UNIVERSITÉ DE PARIS 7
Année 2000-2001, DEUG 2ème année
Groupes et arithmétique (MT282)

6 Nombres de Carmichael, symboles de Legendre (et révisions)

6.1 Indicatrice de Carmichael

On rappelle qu'un entier n est dit *nombre de Carmichael* si et seulement si n n'est pas premier et si $\lambda(n)|(n-1)$, où $\lambda(n)$ désigne l'indicatrice de Carmichael de n.

1. Soit n un entier > 0 de décomposition $n = \prod_p p^{e_p}$. Donner une formule donnant $\lambda(n)$ en terme des exposants e_p.

2. Calculer $\lambda(n)$ pour $n \in \{282, 2000, 2001\}$.

3. Vérifier que les nombres suivants sont de Carmichael : 561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633, 62745, 63973, 75361, 101101.

6.2 Propriétés des nombres de Carmichael

Soit n un nombre entier > 0.

1. Soit $n = 2^k n'$ un nombre de Carmichael avec k entier > 0 et n' entier impair. Montrer que, si $k \geq 2$ on a $2|n-1$. En déduire qu'un nombre de Carmichael ne peut pas être multiple de 4. Montrer que tout nombre premier p divisant n' vérifie $(p-1)|(n-1)$. En déduire qu'un nombre de Carmichael ne peut pas être pair.

2. Soit p un nombre premier divisant n. Démontrer que si p^2 divise n, $p(p-1)$ divise $\lambda(n)$ et qu'alors n n'est pas un nombre de Carmichael. En déduire que tout nombre de Carmichael est sans facteur carré (c'est-à-dire non divisible par un carré parfait > 1).

3. Démontrer que le produit de deux nombres premiers ne peut pas être un nombre de Carmichael.

4. Supposons n de Carmichael. Soit p un nombre premier divisant n. Montrer que n/p est congru à 1 modulo $p-1$.

5. Soit $n = \prod_{i \in I} p_i$ un produit de nombres premiers distincts. Démontrer que n est de Carmichael si et seulement si $\prod_i p_i \equiv 1 \pmod{p_j - 1}$ pour tout $j \in I$.

6. Démontrer qu'il n'y pas de nombre de Carmichael < 100.

6.3 Indicatrices d'Euler et de Carmichael

1. Que valent $\phi(n)$ et $\lambda(n)$ lorsque n vaut 1, 2, 4, p^k ou $2p^k$ avec p nombre premier impair ?

2. Soit n un entier tel que $\phi(n) = \lambda(n)$. Démontrer que si n s'écrit $n = n_1 n_2$ avec n_1 et n_2 premiers entre eux, alors $\phi(n_1)$ et $\phi(n_2)$ sont premiers entre eux.

3. Démontrer que $\phi(m)$ est pair pour tout entier m distinct de 1 et 2.

4. En déduire quels sont les entiers tels que $\phi(n) = \lambda(n)$.

6.4 Exposant d'un groupe

Soit G un groupe d'élément neutre e. Lorsqu'il existe un entier n tel que $g^n = e$ $(g \in G)$ on dit que G admet un *exposant* . L'*exposant* de G est le plus petit entier $n > 0$ tel que $g^n = e$ $(g \in G)$.

1. Démontrer que si G est fini, l'exposant de G divise l'ordre de G.
2. Soit n un entier > 1. Quel est l'exposant de $(\mathbf{Z}/n\mathbf{Z})^*$?
3. Soient G_1 et G_2 deux groupes d'exposants u_1 et u_2. Démontrer que l'exposant de $G_1 \times G_2$ est PPCM(u_1, u_2).
4. Donner un exemple de groupe d'ordre infini admettant un exposant.

6.5 Résidus quadratiques généralisés

Soit n un entier > 1. Soit r un entier premier à n. On dit que c'est un *résidu quadratique modulo* n s'il existe $x \in (\mathbf{Z}/n\mathbf{Z})^*$ tel x^2 soit la classe de r modulo n.

1. Soient n et m deux entiers premiers entre eux et r un entier premier à n et m. Démontrer que r est un résidu quadratique modulo nm si et seulement si c'est un résidu quadratique modulo n et modulo m.
2. Soient p un nombre premier impair et k un entier > 1. Soit r un entier premier à p. Démontrer que r est un résidu quadratique modulo p^k si et seulement si r est un résidu quadratique modulo p.
3. Quels sont les résidus quadratiques modulo 4, modulo 8 et modulo 16 ?
4. Soient k un nombre entier > 3 et r un entier impair. Démontrer que r est un résidu quadratique modulo 2^k si et seulement si c'est un résidu quadratique modulo 8 (On rappelle que $(\mathbf{Z}/2^k\mathbf{Z})^*$ est engendré par les classes de 5 et de -1).

6.6 Résidus cubiques

Soit p un nombre premier. On dit qu'un élément $x \in (\mathbf{Z}/p\mathbf{Z})^*$ est un *cube* si et seulement si il existe $y \in (\mathbf{Z}/p\mathbf{Z})^*$ tel que $x = y^3$.

1. Démontrer que l'application $\phi : (\mathbf{Z}/p\mathbf{Z})^* \to (\mathbf{Z}/p\mathbf{Z})^*$ qui à x associe x^3 est un homomorphisme de groupes. Quel est le noyau de ϕ ?
2. Supposons que p soit congru à 2 modulo 3. Démontrer que ϕ est un isomorphisme. En déduire que tout élément de $(\mathbf{Z}/p\mathbf{Z})^*$ est un résidu cubique.
3. Supposons que p soit congru à 1 modulo 3. Soit $x \in (\mathbf{Z}/p\mathbf{Z})^*$. Démontrer que $x^{(p-1)/3}$ est une racine cubique de l'unité dans $(\mathbf{Z}/p\mathbf{Z})^*$. En déduire que x est un résidu cubique si et seulement si $x^{(p-1)/3} = 1$. Combien y a-t-il de résidus cubiques dans $(\mathbf{Z}/p\mathbf{Z})^*$?

6.7 Symbole de Legendre

Calculer les symboles de Legendre suivants : $\left(\frac{2001}{1997}\right)$, $\left(\frac{2000}{691}\right)$, $\left(\frac{2001}{691}\right)$, $\left(\frac{1000000000}{1999}\right)$, $\left(\frac{691}{1997}\right)$, $\left(\frac{2001}{65537}\right)$, $\left(\frac{2000}{65537}\right)$, $\left(\frac{282}{1997}\right)$, $\left(\frac{282}{65537}\right)$, $\left(\frac{282}{691}\right)$.

6.8 Loi de réciprocité quadratique

Soit p un nombre premier > 5.

1. Démontrer que 5 est un résidu quadratique modulo p si et seulement si p est congru à 1 ou -1 modulo 5. Démontrer que 3 est un rédidu quadratique modulo p si et seulement si p est congru à 1 ou 11 modulo 12.
2. À quelle condition 15 est-il un résidu quadratique modulo p ?

6.9 Détermination de $((p-1)/2)\,!$ modulo p

Soit p un nombre premier congru à 3 modulo 4. On a vu dans la feuille 5 que $((p-1)/2)\,!$ est congru à 1 ou -1 modulo p.

1. Démontrer qu'on a
$$((p-1)/2)\,! \equiv \Big(\frac{((p-1)/2)\,!}{p}\Big) \pmod{p}.$$
2. Démontrer qu'on a
$$\Big(\frac{((p-1)/2)\,!}{p}\Big) = \prod_{i=1}^{(p-1)/2} \Big(\frac{i}{p}\Big).$$
3. En déduire que $((p-1)/2)\,!$ est congru à $-(-1)^n$ modulo p, où n est le nombre de résidus quadratiques modulo p dans l'ensemble $\{1, 2, ..., \frac{p-1}{2}\}$.

6.10 Sommes de symboles de Legendre

Soit p un nombre premier impair. On note λ l'application $\mathbf{Z}/p\mathbf{Z} \to \mathbf{C}$ qui à x associe 1 (resp. -1) si $x \in (\mathbf{Z}/p\mathbf{Z})^*$ est (resp. n'est pas) la classe d'un résidu quadratique modulo p et telle que $\lambda(0) = 0$. En d'autres termes on a, pour $n \in \mathbf{Z}$,
$$\lambda(\bar{n}) = \Big(\frac{n}{p}\Big).$$

1. Démontrer que la restriction de λ à $(\mathbf{Z}/p\mathbf{Z})^*$ définit un homomorphisme de groupes $(\mathbf{Z}/p\mathbf{Z})^* \to \mathbf{C}^*$.
2. Démontrer que $\lambda(x^2) = 1$ ($x \in (\mathbf{Z}/p\mathbf{Z})^*$).
3. Démontrer que $\lambda(x/y) = \lambda(xy)$ (x, $y \in (\mathbf{Z}/p\mathbf{Z})^*$).
4. Démontrer que $\sum_{x \in \mathbf{Z}/p\mathbf{Z}} \lambda(x) = 0$.
5. Soient x,$y \in (\mathbf{Z}/p\mathbf{Z})$ tels que $x \neq y$ et $y \neq 0$. Démontrer que $(y+x)/(y-x)$ parcourt $(\mathbf{Z}/p\mathbf{Z}) - \{-1\}$ lorsque x parcourt $(\mathbf{Z}/p\mathbf{Z}) - \{y\}$.
6. En déduire qu'on a
$$\sum_{x \in \mathbf{Z}/p\mathbf{Z}} \lambda(y^2 - x^2) = -\lambda(-1)$$
puis que, pour tout $j \in \mathbf{Z}$ inversible modulo p, on a
$$\sum_{i=0}^{p-1} \Big(\frac{j^2 - i^2}{p}\Big) = -\Big(\frac{-1}{p}\Big).$$
7. Par la même méthode, démontrer que pour tout entier k premier à p on a
$$\sum_{i=0}^{p-1} \Big(\frac{i(k-i)}{p}\Big) = -\Big(\frac{-1}{p}\Big).$$

6.11 Somme de Gauss associée au symbole de Legendre

Soit p un nombre premier impair. Posons $\zeta = e^{\frac{2i\pi}{p}} \in \mathbf{C}$. Considérons la *somme de Gauss*

$$S = \sum_{i=0}^{p-1} \Big(\frac{i}{p}\Big)\zeta^i.$$

1. Démontrer que
$$S^2 = \sum_{i=0}^{p-1}\sum_{j=0}^{p-1} \Big(\frac{ij}{p}\Big)\zeta^{i+j},$$
puis que
$$S^2 = \sum_{i=0}^{p-1}\sum_{k=0}^{p-1} \Big(\frac{i(k-i)}{p}\Big)\zeta^{k}.$$

2. Démontrer que
$$\sum_{i=0}^{p-1} \Big(\frac{i(k-i)}{p}\Big) = (-1)^{\frac{p+1}{2}}$$
si k est un entier premier à p (on pourra utiliser la dernière formule établie dans l'exercice précédent).

3. Démontrer que $\sum_{k=0}^{p-1} \zeta^k = 0$. En déduire que
$$\sum_{k=1}^{p-1}\sum_{i=0}^{p-1} \Big(\frac{i(k-i)}{p}\Big)\zeta^{k} = (-1)^{\frac{p-1}{2}}.$$

4. En déduire que
$$S^2 = (-1)^{\frac{p-1}{2}} p.$$

5. Supposons que p soit un nombre premier congru à 1 (resp. -1) modulo 4. En déduire que $\sqrt{p}$ (resp. $\sqrt{-p}$) est une combinaison linéaire à coefficients entiers de racines p-ièmes de l'unité.

6.12 Groupe dual

Soit G un groupe fini. Considérons l'ensemble $\hat{G}$ des homomorphismes de groupes $G \to \mathbf{C}^*$. Les éléments de $\hat{G}$ sont appelés *caractères* de G.

1. Démontrer que $\hat{G}$, muni de la multiplication des homomorphismes, est un groupe commutatif.

2. Soient n un nombre entier et ζ une racine primitive n-ième de l'unité dans $\mathbf{C}$. Démontrer que si G est cyclique d'ordre n engendré par g, l'application g^* qui à g^k associe ζ^k appartient à $\hat{G}$ ($k \in \mathbf{Z}$). En déduire que $\hat{G}$ est un groupe cyclique d'ordre n engendré par g^*.

3. Soient G_1 et G_2 deux groupes finis d'éléments neutres e_1 et e_2. Soit $\chi \in (G_1 \times G_2)^*$. Démontrer que les applications $\chi_1 : G_1 \to \mathbf{C}^*$ et $\chi_2 : G_2 \to \mathbf{C}^*$ et qui à g_1 et g_2) associe $\chi(g_1, e_2)$ et $\chi(e_1, g_2)$ respectivement appartiennent à $\hat{G}$. En déduire que l'application $(G_1 \times G_2)^* \to G_1^* \times G_2^*$ qui à χ associe (χ_1, χ_2) est un isomorphisme de groupes.

4. En déduire que les groupes G et $\hat{G}$ sont isomorphes lorsque G est un produit de groupes cycliques (NB : tout groupe commutatif fini est produit de groupes cycliques).

6.13 Anneaux en groupes

Soit $(G, .)$ un groupe fini d'ordre n.

1. Soit $g_0 \in G$. Démontrer que l'application $G \to G$ qui à g associe $g_0.g$ est bijective. Soit f une fonction $G \to \mathbf{C}$. Déduire de ce qui précède qu'on a
$$\sum_{g \in G} f(g_0.g) = \sum_{g \in G} f(g).$$

2. Notons A l'ensemble des applications de G dans $\mathbf{C}$. Pour $f_1, f_2 \in A$, notons $f_1 + f_2$ et $f_1 * f_2$ les fonctions définies par
$$(f_1 + f_2)(g) = f_1(g) + f_2(g) \qquad \text{et} \qquad (f_1 * f_2)(g) = \sum_{h \in G} f_1(h) f_2(h^{-1}.g).$$
Démontrer que A muni des lois $+$ et $*$ est un anneau. Démontrer que si G est un groupe commutatif, A est un anneau commutatif.

3. Soit χ un homomorphisme de groupes $G \to \mathbf{C}^*$ (où $\mathbf{C}^*$ muni de la multiplication est un groupe). Posons $S = \sum_{g \in G} \chi(g)$. Soit $g_0 \in G$. Démontrer qu'on a $\chi(g_0)S = S$. Si χ n'est pas constant égal à 1, en déduire qu'on a
$$\sum_{g \in G} \chi(g) = 0.$$

4. Soit χ un homomorphisme de groupes $G \to \mathbf{C}^*$. Soit $g \in G$. Démontrer que $\chi(g)$ est une racine n-ième de l'unité.

5. Soient χ et χ' deux homomorphismes de groupes $G \to \mathbf{C}^*$ qui sont distincts. Démontrer que l'application $G \to \mathbf{C}^*$ qui à g associe $\chi(g)/\chi'(g)$ est un homomorphisme de groupes. Démontrer qu'on a
$$\chi * \chi = n\chi \qquad \text{et} \qquad \chi * \chi' = 0.$$
A-t-on $\chi \in A^*$?

6. Soit χ un homomorphisme de groupes $G \to \mathbf{C}^*$. Démontrer que l'application $A \to \mathbf{C}$ qui à f associe $\sum_{g \in G} f(g)\chi(g)$ est un homomorphisme d'anneaux.

7. Supposons que G est cyclique et engendré par un élément g_0. Démontrer que si $\chi(g_0) = \chi'(g_0)$ on a $\chi = \chi'$. Combien y a-t-il d'homomorphismes de groupes $G \to \mathbf{C}^*$? Soit g un élément de G distinct de l'élément neutre. Démontrer qu'on a
$$\sum_{\chi} \chi(g) = 0,$$
où la somme porte sur tous les homomorphismes $G \to \mathbf{C}^*$.

6.14 Idéal d'un anneau (suite)

Soit A un anneau commutatif. Soit $a \in A$.

1. Montrer que $aA = \{ab \in A / b \in A\}$ est un idéal de A (voir feuille numéro 3), on dit que c'est un *idéal principal*. Cela définit alors un anneau quotient A/aA.

2. Montrer que l'ensemble $A[X]$ des polynômes à coefficients dans A, muni de l'addition et de la multiplication des polynômes, est un anneau commutatif.

3. Démontrer que l'application $\mathbf{C} \to \mathbf{R}[X]/(X^2 + 1)\mathbf{R}[X]$ qui à $a + ib$ associe la classe du polynôme $a + bX$ est un isomorphisme d'anneaux (a, $b \in \mathbf{R}$).

6.15 Matrices à coefficients dans $\mathbf{Z}/p\mathbf{Z}$

Soit p un nombre premier. Notons $\mathrm{M}_2(\mathbf{Z}/p\mathbf{Z})$ l'ensemble des matrices 2×2 à coefficients dans $\mathbf{Z}/p\mathbf{Z}$ et $\mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z})$ le sous-ensemble de $\mathrm{M}_2(\mathbf{Z}/p\mathbf{Z})$ formé par les matrices de déterminant non nul.

1. Démontrer que $\mathrm{M}_2(\mathbf{Z}/p\mathbf{Z})$, muni de l'addition et de la multiplication des matrices, est un anneau.
2. En déduire que $\mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z})$, muni de la multiplication des matrices, est un groupe.
3. Déterminer l'ordre de $\mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z})$.
4. Démontrer que la matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est d'ordre p dans $\mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z})$. Soit a un générateur de $(\mathbf{Z}/p\mathbf{Z})^*$. Démontrer que la matrice $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ est d'ordre $p-1$ dans $\mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z})$.
5. Lorsque $p = 3$, trouver un élément d'ordre 4 dans $\mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z})$.

6.16 Corps finis

Soit p un nombre premier différent de 2. On reprend l'exercice précédent. Soit $u \in (\mathbf{Z}/p\mathbf{Z})^*$ qui n'est pas un résidu quadratique. Posons

$$K_u = \{\begin{pmatrix} a & b \\ bu & a \end{pmatrix} \in \mathrm{M}_2(\mathbf{Z}/p\mathbf{Z}) / a, b \in \mathbf{Z}/p\mathbf{Z}\}.$$

1. Démontrer que si v est un élément de $(\mathbf{Z}/p\mathbf{Z})^*$ qui n'est pas un carré, on a $K_u = K_v$.
2. Démontrer que K_u possède p^2 éléments.
3. Démontrer que K_u est un sous-anneau commutatif de $\mathrm{M}_2(\mathbf{Z}/p\mathbf{Z})$.
4. Soient a, $b \in \mathbf{Z}/p\mathbf{Z}$. Démontrer que $a^2 - ub^2 = 0$ si et seulement si $(a, b) = (0, 0)$.
5. En déduire que K_u est un corps. Quelle est la caractéristique de K_u (voir feuille d'exercices numéro 3) ?
6. Démontrer que l'application $\mathbf{Z}/p\mathbf{Z} \to K_u$ qui à a associe $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ est un homomorphisme d'anneaux injectif.