La loi de réciprocité quadratique

Daniel PERRIN

Ce texte reprend le thème d'un TER (Travail d'Étude et de Recherche de maîtrise) plusieurs fois posé à Orsay. Je me suis notamment appuyé sur les rédactions de Pierre Jalinière, Lucile Morelle et Marie-Noëlle Guy que je remercie.

On renvoie à [DP] pour le b.a. ba de théorie des anneaux et des corps utilisé ici (notions d'extension, de degré, corps de décomposition, etc.)

1 Introduction

On connaît les carrés de $\mathbf{R}$, ce sont les nombres positifs, et ceux de $\mathbf{C}$, ce sont tous les nombres complexes, sans restriction. Cette différence est liée à une autre : le corps $\mathbf{R}$ est ordonné, tandis qu'il n'existe pas d'ordre raisonnable sur $\mathbf{C}$ (i.e. compatible avec les opérations). En effet, si $\mathbf{C}$ était muni d'un ordre total, i serait donc soit positif, soit négatif. Mais dans les deux cas, à cause de la fameuse règle des amis (ou ennemis) de mes amis (ou ennemis), son carré, qui est -1, serait positif, ce qui est absurde. Plus généralement, un théorème d'Artin indique que, pour qu'un corps soit ordonnable, il faut et il suffit que -1 ne soit pas somme de carrés, ce qui nécessite de savoir qui est un carré et qui ne l'est pas.

La recherche des carrés d'un corps commutatif k est importante dans de nombreuses autres questions d'algèbre. Dans la théorie des formes quadratiques, le discriminant (essentiel pour la classification) est défini modulo les carrés. Cette recherche intervient aussi souvent dans la théorie des groupes classiques par le biais du groupe quotient k^*/k^{*2}. En effet, il apparaît dans l'étude du groupe linéaire comme quotient de $PGL(2,k)/PSL(2,k)$. Dans les groupes orthogonaux, si $\Omega(q)$ est le groupe des commutateurs de $O^+(q)$, on a $O^+(q)/\Omega(q) \simeq k^*/k^{*2}$ et $-\mathrm{Id}$ est dans Ω si et seulement si le discriminant de q est un carré.

Dans le cas où le corps k est un corps fini $\mathbf{F}_q$, il s'ajoute aux considérations précédentes des motivations arithmétiques. Par exemple, si l'on cherche à résoudre l'équation diophantienne $ax^2 + by^2 = c$ $(a, b, c \in \mathbf{Z})$, c'est-à-dire à chercher ses solutions entières, on va obtenir des conditions nécessaires

grâce à des arguments de congruences. Si l'on réduit l'équation modulo a par exemple, on trouve $by^2 \equiv c \pmod{a}$ et, pourvu qu'on puisse diviser par b, le quotient c/b devra être un carré modulo a. En particulier, si un nombre premier p est de la forme $x^2 + dy^2$, on voit que $-d$ est un carré modulo p et cela fournit une condition nécessaire. Ce thème est d'ailleurs l'objet d'un autre TER. Ce type de problèmes est très lié aux formes quadratiques sur $\mathbf{Z}$ ou $\mathbf{Q}$ (voir dans [Serre] le paragraphe sur le symbole de Hilbert). La question à laquelle ce texte permettra de répondre est par exemple : le nombre 21467 est-il un carré [1] modulo 65537 ?

2 Généralités sur les carrés de $\mathbf{F}_q$

On rappelle ici quelques résultats bien connus que le lecteur trouvera aussi dans [DP] ou [Serre]. On désigne par p un nombre premier, par q une puissance de p, $q = p^n$ et par $\mathbf{F}_q$ le corps fini à q éléments. On rappelle que le groupe multiplicatif $\mathbf{F}_q^*$ est cyclique d'ordre $q-1$ (voir *loc. cit.*). On rappelle aussi que le groupe [2] de Galois de $\mathbf{F}_{q^d}$ sur $\mathbf{F}_q$ est cyclique d'ordre d, engendré par l'homomorphisme de Frobenius F défini par $F(x) = x^q$, voir 3.5.

2.1 Le cas $p = 2$

Dans ce cas l'application $x \mapsto x^2$ est un homomorphisme de corps (c'est un cas particulier de Frobenius), donc injectif, donc surjectif puisque $\mathbf{F}_q$ est fini, et tout élément de $\mathbf{F}_q$ est un carré, ce qui clôt la recherche.

On suppose désormais que p est impair

2.2 La première suite exacte

Le résultat suivant est évident :

2.1 Proposition. *On a la suite exacte :*

$$1 \to \{\pm 1\} \to \mathbf{F}_q^* \xrightarrow{\gamma} \mathbf{F}_q^{*2} \to 1$$

où γ désigne l'élévation au carré $x \mapsto x^2$.

Le groupe $\mathbf{F}_q^{*2}$ est de cardinal $\dfrac{q-1}{2}$ et il y a $\dfrac{q+1}{2}$ carrés dans $\mathbf{F}_q$.

La denière assertion tient compte du fait que 0 aussi est un carré.

1. La réponse est non.

2. Pour des rudiments de théorie de Galois, voir l'Annexe 1 ci-dessous. Pour plus de détails, voir [S].

2.3 La deuxième suite exacte

2.2 Proposition. *On a la suite exacte :*

$$1 \to \mathbf{F}_q^{*2} \to \mathbf{F}_q^* \xrightarrow{\theta} \{\pm 1\} \to 1$$

où l'on a posé $\theta(x) = x^{\frac{q-1}{2}}$.

En particulier, si x *est dans* $\mathbf{F}_q^*$, x *est un carré si et seulement si on a* $x^{\frac{q-1}{2}} = 1$.

Démonstration. Comme $\mathbf{F}_q^*$ est de cardinal $q-1$, on a, pour tout $x \in \mathbf{F}_q^*$, $x^{q-1} = 1$, donc si $y = \theta(x)$, $y^2 = 1$, ce qui montre que θ est à valeurs dans ± 1. Il est clair que θ est un homomorphisme et que $\mathbf{F}_q^{*2}$ est contenu dans $\operatorname{Ker}\theta$. En fait, il y a égalité. En effet, $\operatorname{Ker}\theta$ est l'ensemble des racines du polynôme $X^{\frac{q-1}{2}} - 1$, il est donc de cardinal $\leq \dfrac{q-1}{2}$ et l'on a vu qu'il y avait exactement ce nombre de carrés non nuls. On en déduit que θ est surjectif pour une raison de cardinal.

2.4 Le nombre -1 est-il un carré de $\mathbf{F}_q$?

Le résultat précédent donne aussitôt :

2.3 Corollaire. *Le nombre* -1 *est un carré de* $\mathbf{F}_q$ *si et seulement si on a* $q \equiv 1 \pmod 4$.

2.5 Le nombre 2 est-il un carré de $\mathbf{F}_q$?

Dans ce cas, le théorème est le suivant :

2.4 Théorème. *Le nombre* 2 *est un carré de* $\mathbf{F}_q$ *si est seulement si on a* $q \equiv \pm 1 \pmod 8$.

Démonstration. Le point de départ est une remarque un peu subtile : on a $2 = 1 + 1$. Cela implique, par Pythagore, que la diagonale d'un carré de côté 1 vaut $\sqrt{2}$. Dans $\mathbf{C}$ on voit ainsi qu'on a $\sqrt{2} = e^{i\pi/4} + e^{-i\pi/4} = \zeta + \zeta^{-1}$ où $\zeta = e^{i\pi/4}$ est une racine primitive huitième de 1. En fait, cette situation est générale :

2.5 Lemme. *Soit* k *un corps de caractéristique différente de* 2 *et* ζ *une racine primitive huitième de* 1 *(habitant dans une extension de* k *éventuellement). Alors on a* $(\zeta + \zeta^{-1})^2 = 2$.

Démonstration. En effet, on a $(\zeta+\zeta^{-1})^2 = \zeta^2+\zeta^{-2}+2$. Or, ζ vérifie $\zeta^8 = 1$ mais $\zeta^4 \neq 1$, donc $\zeta^4+1=0$, soit encore $\zeta^2+\zeta^{-2}=0$ et on a le résultat.

On voit que 2 est un carré dans k si et seulement si $\zeta+\zeta^{-1}$ est dans k.

Dans le cas de $\mathbf{F}_q$, on note déjà que ζ est dans $\mathbf{F}_{q^2}$, corps à q^2 éléments. En effet, comme q est impair, $q^2-1=(q-1)(q+1)$ est produit de deux nombres pairs consécutifs, donc est multiple de 8. Comme $\mathbf{F}_{q^2}^*$ est cyclique, il en résulte qu'il contient un élément d'ordre 8, donc une racine primitive huitième de 1, qu'on note ζ.

On peut alors finir de prouver 2.4. On note F l'homomorphisme de Frobenius $F(x)=x^q$.

• Supposons $q \equiv \pm 1 \pmod 8$. On a $F(\zeta+\zeta^{-1}) = \zeta^q+\zeta^{-q} = \zeta^1+\zeta^{-1}$. On voit que $\zeta+\zeta^{-1}$ est fixé par F, donc qu'il est dans $\mathbf{F}_q$ en vertu de 4.12, donc que 2 est un carré.

• Supposons $q \equiv \pm 3 \pmod 8$. On a $F(\zeta+\zeta^{-1}) = \zeta^q+\zeta^{-q} = \zeta^3+\zeta^{-3}$. Si 2 était un carré, $\zeta+\zeta^{-1}$ serait dans $\mathbf{F}_q$ donc fixé par le Frobenius et on aurait donc $\zeta^3+\zeta^{-3} = \zeta+\zeta^{-1}$, donc $\zeta^4+\zeta^{-2} = \zeta^2+1$ et comme on a $\zeta^4=-1$ et $\zeta^{-2}=-\zeta^2$, on aurait $\zeta^2+1=0$ et ζ serait racine quatrième de l'unité.

2.6 Le cas $q=p$, symbole de Legendre

On suppose désormais qu'on a $q=p$ (p premier impair).

2.6 Définition. *On pose, pour* $x \in \mathbf{F}_p^*$, $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$. *Cette quantité est appelée* **symbole de Legendre** *de* x *modulo* p.

L'application $x \mapsto \left(\frac{x}{p}\right)$ est un homomorphisme (ou caractère) de $\mathbf{F}_p^*$ dans $\{\pm 1\}$ et x est un carré modulo p si et seulement si le symbole de Legendre $\left(\frac{x}{p}\right)$ vaut 1.

Notre objectif est donc de calculer le symbole de Legendre. Le fait que le symbole soit un homomorphisme et les résultats 2.3 et 2.4 permettent de se ramener au cas où x est l'image d'un nombre premier impair n. Calculer directement le reste de 21467^{32768} modulo 65537 est évidemment laborieux, surtout à la main[3]. La loi de réciprocité quadratique permet d'éviter ce calcul.

3. Il y a des programmes d'exponentiation rapide qui permettent à un ordinateur de faire cela en une fraction de seconde.

3 La loi de réciprocité quadratique

3.1 Énoncé, calcul, application

3.1.1 Énoncé

Il s'agit du merveilleux théorème suivant :

3.1 Théorème. *Soient p, n deux nombres premiers impairs. On a la formule :*

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

Autrement dit :

- *si n ou p est congru à 1 modulo 4 on a $\left(\frac{n}{p}\right) = \left(\frac{p}{n}\right)$,*
- *si n et p sont tous deux congrus à -1 modulo 4 on a $\left(\frac{n}{p}\right) = -\left(\frac{p}{n}\right)$.*

3.1.2 Calcul

Avant de prouver ce théorème, donnons un exemple de calcul. On considère $n = 37$ et $p = 1987$ (c'est un nombre premier). Comme 37 est congru à 1 modulo 4 on a :

$$\left(\frac{37}{1987}\right) = \left(\frac{1987}{37}\right) = \left(\frac{26}{37}\right) = \left(\frac{2}{37}\right) \times \left(\frac{13}{37}\right) = -\left(\frac{13}{37}\right) = -\left(\frac{37}{13}\right)$$

$$= -\left(\frac{-2}{13}\right) = -\left(\frac{2}{13}\right) = 1.$$

On voit que 37 est un carré modulo 1987. Pour trouver de quel entier il est le carré, le mieux est d'écrire quelques lignes de programmes, par exemple sur *xcas* :

```
racine(a,p):={
local b;
pour b de 1 jusque (p-1)/2 faire
si b^2 mod p==a alors
Disp b
fsi
fpour }
:;
```

On trouve en une fraction de seconde $632^2 \equiv 37 \pmod{1987}$.

3.1.3 Application

On cherche quels sont les nombres premiers p, distincts de 5, qui s'écrivent sous la forme $x^2 + 5y^2$ avec $x, y \in \mathbf{N}$. Une condition nécessaire est que -5 soit un carré modulo p, autrement dit qu'on ait $\left(\frac{-5}{p}\right) = 1$. On calcule ce symbole :

$$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right) \times \left(\frac{5}{p}\right) = \left(\frac{-1}{p}\right) \times \left(\frac{p}{5}\right)$$

et la condition devient :

$(p \equiv 1 \pmod 4 \text{ et } p \equiv \pm 1 \pmod 5)$ ou $(p \equiv -1 \pmod 4 \text{ et } p \equiv \pm 2 \pmod 5)$.

On montre que seuls les premiers sont effectivement de la forme $x^2 + 5y^2$, pour les autres c'est $2p$ qui l'est (voir le TER sur les anneaux d'entiers).

3.2 La preuve du théorème 3.1

3.2.1 Le principe

L'idée c'est que, pour étudier p modulo n, donc l'image de p dans $(\mathbf{Z}/n\mathbf{Z})^*$, il revient au même d'étudier le comportement du polynôme cyclotomique Φ_n sur $\mathbf{F}_p$. Cette idée intervient aussi pour montrer l'irréductibilité de Φ_n ou le petit théorème de Dirichlet, voir [DP] Ch. III ou ci-dessous Annexe 3. Pour cela, on va regarder le groupe de Galois de Φ_n sur $\mathbf{F}_p$ sous trois angles : comme le groupe d'un polynôme cyclotomique, comme un groupe cyclique, comme un groupe de permutations. On renvoie à l'Annexe 1 pour les généralités sur la théorie de Galois.

3.2.2 Rappels de théorie de Galois 1

• Rappel cyclotomique

Soient n un entier, K un corps de caractéristique ne divisant [4] pas n et $L = D_K(X^n - 1)$. On rappelle (cf. [DP]) que le polynôme cyclotomique $\Phi_{n,K}$ (ou Φ_n s'il n'y a pas d'ambiguïté) est le polynôme à coefficients dans K dont les racines sont les racines n-ièmes primitives de l'unité dans L. Son degré est l'indicatrice d'Euler $\varphi(n)$.

3.2 Proposition. *Soit n un entier positif, K un corps de caractéristique ne divisant pas n, $L = D_K(X^n - 1) = D_K(\Phi_n)$ le corps de décomposition de $X^n - 1$ sur K et soit ζ une racine primitive n-ième de l'unité dans L.*

4. Cette condition assure que les racines n-ièmes de l'unité sont toutes distinctes.

L'extension L/K est galoisienne et on a un homomorphisme injectif de $G := \mathrm{Gal}(L/K)$ dans $(\mathbf{Z}/n\mathbf{Z})^*$ qui à $\sigma \in G$ associe l'entier i_σ défini par $\sigma(\zeta) = \zeta^{i_\sigma}$.

Démonstration. Comme on a supposé que la caractéristique de K ne divise pas n, le polynôme $X^n - 1$ est séparable, donc l'extension L/K est galoisienne. Soit $\sigma \in G$ et posons $\xi = \sigma(\zeta)$. Comme on a $\zeta^n = 1$ et que σ est un homomorphisme, on a $\xi^n = 1$, donc ξ est une racine de l'unité. De plus, en appliquant σ^{-1} à ξ, on voit que c'est une racine primitive. Elle s'écrit donc $\xi = \zeta^{i_\sigma}$ avec i_σ entier et comme $\zeta^n = 1$, on peut considérer que i_σ est un entier modulo n. Si τ est un autre élément du groupe de Galois, on a $\tau(\sigma(\zeta)) = \tau(\zeta^{i_\sigma}) = \tau(\zeta)^{i_\sigma} = \left(\zeta^{i_\tau}\right)^{i_\sigma} = \zeta^{i_\tau i_s}$. On voit que l'application $\sigma \mapsto i_\sigma$ est multiplicative. Appliquant cela avec $\tau = \sigma^{-1}$, on en déduit que i_σ est inversible modulo n et on a établi la proposition.

3.3 *Remarque.* On rappelle que le groupe $(\mathbf{Z}/n\mathbf{Z})^*$ est de cardinal $\varphi(n)$ (voir [DP] Ch. I) et que ce cardinal est $n-1$ si n est premier. Bien entendu, l'homomorphisme précédent n'est pas nécessairement surjectif (penser au cas où K contient une racine primitive ; dans ce cas on a $L = K$ et G est réduit à l'identité). Précisément, comme L est engendré par une racine primitive ζ, il est surjectif si et seulement si ζ est de degré $\varphi(n)$. Comme ce nombre est aussi le degré de Φ_n, cela signifie que Φ_n est irréductible sur K.

- **Rappel Frobenius**

3.4 Proposition. *Soit p un nombre premier et r un entier positif. Le groupe de Galois de $\mathbf{F}_{p^r}$ sur $\mathbf{F}_p$ est engendré par l'homomorphisme*[5] *de Frobenius $F(x) = x^p$.*

Démonstration. On sait que le Frobenius est un homomorphisme : c'est la merveilleuse formule $(x+y)^p = x^p + y^p$ valable en caractéristique p. C'est donc un automorphisme du corps $\mathbf{F}_{p^r}$. Le groupe $\mathbf{F}_{p^r}^*$ est de cardinal $p^r - 1$, de sorte que ses éléments vérifient $x^{p^r-1} = 1$ donc aussi $x^{p^r} = x$ et cette dernière formule vaut aussi pour $x = 0$ donc pour tous les éléments de $\mathbf{F}_{p^r}$. Appliquée avec $r = 1$, cette formule montre que F fixe $\mathbf{F}_p$, donc est dans le groupe de Galois. Appliquée avec r quelconque, elle montre qu'on a $F^r = \mathrm{Id}$. De plus r est exactement l'ordre de F. En effet, si l'on a $F^s = \mathrm{Id}$ avec $s < r$, cela signifie que l'on a pour tout $x \in \mathbf{F}_{p^r}$, $x^{p^s} = x$ et le polynôme $X^{p^s} - X$ a trop de racines pour son degré. Comme on sait (voir 4.11) que le groupe de Galois a pour ordre le degré de l'extension, donc r, on voit que F l'engendre.

- **Les deux ensemble**

5. Familièrement appelé *le Frobenius*.

3.5 Proposition. *Soient p un nombre premier, n un entier premier à p, $K = \mathbf{F}_p$, $L = D_{\mathbf{F}_p}(\Phi_n)$. Le groupe de Galois de L sur K est isomorphe au sous-groupe de $(\mathbf{Z}/n\mathbf{Z})^*$ engendré par p.*

Démonstration. En effet, en vertu de 3.5, le groupe de Galois est engendré par le Frobenius qui vérifie $F(x) = x^p$ pour tout x, en particulier pour $x = \zeta$, racine primitive n-ième de 1. Avec les notations de 3.2 on a donc $i_F = p$ et le résultat.

• **Conséquences**

On a vu que regarder p dans $(\mathbf{Z}/n\mathbf{Z})^*$ c'est exactement regarder le générateur du groupe $\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p)$. Cette simple remarque est riche de conséquences :

1) Dire que p est congru à 1 modulo n signifie que le groupe de Galois est réduit à l'identité, donc que l'extension L/K est triviale, ou encore que $X^n - 1$ est scindé sur K. Cela signifie[6] donc que $\mathbf{F}_p$ contient une racine n-ième primitive de 1. C'est ainsi que l'on montre le petit théorème de Dirichlet : il existe une infinité de p premiers congrus à 1 modulo n, voir Annexe 3.

2) Dire que p engendre $(\mathbf{Z}/n\mathbf{Z})^*$ signifie que le groupe de Galois est isomorphe à $(\mathbf{Z}/n\mathbf{Z})^*$ ou encore que Φ_n est irréductible sur $\mathbf{F}_p$ (voir [DP] Ch. III ou Annexe 3).

3) Dans le cas qui nous intéresse, on a le lemme suivant :

3.6 Lemme. *Soient p, n deux nombres premiers impairs distincts. Le groupe $(\mathbf{Z}/n\mathbf{Z})^*$ est cyclique d'ordre $n-1$ et p est un carré modulo n si et seulement si l'ordre de p modulo n est un diviseur de $(n-1)/2$.*

Démonstration. En effet, dire que p est un carré, $p = r^2$, implique qu'on a $p^{(n-1)/2} = r^{n-1} = 1$. La réciproque est vraie parce que le groupe est cyclique.

3.2.3 Rappels de théorie de Galois 2

• **Permutations**

3.7 Proposition. *Soit K un corps, $P \in K[X]$ un polynôme séparable*[7] *de degré m et $L = D_K(P)$. Alors, l'extension L/K est galoisienne et son groupe de Galois G s'injecte dans $\mathfrak{S}_m$.*

De plus, si l'on a $P = P_1 \cdots P_r$ avec les P_i irréductibles sur K, et si ω_i désigne l'ensemble des racines de P_i dans L, le groupe G laisse stable ω_i et agit transitivement sur ω_i, de sorte que les ω_i sont les orbites de G dans son action sur les racines de P.

6. C'est d'ailleurs clair car $\mathbf{F}_p^*$ étant cyclique, il contient un élément d'ordre n dès que n divise $p-1$.

7. C'est-à-dire admettant m racines distinctes dans $D_K(P)$.

Démonstration. Le groupe de Galois G permute les m racines (distinctes) $x_1, \ldots, x_m$ de P (voir 4.1) et on obtient ainsi un homomorphisme de G dans $\mathfrak{S}_m$. Comme les x_i engendrent L, cet homomorphisme est injectif. Il est clair que les ω_i sont stables par G et le fait que le groupe est transitif sur ces ensembles vient de 4.13.

• **Le cas cyclique**

Dans la situation précédente, lorsque K est fini, G est cyclique engendré par le Frobenius F et si les P_i sont de degrés d_i, F vu comme élément de $\mathfrak{S}_m$ est produit de r cycles disjoints d'ordres d_i.

• **Le cas cyclotomique sur un corps fini**

On va appliquer ce qui précède avec $K = \mathbf{F}_p$ et $P = \Phi_n$. On a d'abord un lemme très général sur les facteurs irréductibles des polynômes cyclotomiques :

3.8 Lemme. *Soit n un entier, K un corps de caractéristique ne divisant pas n, $\Phi_n = P_1 \cdots P_r$ la décomposition en produit de facteurs irréductibles de Φ_n sur K. Alors, les P_i sont tous de même degré $d = \varphi(n)/r$.*

Démonstration. Soit ζ_i une racine de P_i. Comme c'est une racine primitive n-ième de 1, elle engendre toutes les autres et on a donc $K(\zeta_i) = D_K(\Phi_n)$. On voit que les ζ_i ont toutes même degré sur K, c'est-à-dire que les P_i ont tous même degré.

3.9 Corollaire. *Soit n un entier, p un nombre premier ne divisant pas n, $K = \mathbf{F}_p$ le corps à p éléments et $L = D_K(\Phi_n)$. L'homomorphisme de Frobenius F, vu comme permutation des racines de Φ_n, est un produit de r cycles d'ordre d avec $rd = \varphi(n)$. C'est un élément d'ordre d.*

• **Conséquence**

3.10 Corollaire. *Soient n, p deux nombres premiers impairs distincts. On suppose que le polynôme cyclotomique Φ_n est décomposé sur $\mathbf{F}_p$ en produit de r polynômes irréductibles de degré d. On a alors les équivalences suivantes :*

$$p \text{ est un carré modulo } n \iff d \text{ divise } (n-1)/2 \iff r \text{ est pair.}$$

Démonstration. La première équivalence a été vue en 3.6. La seconde vient de la formule $rd = n - 1 = 2 \times \frac{n-1}{2}$.

3.2.4 Discriminant

On vient de caractériser le fait que p est un carré modulo n en termes de Φ_n. Il reste à faire l'autre moitié du travail, donc à préciser quand n est un carré modulo p, toujours dans le cadre adopté, donc en étudiant le polynôme cyclotomique Φ_n sur $\mathbf{F}_p$. La recette est dans le discriminant, voir 5.10 dans l'Annexe 2 ci-dessous :

3.11 Lemme. *Soit n un nombre premier impair. Le discriminant du polynôme Φ_n est égal à $\Delta(\Phi_n) = (-1)^{n(n-1)/2} n^{n-2}$.*

• Rappel de théorie de Galois 3

Le fait que le discriminant d'un polynôme soit un carré se traduit en termes de groupes de Galois (voir 5.4) :

3.12 Proposition. *Soit K un corps, $P \in K[X]$ un polynôme séparable de degré m, Δ son discriminant, $L = D_K(P)$. Alors, le groupe de Galois de L (ou de P), vu comme sous-groupe de $\mathfrak{S}_m$, est contenu dans $\mathfrak{A}_m$ si et seulement si Δ est un carré de K.*

Dans le cas qui nous intéresse on obtient :

3.13 Corollaire. *Soient p, n des nombres premiers impairs distincts. Le discriminant $\Delta(\Phi_n)$ est un carré modulo p si et seulement si $\mathrm{Gal}(\Phi_n)$ est contenu dans $\mathfrak{A}_{n-1}$. C'est équivalent à dire que le Frobenius est une permutation paire, ou encore, avec les notations de 3.9 que r est pair.*

Démonstration. On sait que le groupe de Galois est engendré par le Frobenius et il suffit de savoir quand celui-ci est une permutation paire. Mais, on a vu en 3.9 qu'il est produit de r cycles d'ordre d avec $rd = n-1$. Si r est pair, la permutation est paire dans tous les cas. Si r est impair, comme $n-1$ est pair, c'est que d est pair. Mais alors les d-cycles sont des permutations impaires et leur produit aussi.

3.2.5 La conclusion

En mettant ensemble 3.10 et 3.13, on voit que r est pair est équivalent à la fois au fait que p est un carré modulo n et que $\Delta(\Phi_n)$ est un carré modulo p. Mais, comme n est impair, ce dernier point signifie exactement que $(-1)^{n(n-1)/2} n$ est un carré modulo p. Si n est congru à 1 modulo 4, $n(n-1)/2$ est pair et les symboles de Legendre sont égaux. S'il est congru à -1, on a $\left(\frac{p}{n}\right) = \left(\frac{-n}{p}\right) = \left(\frac{-1}{p}\right) \times \left(\frac{n}{p}\right)$. Si p est congru à 1 modulo 4, les symboles sont encore égaux, mais s'il est congru à -1 ils sont opposés. Cela achève de prouver le théorème.

4 Annexe 1 : un peu de théorie de Galois

Cette annexe vise à rappeler le b-a ba de la théorie de Galois qui sera utile, dans ce sujet et dans d'autres. On utilise les notations et les résultats de [DP]. La rédaction en est parfois sommaire. Le lecteur qui souhaiterait en savoir plus ira consulter l'excellent livre de Ian Stewart [S].

4.1 Introduction

La problématique de la théorie de Galois est la suivante. On a une extension finie [8] de corps $K \subset L$ et on s'intéresse aux extensions intermédiaires $K \subset M \subset L$. Il y a plusieurs raisons pour cela :

• Quand on étudie les constructions à la règle et au compas, on doit déterminer s'il existe une "tour" d'extensions $K = K_0 \subset K_1 \subset \cdots \subset K_n = L$ dans laquelle chaque extension intermédiaire est de degré 2.

• Quand on étudie la résolution par radicaux on cherche aussi de telles tours, mais avec des extensions intermédiaires de la forme $K_{i+1} = K_i(\alpha)$ avec $\alpha^r = a$ pour $a \in K_i$ (donc où $\alpha = \sqrt[r]{a}$ est un radical).

L'idée de la théorie de Galois est d'établir un **dictionnaire** entre ces extensions intermédiaires et les sous-groupes d'un groupe fini associé à l'extension initiale et appelé groupe de Galois. Bien entendu, cela repose sur l'idée que la situation est plus simple du côté des groupes que du côté des corps, ce qui est effectivement le cas.

4.2 Le groupe de Galois

4.1 Définition. *Soit $K \subset L$ une extension. Le groupe de Galois de l'extension est le groupe des automorphismes de corps de L qui induisent l'identité sur K. On le note* $\mathrm{Gal}(L/K)$.

Rappelons qu'un automorphisme de corps est une bijection qui conserve addition et multiplication. L'idée intuitive qu'il faut avoir est la suivante :

4.2 Proposition. *Soit $K \subset L$ une extension et soit $\alpha \in L$ un élément algébrique sur K qui annule le polynôme $P \in K[X]$. Alors, si σ est un élément de* $\mathrm{Gal}(L/K)$*, il envoie α sur une (autre) racine du polynôme P.*

Démonstration. On écrit $P(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$, avec $a_i \in K$ et on applique σ. Comme il fixe K et que c'est un automorphisme, on a $\sigma(P(\alpha)) = \sigma(\alpha)^n + a_{n-1}\,\sigma(\alpha)^{n-1} + \cdots + a_1\,\sigma(\alpha) + a_0 = P(\sigma(\alpha)) = 0$.

8. Cela signifie que L est un K-espace vectoriel de dimension finie. Cette dimension s'appelle le degré de l'extension et on la note $[L : K]$

On voit que les éléments du groupe de Galois permutent les racines de P. Cela pose aussitôt deux questions :

• Les racines de P sont-elles toutes dans L ? (Autrement dit, P est-il scindé dans L ?)

• Ces racines sont-elles toutes distinctes ?

Ces questions conduisent à poser les définitions suivantes :

4.3 Définition. *Soit $K \subset L$ une extension finie.*

1) On dit que l'extension est **normale** *si pour tout polynôme irréductible $P \in K[X]$, si P a une racine dans L il est scindé sur L.*

2) On dit que l'extension est **séparable** *si pour tout polynôme irréductible $P \in K[X]$ admettant une racine dans L, ses racines (dans un corps de décomposition) sont toutes distinctes.*

3) On dit que l'extension est **galoisienne** *si elle est à la fois normale et séparable.*

4.4 *Remarques.* 1) La condition de normalité est essentielle. L'exemple type d'une extension non normale est $\mathbf{Q} \subset \mathbf{Q}(\sqrt[3]{2})$. En effet, le polynôme $X^3 - 2$ a une racine dans cette extension (réelle) mais pas les deux autres qui sont $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$.

2) Cette condition peut sembler difficile à vérifier si on veut le faire pour tout polynôme. Heureusement, on a un critère très simple : une extension est normale si et seulement si c'est le corps de décomposition $D_K(P)$ d'un polynôme $P \in K[X]$, voir [S]. Autrement dit, il suffit de vérifier la condition pour un seul polynôme. Cela montre que $\mathbf{Q} \subset \mathbf{Q}(\sqrt[3]{2}, j) = D_{\mathbf{Q}}(X^3 - 2)$ est normale.

3) La condition de séparabilité est plus délicate, mais elle est automatique en caractéristique zéro ou sur un corps fini, voir ci-dessous.

4.3 Séparabilité

4.5 Définition. *Soit $P \in K[X]$ un polynôme de degré n. On dit que P est* **séparable** *si ses n racines, dans un corps de décomposition de P, sont toutes distinctes. Sinon, on dit que P est inséparable.*

L'intérêt de cette notion est dans la proposition suivante, que nous admettrons :

4.6 Proposition. *Soit K un corps, $P \in K[X]$ un polynôme séparable et $L = D_K(P)$. L'extension L/K est séparable (donc galoisienne). On note $\mathrm{Gal}(P)$ son groupe de Galois. Inversement, toute extension galoisienne est de la forme $L = D_K(P)$ avec P séparable.*

La proposition suivante précise les polynômes séparables :

4.7 Proposition. *Soit $P \in K[X]$ un polynôme, $P = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$ sa décomposition en produit d'irréductibles sur K.*

1) Le polynôme P est séparable si et seulement si les P_i le sont et si les exposants α_i sont tous égaux à 1.

2) Si P est irréductible, il est inséparable si et seulement si son polynôme dérivé P' est le polynôme nul.

3) En caractéristique 0 tout polynôme irréductible est séparable.

4) En caractéristique P, un polynôme irréductible non séparable est de la forme $P(X) = Q(X^p)$. Sur un corps fini, tout polynôme irréductible est séparable.

Démonstration. Le point 1) est clair car deux polynômes irréductibles distincts n'ont pas les mêmes racines.

2) Dire que P n'est pas séparable c'est dire qu'il a une racine double α qui est alors racine de P'. Le *pgcd* de P et P', soit δ, est alors divisible par $X - \alpha$, donc de degré > 0. Mais, comme P est irréductible, on a $\delta = P$, donc P divise P', et cela implique $P' = 0$ pour une raison de degré.

3) On écrit $P(X) = a_n X^n + \cdots + a_0$ avec $n > 0$ et $a_n \neq 0$. On a $P'(X) = n a_n X^{n-1} + \cdots$ et ce polynôme n'est pas nul.

4) Il est clair que seuls les polynômes en X^p peuvent être inséparables puisque leur dérivée doit être le polynôme nul. Supposons K fini. Considérons un polynôme en X^p, $P(X) = a_n X^{np} + \cdots + a_1 X^p + a_0$ avec $a_i \in K$. Sur K, l'homomorphisme de Frobenius $x \mapsto x^p$ est surjectif, de sorte qu'il existe b_i tel que $a_i = b_i^p$. Mais alors, si on pose $Q(X) = b_n X^n + \cdots + b_0$, on a $P = Q^p$, et cela contredit l'irréductibilité de P.

4.8 Corollaire. *Si $K = \mathbf{F}_q$ et $L = \mathbf{F}_{q^n}$ sont des corps finis, l'extension $K \subset L$ est galoisienne.*

Démonstration. En effet, on a $L = D_K(X^{q^n} - X)$, de sorte que l'extension est normale et, comme K est fini, elle est séparable.

4.4 Le théorème de l'élément primitif

Le principal intérêt de la séparabilité réside dans le résultat suivant :

4.9 Théorème. (Théorème de l'élément primitif) *Soit $K \subset L$ une extension séparable. Alors, elle est monogène, autrement dit il existe $\alpha \in L$ tel que $L = K(\alpha)$.*

Par exemple, on vérifie qu'on a $\mathbf{Q}(\sqrt[3]{2}, j) = \mathbf{Q}(\sqrt[3]{2} + j)$. C'est d'ailleurs l'idée de la preuve du théorème, voir [S].

4.5 Le théorème de Galois

4.5.1 La correspondance de Galois

Soit $K \subset L$ une extension et $G = \mathrm{Gal}(L/K)$ son groupe de Galois. Notons $\mathcal{K}$ l'ensemble des extensions intermédiaires $K \subset M \subset L$ et $\mathcal{G}$ l'ensemble des sous-groupes de G. On a deux applications $\Phi : \mathcal{K} \to \mathcal{G}$ et $\Psi : \mathcal{G} \to \mathcal{K}$ définies comme suit.

L'application Φ est la plus naturelle. Elle associe à M le groupe de Galois de l'extension **du haut** $H = \mathrm{Gal}(L/M)$. C'est bien un sous-groupe de G (parmi les automorphismes de L fixant K on se limite à ceux qui fixent M). **Attention** en revanche $\mathrm{Gal}(M/K)$ **n'est pas** un sous-groupe de G, voir plus loin. On note que H fixe M et cela nous conduit au point suivant.

L'application Ψ associe à un sous-groupe H de G son **corps fixe** $M = L^H$:

$$L^H = \{x \in L \ \mid \ \forall \sigma \in H,\ \sigma(x) = x\ \}.$$

4.10 *Remarques.* 1) Les applications Φ et Ψ sont décroissantes relativement à l'inclusion.

2) Le théorème de Galois affirme que, dans le cas galoisien, les applications Φ et Ψ sont réciproques l'une de l'autre. Ce qu'on peut dire d'emblée c'est que si M est dans $\mathcal{K}$ et H dans $\mathcal{G}$ on a $M \subset \Psi \circ \Phi(M)$ et $\Phi \circ \Psi(H) \supset H$.

4.5.2 Le théorème

4.11 Théorème. (Galois) *Soit $K \subset L$ une extension finie galoisienne et G son groupe de Galois. On reprend les notations ci-dessus.*

1) Le groupe G est fini et son cardinal est égal au degré de l'extension.

2) Les applications Φ et Ψ sont des bijections décroissantes réciproques l'une de l'autre.

3) Si $K \subset M \subset L$ est une extension intermédiaire, les propriétés suivantes sont équivalentes :

i) L'extension $K \subset M$ est normale.

ii) Le sous-groupe $\mathrm{Gal}(L/M)$ est distingué dans G.

iii) Pour tout $\sigma \in G$ on a $\sigma(M) = M$.

De plus, on a alors un isomorphisme : $\mathrm{Gal}(M/K) \simeq \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)$.

Démonstration. Comme L/K est séparable, le théorème de l'élément primitif permet de l'écrire $L = K(\alpha)$, avec α de degré n, de polynôme minimal P.

1) Comme l'extension est normale, ce polynôme a n racines (distinctes) dans L : $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ et on a une application de G dans l'ensemble des racines qui associe à σ la racine $\sigma(\alpha)$. Comme α_i est de degré n elle engendre

L, de sorte que l'application est injective. Elle est aussi surjective : si α_i est une racine de P, il existe $\sigma \in G$ tel que $\sigma(\alpha) = \alpha_i$. C'est une conséquence de l'unicité du corps de rupture, voir [DP].

2) Remarquons d'abord que si M est une extension intermédiaire, l'extension $M \subset L$ est galoisienne. En effet, si on a $L = D_K(P)$, avec P séparable, on a aussi $L = D_M(P)$.

Montrons alors que la composée $\Phi \circ \Psi$ est l'identité de $\mathcal{G}$. Soit H un sous-groupe et $M = L^H$ son corps fixe. On a $L = M(\alpha)$. Je dis que α est algébrique sur M de degré $\leq |H|$. En effet, α est racine du polynôme $Q(X) = \prod_{\sigma \in H} (X - \sigma(\alpha))$ et on voit que ce polynôme est invariant sous H (les éléments de H permutent ses facteurs). Cela montre qu'on a $[L : M] \leq |H|$. Considérons alors $H' = \mathrm{Gal}(L/M)$. On a vu ci-dessus qu'il contient H. Mais on a vu aussi en 1) qu'on a $[L : M] = |H'| \geq |H|$. On en déduit $H = H'$ comme annoncé.

Le fait que $\Psi \circ \Phi$ soit l'identité de $\mathcal{K}$ en résulte facilement.

3) On montre l'équivalence de ii) et iii), qui est facile, puis celle de i) et iii). Pour cela on utilise encore le théorème de l'élément primitif en écrivant $M = K(\beta)$ avec Q comme polynôme minimal. Supposons $K \subset M$ normale. Si on a $\sigma \in G$, comme $\sigma(\beta)$ est une racine de Q, elle est dans M et M est stable. Inversement, si M est stable, les racines de Q sont dans M qui est donc égal à $D_K(Q)$, donc normale.

Enfin, l'isomorphisme s'obtient en restreignant les éléments de G à M (qui est stable). Cela donne un homomorphisme de $\mathrm{Gal}(L/K)$ dans $\mathrm{Gal}(M/K)$, dont le noyau est $\mathrm{Gal}(L/M)$ par définition. On a donc une injection

$$\mathrm{Gal}(L/K)/\mathrm{Gal}(L/M) \subset \mathrm{Gal}(M/K)$$

et c'est une bijection car les cardinaux sont égaux (par le point 1 du théorème de Galois et celui de la base télescopique, voir [DP]).

Une conséquence importante du théorème est la suivante :

4.12 Corollaire. *Soit $K \subset L$ une extension galoisienne de groupe G. Le corps fixe de L sous G est égal à K.*

Démonstration. En effet, on a $\Phi(K) = G$, donc $\Psi(G) = L^G = K$.

4.5.3 Conjugués

Le théorème de Galois permet de préciser 4.1 et d'introduire la notion de conjugué :

4.13 Proposition-Définition. *Soit $K \subset L$ une extension galoisienne finie, $G = \mathrm{Gal}(L/K)$. Soient $\alpha, \beta \in L$. Les propriétés suivantes sont équivalentes :*

1) Les nombres α et β ont même polynôme minimal sur K.

2) Il existe $\sigma \in G$ tel que $\sigma(\alpha) = \beta$.

On dit alors que α et β sont **conjugués** *sur K.*

Démonstration. Seule l'implication $1 \Longrightarrow 2$ mérite une preuve. L'unicité du corps de rupture (voir [DP]) fournit un isomorphisme de $K[\alpha]$ sur $K[\beta]$. Celle du corps de décomposition (*loc. cit.*) permet de le prolonger en un automorphisme de $D_K(P) = M$. Enfin, la surjectivité de la restriction $\mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$ vue en 4.11 permet de conclure.

5 Annexe 2 : Discriminant

5.1 Définition et propriété caractéristique

5.1 Notations. Dans toute cette annexe on désigne par K un corps de caractéristique différente de 2, par P un polynôme de degré $n > 0$ à coefficients dans K et par L son corps de décomposition $L = D_K(P)$. On suppose que le polynôme P est séparable c'est-à-dire qu'il admet n racines distinctes dans L, que l'on note $x_1, \ldots, x_n$. L'extension L/K est alors galoisienne et on note G son groupe de Galois, qui s'injecte dans le groupe symétrique $\mathfrak{S}_n$ par la formule : $g(x_i) = x_{\sigma_g(i)}$ (voir 3.7).

5.2 Proposition-Définition. *On pose $\delta = \prod_{1 \le i < j \le n} (x_i - x_j)$ et $\Delta = \delta^2 = \prod_{1 \le i < j \le n} (x_i - x_j)^2$. Le nombre*[9] *$\Delta$ est appelé* **discriminant** *du polynôme P. Les nombres δ et Δ sont des éléments de L^* et on a la formule*

$$\Delta = (-1)^{n(n-1)/2} \prod_{i \neq j} (x_i - x_j).$$

Le signe $(-1)^{n(n-1)/2}$ est égal à 1 si $n \equiv 0, 1 \pmod 4$ et à -1 sinon.

Démonstration. Il suffit de compter les signes $-$, donc les couples (i, j) avec $i > j$, il y en a bien $n(n-1)/2$.

5.3 *Remarque.* Attention, certains auteurs prennent $\Delta = \prod_{i \neq j} (x_i - x_j)$ comme définition du discriminant, mais la proposition suivante montre que c'est mal adapté à la théorie de Galois.

9. On le note $\Delta(P)$ lorsqu'on veut préciser de quel polynôme il est le discriminant.

5.4 Proposition. *Soit g un élément de G et σ_g la permutation associée.*
1) On a les formules $g(\delta) = \epsilon(\sigma_g)\delta$ et $g(\Delta) = \Delta$.
2) Le discriminant Δ est dans K^* (et pas seulement dans L^*).
3) On a les équivalences :

$$\delta \in K^* \iff \Delta \in K^{*2} \iff G \subset \mathfrak{A}_n.$$

Démonstration. La formule avec δ résulte du comptage du nombre d'inversions [10] de σ_g et celle avec Δ est évidente. Le point 2) en résulte car K est le corps fixe de G, voir 4.12. Enfin, le point 3) résulte lui aussi de 1) : si G est formé de permutations paires, les éléments de G fixent δ et inversement.

5.5 *Exemple.* Calculons le discriminant du polynôme du second degré $ax^2 + bx + c$. Ses racines sont x_1 et x_2 et on a $\Delta = (x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = \big(-\frac{b}{a}\big)^2 - 4\frac{c}{a} = \frac{b^2 - 4ac}{a^2}$.

5.2 Calcul du discriminant

5.6 Notations. On reprend les notations précédentes mais on suppose de plus que P est unitaire :

$$P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0.$$

On suppose que la caractéristique du corps ne divise pas n. On considère le polynôme dérivé $P'(x)$ et on note $y_1, \ldots, y_{n-1}$ ses racines. On a donc :

$$P'(X) = nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \cdots + a_1 = n\prod_{j=1}^{n-1}(X - y_j).$$

5.7 Théorème. *Soit Δ le discriminant de P. On a les formules :*

$$\Delta = (-1)^{n(n-1)/2}\prod_{i=1}^{n} P'(x_i) = (-1)^{n(n-1)/2}\prod_{i,j}(x_i - y_j) = (-1)^{n(n-1)/2}n^n\prod_{j=1}^{n-1} P(y_j).$$

Démonstration. On part de la formule $P(X) = \prod_{i=1}^{n}(X - x_i)$ que l'on dérive :

$$P'(X) = \sum_{i=1}^{n}(X - x_1)\cdots\widehat{(X - x_i)}\cdots(X - x_n)$$

10. Voire de la définition de la signature que l'on peut donner par cette formule, vue dans l'anneau de polynômes $K[x_1, \ldots, x_n]$.

où le chapeau signifie que le terme correspondant est omis. On calcule alors $P'(x_i)$. Tous les termes de la somme sont nulles sauf celui où l'on a omis x_i et on a donc, pour i fixé, $P'(x_i) = \prod_{j,j\neq i}(x_i - x_j)$. On en déduit la valeur du produit $\prod_{i=1}^{n} P'(x_i) = \prod_{i,j,\, j\neq i}(x_i - x_j)$ et la première formule vient de 5.2. En utilisant l'expression de P' en fonction de ses racines, on a $P'(x_i) = n\prod_{j=1}^{n-1}(x_i - y_j)$ d'où $\prod_{i=1}^{n} P'(x_i) = n^n \prod_{i,j}(x_i - y_j)$ et la seconde formule. Mais on a aussi $P(y_j) = \prod_{i=1}^{n}(y_j - x_i)$ et donc $\prod_{j=1}^{n-1} P(y_j) = \prod_{i,j}(y_j - x_i)$. Par rapport à l'expression précédente, chaque terme $x_i - y_j$ est changé de signe, ce qui fait $n(n-1)$ changements. Comme ce nombre est pair, le signe est le même et on a bien la troisième formule.

Ces formules permettent de calculer le discriminant du polynôme du troisième degré :

5.8 Proposition. *Le discriminant de $P(X) = X^3 + pX + q$ est $\Delta = -4p^3 - 27q^2$.*

Démonstration. On calcule $P'(X) = 3X^2 + p$ dont les racines sont $y_j = \pm\sqrt{-\dfrac{p}{3}}$, $j = 1, 2$, et on vérifie que le produit $P(y_1)P(y_2)$ vaut $A = \dfrac{27q^2 + 4p^3}{27}$. On a alors $\Delta = -27A$ et le résultat.

5.9 *Exercice.* Montrer que le discriminant de $P(X) = X^n + pX + q$ est donné par la formule :

$$\Delta = (-1)^{n(n-1)/2}\left(n^n q^{n-1} + (-1)^{n-1}(n-1)^{n-1}p^n\right).$$

5.3 Le cas cyclotomique

5.10 Proposition. *1) Soit n un entier quelconque premier à la caractéristique de K. On a $\Delta(X^n - 1) = (-1)^{(n-1)(n+2)/2}\, n^n$.*

2) Soit n un nombre premier impair. On a $\Delta(\Phi_n) = (-1)^{n(n-1)/2} n^{n-2}$.

Démonstration. 1) On peut calculer avec la formule utilisant les $P'(x_i)$, mais ici, il est bien plus simple d'utiliser l'autre. Si l'on pose $P(X) = X^n - 1$ on a $P'(X) = nX^{n-1}$ et son unique racine est 0. On a donc $P(y_j) = -1$ pour tout j et la formule en découle (c'est d'ailleurs un cas particulier de $X^n + pX + q$, voir exercice ci-dessus).

2) Ici, on va utiliser la formule avec les $P'(x_i)$. On a $X^n-1=(X-1)\Phi_n(X)$ ce qui donne $\Phi_n(X)=X^{n-1}+\cdots+X+1$ et aussi, en dérivant, $nX^{n-1}=(X-1)\Phi'_n(X)+\Phi_n(X)$ et, si on applique cela avec $X=\zeta^i$, ζ racine n-ième primitive et $i=1,\ldots,n-1$, on trouve $n\zeta^{i(n-1)}=(\zeta^i-1)\Phi'_n(\zeta^i)$. On a donc $\Phi'_n(\zeta^i)=\dfrac{n\zeta^{i(n-1)}}{\zeta^i-1}\cdot$ Comme on a $\zeta^n=1$, le numérateur est égal à ζ^{-i} et le produit de ces termes est le coefficient constant de Φ_n, soit 1, au signe $(-1)^{n-1}$ près. Les ζ^i-1, eux, sont les racines du polynôme $\Phi_n(X+1)=(X+1)^{n-1}+\cdots+(X+1)+1=X^{n-1}+\cdots+n$ et leur produit est donc $(-1)^{n-1}n$. En définitive, on a $\Delta(\Phi_n)=(-1)^{n(n-1)/2}n^{n-1}\prod_{i=1}^{n-1}\Phi'_n(\zeta^i)=(-1)^{n(n-1)/2}n^{n-2}$.

6 Annexe 3 : variations

Dans toutes ces variations, on utilise l'idée, qui a déjà servi pour la loi de réciprocité, qu'il revient au même d'étudier p modulo n ou d'étudier Φ_n sur $\mathbf{F}_p$.

6.1 L'irréductibilité du polynôme cyclotomique sur Q

6.1 Théorème. *Soit $n\in\mathbf{N}^*$. Le polynôme Φ_n est irréductible dans $\mathbf{Z}[X]$ ou $\mathbf{Q}[X]$.*

Démonstration. Ici, la recette de la preuve est l'équivalence entre le fait que p ne divise pas n et que le polynôme X^n-1 (donc aussi Φ_n) est séparable sur $\mathbf{F}_p$.

On sait que Φ_n est le polynôme produit des $X-\zeta$ étendu à toutes les racines primitives n-ièmes de l'unité. Soit ζ une telle racine et soit P son polynôme minimal sur $\mathbf{Q}$. Ce polynôme est à coefficients entiers (il suffit pour le voir de décomposer X^n-1 en produit de facteurs irréductibles sur $\mathbf{Z}$ et de prendre celui qui s'annule en ζ). Comme ζ annule Φ_n, P divise Φ_n et il suffit de montrer que toute racine de Φ_n est aussi racine de P. Soit donc ξ une racine de Φ_n. Comme ζ est une racine primitive de l'unité, ξ en est une puissance, $\xi=\zeta^m$, et comme ξ est primitive elle aussi, m est premier avec n, donc s'écrit $m=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ où les p_i sont des nombres premiers ne divisant pas n. Pour montrer que ξ est racine de P, il suffit de le faire pour ζ^p avec p ne divisant pas n et de raisonner par récurrence.

On doit donc montrer que ζ et ζ^p sont conjugués sur $\mathbf{Q}$. L'idée serait d'utiliser 4.13, donc de voir qu'il existe $\sigma\in\mathrm{Gal}(\Phi_n)$ tel que $\sigma(\zeta)=\zeta^p$. Sur $\mathbf{Q}$, ce n'est pas évident, mais sur $\mathbf{F}_p$ c'est vrai grâce à Frobenius et c'est là qu'on va travailler.

Notons que, si ζ et ζ^p ne sont pas conjugués, ils ont des polynômes minimaux P et Q différents, donc premiers entre eux (car irréductibles) et que le produit PQ divise $X^n - 1$.

Pour aller sur $\mathbf{F}_p$, il faut disposer d'une réduction modulo p qui permette de réduire ζ. Pour cela, on travaille donc dans l'anneau $\mathbf{Z}[\zeta]$ engendré par ζ. Dans cet anneau on considère l'idéal principal $p\mathbf{Z}[\zeta]$ et un idéal maximal $\mathfrak{P}$ qui le contient. Le quotient $L = \mathbf{Z}[\zeta]/\mathfrak{P}$ est un corps, qui contient $K = \mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$, donc un corps $L = \mathbf{F}_q$ avec $q = p^r$. On note $\overline{\zeta}$ l'image de ζ dans L. Comme Frobenius est dans $\mathrm{Gal}(L/K)$, $\overline{\zeta}$ et $\overline{\zeta}^p$ sont conjugués sur $\mathbf{F}_p$, donc ont même polynôme minimal R. Mais, par réduction modulo p, on a $X^n - 1 = \overline{P}\,\overline{Q}...$ et comme R est le polynôme minimal de $\overline{\zeta}$ et de $\overline{\zeta}^p$, il divise à la fois $\overline{P}$ et $\overline{Q}$, donc R^2 divise $X^n - 1$. Mais cela contredit le fait que $X^n - 1$ est séparable sur $\mathbf{F}_p$.

6.2 Le petit théorème de Dirichlet

6.2 Théorème. *Soit n un entier positif. Il existe une infinité de nombres premiers congrus à 1 modulo n.*

Démonstration. Cette fois, ce qu'on utilise c'est que p est congru à 1 modulo n si et seulement si Φ_n (ou $X^n - 1$) est scindé sur $\mathbf{F}_p$:

6.3 Lemme. *Soit n un entier positif et p un nombre premier ne divisant pas n. Alors, on a $p \equiv 1 \pmod{n}$ si et seulement si Φ_n admet une racine dans $\mathbf{F}_p$ (donc est scindé).*

Démonstration. En effet, dire que $\mathbf{F}_p$ contient une racine de Φ_n signifie qu'il contient un élément d'ordre n. Cela impose que n divise le cardinal de $\mathbf{F}_p^*$ qui vaut $p - 1$ et la réciproque est vraie car ce groupe est cyclique [11].

On peut alors prouver le théorème. On rappelle que Φ_n est unitaire et qu'on a, pour $n \geq 2$, $\Phi_n(0) = 1$. On considère $\Phi_n(k!)$ pour $k \in \mathbf{N}$. Lorsque k tend vers $+\infty$, cette quantité tend vers $+\infty$, donc, pour $k \geq k_0$, on a $\Phi_n(k!) \neq \pm 1$. Soit k un tel nombre. Si p est un facteur premier de $\Phi_n(k!)$, on a $\Phi_n(k!) \equiv 0 \pmod{p}$, ce qui, par le lemme, assure que p est congru à 1 modulo n. Mais on a :

$$\Phi_n(k!) = (k!)^{\varphi(n)} + \sum_{i=1}^{\varphi(n)-1} a_i (k!)^i + 1$$

11. Si l'on est savant, on peut aussi dire que le groupe de Galois du corps de décomposition de Φ_n sur $\mathbf{F}_p$ est engendré par le Frobenius $F(\zeta) = \zeta^p$ et qu'il est égal à l'identité (de sorte que l'extension est triviale) si p est congru à 1 modulo n.

et on voit qu'aucun nombre premier plus petit que k ne divise ce nombre (sinon il diviserait 1). Cela montre que p est plus grand que k et comme cela vaut pour tout $k \geq k_0$, il y a une infinité de p premiers congrus à 1 modulo n.

6.4 *Remarque.* Le vrai théorème de Dirichlet affirme que, pour tout entier a premier avec n, il existe une infinité de nombres premiers congrus à a modulo n. Il est considérablement plus difficile à établir, voir [Serre].

6.3 L'irréductibilité du polynôme cyclotomique sur $\mathbf{F}_p$

On sait que si un polynôme à coefficients entiers est irréductible en réduction modulo p, il l'est sur $\mathbf{Z}$. Malheureusement, ce résultat ne peut pas permettre de prouver l'irréductibilité de Φ_n sur $\mathbf{Z}$ comme le montre le théorème suivant :

6.5 Théorème. *Soit n un entier positif. Il existe un nombre premier p, ne divisant pas n tel que Φ_n soit irréductible sur $\mathbf{F}_p$ si et seulement si le groupe $(\mathbf{Z}/n\mathbf{Z})^*$ est cyclique, i.e. si $n = 1, 2, 4, q^\alpha$ ou $2q^\alpha$ avec q premier impair.*

Démonstration. Pour l'équivalence des deux dernières propriétés voir [DP] Ch. I.

Supposons qu'il existe p premier tel que Φ_n est irréductible sur $\mathbf{F}_p$. En vertu de 3.3, cela implique que son groupe de Galois sur $\mathbf{F}_p$, soit G, est isomorphe à $(\mathbf{Z}/n\mathbf{Z})^*$. Comme G est cyclique puisque le corps de base est fini, cela impose que $(\mathbf{Z}/n\mathbf{Z})^*$ l'est aussi. La réciproque est vraie, mais moins triviale. Si $(\mathbf{Z}/n\mathbf{Z})^*$ est cyclique, il est engendré par un entier a premier à n. Grâce au (vrai) théorème de Dirichlet (voir ci-dessus) on peut supposer que a est un nombre premier p. Sur le corps $\mathbf{F}_p$, le Frobenius engendre donc $(\mathbf{Z}/n\mathbf{Z})^*$ ce qui assure que Φ_n est irréductible.

7 Références

[DP] PERRIN Daniel, *Cours d'Algèbre*, Ellipses, 1996.

[S] STEWART Ian, *Galois theory*, Chapmann-Hall, 1973.

[Serre] SERRE Jean-Pierre, *Cours d'arithmétique*, PUF, 1970.