TD n°3 : Quotients et groupes usuels

3 et 6/10/2023

Nous traiterons dans l'ordre les exercices 1, 3, 4, 6 et 8. Vous pouvez naviguer librement parmi les exercices restants ou parmi ceux de votre polycopié. 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 et vendredis juste avant le TD). Vous pouvez également m'envoyer un mail à nataniel.marquis@dma.ens.fr.

1 Groupes quotients

Exercice 1. Centre et automorphismes intérieurs

Soit G un groupe. Nous notons $\mathrm{Z}(G) = \{g \in G \,|\, \forall h \in G,\ \ gh = hg\}$ le centre de G.

1. Démontrer que l'application
$$\mathrm{Int} : G \to \mathrm{Aut}(G), \quad g \mapsto \left[h \mapsto ghg^{-1}\right]$$
qui à tout élément g associe la conjugaison par g est bien définie et qu'il s'agit d'un morphisme de groupes de noyau $\mathrm{Z}(G)$.
2. Nous définissons le sous-groupe des automorphismes intérieurs comme l'image $\mathrm{Int}(G)$. Déduire de la question précédente que $\mathrm{Z}(G)$ est un sous-groupe distingué de G et qu'il existe un isomorphisme de groupes
$$\mathrm{Int}(G) \cong {}^{G}/_{\mathrm{Z}(G)}.$$
3. Démontrer que $\mathrm{Int}(G)$ est un sous-groupe distingué de $\mathrm{Aut}(G)$.

Exercice 2. Conjugués et ordre

1. Soit G un groupe fini. Montrer que deux éléments conjugués de G ont même ordre. La réciproque est-elle vraie ?
2. Trouver tous les groupes abéliens finis pour lesquels la réciproque est vérifiée.

Exercice 3. Quotient par le centre

Soit G un groupe tel que ${}^{G}/_{\mathrm{Z}(G)}$ est monogène. Démontrer que G est abélien.
Que pouvons-nous déduire de ce résultat concernant le quotient de $\mathbf{H}_8$ par son centre ?

Exercice 4. 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 5. 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

$$\mathrm{M}(G,H) = \sum_{\Gamma \lhd G} \mathrm{I}\left(G/\Gamma, H\right).$$

En déduire qu'il existe une famille d'entiers $(a_\Gamma)_{\Gamma \lhd G}$ indexée sur les sous-groupes distingués de G telle que

$$\mathrm{I}(G,H) = \sum_{\Gamma \lhd G} a_\Gamma \mathrm{M}\left(G/\Gamma, H\right).$$

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.

2 Groupes usuels

Exercice 6. Sous-groupes de $\mathbb{Q}$, première édition

L'exercice suivant porte sur les sous-groupes de $\mathbb{Q}$. On note $\mathbb{P}$ l'ensemble des nombres premiers, s'inspirant de Steinitz, on appelle *nombre superrationnel* toute collection $s = (s_p)_{p\in\mathbb{P}}$ telle que pour tout premier p on a $s_p \in \mathbb{Z}\coprod\{+\infty\}$ et que seul un nombre fini des s_p est négatif. On note $\mathcal{S}$ l'ensemble des nombres superrationnels. [1] On appelle entiers supernaturels les nombres superrationnels dont toutes les "coordonnées" sont positives.

On dispose d'une application naturelle $\iota : \mathbb{Q} \to \mathcal{S}$, associant à $r \in \mathbb{Q}_+$ l'élément $(\mathrm{v}_p(r))_{p\in\mathbb{P}}$, où $\mathrm{v}_p : \mathbb{Q} \to \mathbb{Z}\coprod\{+\infty\}$ est la valuation p-adique [2]. Deux rationnels $r$et r' ont même image si et seulement si $r = \pm r'$. Cette application envoie les entiers sur des entiers supernaturels.

On munit l'ensemble $\mathcal{S}$ des nombres superrationnels de la relation d'ordre $s \preceq s' \Leftrightarrow s_p \leq s'_p$ pour tout $p \in \mathbb{P}$.

1. Un nombre superrationnel est parfois noté suggestivement $\prod_{p\in\mathbb{P}} p^{s_p}$, en omettant éventuellement les exposants nuls, par exemple on a $2^{+\infty}\,3\,5^{+\infty}/7^2 \in \mathcal{S}$.
2. Par définition $\mathrm{v}_p(x)$ vaut $+\infty$ si $x \in \mathbb{Q}$ est nul, et sinon, c'est l'unique entier $m \in \mathbb{Z}$ tel que x s'écrive sous la forme $p^m a/b$ avec a et b entiers et premiers à p.

1. Vérifier les affirmations des paragraphes précédents. Montrer ensuite que l'on a $n|m$ dans $\mathbb{N}$ si et seulement si $\iota(n) \preceq \iota(m)$.
2. Démontrer que tout superrationnel s'écrit de manière unique comme $s_+ - s_-$ où s_+ est un entier supernaturel, s_- est l'image d'un vrai entier par ι, et où s_+ et s_- n'ont pas de coordonnées simultanément non nulles.
3. Montrer que toute famille de $(\mathcal{S}, \preceq)$ possède une borne supérieure.

Pour $s \in \mathcal{S}$ on note $H_s \subset \mathbb{Q}$ l'ensemble des rationnels $r = {}^a\!/_b$ sous forme irréductible tels que $s_- \preceq \iota(a)$ et que $\iota(b) \preceq s_+$. On se propose de montrer que $s \mapsto H_s$ est une bijection croissante de $\mathcal{S}$ sur l'ensemble des sous-groupes non réduits à $\{0\}$ de $\mathbb{Q}$.

3. Montrer que H_s est un sous-groupe de $\mathbb{Q}$, et que l'on a $H_s \subset H_{s'} \Leftrightarrow s \preceq s'$. Décrire $H_{\iota(r_1)}$ pour $r_1 \in \mathbb{Q}^\times$.
4. Soit G un sous-groupe de $\mathbb{Q}$ contenant $\mathbb{Z}$. En posant s_G la borne supérieure de tous les dénominateurs des éléments de G, démontrer que $G = H_{s_G}$.
5. Conclure à la bijectivité (sans l'hypothèse que G contienne $\mathbb{Z}$).
6. À quels nombres superrationnels les sous-groupes $\mathbb{Z}$ et $\mathbb{Q}$ correspondent-ils ?

Exercice 7. Sous-groupes de $\mathbb{Q}$, deuxième édition

Cet exercice va un peu plus loin dans la description des sous-groupes de $\mathbb{Q}$. Il répond d'abord à la question de classement à isomorphisme près. Nous fournissons moins d'étapes intermédiaires qu'à l'exercice précédent.

1. Démontrer que $H_s \cong H_{s'}$ en tant que groupes si et seulement si s et s' diffère en un nombre fini de coordonées et qu'ils sont différents de $+\infty$ en ces coordonnées.
2. Démontrer que pour tout sous ensemble $\mathcal{T} \subseteq \mathcal{S}$, nous avons l'identité

$$\sum_{t \in \mathcal{T}} H_t = H_{\sup \mathcal{T}}.$$

Nous finissons par quelques questions questions concernant les sous-groupes de $\mathbb{Q}/\mathbb{Z}$.

3. Quels sont les sous-groupes de $\mathbb{Q}/\mathbb{Z}$?
4. Le groupe de Prüfer associé à p, $\mathbb{U}_{p^\infty}$, est défini comme le sous-groupes de $\mathbb{C}^\times$ formé des racines p^n-ièmes de l'unité pour un certain n. Démontrer que les groupes de Prüfer sont deux à deux non isomorphes.
5. En démontrant que le sous-groupes des racines de l'unité dans $\mathbb{C}^\times$ est isomorphe à $\mathbb{Q}/\mathbb{Z}$, trouver les sous-groupes du sous-groupe $\mathbb{U}_{p^\infty}$.
6. Démontrer que

$$\mathbb{Q}/\mathbb{Z} = \bigoplus_{p \in \mathbb{P}} H_{p^\infty}/\mathbb{Z}$$

où la somme directe est définie de manière analogue aux espaces vectoriels. Déterminer tous les sous-groupes de $\mathbb{Q}/\mathbb{Z}$ et démontrer qu'ils sont deux à deux non isomorphes.

Exercice 8. Théorème de Kronecker et conséquences

Cet exercice a pour but de démontrer et d'utiliser le théorème de Kronecker sur les sous-groupes de $\mathbb{R}$.

1. Démontrer qu'un sous-groupe de $\mathbb{R}$ est soit dense, soit de la forme $x\mathbb{Z}$ pour un certain réel positif x.

2. Déterminer lesquels des sous-groupes denses[3] de $\mathbb{R}$ suivants sont isomorphes :

$$\mathbb{R},\ \mathbb{Q},\ H_{p^\infty} \text{ pour } p \text{ premier},\ \mathbb{Z}+\sqrt{2}\mathbb{Z},\ \mathbb{Z}+\sqrt{3}\mathbb{Z},\ \sum_{i\in I\setminus\{i_0\}} x_i\mathbb{Q}$$

où $(x_i)_{i\in I}$ est une $\mathbb{Q}$-base de $\mathbb{R}$ et où $i_0 \in I$.

3. Démontrer que pour tout irrationnel α, le sous-groupe $\mathbb{Z}+\alpha\mathbb{Z}$ est dense dans $\mathbb{R}$. En déduire que la suite $(\cos(n))_{n\geq 1}$ est dense dans $[-1,1]$.
4. Démontrer que le sous-groupe $2^{\mathbb{Z}}3^{\mathbb{Z}}$ de $\mathbb{R}_+^\times$ est dense.
5. ◍ Démontrer que le sous-monoïde $2^{\mathbb{N}}3^{-\mathbb{N}}$ de $\mathbb{R}_+^\times$ est dense.

Exercice 9. Sous-groupes de $\mathbb{R}^n$

Nous fixons dans cet exercice un entier naturel n. Nous cherchons à comprendre davantage les sous-groupes de $\mathbb{R}^n$.

1. Soit G un sous-groupe fermé de $\mathbb{R}^n$. Démontrer qu'il existe (V,W), sous-espaces vectoriels supplémentaires de $\mathbb{R}^n$ et un sous-groupe discret $\Gamma \subset W$ tel que

$$G = V \oplus \Gamma.$$

Indication : on pourra considérer le sous-$\mathbb{R}$-espace vectoriel maximal inclus dans G.

2. Soit G un sous-groupe de $\mathbb{R}^n$. Démontrer qu'il existe (V,W), sous-espaces vectoriels supplémentaires de $\mathbb{R}^n$, un sous-groupe dense $\tilde{G} \subseteq V$ et un sous-groupe discret $\Gamma \subset W$ tel que

$$G = \tilde{G} \oplus \Gamma.$$

Exercice 10. Morphismes vers $\mathbb{C}$

1. Démontrer que pour tout $\alpha \in \mathbb{C}$, l'application

$$\varphi_\alpha : \mathbb{R} \to \mathbb{C},\ x \mapsto \alpha x$$

est un morphisme de groupe continu de $(\mathbb{R},+)$ vers $(\mathbb{C},+)$, puis que ce sont les seuls. Sont-ce les seuls ?

2. Démontrer que pour tout $\alpha \in \mathbb{C}$, l'application

$$\exp_\alpha : \mathbb{R} \to \mathbb{C}^\times,\ x \mapsto e^{\alpha x}$$

est un morphisme de groupe continu de $(\mathbb{R},+)$ vers $(\mathbb{C}^\times,\times)$, puis que ce sont les seuls.

3. En déduire que tout morphisme de groupes continu de $\mathbb{U}$ vers $\mathbb{C}^\times$ est de la forme $z \mapsto z^n$ pour un certain $n \in \mathbb{Z}$.

3. On pourra vérifier qu'ils sont effectivement denses.

3 Inclassé

Exercice 12. Autour de symboles de Legendre

Nous commençons par faire une analyse de certains symboles de Legendre.

1. Soit p un nombre premier impair. Démontrer de deux manières différentes que -3 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si X^2+X+1 possède une racine dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si X^3-1 y est scindé [4].

Remarque : on pourra considérer le discriminant du polynôme, ou bien s'inspirer de l'identité $2e^{2i\pi/3} = -1+i\sqrt{3}$ *valable dans* $\mathbb{C}$.

2. En déduire que -3 est un carré modulo p si et seulement si $p=2,3$ ou si $p\equiv 1$ [3].
3. En s'inspirant de l'égalité $e^{2i\pi/8}+e^{-2i\pi/8}$ dans $\mathbb{C}$, démontrer que 2 est un carré modulo p dès lors que $p\equiv 1$ [8].

Nous finissons l'exercice par l'analyse d'un cas particulier. Nous supposons que $p=2^m-1$ pour un entier $m\geq 3$.

4. Donner un exemple de tel premier, puis démontrer que m doit être premier.
5. Démontrer que -3 et 2 sont des carrés. Ceci prouve en particulier que la question 3 n'est pas une équivalence [5]. Quels carrés se trouvent parmi 3 et 6 ?

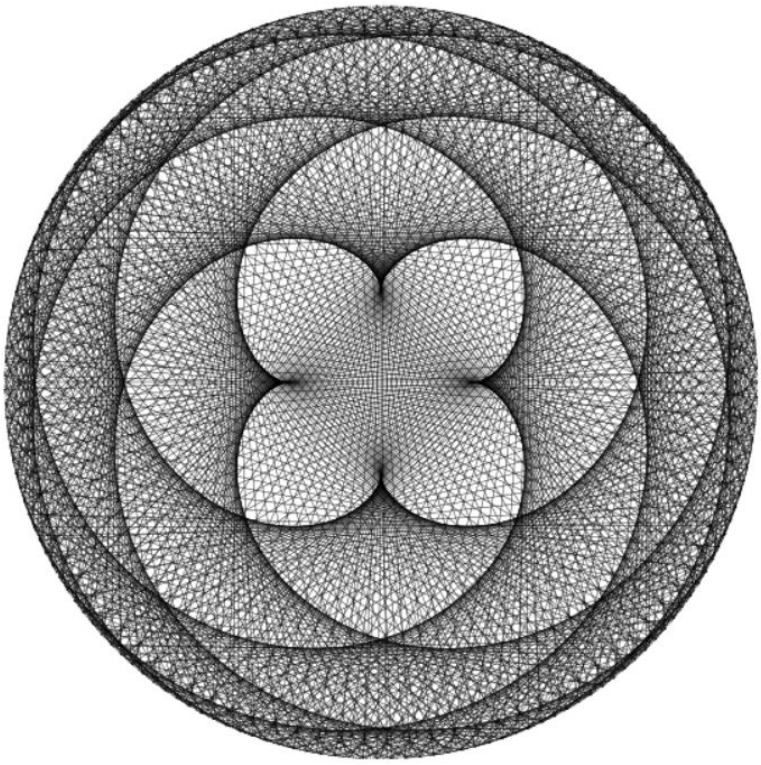

FIGURE 1 – Puissance $702^{\text{iéme}}$ appliquée aux racines 1002-ièmes.

4. Cela signifie qu'il se factorise comme produit de polynômes de degré 1.
5. L'exercice 2.20 du polycopité répond complètement à la question du symbole de Legendre de 2.