TD n°2 : Quotients et groupes abéliens

1 et 4/10/2024

Nous traiterons dans l'ordre les exercices 1, 2, 3 et 5. Vous pouvez naviguer librement parmi les exercices restants. Les exercices les plus délicats de la feuille sont marqués d'un .

Je reste disponible pour toute question concernant le TD, des maths, ou toute autre chose au bureau T13 (j'y suis à coups sûrs les mardis juste avant le TD). Vous pouvez également m'envoyer un mail à nataniel.marquis@dma.ens.fr.

Exercice 1. Sous-groupes d'un quotient

Soit G un groupe, soit $H \triangleleft G$ l'un de ses sous-groupes distingués et $\pi : G \to G/H$ la projection associée.

1. Soit K un sous-groupe de G. Démontrer que $K \cap H \triangleleft K$ puis que π induit un isomorphisme

$$K/K \cap H \cong \pi(K).$$

Nous voulons à présent décrire les sous-groupes de G/H en fonction de ceux de G, puis les quotients correspondant à ceux des sous-groupes qui sont distingués.

2. Démontrer que l'application suivante est une bijection :

$$\{K \leq G \mid H \subseteq K\} \to \left\{\Delta \leq G/H\right\}, \quad K \mapsto \pi(K).$$

3. Démontrer que cette bijection est croissante pour l'inclusion et qu'elle envoie les sous-groupes distingués de G contenant H exactement sur les sous-groupes distingués de G/H.
4. Soit K un sous-groupe distingué de G contenant H. Construire un isomorphisme

$$G/K \cong (G/H)/(K/H).$$

Exercice 2. Quotient par le centre

1. Soit G un groupe tel que $G/\mathrm{Z}(G)$ est monogène. Démontrer que G est abélien.

Nous définissons[1] le *groupe des quaternions*

$$\mathbb{H}_8 = \left\{\pm\mathrm{Id}, \pm I = \pm\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm J = \pm\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \pm K = \pm\begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}\right\} < \mathrm{GL}_2(\mathbb{C}).$$

2. Vérifier que I, J et K sont d'ordre 4 puis que $IJ = K$ et $JI = -K$.
3. Que dire sur le quotient de $\mathbb{H}_8$ par son centre ?

Exercice 3. Produits semi-directs isomorphes

Soient N et K deux groupes. Soient φ et ψ des morphismes de K dans $\mathrm{Aut}(N)$.

1. Supposons qu'il existe $\alpha \in \mathrm{Aut}(K)$ tel que $\psi = \varphi \circ \alpha$. Démontrer que $N \rtimes_\varphi K$ et $N \rtimes_\psi K$ sont isomorphes.

1. Vous pouvez vérifier qu'il s'agit d'un sous-groupe.

2. Supposons qu'il existe $u \in \mathrm{Aut}(N)$ tel que
$$\forall k \in K, \;\; \psi(k) = u \circ \varphi(k) \circ u^{-1}.$$
Démontrer que $N \rtimes_{\varphi} K$ et $N \rtimes_{\psi} K$ sont isomorphes.

Soit p un nombre premier. On définit le groupe des transformations affines[2] de $\mathbb{Z}/p\mathbb{Z}$ comme
$$\mathrm{Aff}(\mathbb{Z}/p\mathbb{Z}) := \{(x \mapsto ax+b) \in \mathrm{Bij}(\mathbb{Z}/p\mathbb{Z}) \,\big|\, a, b \in Z/p\mathbb{Z},\; a \neq 0\}.$$

3. Démontrer que l'ensemble des translations (i.e. pour $a = 1$) est distingué. En déduire que
$$\mathrm{Aff}(\mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z}) \rtimes_{\varphi} (\mathbb{Z}/p\mathbb{Z})^{\times}$$
pour un certain φ que l'on explicitera.
4. Nous pouvons obtenir un isomorphisme pour d'autres φ en utilisant les questions 1 et 2. À quoi correspond le fait de changer ainsi de φ du point de vue des transformations affines ?

Exercice 4. Simplification des 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 $\mathrm{M}(G,H)$ le nombre de morphismes de groupes de G dans H et $\mathrm{I}(G,H)$ le nombre de morphismes de groupes de G dans H qui sont injectifs.

1. Soit G et H deux groupes finis, montrer que
$$\mathrm{M}(G,H) = \sum_{\Gamma \triangleleft G} \mathrm{I}\left({}^{G}/{}_{\Gamma}, H\right).$$
En déduire qu'il existe une famille d'entiers $(a_\Gamma)_{\Gamma \triangleleft G}$ indexée sur les sous-groupes distingués de G telle que
$$\mathrm{I}(G,H) = \sum_{\Gamma \triangleleft G} a_\Gamma \mathrm{M}\left({}^{G}/{}_{\Gamma}, H\right).$$
2. 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 $\mathrm{I}(X,H) = \mathrm{I}(X,K)$. Conclure que $H \cong K$.
3. Trouver un contre-exemple si G est infini.

Exercice 5. Échauffement ?

Quelques questions avec des nombres précis pour pratiquer la structure des groupes abéliens de type fini. Trouver tous les groupes abéliens d'ordre 8 à isomorphisme près, puis d'ordre 500.

Exercice 6. Sous-groupes des groupes abéliens finis

Soit G un groupe abélien fini. Soit d un entier divisant $|G|$. Démontrer qu'il existe un sous-groupe d'ordre d dans G.

2. On peut également le définir comme l'ensemble des bijections telles que $\forall x, y, \lambda, \;\; f(\lambda x + (1-\lambda)y) = \lambda f(x) + (1-\lambda) f(y)$.

Exercice 7. Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$

Le but de cet exercice est de déterminer, pour tout entier n, la structure du groupe des inversibles $(\mathbb{Z}/n\mathbb{Z})^\times$. Nous commençons par essayer de dévisser le problème.

1. Soient A, B deux anneaux dont on notera $+$ et $\times$ les lois. On appelle morphisme d'anneaux une application de A dans B qui est un morphisme de groupes additifs et de monoïdes multiplicatifs. Ceci équivaut aux trois formules

$$\forall a, a' \in A,\ \ f(a+a') = f(a) + f(a'),\ f(aa') = f(a)f(a') \text{ et } f(1) = 1.$$

   Démontrer l'égalité suivante entre les sous-ensembles de $A \times B$:

$$(A \times B)^\times = A^\times \times B^\times.$$

2. Remarquer que l'isomorphisme du théorème des restes choinois est un morphisme d'anneaux. En déduire que pour $\mathrm{pgcd}(n, m) = 1$, le groupe $(\mathbb{Z}/nm\mathbb{Z})^\times$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$.
3. Retrouver ce résultat en utilisant l'exercice 12.

La question précédente permet de se ramener au cas $n = p^k$. Nous allons démontrer que pour tout nombre premier impair p, nous avons

$$\left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times \cong \mathbb{Z}/p^{k-1}(p-1)\mathbb{Z}$$

puis que

$$\forall k \geq 2,\ \ \left(\mathbb{Z}/2^k\mathbb{Z}\right)^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}.$$

4. Démontrer que $(\mathbb{Z}/p^k\mathbb{Z})^\times$ contient un élément d'ordre $p-1$.
5. Démontrer pour tout entier $r \geq 1$,

$$\forall (a, b) \in \mathbb{Z}^2,\ \ a \equiv b \mod p^r \implies a^p \equiv b^p \mod p^{r+1}.$$

   En déduire pour tout premier $p \geq 3$, l'élément $\overline{1+p}$ est d'ordre p^{k-1} dans $(\mathbb{Z}/p^k\mathbb{Z})^\times$. Montrer également que pour $k \geq 2$ $\overline{3}$ est d'ordre 2^{k-2} dans $(\mathbb{Z}/2^k\mathbb{Z})^\times$.
6. Conclure si $p \neq 2$.
7. Traiter le cas $p = 2$.
8. En guise d'application, déterminer les entiers naturels $n \geq 1$ tels que $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique.

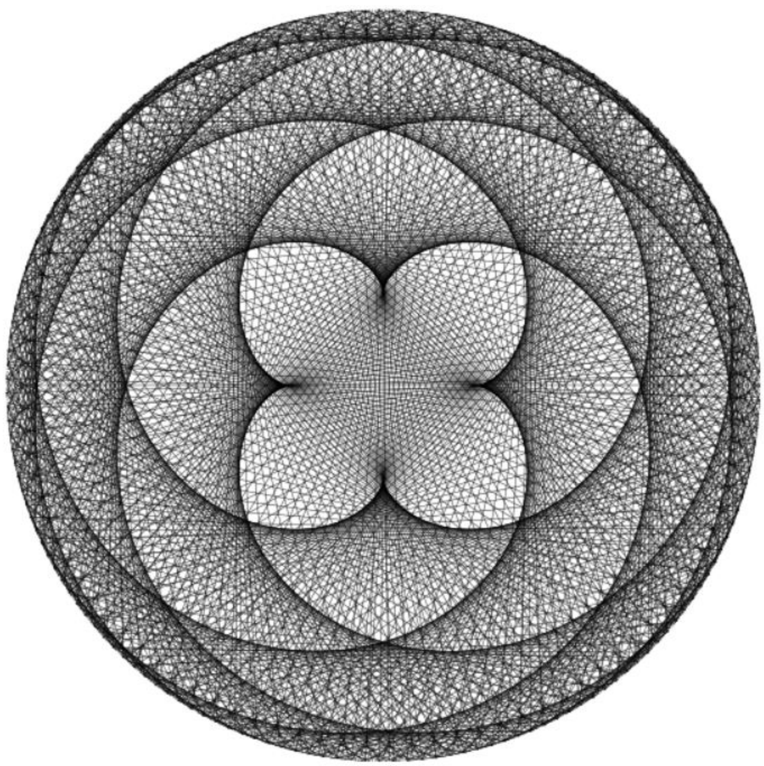

Figure 1 – Puissance $702^{\text{iéme}}$ appliquée aux racines 1002-ièmes.