Cyclotomie

Table des matières

Références

[Ale99] Michel Alessandri : *Thème de géométrie. Groupes en situation géométrique.* Dunod, 1999.

[Com03] François Combes : *Algèbre et géométrie.* Bréal, 2003.

[Dem09] Michel Demazure : *Cours d'algèbre.* Cassini, 2009.

[FG95] Serge Francinou et Hervé Gianella : *Exercice de mathématiques pour l'agrégation, algèbre 1.* Masson, 1995.

[FGN08] Serge Francinou, Hervé Gianella et Serge Nicolas : *Oraux X-ENS, algèbre 1.* Cassini, 2008.

[FGN09] Serge Francinou, Hervé Gianella et Serge Nicolas : *Oraux X-ENS, algèbre 2.* Cassini, 2009.

[HL12] David Hernandez et Yves Laszlo : *Introduction à la théorie de Galois.* Editions Ecole Polytechnique, 2012.

[HW07] Godfrey Harold Hardy et Edward Maitland Wright : *Introduction à la théorie des nombres.* Vuibert-Springer, 2007.

[Per96] Daniel Perrin : *Cours d'algèbre.* Ellipses, 1996.

[Ser70] Jean-Pierre Serre : *Cours d'arithmétique.* puf, 1970.

Commençons par un peu d'étymologie ; cyclotomie est construit d'après les racines grecs κύκλος et τομός [1], soit littéralement « le cercle coupé ».

Pour un corps k et un entier $n \in \mathbb{N}_*$, l'ensemble des *racines $n^{èmes}$ de l'unité* dans k, *i.e.* les racines du polynôme $X^n - 1$ dans k, sera noté $\mu_n(k)$:

$$\mu_n(k) = \{\zeta \in k \ / \ \zeta^n = 1\}.$$

$\mu_n(k)$ est un sous-groupe fini de k^*, donc cyclique, d'ordre inférieur à n. On notera $\mu_n^*(k)$ le sous-ensemble des *racines primitives $n^{èmes}$ de l'unité* de $\mu_n(k)$, *i.e.* les générateurs de ce groupe. En l'absence de précision, ζ_n désignera une racine primitive $n^{\text{ème}}$ de l'unité.

1 Cyclotomie dans $\mathbb{C}$ [Com03, Per96]

Lorsque k est le corps des nombres complexes $\mathbb{C}$, la situation est bien connue, précisément

$$\mu_n(\mathbb{C}) = \left\{1, \zeta, \zeta^2, \dots, \zeta^{n-1}\right\} \quad \text{et} \quad \mu_n^*(\mathbb{C}) = \left\{\zeta^k \ / \ \operatorname{pgcd}(k,n) = 1\right\}, \text{ où } \zeta = \exp\left(\frac{2i\pi}{n}\right).$$

$\mu_n(\mathbb{C})$ est donc un groupe cyclique d'ordre n et, pour tout diviseur d de n, l'unique sous-groupe d'ordre d de $\mu_n(\mathbb{C})$ est $\mu_d(\mathbb{C})$. Ainsi, en classant les éléments de $\mu_n(\mathbb{C})$ selon leur ordre, on obtient la partition suivante :

$$\mu_n(\mathbb{C}) = \bigsqcup_{d|n} \mu_d^*(\mathbb{C}),$$

où $\mu_d^*(\mathbb{C})$ est de cardinal $\varphi(d)$, où φ désigne l'indicateur d'Euler. En particulier, on a $n = \sum_{d|n} \varphi(d)$.

Définition 1.1 Le polynôme unitaire $\prod_{\zeta \in \mu_n^*(\mathbb{C})} (X - \zeta)$, noté Φ_n, est appelé le $n^{ème}$ *polynôme cyclotomique*. Son degré est $\varphi(n)$.

Exemples 1.2 $\Phi_1 = X - 1$, car $\mu_1^*(\mathbb{C}) = \{1\}$. $\Phi_2 = X + 1$, car $\mu_2^*(\mathbb{C}) = \{-1\}$.
$\Phi_3 = X^2 + X + 1$, car $\mu_3^*(\mathbb{C}) = \{j, j^2\}$. $\Phi_4 = X^2 + 1 = \Phi_2(X^2)$, car $\mu_4^*(\mathbb{C}) = \{i, i^3\}$.
$\Phi_5 = \frac{X^5-1}{X-1} = X^4 + X^3 + X^2 + X + 1$, car $\mu_5^*(\mathbb{C}) = \mu_5(\mathbb{C}) \setminus \{1\}$.
$\Phi_6 = X^2 - X + 1 = \Phi_3(-X)$, car $\mu_6^*(\mathbb{C}) = \{-j, -j^2\}$.
$\Phi_7 = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$, car $\mu_7^*(\mathbb{C}) = \mu_7(\mathbb{C}) \setminus \{1\}$.
$\Phi_8 = \frac{X^8-1}{X^4-1} = X^4 + 1 = \Phi_2(X^4)$, car $\mu_8^*(\mathbb{C}) = \mu_8(\mathbb{C}) \setminus \mu_4(\mathbb{C})$.

Proposition 1.3 Pour $n \in \mathbb{N}_*$, on a

$$X^n - 1 = \prod_{d|n} \Phi_d \tag{1}$$

et le $n^{\text{ème}}$ polynôme cyclotomique Φ_n est unitaire à coefficients entiers.

Pour $n \geqslant 2$, $\Phi_n(0) = 1$ et $X^{\varphi(n)} \Phi_n\left(\frac{1}{X}\right) = \Phi_n(X)$.

Pour $n \geqslant 3$, $\Phi_n(x) > 0$, pour tout $x \in \mathbb{R}$, et $\Phi_n(x) > (|x| - 1)^{\varphi(n)}$, pour tout $x \in \mathbb{R}, |x| > 1$.

1. Lire kuklos et tomos.

Démonstration. L'égalité 1 résulte simplement de la décomposition $\mu_n(\mathbb{C}) = \bigsqcup_{d|n} \mu_d^*(\mathbb{C})$. Clairement $\Phi_1 \in \mathbb{Z}[X]$ et est unitaire, on raisonne alors par récurrence, pour $n \in \mathbb{N}_*$, pour montrer que $\Phi_n \in \mathbb{Z}[X]$. Précisément, on utilise l'unicité du reste et du quotient de la division euclidienne dans l'anneau euclidien $\mathbb{C}[X]$ et la possibilité de diviser $X^n - 1$ dans $\mathbb{Z}[X]$ par le polynôme unitaire $\prod_{d|n, d\neq n} \Phi_d \in \mathbb{Z}[X]$.

On a $\Phi_2(0) = 1$. Pour $n \geqslant 3$, pour tout $\zeta \in \mu_n^*(\mathbb{C})$, $\overline{\zeta} \in \mu_n^*(\mathbb{C})$, en outre $\mu_n^*(\mathbb{C}) \cap \mathbb{R} = \emptyset$, ainsi on peut partitionner $\mu_n^*(\mathbb{C}) = \bigsqcup_{i\in I} \left\{\zeta_i, \overline{\zeta_i}\right\}$ par paires de conjugués. On en déduit $\Phi_n(x) = \prod_{i\in I} |x - \zeta_i|^2 > 0$, pour $x \in \mathbb{R}$, et $\Phi_n(0) = \prod_{i\in I} \zeta_i\overline{\zeta_i} = 1$. De plus, pour $x > 1$, $|x - \zeta_i| > x - 1$ et, pour $x < -1$, $|x - \zeta_i| > |x| - 1$ (faire un dessin !), d'où la dernière assertion.

Soit $P_n = X^{\varphi(n)}\Phi_n\left(\frac{1}{X}\right)$, pour $n \geqslant 2$. Ayant $\deg \Phi_n = \varphi(n)$ et $\Phi_n(0) = 1$, P_n est de même degré et unitaire. En outre $\zeta \longmapsto \frac{1}{\zeta} = \overline{\zeta}$ induit une bijection sur $\mu_n^*(\mathbb{C})$ qui est l'ensemble des racines de Φ_n et P_n. Ainsi $P_n \mid \Phi_n$ et, étant unitaires et de même degré, ils sont égaux. *QED*

Remarque 1.4 La formule 1 permet le calcul par récurrence des Φ_n. Pour d'autres formules concernant les polynômes cyclotomiques se reporter à l'exercice 4.1.

Théorème 1.5 Le $n^{\text{ème}}$ polynôme cyclotomique Φ_n est irréductible sur $\mathbb{Q}$ et donc sur $\mathbb{Z}$.

Démonstration. On donne ici la preuve de van der Waerden. Considérons P un facteur irréductible unitaire de Φ_n sur $\mathbb{Q}$, $P \in \mathbb{Z}[X]$ dans la mesure où $\mathbb{Z}$ est un anneau factoriel, $\mathbb{Q} = \mathrm{Frac}(\mathbb{Z})$ et Φ_n est unitaire. Montrer que $P = \Phi_n$ revient à montrer que tous les éléments de $\mu_n^*(\mathbb{C})$ sont des racines de P et il suffit pour cela d'établir que, étant donné ζ une racine de P et p un nombre premier ne divisant pas n, $P(\zeta^p) = 0$. Raisonnons par l'absurde, en supposant que pour un tel ζ et un tel p, $P(\zeta^p) \neq 0$. Il existe $Q \in \mathbb{Z}[X]$ tel que $\Phi_n = PQ$ et ζ^p est racine de Q, donc ζ de $R = Q(X^p)$. Ainsi P et R ont une racine commune, donc un pgcd (unitaire à coefficients entiers) distinct de 1. En particulier les polynômes $\overline{P}$ et $\overline{R}$, obtenus par réduction modulo p, ne sont pas premiers entre eux. Il en va donc de même de $\overline{P}$ et $\overline{Q}$, puisque $\overline{R} = \overline{Q}^p$. En conséquence de quoi $\overline{\Phi_n} = \overline{PQ}$ et donc $X^n - 1$ ont des racines multiples dans $\overline{\mathbb{F}_p}$. Or, par hypothèse sur $p \nmid n$, $X^n - 1$ est séparable sur $\mathbb{F}_p$, d'où une contradiction.

QED

On en déduit en particulier, pour ζ_n une racine primitive $n^{\text{ème}}$ de l'unité dans $\mathbb{C}$, le degré de l'extension, dite *cyclotomique*, $\mathbb{Q}(\zeta_n)/\mathbb{Q}$.

Corollaire 1.6 $\pi_{\zeta_n,\mathbb{Q}} = \Phi_n$ et $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

Corollaire 1.7 Si $\mathrm{pgcd}(m, n) = 1$, alors $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$.

Démonstration. La démonstration du corollaire repose sur le lemme suivant :

Lemme 1.8 Si K et L sont deux corps intermédiaires de l'extension finie M/k, alors $[KL : L] \leqslant [K : k]$.

Démonstration. Il suffit de remarquer que si $(x_i)_{i\in I}$ est une base de K sur k, alors $(x_i)_{i\in I}$ engendre KL sur L.

QED

Nous sommes maintenant en mesure de démontrer le corollaire. Posons $k = \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)$. On saît que $\varphi(m) = [\mathbb{Q}(\zeta_m) : \mathbb{Q}] \geqslant [\mathbb{Q}(\zeta_m) : k] \geqslant [\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n)]$, d'après le lemme. Comme $\operatorname{pgcd}(m,n) = 1$, $\zeta_m\zeta_n$ est une racine primitive $mn^{\text{ème}}$ de l'unité et l'inclusion $\mathbb{Q}(\zeta_m\zeta_n) \subset \mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n)$, valable généralement, est une égalité (faire un dessin du treillis des extensions). Alors

$$[\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n)] = \frac{[\mathbb{Q}(\zeta_m\zeta_n) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_n) : \mathbb{Q}]} = \frac{\varphi(mn)}{\varphi(n)} = \varphi(m).$$

Par conséquent $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = [\mathbb{Q}(\zeta_m) : k]$, d'où la conclusion.

QED

Apparté - L'extension cyclotomique $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. Soit ζ_n une racine primitive $n^{\text{ème}}$ de l'unité dans $\mathbb{C}$, dans le cadre de la théorie de Galois, on peut énoncer la proposition suivante.

Proposition 1.9 L'extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est galoisienne de degré $\varphi(n)$ et le caractère cyclotomique

$$\chi : \operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*,$$

défini comme l'unique application telle que, pour tout $f \in \operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ et pour tout $\zeta \in \mu_n(\mathbb{C})$, $f(\zeta) = \zeta^{\chi(f)}$, réalise un isomorphisme de groupes.

Démonstration. $\mathbb{Q}(\zeta_n)$ est le corps de décomposition dans $\mathbb{C}$ du polynôme séparable $X^n - 1$. Ainsi l'extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est galoisienne et son degré a été donné au corollaire 1.6. Pour l'isomorphisme donné par χ, on pourra consulter [HL12, §6.2].

QED

On peut alors, à l'aide de la correspondance de Galois, généraliser le résultat du corollaire 1.7.

Proposition 1.10 [HL12, Prop. 6.4.1] Pour $m, n \in \mathbb{N}$, on a

$$\mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_{\operatorname{ppcm}(m,n)}) \quad \text{et } \mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{\operatorname{pgcd}(m,n)}).$$

Notons également le résultat important de théorie de Galois suivant, dont une démonstration pour le cas quadratique est proposée à l'exercice 4.9.

Théorème 1.11 - Kronecker-Weber. Toute extension abélienne finie de $\mathbb{Q}$ est un sous-corps d'une extension cyclotomique.

2 Cyclotomie en caractéristique quelconque [Com03, FG95]

Pour un corps quelconque, on peut se demander sous quelles conditions ce dernier contient-il des racines primitives $n^{\text{èmes}}$ de l'unité (cf. proposition 2.1) et ce qu'il advient de l'irréductibilité de Φ_n en caractéristique positive (cf. théorème 2.3) ?

Soit k un corps de caractéristique p quelconque et f l'homomorphisme d'anneaux

$$f : \left| \begin{array}{ccc} \mathbb{Z}[X] & \longrightarrow & k[X] \\ \sum_{i\in\mathbb{N}} a_i X^i & \longmapsto & \sum_{i\in\mathbb{N}} \overline{a_i} X^i \end{array} \right.$$

où $\overline{a_i}$ désigne la classe de a_i modulo p. Notons que si p est nul, f n'est rien d'autre que le morphisme d'inclusion.

Pour $n \in \mathbb{N}_*$, on notera $\Phi_{n,k}$ l'image de Φ_n par f, qui est donc un élément de $k_0[X]$, où k_0 désigne le sous-corps premier de k. Puisque Φ_n est unitaire, $\Phi_{n,k}$ est unitaire et de même degré $\varphi(n)$ que Φ_n. En outre, f étant un homomorphisme d'anneaux, la relation suivante subsiste dans $k[X]$:

$$X^n - 1 = \prod_{d|n} \Phi_{d,k}. \tag{2}$$

Proposition 2.1 Soit k un corps et $n \in \mathbb{N}_*$, s'équivalent :

(i) il existe un sous-groupe de k^* d'ordre n ;

(ii) le polynôme $X^n - 1$ est scindé simple dans k ;

(iii) $\Phi_{n,k}$ a une racine dans k qui est une racine simple de $X^n - 1$;

(iv) $\Phi_{n,k}$ a une racine dans k et la caractéristique de k ne divise pas n.

Le cas échéant, k^* possède un unique sous-groupe d'ordre n, qui correspond à l'ensemble des racines de $X^n - 1$ et est cyclique. Ses $\varphi(n)$ générateurs sont les racines de $\Phi_{n,k}$. Pour tout diviseur d de n, les éléments d'ordre d de ce groupe, et donc de k^*, sont les racines de $\Phi_{d,k}$.

Démonstration. (i) ⇒ (ii) Supposons qu'il existe un sous-groupe G d'ordre n dans k^*, alors, d'après le th. de Lagrange, les éléments de G sont les n racines distinctes de $X^n - 1$ dans k.

(ii) ⇒ (iii) Soit $a_1, \dots a_n$ les n racines distinctes de $X^n - 1$ dans k. Pour tout i, il existe un entier $d|n$ tel que $\Phi_{d,k}(a_i) = 0$. L'égalité $n = \sum_{d|n} \varphi(d)$ implique alors que $\Phi_{n,k}$ soit scindé dans k.

(iii) ⇔ (iv) Soit a une racine de $\Phi_{n,k}$ dans k et donc de $X^n - 1$. a est racine simple de $X^n - 1$ si et seulement si $na^{n-1} \neq 0$, soit $n \neq 0$, puisque $a \neq 0$, ce qui signifie que n n'est pas un multiple de la caractéristique de k.

(iii) ⇒ (i) Soit a une racine de $\Phi_{n,k}$ dans k et m son ordre dans le groupe k^*, qui divise n. Si m était un diviseur strict de n, alors, ayant la factorisation $X^n - 1 = \prod_{d|n} \Phi_{d,k}$, a serait une racine multiple de $X^n - 1$, ce qui est exclu. Ainsi $\langle a \rangle$ est un sous-groupe d'ordre n de k^*.

Le cas échéant, les racines de $X^n - 1$ forment donc l'unique sous-groupe d'ordre n de k^*. En outre, $X^n - 1$ étant scindé simple, $\Phi_{n,k}$ admet $\varphi(n)$ racines distinctes qui engendrent chacune un groupe cyclique d'ordre n, ce sont donc les $\varphi(n)$ générateurs de l'unique sous-groupe (cyclique) d'ordre n de k^*. Pour tout diviseur d de n, cela s'applique au polynôme $X^d - 1$ qui divise $X^n - 1$ et est donc scindé simple dans k.

QED

Remarque 2.2 Lorsque $p \mid n$, notant $n = p^r m$ avec $(p, m) = 1$, on a $X^n - 1 = (X^m - 1)^{p^r}$ dans $k[X]$. Ainsi, $\mu_n(\overline{k}) = \mu_m(\overline{k})$ et il ne peut y avoir de racine primitive $n^{\text{ème}}$ dans k ou ses extensions algébriques.

Théorème 2.3 Soit n un entier $\geqslant 2$ premier à q, puissance d'un nombre premier p, et r l'ordre de la classe de q dans $(\mathbb{Z}/n\mathbb{Z})^*$. $\Phi_{n,\mathbb{F}_p}$ se décompose en un produit de polynômes unitaires irréductibles distincts de même degré r dans $\mathbb{F}_q[X]$.

Démonstration. Par hypothèse, $X^n - 1$ est séparable sur $\mathbb{F}_p$, d'après la proposition précédente, par conséquent $\Phi_{n,\mathbb{F}_p}$ s'écrit comme un produit de polynômes irréductibles distincts $P_1, \dots P_s$ dans $\mathbb{F}_q[X]$. Pour $i \in [\![1, n]\!]$, les racines de P_i dans une extension de $\mathbb{F}_q$ sont des racines primitives $n^{\text{èmes}}$ de l'unité. Comme le groupe multiplicatif d'une extension de degré m de $\mathbb{F}_q$ est cyclique d'ordre $q^m - 1$, $\mathbb{F}_{q^m}$ contient les racines primitives $n^{\text{èmes}}$ de l'unité si et seulement si $q^m \equiv 1 \mod n$. Les P_i sont donc les polynômes minimaux d'éléments de $\mathbb{F}_q$ de degré r, d'où le résultat.

QED

Remarque 2.4 Avec les notations du théorème, $\Phi_{n,\mathbb{F}_p}$ est scindé simple sur $\mathbb{F}_{q^r}$.

On a en outre les liens suivants entre l'ordre n et le degré r sur $\mathbb{F}_q$ d'un élément $\alpha \in \overline{\mathbb{F}_q}$ non nul : si r est donné, $n \mid q^r - 1$ et si n est donné, r est le plus petit entier tel que $q^r \equiv 1 \mod n$. En particulier, $\mathbb{F}_{q^r}$ est la plus petite extension de $\mathbb{F}_q$ contenant des (les !) racines primitives $n^{\text{èmes}}$ de l'unité.

Corollaire 2.5 $\Phi_{n,\mathbb{F}_p}$, pour n premier à p, est irréductible sur $\mathbb{F}_q$, avec q une puissance de p, si et seulement si la classe de q engendre $(\mathbb{Z}/n\mathbb{Z})^*$ (auquel cas ce dernier est cyclique !).

Exemple 2.6 $\Phi_8 = X^4 + 1$ est réductible sur $\mathbb{F}_p$ pour tout nombre premier p, tandis qu'il est irréductible sur $\mathbb{Q}$, puisque notamment $(\mathbb{Z}/8\mathbb{Z})^* \simeq (\mathbb{Z}/2\mathbb{Z})^2$.

Exercice 2.7 - Construction de $\mathbb{F}_{16}$. $\mathbb{F}_{16}$ est le corps de décomposition de $X^{16} - X$ sur $\mathbb{F}_2$. Or on a la factorisation suivante sur $\mathbb{F}_2$:

$$X^{16} - X = X\left(X^{15} - 1\right) = X\Phi_1\Phi_3\Phi_5\Phi_{15}.$$

En outre, la classe de 2 est un générateur de $(\mathbb{Z}/3\mathbb{Z})^*$ et de $(\mathbb{Z}/5\mathbb{Z})^*$, ainsi Φ_3 et Φ_5 sont irréductibles sur $\mathbb{F}_2$. En revanche, la classe de 2 est d'ordre 4 dans $(\mathbb{Z}/15\mathbb{Z})^*$ qui est d'ordre $\varphi(15) = \varphi(3)\varphi(5) = 8$, ainsi Φ_{15} se factorise en un produit de deux polynômes irréductibles de degré 4 sur $\mathbb{F}_2$. Précisément $\Phi_{15} = \left(X^4 + X + 1\right)\left(X^4 + X^3 + 1\right)$. Finalement, on aboutit à la factorisation complète suivante :

$$X^{16} - X = X\left(X - 1\right)\left(X^2 + X + 1\right)\left(X^4 + X^3 + X^2 + X + 1\right)\left(X^4 + X + 1\right)\left(X^4 + X^3 + 1\right).$$

En particulier, les trois polynômes irréductibles de degré 4 qui apparaissent dans cette factorisation sont les 3 polynômes irréductibles de degré 4 sur $\mathbb{F}_2$, qui permettent chacun de réaliser (de façon effective) $\mathbb{F}_{16}$ comme corps de rupture de $\mathbb{F}_2$. L'avantage d'utiliser un des deux facteurs de Φ_{15} réside dans le fait que la classe de X dans le corps de rupture obtenu sera un générateur du groupe multiplicatif de $\mathbb{F}_{16}$.

Proposition 2.8 Si p est un diviseur de n, $\Phi_{n,\mathbb{F}_p}$ est réductible sur $\mathbb{F}_p$, sauf, éventuellement, si on a $p=2$ et $n=2m$, avec m impair. Précisément, on a pour tout $i \in \mathbb{N}_*$, $\Phi_{p^i m,\mathbb{F}_p} = \left(\Phi_{m,\mathbb{F}_p}\right)^{\varphi\left(p^i\right)}$.

Démonstration. La dernière égalité résulte de la dernière formule de l'exercice 4.1 et de l'application du Frobenius. Si $\Phi_{n,\mathbb{F}_p}$ est irréductible sur $\mathbb{F}_p$, on a donc $p=2$ et $n=2m$, avec m impair.

QED

Remarque 2.9 Dans le cas $p=2$ et $n=2m$, avec m impair, puisque $\Phi_{n,\mathbb{F}_2} = \Phi_{m,\mathbb{F}_2}$, d'après l'exercice 4.1, on est ramené au théorème 2.3.

3 Applications

3.1 Un pas vers le théorème de la progression arithmétique Dirichlet [Com03]

Proposition 3.1 - Cas particulier du théorème de Dirichlet. Considérons un entier $a \geqslant 2$.

(i) Pour tout $n \in \mathbb{Z} \setminus \{-1,0,1\}$, les facteurs premiers de $\Phi_a(n)$ sont soit des facteurs premiers de a, soit de la forme $ka+1$, où $k \in \mathbb{N}$.

(ii) Il existe une infinité de nombres premiers de la forme $ka+1$.

(iii) Pour tout nombre premier de la forme $ka+1$, il existe $n \in \mathbb{Z}$ tel que ce nombre soit facteur de $\Phi_a(n)$.

Démonstration. (i) D'après la proposition 1.3, $\Phi_a(n) \in \mathbb{Z}$ et $\Phi_a(n) \geqslant 2$. Soit p un facteur premier de $\Phi_a(n)$, on a $\Phi_a(\overline{n}) = 0$ dans $\mathbb{F}_p$ et $\overline{n}$ est racine de $X^a - 1$. Si $p \nmid a$, alors, d'après la proposition 2.1, $\overline{n}$ engendre un sous-groupe cyclique d'ordre a de $\mathbb{F}_p^*$, ainsi $a \mid p-1$ (th. de Lagrange), d'où la conclusion.

(ii) Soit $F = \{q_1, \ldots, q_r\}$ l'ensemble des facteurs premiers de a et supposons que l'ensemble E des nombres premiers de la forme $ka+1$ soit fini, d'éléments $p_1, \ldots, p_s$. Considérons $n = q_1 \ldots q_r p_1 \ldots p_s$, d'après la proposition 1.3, $\Phi_a(n) \geqslant 2$ et $\Phi_a(n) \equiv 1 \mod p_i$ ou q_j, pour tout i et j (car $\Phi_a(0) = 1$). Soit q un facteur premier de $\Phi_a(n)$, on a $\Phi_a(n) \equiv 0 \mod q$, donc $q \notin E$ et $\notin F$, ce qui est absurde d'après (i).

(iii) Soit p un nombre premier de la forme $ka+1$, alors $a \mid p-1 = |\mathbb{F}_p^*|$. Il existe donc un unique sous-groupe cyclique de $\mathbb{F}_p^*$ d'ordre a. Soit $\overline{n}$ un générateur de ce sous-groupe, d'après la proposition 2.1, on a $\Phi_a(\overline{n}) = 0$, ce qui exprime que p divise $\Phi_a(n)$.

QED

À l'aide de fonctions de la variable complexe, on démontre le résultat plus général suivant (cf. par exemple [Ser70, Chap. VII]) :

Théorème 3.2 - Théorème de la progression arithmétique de Dirichlet – 1837.
Si a et b sont deux entiers naturels premier entre eux, alors il existe une infinité de nombres premiers congrus à a modulo b. Précisément, la densité naturelle de cet ensemble de nombres est $1/\varphi(b)$.

Corollaire 3.3 Pour $n \in \mathbb{Z}$ pair, tout facteur premier de $n^{2^k}+1$ est de la forme $m2^{k+1}+1$.

Démonstration. $\Phi_{2^{k+1}}(X) = \Phi_2\left(X^{2^k}\right) = X^{2^k} + 1$. D'après la proposition, les facteurs premiers de $\Phi_{2^{k+1}}(n) = n^{2^k} + 1$ sont soit de la forme $m2^{k+1} + 1$, soit des diviseurs de 2^{k+1}, ce qui est exclu, puisque $n^{2^k} + 1$ est impair pour n pair.

QED

Ce corollaire s'applique notamment au nombres de Fermat de la forme $F_k = 2^{2^k} + 1$.

Exercice 3.4 - Euler. Montrer que 641 divise F_5.

Exercice 3.5 Montrer que pour tout $k \in \mathbb{N}_*$, il existe une infinité de nombres premiers dont l'écriture décimale contient k zéros consécutifs.

3.2 Constructibilité des polygones réguliers

Pour les définitions et résultats relatifs à la notion de nombres constructibles à la règle et au compas, on renvoie à [Com03, §13.5] ou [HL12, §0.1 et §6.5]. Concernant cette question de la constructibilité, on a le résultat classique suivant.

Théorème 3.6 - Wantzel. Un nombre complexe z est constructible si et seulement s'il existe une suite finie de corps $L_0 = \mathbb{Q} \subset L_1 \subset \cdots \subset L_n$ telle que $z \in L_n$ et $[L_{i+1} : L_i] = 2$, pour tout $1 \leqslant i \leqslant n-1$.

Ce théorème se reformule, modulo la correspondance de Galois et un résultat classique de théorie des groupes qui affirme qu'un p-groupe fini admet des sous-groupes distingués pour tous les ordres possibles, en la proposition plus maniable suivante.

Proposition 3.7 Soit $z \in \mathbb{C}$ algébrique (sur $\mathbb{Q}$) et K le corps de décomposition de $\pi_{z,\mathbb{Q}}$. z est constructible si et seulement si $[K : \mathbb{Q}]$ est une puissance de 2.

Nous sommes alors en mesure d'établir le résultat suivant.

Théorème 3.8 - Gauß-Wantzel. Le polygone régulier à n côtés est constructibles si et seulement si n est le produit d'une puissance de 2 et de nombres premiers de Fermat distincts.

Démonstration. Le polygone régulier à n côtés est constructibles si et seulement si $\zeta_n = e^{2i\pi/n}$ l'est. Or le corps de décompositon de $\pi_{\zeta_n,\mathbb{Q}} = \Phi_n$ est $\mathbb{Q}(\zeta_n)$, ainsi, en vertu de la proposition 3.7, ζ_n est constructible si et seulement si $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ est une puissance de 2. Si $n = 2^{n_0}\prod_{i=1}^{r} p_i^{n_i}$, avec p_i premiers impairs distincts, alors

$$\varphi(n) = 2^{n_0-1}\prod_{i=1}^{r}(p_i - 1)p_i^{n_i-1}.$$

Si $\varphi(n)$ est une puissance de 2, nécessairement $n_i = 1$ et $p_i = 1 + 2^{m_i}$, pour tout $i \geqslant 1$. En outre, si $m_i = ab$, avec a impair et b une puissance de 2, $1 + 2^b \mid p_i$, ainsi $p_i = 1 + 2^b$ et $m_i = b$. La réciproque est claire.

QED

Exemple 3.9 Les premiers nombres de Fermat premiers sont $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ et $F_4 = 65537$. En revanche, F_5 ne l'est pas (cf. exercice 3.4). Les premiers polygones réguliers constructibles sont donc ceux à 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, ... côtés.

Exemple 3.10 - Construction du pentagone régulier. Soit $\zeta = e^{2i\pi/5} = \cos(2\pi/5) + i\sin(2\pi/5)$. Alors $x = 2\cos(2\pi/5) = \zeta + \overline{\zeta}$ et

$$0 = \Phi_5(\zeta) = \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = \zeta^2\left(\zeta^2 + \overline{\zeta}^2 + \zeta + \overline{\zeta} + 1\right) = \zeta^2\left(x^2 + x - 1\right).$$

Ainsi x est la racine positive de $X^2 + X - 1$, à savoir $\frac{\sqrt{5}-1}{2}$, et $\cos(2\pi/5) = \frac{\sqrt{5}-1}{4}$. On déduit aisément de cette formule une construction du pentagone régulier, qui était déjà connue de Ptolémée (1^{er} siècle de notre ère).

3.3 Ordre des éléments de $\mathrm{GL}_n(\mathbb{Q})$ [FGN09, ex. 3.17 et 3.18 p. 199] et [Ale99, Thème II]

On souhaite caractériser, pour $n \in \mathbb{N}_*$ donné, les ordres possibles des éléments de $\mathrm{GL}_n(\mathbb{Q})$. En particulier, nous allons établir que l'ordre d'un éléments d'ordre fini est majoré en fonction de n. On note $\Omega(n)$ l'ensemble des ordres des éléments de $\mathrm{GL}_n(\mathbb{Q})$.

Pour $n = 1$, $\mathrm{GL}_1(\mathbb{Q}) \simeq \mathbb{Q}_*$, ainsi $\Omega(1) = \{1, 2, \infty\}$. Dorénavant, on supposera $n \geqslant 2$. Dans $\mathrm{GL}_n(\mathbb{Q})$ I_n et $-I_n$ sont respectivement d'ordre 1 et 2 et la matrice par blocs suivante est d'ordre infini :

$$\begin{pmatrix} 1 & 1 & \\ 0 & 1 & \\ & & I_{n-2} \end{pmatrix}.$$

Ainsi $\{1, 2, \infty\} \subset \Omega(n)$.

Proposition 3.11 $r \in \Omega(n) \setminus \{+\infty\}$ si et seulement s'il existe des entiers $1 \leqslant d_1 < \cdots < d_k$ tels que $\mathrm{ppcm}(d_i)_{1\leqslant i\leqslant k} = r$ et $\displaystyle\sum_{1\leqslant i\leqslant k} \varphi(d_i) \leqslant n$.

Démonstration. Soit $M \in \mathrm{GL}_n(\mathbb{Q})$ un élément d'ordre r. $X^r - 1$ annule M, ainsi $\pi_M \mid X^r - 1$ (et M est diagonalisable sur $\mathbb{C}$). Or, vu la décomposition en irréductibles sur $\mathbb{Q}$ de $X^r - 1 = \prod_{d|r} \Phi_d$, il existe des entiers $1 \leqslant d_1 < \cdots < d_k$ tels que $\pi_M = \prod \Phi_{d_i}$. D'après le théorème de Cayley-Hamilton (valable sur un anneau commutatif), $n \geqslant \deg \pi_M = \sum \varphi(d_i)$. En outre, $r = \mathrm{ppcm}(d_i)$; en effet, si $m = \mathrm{ppcm}(d_i)$, $m \mid r$, puisque $d_i \mid r$, et $\pi_M \mid \prod_{d|m} \Phi_d = X^m - 1$, autrement dit $M^m = I_n$ et $r \mid m$.

Réciproquement, soit d_i de tels entiers. Alors la matrice par blocs suivante définit un élément d'ordre r de $\mathrm{GL}_n(\mathbb{Q})$:

$$\begin{pmatrix} \mathcal{C}_{\Phi_{d_1}\cdots\Phi_{d_k}} & 0 \\ 0 & I_{n-\sum\varphi(d_i)} \end{pmatrix}$$

QED

Corollaire 3.12 $\Omega(n)$ est un ensemble fini.

Démonstration. Pour tout $\delta > 0, n^{1-\delta} = \underset{n\to+\infty}{o}(\varphi(n))$ (cf. par exemple [Ale99, p. 123]) [2]. Ainsi, avec les notations de la proposition précédente, seul un nombre fini d'entiers d_i conviennent, soit un nombre fini de r possibles.

Alternativement, les relations coefficients-racines montrent que l'ensemble des polynômes de $\mathbb{Z}[X]$ unitaires, de degré n et dont les racines sont des racines de l'unité est fini. Si m est le ppcm des ordres de toutes les racines de tous ces polynômes, alors m est un multiple de n'importe quel $r \in \Omega$ (cf. [FGN09, 3.18 p. 200]).

QED

Exercice 3.13

1. Quels sont les polynômes cyclotomiques de degré 1 et 2 ? De degré impair ?
2. Montrer que $\Omega(2n) = \Omega(2n+1)$, pour $n \in \mathbb{N}_*$.
3. Déterminer $\Omega(2)$ et $\Omega(4)$.
4. Exhiber un élément d'ordre 6 de $\mathrm{GL}_2(\mathbb{Q})$.

Corollaire 3.14 L'ordre d'un sous-groupe fini abélien de $\mathrm{GL}_n(\mathbb{Q})$ est majoré en fonction de n.

Démonstration. Soit G un tel groupe, d'après le théorème de Lagrange, $X^{|G|} - 1$ annule tout élément de G. Ces derniers sont donc co-diagonalisables sur $\mathbb{C}$, puisque G est abélien et $X^{|G|} - 1$ est scindé simple dans $\mathbb{C}$. G est donc conjugué dans $\mathrm{GL}_n(\mathbb{C})$ à un sous-groupe de matrices diagonales inclu dans

$$\left\{ \mathrm{Diag}(\lambda_1, \dots, \lambda_n) \ / \ \lambda_i \in \bigcup_{1\leqslant k\leqslant M(n)} \mu_k(\mathbb{C}) \right\},$$

où $M(n) = \max(\Omega(n) \setminus \{+\infty\})$, soit $|G| \leqslant \frac{M(n)(M(n)+1)}{2} n$.

QED

Remarque 3.15 Alternativement, on pourra se reporter à [FGN09, ex. 3.20 p. 205]. Notons également que le résultat précédent subsiste pour un sous-groupe fini quelconque (non nécessairement abélien), en vertu du théorème suivant :

Théorème 3.16 - Jordan-Frobenius [Ale99, Thème III]**.** Chaque sous-groupe fini de $\mathrm{GL}_n(\mathbb{C})$ contient un sous-groupe normal et abélien d'indice majoré par $9^{2n^2} - 7^{2n^2}$.

Remarque 3.17 Ce qui précède est également valable pour $\mathrm{GL}_n(\mathbb{Z})$.

2. On pourra aussi consulter le chapitre 18 de [HW07] pour des estimations des ordres de grandeurs de fonctions arithmétiques classiques.

3.4 Théorème de Wedderburn

Théorème 3.18 - Théorème de Wedderburn. Un anneau à division fini est un corps.

La preuve de ce théorème donnée dans [Per96, III, §4] utilise la formule 1 et la dernière inégalité de la proposition 1.3.

3.5 DFT et FFT [Dem09, Chap. 4]

3.6 Codes cycliques et codes BCH [Dem09, Chap. 10 et 11]

4 Exercices

Exercice 4.1 [FG95, 5.18 p. 201]

1. Traduire sur les coefficients de Φ_n le fait que ce dernier soit un polynôme réciproque.
2. Montrer que si $p_1^{\alpha_1} \dots p_r^{\alpha_r}$ est la décomposition en facteurs premiers de $n \geqslant 2$, alors
$$\Phi_n(X) = \Phi_{p_1 \dots p_r}\left(X^{p_1^{\alpha_1 - 1} \dots p_r^{\alpha_r - 1}}\right).$$
3. Pour n impair distinct de 1, montrer que $\Phi_{2n}(X) = \Phi_n(-X)$.
4. Pour p premier ne divisant pas n et $i \in \mathbb{N}_*$, établir que
$$\Phi_{p^i n}(X) = \frac{\Phi_n\left(X^{p^i}\right)}{\Phi_n\left(X^{p^{i-1}}\right)}.$$

Exercice 4.2 Pour quels entiers n a-t-on $\varphi(n) \leqslant 10$? Calculer Φ_n pour ces entiers.

Exercice 4.3 Trouver n tel que Φ_n ait d'autres coefficients que 0, 1 et -1 (réponse $n = 105$).

Exercice 4.4 - Construction du pentagone régulier. Soit $\zeta = x + iy$ l'unique racine primitive $5^{\text{ème}}$ de l'unité dans $\mathbb{C}$ vérifiant $x > 0$ et $y > 0$. Déterminer x *(Indication : utiliser* $2x = \zeta + \overline{\zeta}$ *et la réciprocité du polynôme* Φ_n*)*. En déduire que x et y sont constructibles et donner une construction explicite du pentagone régulier.

Exercice 4.5 Soit K une extension finie de $\mathbb{Q}$, montrer qu'il n'y a qu'un nombre fini de racines de l'unité dans K.

Exercice 4.6 Dans quelles extensions $\mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$, y a-t-il des racines de l'unité autres que 1 et -1 ?

Exercice 4.7 Trouver tous les couples (a, b) d'entiers relatifs premiers entre eux tels que $\cos(2\pi a/b)$ soit rationnel. *(Indication : on pourra comparer les polynômes Φ_b et $X^2 - 2\cos(2\pi a/b)\,X + 1$.)*

Exercice 4.8

1. Soit $\zeta \in \mathbb{C}$ une racine primitive $d^{\text{ème}}$ de l'unité et $k = \mathbb{Q}(\zeta)$. Montrer que les seuls racines de l'unité contenues dans k sont les racines $d^{\text{èmes}}$ ou les racines $2d^{\text{èmes}}$ selon que d est pair ou impair.
2. Déduire de la question précédente que si on se donne des entiers d et n tels que $d|n$ et qu'on suppose (d pair) ou (d et n impairs), il existe un corps k tel que $\mu_n(k) \simeq \mathbb{Z}/d\mathbb{Z}$.
3. Montrer que si $d = 2^r - 1$ et si $d \mid n$, il existe k avec $\mu_n(k) \simeq \mathbb{Z}/d\mathbb{Z}$.
4. Montrer que, quelque soit le corps k, $\mu_{30}(k)$ n'est jamais isomorphe à $\mathbb{Z}/5\mathbb{Z}$. Étudier le cas général.

Exercice 4.9 - Théorème de Kronecker-Weber dans le cas quadratique [FG95, 4.26 p. 174]**.**

Soit p un nombre premier impair et $\zeta = e^{\frac{2i\pi}{p}}$. On pose $t = \sum_{k\in\mathbb{F}_p^*} \left(\frac{k}{p}\right) \zeta^k$, où $\left(\frac{k}{p}\right)$ désigne le symbole de Legendre et où ζ^k a un sens évident.

1. Montrer que $t^2 = \left(\frac{-1}{p}\right) p$.
2. En déduire que toute extension quadratique de $\mathbb{Q}$ est contenue dans un corps cyclotomique. *(Indication : on remarquera que $\mathbb{Q}(\xi_m) \subset \mathbb{Q}(\xi_n)$, pour $m \mid n$.)*
3. Déterminer un corps cyclotomique qui contient $\mathbb{Q}\left(\sqrt{-10}\right)$.

Exercice 4.10 - Irréductibilité de $X^p - a$. Soit k un corps, $a \in k$, p un nombre premier et $P = X^p - a$. On souhaite montrer l'équivalence :

(i) P est réductible sur k ;

(ii) P a une racine dans k.

1. Montrer que (ii) implique (i).
2. Établir la réciproque lorsque la caractéristique de k est p.
3. On suppose la caractéristique de k différente de p et $P = QR$, avec Q et R unitaires de degrés respectifs r et s ($r + s = p$ et $0 < r < p$). Calculer b^p, où b désigne le coefficient constant de Q et en déduire que (i) implique (ii).

Exercice 4.11 - Groupe quasi-cyclique de Prüfer [FGN08, ex. 2.18 p. 59]**.** Soit p un nombre premier et $\mathbf{U}_p$ le sous-groupe de $\mathbb{C}_*$ engendré par l'ensemble des nombres $\exp\left(\frac{2i\pi}{p^\alpha}\right)$, où α décrit $\mathbb{N}$.

1. Quels sont les sous-groupes de $\mathbf{U}_p$?
2. Montrer que $\mathbf{U}_p$ est indécomposable, *i.e.* n'est pas isomorphe à un produit direct de deux groupes non triviaux.