TD3 : Groupes profinis

Exercice 1. [Erratum du TD2]
Nous allons établir le résultat suivant :

Proposition. *Soit X un espace topologique compact, et $x \in X$. Alors, l'intersections des ouverts-fermés de X contenant x est connexe*

On fixe X un espace topologique compact, et $x \in X$.

(1) Montrer que X est **normal**, i.e., si $F, G \subset X$ fermés d'intersection vide, on peut trouver deux ouverts de X : U et V, tels que $F \subset U$, $G \subset V$, et $U \cap V = \emptyset$.

On sépare x de y pour tout $x, y \in F \times G$ par $U_{x,y}, V_{x,y}$. Alors $V_x = \cup_y V_{x,y}$ recouvre G mais pas x, et on en extrait un sous-recouvrement fini ; l'intersection selon ce recouvrement des $U_{x,y}$ est un ouvert contenant x et disjoint de V_x.
Ensuite, on écrit $X = X \setminus F \cup \cup_x U_x$, dont on extrait un sous-recouvrement fini. L'intersection des V_x selon ce recouvrement est un ouvert contenant G, disjoint de F
Soit A l'intersection des ouverts fermés de X contenant x. On écrit $A = F \sqcup G$, où F, G ouverts (donc aussi fermés) de A. Sans perte de généralité, on suppose $x \in F$.
Par normalité, on chosit $F \subset U$ et $G \subset V$ ouverts de X tels que $U \cap V = \emptyset$.

(2) Construire un ouvert fermé I de X tel que $x \in I$ et $I \subset U \cup V$.
On écrit $(X \setminus U \cup V) \cap \bigcap_{C_\lambda \text{ voisinage clopen de } x} C_\lambda = \emptyset$ intersections de fermés, donc il existe une sous-intersection finie, $I = \cap_{i=1}^n C_{\lambda_i}$, qui est donc clopen, telle que $(X \setminus (U \cup V)) \cap I = \emptyset$; i.e. $I \subset U \cup V$

(3) En écrivant $I = (I \cap U) \sqcup (I \cap V)$, montrer que $V = \emptyset$.
On a $I = (I \cap U) \sqcup (I \cap V)$, qui sont deux clopen de X. Or $x \in I$, donc $A \subset (I \cap U)$ car c'est un clopen de X contenant x. Maintenant $G \subset A \cap V \subset U \cap V = \emptyset$

(4) En déduire que tout espace topologique compact totalement discontinu a une base de voisinages ouvert-fermés
Si X est totalement discontinu, $A = \{x\}$. Autrement dit, si x, y distincts, on dispose d' un ouvert fermé qui contient x mais pas y. On conclut par la question 4 de l'exercice 2 du TD2
On utilisera la question 4 de l'exercice 2 du TD2

Exercice 2. [Autour de $SL_n(\mathbb{Z})$]

(1) On fixe un entier $k \geq 2$. Montrer que la réduction modulo k des coefficients induit un morphisme de groupe $f_k : SL_n(\mathbb{Z}) \to SL_n(\mathbb{Z}/k\mathbb{Z})$
Bonne définition : Respecte le déterminant (mod p) car $\mathbb{Z} \to \mathbb{Z}/r\mathbb{Z}$ est un morphisme d'anneau, qui commute avec les polynômes
Morphisme de groupe : C'est un polynôme terme à terme, et idem

(2) En déduire que $SL_n(\mathbb{Z})$ est résiduellement fini.
Si deux matrices sont différentes, on a des coefficients qui ne sont pas égaux mod k pour un k suffisemment grand

(3) Montrer que tout vecteur colonne $(a_1, \dots, a_n) \in \mathbb{Z}^n$, est conjugué, par multiplication à gauche par des éléments de $SL_n(\mathbb{Z})$, à $(b, 0, \dots, 0)$; où $b = PGCD(a_1, \dots, a_n)$.
Indice : Commencer par le cas $n = 2$.
On le fait par récurrence. Pour $s, t \in \mathbb{Z}^2$ dont le PGCD vaut d, on se donne a, b tels que $as + bt = d$ (Bézout).
Alors la matrice $\begin{pmatrix} s & t \\ -b/d & a/d \end{pmatrix}$ convient.
Pour $n \leq 2$ vecteurs, on applique l'algorithme précédent aux deux premiers (en complétent la matrice avec l'identité sur le gros bloc). On itère par récurrence ; par associativité du PGCD, on a le résultat souhaité.

(4) Montrer que si $M \in M_n(\mathbb{Z})$, il existe $P, Q \in SL_n(\mathbb{Z})$ tels que :

$$PMQ = diag(d_1, \dots, d_r, 0, \dots, 0)$$

pour des entiers relatifs $d_1 | d_2 | \dots | d_r$.
Pour une preuve de ce théorème et des corrolaires, voir ici (vers la page 57)
Par la question précédente, on peut écrire $PMQ = \begin{pmatrix} d & * & \dots & * \\ 0 & * & \dots & * \\ \vdots & * & \dots & * \\ 0 & * & \dots & * \end{pmatrix}$
Si d divise tous les termes $*$, on peut, après transvection, obtenir la première ligne $(d, 0, \dots, 0)$. On continue par récurrence sur le bloc en bas à droite.
Sinon, il existe un coefficient qui n'est pas divisible par d. Notons le a. Quitte à sommer la ligne contenant ce a avec la première ligne autre on obtient une matrice de la forme (On écrit a sur la 2e colonne pour simplifier l'écriture, mais il est a priori en position arbitraire (sur la première ligne)) $\begin{pmatrix} d & a & \dots & * \\ 0 & * & \dots & * \\ \vdots & * & \dots & * \\ 0 & * & \dots & * \end{pmatrix}$ La question précédente permet de transformer la matrice pour obtenir $\begin{pmatrix} PGCD(d,a) & 0 & \dots & 0 \\ * & * & \dots & * \\ \vdots & * & \dots & * \\ * & * & \dots & * \end{pmatrix}$
ce qui est, après transposition (qui ne change rien à l'argument), la forme initiale de la matrice, où on a remplacé d par un diviseur propre de d.
Ainsi en un nombre fini d'étape, nous obtenons l'écriture attendue
Pour une preuve de ce théorème et des corrolaires, voir ici (vers la page 57)

(5) Soit $b_1, \dots, b_N \in (\mathbb{Z}/p^k\mathbb{Z})^N$. Montrer qu'il existe $(a_1, \dots, a_N) \in \mathbb{Z}^N$ tels que :
- Pour tout i, $a_i \cong b_i \mod p^k$
- Pour tout $i \neq j$; $PGCD(a_i, a_j)$ est une puissance de p

On suppose donné des relevés de $b_1, \dots, b_n$ en des $a_1, \dots, a_n$ dont tous les PGCD deux à deux soient des puissances de p
On veut lifter b_{n+1} en un a_{n+1} dont la réduction mod p^k soit prescrite. Pour $a \in \mathbb{Z}$, on note $a' = a/p^{v_p}(a)$ la "partie première à p de a". Avec les hypothèses effectuées, les a_i' sont premiers entre eux
Par théorème des restes chinois, l'application $\mathbb{Z} \to \prod_{i=1}^n, \mathbb{Z}/a_i'\mathbb{Z} \times \mathbb{Z}/p^k\mathbb{Z}$ est surjective. On peut donc trouver a_{n+1} qui soit premier avec tous les a_i' (par exemple,

congrue à 1 modulo a'_i), et congru à b_{n+1} modulo p^k
Le PGCD de a_{n+1} et a'_i est 1, donc le PGCD de a_{n+1} et a_i est une puissance de p

(6) En déduire que, si k est premier, l'application f_k sont surjectifs.

Méthode 1 : On accepte que le résultat de la question 4 est vrai en remplaçant R par tout anneau principal, y compris $R = \mathbb{Z}/p^k\mathbb{Z}$. Ce faisant, on a pas besoin de la question 5. En effet, toute matrice $M \in SL_n(\mathbb{Z}/p^k\mathbb{Z})$ est équivalente via des matrices de $SL_n(\mathbb{Z}/p^k\mathbb{Z})$ à l'identité de $\mathbb{Z}/p$. De plus, par l'algorithme, les matrices de changement de base sont obtenues comme produit de matrices de transvections ; et on peut les relever à chaque fois en une matrice de $SL_n(\mathbb{Z})$ de manière naturelle. En suivant ces choix, on obtient deux relevés $P, Q \in SL_n(\mathbb{Z})$ telles que $f_{p^k}(P)Mf_{p^k}(Q) = Id$, et a fortiori $M = f_{p^k}\left(P^{-1}Q^{-1}\right)$
Autrement dit : $SL_n(\mathbb{Z}/N\mathbb{Z})$ est engendré par les matrices de transvections, qui se relèvent clairement en des matrices de transvection de $SL_n(\mathbb{Z})$

Méthode 2 : On bidouille à partir de la diagonalisation sur $\mathbb{Z}$. Soit $M \in SL_n(Z/p^k\mathbb{Z})$. On la relève en une matrice $\tilde{M} \in M_n(\mathbb{Z})$ en relevant tous les élements de M d'une manière donnée par la question précédente. On diagonalise $\tilde{M}$ par la question 4 : $\tilde{M} = P_1D_1Q_1$, où $D_1 = diag(d_1, \dots, d_n)$. En suivant l'algorithme, on sait d_1 est une puissance de p (en général, d_1 est le PGCD des éléments de $\tilde{M}$). Comme la matrice est inversible mod p^k, on a $d_1 = \pm 1$

Attention : J'ai affirmé en TD que tous les d_i étaient alors des puissances de p : C'est faux, on le voit sur une matrice 2x2 explicite par exemple. En général, d_i est le PGCD des mineurs d'ordre i de la matrice.

Maintenant, soit D'_1 le bloc de taille $n-1$ en bas à droite de D_1. On trouve une autre matrice N_1 dont les coefficients vérifient les conditions de la question (5) et qui a le même résidu modulo p^k que D'_1. Changer $\tilde{M}$ en $\tilde{M}_2 = P_1(diag(1, N_1))Q_1$ ne change pas le fait que son résidu modulo p^k est M.
On écrit $N_1 = P_2D_2Q_2$ comme dans la question 4 ; et le premier terme de D_2 est 1 par le même argument.
On a maintenant écrit $\tilde{M}_2 = P_1diag(1, P_2)diag(1, N_1)diag(1, Q_2)Q_1$ produit de matrices dans $SL_n(\mathbb{Z})$. Ce qu'on a gagné, c'est que maintenant les 2 premiers termes diagonaux de la matrice diagonale sont égaux à 1
En appliquant ce procédé n fois, on obtient une matrice identité au milieu, et $\tilde{M}_n$ est un relevé de M qui est dans $SL_n(\mathbb{Z})$

(7) (Bonus) : Que dire de f_r pour n quelconque ?

C'est encore vrai, par essentiellement le même argument (plus facile à voir avec la diagonalisation sur les anneaux principaux).
On remarque d'ailleurs qu'il découle du théorème des restes chinois que, si $PGCD(n, m) = 1, SL_n(\mathbb{Z}/kl\mathbb{Z}) \cong SL_n(k\mathbb{Z}) \times SL_n(l\mathbb{Z})$. Cela découle purement formellement du théorème des restes chinois et du fait que SL_n, vu comme foncteur $Ring \to Grp$, préserve les produits. Cela ne permet malheureusement pas de répondre à la question.