Polynômes cyclotomiques + Dirichlet faible + Application aux GAF + Bonus : Galois inverse

Dans ce développement, on prouve que les polynômes cyclotomiques sont irréductibles, on en déduit un cas particulier du théorème de la progression arithmétique de Dirichlet, dont on déduit que tous les groupes abéliens finis (GAF) sont des quotients de groupes de la forme $\mathbb{Z}/n\mathbb{Z}^\times$.

Une application (optionnelle à ce développement) est que tout groupe abélien fini est un groupe de Galois d'une extension galoisienne [1].

Vous pouvez librement adapter ce développement : si vous voulez en faire un développement pas trop dur (mais de bon niveau quand même !), vous pouvez ignorer l'application à Galois. Si vous voulez faire du Galois, alors il faudra ignorer certains trucs de base sur les polynômes cyclotomiques (en allant directement vers la preuve de leur irréductibilité qui me semble essentielle).

Dans mon cas, je faisais tout depuis les trucs de base jusqu'à l'application aux GAF, mais je comptais mettre l'application à Galois dans le plan, hors du développement.

Par contre, il est incontournable de maîtriser chaque point dans cette feuille (à part Galois si c'est pas votre tasse de thé) !

I. Polynômes cyclotomiques

0.1 Trucs de base (optionnel)

Définition I.0.1. (Polynômes cyclotomiques) $\Phi_n = \prod_{k\wedge n=1} (X - \omega^k)$ où $\omega = e^{2\pi i k/n}$.

Proposition I.0.2.
$\prod_{d|n} \Phi_d = X^n - 1$.

Preuve. Trier les éléments $k \in [\![1, n]\!]$ selon leur pgcd avec n revient à les trier selon leur ordre dans $\mathbb{Z}/n\mathbb{Z}$. □

Proposition I.0.3.
$\forall n \in \mathbb{N}^*$, $\Phi_n \in \mathbb{Z}[X]$.

Preuve. Récurrence forte sur n en obtenant Φ_n comme quotient de $X^n - 1$ et des Φ_d pour une division euclidienne dans $\mathbb{Z}[X]$ (possible car on divise par des polynômes unitaires). □

Pour la preuve de l'irréductibilité, vous pouvez (ou non) prouver ce lemme (ou simplement le mentionner à l'oral selon la leçon) :

Lemme I.0.4. Gauss
Soit $Q \in \mathbb{Q}[X]$ un polynôme unitaire divisant (dans $\mathbb{Q}[X]$) un polynôme $P \in \mathbb{Z}[X]$ unitaire. Alors $Q \in \mathbb{Z}[X]$.

Preuve. Soit $R = P/Q \in \mathbb{Q}[X]$. Comme $Q, R \in \mathbb{Q}[X]$, il existe $a, b \in \mathbb{Z}^*$ (entiers non nuls) tq $aR, bQ \in \mathbb{Z}[X]$. Alors $aRbQ = abP$ donc par le lemme de Gauss sur le contenu, $c(aR)c(bQ) = ab$ (car $c(P) = 1$). Alors $\frac{aR}{c(aR)}\frac{bQ}{c(bQ)} = P$. En regardant les coefficients dominants, on trouve que celui de $\frac{bQ}{c(bQ)}$ est inversible, mais comme Q est unitaire, ça veut dire que $\frac{b}{c(bQ)}$ est inversible. Or, $\frac{bQ}{c(bQ)} \in \mathbb{Z}[X]$ (par définition du contenu) donc $Q \in \mathbb{Z}[X]$. Remarque : la même chose marche pour R. □

0.2 Irréductibilité

1. C'est une réponse partielle au problème de Galois inverse. En fait, tous les groupes résolubles ont cette propriété, mais c'est difficile.

Théorème I.0.5.
Les Φ_n sont irréductibles.

Preuve. **Etape 1 : réduction du problème** : Soit ω une racine primitive n-ième de l'unité (i.e. un élément d'ordre n dans $\mathbb{C}^\times$). Soit μ_x le polynôme minimal sur $\mathbb{Q}$ d'un élément $x \in \mathbb{C}$ algébrique. But : si $k \wedge n = 1$, prouver que $\mu_\omega = \mu_{\omega^k}$ (ça prouve que $\Phi_n = \mu_\omega$ d'où l'irréductibilité de Φ_n). En décomposant k comme un produit de nombres premiers, il suffit de prouver ce résultat pour k premier (puis de l'itérer). On prend donc p un nombre premier ne divisant pas n.

Etape 2 : comparaison des polynômes minimaux : On remarque que $\mu_{\omega^p}(X^p)$ est nul en ω donc $\mu_\omega \mid \mu_{\omega^p}(X^p)$, on prend Q le quotient de cette division, qui, par le lemme I.0.4, est dans $\mathbb{Z}[X]$. On note $\overline{P} \in \mathbb{F}_p[X]$ la réduction modulo p d'un élément $P \in \mathbb{Z}[X]$. On a donc $\overline{Q}\overline{\mu_\omega} = \overline{\mu_{\omega^p}(X^p)}$. Ce dernier polynôme est égal à $\overline{\mu_{\omega^p}(X)}^p$ par le petit théorème de Fermat donc $\overline{\mu_\omega}$ divise $\overline{\mu_{\omega^p}}$.

Etape 3 : conclusion : Supposons par l'absurde que $\mu_\omega \neq \mu_{\omega^p}$. Comme p et n sont premiers entre eux, ω^p est encore une racine primitive n-ième de l'unité donc est une racine de Φ_n. Alors, puisque la formule I.0.2 donne la divisibilité $\mu_\omega \mu_{\omega^p} \mid X^n - 1$, on a $\overline{\mu_\omega \mu_{\omega^p}} \mid \overline{X^n - 1}$. Par conséquent, μ_ω^2 divise $\overline{X^n - 1}$ qui admet donc un facteur double. Un calcul simple montre qu'alors il n'est pas premier à sa dérivée. Or, sa dérivée est nX^{n-1} qui, puisque $\overline{n} \neq 0 \in \mathbb{F}_p$, est clairement premier à $\overline{X^n - 1}$. C'est une contradiction. □

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

Il faut connaître la version forte (mais pas sa preuve, sauf si vous êtes le GOAT) : si $a \wedge b = 1$, alors il exite une infinité de nombres premiers p tq $p \equiv a[b]$. La version suivante est déjà très intéressante :

Théorème II.0.1. Dirichlet faible
Soit $m \in \mathbb{N}*$. Il existe une infinité de nombres premiers p congrus à 1 modulo m.

Preuve. Il suffit de prouver que pour tout $k > m$, il existe un nombre premier $p > k$ congru à 1 modulo m. Notre candidat sera p un diviseur premier quelconque de $\Phi_m(k!)$. p est donc premier à $k!$ [2]. Donc $p > k$ comme voulu, et $p \wedge m = 1$.

Reste à prouver que $p \equiv 1[m]$. Il suffit de prouver que $m \mid p-1$, il suffit donc de trouver un élément de $\mathbb{F}_p^\times$ d'ordre exactement m et d'appliquer le théorème de Lagrange. On pose $x = \overline{k!} \in \mathbb{F}_p$. Alors $\overline{\Phi_m}(x) = 0$ dans $\mathbb{F}_p$. Donc comme $\overline{\Phi_m} \mid \overline{X^m - 1}$, on a $x^m = 1$ donc l'ordre de x divise m. On note $\omega \mid m$ l'ordre de x. Supposons par l'absurde que $\omega \neq m$. Alors, puisque $x^\omega - 1 = 0$, on a par I.0.2 que $\prod_{d \mid \omega} \Phi_d(x) = 0$ donc il existe $d \mid \omega$ (donc $d \neq m$) tel que $\Phi_d(x) = 0$. Donc, puisque, encore par I.0.2, $\Phi_d \Phi_m \mid X^m - 1$, on a que x est une racine double de $\overline{X^m - 1}$ donc ce polynôme est encore non premier à sa dérivée, ce qui est impossible (même argument que précédemment). Donc $\omega = m$, cqfd. □

III. Application aux GAF

Corollaire III.0.1.
Tout groupe abélien fini est un quotient d'un groupe $\mathbb{Z}/n\mathbb{Z}^\times$ pour un certain n.

Preuve. Par théorème de structure des GAF, il existe m_i tq $G \simeq \prod_{i=1}^{r} \mathbb{Z}/m_i\mathbb{Z}$. Pour chaque i, prenez un nombre p_i (par dirichlet faible) premier congru à 1 modulo m_i, et tels que $p_1 < p_2 < \cdots < p_r$. Alors $n = \prod_i p_i$ convient puisque $\mathbb{Z}/n\mathbb{Z}^\times \simeq \prod_{i=1}^{r} \mathbb{Z}/p_i\mathbb{Z}^\times \simeq \prod_{i=1}^{r} \mathbb{Z}/(p_i - 1)\mathbb{Z}$. Comme m_i divise $p_i - 1$, il existe

2. car $\Phi_m(0) = \pm 1$ car c'est un entier de module 1 puisque produit de racines de l'unité

une surjection canonique $\mathbb{Z}/(p_i-1)\mathbb{Z} \twoheadrightarrow \mathbb{Z}/m_i\mathbb{Z}$ donc une surjection $\mathbb{Z}/n\mathbb{Z}^\times \twoheadrightarrow G$ donc G est un quotient de $\mathbb{Z}/n\mathbb{Z}^\times$. □

IV. Problème inverse de Galois pour les GAF (optionnel)

Vous avez tout à fait le droit, dans le cadre de l'agreg, de ne jamais vous intéresser à la théorie de Galois. Mais peut-on se passer d'une théorie si belle ? Peut-on se passer d'une théorie qui peut vous faire une belle partie HP dans la moitié des leçons d'algèbre au programme, afin de bien vous la péter [3] ?

Corollaire IV.0.1.
Si G est un groupe abélien fini, alors il existe $\mathbb{K}/\mathbb{Q}$ une extension galoisienne finie de $\mathbb{Q}$ telle que $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \simeq G$.

Preuve. Considérer le n donné par le corollaire précédent. Alors l'extension $\mathbb{Q}(\omega)/\mathbb{Q}$, où $\omega = e^{2\pi i/n}$ est galoisienne de groupe $\mathbb{Z}/n\mathbb{Z}^\times$ (classique, au fond ça utilise juste l'irréductibilité de Φ_n). Ainsi, votre groupe G est quotient de $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ donc il existe un sous-groupe distingué H de $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ tel que $G \simeq \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})/H$. D'un côté, H est un sous-groupe de $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ donc par la correspondance de Galois il existe un corps $\mathbb{Q} \subset \mathbb{K} \subset \mathbb{Q}(\omega)$ tel que $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{K}) = H$. De l'autre côté, toujours par la correspondance de Galois, le fait que $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{K})$ soit distingué implique que l'extension $\mathbb{K}/\mathbb{Q}$ est galoisienne, et on a $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})/\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{K}) \simeq \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$. On a donc gagné ! □

Références

Tout ça doit exister dans le Perrin. Le Rombaldi peut vous aider avec le contenu des polynômes pour le lemme de Gauss.

Pour apprendre la théorie de Galois, je ne peux que vous conseiller les polycopiés de Nicolas Tosel (ultra clairs et complets, vont droit au but dans un langage compréhensible par un élève de maths sup), chinables sur le web mais évidemments interdits le jour de l'oral). Ou sinon Le Grand Combat (Berhuy)/Gozard/Petit Compagnon des nombres (de Boyer)/etc dans votre BU préférée.

3. à condition de savoir faire quelques exos sur ce que vous dites. Le jury peut vous détester si vous ne maîtrisez pas des trucs qu'il trouve basiques dans un sujet HP que vous présentez