École Normale Supérieure, Année 2019-2020

1e année, Algèbre 1

**TD n° 2 : Groupes abéliens**

---

**Exercice 1.**

Montrer que les groupes $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$ et $\mathbb{Z}/100\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ sont isomorphes.

**Exercice 2.**

Soit $G$ un groupe abélien fini qui n'est pas monogène. Montrer qu'il existe un nombre premier $p$ tel que $G$ possède un sous-groupe isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

**Exercice 3.**

Faire la liste des groupes abéliens de cardinal 360. Plus généralement, combien y a t'il de groupes abéliens de cardinal $n$ fixé ? Quelle est la relation avec le nombre de classes de conjugaison dans $\mathfrak{S}_n$ ?

**Exercice 4.**

Soit $G$ un groupe abélien fini. Montrer qu'il existe dans $G$ un élément d'ordre égal à l'exposant de $G$. On rappelle que *l'exposant de* $G$ est le ppcm des ordres des éléments de $G$. Et si $G$ n'est pas abélien ?

**Exercice 5.**

Soit $G$ un groupe et $H$ un sous-groupe abélien distingué de $G$. On note $\pi\colon G \to G/H$ la projection et on suppose qu'on a une section de $\pi$, i.e. un morphisme $s\colon G/H \to G$ tel que $\pi \circ s = \mathrm{id}_{G/H}$.

1. Montrer que si $s(G/H)$ est distingué dans $G$, alors $G \cong H \times G/H$.
2. Trouver un contre-exemple si $s(G/H)$ n'est pas distingué dans $G$.

**Exercice 6.**

Soit $K$ un corps et soit $G \subset K^*$ un sous-groupe fini d'ordre $n$. On va montrer que $G$ est un groupe cyclique.

1. Montrer que l'ordre de tout élément de $G$ divise $n$.
2. Soit $d$ un diviseur de $n$ et $x \in G$ d'ordre $d$. Soit $H$ le sous-groupe cyclique de $G$ engendré par $x$. Montrer que tout élément d'ordre $d$ est dans $H$.
3. On note $N(d)$ le nombre d'éléments de $G$ d'ordre $d$. Montrer que si $N(d)$ n'est pas nul alors $N(d) = \varphi(d)$ puis que $\sum_{d|n,\ d>0} N(d) = n$.
4. Conclure.

En particulier, si $p$ est un nombre premier, $(\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$, et si $K$ est un corps fini, $K^*$ est un groupe cyclique.

**Exercice 7.**

Si $A$ est un anneau, on note $A^\times$ le groupe (multiplicatif) des éléments inversibles de $A$.

1. Soit $G$ un groupe monogène. Montrer que le groupe des automorphismes de $G$ est en bijection avec l'ensemble des générateurs de $G$.
2. Montrer que pour tout $n \in \mathbb{N}$, on a un isomorphisme de groupes $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.
3. Soit $p$ un nombre premier impair et soit $\alpha \geq 1$. Quel est l'ordre de $1+p$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ ? En déduire que $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \cong \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$.
4. Expliciter $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ pour $\alpha \geq 1$.
5. En déduire $(\mathbb{Z}/n\mathbb{Z})^\times$ pour $n \in \mathbb{N}$. Expliciter $(\mathbb{Z}/187\mathbb{Z})^\times$.
6. Déterminer les entiers $n \in \mathbb{N}$ tels que $(\mathbb{Z}/n\mathbb{Z})^*$ est monogène.

**Exercice 8.** †

On se propose de redémontrer le théorème de structure des groupes abéliens finis.

On appelle caractère d'un groupe abélien fini $G$ tout morphisme $G \to \mathbb{C}^*$.

1. Si $H$ est un sous-groupe d'un groupe abélien fini $G$, montrer que tout caractère de $H$ se prolonge en un caractère de $G$.
2. Soit $G$ un groupe abélien fini. On note $H$ un sous-groupe de $G$ engendré par un élément de $G$ d'ordre maximal. Montrer que l'on a un isomorphisme $G \cong H \times G/H$.
3. Conclure.

**Exercice 9. [Objets injectifs et groupes divisibles]**†

Soit $G$ un groupe abélien. On dit que $G$ est *divisible* si pour tout $x \in G$ et $n \in \mathbb{N}^*$ il existe $y \in G$ tel que $ny = x$. On dit que $G$ est *injectif* si pour toute injection de groupes abéliens $\iota\colon X \hookrightarrow Y$, tout morphisme $\psi\colon X \to G$ s'étend en un morphisme $\tilde{\psi}\colon Y \to G$.

1. Montrer qu'un groupe abélien est injectif si et seulement s'il est divisible.
2. Montrer que tout groupe abélien se plonge (i.e. admet un morphisme injectif) dans un groupe injectif.
3. Soit $p$ un nombre premier. Le *$p$-groupe de Prüfer* est le sous-groupe de $\mathbb{Q}/\mathbb{Z}$ de la forme
$$\mathbb{Z}\left[\frac{1}{p}\right]/\mathbb{Z} := \left\{\frac{a}{p^n} \in \mathbb{Q}/\mathbb{Z}\ ;\ n \in \mathbb{N},\ a \in \mathbb{Z}\right\}.$$
Montrer que tout groupe abélien divisible est somme directe de copies de $\mathbb{Q}$ et de groupes de Prüfer.

**Exercice 10. [Simplification pour les groupes finis]**

Le but de cet exercice est de montrer que si $G$, $H$ et $K$ sont trois groupes finis et si on a un isomorphisme $G \times H \cong G \times K$ alors $H \cong K$. On notera $M(G,H)$ le nombre de morphismes de groupes de $G$ dans $H$ et $I(G,H)$ le nombre de morphismes de groupes de $G$ dans $H$ qui sont injectifs.

1. Expliquer pourquoi l'énoncé de simplification est vrai si les groupes sont abéliens.
2. Soit $G$ et $H$ deux groupes finis, montrer que
$$M(G,H) = \sum_{\Gamma \triangleleft G} I(G/\Gamma, H).$$
En déduire qu'il existe une famille d'entiers $(a_\Gamma)_{\Gamma \triangleleft G}$ indexée sur les sous-groupes distingués de $G$ telle que
$$I(G,H) = \sum_{\Gamma \triangleleft G} a_\Gamma M(G/\Gamma, H).$$
3. Soit $G$, $H$, $K$ trois groupes finis tels qu'on ait un isomorphisme $G \times H \cong G \times K$. Montrer que pour tout groupe fini $X$ on a $M(X,H) = M(X,K)$ et que $I(X,H) = I(X,K)$. Puis, conclure que $H \cong K$.
4. Trouver un contre-exemple si $G$ est infini.

**Exercice 11. [Théorème de Wilson]**

Soit $G$ un groupe abélien fini. Soit $G_2 = \{x \in G \mid 2x = 0\}$. On pose
$$x = \sum_{g \in G} g.$$

1. Montrer que $x \neq 0$ si et seulement si $G_2$ est de cardinal 2. Dans ce cas, $x$ est l'unique élément non nul de $G_2$.
2. En déduire le théorème de Wilson : pour tout nombre premier $p$, $(p-1)! \equiv -1 \pmod p$.

*Les trois exercices qui suivent sortent largement du cadre du cours. Ils se suivent et présentent une construction extrêmement importante en arithmétique. Ils sont bien-sûr facultatifs et ne seront pas abordés en TD.*

**Exercice 12. [Limites projectives et complétés]$^\dagger$**

On appelle *système projectif de groupes finis* la donnée pour un ensemble ordonné filtrant $(I, \leqslant)$, d'une famille de groupes finis $(G_i)_{i\in I}$ et pour tout $i, j \in I$ tel que $j \leqslant i$ d'un morphisme $f_{ij}\colon G_i \to G_j$ tel que

- $\forall i \in I,\ f_{ii} = \mathrm{id}_{G_i}$,
- $\forall i, j, k \in I$, tel que $k \leqslant j \leqslant i,\ f_{jk} \circ f_{ij} = f_{ik}$.

À partir d'un tel système projectif on construit la *limite projective*

$$\varprojlim_i G_i = \left\{(x_i)_{i\in I} \in \prod G_i \mid \forall i, j \in I,\ f_{ij}(x_i) = x_j \text{ si } j \leqslant i\right\}.$$

On dira qu'un groupe qui est limite projective de groupes fini est un groupe *profini*, on notera $f_i\colon G \to G_i$ le morphisme de projection pour tout $i \in I$.

1. En supposant que les $f_{ij}$ sont surjectifs et les $G_i$ non-nuls montrer $\varprojlim_i G_i$ est non-nul.
2. Soit $G \cong \varprojlim_i G_i$ un groupe profini. Soit $H$ groupe et $(\varphi_i\colon H \to G_i)$ une famille de morphismes tels que pour tout $i, j \in I$ avec $j \leqslant i$ on ait $f_{ij} \circ \varphi_i = \varphi_j$. Montrer qu'il existe un unique morphisme $\varphi\colon H \to G$ tel que pour tout $i \in I$ on ait $\varphi_i = f_i \circ \varphi$.
3. Soit $G$ un groupe et $I$ l'ensemble de ses sous-groupes distingués d'indices finis ordonnés par l'inclusion. On définit $\widehat{G} = \varprojlim_{K\in I} G/K$ le *complété profini* de $G$. Donner un exemple d'un groupe $G$ profini tel que $G \to \widehat{G}$ ne soit pas un isomorphisme.
4. On définit *les entiers p-adiques* $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^i\mathbb{Z}$ où les morphismes sont les morphismes de réduction. Montrer que $\widehat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$ où le produit se fait sur tous les nombres premiers. On notera que c'est même un isomorphisme d'anneaux (topologiques).
5. Cette dernière question demande un peu de topologie. On munit $G = \varprojlim_i G_i$ de la topologie produit où chaque $G_i$ est muni de la topologie discrète. Montrer que $G$ est compact et que les composantes connexes sont réduites à des points (on dit que la topologie est *totalement discontinue*). Inversement, montrer que si $G$ est un groupe topologique compact muni d'une base de voisinages ouverts constituée de sous-groupes distingués, alors $G$ est profini.

**Exercice 13. [Dualité de Pontryagin]$^{\dagger\dagger}$**

Soit $G$ un groupe abélien. On pose $G^\vee = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ son *dual de Pontryagin*. On rappelle qu'un groupe abélien $G$ est dit *de torsion* si pour tout élément $x \in G$ il existe un entier $n \in \mathbb{N}$ tel que $nx = 0$ et que $G$ est *divisible* si pour tout $x \in G$ et $n \in \mathbb{N}^*$ il existe $y \in G$ tel que $ny = x$.

1. Montrer que si $G$ est un groupe abélien profini alors $G^\vee$ est abélien de torsion ; et réciproquement. Montrer de plus que si $G$ est sans torsion alors $G^\vee$ est divisible ; et réciproquement.
2. Montrer que si $G$ est abélien profini ou abélien de torsion alors $(G^\vee)^\vee \cong G$.
3. Montrer qu'un groupe abélien profini sans torsion est isomorphe à un produit de groupes de la forme $\mathbb{Z}_p$.

**Exercice 14.** $^{\dagger\dagger}$

Soit $n \geqslant 1$ un entier et $G = \mathrm{SL}_n(\mathbb{Z})$. Montrer que le morphisme universel $\widehat{G} \to \prod_p \mathrm{SL}_n(\mathbb{Z}_p)$ est un isomorphisme si et seulement si $n \neq 2$.