Cyclotomie

Salim Rostam
Complément d'algèbre pour l'agrégation, ENS Rennes

1 Racines de l'unité

Soit k un corps commutatif. On note $\mathrm{char}(k)$ sa caractéristique.

Définition 1.1. Une *racine de l'unité* de k est un élément $\zeta \in k^\times$ d'ordre fini. Si $\zeta^m = 1$ on dit que ζ est une racine m-ième de l'unité, et si ζ est d'*ordre* n alors on dit que ζ est une racine *primitive* n-ième de l'unité.

Remarque 1.2. L'ordre de $\zeta \in k^\times$ est $\#\langle\zeta\rangle$.

On note $\mu_n(k) \coloneqq \{\zeta \in k^\times : \zeta^n = 1\}$ l'ensemble des racines n-ièmes de l'unité de k et $\mu_n^\times(k) \subseteq \mu_n(k)$ l'ensemble des racines n-ièmes primitives de l'unité de k. On a toujours $\mu_n(k) \neq \emptyset$ puisque $1 \in \mu_n(k)$, en revanche on peut avoir $\mu_n^\times(k) = \emptyset$ (par exemple $\mu_3^\times(\mathbb{Q}) = \emptyset$; voir aussi le Corollaire 1.13).

Proposition 1.3. *L'ensemble $\mu_n(k)$ est un sous-groupe de $k^\times$ d'ordre au plus n, en particulier $\mu_n(k)$ est cyclique.*

Démonstration. On a $\mu_n(k) = \{x \in k : x^n = 1\}$ donc $\mu_n(k) = Z_k(X^n - 1)$. Puisque k est commutatif, on en déduit que $\mu_n(k)$ est un groupe et qu'il est d'ordre au plus n. Le fait qu'il soit cyclique est un théorème classique, plus généralement si H est un sous-groupe d'ordre $N \in \mathbb{N}^*$ de $k^\times$ alors H est cyclique. On en donne trois démonstrations.

1. (Cf. [Per, Théorème 2.7]) Si $x \in H$ est d'ordre $d \mid N$ alors $\langle x\rangle \subseteq H$ est de cardinal d, de plus tous les éléments de $\langle x\rangle$ sont d'ordre divisant d. Or, les éléments de H d'ordre divisant d sont tous racines sur k de $X^d - 1$, donc (puisque k est commutatif) il y en a au plus d. Ainsi, le sous-groupe $\langle x\rangle$ est exactement l'ensemble des éléments de H d'ordre divisant d. De plus, le sous-groupe $\langle x\rangle \simeq \mathbb{Z}/d\mathbb{Z}$ possède exactement $\varphi(d)$ éléments d'ordre d, où φ est la fonction indicatrice d'Euler. Ainsi, pour $d \mid N$, le nombre n_d d'éléments d'ordre d de H vaut soit 0 soit $\varphi(d)$. Puisque $N = \sum_{d|N} n_d$ et que l'on sait que $N = \sum_{d|N} \varphi(d)$ (compter les éléments d'ordre d dans $\mathbb{Z}/N\mathbb{Z}$ ou voir [Gou, Proposition 6 page 32]), on conclut que $n_d = \varphi(d)$ en particulier $n_N = \varphi(N) \geq 1$ donc H est cyclique car possède un élément d'ordre N.
2. (Cf. Mercier *Cours de géométrie* Lemme 16 p.296.) Si $N = 1$ le théorème est vrai, on suppose donc $N \geq 2$. On écrit $N = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ la décomposition de N en produit de facteurs premiers. Puisque H est commutatif, il suffit de trouver un élément d'ordre $p_i^{\alpha_i}$ pour tout i. Si tous les éléments de H sont d'ordre $p_1^{\beta_1} \cdots p_r^{\beta_r}$ avec $\beta_i < \alpha_i$ alors tous les éléments de H sont d'ordre divisant $\frac{n}{p_i}$ donc sont racines de $X^{\frac{n}{p_i}} - 1 \in k[X]$. Or, puisque k est commutatif ce polynôme possède au plus $\frac{n}{p_i}$ racines, ce qui est impossible puisque $\#H = n$. Ainsi, il existe un élément $x \in H$ d'ordre $p_i^{\alpha_i} q$ avec $q = \prod_{j \neq i} p_j^{\beta_j}$ donc $x^q \in H$ est d'ordre $p_i^{\alpha_i}$ et c'est ce qu'on voulait.

3. (Besoin d'une référence.) On raisonne par récurrence sur N, avec les mêmes arguments qu'avant. Si $N = 1$ c'est bon. Si $N = p^k$ avec p premier et $k \geq 1$, supposons que H ne soit pas cyclique. Alors tout $x \in H$ vérifie $x^{p^{k-1}} = 1$ donc $\#H \leq p^{k-1}$ ce qui est absurde. Si maintenant $N = ab$ avec $\mathrm{pgcd}(a, b) = 1$ et $a, b < N$, on considère l'application $f : \left| \begin{array}{ccc} H & \to & H \\ x & \mapsto & x^a \end{array} \right.$. C'est un morphisme de groupe car k est commutatif. On a $\#\ker f \leq a$ et $\#\,\mathrm{im} f \leq b$, de plus $N = \#H = (\#\ker f)(\#\,\mathrm{im} f)$ donc $\#\ker f = a$ et $\#\,\mathrm{im} f = b$. Ainsi, par hypothèse de récurrence on peut trouver un élément x d'ordre a dans $\ker f \subseteq H$ et un élément y d'ordre b dans $\mathrm{im} f \subseteq H$ et on conclut puisque $xy \in H$ est d'ordre $ab = N$.

□

Remarque 1.4 (Cf. [Per, VII.1]). La proposition précédente devient fausse si k n'est pas commutatif ! Par exemple, considérons le corps $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ (non commutatif, donc) des quaternions, donné par $i^2 = j^2 = k^2 = ijk = -1$. On a un antiautomorphisme de conjugaison $q = a + bi + cj + dk \mapsto \bar{q} := a - bi - cj - dk$. On a $q \in \mathbb{R} \iff \bar{q} = q$, et $\bar{q} = -q$ si et seulement si $q = bi + cj + dk$ est un quaternion *pur*. La *norme* de $q = a + bi + cj + dk \in \mathbb{H}$ est donnée par $N(q) := q\bar{q} = a^2 + b^2 + c^2 + d^2$. Ainsi, les quaternions purs de norme 1 sont ceux donnés par $b^2 + c^2 + d^2 = 1$ et vérifient $1 = N(q) = q\bar{q} = -q^2$ donc $(iq)^2 = 1$. On conclut puisqu'il y a une infinité de $b, c, d \in \mathbb{R}$ qui conviennent, en particulier, le corps non commutatif $\mathbb{H}$ possède une infinité de racines carrées de l'unité.

Lemme 1.5. *Pour $n \in \mathbb{N}^*$, on considère le polynôme $P_n := X^n - 1 \in k[X]$.*
- *Si $\mathrm{char}(k) \nmid n$, le polynôme P_n est sans facteur carré.*
- *Si $\mathrm{char}(k) \mid n$, alors en écrivant $n = p^\alpha m$ avec $p := \mathrm{char}(k) \neq 0$ et $p \nmid m$, on a $P_n(X) = P_m(X)^{p^\alpha}$ et P_m est sans facteur carré.*

Démonstration. Si $\mathrm{char}(k) \nmid n$, alors $P_n' = nX^{n-1} \in k[X]$ est non nul donc P_n n'a pas de facteur carré. On suppose maintenant $\mathrm{char}(k) \mid n$ et soient m, p, α comme dans l'énoncé. En particulier, puisque $n \geq 1$ on a bien $p \neq 0$, et $\alpha \geq 1$ puisque $p \mid n$. En remarquant que $(-1)^{p^\alpha} = -1$ dans k et utilisant le morphisme de Frobenius, on a

$$P_n(X) = X^n - 1 = X^{p^\alpha m} + (-1)^{p^\alpha} = (X^m + (-1))^{p^\alpha} = P_m(X)^{p^\alpha}.$$

On conclut puisque P_m est sans facteur carré car $p = \mathrm{char}(k) \nmid m$. □

Remarque 1.6. Avec les notations du Lemme 1.5, on a $m < n$.

Proposition 1.7. *On suppose que $\mathrm{char}(k) \mid n$. Alors si $n = p^\alpha m$ avec $p \nmid m$, on a $\mu_n(k) = \mu_m(k)$.*

Démonstration. En effet, si $x \in \mu_n(k)$ alors $x^n - 1 = 0$ donc par le Lemme 1.5 on a $(x^m - 1)^{p^\alpha} = 0$ donc, puisque k est intègre, on a $x^m - 1 = 0$ donc $x \in \mu_m(k)$. L'inclusion inverse est claire puisque $m \mid n$. □

Corollaire 1.8. *Si k possède une racine primitive n-ième de l'unité alors $\mathrm{char}(k) \nmid n$. Autrement dit, si $\mathrm{char}(k) \mid n$ alors k ne possède pas de racine primitive n-ième de l'unité.*

Démonstration. Si k possède une racine primitive n-ième ζ de l'unité alors $\#\langle\zeta\rangle = n$. Par la Proposition 1.3 on a $\#\mu_n(k) \leq n$, donc puisque $\langle\zeta\rangle \subseteq \mu_n(k)$ on en déduit que $\mu_n(k) = \langle\zeta\rangle$ est de cardinal n. Ainsi, si on avait $\mathrm{char}(k) \mid n$ alors par les Propositions 1.3 et 1.7 on aurait $\#\mu_n(k) \leq m < n$ (cf. Remarque 1.6) ce qui est absurde, donc $\mathrm{char}(k) \nmid n$. □

Remarque 1.9. La réciproque du Corollaire 1.8 n'est pas toujours vérifiée, voir par exemple $0 \nmid 3$ mais $\mu_3^\times(\mathbb{Q}) = \emptyset$. Voir aussi le Corollaire 1.13.

La Proposition 1.7 montre qu'il suffit d'étudier les groupes $\mu_n(k)$ pour $\mathrm{char}(k) \nmid n$. Désormais, on fera systématiquement cette hypothèse et on désignera par k_n un corps de décomposition de $P_n = X^n - 1$ sur k.

Proposition 1.10. *On suppose* $\mathrm{char}(k) \nmid n$. *On a* $\#\mu_n(k_n) = n$ *et* $\#\mu_n^\times(k_n) = \varphi(n)$. *En particulier on a* $\mu_n(k_n) \simeq \mathbb{Z}/n\mathbb{Z}$ *et* $\mu_n^\times(k_n) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.

Démonstration. Puisque $\mathrm{char}(k) \nmid n$, par le Lemme 1.5 le polynôme $X^n - 1$ est sans facteur carré donc ne possède pas de racine multiple, ainsi $\#\mu_n(k_n) = n$. Les éléments de $\mu_n^\times(k_n)$ sont alors exactement les éléments d'ordre n de $\mu_n(k_n)$, donc par la preuve de la Proposition 1.3 on a $\#\mu_n(k_n) = \varphi(n)$. On conclut puisque $\mu_n(k_n)$ est cyclique par la Proposition 1.3 et en utilisant la définition de $\mu_n^\times(k_n)$. □

Remarque 1.11. Je trouve qu'écrire $\mu_n^\times(k_n) \simeq \mu_n(k_n)^\times$ est un peu maladroit, puisque l'on voit d'habitude $\mu_n(k_n)$ plutôt comme un groupe et non comme un anneau (en tout cas, c'est le cas pour moi).

Remarque 1.12. Directement à partir de la Proposition 1.3, si $k = \mathbb{F}_q$ alors $k^\times \simeq \mathbb{Z}/(q-1)\mathbb{Z}$ et donc $\#\mu_n(k) = n \wedge (q-1)$.

Corollaire 1.13. *On suppose* $\mathrm{char}(k) \nmid n$. *On a* $\#\mu_n(k) = d$ *où* $d \mid n$. *En particulier :*
- *si* $d = n$ *alors* $\mu_n(k) \simeq \mathbb{Z}/n\mathbb{Z}$ *et* $\mu_n^\times(k) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$;
- *si* $d < n$ *alors* $\mu_n(k) \simeq \mathbb{Z}/d\mathbb{Z}$ *et* $\mu_n^\times(k) = \emptyset$.

Démonstration. Le cardinal de $\mu_n(k)$ divise n puisque $\mu_n(k)$ est un sous-groupe de $\mu_n(k_n)$, qui est lui de cardinal n par la Proposition 1.10. Pour l'isomorphisme $\mu_n(k) \simeq \mathbb{Z}/d\mathbb{Z}$, soit on utilise la structure des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ soit on réutilise la Proposition 1.3 pour dire que $\mu_n(k)$ est cyclique. L'isomorphisme pour $\mu_n^\times(k)$ découle de la définition. □

Concluons cette section par une idée de développement.

Théorème 1.14. *On considère un polygone* $\mathcal{P}$ *du plan. Si on considère le polygone dont les sommets sont les milieux des côtés de* $\mathcal{P}$ *(pris dans le même ordre) et que l'on répète ce processus, à la limite les sommets du polygone convergent vers le centre de gravité de* $\mathcal{P}$.

Idée de la preuve. On écrit le processus avec des affixes complexes. On obtient alors une relation de récurrence entre deux vecteurs donnée par une matrice circulante. On étudie le comportement asymptotique en diagonalisant ladite matrice (c'est là que les racines de l'unité interviennent ; cf. [Gou, Exercice 4 page 180]). Pour une preuve complète, voir le tout nouveau « 131 développements pour l'oral » (développement 69), co-écrit par entre autres deux anciens de l'ENS Rennes ! □

Il peut être nécessaire de broder un peu autour pour remplir le temps nécessaire (si on se place dans $\mathbb{R}^n$, vitesse de convergence, caractère stationnaire,...).

2 Polynômes cyclotomiques

On rappelle que $n \in \mathbb{N}^*$ et que k_n désigne un corps de décomposition de $X^n - 1$ sur k.

Définition 2.1. Le n-ième *polynôme cyclotomique*, noté $\Phi_{n,k}$, est défini par

$$\Phi_{n,k}(X) := \prod_{\zeta \in \mu_n^\times(k_n)} (X - \zeta) \in k_n[X].$$

D'après le Corollaire 1.8, si $\mathrm{char}(k) \mid n$ alors $\Phi_{n,k}(X) = 1$. On supposera donc systématiquement que $\mathrm{char}(k) \nmid n$.

Remarque 2.2. Si k' est le sous-corps premier de k alors le corps de décomposition k'_n de P_n sur k' est un sous-corps de k_n. En outre, on a ($\mu_n(k'_n) = \mu_n(k_n)$ et) $\mu_n^\times(k'_n) = \mu_n^\times(k_n)$ donc $\Phi_{n,k'}(X) = \Phi_{n,k}(X) \in k'_n[X]$. Ainsi, il suffit d'étudier les cas $k = \mathbb{F}_p$ et $k = \mathbb{Q}$.

Propriété 2.3. *On rappelle que* $\mathrm{char}(k) \nmid n$. *Le polynôme* $\Phi_{n,k}$ *est unitaire et de degré* $\varphi(n)$.

Démonstration. Le caractère unitaire résulte de la définition, et pour le degré on applique la Proposition 1.10. □

Proposition 2.4. *On rappelle que* $\mathrm{char}(k) \nmid n$. *On a :*

$$X^n - 1 = \prod_{d|n} \Phi_{d,k}(X).$$

Démonstration. Puisque $\mu_n(k_n) = \sqcup_{d|n} \mu_d^\times(k_n)$, on a

$$\prod_{\zeta \in \mu_n(k_n)} (X - \zeta) = \prod_{d|n} \prod_{\zeta \in \mu_d^\times(k_n)} (X - \zeta),$$

et on trouve l'égalité annoncée. □

Remarque 2.5. En passant au degré (cf. Propriété 2.3), on retrouve la formule $n = \sum_{d|n} \varphi(d)$.

Remarque 2.6. En utilisant la formule d'inversion de Möbius dans le groupe abélien $k_n(X)^\times$, on trouve

$$\Phi_{n,k}(X) = \prod_{d|n} \left(X^{\frac{n}{d}} - 1\right)^{\mu(d)}.$$

Corollaire 2.7. *On rappelle que* $\mathrm{char}(k) \nmid n$ *et on désigne par* k' *le sous-corps premier de* k. *Alors* $\Phi_{n,k} \in k'[X]$, *de plus si* $k' = \mathbb{Q}$ *alors* $\Phi_{n,k} \in \mathbb{Z}[X]$.

Démonstration. Les deux assertions vont découler du fait que la division euclidienne de $X^n - 1$ par $\prod_{\substack{d|n \\ d<n}} \Phi_{d,k}$ donne exactement $\Phi_{n,k}$ et que l'algorithme de la division euclidienne ne fait pas sortir du corps des coefficients. Ainsi, on montre la première assertion par récurrence forte, en observant que $\Phi_{1,k} = X - 1$ et $X^n - 1$ sont dans $k'[X]$. Pour la deuxième, on modifie cette récurrence en remarquant que l'on divise par des polynômes unitaires (cf. Propriété 2.3) donc les divisions euclidiennes se passent dans $\mathbb{Z}[X]$. □

Corollaire 2.8. *On rappelle que* $\mathrm{char}(k) \nmid n$. *Si* $c : \mathbb{Z} \to k$ *est le morphisme canonique et si l'on désigne toujours par* c *son prolongement en le morphisme* $c : \mathbb{Z}[X] \to k[X]$, *alors*

$$\Phi_{n,k} = c\left(\Phi_{n,\mathbb{Q}}\right).$$

En particulier, $\Phi_{n,\mathbb{F}_p}$ *s'obtient en réduisant modulo* p *les coefficients de* $\Phi_{n,\mathbb{Q}}$.

Démonstration. Tout d'abord, remarquons que $c\left(\Phi_{n,\mathbb{Q}}\right)$ est bien défini puisque $\Phi_{n,\mathbb{Q}} \in \mathbb{Z}[X]$ par le corollaire précédent. Pour montrer l'égalité annoncée, on va encore utiliser une récurrence forte. On a bien $\Phi_{1,\mathbb{Q}} = X - 1$ et $\Phi_{1,k} = X - 1 = c(\Phi_{1,\mathbb{Q}})$. Supposons que $\Phi_{m,k} = c(\Phi_{m,\mathbb{Q}})$ pour tout $m < n$. On pose

$$P_k(X) \coloneqq \prod_{\substack{d|n \\ d<n}} \Phi_{d,k}.$$

D'après la remarque initiale on a $P_{\mathbb{Q}}(X) \in \mathbb{Z}[X]$, et par hypothèse de récurrence on a $c(P_{\mathbb{Q}}) = P_k$. Maintenant, d'après la relation de la Proposition 2.4, on peut écrire

$$X^n - 1 = \Phi_{n,\mathbb{Q}}(X) P_{\mathbb{Q}}(X).$$

Tous les polynômes sont à coefficients dans $\mathbb{Z}[X]$ donc on peut appliquer c et on trouve

$$X^n - 1 = c\left(\Phi_{n,\mathbb{Q}}(X)\right) P_k(X)$$

On conclut puisqu'alors, par la Proposition 2.4,

$$c\left(\Phi_{n,\mathbb{Q}}(X)\right) = \frac{X^n - 1}{P_k(X)} = \Phi_{n,k}.$$

□

On pourra donc écrire Φ_n à la place de $\Phi_{n,k}$. La Proposition 2.4 donne alors un algorithme de calcul de Φ_n. On trouve :

$$\begin{aligned}
\Phi_1 &= \prod_{\zeta \in \mu_1^\times(\mathbb{C})} (X - \zeta) && = X - 1,\\
\Phi_2 &= \frac{X^2-1}{\Phi_1} = \frac{X^2-1}{X-1} && = X + 1,\\
\Phi_3 &= \frac{X^3-1}{\Phi_1} = \frac{X^3-1}{X-1} && = X^2 + X + 1,\\
\Phi_4 &= \frac{X^4-1}{\Phi_1\Phi_2} = \frac{X^4-1}{(X-1)(X+1)} && = X^2 + 1,\\
\Phi_5 &= \frac{X^5-1}{\Phi_1} = \frac{X^5-1}{X-1} && = X^4 + X^3 + X^2 + X + 1,\\
\Phi_6 &= \frac{X^6-1}{\Phi_1\Phi_2\Phi_3} = \frac{X^6-1}{(X-1)(X+1)(X^2+X+1)} && = X^2 - X + 1,\\
\Phi_7 &= \frac{X^7-1}{\Phi_1} = \frac{X^7-1}{X-1} && = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1,\\
\Phi_8 &= \frac{X^8-1}{\Phi_1\Phi_2\Phi_4} = \frac{X^8-1}{(X-1)(X+1)(X^2+1)} && = X^4 + 1.
\end{aligned}$$

De façon générale, on a $\Phi_p = \sum_{i=0}^{p-1} X^i$ si p est premier.

3 Deux développements possibles

Théorème 3.1 (Wedderburn[1], Dickson (1905))**.** *Tout corps fini est commutatif.*

Idée de la preuve. (Cf. [Per, Théorème 4.9 page 82].) On fait opérer par conjugaison le groupe multiplicatif d'un corps non commutatif de cardinal q^n sur lui-même (où q est le cardinal du centre). Les cardinaux des orbites seront de la forme $\frac{q^n-1}{q^d-1}$ pour $d \mid n$, qui s'exprime donc, par la Proposition 2.4, comme un produit de polynômes cyclotomiques $\Phi_m(q)$ où m divise n mais pas d. La formule des classes donne alors $|\Phi_n(q)| \leq q - 1$, mais cette inégalité est impossible si l'on revient à la définition de $\Phi_n \in \mathbb{Q}[X]$. □

1. Joseph Henry Maclagan Wedderburn, 1882–1948.

Théorème 3.2. *Le polynôme $\Phi_n \in \mathbb{Z}[X]$ est irréductible.*

Idée de la preuve. (Cf. [Per, Théorème 4.10 page 82].) On montre que toutes les racines primitives n-ièmes de l'unité dans $\mathbb{Q}$ ont le même polynôme minimal et qu'il est dans $\mathbb{Z}[X]$, à coup de factorialité de $\mathbb{Z}[X]$ et de morphisme de Frobenius dans $\mathbb{F}_p[X]$ pour p premier ne divisant pas n. On conclut par un argument de degré. □

Corollaire 3.3. *Le polynôme Φ_n est irréductible sur $\mathbb{Q}$ et c'est le polynôme minimal sur $\mathbb{Q}$ de toute racine complexe primitive n-ième de l'unité. En particulier :*

- *si $P \in \mathbb{Q}[X]$ possède une racine complexe dans $\mu_n^\times(\mathbb{C})$ alors $\Phi_n \mid P$;*
- *si toutes les racines complexes de $P \in \mathbb{Q}[X]$ sont dans $\mu_n(\mathbb{C})$ alors P est un produit de polynômes cyclotomiques (à multiplication par un scalaire près).*

Remarque 3.4. Un polynôme $P \in \mathbb{Z}[X]$ est irréductible sur $\mathbb{Z}$ si et seulement s'il est irréductible sur $\mathbb{Q}$ et est de contenu (pgcd des coefficients) égal à 1. En particulier, si P est unitaire alors P est irréductible sur $\mathbb{Z}$ si et seulement s'il est irréductible sur $\mathbb{Q}$.

Corollaire 3.5. *Si $\zeta \in \mu_n^\times(\mathbb{C})$ alors $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$.*

Remarque 3.6. Pour $n \in \mathbb{N}^*$, soit $\zeta_n \in \mu_n^\times(\mathbb{C})$. Une extension de la forme $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est appelée *cyclotomique* ; son groupe de Galois est $(\mathbb{Z}/n\mathbb{Z})^\times$. Si m et n sont premiers entre eux, on peut montrer que $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$ (cf. [Per, Corollaire 4.12 page 83]). Plus généralement, en utilisant la correspondance de Galois on peut montrer que $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{\mathrm{pgcd}(m,n)})$, ainsi que $\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_{\mathrm{ppcm}(m,n)})$. Concluons cette remarque en énonçant le théorème de Kronecker–Weber : toute extension finie abélienne (c'est-à-dire, de groupe de Galois abélien) de $\mathbb{Q}$ est un sous-corps d'une extension cyclotomique.

Le Théorème 3.2 est faux sur $\mathbb{F}_p$, comme on va le montrer dans la Proposition 3.8

Lemme 3.7. *Si a et b ne sont pas des carrés dans $\mathbb{F}_p$ alors ab en est un.*

Démonstration. (Cf. [Per, III.2.*d*) page 74].) Le lemme est vrai si $p = 2$. Si maintenant $p \geq 3$, soit $\mathbb{F}_p^{\times 2}$ le groupe des carrés de $\mathbb{F}_p^\times$. L'application $\left|\begin{array}{ccc} \mathbb{F}_p^\times & \to & \mathbb{F}_p^{\times 2} \\ x & \mapsto & x^2 \end{array}\right.$ est un morphisme surjectif de groupes, de noyau $\mu_2(\mathbb{F}_p) = \{\pm 1\}$ qui est de cardinal 2 puisque $p \neq 2$. Ainsi, on a $\#\mathbb{F}_p^{\times 2} = \frac{\#\mathbb{F}_p^\times}{2}$ donc $\mathbb{F}_p^\times/\mathbb{F}_p^{\times 2} \simeq \mathbb{Z}/2\mathbb{Z}$. On conclut puisque si a et b ne sont pas des carrés alors $a, b \in \mathbb{F}_p^\times$ et leurs images dans $\mathbb{Z}/2\mathbb{Z}$ sont 1, donc l'image de $ab \in \mathbb{F}_p^\times$ est $1 + 1 = 0$ donc $ab \in \mathbb{F}_p^{\times 2}$. □

Proposition 3.8. *Le polynôme $\Phi_8 = X^4 + 1$ est réductible sur tous les $\mathbb{F}_p$.*

Démonstration. Rappelons que l'on a vu que $\Phi_8 = X^4 + 1$ à la fin de la Section 2. On va distinguer les cas selon si -1, 2 et -2 sont des carrés dans $\mathbb{F}_p$ ou non.

- Si -1 est un carré dans $\mathbb{F}_p$ alors on peut écrire $-1 = a^2$ avec $a \in \mathbb{F}_p$ donc

$$\Phi_8 = X^4 + 1 = X^4 - (-1) = \left(X^2\right)^2 - a^2 = (X^2 - a)(X^2 + a)$$

  est réductible.
- Si 2 est un carré dans $\mathbb{F}_p$ alors on peut écrire $2 = a^2$ avec $a \in \mathbb{F}_p$ donc

$$\Phi_8 = X^4 + 1 = (X^4 + 2X^2 + 1) - 2X^2 = (X^2 + 1)^2 - (aX)^2 = (X^2 - aX + 1)(X^2 + aX + 1),$$

  est réductible.

— Si -2 est un carré dans $\mathbb{F}_p$ alors on peut écrire $-2 = a^2$ avec $a \in \mathbb{F}_p$ donc

$$\Phi_8 = X^4+1 = (X^4-2X^2+1)-(-2)X^2 = (X^2-1)^2-(aX)^2 = (X^2-aX-1)(X^2+aX+1),$$

est réductible.

D'après le Lemme 3.7, on est au moins dans l'un des trois cas puisque $-2 = (-1) \times 2$. □

Remarque 3.9. Si l'on parle de ça, il peut être bon de savoir quand -1 est un carré dans $\mathbb{F}_p$, même dans $\mathbb{F}_q$. C'est le cas si et seulement si $q \equiv 1 \pmod 4$ (cf. [Per, Corollaire 2.13 page 75]).

On peut même donner un énoncé général quant à la réductibilité de Φ_n sur $\mathbb{F}_q$.

Théorème 3.10. *Soit q une puissance d'un nombre premier. On suppose que q et n sont premiers entre eux. Le polynôme Φ_n se décompose en un produit de $\frac{\varphi(n)}{r}$ polynômes irréductibles sur $\mathbb{F}_q$ distincts de même degré r, où r l'ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^\times$.*

Démonstration. (Cf. [Dem, Proposition 9.17 page 217].) Le fait que les facteurs irréductibles soient distincts vient du fait que Φ_n est sans facteur carré (cf. Lemme 1.5 et Proposition 2.4). On va maintenant montrer que tout facteur irréductible est de degré r, et on en déduira qu'il y a exactement $\frac{\varphi(n)}{r}$ facteurs irréductibles par passage au degré. Soit $P \in \mathbb{F}_q[X]$ un facteur irréductible de Φ_n, soit s son degré et soit ζ une racine de P (dans un corps de rupture). On a $\mathbb{F}_q(\zeta) \simeq \mathbb{F}_{q^s}$ donc $\zeta^{q^s-1} = 1$. Puisque ζ est également une racine de Φ_n, la racine ζ est d'ordre n donc n divise $q^s - 1$. Ainsi, on a $q^s = 1 \pmod n$ donc $r \mid s$. Réciproquement, puisque $\zeta^n = 1$ et que n divise $q^r - 1$ on a $\zeta^{q^r} = \zeta$. On en déduit que $\zeta \in \mathbb{F}_{q^r}$ (puisque $\mathbb{F}_{q^r}$ est le corps de décomposition de $X^{q^r} - X$ sur $\mathbb{F}_q$) et donc $\mathbb{F}_{q^s} \simeq \mathbb{F}_q(\zeta) \subseteq \mathbb{F}_{q^r}$, d'où $s \mid r$. □

Remarque 3.11. L'hypothèse q et n premiers entre eux est simplement l'hypothèse habituelle sur la caractéristique, qui devient ici $\mathrm{char}(\mathbb{F}_q) \nmid n$.

Corollaire 3.12. *Soit q une puissance d'un nombre premier. On suppose que q et n sont premiers entre eux. Le polynôme Φ_n est irréductible sur $\mathbb{F}_q$ si et seulement si q engendre $(\mathbb{Z}/n\mathbb{Z})^\times$.*

Exemple 3.13. Le groupe $(\mathbb{Z}/8\mathbb{Z})^\times$ n'est pas cyclique (on peut constater que tout élément est d'ordre 2 ou savoir que $(\mathbb{Z}/8\mathbb{Z})^\times \simeq (\mathbb{Z}/2\mathbb{Z})^2$) donc Φ_8 n'est jamais irréductible sur $\mathbb{F}_q$ si q n'est pas une puissance de 2. On retrouve donc un cas particulier de la Proposition 3.8.

Remarque 3.14. Si l'on parle de ça, il peut être bon (voire préférable) de savoir des choses sur l'irréductibilité dans $\mathbb{F}_q[X]$, par exemple :

— le nombre de polynômes irréductibles de degré fixé, voir par exemple [Per, Exercice 8) page 89] ;
— quelques critères, voir par exemple [Per, Théorèmes 3.9 page 78 et 3.14 page 79],
— un algorithme de décomposition, par exemple celui de Berlekamp : voir par exemple [Dem, §9.6.2] ;

ainsi que des choses sur quand est-ce que $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique, voir par exemple les Propositions 7.4 et 7.6 page 25 de [Per], et dans un deuxième temps la Proposition 7.10 page 26 (la règle explicite étant donnée au 3) du Théorème 4.14 page 84).

4 Carrés dans les corps finis

(Cf. [Per, III.2.d] et [Dem, §5.1].) Dans toute cette section, on désigne par p un nombre premier impair et par q une puissance de p. On désigne par $\mathbb{F}_q^{\times 2}$ l'ensemble des carrés de $\mathbb{F}_q^\times$. C'est un sous-groupe de $\mathbb{F}_q^\times$ (par commutativité). Les éléments de $\mathbb{F}_q^{\times 2}$ sont appelés *résidus quadratiques* modulo q.

Lemme 4.1. *On a* $\#\mathbb{F}_q^{\times 2} = \frac{q-1}{2}$.

Démonstration. Comme dans la preuve du Lemme 3.7, on considère l'application $f : \mathbb{F}_q^\times \to \mathbb{F}_q^{\times 2}$ définie par $f(x) \coloneqq x^2$. L'application f est un morphisme de groupes surjectif, de noyau l'ensemble des $x \in \mathbb{F}_q^\times$ vérifiant $x^2 = 1$. Puisque $p \neq 2$, ce noyau est de cardinal 2 et vaut $\{\pm 1\}$. Ainsi, par le premier théorème d'isomorphisme on a $\#\operatorname{im} f = \frac{\#\mathbb{F}_q^\times}{\#\ker f} = \frac{q-1}{2}$. □

Remarque 4.2. Si $p = 2$ alors le morphisme $\mathbb{F}_q^\times \to \mathbb{F}_q^\times$ donné par $x \mapsto x^2$ est injectif, donc bijectif par égalité des cardinaux. En particulier, tout élément possède une unique racine carrée. Rappelons que dans ce cas, l'application $\mathbb{F}_q \to \mathbb{F}_q$ donnée par $x \mapsto x^2$ est un morphisme de corps, appelé *morphisme de Frobenius*.

Proposition 4.3. *Pour tout* $x \in \mathbb{F}_q^\times$ *on a* $x \in \mathbb{F}_q^{\times 2} \iff x^{\frac{q-1}{2}} = 1$.

Démonstration. Soit Z l'ensemble des racines du polynôme $X^{\frac{q-1}{2}} - 1$ sur $\mathbb{F}_q$. On a $\#Z \leq \frac{q-1}{2}$ (car $\mathbb{F}_q$ est commutatif) et par le lemme et le théorème de Lagrange on a $Z \supseteq \mathbb{F}_q^{\times 2}$. On conclut que $Z = \mathbb{F}_q^{\times 2}$ par égalité des cardinaux. □

Corollaire 4.4 ([Per, Corollaire 2.13 p. 75])**.** -1 *est un carré dans* $\mathbb{F}_q$ *si et seulement si* $q \equiv 1 \pmod 4$.

Démonstration. Par la proposition précédente on a -1 est un carré dans $\mathbb{F}_q$ ssi $(-1)^{\frac{q-1}{2}} = 1$ dans F_q ssi $(-1)^{\frac{q-1}{2}} = 1$ dans $\mathbb{Z}$ (puisque $\operatorname{char}(\mathbb{F}_q) = p$ est impair) ssi $\frac{q-1}{2}$ est pair ssi $q \equiv 1 \pmod 4$. □

Application 4.5 ([Per, Application 2.16 p. 76])**.** Il existe une infinité de nombres premiers de la forme $4m + 1$ pour $m \in \mathbb{N}^*$.

Démonstration. Soit $n \geq 2$ et soit p un facteur premier (impair) de $n!^2 + 1$. Si $p \leq n$ alors $p \mid n!$ donc on obtient $p \mid 1$ ce qui est absurde, donc $p > n$ (on retrouve au passage le fait qu'il y a une infinité de nombres premiers). De plus, puisque $n!^2 = -1 \pmod p$ donc -1 est un carré modulo p donc $p \equiv 1 \pmod 4$ par le corollaire. On peut donc trouver de tels nombres premiers arbitrairement grand et il y en a donc une infinité. □

On s'intéresse maintenant au cas $q = p$.

Définition 4.6. Soit $x \in \mathbb{F}_p^\times$. On définit le *symbole de Legendre*[2] $\left(\frac{x}{p}\right)$ par

$$\left(\frac{x}{p}\right) \coloneqq \begin{cases} 1, & \text{si } x \text{ est un carré dans } \mathbb{F}_p, \\ -1, & \text{sinon.} \end{cases}$$

Par la Proposition 4.3 on obtient

$$\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}, \tag{4.7}$$

pour tout $x \in \mathbb{F}_p$. Par exemple, on a

$$\left(\frac{-3}{17}\right) \equiv (-3)^8 \equiv 9^4 \equiv 81^2 \equiv (-4)^2 \equiv 16 \equiv -1 \pmod{17},$$

donc -3 n'est pas un résidu quadratique modulo 17.

2. Adrien-Marie Legendre, 1752–1833.

Lemme 4.8. *L'application* $\mathbb{F}_p^\times \ni x \mapsto \left(\frac{x}{p}\right)$ *est l'unique morphisme non trivial* $\mathbb{F}_p^\times \to \{\pm 1\}$.

Démonstration. Le symbole de Legendre est un morphisme par (4.7), qui est non trivial par le Lemme 4.1. Si maintenant $f : \mathbb{F}_p^\times \to \{\pm 1\}$ est un morphisme non trivial, il est surjectif et donc $\#\ker f = \frac{\#\mathbb{F}_p^\times}{2} = \frac{p-1}{2}$. Ainsi, par le théorème de Lagrange les éléments de $\ker f$ sont des racines du polynôme $X^{\frac{p-1}{2}} - 1 \in \mathbb{F}_p[X]$ donc $\ker f \subseteq \mathbb{F}_p^{\times 2}$ par la Proposition 4.3. Par égalité des cardinaux on a $\ker f = \mathbb{F}_p^{\times 2}$, ce qui conclut la preuve. □

Proposition 4.9 ([Dem, Fin du §5.2.1 p. 119])**.** *On a*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{si } p \equiv \pm 1 \pmod 8, \\ -1, & \text{sinon } (p \equiv \pm 3 \pmod 8). \end{cases}$$

Démonstration. Considérons l'anneau $A := \mathbb{F}_p[X]/\langle X^4 + 1\rangle$ et notons α la classe de X. On a $\alpha^4 = -1$ par définition, ainsi α est inversible et $\alpha^{-1} = -\alpha^3$. Avec $\beta := \alpha + \alpha^{-1}$ on a

$$\beta^2 = \alpha^2 + \alpha^{-2} + 2 = \alpha^{-2}(\alpha^4 + 1) + 2 = 2.$$

Ainsi, par la Proposition 4.3, dans A on a

$$\left(\frac{2}{p}\right) = 2^{\frac{p-1}{2}} = \beta^{p-1} = \frac{\beta^p}{\beta}. \tag{4.10}$$

Notons que $\beta \in A^\times$ puisque $\beta^2 = 2 \in A^\times$ puisque $2 \in \mathbb{F}_p^\times$ puisque p est impair. En utilisant le morphisme de Frobenius en caractéristique p on a $\beta^p = (\alpha + \alpha^{-1})^p = \alpha^p + \alpha^{-p}$. Puisque p est impair, on obtient alors :

$$\alpha^p = \begin{cases} \alpha^{\pm 1}, & \text{si } p \equiv \pm 1 \pmod 8, \\ \alpha^{\pm 3} = -\alpha^{\mp 1}, & \text{sinon } (p \equiv \pm 3 \pmod 8), \end{cases}$$

donc, par (4.10),

$$\left(\frac{2}{p}\right) = \frac{\beta^p}{\beta} = \frac{\alpha^p + \alpha^{-p}}{\alpha + \alpha^{-1}} = \begin{cases} 1, & \text{si } p \equiv \pm 1 \pmod 8, \\ -1, & \text{sinon } (p \equiv \pm 3 \pmod 8), \end{cases}$$

ce qui achève la preuve, l'égalité correspondante $\left(\frac{2}{p}\right) = \pm 1$ étant également valable dans $\mathbb{Z}$ puisque $1 \neq -1$ dans A puisque $p \neq 2$. □

Concluons cette section par la célèbre *loi de réciprocité quadratique*, qui relie le fait que deux premiers impairs soient résidus quadratiques l'un l'autre. À l'aide de la proposition précédente, on peut alors calculer $\left(\frac{n}{p}\right)$ pour tout entier n.

Théorème 4.11 (Gauss[3])**.** *Si p et q sont deux nombres premiers impairs distincts alors*

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

Une démonstration de la loi de réciprocité quadratique compatible avec une dizaine de leçons peut se trouver dans [CaGe].

3. Carl Friedrich Gauss, 1777–1855.

Remarque 4.12. Pour effectivement calculer un symbole de Legendre, on utilise en fait le symbole de *Jacobi*, qui est une généralisation à n'importe quel « dénominateur ». Les règles de calcul restent les mêmes, mais pas la propriété d'être égal à 1 ssi le « numérateur » est un carré (sauf si le dénominateur est un nombre premier, auquel cas c'est un symbole de Legendre). En particulier, on peut utiliser la loi de réciprocité quadratique, qui permet de calculer le symbole de Legendre avec la même complexité que l'algorithme de division euclidienne.

Remarque 4.13. Le symbole de Jacobi peut être utilisé dans des tests de primalité (dans la même idée que ceux qui utilisent le petit théorème de Fermat, cf. (4.7)), par exemple les tests de Solovay–Strassen et Miller–Rabin.

Références

[CaGe] P. Caldero et J. Germoni, *Histoires hédonistes de groupes et de géométries*. Calvage & Mounet.

[Dem] M. Demazure, *Cours d'algèbre* (2e édition). Nouvelle bibliothèque mathématique, Cassini.

[Gou] X. Gourdon, *Algèbre* (2e édition). Les maths en tête, Ellipses.

[Per] D. Perrin, *Cours d'algèbre*. CAPES / Agrégation, Ellipses.