Séminaire Delange-Pisot-Poitou. Théorie des nombres

Gérard Rauzy

Caractères sur les groupes abéliens finis. Caractères sur les classes de restes

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 2 (1960-1961), exp. n° 3, p. 1-7

<http://www.numdam.org/item?id=SDPP_1960-1961__2__A3_0>

Séminaire DELANGE-PISOT
(Théorie des nombres)
2e année, 1960/61, n° 3

12 décembre 1960

CARACTÈRES SUR LES GROUPES ABÉLIENS FINIS
CARACTÈRES SUR LES CLASSES DE RESTES

par Gérard RAUZY

I. Groupes abéliens finis.

1. Ordre du groupe. Ordre d'un élément.

Soit $\mathcal{G}$ un groupe abélien fini noté multiplicativement, d'élément neutre E. On nomme ordre de $\mathcal{G}$ le nombre n d'éléments de $\mathcal{G}$.

Soit A un élément de $\mathcal{G}$: considérons les $n+1$ éléments $A, A^2, \ldots, A^{n+1}$; ils appartiennent tous au groupe $\mathcal{G}$, donc deux d'entre eux certainement égaux, soit par exemple : $A^h = A^k$ avec $1 \leqslant h < k \leqslant n+1$, d'où $A^{k-h} = E$ avec $1 \leqslant k-h \leqslant n$.

Soit alors ν le plus petit entier positif tel que $A^\nu = E$ $(1 \leqslant \nu \leqslant n)$. ν est nommé l'ordre de A.

L'ensemble $\{E, A, \ldots, A^{\nu-1}\}$ forme évidemment un sous-groupe cyclique d'ordre ν du groupe $\mathcal{G}$, l'ordre d'un élément divise donc l'ordre du groupe.

2. Récurrence dans les groupes abéliens finis.

Les démonstrations par récurrence sur les groupes abéliens finis s'appuient sur deux lemmes :

a. Soit $\mathcal{U}$ un groupe abélien fini $\mathcal{V}$ un sous-groupe de $\mathcal{U}$ d'index k (c'est-à-dire tel que l'ordre de $\mathcal{U}/\mathcal{V}$ soit égal à k). Si $\mathcal{U}/\mathcal{V}$ est cyclique, il existe un élément R de $\mathcal{U}$, n'appartenant pas à $\mathcal{V}$, tel que tout élément A de $\mathcal{U}$ s'écrit de manière unique sous la forme : $A = R^h W$ avec $W \in \mathcal{V}$ et h entier mod k.

En effet $\mathcal{U}/\mathcal{V}$ est cyclique, il existe donc $r \in \mathcal{U}/\mathcal{V}$ tel que tout élément a de $\mathcal{U}/\mathcal{V}$ s'écrive de manière unique sous la forme : $a = r^h$, h entier mod k.

Soient R un élément de r et A un élément de $\mathcal{U}$ appartenant à la classe a de $\mathcal{U}/\mathcal{V}$. Il existe un seul entier h mod k tel que $a = r^h$ c'est-à-dire tel que

$W = AR^{-h}$ soit élément de $\mathcal{V}$. On peut donc bien écrire de manière unique $A = R^h W$ avec $W \in \mathcal{V}$ et h entier mod k.

b. Si $\mathcal{U}$ est un groupe abélien fini, il existe une suite finie $\mathcal{U}_0 \subseteq \mathcal{U}_1 \ldots \subseteq \mathcal{U}_s$ de sous-groupes de $\mathcal{U}$ tels que $\mathcal{U}_0 = \{E\}$, $\mathcal{U}_s = \mathcal{U}$ et tels que $\mathcal{U}_i/\mathcal{U}_{i-1}$ soit cyclique quel que soit $i = 1, 2, \ldots, s$.

Soit n l'ordre de $\mathcal{U}$. Si $n = 1$, il suffit de prendre $s = 0$, $\mathcal{U}_0 = \mathcal{U} = \{E\}$. Si $n > 1$, il existe un élément R_1 de $\mathcal{U}$ différent de $\mathcal{U}$, Soit ν_1 l'ordre de R_1. Nous prendrons $\mathcal{U}_0 = \{E\}$, $\mathcal{U}_1 = \{E, R_1, \ldots, R_1^{\nu_1 - 1}\}$. $\mathcal{U}_1/\mathcal{U}_0$ est évidemment cyclique ; $\mathcal{U}_1$ a au moins deux éléments distincts puisque $R_1 \neq E$. Si $\mathcal{U}_1 = \mathcal{U}$ nous prenons $s = 1$. Sinon nous pouvons continuer en prenant $R_2 \in \mathcal{U}$, $R_2 \notin \mathcal{U}_1$ et $\mathcal{U}_2 = \{WR_2^h ; W \in \mathcal{U}_1, h \text{ entier mod } \nu_2\}$.

L'ordre de chacun de ces sous-groupes augmentant à chaque fois, le processus s'arrêtera pour un $s \leqslant n - 1$, tel que $\mathcal{U}_s = \mathcal{U}$.

3. Décomposition en produit.

De ce qui précède résulte que l'on peut écrire tout élément A de $\mathcal{U}$, de manière unique sous la forme

$$A = \prod_1^s W_i^{\alpha_i} \begin{cases} W_i \in \mathcal{U}_i, \quad W_i \notin \mathcal{U}_{i-1} \\ \alpha_i \text{ entier mod } n_i \text{ (index de } \mathcal{U}_{i-1} \text{ dans } \mathcal{U}_i) \\ \prod n_i = n \end{cases}.$$

Le groupe $\mathcal{U}$ est donc un produit direct de groupes cycliques.

II. Caractères : définition et existence.

1. DÉFINITION. - On appelle caractère sur le groupe abélien $\mathcal{U}$ d'ordre n, une fonction χ définie sur ce groupe à valeurs réelles ou complexes, telle que $\chi(AB) = \chi(A)\,\chi(B)$ et non partout nulle.

Soit alors $A \in \mathcal{U}$ tel que $\chi(A) \neq 0$; si ν est l'ordre de A, ν divise n donc $A^n = E$. Donc $\chi(E) = \chi(A^n) = (\chi(A))^n$ est différent de 0. Comme $\chi(E) = \chi(E \times E) = (\chi(E))^2$, il en résulte que $\chi(E) = 1$ et que $\chi(A)$ est une racine n-ième de l'unité quel que soit $A \in \mathcal{U}$. En particulier $\chi(A) \neq 0$ quel que soit A.

2. Groupe des caractères sur $\mathcal{U}$.

La fonction ε telle que $\varepsilon(A) = 1$ quel que soit $A \in \mathcal{U}$, est évidemment un caractère sur $\mathcal{U}$. Si χ est un caractère, la fonction $\chi^{-1} = \overline{\chi}$ telle que, quel que soit A,

$$\chi^{-1}(A) = (\chi(A))^{-1} = \overline{\chi(A)} = \chi(A^{-1})$$

est également un caractère. Si χ et χ' sont des caractères, la fonction $\chi\chi'$ telle que $\chi\chi'(A) = \chi(A)\,\chi'(A)$ est un caractère et $\chi\chi' = \chi'\chi$, $\chi\chi^{-1} = \varepsilon$.

Les caractères forment donc un groupe $\mathfrak{X}$ abélien d'élément unité ε que l'on nommera le caractère principal.

On nomme caractères quadratiques ou réels les caractères tels que $\chi = \overline{\chi}$, soit $\chi^2 = \varepsilon$.

3. Le groupe $\mathfrak{X}$ est d'ordre n.

Montrons-le par récurrence : d'après le lemme (b) de I, paragraphe 2, il suffit de montrer que si $\mathcal{V}'$ est un sous-groupe d'index k de $\mathcal{V}$, un caractère de $\mathcal{V}'$ peut se prolonger exactement de k manières distinctes sur $\mathcal{V}$ (deux caractères distincts de $\mathcal{V}'$ donnant nécessairement des prolongements distincts, puisque distincts sur la restriction à $\mathcal{V}'$).

Or il existe $R \in \mathcal{V}$, $R \notin \mathcal{V}'$ tel que tout $A \in \mathcal{V}$ s'écrit de manière unique $A = R^h W$ avec $W \in \mathcal{V}'$, h entier mod k.

Soient χ un caractère de $\mathcal{V}'$, ψ un caractère de $\mathcal{V}$ prolongeant χ, c'est-à-dire tel que :

$$\psi(A) = \chi(A) \qquad \text{pour tout } A \in \mathcal{V}' \ .$$

R^k est nécessairement un élément de $\mathcal{V}'$, donc $\psi(R)$ est nécessairement une racine k-ième de $\chi(R^k)$. Réciproquement, si ζ est une telle racine pour tout $A = R^h W$, on posera $\psi(A) = \zeta^h \chi(W)$.

Comme $\zeta \neq \zeta'$ entraîne $\psi(R) = \zeta \neq \psi'(R) = \zeta'$, on voit que, à tout caractère χ de $\mathcal{V}'$, correspondent exactement k caractères distincts de $\mathcal{V}$.

La propriété est bien montrée puisque la restriction à $\mathcal{V}'$ d'un caractère de $\mathcal{V}$ est bien un caractère de $\mathcal{V}'$.

III. Relations entre les caractères.

1. Soit B un élément de $\mathcal{U}$: quand A décrit $\mathcal{U}$, le produit AB décrit $\mathcal{U}$, les deux sommes $S_\chi = \sum_A \chi(A)$ et $S_\chi(B) = \sum_A \chi(AB)$ sont donc égales. Or $S_\chi(B) = \chi(B)\, S_\chi$. Si $\chi \neq \varepsilon$, il existe B tel que $\chi(B) \neq 1$, donc dans ce cas $S_\chi = 0$. Evidemment, si $\chi = \varepsilon$, $S_\varepsilon = \sum_A 1 = n$.

2. Donc $\begin{cases} S_\chi = 0 & \text{si } \chi \neq \varepsilon \\ S_\chi = n & \text{si } \chi = \varepsilon \end{cases}$

il en résulte que :

$$S_{\chi\psi^{-1}} = S_{\chi\overline{\psi}} = \sum_A \chi(A)\,\overline{\psi(A)} = \begin{cases} 0 & \text{si } \chi \neq \psi \\ n & \text{si } \chi = \psi \end{cases} .$$

3. Ordonnons en les indiçant de A à n les éléments $A_1, \ldots, A_n$ de $\mathcal{U}$ et les éléments $\chi_1, \ldots, \chi_n$ de $\mathfrak{X}$. Considérons la matrice

$$C = [c_{ij}], \qquad \begin{matrix} i \text{ indice des lignes} & (i = 1, \ldots, n) \\ j \text{ indice des colonnes} & (j = 1, \ldots, n) \end{matrix}$$

où $c_{ij} = \chi_i(A_j)$.

Les égalités précédentes s'écrivent alors : $C \times {}^t\overline{C} = n\mathfrak{I}$, où $\mathfrak{I}$ est la matrice unité. Ceci prouve que C est inversible et que : $C^{-1} = \frac{1}{n}\,{}^t\overline{C}$.

Il en résulte de manière générale que les deux systèmes d'équations :

$$\sum_A \chi(A)\, x_A = y_\chi \qquad \text{et} \qquad \frac{1}{n}\sum_\chi \overline{\chi(A)}\, y_\chi = x_A$$

où x_A $(A \in \mathcal{U})$ et y_χ $(\chi \in \mathfrak{X})$ sont des variables, sont équivalents.

Il en résulte en particulier les formules précédemment établies, c'est-à-dire

$$\sum_\chi \chi(A) = \begin{cases} 0 & \text{si } A \neq E \\ n & \text{si } A = E \end{cases} .$$

Nous allons maintenant préciser cette notion de dualité.

IV. Principe de dualité.

Soit $\mathfrak{X}$ le groupe du caractère de $\mathfrak{U}$. Alors le groupe $\mathfrak{K}$ des caractères de $\mathfrak{X}$ est isomorphe au groupe $\mathfrak{U}$.

A tout élément A de $\mathfrak{U}$ faisons correspondre la fonction K_A définie sur $\mathfrak{X}$ à valeurs réelles ou complexes par : $K_A(\chi) = \chi(A)$.

On voit sans peine que K_A est un caractère sur $\mathfrak{X}$, et que $K_A K_B = K_{AB}$.

En outre, si $A \neq B$, $AB^{-1} \neq E$, donc, comme $\sum_{\chi} \chi(AB^{-1}) = 0$, d'après III, paragraphe 3, il existe χ, tel que $\chi(AB^{-1}) \neq 1$; on a donc $\chi(A) \neq \chi(B)$, soit enfin $K_A(\chi) \neq K_B(\chi)$. Deux éléments A et B distincts donnent deux caractères K_A et K_B distincts. L'ordre de $\mathfrak{K}$ étant égal à l'ordre de $\mathfrak{U}$, nous avons bien mis en évidence un isomorphisme $A \leftrightarrow K_A$ entre les groupes $\mathfrak{U}$ et $\mathfrak{K}$.

V. Caractères sur les classes de restes.

1. Nous noterons $\mathfrak{S}_m$ le groupe multiplicatif des classes de restes modulo m, premiers avec m (où m est un entier positif). L'ordre n de ce groupe est égal à $\varphi(m)$ où φ est la fonction d'Euler.

2. Caractères modulo m.

A tout caractère χ sur le groupe $\mathfrak{S}_m$, nous associons une fonction χ définie sur l'ensemble des entiers premiers avec m, que nous nommons caractère mod m, de la manière suivante : soit a un entier tel que $(a, m) = 1$; a appartient à une classe de reste $A \in \mathfrak{S}_m$; nous posons alors $\chi(a) = \chi(A)$.

3. PROPRIÉTÉS. - Il est évident alors que χ est un caractère modulo m, si et seulement si

$$\begin{cases} \chi(a)\,\chi(b) = \chi(ab) \\ \chi(a) = 1 \quad \text{si} \quad a \equiv 1(m) \end{cases}$$

ce qui entraîne de manière générale $\chi(a) = \chi(a')$ si $a \equiv a'(m)$.

VI. Conducteur d'un caractère mod m.

1. "Erklärungsmodul" et prolongement.

Soit χ un caractère mod m, soit m' un entier positif. m' est dit un

"Erklärungsmodul" pour χ si $\begin{cases} a \equiv 1 \pmod{m'} \text{ entraîne } \chi(a) = 1 \\ (a, m) = 1 \end{cases}$.

m est évidemment un Erklärungsmodul pour χ.

Soit χ un caractère mod m, m' un Erklärungsmodul pour χ, alors on peut prolonger de manière unique χ en un caractère ψ mod m', tel que $\chi(a) = \psi(a)$ si a est premier à la fois avec m et avec m'.

a. Soit x premier avec m'. Alors il existe y premier avec m et tel que $x \equiv y(m')$. En effet, soit $m = \prod q^{\alpha_q}$ la décomposition de m en facteurs premiers, et soit $m_0 = \prod_{(q, m')=1} q^{\alpha_q}$ $(m_0, m') = 1$, donc le système de congruences $\begin{cases} y \equiv x \pmod{m'} \\ y \equiv 1 \pmod{m_0} \end{cases}$ a une solution y. Il suffit de montrer que y est premier avec m ; or si p premier divise m, comme $m = m_0 \prod_{q/m'} q^{\alpha_q}$, p divise ou bien m_0 ou bien $\prod_{q/m'} q^{\alpha_q}$ donc a fortiori m'. Mais si p divise m_0, comme $y \equiv 1 \pmod{m_0}$, p ne divise pas y, et de même si p divise m', comme $(x, m') = 1$, p ne divise pas x, donc non plus y puisque $y \equiv x \pmod{m'}$.

b. Si y' est aussi un nombre premier avec m et tel que $x \equiv y' \pmod{m'}$, $\chi(y) = \chi(y')$. En effet on a alors : $x \equiv y \equiv y' \pmod{m'}$. Or x étant premier à m', il existe c tel que $cx \equiv 1 (m')$. En appliquant le lemme précédent à c qui est évidemment premier avec m', nous en déduisons qu'il existe d premier avec m et tel que $d \equiv c \pmod{m'}$. On a donc : $dy \equiv dy' \equiv cx \equiv 1 \pmod{m'}$, donc $\chi(dy) = \chi(dy') = 1$, d'où $\chi(y) = \chi(y')$.

c. Pour chaque x premier avec m' nous pouvons donc définir $\psi(x) = \chi(y)$ où y est l'un des nombres congrus à x mod m' et premiers avec m.

On a évidemment $\psi(a) = \chi(a)$ si a est premier à la fois avec m et m'.

D'autre part si, à x premier avec m', nous associons selon (a), y, et si, à x' premier avec m' nous associons y', à xx' nous pourrons associer yy', donc $\psi(xx') = \psi(x)\,\psi(x')$. Enfin, si $x \equiv 1 \pmod{m'}$, alors $y \equiv 1 \pmod{m'}$, donc $\chi(y) = 1$, donc $\psi(x) = 1$. ψ est bien un caractère mod m'.

2. Si m est un Erklärungsmodul pour χ, alors λm est aussi un Erklärungsmodul quel que soit λ entier positif : c'est évident.

3. Si m_1 et m_2 sont deux Erklärungsmoduln pour χ, alors leur p. g. c. d.

(m_1 , m_2) est aussi un Erklärungsmodul pour χ .

En effet, soient

$$d = (m_1 , m_2)$$
$$\pi = [m_1 , m_2] \qquad (\pi \text{ p. p. c. m. de } m_1 , m_2) \quad .$$

D'après les paragraphes (1) et (2) nous pouvons considérer χ comme un caractère mod π pour lequel m_1 et m_2 sont des Erklärungsmoduln. Soient alors deux nombres a_1 et a_2 premiers avec π tels que $a_1 \equiv a_2(d)$. Alors, il existe a tel que

$$(a , \pi)=1 \quad a \equiv a_1(m_1)$$
$$a \equiv a_2(m_2) \quad .$$

Par suite $\chi(a_1) = \chi(a)$ puisque m_1 est Erklärungsmodul, et de même $\chi(a_2) = \chi(a)$. Donc $a_1 \equiv a_2(d)$ entraîne $\chi(a_1) = \chi(a_2)$. En particulier $\chi(a) = 1$ si $a \equiv 1$ (d) .

4. Tous les Erklärungsmoduln de χ sont les multiples d'un même Erklärungsmodul $\rho(\chi)$ que l'on nomme conducteur de χ .

Considérons l'ensemble $\mathfrak{M}$ des Erklärungsmodul de χ . Soit $\rho(\chi)$ le plus petit d'entre eux. Alors si $m \in \mathfrak{M}$, $(m , \rho(\chi))$ est un Erklärungsmodul. Or $(m , f(\chi)) \leqslant f(\chi)$ donc $(m , \rho(\chi)) = \rho(\chi)$, m est multiple de $f(\chi)$.

5. Soient χ un caractère, $\rho(\chi)$ son conducteurs : nous nommerons caractère propre la fonction χ égale à 0 pour tout a non premier avec $\rho(\chi)$, à la valeur obtenue en prolongement χ pour l'Erklärungsmodul $\rho(\chi)$ pour tout a premier avec $\rho(\chi)$.

6. Soit $m = m_1 m_2 \dots m_r$ où $(m_i , m_j) = 1$ si $i \neq j$. Alors, le groupe des caractères modulo m est le produit direct des groupes des caractères mod m_i , c'est-à-dire que χ caractère modulo m s'écrit de manière unique

$$\chi = \prod_{i=1}^{r} \chi_i \quad \text{où } \chi_i \text{ est un caractère mod } m_i \text{ . En outre } \rho(\chi) = \rho(\chi_1) \dots \rho(\chi_r) \text{ .}$$

C'est évident car tout a premier avec m s'écrit de façon unique $a = \prod a_i$ où $(a_i , m_i) = 1$.