Autour de l'ordre

Samuel Rochetin

Dimanche 29 mai 2016

Exercices sur l'ordre

Exercice 1

Soient G un groupe multiplicatif fini d'élément neutre 1 et a, b deux éléments de G. Montrer que :

1. a et a^{-1} ont même ordre.
2. a et bab^{-1} ont même ordre.
3. ab et ba ont même ordre.

Exercice 2

1. Montrer que tout élément du groupe $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ admet pour ordre un diviseur de 12.
2. Montrer que l'élément $(1, 1)$ du groupe $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ est d'ordre 24.
3. Que peut-on déduire concernant les groupes $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$?

Exercice 3

Soit G un groupe abélien d'ordre 100.

1. Montrer qu'il existe un 2-groupe $G(2)$ et un 5-groupe $G(5)$ tels que $G \simeq G(2) \times G(5)$.
2. Montrer que $G(2)$ contient un élément d'ordre 2 et que $G(5)$ contient un élément d'ordre 5.
3. En déduire que G contient un élément d'ordre 10.

Exercice 4

Soient H et K deux groupes multiplicatifs.

1. Soient h un élément d'ordre p de H et k un élément d'ordre q de K. Montrer que (h, k) est un élément d'ordre $PPCM(p, q)$ de $H \times K$.
2. On suppose que H et K sont cycliques. Montrer que $H \times K$ est cyclique si et seulement si les ordres de H et K sont premiers entre eux.

Une formule d'ordre

Soient G un groupe fini et H, K deux sous-groupes de G. Nous posons $L = H \cap K$ et notons $(K/L)_g$ l'ensemble des classes à gauche de K modulo L.

1. Expliquer pourquoi il existe un entier n tel que $(K/L)_g = \{k_1 L, \ldots, k_n L\}$, où $k_1, \ldots, k_n$ sont des éléments de K.
2. (a) Montrer que $\forall i \in [\![1; n]\!], k_i H \neq \emptyset$.
   (b) Montrer que si $i \neq j$, alors $k_i H \cap k_j H = \emptyset$.
   (c) Montrer que $KH = \bigcup_{i=1}^{n} k_i H$.
   (d) En déduire que $|KH| = \sum_{i=1}^{n} |k_i H|$.
3. En remarquant que $f_{k_i} : H \to k_i H, h \mapsto k_i h$ est une bijection, montrer que $|k_i H| = |H|$.
4. En déduire que $|KH| = \dfrac{|H||K|}{|H \cap K|}$.

Corrigé

Exercices sur l'ordre

Exercice 1

1. Soient n l'ordre de a et m l'ordre de a^{-1}. $1 = 1^n = (aa^{-1})^n = aa^{-1}\dots aa^{-1} = a^n(a^{-1})^n = (a^{-1})^n$ car un élément et son inverse commutent toujours et par définition de l'ordre de a. Donc m divise n. On obtient de même $1 = (aa^{-1})^m = a^m$ donc n divise m. Comme m, n sont positifs, il vient $n = m$.
2. Soient n l'ordre de a et m l'ordre de bab^{-1}. $(bab^{-1})^n = bab^{-1}\dots bab^{-1} = ba^nb^1 = bb^{-1} = 1$ par simplification en cascade et définition de l'ordre de a. Donc m divise n. Par ailleurs, $1 = (bab^{-1})^m = ba^mb^{-1}$. Il vient $b = b * a^m$ en multipliant à droite par b, puis $1 = a^m$ en multipliant à gauche par b^{-1}. Donc n divise m. D'où $n = m$.
3. Soient n l'ordre de ab et m l'ordre de ba. $1 = (ab)^n = ab\dots ab = a(ba)^{n-1}b$. Il vient $a^{-1} = (ba)^{n-1}b$ puis $a^{-1}b^{-1} = (ba)^{n-1}$, c'est-à-dire $(ba)^{-1} = (ba)^{n-1}$, d'où $(ba)^n = 1$. Donc m divise n. Par symétrie du problème, on obtient n divise m puis $n = m$. Autre solution : d'après la question précédente, ab est du même ordre que $b(ab)b^{-1} = ba$.

Exercice 2

1. Soit $(x, y) \in \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. $4x = 0$ et $6y = 0$ donc $12x = 0$ et $12y = 0$. Donc $12(x, y) = (12x, 12y) = (0, 0)$. Donc l'ordre de (x, y) divise 12.
2. Soit n l'ordre de $(1, 1) \in \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. $n(1, 1) = (n, n) = (0, 0) \iff 3 \mid n$ et $8 \mid n \iff 24 \mid n$ (corollaire du théorème de Gauss, car $3 \wedge 8 = 1$).
3. 24 n'est pas un diviseur de 12 donc les groupes $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ ne sont pas isomorphes.

Exercice 3

Nous utilisons la notation multiplicative.

1. Les diviseurs premiers de 100 sont 2 et 5, donc d'après le théorème de structure des groupes abéliens finis, il existe un 2-groupe $G(2)$ et un 5-groupe $G(5)$ tels que $G \simeq G(2) \times G(5)$.
2. D'après le théorème de Lagrange, $|G(2)|$ divise $|G|$. Or, $|G(2)|$ est une puissance de 2, donc $|G(2)| = 2$ ou 4. Si $|G(2)| = 2$, alors $|G(5)| = 50$. Or, 50 n'est pas une puissance de 5. Donc $|G(2)| = 4$. Il s'ensuit $|G(5)| = 25$.

   Soit $x \in G(2)$, non neutre. D'après le théorème de Lagrange, l'ordre de x divise $|G(2)| = 4$ donc vaut 2 ou 4. Si l'ordre de x vaut 2, alors cela répond à la question. Sinon, l'ordre de x vaut 4 donc l'ordre de x^2 vaut 2, ce qui répond à la question.

   Même principe pour $G(5)$.
3. Soient $x \in G(2)$ d'ordre 2 et $y \in G(5)$ d'ordre 5. Considérons l'élément $z = xy$. Clairement, $z \in G$. Puisque $z^{10} = (x^2)^5(y^5)^2 = 1$, l'ordre de z divise 10, donc vaut 1, 2, 5 ou 10. Si l'ordre de z vaut 1, alors $y = x^{-1}$, ce qui est impossible car y est d'ordre 5 et x^{-1} est d'ordre 2 (même ordre que x). Si l'ordre de z vaut 2, alors $y^2 = 1$, ce qui est impossible car y est d'ordre 5. Si l'ordre de z vaut 5, alors $x = 1$, ce qui est impossible car x est d'ordre 2. Donc z est d'ordre 10, ce qui répond à la question.

Exercice 4

1. Soit n l'ordre de (h, k). $(h, k)^n = (h^n, k^n) = (1, 1)$ donc $p \mid n$ et $q \mid n$. Par définition, le plus petit entier n vérifiant ces conditions est $n = PPCM(p, q)$.
2. Soient p, q les ordres respectifs de H, K. Supposons $p \wedge q = 1$. Alors $PPCM(p, q) = pq$. Soient h, k des générateurs respectivement de H, K. Alors l'ordre de (h, k) est $PPCM(p, q) = pq$, d'après la question précédente. Or, $\#H \times K = pq$. Donc $H \times K$ est un groupe cyclique (engendré par (h, k)). Réciproquement, supposons que $H \times K$ soit cyclique. Soit (h, k) un générateur de $H \times K$. Puisque $\#H \times K = pq$, l'ordre de (h, k) est pq. Or, h, k sont nécessairement générateurs respectivement de H, K donc sont d'ordres respectifs p, q. Donc l'ordre de (h, k) est $PPCM(p, q)$ d'après la question précédente. On a donc $PPCM(p, q) = pq$. Donc $p \wedge q = 1$.

Une formule d'ordre

1. K est un groupe fini. Soit k un élément de K. La classe à gauche de k modulo L est l'ensemble kL. Soit n l'indice de L dans K. Soit $k_1, \dots, k_n$ un système de représentants. L'ensemble des classes à gauche de K modulo L est l'ensemble $\{k_1L, \dots, k_nL\} = (K/L)_g$.

2. (a) k_iH contient $k_ie_H = k_i$.

   (b) S'il existe h, h' éléments de H tels que $k_ih = k_jh'$, alors $k_j^{-1}k_i = h'h^{-1} \in H \cap K = L$. Donc $k_i \in k_jL$. Donc $k_iL = k_jL$. Impossible car $k_iL \cap k_jL = \emptyset$.

   (c) On a $\bigcup_{i=1}^{n} k_iH \subset KH$. Vérifions l'inclusion réciproque. Soit $kh \in KH$. Comme les k_iL forment une partition de K, il existe un indice i et un élément l de L tels que $k = k_il$. Donc $kh = k_i(lh) \in k_iH$ car $L \subset H$.

   (d) D'après les questions précédentes, les k_iH forment une partition de KH. D'où la formule.

3. f_{k_i} est une bijection évidente d'inverse $f_{k_i^{-1}}$, les ensembles H et k_iH sont finis, d'où la formule.

4. D'après les questions précédentes, nous avons $|KH| = n|H| = |H|[K : L] = \dfrac{|H||K|}{|L|} = \dfrac{|H||K|}{|H \cap K|}$ en utilisant le théorème de Lagrange.