K = k[\alpha]$ sur k de $X^n - a$ sera aussi un corps de décomposition : $\alpha^n = a$. On note G le

groupe de Galois de K/k . Un élément $g \in G$ est par ailleurs caractérisé par son action sur α qui est nécessairement de la forme ζa pour ζ une racine n -ième de l'unité ; on définit ainsi une injection

$$i : G \hookrightarrow \mu_n(k) \simeq \mathbb{Z}/n\mathbb{Z}.$$

Lemme III.4.1. — *Le polynôme $X^n - a$ est irréductible si et seulement si a n'est pas une puissance d -ième dans k pour tout diviseur d de n distinct de 1.*

Démonstration. — Rappelons que P est irréductible si et seulement si $[K : k] = \deg P = n$ et donc si et seulement si le morphisme i ci-avant est un isomorphisme. Ainsi si P est irréductible et si $\alpha^d \in K$ alors comme $g(\alpha^d) = \alpha^d$, on en déduit que l'image de i est contenue dans $\mu_d(k)$ et donc $d = n$. Réciproquement si P n'était pas irréductible alors G est de cardinal un diviseur strict d de n : on a alors $g(\alpha)/\alpha \in \mu_d(k)$ et donc $g(\alpha^d) = \alpha^d$ pour tout $g \in G$ soit $\alpha^d \in k$. \square

Ainsi les groupes de Galois associés aux extensions $k[\alpha]/k$ avec $\alpha^n \in k$ et $\#\mu_n(k) = n$, sont cycliques. Le fait important est que la réciproque est vraie ce qui permet de caractériser de telles extensions en termes de théorie des groupes.

Théorème III.4.2. — (**Kummer**)

Soit K/k une extension galoisienne avec k contenant les racines n -ième de l'unité où $n = [K : k]$. Alors $\text{Gal}(K/k)$ est cyclique si et seulement s'il existe $a \in k$ tel que K soit le corps de rupture (et donc décomposition) de $X^n - a$.

Démonstration. — Il reste donc à prouver la réciproque. Notons g un générateur du groupe de Galois, il vérifie donc $g^n = \text{Id}$ que l'on voit comme une égalité dans $\mathcal{L}_k(K)$. Comme $X^n - 1$ est scindé sur k et à racines simples, on en déduit que l'endomorphisme g est diagonalisable ; de la formule $g(xy^{-1}) = g(x)g(y)^{-1}$, on en déduit que l'ensemble des valeurs propres est un sous-groupe de $\mu_n(k)$ qui est donc cyclique d'ordre d . Si on avait $d < n$ alors $g^d = \text{Id}$ ce qui n'est pas puisque g est un générateur du groupe de Galois lequel est de cardinal n . Ainsi g admet un vecteur propre x associée à une valeur propre ζ qui est une racine primitive n -ième de l'unité. Ainsi x admet n conjugués, à savoir les $\zeta^i x$ pour $i = 0, \dots, n - 1$ et donc $K = k[x]$ avec

$$\mu_{x,k}(X) = \prod_{i=0}^{n-1} (X - \zeta^i x) = X^n - a,$$

avec $a \in k$. \square

III.4.3. Extensions résolubles. — Pour simplifier nous supposons dans ce paragraphe que k est de caractéristique nulle.

Définition III.4.3. — Une extension K/k est dite *radicale* s'il existe une suite de corps

$$k = K_0 \subset K_1 \subset \dots \subset K_n = K$$

telle que $K_{i+1} = K[x_i]$ avec $x_i^{n_i} \in K_i$. Elle est dite *résoluble* s'il existe une extension finie L/K telle que L/k est radicale.

Remarque : si K/k est résoluble alors tout $x \in K$ s'exprime à l'aide de fractions rationnelles et d'extractions successives de radicaux à partir d'éléments de k .

Remarque : dans la définition de résoluble, si K est contenue dans une clôture algébrique Ω de k , on peut se ramener à L contenue dans Ω .

Lemme III.4.4. — Soient E/K et F/K deux extensions radicales (resp. résolubles) contenues dans une clôture algébrique Ω de K ; alors l'extension composée EF/K est radicale (resp. résoluble).

Démonstration. — Soient

$$K = E_0 \subset E_1 = E_0[x_1] \subset E_2 = E_1[x_2] \subset \cdots \subset E_n = E_{n-1}[x_n] = E$$

et

$$K = F_0 \subset F_1 = F_0[y_1] \subset \cdots \subset F_m = F_{m-1}[y_m] = F$$

telles que pour tout $i = 1, \dots, n$ (resp. $j = 1, \dots, m$) il existe une puissance de x_i (resp. y_j) qui appartienne à E_{i-1} (resp. F_{j-1}). Alors

$$K = E_0 \subset \cdots \subset E_n \subset EF_1 = E_n[y_1] \subset \cdots \subset EF_m = EF_{m-1}[y_m] = EF$$

réalise EF/K comme une extension radicale.

Si E/K et F/K sont résolubles, soient alors $E \subset L \subset \Omega$ et $F \subset L' \subset \Omega$ telles que L/K et L'/K sont radicales et LL'/K est radicale et contient EF/K qui est donc résoluble. \square

Lemme III.4.5. — Soit K/k une extension finie radicale (resp. résoluble) ; sa clôture galoisienne E/k dans une clôture algébrique Ω fixée est encore radicale (resp. résoluble).

Démonstration. — Par définition E est le sous-corps de Ω engendré par les $\sigma(K)$ pour σ décrivant les k -homomorphismes de K dans Ω . Comme K/k est radicale (resp. résoluble), l'image par σ d'une filtration $k = K_0 \subset \cdots \subset K_n = K$ comme dans la définition III.4.3, définit une filtration de $\sigma(K)$ montrant que $\sigma(K)/k$ est radicale (resp. résoluble). Le résultat découle alors du lemme précédent. \square

Théorème III.4.6. — Soit k un corps de caractéristique nulle ; une extension galoisienne K/k est résoluble si et seulement si son groupe de Galois est résoluble.

Démonstration. — a) Commençons par le sens direct en supposant que K/k est radicale et traitons le cas où k contient les racines de l'unité d'ordre $[K : k]$. On raisonne par récurrence sur $[K : k]$: on note $G = \text{Gal}(K/K_0)$ et $H = \text{Gal}(K : K_1)$. Comme $[K : K_1]$ divise $[K : K_0]$ alors K_1 contient les racines de l'unité d'ordre $[K : K_1]$ de sorte que K_1/K est galoisienne. On applique alors l'hypothèse de récurrence à l'extension radicale galoisienne K/K_1 de sorte que H est résoluble. De la suite exacte

$$1 \rightarrow H \rightarrow G \rightarrow G/H \rightarrow 1$$

et du fait que, d'après le théorème III.4.2, $G/H = \text{Gal}(K_1/K_0)$ est cyclique, on en déduit que G est résoluble.

b) Traitons à présent le cas où K/k est une extension résoluble quelconque et $K \subset E$ une extension finie telle que E/k est radicale. Soit Ω une clôture algébrique de E et soit L la clôture galoisienne de E/k dans Ω de sorte que d'après le lemme précédent, L/k est radicale galoisienne. Pour se ramener au cas précédent, on note $k' \subset \Omega$ l'extension de k engendrée par une racine primitive de l'unité d'ordre $[L : k]$. D'après le lemme précédent, pour $L' = k'L$, l'extension L'/k' vérifie les conditions de a) et donc $\text{Gal}(L'/k')$ est résoluble. Comme $\text{Gal}(K/k)$ est un quotient de $\text{Gal}(L'/k)$ il suffit de montrer que ce dernier est résoluble. De la suite exacte courte

$$1 \rightarrow \text{Gal}(L'/k') \rightarrow \text{Gal}(L'/k) \rightarrow \text{Gal}(k'/k) \rightarrow 1$$

et du fait que $\text{Gal}(k'/k)$ en tant que sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^\times$ pour $n = [L : k]$, est un groupe cyclique, il résulte que $\text{Gal}' L'/k$ est résoluble.

c) Étudions à présent la réciproque, i.e. on suppose que $\text{Gal}(K/k)$ est résoluble. On commence par le cas où k contient les racines de l'unité d'ordre $[K : k]$ et montrons, par récurrence sur $[K : k]$, que K/k est radicale. Soit alors H un sous-groupe distingué de $G = \text{Gal}(K/k)$ tel que G/H soit cyclique. Ainsi l'extension galoisienne K^H/k a un groupe de Galois H qui est cyclique et comme k contient les racines d'ordre $\#H$, d'après III.4.2, K^H/k est radicale. Par récurrence K/K^H est aussi radicale et donc K/k est radicale.

d) Dans le cas général, notons Ω une clôture algébrique de K et soit $k' \subset \Omega$ le corps engendré sur k par une racine de l'unité d'ordre $[K : k]$. Pour $K' = k'K$, le groupe de Galois $\text{Gal}(K'/k') \simeq \text{Gal}(K/k)$ est résoluble de sorte que d'après c), K'/k' est radicale. Comme k'/k est radicale alors K'/k est radicale et K/k est donc résoluble. \square

III.5. Calculer les groupes de Galois sur \mathbb{Q}

On se propose dans ce paragraphe de donner différentes techniques pour calculer le groupe de Galois d'une extension galoisienne K/\mathbb{Q} . On a vu que K pouvait se décrire comme le corps de décomposition sur \mathbb{Q} d'un polynôme $P(X) \in \mathbb{Q}[X]$. En considérant $a^n P(\frac{X}{a})$, on se ramène au cas où $P \in \mathbb{Z}[X]$ est unitaire et on notera x_1, \dots, x_n les racines de P dans $K = \mathbb{Q}(x_1, \dots, x_n)$.

III.5.1. quand on voit les racines. — La situation favorable, similaire à celle des extensions de Kummer où $P(X) = X^n - a$, est celle où les racines de P sont explicites et où l'action des éléments du groupe de Galois se décrit explicitement.

Considérons par exemple $K = \mathbb{Q}(i + \sqrt{2})$. Vérifions tout d'abord que K/\mathbb{Q} est bien galoisienne. Comme $-1/2$ n'est pas un carré dans \mathbb{Q} , $\mathbb{Q}(i)$ et $\mathbb{Q}(\sqrt{2})$ sont deux extensions quadratiques distinctes de \mathbb{Q} de sorte que leur composé $L = \mathbb{Q}(i, \sqrt{2})$ est une extension galoisienne de degré 4 de \mathbb{Q} . On peut décrire l'action du groupe de Galois $\text{Gal}(L/\mathbb{Q}) = \{Id, \tau_1, \tau_2, \tau_3\}$ sur i et $\sqrt{2}$:

$$\tau_1(i) = -i, \tau_1(\sqrt{2}) = \sqrt{2}, \tau_2(i) = i, \tau_2(\sqrt{2}) = -\sqrt{2}, \tau_3(i) = -i, \tau_3(\sqrt{2}) = -\sqrt{2}.$$

Seul Id laisse fixe l'élément $\alpha = i + \sqrt{2}$ de L . On en déduit que le corps engendré par α est L tout entier, c'est-à-dire $L = K$.

III.5.2. comme sous-groupe de \mathfrak{S}_n . — Le groupe de Galois $G = \text{Gal}(K/\mathbb{Q})$ permute les racines de P et, comme K est engendré sur \mathbb{Q} par les racines de P , tout élément de G est complètement déterminé par son action sur les racines de P . On peut ainsi considérer G comme un sous-groupe de \mathfrak{S}_n .

Proposition III.5.1. — *Le groupe G vu comme sous-groupe de \mathfrak{S}_n est contenu dans \mathcal{A}_n si et seulement si le discriminant $D(P)$ est un carré dans \mathbb{Q} .*

Démonstration. — Notons comme précédemment $\delta(P) = \prod_{1 \leq i < j \leq n} (x_i - x_j)$ de sorte que $D(P) = \delta(P)^2$. Par définition de la signature, cf. ??, pour tout $g \in G$ on a $g(\delta(P)) = \epsilon(g)\delta(P)$ où $\epsilon(g)$ est la signature de $g \in G$ vu comme une permutation de \mathfrak{S}_n . Ainsi $G \subset \mathcal{A}_n$ est équivalent à demander que $\delta(P) \in \mathbb{Q}$, d'où le résultat. \square

Exemple : le discriminant $P(X) = X^3 - 3X + 1$ est $-4(-3)^3 - 27 = 81 = 9^2$ et donc $G \subset \mathcal{A}_3$ de sorte que G n'étant pas trivial, $G = \mathcal{A}_3$.

Proposition III.5.2. — *On suppose que $P \in \mathbb{Q}[X]$ n'admet que des racines simples. Alors P est irréductible si et seulement si l'action de G sur les racines de P est transitive.*

Démonstration. — Dans le sens direct, pour x_i et x_j deux racines de P , par unicité du corps de rupture il existe un \mathbb{Q} -isomorphisme $\sigma : \mathbb{Q}[x_i] \simeq \mathbb{Q}[x_j]$ tel que $\sigma(x_i) = x_j$. D'après ??, cet isomorphisme se prolonge en un \mathbb{Q} -isomorphisme $K \simeq K$, i.e. il existe $g \in G$ tel que $g(x_i) = x_j$.

Réciproquement soit $Q = \mu_{x_1, \mathbb{Q}}$ un facteur irréductible de P annihilant x_1 . Pour $1 < i \leq n$, il existe $g \in G$ tel que $g(x_1) = x_i$ de sorte que $Q(x_i) = 0$ et donc $Q|P$ possède les mêmes racines que P ce qui prouve, les racines étant simples, que P est irréductible. \square

Remarque : lorsque P est irréductible, comme K contient un corps de rupture $\mathbb{Q}[x_i]$, le cardinal de G est divisible $\deg P = [\mathbb{Q}[x_i] : \mathbb{Q}]$.

Corollaire III.5.3. — *Si P est irréductible de degré p premier avec exactement deux racines non réelles alors $G \simeq \mathfrak{S}_p$.*

Démonstration. — Comme p divise $\sharp G$ et que les seuls éléments d'ordre p de \mathfrak{S}_p sont les p -cycles, on en déduit que G contient un p -cycle. La conjugaison complexe définit en outre une transposition dans G . On conclut alors en utilisant que \mathfrak{S}_p est engendré par un p -cycle et une transposition quelconques. \square

Proposition III.5.4. — *On suppose que P n'admet que des racines simples et que les orbites de l'action de G sur les racines de P sont de cardinal m_1, \dots, m_r . Alors P se factorise sous la forme $P = P_1 \cdots P_r$ avec P_i irréductible de degré m_i .*

Démonstration. — Pour une telle orbite \mathcal{O} on note $P_{\mathcal{O}} = \prod_{x_i \in \mathcal{O}} (X - x_i)$; comme $g(P_{\mathcal{O}}) = P_{\mathcal{O}}$ pour tout $g \in G$ on en déduit que $P_{\mathcal{O}} \in \mathbb{Q}[X]$. Soit alors Q un facteur irréductible de $P_{\mathcal{O}}$; les racines de Q forment alors un sous-ensemble de \mathcal{O} stable sous l'action de G et donc $Q = P_{\mathcal{O}}$. \square

III.5.3. par spécialisation. — Soit $P \in \mathbb{Z}[X]$ unitaire et K/\mathbb{Q} le corps de décomposition de P sur \mathbb{Q} : $K = \mathbb{Q}(x_1, \dots, x_n)$ où x_1, \dots, x_n sont les racines de P . On note

$$A = \mathbb{Z}[x_1, \dots, x_n].$$

Remarque : avec les notions du §??, les x_i sont des entiers et A est donc un sous-anneau de l'anneau des entiers \mathcal{O}_K de K . En particulier comme le corps des fractions de A est K , \mathcal{O}_K est un A -module de type fini.

Lemme III.5.5. — *L'anneau $\bar{A} = A/pA$ est non nul.*

Démonstration. — Dans le cas contraire il existerait $a \in A$ tel que $1 = pa$. En prenant la norme $N_{\mathbb{Q}[a]/\mathbb{Q}}$ au sens du §?? i.e. $N(z) = \prod_{i=1}^d \sigma_i(z)$ où $\sigma_1, \dots, \sigma_d$ sont les \mathbb{Q} -morphisms de $\mathbb{Q}[a]$ dans \mathbb{C} , on aurait

$$1 = N(pa) = p^d N(a) \text{ avec } N(a) \in \mathbb{Z}$$

car a est entier, ce qui est absurde. \square

Remarque : comme \mathcal{O}_K est un A -module fini, le discriminant D de \mathcal{O}_K sur A est bien défini et pour p ne divisant pas D , les localisés en p de A et \mathcal{O}_K sont alors égaux et donc en particulier pour ces premiers $A/pA \simeq \mathcal{O}_K/p\mathcal{O}_K$: moralement quitte à écarter un ensemble fini de nombre premiers, cela revient au même de travailler avec \mathcal{O}_K ou avec A , cf. ??.

Soit $\overline{\mathfrak{P}}$ un idéal maximal de \overline{A} et \mathfrak{P} son image inverse dans A : on a $\mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$. Le corps $\kappa = \overline{A}/\overline{\mathfrak{P}}$ est un corps de décomposition sur \mathbb{F}_p de \overline{P} et donc une extension finie de \mathbb{F}_p .

Définition III.5.6. — Comme le groupe de Galois $\text{Gal}(K/\mathbb{Q})$ permute les x_i , il stabilise A et on note $D_{\mathfrak{P}}$ son sous-groupe qui stabilise \mathfrak{P} : $D_{\mathfrak{P}}$ est appelé *le groupe de décomposition de \mathfrak{P}* .

Remarque : en fait le groupe de décomposition $D_{\mathfrak{P}}$ dépend peu de \mathfrak{P} mais plutôt de p . En effet si \mathfrak{Q} en est un autre alors il existe $g \in \text{Gal}(K/\mathbb{Q})$ tel que $\mathfrak{Q} = g(\mathfrak{P})$: dans le cas contraire on aurait $\mathfrak{Q} + g(\mathfrak{P}) = A$ pour tout $g \in \text{Gal}(K/\mathbb{Q})$ et d'après le lemme chinois, on aurait $x \in A$ tel que $x \equiv 1 \pmod{g(\mathfrak{P})}$ pour tout $g \in \text{Gal}(K/\mathbb{Q})$ et $x \equiv 0 \pmod{\mathfrak{Q}}$. Or la norme $\prod_{g \in \text{Gal}(K/\mathbb{Q})} g(x) \in p\mathbb{Z} = \mathfrak{Q} \cap \mathbb{Z} = \mathfrak{P} \cap \mathbb{Z}$ et donc appartient également à \mathfrak{P} et donc un des facteurs $g(x) \in \mathfrak{P}$ soit $x \equiv 0 \pmod{g^{-1}(\mathfrak{P})}$, contradiction.

On en déduit alors que

$$D_{\mathfrak{Q}} = gD_{\mathfrak{P}}g^{-1}$$

en particulier si $\text{Gal}(K/\mathbb{Q})$ est abélien alors $D_{\mathfrak{Q}} = D_{\mathfrak{P}}$ et on le note D_p .

Théorème III.5.7. — *L'action de $\text{Gal}(K/\mathbb{Q})$ sur A induit une action de $D_{\mathfrak{P}}$ sur κ et le morphisme induit*

$$D_{\mathfrak{P}} \longrightarrow \text{Gal}(\kappa/\mathbb{F}_p)$$

est surjectif. Si \overline{P} est à racines simples dans $\overline{\mathbb{F}_p}$ alors la flèche précédent est aussi injective.

Démonstration. — Soit x un générateur de κ/\mathbb{F}_p de sorte qu'un élément σ_0 de $\text{Gal}(\kappa/\mathbb{F}_p)$ est déterminé par $\sigma_0(x)$. Par construction $g \in \text{Gal}(K/\mathbb{Q})$ induit une flèche surjective $A \rightarrow A \rightarrow A/g^{-1}(\mathfrak{P})$ et donc un isomorphisme

$$A/g^{-1}(\mathfrak{P}) \simeq A/\mathfrak{P},$$

avec $g^{-1}(\mathfrak{P}) = \mathfrak{P}$ si et seulement si $g \in D_{\mathfrak{P}}$. Notons $\mathfrak{Q}_1, \dots, \mathfrak{Q}_r$ les différents idéaux de la forme $g^{-1}(\mathfrak{P})$ pour $g \notin D_{\mathfrak{P}}$. Comme les $\mathfrak{Q}_0, \mathfrak{Q}_1, \dots, \mathfrak{Q}_r$ sont distincts deux à deux et maximaux, on a $\mathfrak{Q}_i + \mathfrak{Q}_j = A$ pour tous $i \neq j$. D'après le lemme chinois on peut donc trouver $z \in A$ tel que :

$$z \equiv x \pmod{\mathfrak{P}_0} \text{ et } z \equiv 0 \pmod{g^{-1}(\mathfrak{P})} \text{ pour } g \notin D_{\mathfrak{P}}.$$

On a alors $g(z) \in \mathfrak{P}$ pour $g \notin D_{\mathfrak{P}}$ et le polynôme

$$\prod_{g \in \text{Gal}(K/\mathbb{Q})} (X - g(z)) \in \mathbb{Z}[X]$$

a son image dans $\kappa[X]$ de la forme

$$\prod_{g \in D_{\mathfrak{P}}} (X - \overline{g(z)}) \prod_{g \notin D_{\mathfrak{P}}} X.$$

Or $x = \overline{z}$ est racine de ce polynôme de sorte que

$$\mu_{x, \mathbb{F}_p}(X) = \prod_{g \in \text{Gal}(\kappa/\mathbb{F}_p)} (X - \sigma(x)) \text{ divise } \prod_{g \in D_{\mathfrak{P}}} (X - \overline{g(z)})$$

et donc il existe $g \in D_{\mathfrak{P}}$ tel que $\sigma_0(x) = \overline{g(z)}$, ce qui finit de prouver la surjectivité.

Dans le cas où les racines de \bar{P} sont simples alors l'application qui à une racine de P associe sa réduction modulo p définit une bijection entre les racines de P et celles de \bar{P} . L'injectivité découle alors du diagramme commutatif suivant :

$$\begin{array}{ccccc} D_{\mathfrak{F}} & \longrightarrow & \text{Gal}(\kappa/\mathbb{F}_p) & \hookrightarrow & \mathfrak{S}(\{\bar{x}_1, \dots, \bar{x}_n\}) \\ \downarrow & & & & \nearrow \\ \text{Gal}(K/\mathbb{Q}) & \hookrightarrow & \mathfrak{S}(\{x_1, \dots, x_n\}) & & \end{array}$$

□

Remarque : ainsi si on a une permutation des racines de \bar{P} alors il existe une permutation des racines de P du même type. En particulier si \bar{P} est irréductible alors il existe un cycle de longueur n dans $\text{Gal}(K/\mathbb{Q})$.

Remarque : notons que \bar{P} a des racines simples si et seulement si p ne divise pas son discriminant, autrement dit pour tout nombre premier p sauf un nombre fini, on peut définir la classe de conjugaison $(p, K/\mathbb{Q})$ du frobenius de $\text{Gal}(\kappa/\mathbb{F}_p)$ dans $\text{Gal}(K/\mathbb{Q})$ qui, d'après ce qui précède, ne dépend que du premier p considéré.

Théorème III.5.8. — (Cebotarev)

Soit C une classe de conjugaison dans $\text{Gal}(K/\mathbb{Q})$ alors la limite de la suite

$$n \mapsto \frac{\#\{p \text{ premier tels que } (p, K/\mathbb{Q}) = C \text{ et } p \leq n\}}{\#\{p \text{ premiers tels que } p \leq n\}}$$

existe et vaut $\frac{\#C}{\#G}$.

Remarque : la preuve de ce résultat repose sur des techniques finies de fonctions holomorphes qui nous entraîneraient trop loin d'exposer ici. Moralement ce résultat affirme qu'essayer de calculer le groupe de Galois $\text{Gal}(K/\mathbb{Q})$ par spécialisation nous donnera rapidement la structure de cycles des différents éléments de $\text{Gal}(K/\mathbb{Q})$; en revanche, sauf en petites dimensions ou pour de gros sous-groupes de \mathfrak{S}_n , il est difficile de recoller ces informations locales pour reconstruire tout le groupe de Galois.

Remarque : $(p, K/\mathbb{Q})$ trivial est équivalent à demander que \bar{P} soit scindé. Ainsi le théorème de Cebotarev nous dit qu'il existe une infinité de p tels que \bar{P} est scindé; évidemment ce sont les mauvais p du point de vue du calcul du groupe de Galois.

III.5.4. Résolvantes. —

Définition III.5.9. — Soient $F(X_1, \dots, X_n) \in \mathbb{Z}[X_1, \dots, X_n]$, un sous-groupe $G \subset \mathfrak{S}_n$ et un polynôme unitaire $P(X) \in \mathbb{Z}[X]$ dont on note $\alpha_1, \dots, \alpha_n$ les racines. On note alors

$$H = \text{Stab}_G(F) = \left\{ \sigma \in G : F(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = F(X_1, \dots, X_n) \right\}$$

le stabilisateur de F dans G . Alors la résolvante $\text{Res}_G(F, P)$ est défini par

$$\text{Res}_G(F, P)(X) = \prod_{\sigma \in G/H} (X - F(\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)})).$$

Remarque : dans la définition précédente σ décrit une ensemble fixé de représentants quelconque de G/H ; le résultat n'en dépend pas puisque $H = \text{Stab}_G(F)$.

Proposition III.5.10. — Si le groupe de Galois $\text{Gal}(P)$ de P est conjugué dans G à un sous-groupe de $H = \text{Stab}_G(F)$ alors $\text{Res}_G(F, P)$ a une racine dans \mathbb{Z} . En outre si $\text{Res}_G(F, P)$ a une racine simple dans \mathbb{Z} alors $\text{Gal}(P)$ est conjugué à un sous-groupe de H .

Démonstration. — Supposons que $\text{Gal}(P) = \sigma^{-1}N\sigma$ avec N un sous-groupe de H et $\sigma \in G$. Soient $\tau = \sigma^{-1}\nu\sigma \in \text{Gal}(P)$ et $F(\alpha_{\sigma^{-1}(1)}, \dots, \alpha_{\sigma^{-1}(n)})$ une des racines de $\text{Res}_G(F, P)$. On a alors :

$$\begin{aligned} \tau F(\alpha_{\sigma^{-1}(1)}, \dots, \alpha_{\sigma^{-1}(n)}) &= \sigma^{-1}\nu\sigma F(\alpha_{\sigma^{-1}(1)}, \dots, \alpha_{\sigma^{-1}(n)}) \\ &= \sigma^{-1}\nu F(\alpha_1, \dots, \alpha_n) \\ &= \sigma^{-1}F(\alpha_{\nu(1)}, \dots, \alpha_{\nu(n)}) \\ &= \sigma^{-1}F(\alpha_1, \dots, \alpha_n) \\ &= F(\alpha_{\sigma^{-1}(1)}, \dots, \alpha_{\sigma^{-1}(n)}). \end{aligned}$$

Ainsi comme $F(\alpha_{\sigma^{-1}(1)}, \dots, \alpha_{\sigma^{-1}(n)})$ est fixe par $\text{Gal}(P)$, elle appartient à \mathbb{Q} et à \mathbb{Z} car les α_i sont des entiers algébriques au sens de la définition ??.

Réciproquement si $F(\alpha_{\sigma^{-1}(1)}, \dots, \alpha_{\sigma^{-1}(n)}) \in \mathbb{Z}$ est une racine simple alors elle est fixe par $\text{Gal}(P)$ et donc pour tout $\tau \in \text{Gal}(P)$

$$\tau F(\alpha_{\sigma^{-1}(1)}, \dots, \alpha_{\sigma^{-1}(n)}) = F(\alpha_{\sigma^{-1}(1)}, \dots, \alpha_{\sigma^{-1}(n)}).$$

Notons que comme $\text{Stab}_G(\sigma^{-1}F) = \sigma^{-1}\text{Stab}_G(F)\sigma$ alors $\text{Res}_G(\sigma^{-1}F, P) = \text{Res}_G(F, P)$ et donc, comme $F(\alpha_{\sigma^{-1}(1)}, \dots, \alpha_{\sigma^{-1}(n)})$ est une racine simple, alors $\tau \in \text{Stab}_G(\sigma^{-1}F) = \sigma^{-1}H\sigma$ et $\text{Gal}(P) \subset \sigma^{-1}H\sigma$. \square

Remarque : d'un point de vue pratique, on calcule des approximations assez précises des racines de P puis des $F(\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)})$ afin de savoir quand $\text{Res}_G(F, P)$ a une racine simple dans \mathbb{Z} .

Exemple : soit $F(X_1, \dots, X_n) = \prod_{i < j} (X_i - X_j)$ avec $G = \mathfrak{S}_n$. On vérifie que $H = \text{Stab}_G(F) = \mathcal{A}_n$ et

$$\text{Res}_G(F, P) = \left(X - \prod_{i < j} (\alpha_i - \alpha_j) \right) \left(X + \prod_{i < j} (\alpha_i - \alpha_j) \right) = X^2 - \text{Disc}(P).$$

Par hypothèse $P(X)$ est irréductible et donc $\text{Disc}(P) \neq 0$; ainsi $X^2 - \text{Disc}(P)$ a une racine simple dans \mathbb{Z} si et seulement si c'est un carré et on retrouve la condition de la proposition III.5.1.

Le principe pour $n \leq 31$, est de lister les sous-groupes transitifs de \mathfrak{S}_n et pour chacun d'entre eux de calculer un F qui le caractérise parmi ses sous-groupes, puis on calcule si la résultante a une racine dans \mathbb{Z} ou non.

III.5.5. Théorie de Galois inverse. — Plutôt que de calculer un groupe de Galois d'une extension galoisienne, on se propose de considérer le problème dans l'autre sens : étant donné un groupe essayer de construire une extension K/\mathbb{Q} dont le groupe de Galois est ce groupe. Dans la suite nous noterons $G = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ et il s'agit alors de déterminer si un groupe donné est un quotient de G .

Proposition III.5.11. — Tout groupe abélien fini est quotient de G .

Démonstration. — Rappelons que le groupe de Galois de l'extension cyclotomique est $(\mathbb{Z}/n\mathbb{Z})^\times$ et, comme tout quotient du groupe de Galois d'une extension galoisienne de \mathbb{Q} est un quotient de G , il suffit de montrer que tout groupe abélien fini est quotient de $(\mathbb{Z}/n\mathbb{Z})^\times$

pour un n convenable. Rappelons aussi que si n est de la forme $p_1 \cdots p_m$ où les p_i sont des nombres premiers distincts alors

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq \mathbb{Z}/(p_1 - 1)\mathbb{Z} \times \cdots \times \mathbb{Z}/(p_m - 1)\mathbb{Z}.$$

Ainsi si n_1, \dots, n_m sont des entiers divisant respectivement $p_1 - 1, \dots, p_m - 1$ alors $\prod_{i=1}^m \mathbb{Z}/n_i\mathbb{Z}$ est un quotient de $(\mathbb{Z}/n\mathbb{Z})^\times$.

Un groupe abélien fini H est un produit de groupe cyclique et donc de la forme $\prod_{i=1}^m \mathbb{Z}/n_i\mathbb{Z}$; on choisit alors, d'après le théorème de Dirichlet, des nombres premiers p_1, \dots, p_m distincts deux à deux tels que $n_i \equiv 1 \pmod{p_i}$ pour tout $i = 1, \dots, m$, de sorte que H est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^\times$. \square

Premiers exemples non commutatifs :

- \mathfrak{S}_3 est le groupe de Galois de $X^3 - 2$;
- D_4 est le groupe de Galois de $X^4 - 2$;
- \mathbb{H}_8 est le groupe de Galois de $\mathbb{Q}(\sqrt{(2 + \sqrt{2})(3 + \sqrt{6})})$.

Théorème III.5.12. — (Shafarevich)

Tout groupe fini résoluble est quotient de G .

Remarque : rappelons que d'après le théorème de Feit-Thompson, tout groupe d'ordre impair est résoluble. En outre on conjecture que tout groupe fini est quotient de G . Hilbert a démontré que les groupes alternés sont des quotients de G mais, par exemple on ne sait pas si les groupes de la forme $GL_n(\mathbb{F}_q)$ le sont.

III.5.6. Cas d'un corps de fonctions en une variable. — Nous nous intéressons au groupe de galois de l'extension $k(t)/k$ où t est une indéterminée.

Proposition III.5.13. — *Soit $F(t) = \frac{P(t)}{Q(t)} \in k(t)$ une fraction rationnelle non constante écrite sous forme irréductible, alors*

- 1) F est transcendant sur k ;
- 2) le polynôme $P(X) - FQ(X) \in k(F)[X]$ est irréductible;
- 3) $k(t)/k(F)$ est une extension finie de degré $\max(\deg P, \deg Q)$.

Démonstration. — 1) Si F était algébrique il serait solution d'une équation $X^n + a_1X^{n-1} + \cdots + a_n = 0$ ce qui donnerait

$$P(t)^n + a_1P(t)^{n-1}Q(t) + \cdots + a_nQ(t)^n = 0$$

de sorte que P (resp. Q) diviserait $a_nQ(t)^n$ (resp. $P(t)^n$) soit comme $P \wedge Q = 1$ par hypothèse, P (resp. Q) est une constante et F serait une constante ce qui est exclu par hypothèse.

2-3) Le polynôme $P(X) - FQ(X) \in k(F)[X]$ admet $t \in k(t)$ pour racine et a pour degré $d = \max(\deg P, \deg Q)$. Ainsi 3) découle de 2). Rappelons que $k[X, Y]$ est un anneau factoriel et que comme le contenu de $P(X) - YQ(X) \in k[X][Y]$ est égal à 1 alors d'après le théorème de Gauss, en tant que polynôme de degré 1 en Y , le polynôme $P(X) - YQ(X)$ est irréductible dans $k[X, Y]$ et $k(Y)[X]$. Or d'après 1) l'application $Y \mapsto F$ induit un isomorphisme $k(Y)[X] \simeq k(F)[X]$ qui envoie $P(X) - YQ(X)$ sur $P(X) - FQ(X)$ ce qui finit de prouver 2). \square

Exemple : soient σ et τ les \mathbb{C} -automorphismes de $\mathbb{C}(t)$ définis par

$$\sigma(F(t)) = F(\zeta_n t), \quad \text{et} \quad \tau(F(t)) = F(t^{-1}),$$

où $\zeta_n = e^{2i\pi/n}$. Ils sont respectivement d'ordre n et 2 avec $\tau \circ \sigma \circ \tau^{-1} = \sigma^{-1}$ de sorte que σ et τ engendrent un groupe G isomorphe au groupe diédral D_n . On note $k = \mathbb{C}(t)^G$ de sorte que $\mathbb{C}(t)/k$ est une extension galoisienne de groupe de Galois D_n . Posons

$$F(t) := t^n + t^{-n} \in \mathbb{C}(t),$$

avec $\mathbb{C}(F) \subset k$, l'égalité découlant du point 3) de la proposition précédente.

Remarque : l'extension $k(t)/k$ est de degré infini de sorte que la théorie de Galois telle qu'exposée précédemment ne s'applique pas. Notons tout de même $\text{Gal}(k(t)/k)$ le groupe des k -automorphismes de $k(t)$.

Proposition III.5.14. — 1) Pour tout $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, k)$, la fonction $\phi_g : k(t) \rightarrow k(t)$ définie par

$$F(t) \mapsto F\left(\frac{at+b}{ct+d}\right)$$

est un élément de $\text{Gal}(k(t)/k)$.

2) L'application $g \mapsto \phi_{g^{-1}}$ définit un isomorphisme

$$PGL(2, k) \simeq \text{Gal}(k(t)/k).$$

Démonstration. — 1) L'application $\phi'_g : k[t] \rightarrow k(t)$ est injective car $F(t) = \frac{at+b}{ct+d}$ est transcendant sur k d'après la proposition précédente. Ainsi ϕ'_g se prolonge en un morphisme injectif de $k(t)$ d'image $k(F)$ qui d'après la proposition précédente est un sous-corps de $k(t)$ de degré 1, i.e. $k(F) = k(t)$.

2) La propriété de morphisme découle de l'expression

$$\frac{a \frac{a't+b'}{c't+d'} + b}{c \frac{a't+b'}{c't+d'}} = \frac{(aa' + bc')t + (ab' + bd')}{(ca' + dc')t + (cb' + dd')}$$

et du calcul du produit matriciel

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}.$$

Pour la surjectivité, soit $\sigma \in \text{Gal}(k(t)/k)$; pour tout $F \in k(t)$ on a alors $\sigma F(t) = F(\alpha(t))$ et en particulier, comme $k(\sigma(t)) = k(t)$, d'après la proposition précédente, $\sigma(t) = \frac{P(t)}{Q(t)}$ avec $\max(\deg P, \deg Q) = 1$. Ainsi $\sigma(t)$ est de la forme $\frac{at+b}{ct+d}$ i.e. $\sigma = \phi_g$ pour $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. En ce qui concerne l'injectivité, l'égalité $\frac{at+b}{ct+d} = t$ est équivalente à $b = c = 0$ et $a = d$ d'où le résultat. \square

Remarque : en ce qui concerne le problème de Galois inverse, la situation est d'autant plus simple que, pour la plupart des corps k , les sous-groupes finis de $PGL(2, k)$ sont connus. Par exemple pour $k = \mathbb{C}$, les sous-groupes finis sont :

- les groupes cycliques $\mathbb{Z}/n\mathbb{Z}$ pour $n \geq 1$;
- les groupes diédraux D_n de cardinal $2n$ pour $n \geq 2$;
- le groupe \mathcal{A}_4 ;

- le groupe \mathcal{A}_5 ;
- le groupe \mathfrak{S}_5 .

En outre deux tels sous-groupes abstraitement isomorphes sont en fait conjugués dans $PGL(2, \mathbb{C})$. Pour les familles infinies nous avons déjà donné une description explicite d'une extension associée. Pour les autres, en utilisant les polyèdres réguliers qui leur sont associés, on construit des extensions explicites : ainsi pour \mathfrak{S}_4 on obtient $\mathbb{C}(\frac{(t^8+14t^4+1)^3}{t^4(t^4-1)^4})$. Le fait que l'extension soit monogène est même plus générale comme l'affirme le théorème suivant.

Théorème III.5.15. — *(de Lüroth)* Soit K/k une extension intermédiaire de $k(t)/k$; il existe alors $F \in k(t)$ tel que $K = k(F) \simeq k(t)$.

Démonstration. — On suppose que $K \neq k$ et soit $F \in K - k$. Comme $k(F) \subset K$ et que t est algébrique sur $k(t)$ d'après la proposition III.5.13, on en déduit que $k(t)/K$ est algébrique et que K/k n'est pas de degré fini. Soit $P(X)$ le polynôme minimal de t sur K

$$X^n + F_1(t)X^{n-1} + \dots + F_n(t).$$

On écrit chaque F_i sous forme irréductible $P_i(t)/Q_i(t)$; en multipliant P par le ppcm des Q_i , on obtient un polynôme annulateur de t

$$P(X, t) = a_0(t)X^n + \dots + a_n(t) \in k[t][X].$$

Comme t n'est pas algébrique sur k , l'un des $a_i(t)/a_0(t)$ n'est pas constant et posons

$$A(X, T) = a_0(T)a_i(X) - a_i(T)a_0(X) \in K.$$

Comme $A(X, t) = 0$ on en déduit que $P(X, t)$ divise $A(X, t)$ dans $k(t)[X]$ et comme le contenu de $A(X, t)$ dans $k[t]$ est égal à 1 alors il existe $B(X, t) \in k[X, t]$ tel que

$$A(X, t) = P(X, t)B(X, t) \text{ dans } k[t, X].$$

Par ailleurs $\deg_t a_i$ et $\deg_t a_0$ sont inférieurs ou égaux à $\deg_t P$ et comme $\deg_t (a_0(t)a_i(X) - a_i(t)a_0(X)) = \deg_t B + \deg_t F$, on en déduit que $\deg_t B = 0$ et donc $B(X, t) = B(X)$. Or $a_0(t)a_i(X) - a_i(t)a_0(t)$ est symétrique en t et X et est donc aussi divisible par $B(t)$. Ainsi $B(t)$ divise $B(X)P(X, t)$ et comme $B(t) \wedge B(X) = 1$, on en déduit que $B(t)$ divise $P(X, t)$ ce qui impose que $B(t)$ est un polynôme constant. Ainsi $P(X, t)$ est aussi symétrique ne X et t et donc $\deg_X P = \deg_t P = n$.

On a ainsi $k(\frac{a_i}{a_0}) \subset K$ avec $[k(t) : k(\frac{a_i}{a_0})] = n = [k(t) : K]$ de sorte que $K = k(\frac{a_i}{a_0})$, d'où le résultat. \square

Remarque : signalons que le théorème de Lüroth en vrai en dimension 2 pour $\mathbb{C}(t_1, t_2)$ mais ne l'est plus en dimension 3.