Cyclotomie

Et, de ta plus belle écriture,
Note ce qu'il faudrait qu'il advînt de mon corps
Lorsque mon âme et lui ne seront plus d'accord
Que sur un seul point : la rupture.

Georges Brassens, *Supplique pour être enterré à la plage de Sète*

— *Leçons concernées :* Groupe des nombres complexes de module 1, Groupes finis, Exemples de parties génératrices d'un groupe, Nombres premiers, Corps finis, Extensions de corps, Exemples de nombres remarquables, Polynômes irréductibles à une indéterminée, Racines d'un polynôme, Dimension d'un espace vectoriel, Exemples d'utilisation de techniques d'algèbre en géométrie...

— *Développements possibles :* Irréductibilité des polynômes cyclotomiques sur $\mathbf{Z}$, leur image dans $\mathbf{F}_q[X]$ et leur factorisation, transformation de Fourier rapide pour le produit de polynômes, théorème de Wedderburn, version faible du théorème de la progression arithmétique de Dirichlet, polygones réguliers constructibles à la règle et au compas.

Ce complément de cours est très largement inspiré de [Per, §III.4] et [Goz, Chap. VI et VII] (je trouve cette seconde référence plus détaillée) ainsi que des notes du cours sur la cyclotomie donné par Salim Rostam les années précédentes (accessibles en suivant ce lien). D'autres références sont citées au fil du texte, notamment sur la constructibilité à la règle et au compas. Vous trouverez une sélection d'exercices en lien avec le thème de la cyclotomie dans la section 5, ainsi que sur la page de Salim Rostam (avec des corrections).

1. Racines de l'unité

Définition 1.1. *Soit K un corps et n un entier supérieur ou égal à 1. On note $\mu_n(K)$ l'ensemble des racines n^{e} de l'unité dans K, c'est-à-dire l'ensemble des $x \in K$ tels que $x^n = 1$. On note $\mu_n^\star(K)$ l'ensembles des racines primitives n^{e} de l'unité, c'est-à-dire l'ensemble des éléments de K dont l'ordre multiplicatif est exactement égal à n.*

Remarque 1.2. On a toujours $1 \in \mu_n(K)$. Par contre, $\mu_n^\star(K)$ peut être vide. Par exemple $\mu_3^\star(\mathbf{R}) = \emptyset$ car la seule racine cubique de l'unité dans $\mathbf{R}$ est 1 qui est d'ordre 1, donc ce n'est pas une racine primitive.

Proposition 1.3. *$\mu_n(K)$ est un sous-groupe cyclique de $K^\times$ de cardinal au plus n.*

Démonstration. Commençons par montrer que $\mu_n(K)$ est un sous-groupe de $K^\times$. Tout d'abord on a bien $1 \in \mu_n(K)$. D'autre part, si $x, y \in \mu_n(K)$ alors $(xy)^n = x^n y^n = 1$ (on utilise ici le fait qu'un corps est commutatif). La stabilité par passage à l'inverse est claire.
Maintenant, $\mu_n(K)$ est formé des racines dans K du polynôme $X^n - 1$, qui ne peut pas avoir plus de racines que son degré, ce qui prouve que $|\mu_n(K)| \leqslant n$. Enfin, $\mu_n(K)$ est cyclique en tant que sous-groupe fini du groupe multiplicatif d'un corps. Nous verrons une preuve de ce fait dans le complément sur les corps finis. Vous trouverez aussi trois preuves dans les notes de Salim Rostam sur la cyclotomie. □

Prenons le temps d'apprécier ce résultat, ce n'est pas tous les jours que les racines d'un polynôme forment un groupe, qui plus est cyclique ! Cela nous place au carrefour des leçons sur les racines de polynômes et de celles sur les groupes, et permet de montrer plein de beaux résultats.

Remarque 1.4. Rappelons que le « bon » cadre pour qu'un polynôme ait moins de racines que son degré (au sens large) est celui des polynômes à coefficients dans un anneau commutatif intègre. En effet :

— Soit A un anneau commutatif (pas nécessairement intègre), soit $P \in A[X]$ et soit $a \in A$. Alors *comme le polynôme $X-a$ a un coefficient dominant inversible dans A*, on peut effectuer la division euclidienne de P par $X-a$, pour écrire $P = (X-a)Q + r$ où $Q \in A[X]$ et $r \in A$. Ensuite, comme A est commutatif, l'évaluation en a est un morphisme d'anneaux [1], donc $P(a) = 0$ si et seulement si $r = 0$, si et seulement si $(X-a) \mid P$.

— Maintenant, on a besoin que A soit intègre pour montrer que si b est une autre racine, alors $(X-a)(X-b)$ divise P. En effet, lorsque l'on évalue en b l'égalité $P = (X-a)Q$, on a besoin d'intégrité pour affirmer que $P(b) = 0$ implique $Q(b) = 0$ *(car $b - a \neq 0$ et A est intègre)*.

En l'absence d'intégrité, on peut penser à l'exemple du polynôme $2X$, qui a deux racines dans $\mathbf{Z}/4\mathbf{Z}$, bien qu'il soit de degré 1, ou à X^2-1 qui a 4 racines dans $\mathbf{Z}/8\mathbf{Z}$, bien qu'il soit de degré 2. En l'absence de commutativité, on peut penser à l'algèbre des quaternions, dans laquelle on trouve une infinité de racines du polynômes X^2-1. En effet, tout quaternion pur [2] $q = bi + cj + dk$ satisfait $\overline{q} = -q$ et donc $N(q) = q\overline{q} = -q^2 = (iq)^2$. Ainsi, tout triplet de réels (b, c, d) satisfaisant $b^2 + c^2 + d^2 = 1$ nous donne un quaternion pur $q = bi + cj + dk$ de norme 1, et donc iq est une racine carrée de l'unité.

Lemme 1.5. *Soit K un corps, dont on note p la caractéristique (éventuellement nulle), et soit $n \geqslant 1$.*

— *Si p ne divise pas n alors le polynôme $X^n - 1$ est séparable (i.e. scindé à racines simples dans une clôture algébrique de K).*

— *Si p divise n, alors en écrivant $n = p^\alpha m$ avec $\operatorname{pgcd}(m, p) = 1$ et $\alpha \geqslant 1$, on a*

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

Démonstration. La dérivée du polynôme $P := X^n - 1$ est $P' = nX^{n-1}$, et si n est premier avec p ce polynôme est non-nul avec pour unique racine 0 (de multiplicité $n-1$), qui n'est pas racine de $X^n - 1$. Donc toutes les racines de P (dans un corps de décomposition de P sur K, ou dans une clotûre algébrique de K si l'on s'autorise à parler de clôture algébrique) sont simples [3].

Si par contre on a $n = p^\alpha m$, alors comme $(-1)^{p^\alpha} = -1$ dans K (y compris en caractéristique 2 puisque dans ce cas $-1 = 1$), on peut écrire

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

par linéarité du Frobenius. □

Corollaire 1.6. *Avec les notations précédentes, si l'on est dans le cas $n = p^\alpha m$ du lemme précédent on a $\mu_n(K) = \mu_m(K)$. En particulier, il n'y a aucune racine primitive n^{e} dans K.*

C'est pourquoi lorsque la caractéristique p est positive, on a tendance à supposer (parfois un peu trop implicitement) que n est premier avec p pour les questions qui concernent les racines n^{e} de l'unité et les polynômes cyclotomiques. Nous ferons cette hypothèse dans la plupart des énoncés à partir de maintenant, mais nous ferons quelques remarques pour bien nous convaincre qu'il peut se passer des choses différentes dans le cas où elle n'est pas satisfaite.

1. En effet, si A n'était pas commutatif et si $a, b \in A$ étaient deux éléments ne commutant pas, alors en considérant $P = X$ et $Q = bX$, on aurait $\operatorname{ev}_a(PQ) \neq \operatorname{ev}_a(P)\operatorname{ev}_a(Q)$. Le fait que l'évaluation soit un morphisme d'anneaux requiert donc vraiment la commutativité.

2. On appelle *quaternion pur* un quaternion dont la partie réelle est nulle, c'est-à-dire qui a un coefficient a égal à 0 dans l'écriture $q = a1 + bi + cj + dk$.

3. Une rédaction alternative pour montrer que P est séparable est de montrer que $\operatorname{pgcd}(P, P') = 1$. Or dans le cas où p ne divise pas n, l'entier n est inversible dans K et on peut écrire la relation de Bézout

$$\frac{1}{n}XP' - P = 1.$$

Proposition 1.7. *Soit K un corps dont la caractéristique ne divise pas l'entier n. Notons K_n « le » corps de décomposition de $X^n - 1$ sur K. Alors $\mu_n(K_n)$ est un groupe cyclique d'ordre n et $\mu_n^\star(K_n)$ est de cardinal $\varphi(n)$.*

Démonstration. Comme la caractéristique de K ne divise pas n, le polynôme $X^n - 1$ est scindé à racines simples dans son corps de décomposition (Lemme 1.5) donc $|\mu_n(K_n)| = n$, et l'on savait déjà que $\mu_n(K_n)$ était cyclique d'après la Proposition 1.3. Prenons un générateur ζ de $\mu_n(K_n)$ (c'est-à-dire une racine primitive n^{e} de l'unité). Alors

$$\mu_n(K_n) = \left\{\zeta^k,\ k \in \{0, \dots, n-1\}\right\}$$

et parmi les ζ^k, seuls ceux pour lesquels k est premier avec n sont également d'ordre n (*cf.* Exercice 5.1). Or $\varphi(n)$ est précisément le nombre de tels k. □

Remarque 1.8. Bien sûr $\mu_n^\star(K_n)$ n'est pas un sous-groupe de $K_n^\times$, il ne contient même pas 1 (sauf pour $n = 1$).

Corollaire 1.9. *$\mu_n(K)$ est un groupe cyclique d'ordre d pour un certain diviseur d de n.*

Démonstration. Si la caractéristique de K ne divise pas n alors $\mu_n(K)$ est un sous-groupe de $\mu_n(K_n)$, qui est un groupe cyclique d'ordre n, donc il est cylique d'ordre un diviseur de n (c'est un résultat classique sur la classification des sous-groupes d'un groupe cyclique). Si jamais la caractéristique divise n on utilise le Corollaire 1.6 pour se ramener au cas précédent. □

Exemple 1.10. Pour illustrer le corollaire précédent, voici une question à laquelle il peut être bon d'avoir réfléchi. Soit $n \geqslant 1$ et $q = p^r$ une puissance de nombre premier. Combien y-a-t-il de racines n^{e} de l'unité dans $\mathbf{F}_q$?
La réponse est $\operatorname{pgcd}(n, q-1) =: d$. En effet, $\mathbf{F}_q^\times$ est un groupe d'ordre $q-1$, donc l'ordre de n'importe quel élément $x \in \mathbf{F}_q^\times$ doit diviser $q-1$. Si de plus $x^n = 1$, alors l'ordre de x doit aussi diviser n, et donc finalement, l'ordre d'un élément $x \in \mu_n(\mathbf{F}_q)$ doit diviser le pgcd de n et de $q-1$. Ainsi, $\mu_n(\mathbf{F}_q) \subseteq \mu_d(\mathbf{F}_q)$. Mais réciproquement, comme d divise n il est clair que $\mu_d(\mathbf{F}_q) \subseteq \mu_n(\mathbf{F}_q)$. On a donc montré que

$$\mu_n(\mathbf{F}_q) = \mu_d(\mathbf{F}_q) \quad \text{où } d = \operatorname{pgcd}(n, q-1).$$

De plus, comme $\mathbf{F}_q^\times$ est *cyclique* d'ordre $q-1$, il admet un unique sous-groupe (cyclique lui aussi) d'ordre δ pour tout diviseur δ de $q-1$, explicitement donné par $\mu_\delta(\mathbf{F}_q)$ (*cf.* Exercice 5.1). En particulier pour $\delta = d$, cela montre que $\mu_d(\mathbf{F}_q)$ est un groupe cyclique d'ordre d, et nous donne la conclusion annoncée.

2. Polynômes cyclotomiques sur Q

Dans cette section, nous commençons par un point de vue très concret sur les polynômes cyclotomiques sur $\mathbf{Q}$, sans parler de corps de décomposition mais juste en prenant les racines complexes de l'unité dont on a l'habitude. Nous parlerons de corps de décomposition dans la section suivante, qui traite le cas des polynômes cyclotomiques sur un corps quelconque (mais nous verrons qu'ils sont très liés aux polynômes cyclotomiques sur $\mathbf{Q}$).

Définition 2.1. *Soit $n \geqslant 1$. Le n^{e} polynôme cyclotomique sur $\mathbf{Q}$ est défini comme*

$$\Phi_{n,\mathbf{Q}} := \prod_{\zeta \in \mu_n^\star(\mathbf{C})} (X - \zeta)$$

A priori, il s'agit d'un polynôme à coefficients complexes, mais comme on l'appelle « polynôme cyclotomique sur $\mathbf{Q}$ », vous voyez sans doute venir la suite : nous allons montrer qu'il est à coefficients rationnels (et même entiers) et qu'il est le polynôme minimal sur $\mathbf{Q}$ de n'importe quelle racine primitive n^{e} de l'unité dans $\mathbf{C}$.
La difficulté des démonstrations se cache principalement dans les passages entre $\mathbf{Z}[X]$ et $\mathbf{Q}[X]$. Il y a

en effet un risque de confusion entre les divisions euclidiennes dans l'un ou l'autre de ces anneaux, ainsi qu'entre les polynômes irréductibles dans l'un ou dans l'autre. Afin de clarifier cela, nous allons suivre l'approche de [Goz] en isolant du mieux possible les arguments qui concernent le passage de $\mathbf{Q}[X]$ à $\mathbf{Z}[X]$ dans les lemmes 2.3 et 2.6.
La relation suivante est essentielle pour la suite :

Lemme 2.2. *Pour tout $n \geqslant 1$, on a $X^n - 1 = \prod_{d|n} \Phi_{d,\mathbf{Q}}$*

Démonstration. Cela vient du regroupement des racines n^{e} de l'unité selon leur ordre, qui doit être un diviseur d de n. Il est important de remarquer qu'on utilise ici la simplicité des racines de $X^n - 1$, nous y reviendrons dans la section 3, où des problèmes apparaissent en caractéristique positive. □

Une fois que l'on a cette relation, le fait que $\Phi_{n,\mathbf{Q}}$ est à coefficients entiers tombe facilement par récurrence, en utilisant le lemme suivant.

Lemme 2.3 (le cas facile)**.** *Considérons trois polynômes $A, B, P \in \mathbf{C}[X]$ tels que $P = AB$. Si P et A sont à coefficients entiers et A est unitaire, alors B est à coefficients entiers.*

Démonstration. Comme P et A appartiennent à $\mathbf{Z}[X]$ et A est unitaire (donc son coefficient dominant est inversible dans $\mathbf{Z}$), on peut effectuer la division euclidienne de P par A dans $\mathbf{Z}[X]$:

$$P = AQ + R$$

où $Q, R \in \mathbf{Z}[X]$ et $\deg(R) < \deg(A)$. Il suffit alors de dire que cette division euclidienne est aussi une division euclidienne dans $\mathbf{C}[X]$, tout comme l'égalité $P = AB$! On conclut donc par unicité de la division euclidienne que $B = Q \in \mathbf{Z}[X]$ (et $R = 0$). □

Remarque 2.4. L'argument d'unicité de la division euclidienne n'est pas difficile, on peut aussi le reproduire dans ce contexte : on a $P = AB = AQ + R$, donc $A(B - Q) = R$ et on conclut en considérant les degrés que cela ne peut être vrai que si $B = Q$ et $R = 0$.

Proposition 2.5. *Pour tout $n \geqslant 1$, $\Phi_{n,\mathbf{Q}}$ est un polynôme unitaire à coefficients entiers.*

Démonstration. Montrons ce résultat par récurrence sur n.

— Pour $n = 1$, on $\Phi_{1,\mathbf{Q}} = X - 1$, qui est bien unitaire à coefficients entiers.

— Soit $n \geqslant 2$. Si la propriété est vraie jusqu'au rang $n - 1$, alors

$$F(X) := \prod_{\substack{d|n \\ d<n}} \Phi_{d,\mathbf{Q}}$$

est unitaire à coefficients entiers et d'après le Lemme 2.2

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

A priori, c'est une factorisation dans $\mathbf{C}[X]$, mais grâce au Lemme 2.3 (avec $P = X^n - 1$ et $A = F$) on conclut que $\Phi_{n,\mathbf{Q}}$ est à coefficients entiers (et il est unitaire car $X^n - 1$ et F le sont).

□

Cependant, dans la preuve de l'irréductibité des polynômes cyclotomiques, on a besoin d'une version légèrement plus forte du Lemme 2.3, qui ne repose pas seulement sur l'unicité de la division euclidienne.

Lemme 2.6 (le cas moins facile, voir [Goz, Lemme VI.8])**.** *Considérons trois polynômes $A, B, P \in \mathbf{Q}[X]$ tels que $P = AB$. Si P et A sont unitaires et P est à coefficients entiers, alors A et B sont à coefficients entiers (et B est unitaire).*

Démonstration. Tout d'abord, le fait que P et A soient unitaires implique que B l'est aussi. Les polynômes A et B sont donc de la forme

$$A = X^n + \sum_{i=0}^{n-1} a_i X^i \quad \text{et} \quad B = X^m + \sum_{i=0}^{m-1} b_i X^i$$

où $a_i = \frac{p_i}{q_i}$ pour deux entiers $p_i \in \mathbf{Z}$ et $q_i \in \mathbf{N}^*$ premiers entre eux. Soit $q \in \mathbf{N}^*$ un multiple commun à tous les q_i. Alors on a

$$qA = qX^n + \sum_{i=0}^{n-1} z_i X^i \tag{1}$$

où les z_i sont des entiers. Quitte à diviser cette égalité par le pgcd de $q, z_0, \ldots, z_{n-1}$, on peut supposer que le contenu[4] de qA est égal à 1. De même, on peut trouver un entier $r \in \mathbf{N}^*$ tel que rB soit un polynôme à coefficients entiers dont le contenu est égal à 1 (on dit que qA et rB sont *primitifs*). Or d'après l'un des lemmes de Gauss, le produit de deux polynômes primitifs est primitif : voir [Goz, Lemme I.50]. Donc $(qA)(rB) = qrP$ est primitif, mais comme P est à coefficients entiers, cela veut dire que qr multiplié par le pgcd des coefficients de P est égal à 1, donc $q = r = 1$, ce qui prouve que A et B appartiennent à $\mathbf{Z}[X]$. □

Remarque 2.7. (1) Noter que c'est dans l'étape « quitte à diviser » qu'on utilise le fait que A est unitaire : en effet, si par exemple on avait $A = \frac{2}{3}(X+1)$, alors on devrait multiplier par 3 pour le rendre à coefficients entiers, on écrirait donc $3A = 2(X+1)$, mais alors la division par 2 que l'on aimerait faire pour rendre le terme de droite primitif nous oblige à écrire $\frac{3}{2}A = X + 1$, et donc on ne multiplie plus A par un entier, mais par un rationnel. Le point important dans le preuve ci-dessus est que le pgcd de $q, z_0, \ldots, z_{n-1}$ divise q, qui est le coefficient devant A dans (1).

(2) Pour le tout dernier argument, on sait en fait que le pgcd des coefficients de P est égal à 1, car P est unitaire à coefficients entiers, mais on n'en a pas besoin. Le fait que P soit unitaire sert à montrer que B est lui aussi unitaire.

Théorème 2.8. *Soit $n \geqslant 1$. Le polynôme $\Phi_{n,\mathbf{Q}}$ est irréductible dans $\mathbf{Q}[X]$ (donc dans $\mathbf{Z}[X]$ car il est unitaire).*

Démonstration. Soit ζ une racine primitive n^{e} de l'unité dans $\mathbf{C}$ et soit f son polynôme minimal sur $\mathbf{Q}$. Nous allons montrer que $\Phi_{n,\mathbf{Q}} = f$, ce qui prouvera bien que $\Phi_{n,\mathbf{Q}}$ est irréductible.

- Tout d'abord, comme $\Phi_{n,\mathbf{Q}}$ est un polynôme annulateur de ζ, on sait que f divise $\Phi_{n,\mathbf{Q}}$ dans $\mathbf{Q}[X]$.
- Pour montrer qu'il y a égalité, nous allons montrer que $\deg(f) \geqslant \deg(\Phi_{n,\mathbf{Q}})$ en montrant que toute racine primitive n^{e} de l'unité est racine de f, puis la conclusion découlera simplement du fait que les deux polynômes sont unitaires.
  Maintenant, pour montrer que toute racine primitive n^{e} de l'unité est racine de f, comment fait-on ? En fait, il suffit d'observer que ces racines primitives sont les ζ^k pour les entiers $k \geqslant 1$ qui sont premiers avec n. Ainsi, elles sont obtenues en élevant successivement la racine primitive ζ à des puissances premières, ne divisant pas n. Il suffit donc de montrer que si u est une racine de f et p un nombre premier ne divisant pas n, alors u^p est aussi une racine de f. C'est que nous prouvons maintenant :
  (1) Comme $X^n - 1$ est un polynôme annulateur de ζ et f est le polynôme minimal de ζ, le polynôme f divise $X^n - 1$, donc on peut écrire

  $$X^n - 1 = f(X)h(X)$$

  où $h \in \mathbf{Q}[X]$. Mais f est unitaire et $X^n - 1$ est à coefficients entiers, donc le Lemme 2.6 nous dit que f et h sont aussi à coefficients entiers.
  (2) L'égalité ci-dessus montre aussi que toute racine de f est une racine n^{e} de l'unité, donc

  $$0 = (u^n)^p - 1 = (u^p)^n - 1 = f(u^p)h(u^p). \tag{$\star$}$$

4. Le contenu d'un polynôme à coefficients entiers est défini comme le pgcd de ses coefficients.

On s'approche du but ! (rappelons que l'on cherche à montrer que $f(u^p) = 0$).
(3) Si, par l'absurde, $f(u^p) \neq 0$. Alors d'après ($\star$), $h(u^p) = 0$, donc le polynôme $h(X^p)$ est un polynôme à coefficients rationnels (et même entiers) qui s'annule en u, donc f divise $h(X^p)$ dans $\mathbf{Q}[X]$. On peut donc écrire

$$h(X^p) = f(X)g(X) \qquad (\star\star)$$

pour un certain $g \in \mathbf{Q}[X]$. Mais comme f et $h(X^p)$ sont à coefficients entiers (voir l'étape (1)) et f est unitaire, on peut appliquer le Lemme 2.3 (le cas facile) pour montrer qu'en fait g appartient à $\mathbf{Z}[X]$. On peut donc réduire l'égalité ($\star\star$) modulo p et utiliser le fait que

$$\overline{h(X^p)} = \overline{h(X)}^p$$

pour écrire

$$\overline{h(X)}^p = \overline{f(X)}.\overline{g(X)}.$$

Maintenant, si θ est un facteur irréductible de $\overline{f(X)}$ dans $\mathbf{F}_p[X]$, il divise $\overline{h(X)}^p$, donc divise $\overline{h(X)}$. En revenant à l'égalité $X^n - 1 = f(X)h(X)$, on en déduirait que $X^n - 1$ est divisible par θ^2 dans $\mathbf{F}_p[X]$, ce qui contredit le fait qu'il est séparable (il est premier avec sa dérivée nX^{n-1} car n est premier avec p).

□

Corollaire 2.9. *Si ζ est une racine primitive n^{e} de l'unité dans $\mathbf{C}$, l'extension $\mathbf{Q}(\zeta)/\mathbf{Q}$ est de degré $\varphi(n)$.*

Démonstration. Le degré de l'extension considérée est le degré du polynôme minimal de ζ sur $\mathbf{Q}$, qui d'après le théorème précédent n'est nul autre que $\Phi_{n,\mathbf{Q}}$, qui est bien de degré $\varphi(n)$. □

Enfin, on peut également déterminer le groupe des automorphismes d'un corps cyclotomique :

Proposition 2.10. *Si $\zeta \in \mu_n^\star(\mathbf{C})$, le groupe des automorphismes du corps $\mathbf{Q}(\zeta)$ est isomorphe à $(\mathbf{Z}/n\mathbf{Z})^\times$.*

Démonstration. *cf.* Exercice 5.3. □

Remarque 2.11. Pour la culture : on appelle *extension abélienne* toute extension de corps qui est galoisienne et dont le groupe de Galois est abélien. Le célèbre (et difficile !) théorème de Kronecker-Weber nous dit que tout extension abélienne finie $K/\mathbf{Q}$ est contenue dans une extension cyclotomique.

Enfin, terminons par une preuve élémentaire d'un fait classique sur les extensions galoisiennes : dans $\mathbf{Q}(\zeta)$, les éléments de $\mathbf{Q}$ sont caractérisés par le fait qu'ils sont fixés par tous les automorphismes.

Proposition 2.12. *Soit $\zeta \in \mu_n^\star(\mathbf{C})$ et soit $K := \mathbf{Q}(\zeta)$. On note G le groupe des automorphismes de K (qui est aussi appelé le groupe de Galois de l'extension $K/\mathbf{Q}$). Alors le « sous-corps fixe »*

$$K^G := \{x \in K \mid \forall \sigma \in G,\ \sigma(x) = x\}$$

est égal à $\mathbf{Q}$.

Démonstration. *cf.* Exercice 5.4. La preuve s'appuie sur la description des automorphismes de K fournie par l'Exercice 5.3. □

3. Polynômes cyclotomiques sur un corps quelconque

Soit K un corps. Notons K_n « le » corps de décomposition du polynôme $X^n - 1$ sur K.

Définition 3.1. *Le n^{e} polynôme cyclotomique sur K est défini comme*

$$\Phi_{n,K} := \prod_{\zeta \in \mu_n^\star(K_n)} (X - \zeta).$$

A priori, c'est un élément de $K_n[X]$, mais nous allons voir plus bas qu'il est à coefficients dans K.

Sans faire d'hypothèse sur le lien entre n et la caractéristique, on peut toujours affirmer que

$$\mu_n(K_n) = \bigsqcup_{d|n} \mu_d^\star(K_n). \tag{2}$$

C'est à l'étape suivante qu'une différence majeure avec le cas de la caractéristique 0 apparaît. En effet, il n'est plus toujours vrai que

$$X^n - 1 = \prod_{\zeta \in \mu_n(K_n)} (X - \zeta). \tag{3}$$

En effet, si la caractéristique de K divise n, le Lemme 1.5 montre que les racines de l'unité apparaissent avec des multiplicités. Par exemple, sur $K = \mathbf{F}_2$, le polynôme $X^2 - 1$ est égal à $(X-1)^2$, donc son corps de décomposition est $\mathbf{F}_2$, et il admet une seule racine dans ce corps (qui est 1, avec multiplicité 2). Ainsi,

$$X^2 - 1 \neq \prod_{\zeta \in \mu_2(\mathbf{F}_2)} (X - \zeta) = X - 1.$$

La formule de récurrence sur les polynômes cylotomiques n'est donc vraie qu'en ajoutant l'hypothèse que la caractéristique de K ne divise pas n. Dans ce cas on peut bien écrire (3) car les racines de $X^n - 1$ sont simples (le polynôme $X^n - 1$ est séparable car premier avec son polynôme dérivé), puis utiliser (2) pour faire apparaître les polynômes cyclotomiques. On obtient ainsi le lemme suivant.

Lemme 3.2. *Soit K un corps et $n \geqslant 1$ un entier qui n'est pas divisible par la caractéristique de K, alors on a*

$$X^n - 1 = \prod_{d|n} \Phi_{d,K}$$

Remarque 3.3. Au risque d'être répétitif, considérons le cas $n = 2$ et $K = \mathbf{F}_2$ pour voir que ce lemme n'est alors pas vrai. D'après la Définition 3.1, on a $\Phi_{1,\mathbf{F}_2} = X - 1$ et $\Phi_{2,\mathbf{F}_2} = 1$ (car 1 est la seule racine carrée de l'unité dans $\mathbf{F}_2$, et elle n'est pas primitive). Donc $X^2 - 1 \neq \Phi_{1,\mathbf{F}_2}\Phi_{2,\mathbf{F}_2}$.

Puisque la formule de récurrence est la clef de voûte des preuves qui suivent : **on suppose dans toute la suite que n est premier avec la caractéristique de K.**
Le résultat suivant nous dit qu'en réalité, ces polynômes cyclotomiques $\Phi_{n,K}$ ne sont pas si nouveaux que cela, car ils sont simplement l'image naturelle des polynômes cyclotomiques sur $\mathbf{Q}$ (en voyant les coefficients entiers de ces derniers comme des $1_K + \cdots + 1_K$ dans le corps K).

Proposition 3.4. *Soit $c\colon \mathbf{Z}[X] \to K[X]$ le morphisme canonique. On a*

$$\Phi_{n,K} = c(\Phi_{n,\mathbf{Q}}).$$

En particulier $\Phi_{n,K} \in K[X]$.

Démonstration. Par récurrence sur n :

- Pour $n = 1$, on a $\Phi_{1,K} = X - 1 = c(\Phi_{1,\mathbf{Q}})$.
- Soit $n \geqslant 2$. Si pour tout $d < n$ on a $\Phi_{d,K} = c(\Phi_{d,\mathbf{Q}})$ alors : notons

$$\Psi_{n,K} = \prod_{\substack{d|n \\ d<n}} \Phi_{n,K} \quad \text{et} \quad \Psi_{n,\mathbf{Q}} = \prod_{\substack{d|n \\ d<n}} \Phi_{n,\mathbf{Q}}.$$

Par hypothèse de récurrence, on a $\Psi_{n,K} = c(\Psi_{n,\mathbf{Q}})$.
Maintenant, on a d'une part d'après le Lemme 2.2

$$X^n - 1 = \Phi_{n,\mathbf{Q}}\Psi_{n,\mathbf{Q}}$$

et donc (cette égalité ayant lieu dans $\mathbf{Z}[X]$ on peut lui appliquer c) :

$$X^n - 1 = c(\Phi_{n,\mathbf{Q}})c(\Psi_{n,\mathbf{Q}}) = c(\Phi_{n,\mathbf{Q}})\Psi_{n,K}. \tag{4}$$

D'autre part, d'après le Lemme 3.2

$$X^n - 1 = \Phi_{n,K}\Psi_{n,K} \tag{5}$$

Ainsi, d'après (4) et (5) et l'unicité de la division euclidienne dans $K_n[X]$, on a bien $\Phi_{n,K} = c(\Phi_{n,\mathbf{Q}})$.

□

C'est grâce à cette proposition que l'on peut se permettre de noter Φ_n plutôt que $\Phi_{n,K}$, car en fait ce sont essentiellement les mêmes polynômes pour n'importe quel K : les polynômes cyclotomiques sur $\mathbf{Q}$ dont les coefficients entiers sont lus comme des $1_K + \cdots + 1_K$ dans le corps K dans lequel on décide de les considérer.

Remarque 3.5. Si la caractéristique de K divise n, rien de va plus ! Par exemple, nous avons vu que $\Phi_{2,\mathbf{F}_2} = 1$ mais ce dernier n'est alors pas la réduction modulo 2 de $\Phi_{2,\mathbf{Q}} = X + 1$.

Théorème 3.6 (*cf.* [Dem, Prop. 9.17])**.** *Soit q une puissance d'un nombre premier p, et soit $n \geqslant 2$ un entier premier à p. On note r l'ordre de q dans $(\mathbf{Z}/n\mathbf{Z})^\times$ et $\overline{\Phi}_n$ l'image de Φ_n via le morphisme canonique $\mathbf{Z}[X] \to \mathbf{F}_q[X]$. Alors $\overline{\Phi}_n$ se décompose dans $\mathbf{F}_q[X]$ en produit de $\frac{\varphi(n)}{r}$ polynômes irréductibles unitaires distincts, tous de même degré r.*

Démonstration. Soit K un corps de décomposition de $X^{q^r} - X$ sur $\mathbf{F}_q$ (nous verrons dans le cours sur les corps finis que c'est une extension de degré r de $\mathbf{F}_q$). Comme, par définition de r, on a $q^r \equiv 1 \,(\mathrm{mod}\, n)$, l'entier n divise $q^r - 1$, et donc $X^n - 1$ divise $X^{q^r-1} - 1$, qui lui-même divise $X^{q^r} - X$. Ainsi, $X^n - 1$ est scindé dans K, c'est-à-dire : K contient n racines $n^{\text{èmes}}$ de l'unité.
Soit $P \in \mathbf{F}_q[X]$ un facteur irréductible de $\overline{\Phi}_n$. On note s le degré de P, et notre objectif est de montrer que $s = r$. Comme P divise $\overline{\Phi}_n$, qui lui-même divise $X^n - 1$, on en déduit que P est scindé sur K. Soit $\zeta \in K$ une racine de P et soit $\mathbf{F}_q(\zeta)$ le sous-corps de K engendré par ζ (c'est un corps de rupture de P).

- Comme P est irréductible sur $\mathbf{F}_q$, il est le polynôme minimal de ζ, et donc l'extension $\mathbf{F}_q(\zeta)/\mathbf{F}_q$ est de degré s. Par multiplicativité du degré dans les extensions de corps, $s = [\mathbf{F}_q(\zeta) : \mathbf{F}_q]$ divise $[K : \mathbf{F}_q] = r$.
- D'autre part, le groupe multiplicatif $\mathbf{F}_q(\zeta)^\times$ est de cardinal $q^s - 1$. Donc l'ordre de ζ divise $q^s - 1$ d'après le théorème de Lagrange. Mais cet ordre est égal à n, car ζ est racine de $\overline{\Phi}_n$ et ce dernier est égal à $\Phi_{n,\mathbf{F}_q}$ d'après la Proposition 3.4. Donc n divise $q^s - 1$, c'est-à-dire $q^s \equiv 1 \,(\mathrm{mod}\, n)$. Donc l'ordre de q dans $(\mathbf{Z}/n\mathbf{Z})^\times$ divise s.

Finalement $s = r$, donc toutes les facteurs irréductibles sont de degré r. Le fait qu'ils soient distincts vient simplement de l'hypothèse de coprimalité de n à la caractéristique, qui assure que $X^n - 1$ est sans facteur carré dans $\mathbf{F}_q[X]$ (et donc c'est aussi le cas de $\Phi_{n,\mathbf{F}_q}$ qui le divise). □

Corollaire 3.7. *Sous les hypothèses du théorème précédent, $\overline{\Phi}_n$ est irréductible sur $\mathbf{F}_q$ si et seulement si q engendre $(\mathbf{Z}/n\mathbf{Z})^\times$.*

Démonstration. C'est un corollaire immédiat du théorème précédent, mais on peut aussi démontrer ce résultat directement, sans le voir comme un cas particulier du Théorème 3.6 : voir [Ort, p. 143]. Cependant la preuve est plus ou moins du même niveau de difficulté... □

Corollaire 3.8. *$\Phi_8 = X^4 + 1$ est réductible sur tous les $\mathbf{F}_q$, bien qu'irréductible sur $\mathbf{Z}$.*

Démonstration. On peut se convaincre rapidement à la main du fait que $(\mathbf{Z}/8\mathbf{Z})^\times$ n'est pas cyclique (c'est un groupe à 4 éléments, mais tous ses éléments sont d'ordre 2), et la conclusion nous est alors donnée par le corollaire précédent lorsque q est impair. Lorsque q est pair, on a $X^4 + 1 = (X + 1)^4$ par linéarité du Frobenius (utilisé en caractéristique deux ici). Enfin, Φ_8 est irréductible sur $\mathbf{Z}$ d'après le Théorème 2.8. □

Remarque 3.9. (1) Bien sûr, il n'est pas difficile de construire un polynôme réductible sur tous les $\mathbf{F}_q$, il suffit de prendre X^2, ou $(X-1)^2$ par exemple, mais ces polynômes sont également réductibles sur $\mathbf{Z}$. L'intérêt du corollaire précédent est que Φ_8 est irréductible sur $\mathbf{Z}$, bien que réductible dans tous les corps finis. Cet exemple nie en quelques sorte l'existence d'un *principe local-global* pour la réductibilité de polynômes à coefficients entiers : on ne peut pas espérer montrer qu'un polynôme est réductible sur $\mathbf{Z}$ (c'est le côté qu'on appelle global) en montrant qu'il est réductible sur tous les $\mathbf{F}_q$ (c'est le côté qu'on appelle local). Un exemple notable de principe local-global est le théorème de Hasse-Minkowski : voir par exemple [Ser].

(2) Le Théorème 3.6 étant quelque peu difficile, il est bon de savoir qu'on peut montrer relativement élémentairement que X^4+1 est réductible sur tous les $\mathbf{F}_p$: c'est un bon exercice qui fait réviser les résultats sur les carrés dans les corps finis (voir les notes du cours de Salim Rostam).

(3) En fait, on peut montrer qu'il n'existe pas de contre-exemple de degré 2 ou 3 : si un polynôme à coefficients entiers de degré 2 ou 3 est irréductible sur $\mathbf{Z}$, alors il existera toujours au moins un premier p (en fait une infinité) tel qu'il soit irréductible dans $\mathbf{F}_p[X]$. Cela dépasse cependant le cadre de l'agrégation !

4. Applications

Voici quelques applications des polynômes cyclotomiques, chaque section correspond plus ou moins à un développement, mais les résultats des sections précédentes peuvent aussi faire l'objet de développements !

4.1. Transformée de Fourier rapide pour le produit de polynômes

Voir [Pey] ou cette note de Matthieu Romagny : `https://agreg-maths.univ-rennes1.fr/journal/2020/fft.pdf`

4.2. Le théorème de Wedderburn

Un développement classique dont la preuve fait intervenir les polynômes cyclotomiques :

Théorème 4.1 (Wedderburn). *Toute algèbre à division finie est commutative.*

Démonstration. cf. [Per, p. 82] ou [Goz, Th. VII.4]. □

4.3. Une version faible du théorème de la progression arithmétique de Dirichlet

Pour commencer rappelons la version classique du théorème de la progression arithmétique :

Théorème 4.2 (Dirichlet). *Soit a et n deux entiers premiers entre eux. Il existe une infinité de nombres premiers congrus à a modulo n.*

On l'appelle théorème de la progression arithmétique car une autre façon de le dire est la suivante : « la progression arithmétique $a, a+n, a+2n, a+3n, \ldots$ contient une infinité de nombres premiers ».

En utilisant des arguments sur les racines de l'unité dans $\mathbf{F}_p$ et les polynômes cyclotomiques, nous allons montrer le cas particulier $a=1$:

Théorème 4.3 (Version faible du théorème de Dirichlet). *Soit n un entier supérieur ou égal à 2. Il existe une infinité de nombres premiers congrus à 1 modulo n.*

Le preuve repose sur la critère suivant qui relie le fait d'être congru à 1 modulo n et les racines de l'unité dans $\mathbf{F}_p$.

Lemme 4.4. *Soit $n \geqslant 2$ et soit p un nombre premier. Il existe une racine primitive n^{e} de l'unité dans $\mathbf{F}_p$ si et seulement si $p \equiv 1 \pmod{n}$.*

Démonstration. — *Preuve s'appuyant sur des résultats précédents :* d'après le Corollaire **??**, on sait que $\mu_n(\mathbf{F}_p)$ est un groupe cyclique de cardinal d divisant n, et donc il admet un élément d'ordre n si et seulement si il est de cardinal n. Maintenant, d'après l'Exemple **??**, le cardinal de $\mu_n(\mathbf{F}_p)$ est le $\mathrm{pgcd}(n, p-1)$. Donc $|\mu_n(\mathbf{F}_p)| = n$ si et seulement si n divise $p-1$, ce qui donne le résultat voulu.

— *Preuve dans ce cas particulier :* Le groupe $\mathbf{F}_p^\times$ étant cyclique d'ordre $p-1$, il contient un élément d'ordre n si et seulement si n divise $p-1$. En effet, l'ordre d'un élément dans un groupe divise le cardinal du groupe (Théorème de Lagrange), ce qui donne une implication, et pour la réciproque : si n divise $p-1$ et qu'on prend ζ un générateur de $\mathbf{F}_p^\times$ alors $\zeta^{\frac{p-1}{n}}$ est d'ordre n (*cf.* Exercice 5.1, question 1).

□

Démonstration du Théorème 4.3 : Nous allons montrer que pour tout $k > n$, il existe un nombre premier $p \equiv 1 \pmod{n}$ tel que $p > k$.
Soit $k > n$. On pose $a := k!$, et on va montrer que si l'on prend p un facteur premier de $\Phi_n(a)$, alors celui-ci est nécessairement strictement supérieur à k, et satisfait $p \equiv 1 \pmod{n}$.

— Tout d'abord, avant de prendre un facteur premier de $\Phi_n(a)$, on doit montrer qu'il en admet, c'est-à-dire qu'il n'est pas égal à ± 1. Or (je conseille de faire un dessin pour se convaincre de la première inégalité qui apparaît ci-dessous) :

$$|\Phi_n(a)| = \prod_{\zeta \in \mu_n^\star(\mathbf{C})} |a - \zeta| \geqslant \prod_{\zeta \in \mu_n^\star(\mathbf{C})} (a-1) \geqslant 5^{\varphi(n)} \geqslant 5.$$

car $a = k!$ et $k > n \geqslant 2$. On a donc bien montré que $\Phi_n(a)$ n'était pas un inversible de $\mathbf{Z}$.

— Soit p un facteur premier de $\Phi_n(a)$. Si, par l'absurde, on avait $p \leqslant k$. Alors p diviserait a, et donc diviserait $\Phi_n(a) - \Phi_n(0)$ car c'est un polynôme en a à coefficients entiers, dont on a tué le terme constant. Mais comme d'autre part p divise $\Phi_n(a)$, on en déduirait que p divise $\Phi_n(0)$. Or c'est impossible car $\Phi_n(0) = \pm 1$ (en effet, $\Phi_n(0)$ est un entier, mais il est aussi égal au signe près au produit des racines primitives n^{e} de l'unité dans $\mathbf{C}$, donc de module 1). Ainsi, $p > k$.

Preuve alternative : comme p divise $\Phi_n(a)$, il divise $a^n - 1$ (car Φ_n divise $X^n - 1$) et donc p ne peut pas diviser a car sinon il diviserait 1.

— Enfin, pour montrer que $p \equiv 1 \pmod{n}$, on utilise le Lemme 4.4 qui nous dit qu'il suffit de montrer que $\mathbf{F}_p$ contient une racine primitive n^{e} de l'unité. Or comme p divise $\Phi_n(a)$, on a $\overline{\Phi}_n(\overline{a}) = 0$ dans $\mathbf{F}_p$. Mais d'après la Proposition 3.4, $\overline{\Phi}_n$ est le $n^{\text{ème}}$ polynôme cyclotomique sur $\mathbf{F}_p$ (car l'hypothèse « p ne divise pas n » est satisfaite car $p > k > n$). Donc les racines de $\overline{\Phi}_n$ dans un corps de décomposition de $X^n - 1$ sur $\mathbf{F}_p$ sont exactement les racines primitives $n^{\text{èmes}}$ de l'unité. Donc $\overline{a}$ est une racine primitive $n^{\text{ème}}$ qui appartient à $\mathbf{F}_p$, ce qui conclut.

Preuve alternative : si l'on veut éviter d'utiliser la Proposition 3.4 et ne parler que de polynômes cyclotomiques sur $\mathbf{Q}$, on peut procéder ainsi : si $\overline{a}$ était d'ordre $d < n$ dans $\mathbf{F}_p^\times$ alors on aurait $\overline{a}^d - 1 \equiv 0 \pmod{p}$, mais on sait que $\overline{a}^d - 1 = \prod_{d'|d} \overline{\Phi}_{d'}(\overline{a})$ (c'est juste l'évaluation en a et la réduction modulo p de l'égalité du Lemme 2.2). Donc il existe au moins un diviseur d' de d tel que $\overline{\Phi}_{d'}(\overline{a}) = 0$ dans $\mathbf{F}_p$. Mais comme on a aussi $\overline{\Phi}_n(\overline{a}) = 0$, la formule

$$X^n - 1 = \prod_{d|n} \overline{\Phi}_d$$

montre que $\overline{a}$ est racine de multiplicité au moins égale à 2 de $X^n - 1$ dans $\mathbf{F}_p$. Or ceci est impossible car $X^n - 1$ est séparable car p est premier avec n (car $p > k > n$).

Remarque 4.5. La preuve précédente est inspirée de l'exercice 14 p.93 de [Per] et de la preuve de la Proposition VII.13 de [Goz]. Une présentation légèrement différente se trouve dans [CP] (preuve par

l'absurde qui rend plus clair le parallèle avec la preuve d'Euclide de l'infinité des nombres premiers). Nous avons même la chance de pouvoir voir l'exercice corrigé au tableau par Philippe Caldero sur sa chaîne : https://www.youtube.com/watch?v=2B6467zbnrU. En fin de vidéo, il fait la remarque qu'Euclide, en montrant qu'il existe une infinité de nombres premiers (essentiellement en considérant un facteur premier de $k!+1$) était en fait en train de faire un cas particulier de la preuve ci-dessus, car $k!+1$ n'est rien d'autre que $\Phi_2(k!)$. Cela lui donnait l'existence d'une infinité de nombres premiers congrus à 1 modulo 2, c'est-à-dire impairs. Pour n quelconque, nous avons vu que ce sont les facteurs premiers de $\Phi_n(k!)$ qui nous ont permis de montrer qu'il existe une infinité de nombres premiers congrus à 1 modulo n.

Remarque 4.6. Pour $n = 10$, le Théorème 4.3 est très concret : il affirme qu'il existe une infinité de nombres premiers qui terminent par un 1 (en écriture décimale).

4.4. Constructibilité de polygones réguliers

Dans ce paragraphe, nous allons voir que l'étude des extensions cyclotomiques permet de répondre à une question géométrique très concrète : quels polygones réguliers sont constructibles à la règle et au compas ?
Avant de s'attaquer à cette question, il nous faut donner une définition précise de ce qu'on entend par constructible à la règle et au compas. Comme on s'y attend, un point va être constructible si il est possible de le réaliser comme intersection de droites ou de cercles s'appuyant sur des points précédemment construits. C'est ce qu'on dit ci-dessous :

Définition 4.7.
— *Étant donnée une partie $S \subseteq \mathbf{C}$, on appelle « courbes de S » les droites passant par deux points de S et les cercles centrés en un point de S et de rayon la distance entre deux points de S.*
— *On dit qu'un nombre complexe z est constructible à la règle et au compas en une étape à partir de S si z est un point d'intersection de deux courbes de S distinctes.*
— *On dit que z est constructible en n étapes s'il existe une suite $z_1, \dots, z_n$ telle que $z_n = z$ et pour tout i, le nombre complexe z_{i+1} est constructible en une étape à partir de $S \cup \{z_1, \dots, z_i\}$.*
— *Enfin, z est dit constructible s'il existe un entier n tel que z soit constructible en n étapes à partir de $S = \{0, 1\}$. On note $\mathscr{C}$ l'ensemble des nombres complexes constructibles.*

Remarque 4.8. Dans la définition des courbes de S, nous avons autorisé les « reports de longueurs », car on pouvait aller chercher n'importe quel rayon entre deux points de S, puis centrer le cercle en un autre point. On pourrait donner une définition alternative en autorisant seulement les cercles s'appuyant sur deux points de S, mais en fait ces deux constructions donnent exactement les mêmes ensembles de nombres constructibles, *cf.* [Goz, Prop. IV.6].

On peut montrer (*cf.* Exercice 5.7) le résultat suivant (ce n'est pas évident, il faut se souvenir de certaines constructions élémentaires à la règle et au compas, que l'on ne révise pas beaucoup au cours des études supérieures).

Proposition 4.9. *$\mathscr{C}$ est un sous-corps de $\mathbf{C}$ stable par racine carrée (dans le sens suivant : si $\alpha \in \mathscr{C}$ alors les racines complexes du polynôme $X^2 - \alpha$ sont elles aussi constructibles).*

Enfin, le théorème principal que nous allons utiliser pour répondre à notre problème de construction de polygones réguliers est le théorème de Wantzel :

Théorème 4.10 (Wantzel, voir par exemple [Tau, Th. 11.4.7])**.** *Un nombre complexe z est constructible si et seulement si il existe un entier n et une tour d'extensions quadratiques*

$$\mathbf{Q} = L_0 \subset L_1 \subset \cdots \subset L_n \subset \mathbf{C}$$

telle que $z \in L_n$.

Remarque 4.11. « Tour d'extensions quadratiques » signifie que pour tout $i \in \{0, \dots, n-1\}$, $[L_{i+1} : L_i] = 2$.

Avant de démontrer ce théorème, nous énonçons un lemme intermédiaire qui dit que les constructions à la règle et au compas ne risquent pas de faire apparaître d'équations de degré supérieur à 2 (ce qui n'est pas clair à priori pour l'intersection de deux cercles notamment).

Lemme 4.12. *Soit K un sous-corps de $\mathbf{R}$. On note $\mathcal{U} := K \times K$ l'ensemble des points du plan $\mathbf{R}^2$ à coordonnées dans K, on désigne par $\mathcal{D}$ l'ensemble des droites passant par deux points de $\mathcal{U}$ et par $\mathcal{C}$ l'ensemble des cercles centrés en un point de $\mathcal{U}$ et de rayon la distance entre deux points de $\mathcal{U}$.*

(1) *Si $d \in \mathcal{D}$, alors d admet au moins une équation à coefficients dans K.*
(2) *Si $\gamma \in \mathcal{C}$, alors γ admet au moins une équation à coefficients dans K.*
(3) *Si $d_1, d_2 \in \mathcal{D}$ sont deux droites distinctes sécantes en un point M alors $M \in \mathcal{U}$.*
(4) *Si M est un point commun à une droite $d \in \mathcal{D}$ et un cercle $\gamma \in \mathcal{C}$ alors ou bien $M \in \mathcal{U}$, ou bien il existe une extension quadratique L/K telle que les coordonnées de M appartiennent à L.*
(5) *Si M est un point commun à deux cercles distincts $\gamma_1, \gamma_2 \in \mathcal{C}$, alors ou bien $M \in \mathcal{U}$ ou bien il existe une extension quadratique L/K telle que les coordonnées de M appartiennent à L.*

Démonstration. *cf.* [Goz, Prop. IV.11]. Nous présentons seulement la preuve de quelques uns des points. Par exemple pour (2), si $\gamma \in \mathcal{C}$ et qu'on note $C \in \mathcal{U}$ le centre du cercle et $A, B \in \mathcal{U}$ deux points dont la distance est le rayon de γ alors une équation de γ est donnée par

$$|z - z_C|^2 = |z_B - z_A|^2$$

où on a noté $z_M = x_M + iy_M$ l'affixe de M pour $M \in \{A, B, C\}$. C'est-à-dire

$$\gamma = \left\{z = x + iy \in \mathbf{C}; |z - z_C|^2 = |z_B - z_A|^2\right\}$$

En développant, on obtient l'équation de γ sous la forme

$$x^2 + y^2 - 2x_C x - 2y_C y + x_C^2 + y_C^2 - (x_B - x_A)^2 - (y_B - y_A)^2 = 0$$

qui est bien une équation en (x, y) à coefficients dans K car les coordonnées de A, B, C appartiennent à K et K est un sous-corps de $\mathbf{R}$.

Pour le point (4), si $M = (x, y)$ est à l'intersection d'une droite de $\mathcal{D}$ et d'un cercle de $\mathcal{C}$, alors d'après (1) et (2), il existe $a, b, c, d, e, f \in K$ tels que

$$\begin{cases} ax + by + c = 0 \\ x^2 + y^2 + 2dx + 2ey + f = 0 \end{cases}$$

Comme a et b ne sont pas simultanément nuls, on peut par exemple supposer $a \neq 0$ et en déduire que

$$x = -\frac{by + c}{a}$$

appartient à $K(y)$, de sorte que $K(x, y) = K(y)$. Enfin, en injectant $x = -\frac{by+c}{a}$ dans l'équation du cercle, on obtient une équation polynomiale de degré au plus deux, à coefficients dans K, satisfaite par y, donc $[K(y) : K] \leqslant 2$. On a donc bien montré, en prenant $L = K(y)$ qu'il existait une extension de degré au plus 2, qui contenait à la fois x et y (en effet, on a vu précédemment que x appartenait à $K(y)$).

Pour le point (5), si (x, y) est à l'intersection de deux cercles de $\mathcal{C}$ distincts alors ses coordonnées satisfont un système à coefficients dans K de la forme

$$\begin{cases} x^2 + y^2 + 2ax + 2by + c = 0 \\ x^2 + y^2 + 2a'x + 2b'y + c' = 0 \end{cases}$$

Mais en effectuant la soustraction des deux lignes on montre que ce système est équivalent à

$$\begin{cases} x^2 + y^2 + 2ax + 2by + c = 0 \\ 2(a' - a)x + 2(b' - b)y + c' - c = 0 \end{cases}$$

ce qui nous ramène au cas précédent puisque la deuxième ligne est maintenant l'équation d'une droite. □

Démonstration du Théorème 4.10. On reproduit ici à peu de choses près les preuves très détaillées qui se trouvent dans [Car] ou [Goz, Th. IV.12 et XVII. 2] par exemple.

— Si z est constructible alors il existe un entier k et une suite de nombres complexes $z_1, \dots, z_k$ telle que $z_k = z$ et
  — z_1 est constructible en une étape à partir de $\{0, 1\}$,
  — z_2 est constructible en une étape à partir de $\{0, 1\} \cup \{z_1\}$
  — ...
  — z_k est constructible en une étape à partir de $\{0, 1\} \cup \{z_1, \dots, z_{k-1}\}$.

  Pour tout $j \in \{1, \dots, k\}$, on note $z_j = x_j + iy_j$ et $K_j = K_{j-1}(x_j, y_j)$ avec $K_0 = \mathbf{Q}$. On construit ainsi une suite croissante de sous-corps de $\mathbf{R}$ (n'ayez crainte, nous rajouterons le nombre complexe i au bout de la tour, cela arrivera en temps voulu et ne causera pas de grande difficulté).
  Montrons que pour tout $j \in \{1, \dots, k\}$, on a $[K_j : K_{j-1}] \leqslant 2$.

  Soit $j \in \{1, \dots, k\}$. Alors comme z_j est construtible en une étape à partir de $\{0, 1\} \cup \{z_1, \dots, z_{j-1}\}$ et que ces points sont à coordonnées dans K_{j-1}, tous les cas $(3) - (5)$ du Lemme 4.12 nous assurent qu'on engendre une extension de degré au plus 2 en adjoignant à K_{j-1} les coordonnées x_j et y_j, ce qui montre bien que $[K_j : K_{j-1}] \leqslant 2$.

  Enfin, on ajoute $K_{k+1} = K_k(i)$ à la fin de cette tour d'extensions. C'est une extension quadratique car $i \notin K_k$ car K_k est un sous-corps de $\mathbf{R}$ (on n'a fait qu'ajouter successivement les réels correspondant aux coordonnées des points $z_1, \dots, z_k$).

  Ainsi, on a construit une tour d'extensions $K_0 \subseteq K_1 \subseteq \cdots \subseteq K_{k+1}$ telle que $z = x + iy \in K_{k+1}$ et pour tout $j \in \{1, \dots, k+1\}, [K_j : K_{j-1}] \leqslant 2$. Il suffit alors d'extraire de cette suite d'extensions une sous-suite strictement croissante (autrement dit on enlève les redondances $K_j = K_{j-1}$ qui apparaissent lorsque $[K_j : K_{j-1}]$ est égal à 1) pour obtenir une tour d'extensions quadratiques comme dans l'énoncé.

— Réciproquement, s'il existe une telle tour d'extensions quadratiques, nous allons montrer par récurrence sur i que pour tout $i \in \{1, \dots, n\}$ on a $L_i \subseteq \mathscr{C}$.
  Tout d'abord, comme $\mathscr{C}$ est un sous-corps de $\mathbf{C}$, il contient $\mathbf{Q}$, donc on a bien $L_0 \subseteq \mathscr{C}$.
  Soit $i \in \{0, \dots, n-1\}$. Si l'on suppose que $L_i \subseteq \mathscr{C}$, montrons que $L_{i+1} \subseteq \mathscr{C}$. Soit $\alpha \in L_{i+1}$. Comme $[L_{i+1} : L_i] = 2$, la famille $1, \alpha, \alpha^2$ est nécessairement liée sur L_i, donc il existe $a, b, c \in L_i$ (non tous nuls) tels que $a\alpha^2 + b\alpha + c = 0$. Donc si $a = 0$, on a $\alpha = -c/b \in L_i \subseteq \mathscr{C}$, donc $\alpha \in \mathscr{C}$. Si $a \neq 0$, alors en notant δ un complexe tel que $\delta^2 = b^2 - 4ac$, on a $\alpha = \frac{-b \pm \delta}{2a}$ qui appartient à $\mathscr{C}$ car $a, b, c \in L_i \subseteq \mathscr{C}$ et $\mathscr{C}$ est un sous-corps de $\mathbf{C}$ stable par racine carrée.

□

Corollaire 4.13. *Si $z \in \mathscr{C}$ alors $[\mathbf{Q}(z) : \mathbf{Q}]$ est une puissance de 2.*

Démonstration. Si z est constructible, alors d'après le théorème de Wantzel il existe une tour d'extension quadratiques

$$\mathbf{Q} = L_0 \subset L_1 \subset \cdots \subset L_n \subset \mathbf{C}$$

telle que $z \in L_n$. Par multiplicativité du degré dans les tours d'extensions, on a

$$[L_n : \mathbf{Q}] = \prod_{i=0}^{n-1} [L_{i+1} : L_i] = 2^n$$

et comme $z \in L_n$, on a $\mathbf{Q}(z) \subseteq L_n$ et donc $[\mathbf{Q}(z) : \mathbf{Q}]$ divise $[L_n : \mathbf{Q}]$, d'où le résultat. □

Remarque 4.14. (1) Le Corollaire 4.13 permet d'apporter une réponse à certains problèmes grecs classiques tels que l'impossibilité de la duplication du cube, de la trisection de l'angle, de la quadrature du cercle : *cf.* [Per, p. 69, 70].

(2) La réciproque du Corollaire 4.13 est fausse : *cf.* [Goz, Prop. IV.33].

(3) En faisant appel à la théorie de Galois, on peut obtenir une condition nécessaire et suffisante à la constructibilité (*cf.* [Goz, Th. XVII.4] dans le cas réel) :
Un complexe z est constructible si et seulement si il est algébrique et le corps de décomposition D du polynôme minimal de z sur $\mathbf{Q}$ satisfait $[D : \mathbf{Q}] = 2^n$ pour un certain entier n.
On peut aussi y arriver sans utiliser la théorie de Galois, *cf.* la note d'Antoine Chambert-Loir accessible ici : https://webusers.imj-prg.fr/~antoine.chambert-loir/publications/papers/compas5.pdf

Nous avons maintenant tous les outils pour démontrer le théorème de Gauss-Wantzel, qui caractérise les entiers n pour lesquels le polygone régulier à n côtés est constructible à la règle et au compas. La caractérisation fait intervenir les nombres de Fermat, dont nous rappelons maintenant la définition.

Définition 4.15. *Pour tout $k \in \mathbf{N}$, on note $F_k := 2^{2^k} + 1$ et on l'appelle le k^e nombre de Fermat.*

Les nombres F_0, F_1, F_2, F_3, F_4 sont premiers, et Fermat avait conjecturé que tous les F_k étaient premiers. Cependant Euler a démontré que F_5 n'était pas premier, et on sait désormais que pour tout $k \in \{5, \ldots, 32\}$, F_k n'est pas premier. On soupçonne, mais on ne sait pas démontrer, que les seuls nombres premiers de Fermat sont les 5 premiers.

Le lemme suivant explique la présence d'une puissance de 2 dans la définition des nombres de Fermat (si l'on veut avoir un peu d'espoir qu'ils soient premiers) :

Lemme 4.16. *Soit $m \geqslant 1$. Si $2^m + 1$ est premier alors m est une puissance de 2.*

Théorème 4.17 (Gauss-Wantzel)**.** *Le polygone régulier à n côtés est constructible à la règle et au compas si et seulement si n est le produit d'une puissance de 2 et de nombres premiers de Fermat distincts.*

5. Exercices

Exercice 5.1. *Trois questions incontournables*

Soit $(G, .)$ un groupe quelconque,

1. Soit $x \in G$ un élément d'ordre $n \geqslant 1$. Montrer que pour tout $k \geqslant 1$, l'ordre de x^k est égal à $\frac{n}{\text{pgcd}(n,k)}$.
2. Montrer que si G est un groupe cyclique d'ordre n, alors pour tout diviseur positif d de n, il admet un unique sous-groupe d'ordre d, explicitement donné par $\{y \in G \mid y^d = 1\}$.
3. Soit $a, b \in G$ deux éléments d'ordres respectifs m et n. Montrer que si a et b commutent et m et n sont premiers entre eux, alors ab est d'ordre mn. Trouver un contre exemple lorsque l'on retire l'une des hypothèses.

Cet exercice s'applique en particulier au cas du groupe $\mathbf{C}^\times$, et nous dit par exemple que si ζ est une racine primitive n^{e} de l'unité dans $\mathbf{C}$, les autres racines primitives sont les ζ^k pour k premier avec n.

Exercice 5.2. Soit m et n deux entiers supérieurs ou égaux à 3. Combien de sommets en commun ont les polygones réguliers à n côtés et à m côtés ?

Exercice 5.3. *Groupe de Galois d'une extension cyclotomique*

Soit $n \geqslant 2$ et soit $\zeta \in \mu_n^\star(\mathbf{C})$. On note G le groupe des automorphismes du corps $\mathbf{Q}(\zeta)$ (mais comme un automorphisme fixe le sous-corps premier, ce groupe est aussi ce qu'on appelle le groupe de Galois de l'extension $\mathbf{Q}(\zeta)/\mathbf{Q}$).

1. Montrer que pour tout $\sigma \in G$, il existe un entier $m(\sigma)$, unique modulo n et inversible modulo n, tel que $\sigma(\zeta) = \zeta^{m(\sigma)}$.
2. Montrer que
$$\begin{array}{ccc} G & \to & (\mathbf{Z}/n\mathbf{Z})^\times \\ \sigma & \mapsto & m(\sigma) \,(\text{mod}\, n) \end{array}$$
est un isomorphisme de groupes.

Exercice 5.4. Soit $\zeta \in \mu_n^\star(\mathbf{C})$ et soit $K := \mathbf{Q}(\zeta)$. On note G le groupe des automorphismes de K (qui a été déterminé à l'exercice précédent). Montrer que le « sous-corps fixe »

$$K^G := \{x \in K \mid \forall \sigma \in G,\ \sigma(x) = x\}$$

est égal à $\mathbf{Q}$.

Exercice 5.5. *Racines complexes de l'unité et caractères des corps finis*

On rappelle que les caractères d'un groupe abélien $(G, .)$ sont les morphismes de groupes de $(G, .)$ dans $(\mathbf{C}^\times, .)$. Soit p un nombre premier. Pour tout $a \in \mathbf{F}_p$, on définit

$$\begin{array}{rccc} \psi_a & : & \mathbf{F}_p & \to & \mathbf{C}^\times \\ & & x & \mapsto & e^{\frac{2i\pi ax}{p}} \end{array}$$

1. Montrer que les caractères du groupe additif $\mathbf{F}_p$ sont exactement les ψ_a.
2. Réinterpréter l'égalité
$$\sum_{k=0}^{p-1} e^{\frac{2i\pi k}{p}} = 0$$
en termes d'orthogonalité des caractères.

Exercice 5.6. *Polynômes et palindromes*

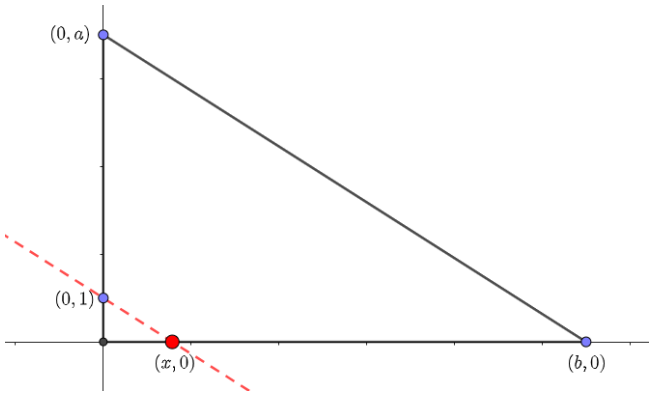
Dans cet exercice, nous allons montrer que pour tout $n > 1$, la suite des coefficients du polynôme Φ_n est un palindrome : on lit la même suite de coefficients qu'on la lise de gauche à droite ou de droite à gauche.
Si $P = \sum_{k=0}^{n} a_k X^k \in \mathbf{R}[X]$, on définit son polynôme réciproque $P^\star$ comme

$$P^\star(X) := \sum_{k=0}^{n} a_{n-k} X^k$$

1. Soit $\alpha \in \mathbf{C}$ un nombre complexe de module 1, algébrique sur $\mathbf{Q}$. Montrer que son polynôme minimal est égal ou opposé à son polynôme réciproque.
2. Montrer que si l'on suppose de plus $\alpha \neq 1$, alors son polynôme minimal est égal à son polynôme réciproque. Remarquer que cela s'applique aux polynômes cyclotomiques Φ_n pour $n > 1$.

Exercice 5.7. *Quelques constructions à la règle et au compas*

1. Soit A, B deux points du plan. Comment trace-t-on la médiatrice du segment $[AB]$ à la règle et au compas ?
2. Si C est un troisième point, comment trace-t-on la perpendiculaire à (AB) passant par C ? On pourra distinguer les cas $C \in (AB)$ et $C \notin (AB)$.
3. En déduire qu'un nombre complexe $z = x + iy$ est constructible si et seulement si x et y le sont.
4. Comment trace-t-on la parallèle à (AB) passant par C ?
5. Montrer que tout rationnel est constructible. *Indication :*



6. Montrer que l'ensemble $\mathscr{C}_{\mathbf{R}}$ des nombres réels constructibles est un sous-corps de $\mathbf{R}$.
7. Montrer que si x est un réel positif constructible alors $\sqrt{x}$ est constructible.
8. En déduire la Proposition 4.9. *Indication : s'appuyer sur la question 3 et ce qu'on sait du cas réel.*

Exercice 5.8. *Sommes de Ramanujan*

Pour $m \in \mathbf{N}^*$ et $n \in \mathbf{N}$, on note

$$S(m,n) := \sum_{\zeta \in \mu_m(\mathbf{C})} \zeta^n \quad \text{resp.} \quad S^\star(m,n) := \sum_{\zeta \in \mu_m^\star(\mathbf{C})} \zeta^n$$

la somme des puissances n^{e} des racines m^{e} de l'unité, resp. la somme des puissances n^{e} des racines primitives m^{e} de l'unité.

1. Montrer que $S(m,n) = \sum_{d|m} S^\star(d,n)$.
2. En utilisant la formule d'inversion de Möbius, en déduire que $S^\star(m,n) = \sum_{d|m} S(d,n)\mu\left(\frac{m}{d}\right)$.
3. Déterminer une expression plus simple de $S(d,n)$ et en déduire que

$$S^\star(m,n) = \sum_{d|\mathrm{pgcd}(m,n)} d\mu\left(\frac{m}{d}\right)$$

4. En déduire la valeur du coefficient du terme de degré $\varphi(m)-1$ de Φ_m.
5. Observer que si m a un facteur carré, les racines primitives m^{e} ne sont pas linéairement indépendantes sur $\mathbf{Q}$. En fait, les racines primitives m^{e} sont linéairement indépendantes sur $\mathbf{Q}$ si et seulement si m est sans facteur carré, mais le sens que nous n'avons pas démontré est plus difficile.

Références

[Car] Jean-Claude Carrega. *Théorie des corps, la règle et le compas.* Hermann.

[CP] Philippe Caldero and Marie Peronnier. *Carnet de voyage en Algébrie.* Calvage et Mounet.

[Dem] Michel Demazure. *Cours d'Algèbre.* Cassini.

[Goz] Ivan Gozard. *Théorie de Galois.* Ellipses.

[Ort] Pascal Ortiz. *Exercices d'Algèbre.* Ellipses.

[Per] Daniel Perrin. *Cours d'Algèbre.* Ellipses.

[Pey] Gabriel Peyré. *L'algèbre discrète de la transformée de Fourier.* Ellipses.

[Ser] Jean-Pierre Serre. *Cours d'Arithmétique.* Presses universitaires de France.

[Tau] Patrice Tauvel. *Corps commutatifs et théorie de Galois.* Calvage et Mounet.