1e année, Algèbre 1

TD n° 4 : Notes et corrections

Exercice 1. Échauffements

Les questions sont indépendantes.

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.
2. Faire la liste des groupes abéliens de cardinal 360.
3. Déterminer tous les sous-groupes de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.
4. Déterminer, à isomorphisme près, tous les groupes abéliens G possédant un sous-groupe H tel que $H \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong G/H$.

Correction exercice 1

1. Les deux groupes sont d'ordre $27000 = 2^3 \cdot 3^3 \cdot 5^3$ et les diviseurs élémentaires sont $2 \cdot 3 \cdot 5 = 30$ et $30^2 = 900$.
2. On décompose $360 = 2^3 \cdot 3^2 \cdot 5$ pour raisonner sur les facteurs invariants. S'il n'y en a qu'un seul, c'est le groupe cyclique d'ordre 360. Supposons qu'il y en ait deux $\lambda_1 \mid \lambda_2$ et $\lambda_1\lambda_2 = 360$, donc $\lambda_2 = 5 \cdot 3^i \cdot 2^j$ avec $i = 1, 2$ et $j = 2, 3$ et $(i, j) \neq (2, 3)$ ce qui donne 3 possibilités :
$$\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/60\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/180\mathbb{Z},\quad \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/120\mathbb{Z}.$$
Il y a au plus 3 diviseurs élémentaires. Dans ce cas $\lambda_1 \mid \lambda_2 \mid \lambda_3$ avec $\lambda_1\lambda_2\lambda_3 = 360$. Ainsi $\lambda_1 = 2$ donc nécessairement $\lambda_3 = 5 \cdot 3^i \cdot 2$ où $i = 1, 2$ ce qui donne les 2 dernières possibilités :
$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/90\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/30\mathbb{Z},$$
On trouve 6 groupes abéliens non-isomorphes.
3. Le groupe est de cardinal $8 = 2^3$ et ses diviseurs élémentaires sont $2 \mid 4$.On raisonne sur les ordres des éléments non-triviaux qui sont 2 ou 4. Soit (x, y) un élément d'ordre 4. Alors $x = 1 \implies y = 1, 3$ sinon il serait d'ordre 2 donc on a deux sous-groupes cycliques d'ordre 4 soit celui engendré par $(1, 1)$ et celui engendré par $(0, 1)$. Il y a donc 3 éléments d'ordre 2 et on reconnait le groupe de Klein $\mathbb{Z}/2\mathbb{Z} \times 2\mathbb{Z}/4\mathbb{Z}$ qui lui même contient 3 sous-groupes d'ordre 2 engendrés par $(1, 2)$, $(0, 2)$, $(1, 0)$. Ce qui nous fait un total de huit sous-groupes : trois d'ordre 4 dont deux cycliques et trois d'ordre 2, le sous-groupe trivial et le groupe lui même.
4. On a $|G| = [G : H] \cdot |H| = 16 = 2^4$ et on peut raisonner sur les diviseurs élémentaires. Remarquons que G ne peut pas contenir d'élément d'ordre 8 : si c'était le cas, on aurait un élément d'ordre 8 qui serait nécessairement d'ordre 2 modulo H mais dont le carré serait aussi d'ordre 2 modulo H. Les diviseurs élémentaires sont donc $2 \mid 2 \mid 4$, $4 \mid 4$ et $2 \mid 2 \mid 2 \mid 2$ ce qui donne
$$G = (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/4\mathbb{Z},\ (\mathbb{Z}/4\mathbb{Z})^2, (\mathbb{Z}/2\mathbb{Z})^4, \text{par ex. } H = \langle(1,0,0),(0,0,2)\rangle, \langle(2,0),(0,2)\rangle\langle(1,0,0,0),(0,1,0,0)\rangle.$$

Exercice 2.

Soit G un groupe abélien.

1. Soient $m, n \in \mathbb{Z}$ premiers entre eux. Montrer $G[mn] = G[n] \oplus G[m]$.
2. Supposons G fini. Montrer que si G n'est pas cyclique, il existe un nombre premier p tel que G contienne un sous-groupe isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.
3. Calculer $\mathrm{g}(n)$, le nombre de groupe abéliens non-isomorphes d'ordre $n \in \mathbb{N}$. On pourra commencer par montrer $\forall n, m \in \mathbb{N}$, $(n, m) = 1 \implies \mathrm{g}(nm) = \mathrm{g}(n)\mathrm{g}(m)$ puis obtenir pour p premier $\mathrm{g}(p^k) = \mathrm{p}(k)$, le *nombre de partitions* de l'entier k.

Correction exercice 2

1. On a $G[n]+G[m]\subset G[nm]$. Par Bezout on trouve $u,v\in\mathbb{Z}$ tel que $un+vm=1$ et donc $z=\underbrace{vmz}_{\in G[n]}+\underbrace{unz}_{\in G[m]}$ d'où l'inclusion réciproque. Finalement, si $z\in G[n]\cap G[m]$ alors par la décomposition précédente, $z=0+0$ et donc $G[n]\oplus G[m]=G[nm]$.

2. Si G est abélien fini il est déterminé par ses diviseurs élémentaires. Comme il n'est pas monogène, il en possède au moins deux : $\lambda_1\mid\lambda_2$. Il existe p premier tel que $p\mid\lambda_1$ et a donc $p\mid\lambda_2$. Par le théorème de structure on a $\mathbb{Z}/\lambda_1\mathbb{Z}\times\mathbb{Z}/\lambda_2\mathbb{Z}\subset G$ et donc on a le sous-groupe voulu : $\frac{\lambda_1}{p}\mathbb{Z}/\lambda_1\mathbb{Z}\times\frac{\lambda_2}{p}\mathbb{Z}/\lambda_2\mathbb{Z}\cong\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$.

3. Soit n fixé, $n=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ sa décomposition en facteurs premiers. La première question nous assure que si G est d'ordre n alors $G\cong\bigoplus_{i=1}^r G[p_i^{\alpha_i}]$ et donc $\mathrm{g}(n)=\mathrm{g}(p_1^{\alpha_1})\cdots\mathrm{g}(p_r^{\alpha_r})$. Comptons les classes d'isomorphisme de groupes abéliens d'ordre p^k. D'après la classification des groupes abéliens finis, ces classes d'isomorphismes sont déterminées par les diviseurs élémentaires $\lambda_1\mid\lambda_2\mid\cdots\mid p^k$ dont le produit est p^k. Ainsi, $\lambda_i=p^{k_i}$ vérifiant $k_1\leqslant k_2\leqslant\cdots\leqslant k_j$ et $k_1+k_2+\ldots k_j=k$, ce qui donne bien une partition de k. Réciproquement une telle partition détermine les diviseurs élémentaires, ce qui permet de conclure que $g(p^k)=p(k)$ et finalement
$$\mathrm{g}(n)=\mathrm{p}(\alpha_1)\cdots\mathrm{p}(\alpha_r).$$

Exercice 3. Cercle modulo p

Soit p un nombre premier $\neq 2$, soit $C=\{(x,y)\in(\mathbb{Z}/p\mathbb{Z})^2\mid x^2+y^2=1\}$. Montrer $\mathrm{J}(\chi,\chi^{-1})=-\chi(-1)$ pour tout $\chi\in\widehat{(\mathbb{Z}/p\mathbb{Z})^\times}$ tel que $\chi\neq 1$. En déduire $|C|=p-(-1)^{\frac{p-1}{2}}$.

Correction exercice 3

Calculons la somme de Jacobi :
$$\mathrm{J}(\chi,\chi^{-1})=\sum_{\substack{x,y\in(\mathbb{Z}/p\mathbb{Z})\\x+y=1}}\underbrace{\chi(x)\chi^{-1}(y)}_{=\chi(\frac{x}{y})}=\sum_{\substack{x\in(\mathbb{Z}/p\mathbb{Z})\\x\neq1}}\chi\left(\frac{x}{1-x}\right).$$
Remarquons alors que l'homographie $x\mapsto\left(\frac{1-x}{x}\right)=\left(\frac{1}{x}-1\right)$ est une bijection de $\mathbb{Z}/p\mathbb{Z}-\{0\}$, sur $\mathbb{Z}/p\mathbb{Z}-\{-1\}$, ce qui permet d'écrire la somme comme
$$\mathrm{J}(\chi,\chi^{-1})=\sum_{x\in(\mathbb{Z}/p\mathbb{Z})}\chi(x)-\chi(-1).$$
La somme est nulle car $\chi\neq1$ et on en déduit $\mathrm{J}(\chi,\chi^{-1})=-\chi(-1)$. Notons $\chi_2\colon x\mapsto\left(\dfrac{x}{p}\right)$ le symbole de Legendre de $\mathbb{Z}/p\mathbb{Z}$. On raisonne comme dans le cours pour écrire
$$|C|=\sum_{\substack{a,b\in(\mathbb{Z}/p\mathbb{Z})\\a+b=1}}\mathrm{N}(x^2=a)\mathrm{N}(y^2=b)=\underbrace{\mathrm{J}(1,1)}_{=p-2}+\underbrace{\mathrm{J}(1,\chi_2)+\mathrm{J}(\chi_2,1)}_{=2}+\underbrace{\mathrm{J}(\chi_2,\chi_2)}_{=-\chi_2(-1)}.$$
Comme $\chi_2(-1)=(-1)^{\frac{p-1}{2}}$ on conclut qu'on a bien $|C|=p-(-1)^{\frac{p-1}{2}}$.

Exercice 4.

Soit G un groupe abélien fini. Soit $d\mid|G|$, montrer que G contient un sous-groupe d'ordre d.

Correction exercice 4

À tout groupe abélien fini G on associe la décomposition en facteurs premiers de son ordre $|G|=\prod_{p\in\mathcal{P}}p^{\mathrm{v}_p(G)}$. On raisonne par récurrence sur $\sum_{p\in\mathcal{P}}\mathrm{v}_p(G)$: soit $p\in\mathcal{P}$ premier. On sait d'après le lemme de Cauchy que si $p\mid|G|$ alors G contient un sous-groupe d'ordre p, notons le $C_p\subset G$. Comme G est abélien on peut passer au quotient et obtenir G/C_p, un groupe d'ordre $\frac{n}{p}$ dont les sous-groupes correspondent aux sous-groupes de G contenant C_p. Supposons que l'hypothèse est vérifiée pour G/C_p, sachant qu'on l'a vérifié pour les groupes d'ordre premier. Alors pour $d\mid|G|$, soit $p\mid d$, alors on sait que G/C_p contient un sous-groupe d'ordre $\frac{d}{p}$ et on en conclut que G contient un sous-groupe d'ordre d.

Exercice 5.

1. Soit G un groupe tel que $g^2 = 1$ pour tout $g \in G$. Montrer que G est abélien, puis $G \cong (\mathbb{Z}/2\mathbb{Z})^{(I)}$ pour un certain ensemble I.
2. Montrer que le sous-ensemble des *matrices unipotentes* $\mathrm{U}_n(k)$ est un sous-groupe de $\mathrm{GL}_n(k)$ pour $n \geqslant 1$ et k un corps.
3. Soit p un nombre premier. On suppose $p \geq n$. Montrer $g^p = 1$ pour tout $g \in \mathrm{U}_n(\mathbb{Z}/p\mathbb{Z})$.
4. En déduire que pour $p > 3$ premier, il existe un groupe non abélien G d'ordre p^3 tel que $g^p = 1$ pour tout $g \in G$.

Correction exercice 5

1. Soit $G \to G$ l'application donnée par l'inverse $g \mapsto g^{-1}$; on sait que le groupe est abélien si, et seulement si, cette application est un morphisme. Si pour tout $g \in G$ on a $g^2 = e$, alors l'application d'inversion est l'identité donc G est abélien. Plus formellement, soit $g_1, g_2 \in G$, alors $g_1 g_2 = g_1^{-1} g_2^{-1} = (g_2 g_1)^{-1} = g_2 g_1$, qui est en réalité le même argument. On a donc montré que G est un $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel. On sait que tout espace vectoriel possède une base, donc on peut se donner une base de G indexé par un ensemble I. Ainsi, on obtient un isomorphisme $G \cong (\mathbb{Z}/2\mathbb{Z})^{(I)}$ de $\mathbb{Z}/2\mathbb{Z}$-espaces vectoriels et donc de groupes abéliens.
2. Pour tout $A \in \mathrm{U}_n(k)$, notons $N_A \coloneqq A - \mathrm{id}_n$ qui est une matrice triangulaire supérieure stricte. Notons que ces matrices forment un anneau. Soit $A, B \in \mathrm{U}_n(k)$, alors on veut montrer que $A^{-1}B \in \mathrm{U}_n(k)$. Soit N_A et N_B triangulaires supérieures strictes et tels que $A = \mathrm{id}_n + N_A$ et $B = \mathrm{id}_n + N_B$, alors

$$A^{-1}B = \left(\mathrm{id}_n + \underbrace{\left(\sum_{k=1}^{n} (-N_A)^n \right)}_{=N_{A^{-1}}} \right) (\mathrm{id}_n + N_B) = \mathrm{id}_n + \underbrace{N_{A^{-1}} + (N_{A^{-1}} + \mathrm{id}_n) N_B}_{=N_{A^{-1}B}} = \mathrm{id}_n + N_{A^{-1}B} \in \mathrm{U}_n(k).$$

3. Soit $g = \mathrm{id}_n + \mathrm{j}(g)$, on calcule

$$g^p = (\mathrm{id}_n + \mathrm{j}(g))^p = \mathrm{id}_n + \sum_{k=1}^{p-1} \underbrace{\binom{p}{k}}_{\equiv 0} \mathrm{j}(g)^k + \mathrm{j}(g)^p = \mathrm{id}_n + \mathrm{j}(g)^p = \mathrm{id}_n,$$

   en effet $\mathrm{j}(g)^p = \mathrm{j}(g)^{p-n}\mathrm{j}(g)^n = 0$ par son caractère nilpotent. On peut noter que pour $A, B \in \mathrm{M}_n(\mathbb{Z}/p\mathbb{Z})$ deux matrices qui commutent on a plus généralement $(A+B)^p = A^p + B^p$.
4. On pose $n = 3$, $\mathrm{U}_3(\mathbb{Z}/p\mathbb{Z})$ est non-abélien et on vient de vérifier que tout élément non-trivial est d'ordre p puisque $p > 3$. C'est le *groupe d'Heisenberg*, qui est d'une grande importance autant en physique quantique qu'en mathématiques.

Exercice 7. Exemples de groupes divisibles

1. Montrer que $\mathbb{Q}$ est un groupe injectif. De même, justifier que $\mathbb{Q}/\mathbb{Z}$ est injectif mais de torsion.
2. Montrer que pour les *p-groupes de Prüfer* on a un isomorphisme $\mathbb{Z}\left[\frac{1}{p}\right]/\mathbb{Z} \cong \mu_{p^\infty}$.
3. Montrer la décomposition $\mathbb{Q}/\mathbb{Z} = \bigoplus_{p \in \mathcal{P}} \mathbb{Z}\left[\frac{1}{p}\right]/\mathbb{Z}$. Conclure que $\mathbb{Q}/\mathbb{Z} \cong \mathbb{U}(1)_{\mathrm{tors}}$.
4. Montrer que tout groupe abélien fini se *plonge* dans une somme de $\mathbb{Q}/\mathbb{Z}$.

Correction exercice 7

1. Traitons l'injectivité de $\mathbb{Q}$, celle de $\mathbb{Q}/\mathbb{Z}$ est similaire. Soit $\iota \colon A \to B$ une injection de groupes abéliens. Soit $f \colon A \to \mathbb{Q}$ un morphisme et soit $b \in B \setminus \iota(A)$. On veut étendre f en $\tilde{f} \colon A_b \to \mathbb{Q}$ où A_b est le sous-groupe de B engendré par $\iota(A)$ et b. On a deux cas :
   - supposons qu'il existe $n \in \mathbb{N}$ tel que $nb \in \iota(A)$ et considérons le plus petit tel entier n. Posons $\tilde{f}(b) = \frac{1}{n} f(b^n)$ puis pour $x \in A_b$, que l'on représente de manière unique par $a + ub$ pour $u \in \mathbb{Z}$ tel que $0 \leqslant u \leqslant n-1$, $\tilde{f}(x) = f(a) + u\tilde{f}(b)$. On vérifie alors $\tilde{f} \colon A_b \to \mathbb{Q}$ est bien définie.

- Supposons le contraire, alors $\mathbb{Z} \to A_b$ donné par $1 \mapsto b$. L'image est un groupe monogène infini disjoint de A par hypothèse, donc $A_b = A \oplus b\mathbb{Z}$. Il suffit alors de poser $\tilde{f}(b) := 0$ et $\tilde{f}\colon A_b \to \mathbb{Q}$ est défini pour $a + ub \in A_b$ avec $a \in A, u \in \mathbb{Z}$ on obtient $\tilde{f}\colon A_b \to \mathbb{Q}$ défini par $\tilde{f}(a + ub) = f(a)$.

À l'aide du lemme de Zorn, on peut alors construire un prolongement maximal et utiliser ce qui précède pour conclure qu'un prolongement maximal est nécessairement un prolongement à B tout entier. La preuve est essentiellement la même pour $\mathbb{Q}/\mathbb{Z}$ qui est bien un groupe de torsion.

2. Il suffit de poser pour tout $n \geqslant 1$ l'application $\rho_n\colon \frac{1}{p^n}\mathbb{Z} \to \mathbb{U}(1)$ définie par $q \mapsto \exp(2i\pi q)$ sur le sous-groupe $\frac{1}{p^n}\mathbb{Z} \subset \mathbb{Q}$. L'image est $\mu_{p^n}(\mathbb{C})$ et le noyau $\mathbb{Z}$. On obtient en passant au quotient un isomorphisme $\frac{1}{p^n}\mathbb{Z}/\mathbb{Z} \xrightarrow{\sim} \mu_{p^n}(\mathbb{C})$. Il suffit ensuite de "passer à la limite" puisque comme on a bien $\rho_n\big|_{p^{-m}\mathbb{Z}} = \rho_m$ pour $m \leqslant n$ on définit simplement $\rho\colon \mathbb{Z}\left[\frac{1}{p}\right]/\mathbb{Z} \to \mu_{p^\infty}$ par $q \mapsto \exp(2i\pi q)$ qui vérifie pour tout $n \in \mathbb{N}$, $\rho\big|_{p^{-m}\mathbb{Z}} = \rho_m$ et qui définit une bijection. En effet, il suffit de vérifier l'injectivité et la surjectivité en utilisant que pour les deux groupes, tout élément est contenu dans un sous-groupe de torsion p-primaire fini. La construction sous-jacente est celle de la *limite inductive*. Remarquez qu'on aurait pu raisonner à l'aide du logarithme en utilisant l'injectivité d'un des deux groupes.
3. Il suffit d'utiliser que si G est un groupe de torsion alors $G = \bigoplus_{p\in\mathcal{P}} G[p^\infty]$ où $G[p^\infty] := \{x \in G \mid \exists n, p^n x = 0\}$. L'isomorphisme s'obtient alors en combinant cet argument et la question précédente.
4. Il suffit de montrer que tout groupe cyclique se plonge dans $\mathbb{Q}/\mathbb{Z}$. Soit C un groupe cyclique d'ordre n et soit $g \in C$ un générateur. Posons le caractère $\chi_g\colon C \to \mathbb{U}(1)$ défini par $g^k \mapsto \exp\left(\frac{2i\pi k}{n}\right)$. Il est injectif et son image est contenue dans $\mathbb{U}(1)_{\text{tors}}$. On compose avec l'isomorphisme $\mathbb{Q}/\mathbb{Z} \cong \mathbb{U}(1)_{\text{tors}}$ de la question précédente pour conclure.

Exercice 8. Objets injectifs et groupes divisibles

Soit G un groupe abélien.

1. Montrer qu'un groupe abélien est *injectif* si, et seulement s'il est *divisible*.
2. Montrer que tout groupe abélien se plonge dans un groupe injectif.
3. Montrer que tout groupe abélien divisible est somme directe de copies de $\mathbb{Q}$ et de *p-groupes de Prüfer*. En déduire le théorème de classification des groupes abéliens de type finis.

Correction exercice 8

1. Rappelons qu'il à été vu en cours que tout groupe abélien divisible est injectif (cf. proposition 2.7). Soit G un groupe injectif, montrons qu'il est divisible. Soit $y \in G$ on considère l'application $f_y\colon \mathbb{Z} \to G$ donnée par $f_y(1) = y$. On considère aussi $[n]\colon \mathbb{Z} \to \mathbb{Z}$ la multiplication par n, qui est injective. Alors, l'injectivité de G assure qu'il existe $h\colon \mathbb{Z} \to G$ tel que $h \circ [n] = f_y$. Ainsi pour $x = h(1)$ on a $nx = h(n) = f(1) = y$, ce qui montre ce qu'on voulait.
2. On sait d'après l'exercice précédent que c'est bien le cas pour les groupes abéliens finis. Soit H un groupe, considérons l'ensemble des couples $\{(N, \iota_N)\}$ où $N \subset H$ est un sous-groupe et $\iota_N\colon N \to D$ est une injection dans un groupe divisible D quelconque. Comme chaque chaine totalement ordonnée admet un majorant, on peut appliquer Zorn pour en déduire qu'il existe un élément maximal (N_1, ι_1). Supposons que cet élément n'est pas H tout entier, alors il existe $x \in H \setminus N_1$. Supposons qu'il existe $n \in \mathbb{N}$ tel que $nx \in N_1$, alors $n\iota_1(x) \in D$ et donc on peut définir $\iota(x) \in D$, ce qui donne une contradiction. Sinon $N_1 \oplus \underbrace{\langle x \rangle}_{\cong\mathbb{Z}}$ et on choisit $D \times \mathbb{Q}$ avec $x \mapsto 1 \in \mathbb{Q}$, ce qui contredit encore une fois la maximalité. Ainsi, H se plonge dans un groupe injectif par ι_1.
3. Soit G un groupe divisible. La première observation est qu'on a $G = G' \times G_{\text{tors}}$ où G' est sans torsion et G_{tors} est de torsion. De plus, on peut supposer que G est *simple* i.e. il ne contient pas de sous-groupe divisible strict : en effet, s'il en contient un, $G' \subsetneq G$, alors par l'injectivité on étend l'identité de G' en $G \to G'$ dont le noyau G'' vérifie $G = G' \oplus G''$. Un groupe abélien sans torsion contient un sous-groupe isomorphe à $\mathbb{Z}$ et par la divisibilité on en déduit qu'il contient un sous-groupe isomorphe à $\mathbb{Q}$, donc $G = \mathbb{Q}$ si G est simple sans torsion. S'il est de torsion, comme il est simple, il existe un premier p tel que $G = G_p$ et donc il contient un sous-groupe cyclique d'ordre p : mais alors la divisibilité permet d'obtenir un sous-groupe qui est un p-groupe de Prüfer, ce qui termine la preuve. Le détail de la dernière question est omis.