Une Condition suffisante pour que ton petit cousin puisse lire la table de caractères (i.e. elle est à valeur dans $\mathbb{Z}$)

Introduction

Voilà un chouette développement très recasable. J'ai rédigé ma version en utilisant de la théorie de Galois qui rend naturels beaucoup d'arguments.

Peut-être que grâce à ces raccourcis galoisiens, si vous arrivez à tout faire assez vite, vous arriverez à caser dedans l'irréductibilité des polynômes cyclotomiques (traditionnellement admise pour ce développement). Si vous y arrivez ça peut être hyper stylé comme développement. Peut-être que si vous enlevez la partie « groupe symétrique » selon le recasage... à vous le fun.

Pro tip : mettez dans votre annexe une table de caractères pas dans $\mathbb{Z}$, du genre D_3 ou tout ce que vous trouverez. Le jury adore les contre-exemples...

I. Prérequis cyclotomiques

Soit G un groupe de cardinal n. On ne parle qu'à la toute fin du groupe symétrique.

Théorème I.0.1.
Une racine primitive n-ièmes de l'unité ω est algébrique sur $\mathbb{Q}$ de polynôme minimal annulateur $\varphi_n = \prod_{k\wedge n=1} X - \omega^k$ qui est de plus à coefficients dans $\mathbb{Z}$.

Preuve. Généralement admis pour ce développement. □

Si $k \wedge n = 1$. Par caractérisation des $\mathbb{Q}$-conjugués, il existe un endomorphisme du corps $\mathbb{Q}(\omega)$ envoyant ω vers ω^k (il est unique car $\mathbb{Q}(\omega)$ engendrée par ω). On le note ζ_k.

Théorème I.0.2.
L'extension $\mathbb{Q}(\omega)/\mathbb{Q}$ est galoisienne de degré $\varphi(n)$ et de groupe de Galois isomorphe à $(\mathbb{Z}/n\mathbb{Z})^\times$ via $k \mapsto \zeta_k$.

Preuve. Galoisienne comme corps de décomposition de $X^n - 1$ sur $\mathbb{Q}$ de caractéristique nulle, le degré par l'étude du polynôme cyclotomique φ_n.

L'application du théorème est alors bien définie (car...) et c'est un morphisme de groupes (car...). Elle est injective car l'image de ω par un morphisme détermine les autre images. Par cardinalité, c'est un isomorphisme. □

II. Entiers algébriques

Les résultats de cette section peuvent être admis pour ce développement. Preuves à connaître.

Définition II.0.1. Un entier algébrique (sur $\mathbb{Q}$) est un nombre algébrique dont le polynôme minimal est à coefficients dans $\mathbb{Z}$.

Définition équivalente (Warning ! Non trivial ! Mais très important ! c.f. lemme de Gauss !) : c'est un nombre annulé par un polynôme unitaire à coefficients entiers.

Lemme II.0.2.
L'ensemble des entiers algébriques sur $\mathbb{Q}$ forme un anneau A qui contient $\mathbb{Z}$. On a $A \cap \mathbb{Q} = \mathbb{Z}$.

Contactez-moi en cas de coquille s'il vous plaît ! prenom.nom@ens-lyon.fr

Preuve. PreuveS du fait que A est un anneau... par le résultant (option C goes brrrr je vous recommande cette preuve), par construction explicite d'annulateurs et théorème des polynômes symétriques (preuve à connaître pour tout le monde !), par Cailey-Hamilton dans les modules de type fini (c'est la meilleure preuve mais c'est plus cher...). Faites vos propres recherches par contre.

Preuve du fait que $A \cap \mathbb{Q} = \mathbb{Z}$: si $x \in \mathbb{Q} \cap A$, alors le polynôme minimal de x s'écrit $X - u$ où $u \in \mathbb{Z}$. Donc $x = u \in \mathbb{Z}$. □

III. L'action sur $\mathbb{Z}[\omega]$

On définit $\mathbb{Z}[\omega]$ comme l'image du morphisme $\mathbb{Z}[X] \to \mathbb{Q}(\omega)$. Le groupe de Galois (ici, nous appelerons sans ambiguïté LE groupe de Galois le groupe de $\mathbb{Q}[\omega]/\mathbb{Q}$) agit de façon évidente sur $\mathbb{Q}(\omega)$. Si $P(\omega) \in \mathbb{Z}[\omega]$, alors pour $g \in \mathrm{Gal}\,(\mathbb{Q}(\omega)/\mathbb{Q})$, $g{\cdot}P(\omega) = P(g{\cdot}\omega) = P(\omega^k) = P(X^k)(\omega) \in \mathbb{Z}[\omega]$. Ainsi, l'action se restreint en une action sur $\mathbb{Z}[\omega]$.

Comme le groupe de Galois fixe les élements du corps de base, il fixe ceux de $\mathbb{Z}$, et ainsi fixe $\mathbb{Z}$. Réciproquement, montrons que le fixateur de cette action est exactement $\mathbb{Z}$.

Si $x \in \mathbb{Z}[\omega]^G$, alors le fait que x soit fixé implique par théorie de Galois qu'il est dans le corps de base de l'extension, ici, $\mathbb{Q}$. Mais alors x est à la fois un entier algébrique et un rationnel donc un entier. D'où : $\mathbb{Z}[\omega]^G = \mathbb{Z}$.

Ici notre groupe G fait son entrée fanfaronnante.

Lemme III.0.1.
Soit V, ρ une représentation finie de G. Alors si $g \in G$, alors $\rho(g)$ est diagonalisable à valeurs propres dans $\mathbb{U}_n$. Ainsi, les caractères de G sont à image dans $\mathbb{Z}[\omega]$.

Preuve. Ben $g^n = 1$ donc vous connaissez la chanson. □

IV. L'action sur les caractères

Si $k \in (\mathbb{Z}/n\mathbb{Z})^\times$ et $g \in G$, on pose $k{\cdot}g = g^k$ (bien défini car...).

Remarque IV.0.1. On note $\mathcal{C}$ l'ensemble des fonctions centrales de $G \to \mathbb{C}$. Ce qu'on vient de faire définit une action naturelle de $(\mathbb{Z}/n\mathbb{Z})^\times$ sur $\mathcal{C}$ (qu'il n'est pas nécessaire d'expliciter sauf pour faire joli dans certains recasages).

Lemme IV.0.2.
Soit V, ρ une représentation finie de G et χ son caractère. Alors pour tout $k \in (\mathbb{Z}/n\mathbb{Z})^\times$, $g \in G$, $\chi(k{\cdot}g) = k{\cdot}\chi(g)$.

Preuve. Diagonaliser g et calculer explicitement. □

Remarque IV.0.3. Ces deux actions naturelles de $(\mathbb{Z}/n\mathbb{Z})^\times$ agissent pareil sur les caractères !

Théorème IV.0.4.
La table de caractère est à valeurs dans $\mathbb{Z}$ si et seulement si $\forall g \in G$, $\forall \chi$ irréductible, $\chi(g) = \chi(g^k)$.

Or, cette propriété est vérifiée dès que $\forall g \in G$, $\forall k \in (\mathbb{Z}/n\mathbb{Z})^\times$, g et g^k sont conjugués.

V. Application au groupe symétrique

Contactez-moi en cas de coquille s'il vous plaît ! prenom.nom@ens-lyon.fr

Lemme V.0.1.
Soit $\sigma \in \mathfrak{S}_n$. Alors σ est un cycle si et seulement si l'action de $\langle\sigma\rangle$ sur son support est transitive.

Lemme V.0.2.
Soit $\sigma \in \mathfrak{S}_n$ un cycle dont le support est de cardinal m. Soit k premier à m. Alors σ^k est encore un cycle de même support.

Preuve. On a une action de $\mathbb{Z}$ sur son support X, transitive. Le cycle est d'ordre m donc l'action peut passer au quotient à $\mathbb{Z}/m\mathbb{Z}$, et est toujours transitive sur X.

Montrons que l'action de $\langle c^k \rangle$ sur X est transitive. Elle l'est si et seulement si l'action précédente restreinte à $k(\mathbb{Z}/m\mathbb{Z})$ est encore transitive. Or, k est premier à m, donc $k(\mathbb{Z}/m\mathbb{Z}) = \mathbb{Z}/m\mathbb{Z}$. Cela montre que l'action de $\langle c^k \rangle$ sur X est transitive donc que X est le support de σ^k. Le lemme précédent assure que σ^k est un cycle. □

Autre rédaction : prendre un inverse de k modulo m et faire explicitement.

Théorème V.0.3.
Soit $n \geqslant 1$. Soit $\sigma \in \mathfrak{S}_n$. Alors, si k est premier avec $n!$, alors σ est conjuguée à σ^k.

Preuve. On écrit $\sigma = c_1 \dots c_r$ en produit de cycles. Comme ils sont à supports disjoints, ils commutent, donc $\sigma^k = c_1^k \dots c_r^k$.

On sait que k est premier à $n!$ donc à tous les $1, 2, \dots, n$. Donc k est premier avec tous les ordres de ces cycles. Donc c_i^k est aussi un cycle de même support que c_i. Donc σ et σ^k ont le même type cyclique. Donc sont conjuguées. □