Sorbonne Université
Théorie des Nombres 2 (MU4MA034)
Mars–Mai 2021.

Séance 10, 9 avril 2021

- Si a et b sont des entiers, $(a \mid b)$ désigne le symbole de Kronecker associé à eux.
- Si A est un groupe abstrait, $\mathbb{X}(A)$ note le groupe des caractères linéaires de A, c'est à dire, de morphismes de groupe $A \to \mathbb{C}^\times$.
- Une fonction $f : \mathbb{Z} \to \mathbb{C}$ est totalement multiplicative si $f(mn) = f(m)f(n)$ pour tous $m, n \in \mathbb{Z}$.
- Pour chaque entier $d > 0$, on désigne par $\mathbb{1}_d$ la fonction $\mathbb{Z} \to \mathbb{C}$ qui vaut 1 sur les entiers premiers avec d et zéro ailleurs.

Exercice 1. Dans cet exercice, on fera appel aux caractères de Dirichlet décrits à l'Exercice 3 de la dernière séance :

$$\widetilde{\psi}(k) = \begin{cases} 0, & \text{si } k \text{ est pair,} \\ 1, & \text{si } k \equiv 1\ (4), \\ -1, & \text{si } k \equiv 3\ (4), \end{cases} \qquad \widetilde{\lambda}(k) = \begin{cases} 0, & \text{si } k \text{ est pair,} \\ 1, & \text{si } k \equiv 1, 5\ (8), \\ -1, & \text{si } k \equiv 3, 7\ (8), \end{cases}$$

$$\widetilde{\mu}(k) = \begin{cases} 0, & \text{si } k \text{ est pair,} \\ 1, & \text{si } k \equiv 1, 3\ (8), \\ -1, & \text{si } k \equiv 5, 7\ (8), \end{cases} \qquad \widetilde{\nu}(k) = \begin{cases} 0, & \text{si } k \text{ est pair,} \\ 1, & \text{si } k \equiv \pm 1\ (8), \\ -1, & \text{si } k \equiv \pm 3\ (8). \end{cases}$$

(On note que $\widetilde{\psi} = \widetilde{\lambda}$.)

1/ Exprimer les symboles de Kronecker suivants à l'aides des caractères de Dirichlet précédents.

$$(* \mid 2), \quad (2 \mid *), \quad (4 \mid *), \quad (-4 \mid *), \quad (8 \mid *), \quad (-8 \mid *).$$

Correction. Étude de $(* \mid 2)$.— Par définition, $\widetilde{\nu} = (* \mid 2)$.

Étude de $(2 \mid *)$.— Si p est un nombre premier impair, alors, d'après un exercice de la première feuille de TDs, on a

$$(2 \mid p) = \begin{cases} 1, & \text{si } p \equiv \pm 1\ (8), \\ -1, & \text{si } p \equiv \pm 3\ (8). \end{cases}$$

Puis, $(2 \mid n) = 0$ si et seulement si n est pair. Il suit que $(2 \mid *) = \widetilde{\nu}$.

Étude de $(4 \mid *)$.— On note que $(4 \mid n) = 0$ si n est pair et $(4 \mid p) = 1$ pour n'importe quel premier impair p. Donc, $(4 \mid *)$ n'est rien d'autre que le caractère $\mathbb{1}_2 \in X_2$.

Étude de $(-4 \mid *)$.—On note que $(-4 \mid n) = 0$ si n est pair et, pour chaque premier impair p, $(-4 \mid p) = (-1 \mid p)$. Par le supplément de la réciprocité quadratique on a

$$(-1 \mid p) = \begin{cases} 1, & \text{si } p \equiv 1 \ (4), \\ -1, & \text{si } p \equiv 3 \ (4). \end{cases}$$

Il suit que $(-4 \mid k) = \widetilde{\psi}(k)$ sur les nombres premiers. De plus, $(-4 \mid -1) = -1$ et donc, $(-4 \mid *) = \widetilde{\psi} = \widetilde{\lambda}$.

Étude de $(8 \mid *)$.— On note que $(8 \mid *)$ est nul sur les pairs. Ensuite, si p est un premier impair, alors $(8 \mid p) = (2 \mid p)$ car le symbole de Legendre est totalement multiplicatif. Donc $(8 \mid *) = \widetilde{\nu}$, dans les notations de l'exercice 3.

Étude de $(-8 \mid *)$.— On note que $(-8 \mid *)$ est nul sur les pairs. Ensuite, si p est un premier impair, alors $(-8 \mid p) = (-1 \mid p)(2 \mid p)$. Donc $(-8 \mid p) = \widetilde{\lambda}(p)\widetilde{\nu}(p) = \widetilde{\mu}(p)$, d'après les questions précédentes. Puisque $(-8 \mid m) = \widetilde{\mu}(m)$ pour m pair, et $(-8 \mid -1) = -1 = \widetilde{\mu}(-1)$, on déduit $\widetilde{\mu} = (-8 \mid *)$. □

2/ On souhaite étudier $(3 \mid *)$ et constater qu'il n'est pas un caractère de Dirichlet.

a/ Calculer $(3 \mid n)$ pour $n \in \{1, \dots, 7\}$ en utilisant la réciprocité quadratique pour le symbole de Jacobi. Constater que $(3 \mid *)$ *n'est pas un caractère de Dirichlet modulo 3.*

Correction. Si n est impair, la réciprocité quadratique pour le symbole de Jacobi (vue en TdN1) dit que

$$(3 \mid n) = (-1)^{(n-1)/2}(n \mid 3)$$

et donc

	1	2	3	4	5	6	7
$(3 \mid *)$	1	-1	0	1	-1	0	-1

Il suit que $(3 \mid *)$ n'est pas 3-périodique. □

b/ Montrer que $(3 \mid 6k+1) = (-1)^k$. Utiliser ce fait pour prouver que si $q > 0$ est une période de $(3 \mid *)$, alors $6 \mid q$. Puis, à partir de $(3 \mid 2^l) = (3 \mid 2^l + q)$, déduire que

$$2^l \cdot 6 \mid q \quad \Rightarrow \quad 2^{l+1} \cdot 6 \mid q.$$

Conclure que $(3 \mid *)$ n'est pas périodique et donc *n'est pas un caractère de Dirichlet.* (Un résultat de Allouche et Goldmakher montre que $(d \mid *)$ n'est jamais périodique si $d \equiv 3$ (4).)

Correction. La formule $(3 \mid 6k+1) = (-1)^{3k} = (-1)^k$ suit facilement de la réciprocité pour le symbole de Jacobi : $(3 \mid n) = (-1)^{(n-1)/2}(n \mid 3)$. Or, $0 = (3 \mid 0) = (3 \mid q) = 0$ et donc $3 \mid q$. En écrivant $q = 3r$, on voit que $1 = (3 \mid 1+6r) = (-1)^r \Rightarrow r$ est pair. On écrit alors $q = 2^l 6s$, avec $l \in \mathbb{N}$ et s impair. Il suit que

$$\begin{aligned}(3 \mid 2^l) &= (3 \mid 2^l + 2^l 6s) \\ &= (3 \mid 2^l)(3 \mid 1+6s) \\ &= (3 \mid 2^l)(-1)^s \\ &\Rightarrow 2 \mid s.\end{aligned}$$

Une contradiction. Ceci montre que q n'existe pas, et que $(3 \mid *)$ n'est pas périodique. $\square$

Exercice 2 (Périodicité du symbole de Kronecker)**.** On étudie la périodicité du symbole de Kronecker $(d \mid *)$ pour d convenable.

1/ Soit p un nombre premier $\equiv 1$ (4). Montrer que $(p \mid n) = (n \mid p)$ pour tout $n \in \mathbb{Z}$. En déduire que $(p \mid *)$ est un caractère de Dirichlet modulo p.

Correction. On sait que $(p \mid *)$ et $(* \mid p)$ sont complètement multiplicatives ; ceci étant, il suffit de vérifier que $(p \mid *)$ et $(* \mid p)$ coïncident sur les premiers impairs, sur 2, et sur -1.

Si n est un premier impair, alors $(p \mid n)$ est le symbole de Legendre et la réciprocité quadratique donne $(p \mid n) = (n \mid p)$. Ensuite, en faisant appel à un exercice précédent de ces TDs (ou au cours de TdN1) on sait que

$$(2 \mid p) = \begin{cases} +1, & p \equiv \pm 1 \ (8), \\ -1, & p \equiv \pm 3 \ (8). \end{cases}$$

Donc $(p \mid 2) = (2 \mid p)$. Finalement, si $n = -1$ alors $(p \mid -1) = 1$ et $(-1 \mid p) = 1$ (par le supplément de la réciprocité quadratique). $\square$

2/ Soit p un nombre premier $\equiv 3$ (4). Montrer que $(-p \mid n) = (n \mid p)$; en déduire que $(-p \mid *)$ est un caractère de Dirichlet modulo p.

Correction. On suit la même stratégie : Puisque $(-p \mid *)$ et $(* \mid p)$ sont complètement multiplicatives, il suffit de vérifier l'égalité pour $n = -1$, $n = 2$ et n un premier impair. On a $(-p \mid -1) = -1$, par définition, et $(-1 \mid p) = -1$ par le complément de la réciprocité quadratique allié à $p \equiv 3$ (4).

Par définition, $(-p \mid 2) = (-1 \mid 2)(p \mid 2) = (p \mid 2)$. Puis,

$$(p \mid 2) = \begin{cases} +1 & p \equiv \pm 1 \ (8), \\ -1 & p \equiv \pm 3 \ (8). \end{cases}$$

Or, mais

$$(2 \mid p) = \begin{cases} +1 & p \equiv \pm 1 \ (8), \\ -1 & p \equiv \pm 3 \ (8), \end{cases}$$

comme on a vu à lors des premières feuilles d'exercices (ou en TdN1).

Ensuite, si n et un nombre premier impair, alors la réciprocité quadratique et le fait que $p \equiv 3 \ (4)$ montrent que

$$\begin{aligned}(-p \mid n) &= (-1)^{\frac{n-1}{2}} (p \mid n) \\ &= (-1)^{\frac{n-1}{2}} (-1)^{\frac{n-1}{2} \cdot \frac{p-1}{2}} (n \mid p) \\ &= (n \mid p).\end{aligned}$$

□

3/ Soient d et e des entiers tels que $(d \mid *)$ et $(e \mid *)$ sont des caractères de Dirichlet modulo $|d|$ et $|e|$ respectivement. Prouver que $(de \mid *) = (d \mid *)(e \mid *)$. En déduire que $(de \mid *)$ est un caractère de Dirichlet modulo $|de|$.

Correction. Si p est un nombre premier impair, alors $(de \mid p) = (d \mid p)(e \mid p)$ (ceci est vrai pour le symbole de Legendre). Ensuite, comme $(* \mid 2) : \mathbb{Z} \to \mathbb{C}$ est totalement multiplicative—on sait que $(* \mid 2) = \widetilde{\nu}$, où $\nu : (\mathbb{Z}/8)^\times \to \mathbb{C}^\times$ est comme dans l'exercice 3, par exemple—on déduit que $(de \mid 2) = (d \mid 2)(e \mid 2)$. Finalement, $(d \mid -1) = \mathrm{sgn}(d)$ et $(e \mid -1) = \mathrm{sgn}(e)$. Donc $(de \mid -1) = \mathrm{sgn}(de) = (d \mid -1)(e \mid -1)$. Il suit que les fonctions totalement multiplicatives $(de \mid *)$ et $(d \mid *)(e \mid *)$ coincident sur $-1, 2$ et les premiers impairs, d'où elles coincident.

La vérification du fait que $(d \mid *)(e \mid *)$ est un caractère de Dirichlet modulo $|de|$ est simple, en vu du fait que $(d \mid *)$ et $(e \mid *)$ sont des caractères de Dirichlet. □

4/ Soit d un entier qui est $\equiv 1 \ (4)$ et qui n'a pas de facteurs carrés. Montrer que $(d \mid *)$ est un caractère de Dirichlet modulo $|d|$. Indication : Faire une récurrence sur le nombre de facteur premiers de $|d|$.

Correction. On suppose que $|d|$ est un nombre premier. Si $d > 0$, alors $(d \mid *)$ est un caractère de Dirichlet modulo d d'après la question 1. Si $d < 0$ alors $p = -d$ est un nombre premier $\equiv 3 \ (4)$ et $(-p \mid *) = (d \mid *)$ est un caractère de Dirichlet modulo $|d|$ d'après la question 2. On suppose maintenant que $|d|$ n'est pas premier. Il suit que $d = pe$ avec p un nombre premier tel que $p \nmid e$; bien évidemment, $|e|$ a moins de facteurs premiers que d.

Si $p \equiv 1 \ (4)$ alors $e \equiv 1 \ (4)$. La récurrence montre que $(p \mid *)$ et $(e \mid *)$ sont des caractères de Dirichlet. Par conséquent, $(pe \mid *)$ est caractère de Dirichlet. Si $p \equiv 3 \ (4)$

alors $(-p \mid *)$ et $(-e \mid *)$ sont des caractères de Dirichlet modulo p et $|e|$, et donc $(d \mid *)$ est caractère de Dirichlet modulo $|d|$. □

5/ Soit $d = 4m$ avec $m \equiv 3\ (4)$ sans facteurs carrés. Montrer que $(d \mid *)$ est un caractère de Dirichlet modulo $|d|$. Indication : Faire une récurrence sur le nombre de facteur premiers de $|m|$.

Correction. On suppose $m = p$, avec p nombre premier. Donc, $p \equiv 3\ (4) \Rightarrow (-p \mid *) \in X_p$. Il suit que $(d \mid *) = (-4 \mid *)(-p \mid *)$ appartient à $X_{|d|}$. On suppose $m = -p$ avec p un nombre premier $\equiv 1\ (4)$. On sait que $(p \mid *) \in X_p \Rightarrow (d \mid *) = (-4 \mid *)(p \mid *) \in X_{4|p|}$.
Soit $m = pn$, avec p un nombre premier *impair*; il est clair que $|n|$ possède moins de facteur premiers que m et par hypothèse $(n \mid *) \in X_{|n|}$. Si $p \equiv 1\ (4) \Rightarrow n \equiv 3\ (4)$ $\Rightarrow (4n \mid *) \in X_{4|n|}$ par récurrence. Donc $(4m \mid *) = (4n \mid *)(p \mid *) \in X_{4|m|}$ parce que $(p \mid *) \in X_p$.
Si $p \equiv 3\ (4) \Rightarrow n \equiv 1\ (4) \Rightarrow (-4n \mid *) \in X_{4|n|}$ par récurrence. Donc, $(d \mid *) = (-p \mid *)(-4n \mid *) \in X_{4|m|}$.

□

6/ Soit $d = 8m$ avec m un entier impair sans facteur carré. Montrer que $(d \mid *)$ est un caractère de Dirichlet modulo $|d|$.

Correction. On fait une récurrence sur le nombre de facteurs premiers de $|m|$. Si $m = p$ est un nombre premier, alors soit $(p \mid *) \in X_p$, soit $(-p \mid *) \in X_p$. Quoiqu'il en soit, $(d \mid *) = (8 \mid *)(p \mid *)$ ou $(d \mid *) = (-8 \mid *)(-p \mid *)$ et $(d \mid *) \in X_{|d|}$. Le cas général s'obtient dans les mêmes lignes. □

7/ En déduire que si d est le discriminant d'un corps quadratique, alors $(d \mid *)$ est un caractère de Dirichlet modulo $|d|$.

Exercice 3. Soient ω une racine primitive 8-ème de l'unité, K le corps de nombres $\mathbb{Q}(\omega)$ et χ_d le caractère de Dirichlet défini par le symbole de Kronecker : $\chi_d(n) = (d \mid n)$. (Ceci signifie que d est choisi pour que χ_d soit un caractère de Dirichlet.) Montrer que si $\Re s > 1$, alors

$$\zeta_K(s) = \zeta(s)L(\chi_{-4}; s)L(\chi_8; s)L(\chi_{-8}; s).$$

Correction. On note que $0 = \chi_{-4}(n) = \chi_8(n) = \chi_{-8}(n)$ si n est pair. Ensuite, si p est premier impair, alors

$$\chi_{-4}(p) = \begin{cases} 1, & \text{si } p \equiv 1, 5\ (8), \\ -1, & \text{si } p \equiv 3, 7\ (8), \end{cases}$$

$$\chi_8(p) = \begin{cases} 1 & \text{si } p \equiv 1 \ (8), \\ -1 & \text{si } p \equiv 3 \ (8), \\ -1 & \text{si } p \equiv 5 \ (8), \\ 1 & \text{si } p \equiv 7 \ (8) \end{cases}$$

et

$$\chi_{-8}(p) = \begin{cases} 1 & \text{si } p \equiv 1 \ (8), \\ 1 & \text{si } p \equiv 3 \ (8), \\ -1 & \text{si } p \equiv 5 \ (8), \\ -1 & \text{si } p \equiv 7 \ (8). \end{cases}$$

Soit p un nombre premier. On sait que si $p = 2$ alors p se ramifie totalement dans K (voir l'exercice 2 de la Séance 4 pour l'égalité $\mathfrak{O}_K = \mathbb{Z}[\omega]$, et ensuite l'exercice 3 de la Séance 6 pour déduire que p est totalement ramifié). Ensuite, si $p \equiv 1 \ (8)$, on sait que p est totalement décomposé (Séance 6, Exercice 4) : $p\mathfrak{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_4$. Puis, si $p \equiv 3, 5, 7 \ (8)$, on a vu, (même séance), que p se décompose comme produit de deux idéaux de norme p^2 car $3, 5, 7$ ont tous ordre 2 en $(\mathbb{Z}/8)^\times$. En conclusion,

$$\prod_{\mathfrak{p}|2} (1 - \mathrm{N}\mathfrak{p}^{-s})^{-1} = (1 - 2^{-s})^{-1},$$

si $p \equiv 1 \ (8)$ alors

$$\prod_{\mathfrak{p}|p} (1 - \mathrm{N}\mathfrak{p}^{-s})^{-1} = (1 - p^{-s})^{-4},$$

et si $p \equiv 3, 5, 7 \ (8)$ alors

$$\begin{aligned} \prod_{\mathfrak{p}|p} (1 - \mathrm{N}\mathfrak{p}^{-s})^{-1} &= (1 - p^{-2s})^{-2} \\ &= (1 - p^{-s})^{-2}(1 + p^{-s})^{-2}. \end{aligned}$$

Donc, la valeur de $\zeta_K(s)$ est

$$\begin{aligned}
&(1-2^{-s})^{-1} \prod_{p\equiv 1\ (8)} (1-p^{-s})^{-4} \prod_{p\equiv 3}(1-p^{-s})^{-2}(1+p^{-s})^{-2}\times \\
&\prod_{p\equiv 5}(1-p^{-s})^{-2}(1+p^{-s})^{-2} \prod_{p\equiv 7}(1-p^{-s})^{-2}(1+p^{-s})^{-2} \\
&= \zeta(s)\prod_{p\equiv 1}(1-p^{-s})^{-3} \prod_{p\equiv 3}(1-p^{-s})^{-1}(1+p^{-s})^{-2}\times \\
&\prod_{p\equiv 5}(1-p^{-s})^{-1}(1+p^{-s})^{-2}\cdot \prod_{p\equiv 7}(1-p^{-s})^{-1}(1+p^{-s})^{-2} \\
&= \zeta(s)L(\chi_{-4};s)\prod_{p\equiv 1}(1-p^{-s})^{-2} \prod_{p\equiv 3}(1-p^{-s})^{-1}(1+p^{-s})^{-1}\times \\
&\prod_{p\equiv 5}(1+p^{-s})^{-2} \prod_{p\equiv 7}(1-p^{-s})^{-1}(1+p^{-s})^{-1} \\
&= \zeta(s)L(\chi_{-4};s)L(\chi_8;s)\prod_{p\equiv 1}(1-p^{-s})^{-1} \prod_{p\equiv 3}(1-p^{-s})^{-1}\times \\
&\prod_{p\equiv 5}(1+p^{-s})^{-1} \prod_{p\equiv 7}(1+p^{-s})^{-1} \\
&= \zeta(s)L(\chi_{-4};s)L(\chi_8;s)L(\chi_{-8};s).
\end{aligned}$$

$\square$