

SÉMINAIRE N. BOURBAKI

JEAN-PIERRE SERRE

Le théorème de Brauer sur les caractères

Séminaire N. Bourbaki, 1956, exp. n° 111, p. 107-113

<http://www.numdam.org/item?id=SB_1954-1956__3__107_0>

© Association des collaborateurs de Nicolas Bourbaki, 1956, tous droits réservés.

L'accès aux archives du séminaire Bourbaki (<http://www.bourbaki.ens.fr/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

LE THÉOREME DE BRAUER SUR LES CARACTÈRES

par Jean-Pierre SERRE

La démonstration du théorème de Brauer que nous allons exposer est une démonstration de P. ROQUETTE [5], simplifiée par R. BRAUER et J. TATE [4]. La démonstration originale de R. BRAUER [3] était sensiblement plus compliquée.

1. Notations.

Soit G un groupe fini d'ordre n . On notera R l'anneau $\mathbb{Z}[\varepsilon]$ engendré sur $\mathbb{Z}$ par une racine primitive n -ième de l'unité ; on a donc

$$\mathbb{Z} \subset R \subset \mathbb{C}$$

De plus, R admet une base sur $\mathbb{Z}$ formée de $1, \varepsilon, \varepsilon^2, \dots, \varepsilon^N$ (N convenable) ; donc $R/\mathbb{Z}$ est un groupe libre.

On notera $X_{\mathbb{C}}(G)$, ou simplement $X_{\mathbb{C}}$, l'algèbre des fonctions à valeurs complexes sur G , constantes sur les classes de G ; on sait que $X_{\mathbb{C}}$ admet pour base les caractères irréductibles $\chi_1, \dots, \chi_c$ de G (c'est-à-dire les fonctions $g \rightarrow \text{Tr}(U_g)$, où $g \rightarrow U_g$ est une représentation linéaire irréductible de G). On désignera par $X(G)$, ou simplement X , l'ensemble des combinaisons linéaires à coefficients dans $\mathbb{Z}$ des χ_i : c'est l'anneau des caractères de G ; de même, $X_R(G)$, ou simplement X_R , désignera l'ensemble des combinaisons linéaires à coefficients dans R des χ_i . On a donc :

$$(1) \quad X_{\mathbb{C}} = X \otimes_{\mathbb{Z}} \mathbb{C} \quad , \quad X_R = X \otimes_{\mathbb{Z}} R$$

Si θ est un élément de X_R , on a $\theta(g) \in R$ pour tout $g \in G$; en effet, il suffit de le voir lorsque θ est un caractère irréductible, i.e. lorsque $\theta(g) = \text{Tr}(U_g)$, et dans ce cas cela résulte du fait que toutes les valeurs propres de U_g sont des racines n -ièmes de l'unité (puisque $(U_g)^n = 1$). On peut donc considérer les éléments $\theta \in X_R$ comme des fonctions sur G , constantes sur les classes, et à valeurs dans R .

Si H est un sous-groupe de G , l'opération de restriction définit un homomorphisme $\rho_H^G : X(G) \rightarrow X(H)$, d'où $\rho_H^G : X_R(G) \rightarrow X_R(H)$. En sens inverse, si $\psi \in X(H)$, on définira un élément $\tau_G^H(\psi) \in X(G)$, par la formule

$$(2) \quad \tau_G^H(\psi)(g) = \frac{1}{(H:1)} \sum_{x \in G} \psi(x.g.x^{-1}) \quad ,$$

en convenant que $\psi(x.g.x^{-1}) = 0$ si $x.g.x^{-1} \notin H$.

Si $\psi(h) = \text{Tr}(U_h)$, où $h \rightarrow U_h$ est une représentation linéaire de H dans un espace vectoriel complexe E' , on vérifie tout de suite que

$\tau_G^H(\psi)(g) = \text{Tr}(V_g)$, où $g \rightarrow V_g$ est la représentation induite de la représentation $h \rightarrow U_h$. Il s'ensuit bien que, si $\psi \in X(H)$, on a $\tau_G^H(\psi) \in X(G)$.

On définit par la même formule $\tau_G^H : X_R(H) \rightarrow X_R(G)$. On notera que l'application τ_G^H n'est pas un homomorphisme ; mais on a :

$$(3) \quad \tau_G^H(\rho_H^G(\theta) \cdot \psi) = \theta \cdot \tau_G^H(\psi) \quad \text{si} \quad \theta \in X_R(G) \quad , \quad \psi \in X_R(H) \quad .$$

Si K est un sous-groupe de H , on a des formules de transitivité :

$$\rho_G^H \circ \rho_H^K = \rho_K^K \quad \text{et} \quad \tau_G^H \circ \tau_H^K = \tau_K^K \quad .$$

Dans ce qui suit, nous nous donnerons une famille H_α de sous-groupes de G , et nous désignerons par V et V_R les sous-groupes de X et X_R définis par les formules :

$$(4) \quad V = \sum_{\alpha} \tau_G^{H_\alpha}(X(H_\alpha)) \quad , \quad V_R = \sum_{\alpha} \tau_G^{H_\alpha}(X_R(H_\alpha)) \quad .$$

La formule (3) montre que V est un idéal dans X , et V_R un idéal dans X_R . D'ailleurs $V_R = V \otimes_{\mathbb{Z}} R$. Le théorème de Brauer (cf. paragraphe 3) affirme que, si tout sous-groupe "élémentaire" est contenu dans un H_α , on a $V = X$ (tout caractère est combinaison linéaire à coefficients dans $\mathbb{Z}$ de caractères induits par des caractères des H_α). Vu ce qui précède, il suffira de prouver que $V_R = X_R$, c'est-à-dire que $1 \in V_R$.

2. Résultats préliminaires.

Soit p un nombre premier fixé. Un élément $a \in G$ est dit p-régulier si son ordre est premier à p , et p-singulier si son ordre est une puissance de p . Si x est un élément quelconque de G , la considération du sous-groupe cyclique $\langle x \rangle$ engendré par x montre que x peut s'écrire de façon unique sous la forme :

$x = a.y$ où a est p -régulier, y est p -singulier, et a et y commutent.

L'élément a est appelé le facteur p-régulier de x . Deux éléments x et x' sont dits p-conjugués si leurs facteurs p -réguliers sont conjugués au sens ordinaire ; cette relation d'équivalence partage G en p-classes, qui sont évidemment des réunions de classes.

LEMME 1. - Soit θ un élément de X_R tel que $\theta(g) \in \mathbb{Z}$ pour tout $g \in G$. Alors θ est constant mod p sur toute p -classe.

Il suffit évidemment de prouver que, si a est le facteur p -régulier de x , on a $\theta(x) \equiv \theta(a) \pmod{p}$. La restriction de θ au sous-groupe cyclique $\langle x \rangle$ peut s'écrire $\theta = \sum r_j \chi_j$, avec $r_j \in \mathbb{R}$, les χ_j étant des caractères irréductibles de $\langle x \rangle$, donc multiplicatifs. Pour un entier r convenable, on a $x^{p^r} = a^{p^r}$, d'où $\chi_j(x)^{p^r} = \chi_j(a)^{p^r}$, et $\theta(x)^{p^r} \equiv \theta(a)^{p^r} \pmod{p^r}$, d'où la même congruence mod p (car $p^r \cap \mathbb{Z} = p\mathbb{Z}$), et on en tire $\theta(x) \equiv \theta(a) \pmod{p}$. C.Q.F.D.

LEMME 2. - Soient a un élément p -régulier de G , A le sous-groupe cyclique engendré par a , A' le commutant de A dans G , P un p -sous-groupe de Sylow de A' . Il existe alors un élément $\theta \in \tau_G^{A \times P}(X_R(A \times P))$ vérifiant les propriétés suivantes :

- a) $\theta(g) \in \mathbb{Z}$ pour tout $g \in G$.
- b) $\theta(g) = 0$ si g n'appartient pas à la p -classe de a .
- c) $\theta(a) = (A' : P) \not\equiv 0 \pmod{p}$.

(D'après le lemme 1, on a donc $\theta(g) \equiv (A' : P) \pmod{p}$ si g appartient à la p -classe de a).

Notons d'abord que, puisque A et P commutent et ont des ordres premiers entre eux, le sous-groupe de G engendré par A et P peut bien être identifié au produit direct $A \times P$.

Soit χ la fonction définie sur $A = \langle a \rangle$ qui vaut $(A : 1)$ en a et 0 ailleurs ; on vérifie trivialement (caractères d'un groupe cyclique !) qu'elle appartient à $X_R(A)$. La fonction composée $\psi : A \times P \rightarrow A \xrightarrow{\chi} \mathbb{Z}$ appartient donc à $X_R(A \times P)$. Je dis que $\theta = \tau_G^{A \times P}(\psi)$ vérifie les propriétés a), b), c). On a en effet :

$$\theta(g) = \frac{1}{(A \times P : 1)} \sum_{x \in G} \psi(x.g.x^{-1}) = \frac{1}{(P : 1)} M(g) ,$$

en désignant par $M(g)$ le nombre des éléments $x \in G$ tels que $x.g.x^{-1}$ soit égal à $a.y$, avec $y \in P$.

Comme $M(g)$ est toujours divisible par $(P : 1)$, la propriété a) est vérifiée ; d'autre part, on ne peut avoir $M(g) \neq 0$ que si g est p -conjugué à l'élément a , d'où la propriété b) ; enfin, si $g = a$, on ne peut avoir $x.a.x^{-1} = a.y$, avec $y \in P$ que si $y = 1$, et $M(g)$ est donc égal à $(A' : 1)$, d'où c).

3. Les théorèmes d'Artin et de Brauer.

LEMME 3. - Supposons que les sous-groupes H_α recouvrent G . Alors toute fonction sur G , constante sur chaque classe, et dont les valeurs sont des entiers divisibles par $n = (G : 1)$, appartient à V_R .

Appliquant le lemme 2 avec p premier à n , on voit qu'il existe, pour toute classe Γ de G , un élément $\theta_\Gamma \in V_R$, nul en dehors de Γ , et dont la valeur sur Γ est un entier divisant n . D'où, par combinaison linéaire, n'importe quelle fonction vérifiant les conditions du lemme.

THÉOREME 1 (ARTIN [1]). - Tout caractère de G est combinaison linéaire à coefficients rationnels de caractères induits par les caractères des sous-groupes cycliques de G .

Appliquons le lemme 3 à la famille H des sous-groupes cycliques de G ; on voit que la fonction constante égale à n appartient à V_R , d'où $nX_R \subset V_R$, d'où $nX \subset V$, ce qui démontre (en le précisant) le théorème d'Artin.

Si p est un nombre premier, nous dirons qu'un groupe H est p -élémentaire s'il est isomorphe au produit direct d'un groupe cyclique et d'un p -groupe.

LEMME 4. - Si tout sous-groupe p -élémentaire de G est contenu dans un H_α , alors, pour tout entier $r \geq 0$, il existe une fonction $\theta \in V_R$ dont les valeurs sont des entiers congrus à 1 mod p^r .

En appliquant le lemme 2, on voit que, pour toute p -classe Γ , il existe $\sigma_\Gamma \in V_R$, nul en dehors de Γ , et à valeurs entières et $\not\equiv 0 \pmod p$ sur Γ . En posant $\sigma = \sum_\Gamma \sigma_\Gamma$, on obtient un élément de V_R dont les valeurs sont partout $\not\equiv 0 \pmod p$. Si l'on pose alors :

$$\theta = \sigma \varphi(p^r), \quad \varphi \text{ désignant la fonction d'Euler, on aura bien } \theta \equiv 1 \pmod{p^r}.$$

C.Q.F.D.

THÉOREME 2. - Les hypothèses étant celles du lemme précédent, posons $n = n_0 \cdot p^r$, $(n_0, p) = 1$. La fonction constante égale à n_0 appartient à V .

Il suffit de montrer que $n_0 \in V_R$. Or, soit θ l'élément de V_R dont le lemme 4 affirme l'existence, et écrivons :

$$n_0 = n_0(1 - \theta) + n_0 \theta.$$

Comme $n_0(1 - \theta)$ prend des valeurs divisibles par $n_0 \cdot p^r = n$, on a $n_0(1 - \theta) \in V_R$, d'après le lemme 3; d'autre part, on a $n_0 \theta \in V_R$ puisque

$\theta \in V_R$; d'où $n_0 \in V_R$,

C.Q.F.D.

THÉORÈME 3 (BRAUER [3]). - Supposons que, pour tout nombre premier p , tout sous-groupe p -élémentaire de G soit contenu dans l'un des H_α . Alors tout caractère de G est combinaison linéaire, à coefficients dans $\mathbb{Z}$, de caractères induits par des caractères des H_α .

En effet, en appliquant le théorème 2 aux différents nombres premiers p , on voit que $V \cap \mathbb{Z}$ n'est contenu dans aucun $p\mathbb{Z}$, d'où $V \cap \mathbb{Z} = \mathbb{Z}$, et $1 \in V$, ce qui montre bien que $V = X$.

COROLLAIRE. - Pour qu'une fonction φ sur G appartienne à $X(G)$, il faut et il suffit que ses restrictions aux H_α appartiennent aux $X(H_\alpha)$.

En effet, d'après ce qui précède, on a :

$$1 = \sum_{\alpha} n_{\alpha} \cdot \tau_G^{H_{\alpha}}(\psi_{\alpha}), \text{ avec } \psi_{\alpha} \in X(H_{\alpha}).$$

D'où :

$$\varphi = \sum_{\alpha} n_{\alpha} \cdot \tau_G^{H_{\alpha}}(\rho_{H_{\alpha}}^G(\varphi) \cdot \psi_{\alpha}).$$

Si $\rho_{H_{\alpha}}^G(\varphi) \in X(H_{\alpha})$, le second membre appartient bien à $X(G)$, C.Q.F.D.

4. Application du théorème de Brauer.

Nous dirons qu'un caractère χ d'un groupe H est de degré 1 si la représentation correspondante de H est de degré 1 ; il faut et il suffit pour cela que χ soit un homomorphisme de H dans le groupe des racines de l'unité.

THÉORÈME 4. - Tout caractère de G est combinaison linéaire, à coefficients dans $\mathbb{Z}$, de caractères induits par des caractères de degré 1.

Vu le théorème 3, et la transitivité de l'opération d'induction, il suffit de prouver que tout caractère irréductible d'un groupe p -élémentaire est induit par un caractère de degré 1 d'un de ses sous-groupes ; or ceci est un cas particulier du théorème 6 du paragraphe 5, C.Q.F.D.

C'est sous cette forme que le théorème de Brauer est utilisé dans les applications ; en particulier, c'est de là que l'on déduit le caractère méromorphe des fonctions L de ARTIN [1] et WEIL ([7], paragraphe VI). On en tire également :

THÉORÈME 5. - Soit m le p. p. c. m. des ordres des éléments de G . Toute représentation linéaire de G est semblable à une représentation linéaire à coefficients dans le corps $K = \mathbb{Q}(\sqrt[m]{1})$ des racines m -ièmes de l'unité.

Soient ψ_i les caractères des représentations irréductibles de G par rapport à K . Il nous faut montrer que tout caractère ψ de G est une combinaison linéaire à coefficients entiers positifs des ψ_i . Or supposons seulement que l'on ait $\psi = \sum n_i \psi_i$, avec $n_i \in \mathbb{Z}$; je dis que les n_i sont alors nécessairement ≥ 0 . En effet, si par exemple $n_1 < 0$, la représentation irréductible V_1 associée à ψ_1 interviendrait (sur le corps $\mathbb{C}$) dans une somme de représentations V_j , $j \neq 1$; il existerait donc un G -homomorphisme non trivial :

$$V_1 \otimes \mathbb{C} \rightarrow \sum V_j \otimes \mathbb{C}.$$

Maïs la recherche d'un tel G -homomorphisme est un problème linéaire homogène à coefficients dans K ; il existerait donc un homomorphisme non trivial :

$V_1 \rightarrow \sum V_j$, ce qui est absurde, et démontre notre assertion.

D'autre part, on voit tout de suite que toute représentation induite par une représentation de degré 1 est semblable à une représentation à coefficients dans K ; donc son caractère est combinaison linéaire à coefficients dans $\mathbb{Z}$ des ψ_i ; d'après le théorème 4, il en est de même de tout caractère de G , et ce qui précède montre que les coefficients n_i sont positifs. C.Q.F.D.

5. Représentations linéaires d'un groupe vérifiant la propriété (MP).

Nous dirons qu'un groupe fini G vérifie la propriété (MP) s'il possède une suite de sous-groupes invariants emboîtés :

$$\{e\} = G_0 \subset G_1 \subset \dots \subset G_k = G,$$

telle que les quotients successifs G_{i+1}/G_i soient cycliques d'ordre premier. Un groupe p -élémentaire vérifie évidemment (MP) (c'est le cas, plus généralement, de tous les groupes nilpotents).

LEMME 5. - Si un groupe non abélien G vérifie (MP), il existe un sous-groupe invariant abélien H de G , non contenu dans le centre de G .

Soit C le centre de G , et soit $L = G/C$. Il est clair que L vérifie (MP) et est $\neq \{e\}$. Soit $\mathbb{Z}_p$ un sous-groupe cyclique d'ordre premier de L , invariant dans L ; l'image réciproque de ce sous-groupe dans G est le sous-groupe H cherché.

THÉOREME 6. - Toute représentation linéaire irréductible d'un groupe G vérifiant la propriété (MP) est induite par une représentation de degré 1 d'un sous-groupe de G .

Nous raisonnerons par récurrence sur l'ordre de G . On peut supposer que la représentation considérée est fidèle. Si G est abélien, le théorème est trivial. Sinon, soit H un sous-groupe abélien invariant de G , non contenu dans le centre de G . Décomposons par rapport à H l'espace E de la représentation :

$$E = \sum_{\lambda} E_{\lambda}$$

E_{λ} étant le sous-espace propre de E correspondant au caractère irréductible λ de H .

Du fait que H est invariant dans G , le groupe G permute les $E_{\lambda} \neq 0$, et les permute transitivement, puisque E est irréductible. De plus, il y a au moins deux E_{λ} qui sont $\neq 0$, car sinon H opèrerait par homothéties, et serait contenu dans le centre de G .

Soit E_0 l'un des $E_{\lambda} \neq 0$, et soit K le sous-groupe de G laissant stable E_0 ; tous les $E_{\lambda} \neq 0$ s'écrivent alors sous la forme $g.E_0$, $g \in G$, et l'on a $g.E_0 = g'.E_0$ si et seulement si $g.K = g'.K$; puisque E est somme directe des E_{λ} , il en résulte que E est isomorphe à la représentation induite de la représentation de K dans E_0 ; comme E est irréductible, cette représentation est irréductible; puisque $K \neq G$, on peut appliquer l'hypothèse de récurrence à (K, E_0) , et l'on voit que (K, E_0) est elle-même induite par une représentation de degré 1 d'un sous-groupe de K . D'où le théorème, compte tenu de la transitivité de l'opération d'induction.

(Le raisonnement ci-dessus remonte à BLICHFEIDT; cf. VAN DER WAERDEN, [6]. On peut généraliser le théorème 6 à certains groupes de Lie, cf. A. BOREL et J.-P. SERRE [2]).

BIBLIOGRAPHIE

- [1] ARTIN (E.). - Über eine neue Art von L-Reihen, Abhandl. math. Seminar Hamburg. Univ., t. 3, 1923, p. 89-108.
- [2] BOREL (Armand) et SERRE (Jean-Pierre). - Sur certains sous-groupes des groupes de Lie compacts, Comm. Math. Helv., t. 27, 1953, p. 128-139.
- [3] BRAUER (R.). - On Artin's L-series with general group-characters, Ann. of Math., t. 48, 1947, p. 502-514.
- [4] BRAUER (R.) and TATE (J.). - Elementary proof of Brauer's main theorems on characters, Ann. of Math., t. 62, 1955, p. 1-7.
- [5] ROQUETTE (P.). - Arithmetische Untersuchung des Charakterringes einer endlichen Gruppe, J. für reine und angew. Math., t. 190, 1952, p. 148-168.
- [6] VAN DER WAERDEN (B.L.). - Gruppen von linearen Transformationen. - Berlin, Springer, 1935 (Ergebnisse der Mathematik, vierter Band, 2).
- [7] WEIL (André). - Sur la théorie du corps de classes, J. math. Soc. Japan, t. 3, 1951, p. 1-35.