Action sur la Table des Caractères

Travail d'Études et de Recherche de Arthur OHANA,
encadré par Odile GAROTTA

M1 Mathématiques Générales, Université Grenoble Alpes, 2022

Table des matières

1 Introduction

Lorsque l'on souhaite étudier en détail les propriétés d'un groupe fini, on peut rapidement être amené à s'intéresser à ses représentations et donc à dresser sa table des caractères. Le but de cet article est d'établir un certain nombre de résultats concernant cette dernière. Ceux-ci permettront de prévoir certaines valeurs de la table à partir de propriétés du groupe concerné et faciliteront donc la recherche des caractères irréductibles. Inversement, si l'on connaît déjà une table des caractères, on pourra en déduire des propriétés sur le groupe.

Comment trouver plusieurs caractères irréductibles à partir d'un seul ? A quelle condition une table des caractères est-elle à valeurs entières ? Un caractère irréductible s'annule-t-il toujours ? Tel est le genre de questions qui nous intéresse ici. Pour y répondre, on définira des actions de groupes de Galois d'extensions de $\mathbb{Q}$ sur les lignes et les colonnes d'une table des caractères. Mais avant d'en arriver là, il faudra étudier quelques caractéristiques des algèbres de groupes et des entiers algébriques qui sont liées aux représentations.

Dans cet article, on supposera connus les résultats fondamentaux de la théorie des groupes et plus particulièrement ceux concernant les actions de groupes.

On ne redonnera pas explicitement les définitions et théorèmes de base de la théorie des représentations mais ils sont bien sûr primordiaux. Les théorèmes d'orthogonalité des caractères, notamment, seront abondamment utilisés.

De plus, les résultats de la théorie de Galois seront admis, surtout concernant le théorème de prolongement des isomorphismes, les extensions cyclotomiques et la correspondance de Galois.

Enfin, on utilisera des notions élémentaires de la théorie des modules, dans la quatrième partie exclusivement.

2 Notations et premiers résultats

2.1 Notations

Avant tout, commençons par poser quelques notations de base qui seront utilisées tout le long de l'article. Si la plupart sont standards, certains caractères (en gras) sont également fixés pour l'intégralité de cet article. Et, bien sûr, de nouvelles notations seront définies au fur et à mesure des paragraphes.

Si a et b sont entiers, $[|a;b|] = [a;b] \cap \mathbb{Z}$ est l'ensemble des entiers compris entre a et b.

Si E est un ensemble, son cardinal sera noté $|E|$ et l'application identité sur E sera Id_E.

Si A et B sont des ensembles tels que $A \subset B$, $B \setminus A$ désigne l'ensemble des éléments de B n'étant pas dans A. De plus, si f est une application de B vers un ensemble E, $f_{|A}$ est sa restriction à A.

Si a et b sont dans le même ensemble, leur symbole de Kronecker est $\delta_{ab} = \left| \begin{array}{ll} 1 & \text{si } a = b \\ 0 & \text{sinon} \end{array} \right.$.

Si a et b sont entiers, on écrira $a|b$ si a divise b (dans $\mathbb{Z}$) et $a \wedge b$ pour leur plus grand diviseur commun (positif).

De plus, pour tout $m \in \mathbb{N}$, $\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^\times|$ est l'indicatrice d'Euler de m.

Si g est l'élément d'un groupe quelconque, on notera $ord(g)$ son ordre et $<g>$ le sous-groupe qu'il engendre. De même, si H est une partie d'un groupe, $<H>$ est le sous-groupe engendré par H.

Si un groupe A agit sur un ensemble X, $X^A = \{x \in X \mid \forall a \in A,\ a.x = x\}$ désigne l'ensemble des points fixes de X sous l'action de A. De plus, si $x \in X$, $Stab(x) = \{a \in A \mid a.x = x\}$ sera son stabilisateur et $Orb(x) = \{a.x \mid a \in A\}$ son orbite.

Si $f : E \mapsto F$ est un morphisme de groupes ou d'espaces vectoriels, $Ker(f) = f^{-1}(0_B)$ désigne son noyau.

Si V est un espace vectoriel, $End(V)$ sera l'ensemble des applications linéaires de V dans lui-même. L'application trace sera notée tr, pour les endomorphismes comme les matrices.

Soit L et M deux corps avec $M \subset L$, on note L/M l'extension de corps. Le groupe de Galois de cette extension est $Gal(L/M) = Aut_M(L)$, l'ensemble des automorphismes de L valant l'identité sur M.

Si L est un corps, $\overline{L}$ est sa clôture algébrique.

Enfin, si $m \in \mathbb{N}^*$, on notera $\boldsymbol{\zeta_m} \in \mathbb{C}$, une des racines primitives m-ième arbitraire de l'unité.

Dans l'intégralité de cet article, **G sera un groupe fini**. Son **neutre** sera noté **1** et on pose de plus **$n = |G|$** et **e son exposant**.

$Cl(G)$ est l'ensemble des classes de conjugaison de G, $Car(G)$ l'ensemble des caractères de G sur $\mathbb{C}$ et $Irr(G)$ l'ensemble des caractères irréductibles de G sur $\mathbb{C}$.

Enfin, si χ et ψ sont des fonctions centrales sur G, on pose le produit scalaire suivant :
$[\chi|\psi] = \dfrac{1}{n} \displaystyle\sum_{g \in G} \chi(g)\psi(g^{-1})$.

m

2.2 Lemmes préliminaires

Avant d'entrer dans le vif du sujet, il nous faut établir quatre résultats basiques qui serviront à de multiples reprises dans la suite. Il est à noter que, si les deux derniers sont purement techniques, les premiers sont fondamentaux dans le cadre de cet article.

Lemme 2.1 : Si $(\rho; V)$ est une représentation de degré $d \in \mathbb{N}^*$ sur G et χ est son caractère alors, pour tout $g \in G$, $\chi(g)$ est une somme de racines e-ièmes de l'unité. En particulier, $\chi(g) \in \mathbb{Q}(\zeta_e)$.

Preuve : Soit $g \in G$. Comme ρ est un morphisme de groupes et $o(g)\big|e$, on a :

$$\rho(g)^e = \rho(g^e) = \rho(1_G) = Id_V$$

Ainsi, le polynôme $X^e - 1$ annule $\rho(g)$. Comme c'est un polynôme scindé à racines simples sur $\mathbb{C}$, la matrice M de $\rho(g)$ dans la base canonique est semblable à une matrice diagonale. Si P est la matrice de transition et $(\lambda_k)_{1\leq k\leq d}$ sont les valeurs propres de M, on obtient, si I_d est l'identité :

$$I_d = M^e = \left(P \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_d \end{pmatrix} P^{-1} \right)^e = P \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_d \end{pmatrix}^e P^{-1} = P \begin{pmatrix} \lambda_1^e & 0 & \cdots & 0 \\ 0 & \lambda_2^e & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_d^e \end{pmatrix} P^{-1}$$

Ainsi, pour tout $k \in [|1; d|]$, $\lambda_k^e = 1$: ce sont donc des racines e-ièmes de l'unité. $\chi(g)$ étant par définition la somme des λ_k, on obtient le résultat souhaité.

Lemme 2.2 : Soit $m \in \mathbb{N}^*$. $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ est une extension galoisienne, et même abélienne. De plus, $Gal\big(\mathbb{Q}(\zeta_m)/\mathbb{Q}\big) = \{\sigma_k \mid k \in [|1; m|],\ k \wedge m = 1\}$ où σ_k est le $\mathbb{Q}$-automorphisme de $\mathbb{Q}(\zeta_m)$ qui envoie ζ_m sur ζ_m^k.

Preuve : $\mathbb{Q}(\zeta_m)$ est le corps de décomposition du m-ième polynôme cyclotomique, irréductible sur $\mathbb{Q}$, donc l'extension est normale et de degré $\varphi(m)$. Et, comme $\mathbb{Q}$ est de caractéristique 0, l'extension est séparable, donc galoisienne.

De plus, pour tout $k \in [|1; m|]$, si $k \wedge m = 1$, ζ_m^k est aussi une racine du m-ième polynôme cyclotomique et $\zeta_m^k \in \mathbb{Q}(\zeta_m)$. Par théorème de prolongement des automorphismes, le plongement σ_k existe et est dans le groupe de Galois car l'extension est normale. Ainsi, $\sigma_k \in Gal\big(\mathbb{Q}(\zeta_m)/\mathbb{Q}\big)$ et on a donc une inclusion. Mais $|Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})| = \big[\mathbb{Q}(\zeta_m) : \mathbb{Q}\big] = \varphi(m)$. Les σ_k étant différents, on a aussi l'égalité des cardinaux, donc l'égalité de ces ensembles.

Ainsi, $Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ est abélien et même isomorphe à $(\mathbb{Z}/m\mathbb{Z})^\times$, par l'isomorphisme $\begin{cases} \big(\mathbb{Z}/m\mathbb{Z}\big)^\times & \longrightarrow & Gal\big(\mathbb{Q}(\zeta_m)/\mathbb{Q}\big) \\ \overline{k} & \longmapsto & \sigma_k \end{cases}$ (c'est un morphisme car $\sigma_k \circ \sigma_{k'} : \zeta_m \rightsquigarrow \zeta_m^{k\times k'}$).

Lemme 2.3 : Soit $p \in \mathbb{N}$ premier. Pour tout $g \in G$, il existe $(x; y) \in G^2$ tels que $g = xy = yx$, où l'ordre de x est une puissance de p et l'ordre de y est premier avec p.

Preuve : Soit α la valuation p-adique de $ord(g)$ et $b = \frac{ord(g)}{p^\alpha}$. Alors b est premier avec p, donc avec p^α : il existe $(\lambda; \mu) \in \mathbb{Z}^2$ tels que $\lambda p^\alpha + \mu b = 1$. Il ne reste plus qu'à poser

$$x = g^{\mu b} \quad \text{et} \quad y = g^{\lambda p^\alpha}.$$

Par construction, $g = xy = yx$. De plus, $ord(x) = \frac{p^\alpha b}{p^\alpha b \,\wedge\, \mu b} = p^\alpha$ car $p^\alpha \wedge \mu = 1$ par la relation de Bézout précédente. De même, $ord(y) = \frac{p^\alpha b}{p^\alpha b \,\wedge\, \lambda p^\alpha} = b$ et on a donc le résultat.

Lemme 2.4 : Pour tout $g \in G$, les éléments de G qui engendrent le même sous-groupe que g sont exactement les g^m, pour m entier premier avec $n = |G|$.

Preuve : Soit $h \in G$ engendrant le même sous-groupe que g. Alors $h = g^k$ pour un $k \in [|1; n|]$. Mais $ord(g) = ord(h) = \frac{ord(g)}{k \wedge ord(g)}$ donc k est premier avec $ord(g)$.
Si $n = \prod_{i \in I} p_i^{v_i}$ est la décomposition en facteurs premiers, soit $a = \prod_{\substack{i \in I \\ p_i | ord(g)}} p_i^{v_i}$ et $b = \frac{n}{a}$. Alors $ord(g)$ est premier avec b par construction. Par le théorème des restes chinois, il existe donc un entier m congru à 1 modulo b et à k modulo $ord(g)$. La deuxième condition assure $g^m = g^k = h$ tandis que la première donne que m est premier avec b. Mais, comme k, m est premier avec $ord(g)$ donc avec a. Ainsi, m est premier avec $ab = n$ et donc h est bien de la forme voulue.

Réciproquement, si $m \in \mathbb{Z}$ est premier avec n, il l'est avec $ord(g)$ et donc $<g^m>$ a autant d'éléments que $<g>$. Comme $<g^m> \subset <g>$, ce sont les mêmes sous-groupes.

3 Prologue : algèbre de groupe et représentations

Cette partie a pour but d'établir divers résultats qui seront utilisés par la suite. Le premier paragraphe introduit la définition d'une algèbre de groupe tandis que le second se focalise sur les propriétés de son centre. La dernière, indépendante du reste, fournit un théorème dont on fera usage plus tard.

3.1 Algèbre de groupe

Soit L un corps.

Définition : La L-**algèbre du groupe** G, notée $\boldsymbol{L[G]}$, est le L-espace vectoriel de base G et muni de la multipication définie par :

$$\forall (a_g; b_g) \in L^{2n}, \quad \left(\sum_{g\in G} a_g\ g\right)\left(\sum_{h\in G} b_h\ h\right) = \sum_{(g;h)\in G^2} a_g b_h\ gh.$$

Remarque : Cet ensemble est, par construction, une L-algèbre de dimension $n = |G|$. De plus, $L[G]$ est commutative si et seulement si G est abélien.

Théorème 3.1 : Soit $k = |Irr(G)|$ et $(\rho_i; V_i)_{1\leq i\leq k}$ les représentations irréductibles de G, à isomorphisme près. Alors $\Phi : \begin{cases} \mathbb{C}[G] & \longrightarrow & \prod_{i=1}^{k} End(V_i) \\ \sum_{g\in G} a_g\ g & \longmapsto & \left(\sum_{g\in G} a_g\ \rho_i(g)\right)_{1\leq i\leq k} \end{cases}$ est un isomorphisme d'algèbres.

Preuve : Notons tout d'abord que la projection de Φ sur l'un des $End(V_i)$ est la prolongation $\mathbb{C}$-linéaire de ρ_i, qui est un morphisme de groupes. Φ est donc un morphisme d'algèbres, par concaténation de morphismes d'algèbres.

De plus, la dimension de $\prod_{i=1}^{k} End(V_i)$ est $\sum_{i=1}^{k}(d_i)^2 = n$, où d_i est le degré de la i-ème représentation irréductible. Par égalité des dimensions, il suffit donc de montrer que Φ est injective pour conclure.

Soit $x = \sum_{g\in G} a_g\ g \in Ker(\Phi)$. Alors, pour tout $i \in [|1; k|]$, $\sum_{g\in G} a_g\ \rho_i(g) = 0$. Par somme, ce résultat est donc vrai pour toutes les représentations de G, notamment la représentation régulière $(\rho; \mathbb{C}[G])$. En appliquant cela au neutre multiplicatif de $\mathbb{C}[G]$, on trouve $0 = \sum_{g\in G} a_g\ \rho(g)(1) = \sum_{g\in G} a_g\ g$. Ainsi, les coefficients a_g sont tous nuls. On a donc que $Ker(\Phi) = \{0\}$, ce qui donne l'injectivité de Φ.

3.2 Centre d'une algèbre de groupe

Définition : Le **centre** d'une algèbre de groupe $L[G]$ est :

$$\boldsymbol{Z(L[G])} = \{x \in L[G] \mid \forall y \in L[G],\ xy = yx\} = \{x \in L[G] \mid \forall g \in G,\ gxg^{-1} = x\}.$$

Théorème 3.2 : $\left(\sum_{h\in K} h\right)_{K\in Cl(G)}$ est une L-base de $Z(L[G])$. En particulier, c'est un espace vectoriel de dimension est $|Cl(G)|$.

Preuve : Soit $K \in Cl(G)$. Pour tout $g \in G$, $g\Big(\sum_{h\in K} h\Big)g^{-1} = \sum_{h\in K} ghg^{-1} = \sum_{h'\in K} h'$ car la conjugaison par g agit par permutation sur K. Donc ces éléments sont bien dans $Z(L[G])$.

Soit $x = \sum_{h\in G} a_h\ h \in Z(L[G])$. Alors, pour tout $g \in G$:

$$\sum_{h\in G} a_h\ h = x = gxg^{-1} = \sum_{h\in G} a_h\ ghg^{-1}.$$

Ainsi, le coefficient devant h est le même que celui devant ghg^{-1}, pour tout $g \in G$: il est constant sur les classes de conjugaison. Si $a_K \in L$ est la constante associée à la classe K, $x = \sum_{K\in Cl(G)} a_K\Big(\sum_{h\in K} h\Big)$ et cette écriture est unique car celle dans la base G l'est.

Définition : Pour tout $\chi \in Irr(G)$, soit $\boldsymbol{e_\chi} = \dfrac{\chi(1)}{n}\sum_{g\in G}\chi(g^{-1})\ g \quad \in \mathbb{C}[G]$.

Remarque : Les e_χ sont dans $Z(\mathbb{C}[G])$. En effet, comme χ est une fonction centrale, $e_\chi = \sum_{K\in Cl(G)} \dfrac{\chi(1)}{n}\chi(g_K^{-1})\left(\sum_{h\in K} h\right)$, où $g_K \in K$: e_χ est donc un élément du centre, par combinaison linéaire d'éléments du centre.

L'intérêt de ces éléments se révèle lorqu'on regarde leur image par l'isomorphisme du paragraphe précédent. Mais avant d'en arriver là, énonçons un théorème qui resservira dans la partie suivante.

Théorème 3.3 : Soit (ρ, V) une représentation irréductible de G de caractère χ et $(a_g)_{g\in G} \in \mathbb{C}^n$. Si (a_g) est constante sur les classes de conjugaison ($\forall K \in Cl(G), \forall (h;h') \in K^2,\ a_h = a_{h'}$), alors $f = \sum_{g\in G} a_g\ \rho(g) \in End(V)$ est une homothétie de rapport $\lambda = \dfrac{1}{\chi(1)}\sum_{g\in G} a_g\chi(g)$.

Preuve : Ce résultat repose sur le lemme de Schur. Commençons donc par montrer que f est un morphisme de représentations. C'est bien sûr un endomorphisme de V, comme combinaison linéaire d'endomorphismes. De plus, pour tout $h \in G$, on a :
$f \circ \rho(h) = \sum_{g\in G} a_g\ \rho(g)\circ\rho(h) = \sum_{g\in G} a_g\ \rho(gh) = \sum_{g'\in G} a_{hg'h^{-1}}\ \rho(hg') = \sum_{g'\in G} a_{g'}\ \rho(h)\circ\rho(g') = \rho(h)\circ f.$

Ainsi, par le lemme de Schur, f est une homothétie. Si λ est son rapport, comme $\chi(1)$ est la dimension de V, $\lambda\ \chi(1) = tr(\lambda\ id_V) = tr(f) = \sum_{g\in G} a_g\ tr(\rho(g)) = \sum_{g\in G} a_g\ \chi(g)$, d'où le résultat.

Théorème 3.4 : En reprenant les notations du théorème 3.1 et si χ_i est le caractère associé à ρ_i, on a que $\Phi(e_{\chi_i}) = \big(\delta_{ij}\ Id_{V_i}\big)_{1\le j\le k}$, pour tout $i \in [|1;k|]$. En particulier, $(e_{\chi_i})_{1\le i\le k}$ est une base de $Z(\mathbb{C}[G])$ et ce sont des idempotents : $e_{\chi_i}^2 = e_{\chi_i}$, pour tout $i \in [|1;k|]$.

Preuve : Soit $(i;j) \in [|1;k|]^2$. Par le théorème précédent, la j-ième composante de $\Phi(e_{\chi_i})$ est une homothétie de rapport $\dfrac{\chi_i(1)}{n\chi_j(1)} \displaystyle\sum_{g\in G} \chi_i(g^{-1})\ \chi_j(g) = \delta_{ij}$ par orthogonalité des caractères. Ceci donne le premier résultat.

$(e_{\chi_i})_{1\leq i\leq k}$ est donc une famille libre, comme image réciproque d'une famille libre par un isomorphisme. Ces éléments étant dans $Z(\mathbb{C}[G])$, il suffit de rappeler que $k = |Irr(G)| = |Cl(G)|$ est la dimension du centre pour conclure que cette famille en est une base.

Enfin, pour tout $i \in [|1;k|]$, $\Phi(e_{\chi_i}^2) = \Phi(e_{\chi_i})^2 = ((\delta_{ij}\ Id_V)_{1\leq j\leq k})^2 = ((\delta_{ij}\ Id_V)_{1\leq j\leq k}) = \Phi(e_{\chi_i})$. Par injectivité de Φ, on a donc que $e_\chi^2 = e_\chi$: ce sont bien des idempotents.

3.3 Un théorème important

Avant de clore ce prologue, on veut montrer que les caractères sur $\mathbb{C}$ et $\overline{\mathbb{Q}}$ sont les mêmes.

Théorème 3.5 : Soit L un corps algébriquement clos de caractéristique nulle. Il y a exactement $|Cl(G)|$ représentations irréductibles de G sur L, à isomorphisme près. De plus, leurs caractères forment une base orthonormée de l'espace des fonctions centrales de G dans L.

"Preuve" : Ce théorème a déjà été vu dans le cas où $L = \mathbb{C}$. La preuve est similaire dans le cas général et donc admise, notamment pour $L = \overline{\mathbb{Q}}$.

Théorème 3.6 : Soit χ un $\mathbb{C}$-caractère de G et $d \in \mathbb{N}^*$ son degré. Il existe une représentation ρ de G sur $\overline{\mathbb{Q}}$ telle que $\chi = tr(\rho)$.

Preuve : Toute représentation pouvant se décomposer en somme directe de représentations irréductibles, on peut sans perdre de généralité supposer que χ est irréductible.

Soit $k = |Cl(G)| = |Irr(G)|$. Soit $(\chi_j)_{1\leq j\leq k}$ et $(\psi_i)_{1\leq i\leq k}$ les caractères irréductibles de G sur $\mathbb{C}$ et $\overline{\mathbb{Q}}$ respectivement. Pour tout $i \in [|1;k|]$, on peut décomposer ψ_i dans la base des $\mathbb{C}$-caractères irréductibles : soit $(a_{ij})_{1\leq j\leq k} \in \mathbb{N}^k$ non tous nuls tels que $\psi_i = \displaystyle\sum_{j=1}^{k} a_{ij}\chi_j$.

Les $(\psi_i)_{1\leq i\leq k}$ étant orthogonaux, ils forment une base des fonctions centrales de G sur $\mathbb{C}$. Ainsi, la matrice carrée formée par les $(a_{ij})_{1\leq i;j\leq k}$ est une matrice de changement de base, donc inversible. Notamment, elle ne contient pas de colonne de zéros donc, comme ses coefficients sont des entiers naturels, pour tout $s \in [|1;k|]$:

$$\sum_{i=1}^{k} a_{is}^2 \geq 1 \quad \text{d'où} \quad \sum_{s=1}^{k} \chi_s(1)^2 \Big(\sum_{i=1}^{k} a_{is}^2 \Big) \geq \sum_{s=1}^{k} \chi_s(1)^2 = n.$$

D'autre part, on a :

$$n = \sum_{i=1}^{k} \psi_i(1)^2 = \sum_{i=1}^{k} \left(\sum_{j=1}^{k} a_{ij}\chi_j(1) \right)^2 = \sum_{s=1}^{k}\sum_{t=1}^{k} \left(\chi_s(1)\chi_t(1) \sum_{i=1}^{k} a_{is}a_{it} \right).$$

Comme ce sont des sommes de termes positifs et que le total est déjà au moins atteint pour les termes où $s = t$, les autres sont nuls et l'inégalité précédente était une égalité : $\sum_{i=1}^{k} a_{is}a_{it} = \delta_{st}$.

Ainsi, la matrice de changement de base était seulement une matrice de permutation : les familles $(\chi_j)_{1\leq j\leq k}$ et $(\psi_i)_{1\leq i\leq k}$ sont donc les mêmes à l'ordre près. Ceci prouve qu'à chaque caractère irréductible sur $\mathbb{C}$, on peut associer une représentation sur $\overline{\mathbb{Q}}$.

4 Entiers algébriques

Dans cette partie, nous allons montrer que les valeurs des caractères sont des entiers algébriques. Ceci motive l'étude de certaines de leurs propriétés, mais ces dernières utilisent la théorie des modules, dont les résultats de base sont admis.

Définition : Un élément d'un anneau commutatif est appelé **entier sur** $\mathbb{Z}$ s'il est racine d'un polynôme unitaire à coefficients entiers. Si l'anneau en question est $\mathbb{C}$, les entiers sur $\mathbb{Z}$ sont appelés **entiers algébriques** et l'ensemble des entiers algébriques sera noté $\mathbb{E}$.

Commençons par un résutat d'ordre général que l'on réutilisera à de multiples reprises :

Théorème 4.1 : Si x est un entier algébrique rationnel, alors c'est un entier. Autrement dit : $\mathbb{E} \cap \mathbb{Q} = \mathbb{Z}$.

Preuve : Soit x un entier algébrique rationnel : il existe donc $(p; q) \in \mathbb{Z} \times \mathbb{N}^*$, $p \wedge q = 1$, tels que $x = \frac{p}{q}$ ainsi que $(a_i)_{0 \leq i \leq k-1} \in \mathbb{Z}^k$ tels que $a^k + \sum_{i=0}^{k-1} a_i x^i = 0$, pour un $k \in \mathbb{N}^*$.
En remplaçant x par $\frac{p}{q}$ et en multipliant par q^k, on trouve :

$$0 = p^k + \sum_{i=0}^{k-1} a_i p^i q^{k-i} = p^k + q \times \sum_{i=0}^{k-1} a_i p^i q^{k-1-i}.$$

Ceci montre que q divise p^k mais, p et q étant premiers entre eux, ceci implique que $q = 1$ et donc que $x = p \in \mathbb{Z}$.

Le prochain objectif est de montrer que les entiers algébriques forment un anneau, ce qui nécessite un lemme préliminaire.

Lemme : Tout sous-$\mathbb{Z}$-module d'un $\mathbb{Z}$-module de type fini M est lui-même de type fini.

Preuve : Commençons par montrer ce résultat dans le cas où M est une puissance de $\mathbb{Z}$, par récurrence. Un sous-$\mathbb{Z}$-module de $\mathbb{Z}$ étant un idéal, il est engendré par un unique élément, $\mathbb{Z}$ étant principal. Soit maintenant $d \in \mathbb{N}^*$. Supposons que tout sous-$\mathbb{Z}$-module de $\mathbb{Z}^d$ est de type fini et soit N un sous-$\mathbb{Z}$-module de $\mathbb{Z}^{d+1}$.
Soit $p : \left\{ \begin{array}{ccc} N & \longrightarrow & \mathbb{Z} \\ (a_i)_{0 \leq i \leq d} & \longmapsto & a_0 \end{array} \right.$. C'est un morphisme de $\mathbb{Z}$-modules, donc son image est un module engendré par un $y \in \mathbb{Z}$ et il existe un $x \in N$ antécédent de y. De même, $Ker(p) \subset \{0\} \times \mathbb{Z}^d \simeq \mathbb{Z}^d$ est un sous-module, qui admet une famille génératrice finie F par hypothèse de récurrence. Soit E le sous-$\mathbb{Z}$-module de $\mathbb{Z}^{d+1}$ engendré par l'union de F et $\{x\}$. Montrons que $E = N$.
$x \in N$ par définition et, comme $Ker(p) \subset N$, c'est aussi le cas de F donc $E \subset N$. Réciproquement, un élément de N est nécessairement de la forme $\big(ky; (a_i)_{1 \leq i \leq d}\big)$, pour un $k \in \mathbb{Z}$. Mais $\big(ky; (a_i)_{1 \leq i \leq d}\big) = kx + \Big(\big(ky; (a_i)_{1 \leq i \leq d}\big) - kx\Big) \in E$ car le premier terme est un multiple entier de x et le second terme est dans le noyau de p, donc combinaison linéaire de F. Ainsi, $N = E$ et, ce dernier étant de type fini par construction, on a donc prouver le théorème suivant : pour tout $d \in \mathbb{N}^*$, les sous-$\mathbb{Z}$-modules de $\mathbb{Z}^d$ sont de type fini.

Passons maintenant à la preuve du lemme. Soit $d \in \mathbb{N}^*$, $(m_i)_{1\leq i\leq d}$ une famille génératrice de M et N un sous-$\mathbb{Z}$-module de M. Alors $f : \begin{cases} \mathbb{Z}^d & \longrightarrow & M \\ (a_i)_{1\leq i\leq d} & \longmapsto & \sum_{i=1}^{d} a_i\ m_i \end{cases}$ est un morphisme de modules surjectif. Ainsi, l'image réciproque $f^{-1}(N)$ est un sous-module de $\mathbb{Z}^d$, donc de type fini par le premier point. Mais, par surjectivité, $N = f(f^{-1}(N))$: l'image d'un module de type fini par un morphisme étant de type fini, ceci achève la preuve.

Théorème 4.2 : Si A est un anneau commutatif, l'ensemble des entiers sur $\mathbb{Z}$ de A est un sous-anneau de A. Notamment, $\mathbb{E}$ est un anneau.

Preuve : Tout d'abord, les neutres de A sont bien sûr des entiers sur $\mathbb{Z}$, comme racine de X et $X - 1$. Il faut donc vérifier que cet ensemble est stable par les opérations élémentaires.

Soit x et y deux entiers sur $\mathbb{Z}$ de A. On pose $\mathbb{Z}[x]$ l'anneau engendré par x : c'est un $\mathbb{Z}$-module de famille génératrice $(x^i)_{i\in\mathbb{N}}$. De la même façon, on considère $\mathbb{Z}[y]$ et $\mathbb{Z}[x; y]$, les anneaux engendrés par y puis x et y, vus comme des $\mathbb{Z}$-modules.
x étant racine d'un polynôme unitaire à coefficients entiers, il existe $k \in \mathbb{N}^*$ et $(a_i)_{0\leq i\leq k-1} \in \mathbb{Z}^k$ tels que $x^k = -\sum_{i=0}^{k-1} a_i\ x^i$. Ainsi, x^k est une $\mathbb{Z}$-combinaison linéaire de la famille $(x^i)_{0\leq i\leq k-1}$ et, par récurrence, il en va de même pour les puissances supérieures. Cette famille est donc génératrice de $\mathbb{Z}[x]$. De même, il existe $l \in \mathbb{N}^*$ tel que $(y^j)_{0\leq j\leq l-1}$ soit une famille génératrice de $\mathbb{Z}[y]$ et on a alors que $(x^i y^j)_{\substack{0\leq i\leq k-1 \\ 0\leq j\leq l-1}}$ est une famille génératrice de $\mathbb{Z}[x; y]$. Notamment, ce dernier est de type fini.
Soit $a = xy$. Alors $\mathbb{Z}[a] \subset \mathbb{Z}[x; y]$ est un module de type fini d'après le lemme précédent. De plus, la suite des modules engendrés par $(a^i)_{0\leq i\leq k}$ croît avec k (pour l'inclusion) et a pour limite $\mathbb{Z}[a]$. Ce dernier étant de type fini, la suite est constante à partir d'un certain rang $m \in \mathbb{N}$. Notamment, $a^{(m+1)}$ est combinaison linéaire des $(a^i)_{0\leq i\leq m}$ sur $\mathbb{Z}$. On construit ainsi un polynôme unitaire de degré $m + 1$ à coefficients entiers admettant a pour racine.
Ainsi, a est un entier sur $\mathbb{Z}$. Mais ce raisonnement peut aussi être fait pour $a = x + y$ et $a = -x$. Les entiers sur $\mathbb{Z}$ étant stables par plus, moins et fois, ils forment un sous-anneau de A.

Remarque : Ainsi, $\chi(g)$ est un entier algébrique, pour tout $g \in G$ et $\chi \in Car(G)$. En effet, par le lemme de 2.1, c'est une somme de racines de l'unité, qui sont elles-mêmes des entiers algébriques.

Le dernier but de cette partie est d'établir que les degrés des représentations irréductibles divisent l'ordre du groupe. Ceci nécessite un dernier petit lemme.

Lemme : Si A et B sont deux algèbres, $F : A \to B$ est un morphisme d'algèbres et $x \in A$ est un entier sur $\mathbb{Z}$, alors $F(x)$ est aussi un entier sur $\mathbb{Z}$.

Preuve : Puisque x est un entier sur $\mathbb{Z}$, il existe un polynôme P unitaire à coefficients entiers annulant x. Mais, F étant un morphisme d'algèbres, on a : $P(F(x)) = F(P(x)) = F(0) = 0$.
P annule donc aussi $F(x)$, ce qui conclut.

Théorème 4.3 : Soit $\chi \in Irr(G)$. Alors $\chi(1) = deg(\chi)$ divise $n = |G|$.

Preuve : Avant toute chose, posons $d = \chi(1)$, $(\rho; V)$ une représentation associée à χ et, pour tout $K \in Cl(G)$, $e_K = \sum_{g \in K} g \in Z(\mathbb{C}[G])$ et fixons un $g_K \in K$.

Soit $u = \sum_{g \in G} \chi(g^{-1})\ g \in \mathbb{C}[G]$. Comme χ est une fonction centrale, $u = \sum_{K \in Cl(G)} \chi(g_K^{-1})\ e_K$ donc $u \in Z(\mathbb{C}[G])$.

u est de plus un entier sur $\mathbb{Z}$. En effet, les $\chi(g^{-1})$ le sont par la dernière remarque et g annule $X^n - 1$ donc c'est aussi un entier sur $\mathbb{Z}$. Par produits et sommes, les entiers sur $\mathbb{Z}$ formant un anneau, on a le résultat voulu.

La prochaine étape est de montrer que $F : \left\{ \begin{array}{ccc} Z(\mathbb{C}[G]) & \longrightarrow & \mathbb{C} \\ \sum_{K \in Cl(G)} a_K\ e_K & \longmapsto & \frac{1}{d} \sum_{g \in G} a_g \chi(g) \end{array} \right.$, où $a_g = a_K$ si $g \in K$, est un morphisme d'algèbres. C'est le cas de $\phi : \left\{ \begin{array}{ccc} Z(\mathbb{C}[G]) & \longrightarrow & End(V) \\ \sum_{K \in Cl(G)} a_K\ e_K & \longmapsto & \sum_{g \in G} a_g\ \rho(g) \end{array} \right.$.

Mais, par le théorème 3.3, une image de ϕ est nécessairement une homothétie de V et $\psi : \left\{ \begin{array}{ccc} \mathbb{C}\ id_V & \longrightarrow & \mathbb{C} \\ \lambda\ id_V & \longmapsto & \lambda \end{array} \right.$ est aussi un morphisme d'algèbre. Il ne reste plus qu'à constater (toujours d'après le théorème 3.3) que $F = \psi \circ \phi$ pour établir que F est bien un morphisme d'algèbres.

Par le lemme précédent et ces deux points, $F(u)$ est un entier sur $\mathbb{Z}$, donc un entier algébrique. Mais $F(u) = \frac{1}{d} \sum_{g \in G} \chi(g^{-1})\chi(g) = \frac{n}{d} \in \mathbb{Q}$ par le premier théorème d'orthogonalité. Ainsi,

$\frac{n}{d} = F(u) \in \mathbb{E} \cap \mathbb{Q} = \mathbb{Z}$. Il faut donc nécessairement que d divise n.

5 Actions de groupe

Dans cette partie, nous entrons dans le vif du sujet. Les trois premiers paragraphes définissent et donnent des propriétés particulières des actions de groupe dans un cadre général.

Le quatrième paragraphe, quant à lui, pose la définition des deux actions que nous allons étudier : celles du groupe de Galois d'une extension cyclotomique sur $Irr(G)$ d'une part et sur $Cl(G)$ d'autre part.

Le dernier paragraphe exploite les précédents pour tirer des propriétés de ces actions.

5.1 Lemme de Brauer

Soit A un groupe fini agissant à la fois sur $Irr(G)$ et sur $Cl(G)$.
Lemme de Brauer : Si pour tous $\chi \in Irr(G),\ a \in A,\ K \in Cl(G),\ g \in K$, et $g' \in a.K$ on a :

$$a.\chi\ (g') = \chi(g),$$

alors les $a \in A$ fixent autant de caractères irréductibles que de classes de conjugaison.

Preuve : Soit $k = |Cl(G)| = |Irr(G)|$. Soit $(\chi_i)_{1\leq i\leq k}$ les caractères irréductibles de G, $(K_j)_{1\leq j\leq k}$ les classes de conjugaison de G et $(g_j)_{1\leq j\leq k}$ des représentants de chaque classe. On pose $X = \big(\chi_i(g_j)\big)_{1\leq i;j\leq k} \in M_k(\mathbb{C})$ la table des caractères. Par le second théorème d'orthogonalité, les colonnes de X forment une famille libre donc X est inversible.

Soit $a \in A$, $P = (p_{ij})_{1\leq i;j\leq k}$ et $Q = (q_{ij})_{1\leq i;j\leq k}$ dans $M_k(\mathbb{C})$ avec $p_{ij} = \left|\begin{array}{ll} 1 & \text{si } a.\chi_i = \chi_j \\ 0 & \text{sinon} \end{array}\right.$ et $q_{ij} = \left|\begin{array}{ll} 1 & \text{si } K_i = a^{-1}.K_j \\ 0 & \text{sinon} \end{array}\right.$. Le résultat est alors équivalent à $tr(P) = tr(Q)$.

Soit $(i;j) \in [|1;k|]^2$. Le coefficient en i-ème ligne, j-ième colonne de PX est $\displaystyle\sum_{s=1}^{k} p_{is}\chi_s(g_j) = a.\chi_i\ (g_j)$ et celui de XQ est $\displaystyle\sum_{s=1}^{k} \chi_i(g_s)q_{sj} = \chi_i(a^{-1}g_j)$ où $a^{-1}g_j \in a^{-1}.K_j$. Mais d'après l'hypothèse, pour $g = a^{-1}g_j$, $K = a^{-1}.K_j$ et $g' = g_j$, on a $a.\chi_i\ (g_j) = \chi_i(a^{-1}g_j)$.
Ainsi, $PX = XQ$ et donc $P = XQX^{-1}$. Deux matrices semblables ayant même trace, ceci conclut la preuve.

5.2 Actions isomorphes

Soit A un groupe fini agissant à la fois sur un ensemble X et un ensemble Y, tous deux finis (et de même cardinal par contrainte).

Définition : Les deux **actions** de A sont dites **isomorphes** s'il existe une bijection $\alpha : X \to Y$ telle que $a.\alpha(x) = \alpha(a.x)$, pour tous $a \in A$ et $x \in X$. α est appelée **isomorphisme de *A*-ensembles**.

Théorème 5.1 : Les deux actions de A sont isomorphes si et seulement si, pour tout B sous-groupe de A, les actions restreintes de B sur X et Y fixent le même nombre d'éléments.

Preuve : Si α est un isomorphisme de A-ensembles, soit B un sous-groupe de A et $x \in X$.
Alors : x est fixé par l'action de B $\Leftrightarrow$ $\forall a \in B,\ a.x = x$
$\Leftrightarrow$ $\forall a \in B,\ \alpha(a.x) = a.\alpha(x) = \alpha(x)$
$\Leftrightarrow$ $\alpha(x)$ est fixé par l'action de B

α étant une bijection, ceci implique que B fixe autant d'éléments de X que de Y.

Réciproquement, supposons que, pour tout B sous-groupe de A, les actions de B fixent autant d'éléments de X que de Y. Notons tout d'abord que, en prenant B le sous-groupe trivial, on a $|X| = |Y|$. On va montrer que les deux actions sont isomorphes en raisonnant par récurrence forte sur le cardinal de X.
Si X et Y n'ont qu'un seul élément, l'unique application de X dans Y convient. Sinon, on suppose que pour tout couple d'ensembles de (même) cardinal strictement inférieur à $|X|$ et sur lesquels A agit de façon à ce que ses sous-groupes fixent autant d'éléments, on a l'existence d'une bijection $\alpha : X \to Y$ commutant avec l'action.

On peut regarder l'ensemble des sous-groupes de A fixant au moins un point de X, muni de l'inclusion. Cet ensemble est fini car A l'est et il contient le sous-groupe trivial : il admet donc un élément maximal B. Soit $x \in X$ fixé par B. Le stabilisateur de x sous l'action de A étant le plus grand sous-groupe fixant x, c'est B par maximalité. De plus, B fixe autant d'éléments de X que de Y, il existe $y \in Y$ fixé par B. Ainsi, $B \subset Stab(y)$. Mais, $Stab(y)$ fixe un élément de Y, donc aussi un de X : $Stab(y) \subset B$. Finalement : $Stab(x) = B = Stab(y)$. On a donc notamment que les orbites de x et y sous l'action de A ont même cardinal.
De plus, pour tout $(a; a') \in A^2$: $a.x = a'.x \Leftrightarrow a^{-1}a' \in Stab(x) = Stab(y) \Leftrightarrow a.y = a'.y$. On peut donc définir $\alpha_1 : \left\{ \begin{array}{ccc} Orb(x) & \longrightarrow & Orb(y) \\ a.x & \longmapsto & a.y \end{array} \right.$ qui est surjective et donc bijective par égalité des cardinaux. Enfin, α_1 commute bien avec l'action : pour tous $a.x \in Orb(x)$ et $a' \in A$,
$a'.\alpha_1(a.x) = a'.(a.y) = a'a.y = \alpha_1(a'a.x) = \alpha_1(a'.(a.x))$.

Soit maintenant $X' \subset X$ et $Y' \subset Y$ les complémentaires de $Orb(x)$ et $Orb(y)$ respectivement. A agit donc sur X' et Y'. De plus, comme α_1 vérifie les hypothèses et que la première implication a déjà été démontrée, les sous-groupes de A fixent autant d'éléments dans $Orb(x)$ que dans $Orb(y)$. Ceci étant aussi vrai pour X et Y, ça l'est pour X' et Y'. Finalement, les orbites n'étant pas vides, il existe une bijection $\alpha_2 : X' \to Y'$ commutant avec l'action, par hypothèse de récurrence.

Par construction, l'application $\alpha : \left\{ \begin{array}{ccc} X & \longrightarrow & Y \\ x & \longmapsto & \left| \begin{array}{ll} \alpha_1(x) & \text{si } x \in Orb(x) \\ \alpha_2(x) & \text{si } x \in X' \end{array} \right. \end{array} \right.$ est un isomorphisme de A-ensembles, ce qui conclut la preuve.

5.3 Action par automorphismes

Pour ce paragraphe, on fixe A un groupe (fini par contrainte).

Définition : On dit que A **agit** sur G **par automorphismes** s'il existe un morphisme de groupes α de A dans $Aut(G)$. On définit alors l'action $\left\{ \begin{array}{ccc} A \times G & \longrightarrow & G \\ (a; g) & \longmapsto & \boldsymbol{a.g} = \alpha(a)(g) \end{array} \right.$.

Lemme : Si A agit par automorphisme sur G, alors A agit aussi sur $Car(G)$ par $a.\chi : g \to \chi(a^{-1}.g)$, où $a \in A$ et $\chi \in Car(G)$.
De plus : $\forall a \in A,\ \forall (\chi; \psi) \in Car(G)^2,\ \ [a.\chi | a.\psi] = [\chi|\psi]$ et $\chi \in Irr(G) \Leftrightarrow a.\chi \in Irr(G)$.

Preuve : Soit $a \in A,\ \chi \in Car(G)$ et ρ une représentation induisant χ. Alors $\rho' : g \to \rho(a^{-1}.g)$ est aussi une représentation de G, par composition de morphismes, et son caractère de ρ' est $a.\chi$. De plus, si $a' \in A$, on a bien que $(aa').\chi = a.(a'.\chi)$ et $id_A.\chi = \chi$ donc ceci définit bien une action.

Par ailleurs, pour tous $a \in A$ et $(\chi;\psi) \in Car(G)^2$,
$[a.\chi|a.\psi] = \dfrac{1}{n}\sum_{g\in G}\chi(a^{-1}.g)\psi(a^{-1}.g^{-1}) = \dfrac{1}{n}\sum_{g\in G}\chi(g)\psi(g^{-1}) = [\chi|\psi]$ par changement de variable.
Enfin : $\forall a \in A,\ \forall \chi \in Car(G),\quad \chi \in Irr(G) \Leftrightarrow 1 = [\chi|\chi] = [a.\chi|a.\chi] \Leftrightarrow a.\chi \in Irr(G)$.

Théorème 5.2 : On suppose que A est un groupe fini qui agit par automorphismes sur G et tel que $|A| \wedge n = 1$. Si l'action de A fixe tous les caractères irréductibles de G, alors A fixe tout G.

Preuve : Cette preuve se découpe en plusieurs parties. La première est d'utiliser le lemme de Brauer puis, par l'équation aux classes et un peu d'arithmétique, de montrer qu'il y a un point fixe dans chaque classe de conjugaison pour finalement en déduire que tous les éléments de G sont fixés.

Notons tout d'abord que, comme A agit par automorphismes, l'action envoie les classes de conjugaison sur les classes de conjugaison : ceci définit une action de A sur $Cl(G)$.
De plus, pour tous $\chi \in Irr(G),\ a \in A,\ K \in Cl(G),\ g \in K$, et $g' \in a.K$ on a :
$a.\chi\ (g') = \chi(a^{-1}.(a.g)) = \chi(g)$. Par le lemme de Brauer, comme l'action fixe tous les caractères irréductibles, toute classe de conjugaison est envoyée sur elle-même sous l'action de A.

Soit $a \in A$. Par récurrence sur le nombre de diviseurs premiers de l'ordre de a, le lemme 2.3 montre que a s'écrit comme produit d'éléments commutant entre eux et d'ordre la puissance d'un nombre premier. Ainsi, il suffit de vérifier que les éléments de A d'ordre la puissance de n'importe quel nombre premier fixent tout G. On peut donc, sans perdre de généralité, supposer que A est un p-groupe, pour un certain nombre premier p.

Soit $K \in Cl(G)$ et $k = |K|$. Par le premier point, A agit sur K. Ainsi, k est la somme des cardinaux des orbites de cette action. Or on sait que le cardinal d'une orbite est l'indice d'un sous-groupe de A, donc une puissance de p.
De plus, comme $K \in Cl(G)$, $k|n$. Mais $n \wedge |A| = 1$ d'où $n \wedge p = 1$ et donc k est premier avec p. Finalement, k ne peut pas être somme de puissances non nulles de p : une au moins des orbites est restreinte à un élément. Ainsi, il y a au moins un élément de chaque classe de conjugaison qui est fixé par l'action de A.

Soit $C = G^A = \{g \in G \mid \forall a \in A, a.g = g\}$ l'ensemble des points fixes. Comme A agit par automorphismes, on vérifie facilement que C est un sous-groupe de G. De plus, par le point précédent, l'ensemble des conjugués des points fixes est tout G : $\bigcup_{g\in G} gCg^{-1} = G$.
Il ne reste plus qu'à montrer que cette dernière condition implique $C = G$. Soit s l'indice de C dans G et $(g_i)_{1\le i\le s} \in G^s$ tels que $(g_iC)_{1\le i\le s}$ forme une partition de G. Pour tout $g \in g_iC$, $g = g_ih$ avec $h \in C$ donc : $gCg^{-1} = \big(g_ih\big)C\big(g_ih\big)^{-1} = g\big(hCh^{-1}\big)g_i^{-1} = g_iCg_i^{-1}$. Ainsi :

$$G = \bigcup_{g\in G} gCg^{-1} = \bigcup_{i=1}^{s} g_iCg_i^{-1} = \{1\} \cup \bigcup_{i=1}^{s} g_iCg_i^{-1} \setminus \{1\}$$

En passant au cardinal, ceci devient : $s|C| = G \le 1 + s(|C| - 1)$ d'où $s \le 1$. Finalement, l'indice de C dans G est 1 donc $C = G$, ce qu'il fallait démontrer.

5.4 Actions de Galois

Définition : Soit χ un caractère de G. Le corps des valeurs de χ, noté $\mathbb{Q}(\boldsymbol{\chi})$, est l'extension de $\mathbb{Q}$ engendrée par les $\chi(g)$ pour $g \in G$.

Remarque : Par le lemme 2.1, $\mathbb{Q}(\chi) \subset \mathbb{Q}(\zeta_e)$. Ainsi, l'extension $\mathbb{Q}(\chi)/\mathbb{Q}$ est galoisienne (et même abélienne), comme sous-extension d'une extension abélienne.

Soit L un sous-corps de $\mathbb{C}$ tel que $\mathbb{Q}(\chi) \subset L$, pour tout $\chi \in Irr(G)$.

Définition : Comme $\mathbb{Q}(\chi) \subset L$, pour tout $\sigma \in Gal\big(L/\mathbb{Q}\big)$ et $\chi \in Car(G)$, on peut définir $\boldsymbol{\sigma.\chi} : \left\{ \begin{array}{ccc} G & \longrightarrow & \mathbb{C} \\ g & \longmapsto & \sigma\big(\chi(g)\big) \end{array} \right.$.

Théorème 5.3 : L'application $\left\{ \begin{array}{ccc} Gal\big(L/\mathbb{Q}\big) \times Car(G) & \longrightarrow & Car(G) \\ (\sigma;\chi) & \longmapsto & \sigma.\chi \end{array} \right.$ définit une action de groupe.

Preuve : Soit $\sigma \in Gal\big(L/\mathbb{Q}\big)$ et $\chi \in Car(G)$. Il s'agit de trouver une représentation de caractère $\sigma.\chi$.
Par le théorème 3.6, il existe une représentation ρ induisant χ et telle que pour tout $g \in G$, la matrice de $\rho(g)$ dans une base a tous ses coefficients dans $\overline{\mathbb{Q}}$. On peut donc considérer l'extension engendrée par tous les coefficients de toutes ces matrices : elle est finie car engendrée par un nombre fini d'éléments algébriques. En prenant la fermeture normale de cette extension, on obtient une extension $K/\mathbb{Q}$.
Par construction, $K/\mathbb{Q}$ est normale et on a la tour d'extensions $\mathbb{Q} \subset \mathbb{Q}(\chi) \subset K \subset \overline{\mathbb{Q}}$ car $\chi(g)$ est une somme d'élements de K pour tout $g \in G$.
Comme $\mathbb{Q}(\chi)/\mathbb{Q}$ est normale, le plongement $\sigma_{|\mathbb{Q}(\chi)}$ est un $\mathbb{Q}$-automorphsime de $\mathbb{Q}(\chi)$.
Comme $K/\mathbb{Q}$ est normale et $\sigma_{|\mathbb{Q}(\chi)} \in Aut_{\mathbb{Q}}\big(\mathbb{Q}(\chi)\big)$, on peut prolonger $\sigma_{|\mathbb{Q}(\chi)}$ en un $\tau \in Aut_{\mathbb{Q}}(K)$.

Soit $g \in G$. La matrice de $\rho(g)$ dans une base spécifique étant à coefficients dans K, on peut appliquer τ à chaque coefficient. L'ensemble des matrices obtenues quand g varie induit une nouvelle représentation ρ' $\big(g \mapsto \rho'(g)$ sera toujours un morphisme de groupe car τ conserve $+$ et $\times\big)$. De plus, le caractère de ρ' est $\tau.\chi = \sigma.\chi$ car $\tau_{|\mathbb{Q}(\chi)} = \sigma_{|\mathbb{Q}(\chi)}$.
Ainsi, $\sigma.\chi \in Car(G)$. Enfin, l'identité fixe tous les caractères et l'action est clairement compatible avec la composition.

Propriétés : De plus, si $\sigma \in Gal\big(L/\mathbb{Q}\big)$ et $\chi \in Car(G)$, on a :

1. $\mathbb{Q}(\sigma.\chi) = \mathbb{Q}(\chi)$;
2. $[\sigma.\chi;\sigma.\chi] = [\chi;\chi]$;
3. $\sigma.\chi \in Irr(G) \Leftrightarrow \chi \in Irr(G)$;
4. $\{\tau.\chi \;\big|\; \tau \in Gal(L/\mathbb{Q})\} = \{\tau.\chi \;\big|\; \tau \in Gal(\mathbb{Q}(\chi)/\mathbb{Q})\}$

Preuve :

1. $\mathbb{Q}(\sigma.\chi) = \mathbb{Q}\big(\sigma(\chi(g)) \;\big|\; g \in G\big) = \sigma(\mathbb{Q}(\chi)) = Im(\sigma_{|\mathbb{Q}(\chi)}) = \mathbb{Q}(\chi)$;
2. $[\sigma.\chi;\sigma.\chi] = \dfrac{1}{|G|}\displaystyle\sum_{g\in G} \sigma(\chi(g))\overline{\sigma(\chi(g))} = \sigma\left(\dfrac{1}{|G|}\displaystyle\sum_{g\in G} \chi(g)\overline{\chi(g)}\right) = \sigma([\chi;\chi]) = [\chi;\chi]$;
3. $\sigma.\chi \in Irr(G) \Leftrightarrow [\sigma.\chi;\sigma.\chi] = 1 \Leftrightarrow [\chi;\chi] = 1 \Leftrightarrow \chi \in Irr(G)$;
4. $\sigma.\chi = \sigma_{|\mathbb{Q}(\chi)}.\chi$ donc on a l'inclusion directe et la deuxième vient simplement de $\mathbb{Q}(\chi) \subset L$ et du théorème de prolongement des morphismes.

Remarques :

— Le troisième point montre que cette action peut être restreinte à une action sur $Irr(G)$. C'est cette dernière que l'on va étudier à partir de maintenant. Il est à noter que ce résultat permet de trouver des caractères irréductibles à partir d'autres connus.

— Le dernier point montre que, si l'on s'intéresse à un unique χ, on peut prendre L contenant le $\mathbb{Q}(\chi)$ correspondant et faire agir son groupe de Galois sur l'orbite de χ.

Avant de donner une illustration, définissons un deuxième type d'actions, cette fois-ci sur les classes de conjugaison de G. Si son lien avec un groupe de Galois peut sembler artificiel de prime abord, il sera justifier par le paragraphe suivant.

Dans la suite, on prend N un multiple de e et, grâce au lemme 2.4, on pose

$$\Gamma = Gal\big(\mathbb{Q}(\zeta_N)/\mathbb{Q}\big) = \{\sigma_m : \zeta_N \rightsquigarrow \zeta_N^m \;\big|\; m \in [|1;N|],\ m \wedge N = 1\}.$$

Définition : Si $\sigma_m \in \Gamma$ et $K \in Cl(G)$, on pose $\boldsymbol{\sigma_m.K} = \{k^m \mid k \in K\}$.

Théorème 5.4 : L'application $\left\{ \begin{array}{ccc} \Gamma \times Cl(G) & \longrightarrow & Cl(G) \\ (\sigma_m; K) & \longmapsto & \sigma_m.K \end{array} \right.$ définit une action de groupe.

Preuve : Soit $\sigma_m \in \Gamma$ et $K \in Cl(G)$. Si $(k;h) \in K^2$ et $g \in G$ tels que $k = ghg^{-1}$, alors $k^m = (ghg^{-1})^m = gh^m g^{-1}$ donc k^m et h^m sont aussi conjugués : $\sigma_m.K \in Cl(G)$.
L'identité fixe bien les classes d'équivalence et : $\forall(\sigma;\sigma') \in \Gamma^2, \forall K \in Cl(G), \sigma.(\sigma'.K) = (\sigma\sigma').K$.

Remarque : Si l'on s'intéresse à une classe K particulière, on peut considérer l'action similaire de $Gal\big(\mathbb{Q}(\zeta_o)/\mathbb{Q}\big)$ sur l'orbite de K, où o est l'ordre des éléments de K. C'est ce que l'on sera amené à faire à la fin de cet article.

Concluons ce paragraphe en illustrant ces actions sur un exemple concret.

Voici la table des caractères du groupe $PSL_2(\mathbb{F}_{17})$, d'exposant 1224 :

$Classes$	Cl_1	Cl_2	Cl_3	Cl_4	Cl_5	Cl_6	Cl_7	Cl_8	Cl_9	Cl_{10}	Cl_{11}
$Ordres$	1	2	3	4	8	8	9	9	9	17	17
χ_1	1	1	1	1	1	1	1	1	1	1	1
χ_2	9	1	0	1	-1	-1	0	0	0	$\frac{1-\sqrt{17}}{2}$	$\frac{1+\sqrt{17}}{2}$
χ_3	9	1	0	1	-1	-1	0	0	0	$\frac{1+\sqrt{17}}{2}$	$\frac{1-\sqrt{17}}{2}$
χ_4	16	0	-2	0	0	0	1	1	1	-1	-1
χ_5	16	0	1	0	0	0	$-2cos(\frac{2\pi}{9})$	$-2cos(\frac{4\pi}{9})$	$-2cos(\frac{8\pi}{9})$	-1	-1
χ_6	16	0	1	0	0	0	$-2cos(\frac{4\pi}{9})$	$-2cos(\frac{8\pi}{9})$	$-2cos(\frac{2\pi}{9})$	-1	-1
χ_7	16	0	1	0	0	0	$-2cos(\frac{8\pi}{9})$	$-2cos(\frac{2\pi}{9})$	$-2cos(\frac{4\pi}{9})$	-1	-1
χ_8	17	1	-1	1	1	1	-1	-1	-1	0	0
χ_9	18	2	0	-2	0	0	0	0	0	1	1
χ_{10}	18	-2	0	0	$\sqrt{2}$	$-\sqrt{2}$	0	0	0	1	1
χ_{11}	18	-2	0	0	$-\sqrt{2}$	$\sqrt{2}$	0	0	0	1	1

Concrètement, les actions de Galois sur les caractères irréductibles permutent les lignes de cette table. Notons tout d'abord qu'elles fixeront toujours les caractères à valeurs exclusivement rationnelles. Nous reviendrons sur ce cas dans la partie suivante.

On peut par exemple faire agir $Gal\big(\mathbb{Q}(\sqrt{17})/\mathbb{Q}\big)$ sur $\{\chi_2;\chi_3\}$. De même, par les formules d'Euler, si $\sigma : \zeta_9 \rightsquigarrow \zeta_9^2 \in Gal\big(\mathbb{Q}(\zeta_9)/\mathbb{Q}\big)$, alors $\sigma.\chi_5 = \chi_6$ et $\sigma^2.\chi_5 = \chi_7$.

Cependant, si on veut agir sur l'intégralité de $Irr(G)$, il faut choisir $L = \mathbb{Q}\big(\sqrt{2};\sqrt{17};cos(\frac{2\pi}{9})\big)$ ou un corps plus grand. Les orbites de l'action générale correspondante seront donc $\{\chi_2;\chi_3\}$, $\{\chi_5;\chi_6;\chi_7\}$, $\{\chi_{10};\chi_{11}\}$ et les singletons restants.

En ce qui concerne les classes de conjugaison, le premier résultat de la partie suivante va permettre de visualiser l'action directement sur la table. Il donnera par exemple que les orbites sous l'action de $Gal\big(\mathbb{Q}(\zeta_{1224})/\mathbb{Q}\big)$ sont $\{Cl_5;Cl_6\}$, $\{Cl_7;Cl_8;Cl_9\}$, $\{Cl_{10};Cl_{11}\}$ et les singletons restants.

5.5 Propriétés des actions de Galois

Dans ce paragraphe, on reprend N un multiple de e et on fixe la notation $\Gamma = Gal\big(\mathbb{Q}(\zeta_N)/\mathbb{Q}\big)$. Comme $\mathbb{Q}(\chi) \subset \mathbb{Q}(\zeta_N) \subset \mathbb{C}$ pour tout $\chi \in Car(G)$, Γ agit à la fois sur $Car(G)$ et $Cl(G)$ d'après le paragraphe précédent.

Commençons par un propriété fondamentale qui lie ces deux actions. Elle nous permettra, entre autres, de vérifier l'hypothèse du lemme de Brauer :

Propriété : Pour tous $\chi \in Irr(G),\ \sigma_m \in \Gamma,\ K \in Cl(G),\ g \in K$, et $g' \in \sigma_m.K$, on a :

$$\sigma_m.\chi\ (g) = \chi(g^m) = \chi(g').$$

Preuve : A nouveau, soit (ρ, V) une représentation de G induisant χ. Alors $\rho(g^m) = \rho(g)^m$. De plus, comme dans la preuve du lemme 2.1, on peut digonaliser la matrice de $\rho(g)$ dans une base de façon à ce que ses coefficients soient dans $\mathbb{Q}(\zeta_e) \subset \mathbb{Q}(\zeta_N)$. Comme $\sigma_m \in \Gamma = Gal\big(\mathbb{Q}(\zeta_N)/\mathbb{Q}\big)$, $\chi(g^m) = tr(\rho(g^m)) = tr(\rho(g)^m) = \sigma_m\big(tr(\rho(g))\big) = \sigma_m.\chi\ (g)$.

Remarque : Si l'on connaît la table des caractères de G et que l'on veut connaître un $\sigma.K$, il suffit donc d'appliquer σ à la colonne correspondant à K. C'est ce qui permet de déterminer les orbites dans le paragraphe précédent.

Théorème 5.5 : On a défini une action de Γ sur $Irr(G)$ et sur $Cl(G)$. Tout $\sigma \in \Gamma$ fixe le même nombre d'éléments de l'un et l'autre de ces ensembles.

Preuve : Notons d'abord que, si $\sigma \in \Gamma$ et $K \in Cl(G)$, alors :

$$\sigma.K = K \Leftrightarrow K = \sigma^{-1}.(\sigma.K) = \sigma^{-1}.K \quad .$$

Le résultat du théorème découle bien sûr du lemme de Brauer mais, pour cette preuve uniquement, on considère l'action de Γ sur les classes de conjugaison définie par : $(\sigma_m; K) \mapsto \sigma_m^{-1}.K$. La propriété précédente donne exactement l'hypothèse du lemme de Brauer pour cette nouvelle action. Ainsi, tout $\sigma \in \Gamma$ fixe autant de classes de conjugaisons que de caractères irréductibles.
De plus, par le premier point de la preuve, pour tout $\sigma \in \Gamma$, les deux actions de σ sur $Cl(G)$ fixent les mêmes éléments, donc a fortiori le même nombre d'éléments. Ceci conclut le théorème.

Le but est maintenant de voir dans quels cas les deux actions sont isomorphes.

Théorème 5.6 : Si Γ est cyclique, ces deux actions sont isomorphes. C'est notamment le cas si e est la puissance d'un nombre premier impair.

Preuve : Si Γ est cyclique, ses sous-groupes le sont aussi : soit H un sous-groupe et σ un générateur de H.
Les puissances de σ fixent au moins les mêmes éléments que σ donc les éléments fixés par H sont ceux fixés par σ. Or, par le théorème précédent, σ fixe autant d'éléments de $Irr(G)$ que de $Cl(G)$. D'après le théorème 5.1, ceci est équivalent à dire que les actions sont isomorphes.

De plus, par la conclusion du lemme 2.2, Γ est isomorphe à $(\mathbb{Z}/N\mathbb{Z})^\times$, qui est cyclique si N est la puissance d'un nombre premier impair. Ceci conclut si $e = N$. Sinon, un élément de Γ n'étant que la composition d'un élément de $Gal(\mathbb{Q}(\zeta_e)/\mathbb{Q})$ avec un automorphisme laissant la table des caractères invariante, le résultat tient toujours.

Théorème 5.7 : De façon plus générale, ces deux actions sont isomorphes si et seulement si les listes (avec multiplicité) d'ensembles $\big(\mathbb{Q}(\chi)\big)_{\chi\in Irr(G)}$ et $\big(\mathbb{Q}(K)\big)_{K\in Cl(G)}$ sont les mêmes, où $\mathbb{Q}(\boldsymbol{K})$ est le corps engendré sur $\mathbb{Q}$ par les $\chi(g)$, pour $\chi \in Irr(G)$ et $g \in K$.

Preuve : Pour tout $K \in Cl(G)$, soit $g_K \in K$ un représentant. Soit H un sous-groupe de Γ. Si $K \in Cl(G)$, on a : H fixe $\mathbb{Q}(K)$ si et seulement si pour tout $\chi \in Irr(G)$, H fixe $\chi(g_K)$ et donc si et seulement si pour tout $\chi \in Irr(G)$ et $\sigma \in H$, on a $\sigma\big(\chi(g_K)\big) = \sigma.\chi\ (g_K) = \chi(g_K)$. Mais, par la première propriété de ce paragraphe, $\sigma.\chi\ (g_K) = \chi(g_{\sigma.K})$ donc ceci est équivalent à : $\forall\sigma \in H, \forall\chi \in Irr(G), \chi(g_{\sigma.K}) = \chi(g_K)$. Par le second théorème d'orthogonalité des caractères, on a donc l'équivalence :

$$H \text{ fixe } \mathbb{Q}(K) \ \Leftrightarrow\ \forall\sigma \in H,\ \sigma.K = K \ \Leftrightarrow\ H \text{ fixe } K.$$

$$\begin{aligned}\text{On a également :}\quad H \text{ fixe } \mathbb{Q}(\chi) \ &\Leftrightarrow\ \forall g \in G,\ H \text{ fixe } \chi(g) \ \Leftrightarrow\ \forall g \in G, \forall\sigma \in H,\ \ \sigma.\chi\ (g) = \chi(g)\\ &\Leftrightarrow\ H \text{ fixe } \chi\end{aligned}$$

Ainsi, si les listes de l'énoncé sont les mêmes, tout sous-groupe H de G fixera notamment le même nombre d'extensions des deux types et donc de classes de conjugaison et de caractères irréductibles par ce qui précède. D'après la caractérisation du théorème 5.1, les actions sont donc isomorphes.

Réciproquement, si les actions sont isomorphes, tout sous-groupe de Γ fixera le même nombre de caractères irréductibles que de classes de conjugaison.
Si H est un sous-groupe de Γ, on pose E l'ensemble des sous-groupes contenant strictement H. Alors, par la formule du crible et ce qui précède :

$$\begin{aligned}\left|Irr(G)^H \setminus \bigcup_{H'\in E} Irr(G)^{H'}\right| &= \left|Irr(G)^H\right| + \sum_{k=1}^{|E|}(-1)^k \left(\sum_{(H_i)_{1\le i\le k}\in E^k} \left|\bigcap_{i=1}^{k} Irr(G)^{H_i}\right|\right)\\ &= \left|Irr(G)^H\right| + \sum_{k=1}^{|E|}(-1)^k \left(\sum_{(H_i)_{1\le i\le k}\in E^k} \left|Irr(G)^{<(H_i)>}\right|\right)\\ &= \left|Cl(G)^H\right| + \sum_{k=1}^{|E|}(-1)^k \left(\sum_{(H_i)_{1\le i\le k}\in E^k} \left|Cl(G)^{<(H_i)>}\right|\right)\\ &= \left|Cl(G)^H \setminus \bigcup_{H'\in E} Cl(G)^{H'}\right|.\end{aligned}$$

Ceci permet de conclure. En effet, si M est un un sous-corps de $\mathbb{Q}(\zeta_N)$ et $H = \{\sigma \in \Gamma \mid \sigma_{|M} = id_M\}$, alors, d'après la correspondance de Galois, pour tout $\chi \in Irr(G)$, $\mathbb{Q}(\chi) = M$ si et seulement si $\{\sigma \in \Gamma \mid \sigma_{|\mathbb{Q}(\chi)} = id_{\mathbb{Q}(\chi)}\} = H$, ce qui revient à dire que $\chi \in Irr(G)^H \setminus \bigcup_{H' \in E} Irr(G)^{H'}$. De même, $\mathbb{Q}(K) = M$ si et seulement si $K \in Cl(G)^H \setminus \bigcup_{H' \in E} Cl(G)^{H'}$. Par ce qui précède, il y a donc autant de χ que de K qui engendrent M, pour tout M, ce qui achève la preuve.

Remarque : Si l'on connaît la table des caractères de G, ce théorème permet de savoir facilement si les actions sont isomorphes, comme c'est le cas pour $PSL_2(\mathbb{F}_{17})$, par exemple.

Malheureusement, cette propriété n'est pas toujours vérifiée. En effet, le 9-ième groupe d'ordre 32 de la base de données Magma donne un contre-exemple. Voilà sa table des caractères (où i désigne le nombre complexe usuel) :

$Classes$	Cl_1	Cl_2	Cl_3	Cl_4	Cl_5	Cl_6	Cl_7	Cl_8	Cl_9	Cl_{10}	Cl_{11}	Cl_{12}	Cl_{13}	Cl_{14}
$Ordres$	1	4	2	4	2	2	8	4	2	4	2	8	8	8
χ_{st}	1	1	1	1	1	1	1	1	1	1	1	1	1	1
χ_{oui}	1	-1	1	1	1	1	-1	-1	1	1	1	-1	-1	-1
χ_{che}	1	1	-1	1	1	1	-1	1	-1	1	1	-1	-1	-1
χ_{gnon}	1	-1	-1	1	1	1	1	-1	-1	1	1	1	1	1
χ_{noa}	1	i	1	1	-1	1	i	$-i$	-1	-1	-1	$-i$	i	$-i$
χ_{rikou}	1	$-i$	1	1	-1	1	$-i$	i	-1	-1	-1	i	$-i$	i
χ_{lian}	1	i	-1	1	-1	1	$-i$	$-i$	1	-1	-1	i	$-i$	i
$\chi_{limandjaro}$	1	$-i$	-1	1	-1	1	i	i	1	-1	-1	$-i$	i	$-i$
χ_{llBill}	2	0	0	-2	2	2	0	0	0	-2	2	0	0	0
χ_{osque}	2	0	0	-2	-2	2	0	0	0	2	-2	0	0	0
χ_{mono}	2	0	0	0	2	-2	$-\sqrt{2}$	0	0	0	-2	$-\sqrt{2}$	$\sqrt{2}$	$\sqrt{2}$
χ_{pa}	2	0	0	0	2	-2	$\sqrt{2}$	0	0	0	-2	$\sqrt{2}$	$-\sqrt{2}$	$-\sqrt{2}$
χ_{proco}	2	0	0	0	-2	-2	$-i\sqrt{2}$	0	0	0	2	$i\sqrt{2}$	$i\sqrt{2}$	$-i\sqrt{2}$
$\chi_{dimieux?}$	2	0	0	0	-2	-2	$i\sqrt{2}$	0	0	0	2	$-i\sqrt{2}$	$-i\sqrt{2}$	$i\sqrt{2}$

On remarque que les classes de conjugaisons (colonnes) n'engendrent que les $\mathbb{Q}$, $\mathbb{Q}(i)$ et $\mathbb{Q}(i;\sqrt{2})$ alors que le dernier caractère (ligne) engendre l'extension $\mathbb{Q}(i\sqrt{2})/\mathbb{Q}$.

6 Valeurs de la table de caractères

6.1 Éléments réels, éléments rationnels

Le but de ce paragraphe est de trouver des conditions pour prévoir quelles valeurs de la table de caractères seront réelles, puis entières.

Définitions : On définit les notions suivantes :

- $\boldsymbol{g} \in G$ est dit **réel** si : $\forall \chi \in Irr(G),\ \chi(g) \in \mathbb{R}$;
- $\boldsymbol{\chi} \in Irr(G)$ est dit **réel** si : $\forall g \in G,\ \chi(g) \in \mathbb{R}$;
- $\boldsymbol{K} \in Cl(G)$ est dite **réelle** si g est réel pour un $g \in K$.

Remarque : $g \in G$ est réel si et seulement si, pour tout $\chi \in Irr(G),\ \chi(g) = \overline{\chi(g)} = \chi(g^{-1})$.

Théorème 6.1 : G a autant de caractères irréductibles réels que de classes de conjugaison réelles. De plus, il n'y en a qu'une seule si et seulement si $n = |G|$ est impair.

Preuve : Soit $\sigma_{-1} \in Gal(\mathbb{Q}(\zeta_e)/\mathbb{Q})$ la conjugaison complexe sur $\mathbb{Q}(\zeta_e)$. D'après le théorème 5.5, σ_{-1} fixe autant de caractères irréductibles que de classes de conjugaison. Or : $\chi \in Irr(G)$ est fixé par $\sigma_{-1} \Leftrightarrow \forall g \in G, \chi(g) = \overline{\chi(g)} \Leftrightarrow \chi$ est réel. De même : $K \in Cl(G)$ est fixé par $\sigma_{-1} \Leftrightarrow \forall g \in K, \chi(g) = \chi(g^{-1}) \Leftrightarrow K$ est réelle. Ceci donne le premier résultat.

Si G est d'ordre pair, il possède un élément g d'ordre 2. Comme $g = g^{-1}$, $\chi(g) = \chi(g^{-1})$ pour tout $\chi \in Irr(G)$ donc la classe de g est réelle. g étant d'ordre 2, sa classe de conjugaison n'est pas $\{1\}$, qui est toujours réelle. Ainsi, il y au moins deux classes réelles distinctes. Par contraposée, s'il n'y a qu'une seule classe réelle (ou un seul caractère irréductible réel), n est impair.

Si n est impair, soit $g \in G$ réel. Alors pour tout $\chi \in Irr(G)$, $\chi(g) = \chi(g^{-1})$. Par le second théorème d'orthogonalité, g et g^{-1} sont dans la même classe de conjugaison : soit $h \in G$ tel que $g^{-1} = hgh^{-1}$. On a donc $h^2gh^{-2} = hg^{-1}h^{-1} = g$. Comme n est impair, $ord(h)$ l'est aussi et donc $ord(h^2) = \frac{ord(h)}{ord(h) \wedge 2} = ord(h)$ donc h et h^2 engendrent le même sous-groupe. Comme g est fixé par l'action de conjugaison de $<h^2> = <h>$, g est fixé par h. Finalement, $g^{-1} = hgh^{-1} = g$ donc $g = 1$. Ainsi, la seule classe de conjugaison réelle est $\{1\}$, ce qui conclut la preuve.

Remarque : Ce théorème montre que la table des caractères de G a autant de colonnes que de lignes avec des valeurs exclusivement réelles.

Définitions : De même que précédemment :

- $\boldsymbol{g} \in G$ est dit **rationnel** si : $\forall \chi \in Irr(G),\ \chi(g) \in \mathbb{Q}$;
- $\boldsymbol{\chi} \in Irr(G)$ est dit **rationnel** si : $\forall g \in G,\ \chi(g) \in \mathbb{Q}$;
- $\boldsymbol{K} \in Cl(G)$ est dite **rationnelle** si g est rationnel pour un $g \in K$.

Remarque : Les valeurs des caractères étant des entiers algébriques, si un caractère est rationnel, il est même à valeurs entières par le théorème 4.1.

Théorème 6.2 : $g \in G$ est rationnel si et seulement si pour tout $h \in G$ engendrant le même sous-groupe que g, h est conjugué avec g.

Preuve : Si $\chi \in Irr(G)$, l'ensemble des points de $\mathbb{Q}(\chi)$ fixés par $Gal(\mathbb{Q}(\zeta_n))$ est $\mathbb{Q}$. Ainsi :

$$\begin{aligned} g \in G \text{ est rationnel} &\Leftrightarrow \forall \chi \in Irr(G), \quad \chi(g) \in \mathbb{Q} \\ &\Leftrightarrow \forall \chi \in Irr(G), \forall \sigma \in Gal(\mathbb{Q}(\zeta_n)), \quad \sigma.\chi\ (g) = \chi(g) \\ &\Leftrightarrow \forall m \in [|1;n|], m \wedge n = 1, \forall \chi \in Irr(G), \quad \chi(g^m) = \chi(g) \\ &\Leftrightarrow \forall m \in [|1;n|], m \wedge n = 1, \quad g \text{ et } g^m \text{ sont conjugués} \end{aligned}$$

Et cette dernière équivalence donne le résultat par le lemme 2.4.

Théorème 6.3 : Soit $r \in \mathbb{N}^*$. La table des caractères du groupe symétrique S_r est à valeurs entières.

Preuve : D'après le théorème précédent (et le lemme 2.4), il s'agit de montrer que, pour tous $\sigma \in S_r$ et $j \in \mathbb{Z}$ premier avec $r!$, σ et σ^j sont conjugués. On notera $supp(\sigma)$ le support de $\sigma \in S_r$ et id le neutre de S_r.

Soit $k \in [|1;r|]$, $\sigma \in S_r$ un k-cycle et $l \in \mathbb{Z}$. Si $supp(\sigma^l) \neq supp(\sigma)$, soit $a \in supp(\sigma) \setminus supp(\sigma^l)$. Alors $supp(\sigma^l) \subset supp(\sigma) = \{\sigma^i(a) \mid i \in [|1;k|]\}$ car σ est un cycle. Mais, $\forall i \in [|1;k|]$:

$$\sigma^l(\sigma^i(a)) = \sigma^i(\sigma^l(a)) = \sigma^i(a) \quad \text{car } a \notin supp(\sigma^l).$$

Donc $\sigma^i(a) \notin supp(\sigma^l)$, pour tout $i \in [|1;k|]$, d'où $supp(\sigma^l) = \emptyset$. Ainsi, $supp(\sigma^l) = supp(\sigma)$ ou $\sigma^l = id$.

Si $j \in \mathbb{Z}$, soit σ_1 et σ_2 deux cycles à supports disjoints de la décomposition de σ^j, d'ordres respectifs l et m avec $l \leq m$. Alors σ_1^l et σ_2^l apparaissent dans la décomposition de σ^l. Mais, comme $\sigma_1^l = id$, $supp(\sigma^l) \neq supp(\sigma)$, donc $\sigma^l = id$. Mais alors $\sigma_2^l = id$ aussi et donc $l = m$. Ainsi, σ^j se décompose en produit de cycles à supports disjoints de même ordre.

Supposons à présent que j est premier avec $r!$, donc notamment premier avec k. Alors $ord(\sigma^j) = k$. Or, par ce qui précède, σ^j est un produit de cycles de même ordre k'. Ces cycles sont à supports disjoints, donc ils commutent : $k = ord(\sigma^j) = ppcm(k') = k'$. Comme $supp(\sigma^j) \subset supp(\sigma)$, σ^j est nécessairement un k-cycle de même support que σ. Ainsi, σ et σ^j sont conjugués dans S_r (et même dans $S_{supp(\sigma)}$) si σ est un cycle.

On peut maintenant prouver le théorème : soit $\sigma \in S_r$, $\sigma = \prod_{i=1}^{N} \sigma_i$ sa décomposition en produit de cycles à supports disjoints et $j \in \mathbb{Z}$ premier avec $r!$. Par ce qui précède, pour tout $i \in [|1;n|]$, il existe $h_i \in S_{supp(\sigma_i)}$ tel que : $\sigma_i = h_i \sigma_i^j h_i^{-1}$. Ainsi :

$$\begin{aligned} \sigma = \prod_{i=1}^{N} \sigma_i = \prod_{i=1}^{N} h_i \sigma_i^j h_i^{-1} &= \left(\prod_{i=1}^{N} h_i\right)\left(\prod_{i=1}^{N} \sigma_i^j\right)\left(\prod_{i=1}^{N} h_i^{-1}\right) \quad \text{car tous les supports sont disjoints} \\ &= h\sigma^j h^{-1} \quad \text{avec } h = \prod_{i=1}^{N} h_i \in S_r. \end{aligned}$$

Finalement, σ et σ^j sont bien conjugués, ce que l'on voulait montrer.

6.2 Zéros de la table des caractères

A l'instar du paragraphe précédent, le but est ici de prévoir les valeurs de certaines entrées de la table des caractères. Plus précisément, on s'intéresse à l'existence et la position des zéros puis à la position des valeurs ne pouvant pas s'annuler.

Théorème 6.4 : Soit H un sous-groupe de G et $\chi \in Irr(G)$. Alors $\chi(g)$ est non nul pour tout $g \in G \setminus H$ si et seulement si $\chi(g)$ est une racine de l'unité pour tout $g \in G \setminus H$ et $\chi_{|H}$ est un caractère irréductible de H.

Preuve : L'implication indirecte est évidente car les racines de l'unité sont non nulles.

Pour tout $g \in G \setminus H$, soit $C_g = \{g^m \mid m \wedge n = 1\}$. Alors, pour tout $\sigma_m \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, $\sigma_m\left(\prod_{h\in C_g}\chi(h)\right) = \prod_{h\in C_g}\sigma_m.\chi\ (h) = \prod_{h\in C_g}\chi(h^m) = \prod_{h'\in C_g}\chi(h')$ par la propriété du paragraphe 4.5. Comme il est fixé par tous les éléments du groupe de Galois, $\prod_{h\in C_g}\chi(h) \in \mathbb{Q}$ et c'est même un entier car c'est aussi un entier algébrique. En passant au carré du module et comme $\chi(h) \neq 0$ par hypothèse, on obtient : $\prod_{h\in C_g}|\chi(h)|^2 \geq 1$.

Or, par concavité : $ln\left(\frac{1}{|C_g|}\sum_{h\in C_g}|\chi(h)|^2\right) \geq \frac{1}{|C_g|}\sum_{h\in C_g} ln(|\chi(h)|^2) = ln\left(\left(\prod_{h\in C_g}|\chi(h)|^2\right)^{\frac{1}{|C_g|}}\right)$.

En passant à l'exponentielle, on trouve : $\frac{1}{|C_g|}\sum_{h\in C_g}|\chi(h)|^2 \geq \left(\prod_{h\in C_g}|\chi(h)|^2\right)^{\frac{1}{|C_g|}} \geq 1$. Ainsi :

$$\sum_{h\in C_g}|\chi(h)|^2 \geq |C_g|$$

et il y a égalité si et seulement si $|\chi(h)| = 1$ pour tout $h \in C_g$.

De plus, si $C_g \cap H \neq \emptyset$, $C_g \subset H$ car H est un sous-groupe, donc stable par produit. Ainsi, si C_g n'est pas inclus dans H, il en est disjoint. Les C_g étant les classes de la relation d'équivalence "engendre le même groupe que", d'après le lemme 2.4 il existe $(g_i)_{1\leq i\leq r}$ tels que $\left(C_{g_i}\right)_{1\leq i\leq r}$ forme une partition de $G \setminus H$. Ainsi :

$$\begin{aligned} n = \sum_{g\in G}|\chi(g)|^2 &= \sum_{g\in H}|\chi(g)|^2 + \sum_{g\in G\setminus H}|\chi(g)|^2 = |H| \times \left[\chi_{|H};\chi_{|H}\right] + \sum_{i=1}^{r}\sum_{h\in C_{g_i}}|\chi(h)|^2 \\ &\geq |H| \times \left[\chi_{|H};\chi_{|H}\right] + \sum_{i=1}^{r}|C_{g_i}| \geq |H| \times 1 + \sum_{i=1}^{r}|C_{g_i}| \\ &= |H| + |G \setminus H| = n. \end{aligned}$$

Le cas d'égalité de la deuxième inégalité étant $\left[\chi_{|H};\chi_{|H}\right] = 1$ et celui de la première étant $|\chi(h)| = 1$ pour tout $h \in G \setminus H$, il ne reste qu'à montrer que $|\chi(g)|$ est de module 1 si et seulement si c'est une racine de l'unité.

Soit $k \in \mathbb{N}$ et $x = \chi(g)^k$. Si $\sigma_{-1} \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ est la conjugaison complexe, alors, pour tout $\sigma \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, $|\sigma(x)|^2 = \sigma(x) \times \sigma_{-1}(\sigma(x)) = \sigma\big(x \times \sigma_{-1}(x)\big) = \sigma(|x|^2) = 1$.

On sait de plus que x est un entier algébrique dans $\mathbb{Q}(\zeta_n)$: son polynôme minimal est de degré au plus $\varphi(n)$ et est à coefficients entiers. De plus, par les relations coefficients-racines, ces coefficients sont des polynômes symétriques élémentaires en les $\sigma(x) \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Ces derniers étant de module 1, par inégalité triangulaire, le module des coefficients est borné (par le nombre de termes du polynôme symétrique correspondant). Comme ce sont des entiers, il existe donc un nombre fini de polynôme minimal d'une puissance de $\chi(g)$.

Ainsi, si $(\chi(g)^k)_{k\in\mathbb{N}}$ était infinie, le nombre de polynômes minimaux le serait aussi. Cette famille est donc nécessairement finie. Notamment, il existe $(k;k')\in\mathbb{N}^2$, $k\leq k'$ tel que $\chi(g)^k=\chi(g)^{k'}$: $\chi(g)$ est donc une racine $(k'-k)$-ième de l'unité, ce qu'il fallait démontrer.

Exemple : La table des caractères de S_5 est :

Classes	***Id***	2-*cycles*	***3-cycles***	4-*cycles*	***5-cycles***	$\boldsymbol{Cl_6}$	Cl_7
Ordres	1	2	3	4	5	2	6
Cardinaux	1	10	20	30	24	15	20
χ_1	1	1	1	1	1	1	1
χ_2	1	-1	1	-1	1	1	-1
χ_3	4	2	1	0	-1	0	-1
χ_4	4	-2	1	0	-1	0	1
χ_5	5	1	-1	-1	0	1	1
χ_6	5	-1	-1	1	0	1	-1
$\boldsymbol{\chi_7}$	6	0	0	0	1	-2	0

où Cl_6 et Cl_7 sont les classes de conjugaison constituées des doubles transpositions et des produits d'une transposition et d'un 3-cycle (à supports disjoints) respectivement.
Dans le cadre du théorème, si $H=A_5$, le sous-groupe alterné, les classes constituant H sont représentées en rouge et on calcule facilement que seule la restriction de χ_7 n'est plus irréductible. De plus, les caractères de degré 4 s'annulent en dehors de H. Cependant, pour les quatre caractères restants, on constate que les valeurs prises en dehors de H sont 1 et -1, qui sont des racines de l'unité, comme prévu par le théorème.

Bien qu'utilisable en soit, ce théorème permet surtout d'établir le corrolaire suivant :

Théorème de Burnside : Si $\chi\in Irr(G)$ n'est pas de degré 1, il s'annule en au moins un $g\in G$.

Preuve : Si $H=\{1\}$, $\left[\chi_{|H};\chi_{|H}\right]=\chi(1)^2$. Ainsi, si χ n'est pas de degré 1, $\chi_{|H}$ n'est pas irréductible. Par contraposée du théorème précédent, il existe $g\in G\setminus\{1\}$ tel que $\chi(g)=0$.

Le prochain but de ce paragraphe est d'établir deux théorèmes permettant de prévoir l'emplacement de zéros et de valeurs non nulles dans la table des caractères. Mais avant ça, il faut poser quelques notations et établir deux résultats intermédiaires.

Dans le cadre du lemme suivant, posons $K\in Cl(G)$, $m\in\mathbb{N}^*$ ainsi que

$$\boldsymbol{S_m(K)}=\left\{(x_i)_{1\leq i\leq m}\in G^m\;\middle|\;\prod_{i=1}^{m}x_i\in K\right\}\quad\text{et}\quad \boldsymbol{s}:(x_i)_{1\leq i\leq m}\in G^m\mapsto\left(x_m;(x_i)_{1\leq i\leq m-1}\right).$$

Si $(x_i)\in S_m(K)$, alors $x_m\prod_{i=1}^{m-1}x_i$ est le conjugué de $\prod_{i=1}^{m}x_i$ par x_m^{-1} donc $s\big((x_i)\big)\in S_m(K)$. Ainsi, s est un automorphisme d'ordre m de G^m et $<\boldsymbol{s}>$ **agit sur** $\boldsymbol{S_m(K)}$.

Lemme : Soit p premier, v la valuation p-adique de n, $N\in\mathbb{N}^*$ et $m=p^{v+N}$. Si $K\in Cl(G)$ a ses éléments d'ordre divisible par p, le cardinal des $<s>$-orbites de $S_m(K)$ est un multiple de p^N.

Preuve : Soit $x = (x_i)_{1\leq i\leq m} \in S_m(K)$, O sa $<s>$-orbite et H son stabilisateur. H étant un sous-groupe de $<s>$, il est engendré par s^r pour un certain r divisant m. Donc :
$|H| = ord(s^r) = \frac{m}{m \wedge r} = \frac{m}{r}$. Ainsi, $|O| = \frac{|<s>|}{|H|} = r$ car $|<s>| = ord(s) = m$.

En outre, par définition du stabilisateur, s^r fixe x. Donc, si $l = m/r$,
$\big((x_{i+jr})_{1\leq i\leq r}\big)_{0\leq j\leq l-1} = x = s^r\big((x_i)_{1\leq i\leq m}\big) = \Big((x_i + (l-1)r)_{1\leq i\leq l}; \big(x_{i+jr}\big)_{1\leq i\leq r}\big)_{0\leq j\leq l-2}\Big)$. Ainsi, pour tout $j \in [|0, l-1|]$ et $i \in [|1; r|]$, $x_{i+jr} = x_i$. Autrement dit, $x = (y)_{1\leq j\leq l}$, où $y = (x_i)_{1\leq i\leq r}$.

Soit $g = \prod_{i=1}^{m} x_i$. Par ce qui précède, $g = h^l$ avec $h = \prod_{i=1}^{r} x_i$ et, d'après le lemme 2.3, on peut écrire $h = ab$ avec a d'ordre une puissance de p et b d'ordre premier avec p. Il en va donc de même de a^l et b^l respectivement et $g = a^l b^l$. De plus, comme $x \in S_m(K)$, $g \in K$ donc p divise l'ordre de g et donc $1 \neq ord(a^l) = \frac{ord(a)}{ord(a) \wedge l}$. Mais l et $ord(a)$ sont des puissances de p donc $ord(a) \wedge l = min(ord(a); l)$: pour que la non-égalité soit vraie, il faut que l divise strictement $ord(a)$, qui lui-même divise l'ordre du groupe. Finalement, $\frac{p^{v+N}}{r} = l \mid p^v$, d'où $p^N \mid r = |O|$.

Propriété : Pour tous $\chi \in Irr(G)$, $g \in G$ et $m \in \mathbb{N}^*$,

$$\sum_{\substack{(x_1;\ldots;x_m)\in G^m \\ x_1\ldots x_m = g}} \prod_{i=1}^{m} \chi(x_i) = \left(\frac{n}{\chi(1)}\right)^{m-1} \chi(g).$$

Preuve : Soit $\chi \in Irr(G)$ et $e_\chi = \frac{\chi(1)}{n} \sum_{g\in G} \chi(g^{-1})\, g$. D'après le théorème 3.4, $e_\chi^2 = e_\chi$. Ainsi, par récurrence directe, pour tout $m \in \mathbb{N}^*$, $e_\chi^m = e_\chi$.

Si $g \in G$, le coefficient en g^{-1} de cette égalité donne : $\left(\frac{\chi(1)}{n}\right)^m \times \sum_{\substack{(x_1;\ldots;x_m)\in G^m \\ x_1\ldots x_m = g^{-1}}} \prod_{i=1}^{m} \chi(x_i^{-1}) = \frac{\chi(1)}{n}\chi(g)$.

Il ne reste plus qu'à diviser cette égalité par $\left(\frac{\chi(1)}{n}\right)^m$ et faire le changement de variable $(x_1; \ldots; x_m) \mapsto (x_m^{-1}; \ldots; x_1^{-1})$.

Définition : Soit $p \in \mathbb{N}$ un diviseur premier de n, v sa valuation p-adique et $\chi \in Irr(G)$. On dit que χ a ***p*-défaut zéro** si p^v divise le degré de χ.

Théorème 6.5 : Soit p un diviseur premier de n, $\chi \in Irr(G)$ de p-défaut zéro et $g \in G$. Si l'ordre de g est divisible par p, alors $\chi(g) = 0$.

Preuve : Soit v la valuation p-adique de n, $N \in \mathbb{N}^*$, $m = p^{v+N}$, K la classe de conjugaison de g et k son cardinal. Soit $(O_j)_{j\in J}$ l'ensemble des $<s>$-orbites de $S_m(K)$, qui en forme donc une partition.
Alors, en sommant la propriété précédente pour chaque élément de K, on obtient :

$$\left(\frac{n}{\chi(1)}\right)^{m-1} \chi(g) \times k = \sum_{(x_i)\in S_m(K)} \prod_{i=1}^{m} \chi(x_i) = \sum_{j\in J} \left(\sum_{(x_i)\in O_j} \prod_{i=1}^{m} \chi(x_i) \right) = \sum_{j\in J} \left(|O_j| \times \prod_{i=1}^{m} \chi(x_i) \right),$$

la dernière égalité valant pour n'importe quel $(x_i) \in O_j$, car le produit y est constant (s ne fait que permuter les termes).

De plus, par le lemme précédent, $p^N \mid |O_j|$. Donc, les valeurs des caractères étant des entiers algébriques, si on note $\beta = k \times \chi(g)$, $\beta \left(\frac{n}{\chi(1)}\right)^{m-1} = \alpha\ p^N$ pour un $\alpha \in \mathbb{E}$.

De plus, comme χ a p-défaut zéro, $\frac{n}{\chi(1)}$ est premier avec p. Ainsi, $\left(\frac{n}{\chi(1)}\right)^{m-1}$ est nécessairement premier avec p^N donc, en multipliant une relation de Bézout par β, il existe $(u; v) \in \mathbb{Z}^2$ tels que :

$$\beta = up^N\beta \ + \ v\left(\frac{n}{\chi(1)}\right)^{m-1}\beta = p^N\left(uk\ \chi(g) + v\ \alpha\right).$$

Ainsi, pour tout $N \in \mathbb{N}^*$, β est le produit de p^N et d'un entier algébrique. Il reste à en déduire que $\beta = 0$.

Soit P le polynôme minimal de β, qui est donc à coefficients entiers. Par ce qui précède, p^N divise β dans $\mathbb{E}$, donc divise aussi ses puissances. Il faut donc nécessairement que p^N divise le coefficient constant de P dans $\mathbb{E}$ mais aussi dans $\mathbb{Q}$ (les deux termes sont entiers) et donc dans $\mathbb{E} \cap \mathbb{Q} = \mathbb{Z}$. Ceci devant être vrai pour tout N, le coefficient constant est nécessairement nul. Cela implique que le polynôme X divise P, et donc lui soit égal par irréductibilité. Finalement, $0 = \beta = k \times \chi(g)$ donc $\chi(g) = 0$.

Avant d'illustrer ce théorème par un exemple, énonçons-en un autre qui lui est directement lié par son résultat, même si sa preuve repose sur d'autres notions.

Théorème 6.6 : Soit $p \in \mathbb{N}$ premier, $g \in G$ d'ordre une puissance de p et $\chi \in Car(G)$. Si p ne divise pas $\chi(1)$, alors $\chi(g) \neq 0$.

Preuve : Soit $d = \chi(1)$ et $(q; k) \in \mathbb{N}^2$ tel que $q = ord(g) = p^k$. En reprenant le lemme 2.1 avec $ord(g)$ à la place de e, on obtient que $\chi(g)$ est somme de d racines q-ième de l'unité. En réécrivant ces racines comme puissance de ζ_q, on a l'existence de $(a_i)_{0\leq i\leq q-1} \in \mathbb{N}^q$ tels que :

$$\chi(g) = P(\zeta_q) = \sum_{i=0}^{q-1} a_i\ \zeta_q^i \quad \text{et} \quad \sum_{i=0}^{q-1} a_i = d.$$

Supposons que $\chi(g) = 0$. Alors ζ_q annule P et donc $P = \phi_q\ Q$, où ϕ_q est le polynôme minimal de ζ_q et Q est un polynôme sur $\mathbb{Q}$. On veut montrer que Q est à coefficients entiers. P et ϕ_q sont à coefficients entiers et le dernier est même primitif. Q s'écrit sous la forme d'un rationnel a multiplié par un polynôme à coefficients entiers primitif. Par multiplicativité des contenus, a est le contenu de P, donc entier.

Finalement, les coefficients de Q sont entiers et, comme $\phi_q = \sum_{i=0}^{p-1} \left(X^{p^{k-1}}\right)^i$, on a :

$$d = P(1) = \phi_q(1)Q(1) = pQ(1) \in p\mathbb{Z}.$$

Ainsi, $p \mid d$ si $\chi(g) = 0$ et on conclut par contraposée.

Exemple : Pour illustrer les deux derniers théorèmes, revenons sur la table des caractères de $PSL_2(\mathbb{F}_{17})$, d'ordre $2448 = 16 \times 9 \times 17$. Les zéros prévus par le premier théorème sont en violet et les valeurs non nulles données par le second sont en bleu.

$Classes$	Cl_1	Cl_2	Cl_3	Cl_4	Cl_4	Cl_6	Cl_7	Cl_8	Cl_9	Cl_{10}	Cl_{11}
$Ordres$	1	2	3	4	8	8	9	9	9	17	17
χ_1	1	1	1	1	1	1	1	1	1	1	1
χ_2	9	1	0	1	-1	-1	0	0	0	$\frac{1-\sqrt{17}}{2}$	$\frac{1+\sqrt{17}}{2}$
χ_3	9	1	0	1	-1	-1	0	0	0	$\frac{1+\sqrt{17}}{2}$	$\frac{1-\sqrt{17}}{2}$
χ_4	16	0	-2	0	0	0	1	1	1	-1	-1
χ_5	16	0	1	0	0	0	x	y	z	-1	-1
χ_6	16	0	1	0	0	0	y	z	x	-1	-1
χ_7	16	0	1	0	0	0	z	x	y	-1	-1
χ_8	17	1	-1	1	1	1	-1	-1	-1	0	0
χ_9	18	2	0	-2	0	0	0	0	0	1	1
χ_{10}	18	-2	0	0	$\sqrt{2}$	$-\sqrt{2}$	0	0	0	1	1
χ_{11}	18	-2	0	0	$-\sqrt{2}$	$\sqrt{2}$	0	0	0	1	1

Notons que ces théorèmes ne sont pas des équivalences, certaines valeurs (en noires) ne bénéficiant d'aucune information.

6.3 Ordre de certains éléments

Pour ce paragraphe, on fixe un $\chi \in Irr(G)$. De plus, si $m \in \mathbb{N}^*$, $\mathbb{Q}_m$ désignera $\mathbb{Q}(\zeta_m)$, la m-ième extension cyclotomique.

Nous avons vu que les valeurs de la table des caractères étaient incluses dans $\mathbb{Q}_e$ mais, en général, ce corps est loin d'être le plus petit ayant cette propriété. Ceci a été particulièrement mis en évidence dans le cas des groupes symétriques.

Il y a pourtant des liens entre la plus petite extension cyclotomique contenant les valeurs d'une ligne ou d'une colonne de la table et l'ordre des éléments de G. C'est ce que nous allons voir dans ce dernier paragraphe.

Lemme : Soit $g \in G$. Si $\chi(g) \in \mathbb{Q}_{p^v a} \setminus \mathbb{Q}_{p^{v-1}a}$, avec p, v et a des entiers non nuls et p premier ne divisant pas a, alors p^v divise l'ordre de g.

Preuve : L'ordre de g s'écrit $ord(g) = p^w b$, pour certains $w \in \mathbb{N}$ et b premier avec p. Par le raisonnement du lemme 2.1, $\chi(g) \in \mathbb{Q}_{p^w b}$. Si m est le minimum de v et w, on a, par propriété des extensions cyclotomiques :

$$\chi(g) \in \mathbb{Q}_{p^v a} \cap \mathbb{Q}_{p^w b} = \mathbb{Q}_{(p^v a \,\wedge\, p^w b)} = \mathbb{Q}_{p^m (a \wedge b)} \subset \mathbb{Q}_{p^m a}.$$

Comme $\chi(g) \notin \mathbb{Q}_{p^{v-1}a}$, $\mathbb{Q}_{p^m a}$ ne peut pas être inclu dans $\mathbb{Q}_{p^{v-1}a}$. Ainsi, $m \geq v$. Mais m était le minimum de v et w donc nécessairement $m = v$ et donc $v \leq w$. Notamment, $p^v \mid p^w b = ord(g)$.

Théorème 6.7 : Soit F un corps tel que $\mathbb{Q}(\chi) \subset F \subset \mathbb{Q}_n$ et $\Gamma = Gal(F/\mathbb{Q})$. Si $m \in \mathbb{N}^*$ et $(\sigma_i)_{1 \leq i \leq m} \in \Gamma^m$, l'une des propriétés suivantes est vérifiée :

1. il existe $g \in G$ tel que, pour tout $i \in [|1; m|]$, $\chi(g) \neq \sigma_i\big(\chi(g)\big)$;
2. il existe $k \in [|1; m|]$ et $(i_j)_{1 \leq j \leq k} \in [|1; m|]^k$ distincts tels que $\chi = \left(\prod_{j=1}^{k} \sigma_{i_j}\right) \circ \chi$.

Preuve : Pour tout $i \in [|1;m|]$, soit $r_i = id_F - \sigma_i \in End_{\mathbb{Q}}(F)$. Comme $F/\mathbb{Q}$ est incluse dans une extension cyclotomique, donc abélienne, Γ est abélien. Soit donc r la composition des r_i, peu importe l'ordre.

Supposons que $r \circ \chi \neq 0$ et montrons que l'on a alors la première propriété. En effet, dans le cas contraire, pour tout $g \in G$, il existe un $i \in [|1;m|]$ tel que $\chi(g) = \sigma_i(\chi(g))$ c'est à dire $r_i(\chi(g)) = 0$. Mais alors $r(\chi(g)) = \left(\prod_{\substack{j=1 \\ j\neq i}}^{m} r_j\right)\big(r_i(\chi(g))\big) = 0$. Ceci étant vrai pour tout g (en faisant varier i en conséquence), on a une contradiction avec l'hypothèse.

Réciproquement, supposons que $r \circ \chi = 0$ et montrons que l'on a alors la deuxième propriété. En effet, en remplaçant les r_i par $id_F - \sigma_i$ et en développant r, on obtient :

$$0 = r \circ \chi = \chi + \sum_{k=1}^{m} (-1)^k \left(\sum_{1 \leq i_1 < \cdots < i_k \leq m} \left(\prod_{j=1}^{k} \sigma_{i_j} \right) . \chi \right).$$

Γ agissant sur $Irr(G)$, ceci n'est en final qu'une $\mathbb{Z}$-combinaison linéaire de caractères irréductibles. Par indépendance linéaire, au moins l'un des termes de la somme vaut χ (pour un k impair).

Théorème de Brauer : Soit m le plus petit entier tel que $\mathbb{Q}(\chi) \in \mathbb{Q}_m$. Si $m = \prod_{i \in I} p_i^{v_i}$ est sa décomposition en facteurs premiers, alors G a un élément d'ordre $\prod_{\substack{i \in I \\ v_i > 1}} p_i^{v_i}$.

Preuve : Soit $F = \mathbb{Q}_m$, $J = \{i \in I \mid v_i > 1\}$ et, pour tout $i \in J$, $F_i = \mathbb{Q}_{\frac{m}{p_i}}$. Alors, pour tout $i \in J$, le degré de l'extension est $[F : F_i] = \dfrac{[F : \mathbb{Q}]}{[F_i : \mathbb{Q}]} = \dfrac{\varphi(m)}{\varphi(\frac{m}{p_i})} = p_i$ (car $v_i \geq 2$). Ainsi, $Gal(F/F_i)$ est cyclique, engendré par un σ_i d'ordre p_i, pour tout $i \in J$.

Soit $\sigma = \prod_{i \in E} \sigma_i$, pour $E \subset J$. Supposons par l'absurde que $\sigma \in Gal(F/\mathbb{Q})$ fixe χ. Alors $\mathbb{Q}(\chi)$ est fixé par σ. Mais, dans ce cas, pout tout $i \in E$, $\mathbb{Q}(\chi)$ est fixé par $< \sigma^q > = < \sigma_i >$, où $q = \prod_{\substack{j \in E \\ j \neq i}} p_j$.

Finalement, si $i \in E$, $\mathbb{Q}(\chi) \subset F^{<\sigma_i>} = F_i = \mathbb{Q}_{\frac{m}{p_i}}$. Ceci est absurde par définition de m car $\dfrac{m}{p_i} < m$. Ainsi, la deuxième propriété du théorème précédent n'est jamais vérifiée.

Ainsi, par le théorème précédent, il existe $g \in G$ tel que, pour tout $i \in J$, $\chi(g) \neq \sigma_i(\chi(g))$. Donc $\chi(g) \notin F^{<\sigma_i>} = F_i = \mathbb{Q}_{\frac{m}{p_i}}$. Comme $\chi(g) \in \mathbb{Q}_m \setminus \mathbb{Q}_{\frac{m}{p_i}}$, par le lemme précédent, $p_i^{v_i}$ divise $ord(g)$. En faisant varier $i \in J$, $\prod_{i \in J} p_i^{v_i}$ divise donc l'ordre de g. Si d est le quotient, il suffit de prendre g^d.

Lemme : Soit $K \in Cl(G)$, $g \in K$, $\boldsymbol{N} = \{h \in G \mid < hgh^{-1} > = < g > \}$ le normalisateur de $< g >$ et $\boldsymbol{C} = \{h \in G \mid hgh^{-1} = g\}$ le centralisateur de g. Si $o = ord(g)$, les groupes N/C et $Gal\big(\mathbb{Q}_o/\mathbb{Q}(K)\big)$ sont isomorphes et ont donc notamment le même cardinal.

Preuve : Pour tout $h \in N$, d'après le lemme 2.4, il existe un unique $k \in [|1; o|]$, premier avec o, tel que $hgh^{-1} = g^k$. Ceci permet de définir $f : \begin{cases} N & \longrightarrow & (\mathbb{Z}/o\mathbb{Z})^\times \\ h & \longmapsto & \overline{k} \end{cases}$.
Si $hgh^{-1} = g^k$ et $h'gh'^{-1} = g^{k'}$, alors $hh'g(hh')^{-1} = hg^{k'}h^{-1} = g^{kk'}$ donc f est un morphisme de groupes. De plus, $h \in Ker(f)$ si et seulement si $hgh^{-1} = g : C$ est donc le noyau de f.

Par passage au quotient et en composant avec l'isomorphisme du lemme 2.2, on obtient un morphisme injectif $\phi : \begin{cases} N/C & \longrightarrow & Gal\big(\mathbb{Q}_o/\mathbb{Q}\big) \\ \overline{h} & \longmapsto & \sigma_k \end{cases}$. Soit $\sigma_k \in Gal\big(\mathbb{Q}_o/\mathbb{Q}\big)$. On a les équivalences suivantes :

σ_k est dans l'image de $\phi \Leftrightarrow <g^k> = <g> \Leftrightarrow g^k$ est conjugué à g
$\Leftrightarrow \forall \chi \in Irr(G),\ \chi(g^k) = \chi(g) \Leftrightarrow \forall \chi \in Irr(G),\ \sigma_k\big(\chi(g)\big) = \chi(g)$
$\Leftrightarrow \mathbb{Q}(K)$ est fixé par $\sigma_k \Leftrightarrow \sigma_k \in Gal\big(\mathbb{Q}_o/\mathbb{Q}(K)\big)$.

Ainsi, l'image de ϕ est $Gal\big(\mathbb{Q}_o/\mathbb{Q}(K)\big)$, ce qui donne l'isomorphisme souhaité.

Théorème 6.8 : Soit $p \in \mathbb{N}$ premier, H un p-Sylow de G, g appartenant au centre de H et K sa classe de conjugaison. Si K n'est pas rationnelle, le plus petit $r \in \mathbb{N}$ tel que $\mathbb{Q}(K) \subset \mathbb{Q}_{p^r}$ vérifie $ord(g) = p^r$.

Preuve : On reprend les notations du lemme précédent : $o = ord(g) = p^r$, N est le normalisateur de $<g>$ et C le centralisateur de g.
Comme K n'est pas rationnelle et par le raisonnement du lemme 2.1, $\mathbb{Q}_p \subset \mathbb{Q}(K) \subset \mathbb{Q}_o$. Si $r = 1$, le résultat est donc direct. Sinon, supposons par l'absurde que r n'est pas minimal. Dans ce cas, $\mathbb{Q}(K) \subset \mathbb{Q}_{p^{r-1}}$.
Comme $r \geq 2$, on aurait $[\mathbb{Q}_{p^r} : \mathbb{Q}(K)] = [\mathbb{Q}_{p^r} : \mathbb{Q}_{p^{r-1}}] \times [\mathbb{Q}_{p^{r-1}} : \mathbb{Q}(K)] = p \times [\mathbb{Q}_{p^{r-1}} : \mathbb{Q}(K)] \in p\mathbb{Z}$.
Or, par le lemme précédent, $[\mathbb{Q}_{p^r} : \mathbb{Q}(K)] = \big|Gal\big(\mathbb{Q}_o/\mathbb{Q}(K)\big)\big| = \big|N/C\big|$. Ainsi, p divise $\big|N/C\big|$ et donc a fortiori $\big|G/C\big| = \frac{|G|}{|C|}$. Pourtant, comme g est dans le centre de H, son centralisateur C contient forcément H. Ainsi, ce dernier est un sous-groupe de C donc $|H|$ divise $|C|$. Mais H est un p-Sylow donc $|H| = p^v$, où v est la valuation p-adique de $|G|$. Finalement, p ne peut pas diviser $\big|G/C\big|$, ce qui donne la contradiction recherchée.

7 Bibiographie

Cet article repose très largement sur le livre *Character Theory and the McKay Conjecture*, de **Gabriel Navarro**, publié par Cambridge University Press en 2018.

Certains éléments ont été empruntés aux livres *Représentations Linéaires des Groupes Finis*, de **Jean-Pierre Serre**, publié en 1998 par Hermann et *Character Theory of Finite Groups*, de **Martin Isaacs**, publié en 1976 par Academic Press.

Les résultats de la théorie des caractères utilisés ici sont présentés dans le livre de Jean-Pierre Serre. Pour ce qui est de la théorie de Galois, on peut se référer au chapitre 4 du livre *Algèbre : le Grand Combat*, de **Grégory Berhuy**, publié en 2020 par Calvage et Mounet. Et enfin, les résultats admis de la théorie des modules se trouvent dans le cours d'introduction *Modules Over a Ring*, enseigné en 2021 par **Nicolas Mascot** et dont les notes de cours sont téléchargeables *ici*.