École Normale Supérieure, Année 2021-2022

1e année, Algèbre 1

TD n° 2 : Exemples de groupes

`À faire en priorité : 1 - 2 - 3 - 4 - 12 - 13 - 14`
`Ensuite : 16 -17 - 18 - 5`

La fin de la feuille comprend, un formulaire et quelques définitions.

1 Échauffement

Exercice 1.

Montrer que tout sous-groupe de type fini de $\mathbb{Q}$ est de la forme $\lambda\mathbb{Z} \subset \mathbb{Q}$ pour $\lambda \in \mathbb{Q}$.

Exercice 2.

Soient a et b des entiers avec $a, b \geqslant 3$. On pose $\zeta_n = e^{2i\pi/n}$ pour $n \geqslant 1$ et l'on considère les éléments A, B et $U(t)$ de $\mathrm{SL}_2(\mathbb{C})$ définis par

$$A \coloneqq \begin{bmatrix} \zeta_a & 0 \\ 0 & \zeta_a^{-1} \end{bmatrix}, \; B \coloneqq \begin{bmatrix} 0 & -1 \\ 1 & \zeta_b + \zeta_b^{-1} \end{bmatrix}, \; U(t) \coloneqq \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}.$$

1. Montrer que $C \in \mathrm{SL}_2(\mathbb{C})$ est d'ordre a si, et seulement si $\mathrm{tr}(C) = \zeta + \zeta^{-1}$ pour ζ une racine primitive a-ième de l'unité.
2. Montrer que A est d'ordre a, et que B est d'ordre b, dans le groupe $\mathrm{SL}_2(\mathbb{C})$.
3. On pose $B(t) \coloneqq U(t)BU(t)^{-1}$. Calculer la trace de $AB(t)$.
4. On suppose $c \geqslant 3$ entier, ou $c = \infty$. Montrer que pour t bien choisi, le produit $AB(t)$ est d'ordre c.
5. En travaillant dans $\mathbb{Z}/p\mathbb{Z}$ pour $p \equiv 1 \bmod abc$ (avec p premier), à la place du corps $\mathbb{C}$, montrer que pour tous entiers $a, b, c \geqslant 3$, il existe un groupe fini possédant un élément d'ordre a, un autre d'ordre b, de produit d'ordre c.

Exercice 3. Le symbole de Legendre

Soient p un nombre premier impair et $a \in \mathbb{Z}$ premier à p.

1. En utilisant l'application $x \mapsto a/x$, montrer
$$(p-1)! \equiv -\left(\frac{a}{p}\right) a^{(p-1)/2} \bmod p.$$
2. En déduire
$$(p-1)! \equiv -1 \bmod p \text{ \textit{(théorème de Wilson)}}, \; \left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p \text{ \textit{(congruence d'Euler)}}.$$
3. Retrouver $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ pour tout $a, b \in \mathbb{Z}$.

Exercice 4.

Soit p un nombre premier.

1. Montrer que pour $p \equiv 1 \bmod 4$, et $x = \left(\frac{p-1}{2}\right)!$, on a $x^2 \equiv -1 \bmod p$.
2. En considérant le polynôme $X^2 + X + 1$, montrer que -3 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si, et seulement si, on a $p \equiv 1 \bmod 3$ ou $p = 3$.
3. En déduire une condition nécessaire et suffisante sur p pour que 3 soit un carré dans $\mathbb{Z}/p\mathbb{Z}$.
4. *(Euler)* On suppose $p \equiv 1 \bmod 8$. En s'inspirant de l'écriture $\sqrt{2} = e^{2i\pi/8} + e^{-2i\pi/8}$ dans $\mathbb{C}$, montrer que 2 est un carré dans $\mathbb{Z}/p\mathbb{Z}$.

Exercice 5. Vrai-faux

Soit G un groupe. Vrai ou faux ?

1. Si tous les sous-groupes strictes de G sont monogènes alors G est monogène.
2. Si G a un nombre fini de sous-groupes, alors G est fini.
3. Soient x et $y \in G$ d'ordre fini, alors xy est d'ordre fini.
4. Le sous-ensemble $\mathrm{Int}(G) \subset \mathrm{Aut}(G)$ des automorphismes intérieurs est un sous-groupe.

2 Monoïdes

Exercice 6. Quelques cas où l'existence des inverses est automatique

1. Un monoïde M est dit *régulier* si pour tout $x, y, z \in M$, on a $xy = xz \implies y = z$. Montrer qu'un monoïde régulier fini est un groupe.
2. Montrer que si G est un groupe fini, et si H est une partie de G, alors H est un sous-groupe si, et seulement si, H est non vide et stable par produits.
3. Un anneau A est dit *intègre* si pour tout $a, b \in A$ on a $ab = 0 \implies a = 0$ ou $b = 0$. Montrer qu'un anneau intègre fini est à division.

Exercice 7. Monoïdes monogènes

Un monoïde M est dit monogène s'il existe $m \in M$ tel que $M = \{m^n \,;\, n \in \mathbb{N}\}$. Montrer que pour tout entier $n \geqslant 1$ il existe, à isomorphisme près, exactement n monoïdes monogènes M avec $|M| = n$.

Exercice 8. Monoides de cardinal $\leqslant 3$

1. Montrer qu'à isomorphisme près, il existe exactement 2 monoïdes de cardinal 2, à savoir $(\mathbb{Z}/2\mathbb{Z}, +)$ et $(\mathbb{Z}/2\mathbb{Z}, \times)$.
2. Soit M un monoïde à 3 éléments. Montrer que soit M est monogène, soit on a $M \simeq (\mathbb{Z}/3\mathbb{Z}, \times)$, soit on a $x^2 = x$ pour tout $x \in M$.
3. En déduire qu'à isomorphisme près, il existe exactement 7 monoïdes de cardinal 3.

3 Généralités sur les groupes

Exercice 9.

Soit G un groupe fini de cardinal $n \geqslant 1$. Montrer[1] $|\mathrm{Hom}(G, G)| \leqslant n^{\log_2(n)}$.

[1] On pourra commencer par expliquer que pour $g_1, \ldots, g_r \in G$ une famille génératrice un morphisme $\varphi\colon G \to G$ est déterminé par la famille $\varphi(g_1), \ldots, \varphi(g_r) \in G$. Il faudra ensuite en construire une adaptée...

Exercice 10. Propriétés universelles des groupes monogènes

1. Montrer que pour tout groupe G, l'application $\mathrm{Hom}(\mathbb{Z}, G) \to G$ donnée par $\varphi \mapsto \varphi(1)$, est bijective.
2. Soit $N \geqslant 1$. Montrer que pour tout groupe G, l'application $\mathrm{Hom}(\mathbb{Z}/N\mathbb{Z}, G) \to G$ donnée par $\varphi \mapsto \varphi(\overline{1})$, est injective d'image $\{g \in G \mid g^N = 1\}$.
3. Dans le cas où G est abélien, vérifier que les deux applications ci-dessus sont des morphismes de groupes[2].
4. Pour G et G deux groupes monogènes, déterminer la structure du groupe $\mathrm{Hom}(G, G')$.

Exercice 11. Propriété universelle des produits

Soit $\{G_i\}_{i\in I}$ une famille de groupes. Définissons le couple du groupe produit muni de ses projections i.e. $P \coloneqq \prod_{i\in I} G_i$ et pour $i \in I$ on définit $\pi_j \colon P \to G_j$ par $(g_i)_i \mapsto g_j$. Vérifier $\pi_j \in \mathrm{Hom}(P, G_j)$ puis montrer que pour tout groupe H, la pré-composition par les π_j définie bien une bijection

$$\begin{array}{ccc} \mathrm{Hom}(H, P) & \xrightarrow{\sim} & \prod_{i\in I} \mathrm{Hom}(H, G_i) \\ f & \longmapsto & (\pi_i \circ f)_{i\in I} \end{array}$$

Tout comme le problème universel du quotient d'un ensemble par une relation, définir le problème universel du produit d'une famille de groupe sur I dont $(P, \{\pi\}_{i\in I})$ est une solution. Déterminer dans quelle mesure cette solution est unique.

Exercice 12.

Soient G un groupe, et $H \subset K$ deux sous-groupes de G. Montrer

$$[G \colon K] = [G \colon H] \cdot [H \colon K] \in \mathbb{N} \sqcup \{\infty\}.$$

En particulier si deux des trois indices sont finis, le troisième l'est aussi.

4 Groupes cycliques

Exercice 13. Lemme chinois

Soit $n, m \in \mathbb{N}$ deux entiers premier entre eux. Montrer que pour tout couple $(k_1, k_2) \in \mathbb{N}^2$ l'équation

$$\begin{cases} x \equiv k_1 \bmod n \\ x \equiv k_2 \bmod m, \end{cases}$$

admet une unique solution entière telle que $1 \leqslant x \leqslant nm$. En déduire un isomorphisme naturel d'anneaux $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/nm\mathbb{Z}$ puis montrer $\varphi(nm) = \varphi(m)\varphi(n)$ où $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$.

Exercice 14.

Le but de cet exercice est de déterminer, pour tout entier n, la structure du groupe des inversibles $(\mathbb{Z}/n\mathbb{Z})^\times$. L'isomorphisme de $(\mathbb{Z}/nm\mathbb{Z})^\times \cong (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$ pour n et m deux entiers premiers entre eux nous permet de se ramener au cas $n = p^k$. En particulier, on veut montrer pour $k \geqslant 2$ un entier et p un nombre premier impair

$$(\mathbb{Z}/p^k\mathbb{Z})^\times \cong \mathbb{Z}/\varphi(p^k)\mathbb{Z} \text{ puis que } (\mathbb{Z}/2^k\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/2^{k-2}\mathbb{Z}).$$

1. Montrer, sans utiliser le résultat, que $(\mathbb{Z}/187\mathbb{Z})^\times$ n'est pas cyclique puis qu'il est isomorphe au produit de deux groupes cycliques.
2. Montrer que $(\mathbb{Z}/p^k\mathbb{Z})^\times$ contient un élément[3] d'ordre $p-1$.

[2] pour la loi introduite en cours sur $\mathrm{Hom}(H, G)$ quand G est abélien

[3] *Indication* : On pourra considérer $a \in \mathbb{Z}$ dont la classe engendre $(\mathbb{Z}/p\mathbb{Z})^\times$

3. Montrer pour tout entier $k \geqslant 1$, $\forall a, b \in \mathbb{Z},\ a \equiv b \bmod p^k \implies a^p \equiv b^p \bmod p^{k+1}$. En déduire l'ordre de $\overline{(1+p)} \in (\mathbb{Z}/p^k\mathbb{Z})^\times$.

4. Conclure si $p \neq 2$.

5. Traiter le cas[4] $p = 2$.

6. En guise d'application, déterminer les entiers $n \in \mathbb{N}$ tels que $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique.

Exercice 15. Le théorème de Wilson revisité

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

$$x \coloneqq \sum_{g \in G} g.$$

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 une nouvelle preuve du *théorème de Wilson* : pour tout nombre premier p,

$$(p-1)! \equiv -1 \bmod p.$$

5 Sous-groupes $\mathbb{C}$ et $\mathbb{C}^\times$

Exercice 16. Sous-groupes de $\mathbb{R}$

1. Montrer que tout sous-groupe stricte de $\mathbb{R}$ est fermé si, et seulement si, il est monogène.

2. (*Kronecker*) Montrer que si $\alpha \in \mathbb{R} \smallsetminus \mathbb{Q}$, alors $\mathbb{Z} + \mathbb{Z}\alpha$ est dense dans $\mathbb{R}$.

3. Montrer que la suite $(\cos n)_{n \geqslant 1}$ est dense dans $[-1, 1]$.

4. Montrer que tout sous-groupe strict de $\mathbb{U}(1)$ est fermé si, et seulement s'il est cyclique.

Exercice 17. Caractères de $\mathbb{U}(1)$

Soit $\mathbb{U}(1) \subset \mathbb{C}^\times$ le sous-groupe des complexes de norme 1 i.e. $\mathbb{U}(1) \coloneqq \{z \in \mathbb{C} \mid |z| = 1\}$

1. Montrer que tout morphisme continu $\mathbb{R} \to \mathbb{C}$ est de la forme $x \mapsto \alpha x$ avec $\alpha \in \mathbb{C}$. Est-ce encore vrai sans l'hypothèse de continuité ?

2. Montrer que tout morphisme continu $f \colon \mathbb{R} \to \mathbb{C}^\times$ est de classe $\mathscr{C}^\infty$. En déduire[5] que f est de la forme $x \mapsto \exp(\alpha x)$ pour $\alpha \in \mathbb{C}$.

3. En déduire que tout morphisme continu $\mathbb{U}(1) \to \mathbb{C}^\times$ est de la forme $z \mapsto z^n$ avec $n \in \mathbb{Z}$.

4. Soit α un réel. Montrer que $\alpha \in \mathbb{Q}$ si, et seulement si, $\exp(2i\pi\alpha) \in \mathbb{U}(1)$ est d'ordre fini.

Exercice 18. Sous-groupes de $\mathbb{Q}$

Soit $\mathcal{S}$ l'ensemble des entiers surnaturels muni de $\iota \colon \mathbb{N} \to \mathcal{S}$ et ordonné pour la relation de divisibilité.

1. Montrer que l'on a $n \mid m$ dans $\mathbb{N}$ si, et seulement si, $\iota(n) \mid \iota(m)$.

2. Montrer que toute partie de $(\mathcal{S}, |)$ admet une borne supérieure dans $\mathcal{S}$.

Pour $s \in \mathcal{S}$ on note $H_s \subset \mathbb{Q}$ le sous-ensemble des a/b avec $a \in \mathbb{Z}$ et $b \geqslant 1$ tels que $\iota(b) \mid s$. On se propose de montrer que $s \mapsto H_s$ est une bijection de $\mathcal{S}$ sur l'ensemble des sous-groupes de $\mathbb{Q}$ contenant $\mathbb{Z}$.

1. Montrer que H_s est un sous-groupe de $\mathbb{Q}$ contenant $\mathbb{Z}$, et que l'on a $H_s \subset H_{s'} \iff s \mid s'$. Décrire $H_{\iota(n)}$ pour $n \in \mathbb{N}$.

[4] *Indication* : Calculer l'ordre de $\overline{5} \in (\mathbb{Z}/2^k\mathbb{Z})^\times$ pour $k \geqslant 2$.

[5] Rappelons le *théorème de relèvement* qui peut aussi être utilisé pour conclure : Toute application continue $f \colon \mathbb{R} \to \mathbb{C}^\times$ est de la forme $\exp(g)$ avec $g \colon \mathbb{R} \to \mathbb{C}$ continue.

2. Soit H est un sous-groupe de $\mathbb{Q}$ contenant $\mathbb{Z}$. Pour $n, m \in \mathbb{Z}$ premiers entre eux montrer

$$\frac{n}{m} \in H \iff \frac{1}{n} \in H.$$

3. Conclure.

Exercice 19. Théorème de Dirichlet faible

Soit $n \geqslant 1$ un entier. On se propose de montrer qu'il existe une infinité de nombres premiers $p \equiv 1 \bmod n$. On considère le n-ième polynôme cyclotomique

$$\Phi_n = \prod_{\substack{1 \leqslant k < n \\ (k,n)=1}} (X - e^{2ik\pi/n}).$$

C'est un polynôme unitaire de degré $\varphi(n)$ dans $\mathbb{C}[X]$.

1. Montrer $X^n - 1 = \prod_{d|n} \Phi_d$, et en déduire[6] $\Phi_n \in \mathbb{Z}[X]$.
2. Montrer que si k est un corps dans lequel $n \cdot 1 \neq 0$, le polynôme $X^n - 1$ n'a pas de racine double dans k. Puis, en déduire qu'un élément $x \in k^\times$ et d'ordre n si, et seulement si, $\Phi_n(x) = 0$.
3. Montrer que pour tout polynôme $P \in \mathbb{Z}[X]$ non constant, l'ensemble des nombres premiers divisant l'un des entiers $P(n)$ avec $n \in \mathbb{Z}$, est infini.
4. Conclure.

6 Rappels et définitions

6.1 Notations et définitions pour les exercices

- On note $\mathcal{P}$ l'ensemble des nombres premiers.
- Rappelons qu'on définit le *symbole de Legendre* $\left(\frac{a}{p}\right) \in \{+1, -1\}$ pour p premier et $a \in \mathbb{Z},\ (a,p) = 1$ par

$$\left(\frac{a}{p}\right) \coloneqq \begin{cases} +1 & \text{si } \overline{a} \text{ est un carré modulo } p \\ -1 & \text{si } \overline{a} \text{ n'est pas un carré modulo } p \end{cases}$$

- Rappelons qu'on défini pour tout $p \in \mathcal{P}$ *la valuation p-adique* $\mathrm{v}_p \colon \mathbb{Q} \to \mathbb{Z} \sqcup \{\infty\}$ défini pour $x \in \mathbb{Z}$ par $\mathrm{v}_p(x) = \sup\{k \in \mathbb{N} \mid p^k \mid x\} \in \mathbb{N} \sqcup \{\infty\}$ étendue à $\mathbb{Q}$ par son caractère multiplicatif i.e. $\mathrm{v}_p(xy) = \mathrm{v}_p(x) + \mathrm{v}_p(y)$. Remarquez que la donnée de la famille $\{\mathrm{v}_p\}_{p\in\mathcal{P}}$ est équivalente à la décomposition en facteurs premiers de tout entier $x \in \mathbb{N}$ puisque $x = \prod_{p\in\mathcal{P}} p^{\mathrm{v}_p(x)}$.
- Suivant Steinitz, on appelle *entier surnaturel* toute collection $s = (s_p)_{p\in\mathcal{P}}$ telle que pour tout premier p on a $s_p \in \mathbb{N} \sqcup \{\infty\}$. On note $\mathcal{S}$ l'ensemble des entiers surnaturels. Un entier surnaturel est parfois noté suggestivement $\prod_{p\in\mathrm{P}} p^{s_p}$, en omettant éventuellement les exposants nuls, par exemple on a $2^\infty\, 3\, 5^\infty \in \mathcal{S}$. Par ce qui précède, on dispose d'une injection naturelle $\iota \colon \mathbb{N} \to \mathcal{S}$ donnée par $\iota \colon n \in \mathbb{N} \mapsto (\mathrm{v}_p(n))_{p\in\mathcal{P}}$. De plus, on munit l'ensemble $\mathcal{S}$ de la relation d'ordre qui étend naturellement la relation de divisibilité sur $\mathbb{N}$ et qui est définie par

$$\forall s, s' \in \mathcal{S},\ \left[s \mid s' \iff \forall p \in \mathrm{P},\ s_p \leqslant s'_p\right].$$

[6] On rappelle que si on a $P, Q \in \mathbb{Z}[X]$ avec Q unitaire, on dispose d'une *division euclidienne* $P = AQ + B$ avec $A, B \in \mathbb{Z}[X]$ et $\deg B < \deg Q$.

6.2 Formulaire de calcul dans les groupes

Soient x, y, z des éléments d'un groupe G et n, m des entiers positifs, on vérifie aisément les propriétés de calcul suivantes :

$$x^{n+m} = x^n x^m \quad \text{et} \quad \left(x^n\right)^m = x^{nm} \quad (\textit{lois des puissances})$$

$$\left(x^{-1}\right)^n = \left(x^n\right)^{-1} \quad \text{et} \quad (xy)^{-1} = y^{-1}x^{-1} \quad (\textit{lois des inverses})$$

$$xy = xz \implies y = z \quad \text{et} \quad yx = zx \implies y = z \quad (\textit{simplification})$$

$$xy = z \implies y = x^{-1}z \quad \text{et} \quad xy = z \implies x = zy^{-1} \quad (\textit{ bascule})$$