ENS Cachan
M1 mathématiques Arithmétique - 2013-2014

Exercices - Feuille 4

Sommes de Gauß

I. Caractères

Un *caractère multiplicatif* de $\mathbb{F}_p$ est un homomorphisme de groupes multiplicatifs $\chi : \mathbb{F}_p^* \to \mathbb{C}^*$. On note $\varepsilon : a \mapsto 1$ le caractère trivial. On définit le valeur en 0 par $\chi(0) = 0$ si $\chi \neq \varepsilon$ et $\varepsilon(0) = 1$, on trouve une application (qui n'est pas un homomorphisme de groupes) $\chi : \mathbb{F}_p \to \mathbb{C}$.

1. Montrer que $\chi(1) = 1$ et que $\chi(a)$ est une racine $(p-1)$-ième de 1 pour tout $a \in \mathbb{F}_p^*$.
2. Pour tout $a \in \mathbb{F}_p^*$, montrer que $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$ où - est la conjugaison complexe. On écrit simplement χ^{-1} et $\overline{\chi}$ pour $\chi \circ (\ )^{-1}$.
3. Montrer que $\sum_{a \in \mathbb{F}_p} \chi(a) = 0$ si $\chi \neq \varepsilon$, et la somme $= p$ si $\chi = \varepsilon$.
4. Vérifier que le symbole de Legendre $\left(\frac{-}{p}\right) : a \mapsto \left(\frac{a}{p}\right)$ définit un caractère multiplicatif $\chi : \mathbb{F}_p \to \mathbb{C}$, et $\chi \neq \varepsilon$.
5. En suivant les étapes ci-dessous, montrer que le groupe des caractères $Hom(\mathbb{F}_p^*, \mathbb{C}^*)$ est un groupe cyclique d'ordre $p-1$. De plus, si $1 \neq a \in \mathbb{F}_p^*$ il existe un caractère χ tel que $\chi(a) \neq 1$.
5.1. En notant que $\mathbb{F}_p^*$ est un groupe cyclique (engendré par un certain élément g), montrer que le groupe $Hom(\mathbb{F}_p^*, \mathbb{C}^*)$ a au plus $p-1$ éléments.
5.2. Définissons $\lambda(g^k) = exp(\frac{2\pi ik}{p-1})$, c'est un caractère. Soit $n = |Hom(\mathbb{F}_p^*, \mathbb{C}^*)|$, en considérant λ, montrer que $n = p-1$ et déduire que $Hom(\mathbb{F}_p^*, \mathbb{C}^*)$ est un groupe cyclique engendré par λ.
5.3. Pour $1 \neq a \in \mathbb{F}_p^*$, vérifier que $\lambda(a) \neq 1$.
6. Pour $1 \neq a \in \mathbb{F}_p^*$, montrer que $\sum_\chi \chi(a) = 0$.
7. Supposons que $n|p-1$ et que $x^n \equiv a \pmod{p}$ n'a pas de solution. On considère le caractère $\rho = \lambda^{(p-1)/n}$. Vérifier que $\rho(g) = exp(\frac{2\pi i}{n})$ alors $\rho^n = \varepsilon$, et montrer que $\rho(a) \neq 1$.
8. Supposons que $n|p-1$. Montrer que le nombre des caractères multiplicatifs χ tels que $\chi^n = \varepsilon$ égale n.

II. Sommes de Gauß et de Jacobi

Soit ζ un racine primitive p-ième de 1. La somme suivante est bien définie pour chaque caractère multiplicatif χ et pour $a \in \mathbb{F}_p^*$

$$g_a(\chi) = \sum_{x \in \mathbb{F}_p} \chi(x)\zeta^{ax} \left(= \sum_{x \in \mathbb{F}_p^*} \chi(x)\zeta^{ax} \text{ si } \chi \neq \varepsilon \right).$$

1. Montrer que $g_a(\chi) = \overline{\chi}(a) g_1(\chi)$. Montrer que $\overline{g_1(\chi)} = \chi(-1) g_1(\overline{\chi})$.
2. Montrer que $|g_1(\chi)|^2 = p$ si $\chi \neq \varepsilon$, alors $|g_a(\chi)|^2 = p$ si $\chi \neq \varepsilon$. (allusion : faire les calculs en utilisant la définition $(p-1)|g_1(\chi)|^2 = \sum_{a \in \mathbb{F}_p^*} |g_a(\chi)|^2 = \sum g_a(\chi)\overline{g_a(\chi)} = \cdots$)
3.* Soit m un nombre entier premier à p tel que $\chi^m = \varepsilon$. Pour b un entier premier à m on définit $\sigma_b \in Gal(\mathbb{Q}(\zeta_m, \zeta_p)/\mathbb{Q})$ par $\sigma_b : \zeta_m \mapsto \zeta_m^b, \zeta_p \mapsto \zeta_p$. Montrer que $g_1(\chi)^{b-\sigma_b} := \frac{g_1(\chi)^b}{g_1(\chi)^{\sigma_b}} \in \mathbb{Q}(\zeta_m)$, en déduire que $g_1(\chi)^m \in \mathbb{Q}(\zeta_m)$. (allusion : il suffit de montrer que $Gal(Q(\zeta_m, \zeta_p)/\mathbb{Q}(\zeta_m))$ agit trivialement.)

Soient χ et λ des caractères multiplicatifs de $\mathbb{F}_p$. On définit la somme de Jacobi

$$J(\chi,\lambda)=\sum_{\substack{a+b=1\\ a,b\in\mathbb{F}_p}}\chi(a)\lambda(b)$$

4. Montrer que $J(\varepsilon,\varepsilon)=p$ et $J(\varepsilon,\chi)=0$ si $\chi\neq\varepsilon$.
5. Montrer que $J(\chi,\chi^{-1})=-\chi(-1)$ si $\chi\neq\varepsilon$.
6. Montrer que si $\chi\neq\varepsilon$, $\lambda\neq\varepsilon$, et $\chi\lambda\neq\varepsilon$ alors $J(\chi,\lambda)=\frac{g_1(\chi)g_1(\lambda)}{g_1(\chi\lambda)}$. Donc $|J(\chi,\lambda)|=\sqrt{p}$.

III. Nombre de solutions modulo p

1. Notons $N(x^n=a)$ le nombre de solutions modulo p de $x^n\equiv a \pmod p$. Supposons que $n|p-1$. En classifiant a, montrer que $N(x^n=a)=\sum_{\chi^n=\varepsilon}\chi(a)$.
2. Soit $p\equiv 1 \pmod 3$ un nombre premier. Soit $\chi\neq\varepsilon$ un caractère multiplicatif tel que $\chi^3=\varepsilon$, alors ε, χ, et $\chi^2=\bar{\chi}$ sont les trois caractères de I.8. On sait que $N(x^3+y^3=1)=\sum_{a+b=1}N(x^3=a)N(y^3=b)$. En utilisant les sommes de Jacobi, montrer que $|N(x^3+y^3=1)-p+2|\leq 2\sqrt{p}$.

Remarque. Si p est assez grand, l'équation $x^3+y^3=1$ a toujours des solutions modulo p. On a une généralisation pour toute variété algébrique définie sur un corps fini —- estimation de Lang–Weil.

IV.* Théorème de Stickelberger

On va montrer le théorème suivant, dont l'idée de la preuve est dû à Kummer.
Théorème. (Stickelberger) Soit $G\simeq(\mathbb{Z}/m\mathbb{Z})^\times$ le groupe de Galois de l'extension $K=\mathbb{Q}(\zeta_m)/\mathbb{Q}$ et soit $\sigma_a\in G$ l'élément défini par $\zeta_m\mapsto\zeta_m^a$ si $(a,m)=1$. On note

$$\theta=\frac{1}{m}\sum_{\substack{a=1\\(a,m)=1}}^{m}a\sigma_a^{-1}\in\mathbb{Q}[G].$$

Soit l un nombre premier tel que $l\equiv 1 \pmod m$, alors il est complètement décomposé dans K. Soit λ un idéal premier de K au-dessus de l. Si $\beta\in\mathbb{Z}[G]$ satisfait $\beta\theta\in\mathbb{Z}[G]$, alors $\lambda^{\beta\theta}$ est un idéal principal de $\mathcal{O}_K$.

Remarque. D'après le théorème de Čebotarev, ses idéaux λ engendrent le groupe de classes $Cl(K)$ (*cf. Algebraic number theory* de Cassels et Fröhlich, VIII Thm. 4), alors $Cl(K)$ est tué par $\beta\theta$. Il existe une généralisation du théorème où le corps de base est une extension abélienne de $\mathbb{Q}$ (sous-corps d'un corps cyclotomique - Kronecker).
(Pour la théorie des corps cyclotomiques et la théorie d'Iwasawa, voir le livre *Introduction to cyclotomic fields* de Washington. Pour use preuve complète du théorème, voir Ch. 15 et 6)

1. On choisit un générateur s du groupe cyclique $\mathbb{F}_l^*$ et définit le caractère χ par $\chi(s)=\zeta_m$. On considère la somme de Gauß

$$g(\chi)=g_1(\chi)=\sum_{b=1}^{l-1}\chi(b)\zeta_l^b\in\mathcal{O}_{\mathbb{Q}(\zeta_m,\zeta_l)}.$$

Montrer que la factorisation de l'idéal principal $(g(\chi))$ dans $\mathcal{O}_{\mathbb{Q}(\zeta_m,\zeta_l)}$ doit être de la forme

$$(g(\chi))=\prod_{\substack{a=1\\(a,m)=1}}^{m}\sigma_a^{-1}(\mathfrak{L})^{r_a}$$

où r_a est un certain nombre entier $0 \leq r_a \leq l-1$, $\mathfrak{L}$ est un idéal premier au-dessus de λ, et σ_a agit sur $\mathbb{Q}(\zeta_m, \zeta_l)$ par $\zeta_m \mapsto \zeta_m^a$, $\zeta_l \mapsto \zeta_l$. D'après II.3. $(g(\chi))^{l-1} \in \mathbb{Q}(\zeta_m)$, déduire la factorisation suivante dans $\mathcal{O}_{\mathbb{Q}(\zeta_m)}$

$$(g(\chi)^{l-1}) = \prod_{\substack{a=1 \\ (a,m)=1}}^{m} \sigma_a^{-1}(\lambda)^{r_a}.$$

Autrement dit, $\lambda^{\sum_a r_a \sigma_a^{-1}}$ est un idéal principal. On va calculer les nombres r_a.
2. Soit $\tau \in Gal(\mathbb{Q}(\zeta_m, \zeta_l)/\mathbb{Q}(\zeta_m))$ l'élément défini par $\tau : \zeta_l \mapsto \zeta_l^s$. Vérifier que $g(\chi)^\tau = \chi(s)^{-1} g(\chi)$ et $(\zeta_l^s - 1)/(\zeta_l - 1) \equiv s \pmod{\sigma_a^{-1}(\mathfrak{L})}$. Montrer que $g(\chi)/(\zeta_l - 1)^{r_a}$ est un unité dans l'anneau des entiers du corps local $\mathbb{Q}(\zeta_m, \zeta_l)_{\sigma_a^{-1}(\mathfrak{L})}$. Faire agir τ sur cet élément et déduire que

$$\frac{g(\chi)}{(\zeta_l - 1)^{r_a}} \equiv \frac{g(\chi)}{(\zeta_l - 1)^{r_a}} \frac{\chi(s)^{-1}}{s^{r_a}} \pmod{\sigma_a^{-1}(\mathfrak{L})}.$$

Déduire que $\zeta_m^a \equiv s^{-r_a} \pmod{\lambda}$.
3. En utilisant la dernière congruence, montrer qu'il existe un entier c premier à m tel que $r_a \equiv \frac{(l-1)ac}{m} \pmod{l-1}$. En déduire que $r_a = (l-1)\left\{\frac{ac}{m}\right\}$, où $q_0 = \{q\}$ est le nombre réel $0 \leq q_0 < 1$ tel que $q - q_0$ soit un entier. Vérifier que $\sum_a r_a \sigma_a^{-1} = (l-1)\sigma_c \theta$, alors $\lambda^{(l-1)\sigma_c\theta} = (g(\chi)^{l-1})$ est un idéal principal de $\mathcal{O}_{\mathbb{Q}(\zeta_m)}$.
4. Soit $\beta \in \mathbb{Z}[G]$ tel que $\beta\theta \in \mathbb{Z}[G]$. Vérifier que $\lambda^{\beta\theta(l-1)} = (\gamma^{l-1}) \subset \mathcal{O}_{\mathbb{Q}(\zeta_m)}$ avec $\gamma = g(\chi)^{\sigma_c^{-1}\beta}$.
5. Montrer le lemme suivant et déduire que $\gamma \in \mathcal{O}_{\mathbb{Q}(\zeta_m)}$, alors $\lambda^{\beta\theta} = (\gamma)$ est principal.
Lemme. Soit K un corps de nombres et $a \in K^*$. Supposons que $(a) = I^n$ pour un certain idéal (fractionnel) de K. Si $K(a^{1/n})/K$ est ramifié en un idéal premier $\mathfrak{p}$ de K, alors $\mathfrak{p}$ divise n.
(allusion : faire arguments sur le corps local $K_\mathfrak{p}$.)