Algèbre 2 Partiel CORRIGE

Exercice 1 5=2+(1+2) points

1) Démontrer que les groupes multiplicatifs $(\mathbb{R}^*, \cdot)$ et $(\mathbb{C}^*, \cdot)$ ne sont pas isomorphes.

2) Soit H un sous–groupe du groupe $(G, \cdot)$ qui est de cardinal fini ou infini.

i) Rappeler la définition de l'indice de H dans G.

ii) Montrer que H est distingué dans G, si l'indice de H dans G est égal à 2.

1) Supposons que ces deux groupes soient isomorphes et soit f un isomorphisme de $(\mathbb{C}^*, \cdot)$ dans $(\mathbb{R}^*, \cdot)$. Posons $a = f(i)$. Alors $f(i^4) = a^4 = 1$ et donc $a^2 = 1$ puisque $a^2 > 0$. Alors on a $1 = a^2 = f(i^2) = f(-1)$ et $1 = f(1)$. Donc f n'est pas injectif, on a obtenu une contradiction.

2) L'indice de H dans G est, par définition, le cardinal $|G/H|$ de l'ensemble des classes latérales G/H. Si $|G/H| = 2$, il y a deux classes latérales à gauche $G = H \cup gH$ et deux classes latérales à droite $G = H \cup Hg$ avec $g \in G, g \notin H$. Donc pour tout $g \in G$, $g \notin H$ on a $gHg^{-1} = H$ ce qui implique que H est distingué dans G.

Exercice 2 2 points

Soit f un homomorphisme de groupes *non-constant* d'un groupe fini $(G, \cdot)$ dans $(\mathbb{C}^*, \cdot)$.
Calculer $\sum_{x \in G} f(x) \in \mathbb{C}$.
(Indication: Soit $g \in G$ tel que $f(g) \neq 1$ (Un tel g existe, pourquoi?). Calculer $\sum_{x \in G} f(g \cdot x)$ et comparer avec $\sum_{x \in G} f(x)$.)

Puisque f n'est pas constante, il existe $g \in G$ tel que $f(g \neq 1$. Maintenant, l'application $x \mapsto gx$ est une permutation de G : en effet, pour tout $y \in G$, il existe un unique $x \in G$ tel que $y = ax$. On en déduit que $\sum_{x \in G} f(g \cdot x) = \sum_{x \in G} f(x)$.

Mais d'autre part, puisque f est un homomorphisme de groupes, on a aussi $\sum_{x \in G} f(g \cdot x) = \sum_{x \in G} f(g) f(x) = f(g) \sum_{x \in G} f(x)$. Puisque $f(g) \neq 1$, on en déduit que $\sum_{x \in G} f(x) = 0$.

Exercice 3 3,5=1,5+2 points

Un groupe $(G, \cdot)$ est dit *divisible* si, pour tout $g \in G$ et tout $n \in \mathbb{N}^*$, il existe $u \in G$ tel que $u^n = g$.

1. **Le groupe $(\mathbb{Q}, +)$ est-il divisible?**
2. **Montrer que $(\mathbb{Q}, +)$ et $(\mathbb{Q}_+^*, \cdot)$ ne sont pas isomorphes.**

1) Soit $x \in \mathbb{Q}$ et $n \in \mathbb{N}^*$. Alors, si on pose $y = x/n$, c'est un élément de $\mathbb{Q}$ et $ny = x$: le groupe $(\mathbb{Q}, +)$ est divisible.

2) On commence par montrer que si G et H sont deux groupes isomorphes et si G est divisible, alors H est divisible. En effet, soit $\Phi : G \to H$ un isomorphisme. Soit $h \in H$. Il existe $g \in G$ tel que $h = \Phi(g)$. Puisque G est divisible, pour tout $n \geq 1$, il existe $u \in G$ tel que $u^n = g$. Posons $v = \Phi(u)$. Puisque Φ est un isomorphisme de groupes, on a $v^n = h$ et H est divisible.

Pour conclure, il suffit donc de montrer que $(\mathbb{Q}_+^*, \cdot)$ n'est pas divisible. Pour $g = 2$ et $n = 2$, il n'existe par de rationnel u tel que $u^2 = 2$. Les deux groupes ne sont donc pas isomorphes.

Exercice 4 3=1+2 points

1. **Déterminer tous les homomorphismes de groupes de $\mathbb{Z}_3 = \mathbb{Z}/3\mathbb{Z}$ dans $\mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z}$.**
2. **Déterminer tous les homomorphismes de groupes de $\mathbb{Z}_6 = \mathbb{Z}/6\mathbb{Z}$ dans $\mathbb{Z}_8 = \mathbb{Z}/8\mathbb{Z}$.**

1) Soit Φ un tel homomorphisme. Alors $\phi([1]_3)$ a un ordre qui divise 3, puisque $\phi([1]_3)+\phi([1]_3)+\phi([1]_3) = [0]_4$ Mais $\phi([1]_3)$ a aussi un ordre qui divise 4, puisque c'est un élément de $\mathbb{Z}_4$. . Son ordre divise donc le $pgcd(3, 4) = 1$, c'est-à-dire que son ordre est 1. Donc $\phi([1]_3) = [0]_4$. Donc, le seul homomorphisme est le morphisme trivial.

2) Cette fois on a que $\phi([1]_6)$ a pour ordre un diviseur de $pgcd(6,8) = 2$. Son ordre peut donc être égal à 1 ou à 2. Si son ordre est égal à 1, il s'agit du morphisme trivial. Si son ordre est égal à 2, on a nécessairement $\phi([1]_6) = [4]_8$ qui est le seul élément d'ordre 2 de $\mathbb{Z}_8$. Maintenant, il s'agit de voir que cette formule définit bien un morphisme de groupes. Par exemple, on peut remarquer qu'elle donne $\phi(k) = [0]_8$ si k est pair, et $\phi(k) = [4]_8$ si k est impair. A partir de là, il est facile de voir que Φ définit bien un morphisme. .

Exercice 5 7,5=0,5+2+2+3 points

1. **Rapeller le théorème de Lagrange.**
2. **Soit G un groupe et H, K deux sous-groupes de G dont les cardinaux $|H|$ et $|K|$ sont des nombres premiers. En utilisant le théorème de Lagrange, démontrer que l'on a soit $H = K$ ou bien $H \cap K = \{e\}$.**
3. **Démontrer que dans un groupe de cardinal 35, il existe (au moins) un élément d'ordre 5 et (au moins) un élément d'ordre 7.**
4. **Soit $p \geq 3$ un nombre premier et G un groupe abélien de cardinal $2p$ dont l'élément neutre est noté e. Montrer que G est un groupe cyclique.**

1) Soit G un groupe et H un sous-groupe de G. Alors on a: $|G| = |G/H| \cdot |H|$.

2) Soit p l'ordre de H, qui est premier. Puisque un élément de H a un ordre qui divise p, cet ordre ne peut être égal que à 1, si c'est l'élément neutre, ou à p. Autrement dit, tout élément de H autre que l'élément neutre génère H. Il en est de même pour tout élément de K autre que l'élément neutre. Ainsi, si $H \cap K$ contient un élément x différent de e , il contient toutes les puissances de x , donc H et K , et $H = K$.

3) Soit G un tel groupe. Ses éléments peuvent être d'ordre 1, 5, 7 ou 35 (Lagrange). Si G admet un élément a d'ordre 35, on a que G est cyclique. Alors a^5 est d'ordre 7 et a^7 est d'ordre 5.
Supposons donc que G n'est pas cyclique et qu'il n'admet pas d'éléments d'ordre 7. Alors tous ses éléments, sauf l'élément neutre, sont d'ordre 5 , et G est réunion de sous-groupes d'ordre 5. D'après la partie 2), l'intersection de deux de sous-groupes, quand ils sont distincts, est restreinte à e . Notons $G_1, \ldots, G_n$ ces sous-groupes distincts. Alors chaque G_i s'écrit $G_i = \{e\} \cup H_i$, et les $H_1, \ldots, H_n$ sont deux à deux disjoints. Autrement dit, $G = \{e\} \cup H_1 1 \cup ... \cup H_n$ est une partition de G . Comme chaque H_i est de cardinal 4, ceci implique que $35 = 4n + 1$. Mais alors 34 serait un multiple de 4, ce qui n'est pas le cas. Le raisonnement est similaire, si on suppose que G n'admet pas d'éléments d'ordre 5. On aurait alors $35 = 6m + 1$ pour un entier m , ce qui n'est pas le cas puisque 34 n'est pas un multiple de 6.

4) Les ordres possibles des éléments différents de l'élémént neutre de G sont 2, p, $2p$. Il suffit de montrer l'existence de deux éléménts x, y avec $ord(x) = 2$ et $ord(y) = p$, puisqu'alors xy est d'ordre $2p$ et G est cyclique (Ici on utilise que G est abélien!).
i) Supposons qu'il existe un élément d'ordre p. Si tous les éléments de $G \setminus \{e\}$ sont aussi d'ordre p, un raisonement comme dans la partie 3) montre qur $(p-1)$ divise $(|G| - 1) = 2p - 1$ ce qu'il est absurde, car $p \geq 3$. Donc il existe un élément d'ordre 2 et cela termine ce cas.
ii) Supposons que tous les éléments de $G \setminus \{e\}$ sont d'ordre 2. Alors l'exercice 14 de la planche 1 montre que le cardinal de G est une puissance de 2, ce qu'il est absurde. Donc il existe encore un élément d'ordre p. L'énoncé est démontré.

Exercice 6 2 points
Soit H un sous-groupe d'un groupe $(G, \cdot)$ tel que $H \neq G$. Montrer que le sous-groupe engendré par le complémentaire de H dans G est le groupe G tout entier.
Notons K le complémentaire de H et fixons un élément a de K (H est strictement inclus dans G). Nous allons prouver que le sous-groupe engendré par K , que nous allons noter L , est égal à G tout entier. Puisque ce sous-groupe contient déjà K , il suffit de prouver qu'il contient également son complémentaire, à savoir H . Soit donc $x \in H$. Alors ax ne peut pas être un élément de H , sinon $a = axx^{-1}$ serait élément de H lui

aussi. Donc ax est élément de K . Mais alors, $x = a^{-1}ax$ est un élément de L, puisque a et ax sont tous deux éléments de K , donc de L , et que L est un sous-groupe.

Exercice 7 3=1,5+1,5 points

On note $GL(2,\mathbb{Z})$ le groupe des matrices à coefficients dans $\mathbb{Z}$, inversibles dans l'ensemble des matrices à coefficients dans $\mathbb{Z}$.

1) Montrer qu'une matrice carrée d'ordre 2 à coefficients dans $\mathbb{Z}$ est dans $GL(2,\mathbb{Z})$ si, et seulement si, elle a pour déterminant 1 où -1.

2) Dans le groupe $GL(2,\mathbb{Z})$ on pose $A := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $B := \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$.

Déterminer l'ordre de A, de B, de AB.

1) On sait que l'application

$$\det : GL(2,\mathbb{R}) \to \mathbb{R}^*$$

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \det M = ad - bc$$

est un homomorphisme de groupes.

Supposons que

$$N = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2,\mathbb{Z})$$

une matrice inversible à coefficients dans $\mathbb{Z}$ dont la matrice inverse N^{-1} est aussi à coefficients dans $\mathbb{Z}$. On a $\det N \in \mathbb{Z}$ et il est exige que $\det N^{-1} = \frac{1}{\det N}$ soit aussi un élément de $\mathbb{Z}$. Cela n'est possible lorsque $\det N = 1$ ou $\det N = -1$.

Supposons réciproquement que $P \in M_2(\mathbb{Z}) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ soit une matrice à coefficients dans $\mathbb{Z}$ avec $\det P = 1$ ou $\det P = -1$. Alors $P^{-1} = \pm \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ qui est encore à coefficients entiers. Donc $P \in GL(2,\mathbb{Z})$.

2) Des calcules simples montrent que $ord(A) = 3, ord(B) = 4$ et $ord(AB) = +\infty$.