Devoir 1 sur les chapitres 2 et 3
Préparé par : Pr. A. Zekhnini

Exercice 1
Soit $G = \langle \sigma \rangle$ un groupe cyclique. On pose $\Delta = 1 - \sigma$ et $N = \sum_{i=0}^{n-1} \sigma^i$, voir le cours pour les propriétés de Δ et N.

I. Soient A et B deux G-modules et $f : A \longrightarrow B$ un G-morphisme.

1. Démontrer toutes les inclusions suivantes : $f(\ker(\Delta_A)) \subset \ker(\Delta_B)$, $f(N(A)) \subset N(B)$ et $f(\ker(N_A)) \subset \ker(N_B)$, $f(\Delta(A)) \subset \Delta(B)$.
2. Rappeler les définitions des deux groupes de cohomologie $H^0(A)$ et $H^1(A)$.
3. Démontrer qu'il existe une application f_1 induite par f telle que f_1 soit un homomorphisme de $H^1(A)$ dans $H^1(B)$.

II. Soit la suite exacte suivante de G-modules et G-morphismes

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0. \tag{1}$$

1. Quand est ce on dit que le quotient d'Herbrand $q(A)$ est défini ? C'est quoi ce quotient ?
2. Démontrer que si $q(A)$ et $q(C)$ sont définis, alors $q(B)$ l'est aussi.
3. En se basant sur le lemme de l'hexagone exact (voir le cours), démontrer que
$$H^0(A)H^0(C)H^1(B) = H^1(A)H^1(C)H^0(B).$$
4. Déduire que $q(A)q(C) = q(B)$.
5. Dans la suite (1) on remplace le G-module C par B/A qu'on suppose fini.
   a. La suite obtenue est-elle toujours exacte ? Justifier.
   b. Déduire dans ce cas que $q(A) = q(B)$.

Exercice 2
Soit $G = \langle \sigma \rangle$ un groupe cyclique d'ordre n et d'élément neutre 1.

I. Quelques propriétés des groupes cycliques.

1. Démontrer que tout groupe cyclique H d'ordre aussi n est isomorphe à G, en déduire que G est isomorphe au groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$.
2. Justifier pourquoi tout groupe fini d'ordre un nombre premier p est isomorphe au groupe additif $(\mathbb{Z}/p\mathbb{Z}, +)$.
3. Déterminer le nombre des générateurs de G, caractériser ces générateurs ?
4. Rappelez le lien entre $\varphi(n)$, l'indicateur d'Euler de n, et $\mathbb{Z}/n\mathbb{Z}$. Justifier.
5. Démontrer que tout sous-groupe H de G est aussi cyclique d'ordre un diviseur de n.
6. Soit d un diviseur de n, montrer qu'il existe un sous-groupe K de G d'ordre d. Caractériser les sous-groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$ d'ordre d un diviseur de n.
7. Soit d un diviseur de n, considérons l'ensemble $U_d = \{x \in G \mid x^d = 1\}$. Démontrer que U_d est d'ordre d en précisant l'un de ses générateurs. Déduire le nombre d'éléments de G qui ont pour ordre d.
8. Soit un entier naturel n. Démontrer que n est la somme des indicateurs d'Euler de ses diviseurs : $n = \sum_{d|n} \varphi(d)$.
9. Dans cette question, on propose une autre méthode pour démontrer le résultat de la question I8. Soit n un entier naturel, et soit $d \in \mathbb{N}$ un diviseur de n. Posons $S_d = \{a \in \mathbb{N} \mid 1 \leqslant a \leqslant n \text{ et } a \wedge n = d\}$ et $T_d = \{k\frac{n}{d} \mid 1 \leqslant k \leqslant d \text{ et } k \wedge d = 1\}$.
   i. Montrer que les ensembles $(S_d)_{d|n}$ forment une partition de l'ensemble $\{1, 2, \cdots, n\}$.
   ii. Montrer que $S_{\frac{n}{d}} = T_d$. Déduire que $\sum_{d|n} \varphi(d) = n$.

II. Dans toute cette question d désigne un diviseur de n, on pose $n = dm$. Soit A le $\mathbb{Z}$-module libre de rand d défini par :

$$A = \sum_{i=1}^{d} \mathbb{Z}u_i.$$

On définit une action de G sur A de la façon suivante : $\sigma.u_i = \sigma(u_i) = u_{i+1}$ pour $i \leqslant d-1$ et $\sigma.u_d = \sigma(u_d) = u_1$, on dit que G agit sur A par permutation des éléments de la base.

1. Déterminer l'ordre du sous-groupe $G_A = \langle \sigma^d \rangle$ et son indice dans G.
2. Démontrer que σ^d agit comme l'identité sur A.
3. Démontrer les quantités suivantes :
   a. $\ker(N) = \{X = \sum_{i=1}^{d} z_i u_i \mid \sum_{i=1}^{d} z_i = 0\}$.
   b. $Im(\Delta) = \ker(N)$.
   c. $\ker(\Delta) = \mathbb{Z}(\sum_{i=1}^{d} u_i) = \mathbb{Z}(u_1 + u_2 + \cdots + u_d)$.
   d. $Im(N) = m\mathbb{Z}(\sum_{i=1}^{d} u_i) = m\mathbb{Z}(u_1 + u_2 + \cdots + u_d)$.
4. Déduire que $H^0(A) = \mathbb{Z}/m\mathbb{Z}$ et $H^1(A) = 0$ et que $q(A) = [\mathbb{Z} : m\mathbb{Z}]^{-1} = \frac{1}{|G_A|}$.

Exercice 3

Soient L/K une extension cyclique de corps de nombres et $\mathfrak{m}$ un module de K. On définit un homomorphisme $j_{\mathfrak{m}} : \mathbf{I_L} \to \mathbf{I_L^{\mathfrak{m}}}$ sur les premiers par : $j_{\mathfrak{m}}(\mathfrak{P}) = \mathfrak{P}$, si $\mathfrak{P} \nmid \mathfrak{m}$ et $j_{\mathfrak{m}}(\mathfrak{P}) = 1$, si $\mathfrak{P} | \mathfrak{m}$. On rappelle aussi l'application $i : L^* \longrightarrow \mathbf{I_L}; \alpha \longmapsto (\alpha) = \alpha\mathcal{O}_{L^*}$. Enfin, on note $f_{\mathfrak{m}} = j_{\mathfrak{m}} o i$.

1. Déterminer $\ker(j_{\mathfrak{m}})$.
2. Calculer $f_{\mathfrak{m}}(K_{\mathfrak{m}})$ et $f_{\mathfrak{m}}(K_{m,1})$.
3. Donner une démonstration détaillée du Théorème 3.3.1 du cours (la dernière version). Vous pouvez utiliser le livre : Algebraic Number Theory de Janusz pages 175-176, (la preuve de la Proposition 2.3).

À rendre dans deux semaines,
c'est-à-dire avant le 17/06/2020.
Bon courage.