Mathématiques spéciales

Corrigé de la feuille d'exercices n°7

1. Exercices basiques

Exercice 1.

Les ensembles suivants munis des lois considérées sont-ils des groupes ?

1. G est l'ensemble des fonctions de $\mathbb{R} \to \mathbb{R}$ définies par $x \mapsto ax + b$, avec $a \in \mathbb{R}^*$ et $b \in \mathbb{R}$, muni de la composition ;
2. G est l'ensemble des fonctions croissantes de $\mathbb{R}$ dans $\mathbb{R}$, muni de l'addition ;
3. $G = \{f_1, f_2, f_3, f_4\}$, où

$$f_1(x) = x,\ f_2(x) = -x,\ f_3(x) = \frac{1}{x},\ f_4(x) = -\frac{1}{x},$$

muni de la composition.

Correction.

1. On remarque d'abord que la composition est une loi de composition interne pour G. En effet,
$$(ax + b) \circ (cx + d) = acx + (ad + b).$$
La loi $\circ$ est clairement associative (pour toutes les fonctions $f : \mathbb{R} \to \mathbb{R}$, on a effectivement $f \circ (g \circ h) = (f \circ g) \circ h$). La fonction $x \mapsto x$ est un élément neutre, et l'inverse de $x \mapsto ax + b$ est donné par $x \mapsto \frac{1}{a}x - \frac{b}{a}$ - on trouve cet élément en résolvant le système (d'inconnues c et d)
$$\begin{cases} ac &= 1 \\ ad + b &= 0. \end{cases}$$
On aurait aussi pu démontrer que G est un sous-groupe du groupe des permutations de $\mathbb{R}$.
2. Imaginons que G soit un groupe. Son élément neutre est alors forcément la fonction identiquement nulle. Mais prenons la fonction $f(x) = x$ (qui est bien croissante). Son inverse serait la fonction $f(x) = -x$, qui n'est pas croissante ! Donc $(G, +)$ n'est pas un groupe.
3. Calculons d'abord le résultat des différentes compositions :
$$f_1 \circ f_1 = f_1,\ f_1 \circ f_2 = f_2 \circ f_1 = f_2,\ f_1 \circ f_3 = f_3 \circ f_1 = f_3,\ f_1 \circ f_4 = f_4 \circ f_1 = f_4$$
$$f_2 \circ f_2 = f_1,\ f_2 \circ f_3 = f_3 \circ f_2 = f_4,\ f_2 \circ f_4 = f_4 \circ f_2 = f_3$$
$$f_3 \circ f_3 = f_1,\ f_3 \circ f_4 = f_4 \circ f_3 = f_2$$
$$f_4 \circ f_4 = f_1.$$
De ces calculs, on tire que :
   (a) $\circ$ est bien une loi de composition interne pour G. Elle est de plus clairement associative.
   (b) f_1 est élément neutre pour cette loi.
   (c) Chaque élément admet un inverse : lui-même !

   $(G, \circ)$ est bien un groupe. On pourrait démontrer, toujours à partir du résultat des différentes compositions, qu'il est isomorphe au groupe classique $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercice 2.

Soit $(G, \cdot)$ un groupe. Démontrer que les parties suivantes sont des sous-groupes de G :

1. $C(G) = \{x \in G;\ \forall y \in G, xy = yx\}$ ($C(G)$ s'appelle le centre de G) ;
2. $aHa^{-1} = \{aha^{-1};\ h \in H\}$ où $a \in G$ et H est un sous-groupe de G.
3. On suppose de plus que G est abélien. On dit que x est un élément de torsion de G s'il existe $n \in \mathbb{N}$ tel que $x^n = e$. Démontrer que l'ensemble des éléments de torsion de G est un sous-groupe de G.

Correction.

Il suffit, pour chaque cas, d'appliquer le théorème de caractérisation des sous-groupes.

1. e est élément de $C(G)$ car $ey = ye = y$ pour tout $y \in G$. Soient $x_1, x_2 \in C(G)$. Alors, pour tout $y \in G$, on a
$$x_1x_2y = x_1(x_2y) = (x_1y)x_2 = yx_1x_2$$
et donc $x_1x_2 \in C(G)$. Enfin, si $x \in C(G)$, alors pour tout $y \in G$,
$$xy = yx \implies xyx^{-1} = yxx^{-1} = y \implies x^{-1}xyx^{-1} = x^{-1}y \implies yx^{-1} = x^{-1}y$$
où on a multiplié à droite puis à gauche par x^{-1}. On en déduit que $x^{-1} \in C(G)$ qui est donc un sous-groupe de G.
2. Puisque H est un sous-groupe de G, $e \in H$ et donc $aea^{-1} \in G$. Mais $aea^{-1} = e$ et donc $e \in aHa^{-1}$. Soient $x = aha^{-1}$ et $y = ah'a^{-1}$ deux éléments de aHa^{-1} avec donc $h, h' \in H$. On a
$$xy = aha^{-1}ah'a^{-1} = ahh'a^{-1} \in aHa^{-1}$$
puisque $hh' \in H$ (H est un sous-groupe de G). Enfin, on a
$$x^{-1} = (aha^{-1})^{-1} = ah^{-1}a^{-1} \in aHa^{-1}$$
puisque $h^{-1} \in H$. aHa^{-1} est donc bien un sous-groupe de G.
3. Notons T l'ensemble des éléments de torsion de G. On a $e^1 = e$, donc $e \in T$. De plus, si $x, y \in T$, avec respectivement $x^n = e$ et $y^m = e$, il suffit de remarquer que
$$(y^{-1})^m = (y^m)^{-1} = e^{-1} = e$$
puis d'utiliser le fait que x et y^{-1} commutent pour prouver que
$$(xy^{-1})^{nm} = (x^n)^m((y^{-1})^m)^n = e.$$
Ainsi, xy^{-1} est élément de T, et T est bien un sous-groupe de G.

Exercice 3.

Un sous-groupe d'un groupe produit est-il nécessairement produit de deux sous-groupes ?

Correction.

Non, ce n'est pas le cas. Prenons $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$ et $H = \{(x, x);\ x \in \mathbb{Z}\}$. H est clairement un sous-groupe de $\mathbb{Z}^2$, et H ne s'écrit pas $H = A \times B$, sinon on aurait $A = B = \mathbb{Z}$ ce qui n'est pas le cas.

Exercice 4.

Soit G un groupe et H, K deux sous-groupes de G. Démontrer que $H \cup K$ est un sous-groupe de G si et seulement si $H \subset K$ ou $K \subset H$.

Correction.

Si $H \subset K$, alors $H \cup K = K$ qui est un sous-groupe de G. De même, si $K \subset H$, $H \cup K = H$ qui est un sous-groupe de G. Supposons maintenant que $H \cup K$ est un sous-groupe de G et que ni $H \subset K$, ni $K \subset H$. Alors on peut trouver $x \in H \backslash K$ et $y \in K \backslash H$. Puisque $H \cup K$ est un groupe et que $x, y \in H \cup K$, on a $xy \in H \cup K$. Mais si $xy \in H$, alors $y = x^{-1}(xy)$ est le produit de deux éléments de H, qui est un sous-groupe de G, et donc $y \in H$ ce qui est une contradiction. On obtient de même une contradiction dans l'autre cas possible $xy \in K$. L'hypothèse de départ est donc fausse, et on a bien $H \subset K$ ou $K \subset H$.

Exercice 5.

Traduire en termes de morphismes de groupes les propriétés bien connues suivantes (dont le domaine de validité a volontairement été omis) :

1. $\ln(xy) = \ln(x) + \ln(y)$;
2. $|zz'| = |z||z'|$;
3. $\sqrt{xy} = \sqrt{x}\sqrt{y}$;
4. $e^{x+y} = e^x e^y$;
5. $\det(MM') = \det(M)\det(M')$.

Correction.

1. La fonction ln est un morphisme du groupe $(\mathbb{R}_+^*, \cdot)$ dans le groupe $(\mathbb{R}, +)$.
2. La fonction $|\cdot|$ est un morphisme de groupes de $(\mathbb{C}^*, \cdot)$ dans lui-même. Attention, même si la propriété est vraie pour $z = 0$, il faut exclure 0 du groupe !
3. La fonction $\sqrt{\ }$ est un morphisme du groupe $(\mathbb{R}_+^*, \cdot)$ dans lui-même.
4. La fonction exp est un morphisme de groupe de $(\mathbb{R}, +)$ dans $(\mathbb{R}_+^*, \cdot)$.
5. La fonction det est un morphisme de groupe de $GL_n(\mathbb{R})$ dans $(\mathbb{R}^*, \times)$. Là aussi, il faut se restreindre aux éléments inversibles pour bien avoir affaire à un groupe.

Exercice 6.

Déterminer tous les morphismes de $(\mathbb{Z}, +)$ dans lui-même. Lesquels sont injectifs ? surjectifs ?

Correction.

Soit f un morphisme de $(\mathbb{Z},+)$. Prouvons par récurrence que pour tout $n \geq 1$, on a $f(n) = nf(1)$. C'est vrai pour $n = 1$, et si c'est vrai pour n, alors

$$f(n+1) = f(n) + f(1) = nf(1) + f(1) = (n+1)f(1).$$

De plus, pour $n \leq 0$, on a $-n \geq 0$ et donc $f(-n) = -nf(1)$. On en déduit :

$$0 = f(0) = f(n + (-n)) = f(n) + f(-n) = f(n) - nf(1).$$

Ainsi, on a toujours $f(n) = nf(1)$, quel que soit $n \in \mathbb{Z}$. Caractérisons maintenant les morphismes surjectifs. Supposons donc que f est surjectif. Tout élément de $\mathbb{Z} = f(\mathbb{Z})$ est un multiple de $f(1)$. Or, les seuls éléments de $\mathbb{Z}$ qui divisent tous les autres entiers sont 1 et -1. On en déduit que $f(1) = 1$ ou $f(1) = -1$, et donc que $f(n) = n$ ou $f(n) = -n$. Réciproquement, ces deux applications sont clairement des morphismes surjectifs de $(\mathbb{Z},+)$. Déterminons enfin les morphismes injectifs. Soit f un morphisme et $n \in \ker(f)$. Alors $f(n) = nf(1) = 0$. Si $f(1) \neq 0$, alors $f(n) = 0 \iff n = 0$ et f est injectif, et si $f(1) = 0$, alors f n'est pas injectif. Donc tous les morphismes de $(\mathbb{Z},+)$ dans $(\mathbb{Z},+)$ sont injectifs sauf l'application identiquement nulle.

2. Exercices d'entraînement

Exercice 7.

Montrer que les lois suivantes munissent l'ensemble G indiqué d'une structure de groupe, et préciser s'il est abélien :

1. $x \star y = \frac{x+y}{1+xy}$ sur $G =]-1,1[$;
2. $(x,y) \star (x',y') = (x+x', ye^{x'} + y'e^{-x})$ sur $G = \mathbb{R}^2$;

Correction.

1. $(G,\star)$ est un groupe car <ul class="rien">
2. $\star$ est une loi de composition interne sur G : en effet, si $x, y \in G$, alors $x \star y \in G$. Pour prouver cela, étudions la fonction définie sur $]-1,1[$ par

   $$f(t) = \frac{t+y}{1+ty}.$$

   Elle est dérivable sur $[-1,1]$, et sa dérivée vérifie

   $$f'(t) = \frac{1-y^2}{(1+ty)^2} > 0 \text{ sur }]-1,1[.$$

   f est donc strictement croissante sur $[-1,1]$ et on a

   $$f(-1) < x \star y = f(x) < f(1).$$

   Comme $f(-1) = (-1+y)/(1-y) = -1$ et $f(1) = (1+y)/(1+y) = 1$, on obtient bien que $x \star y \in G$.

3. la loi est associative : pour tout $(x, y, z) \in G^3$,

$$\begin{aligned} x \star (y \star z) &= \frac{x + (y \star z)}{1 + x(y \star z)} \\ &= \frac{x + \frac{y+z}{1+yz}}{1 + x\frac{y+z}{1+yz}} \\ &= \frac{x + y + z + xyz}{1 + xy + xz + yz}, \end{aligned}$$

et un calcul similaire donne le même résultat pour $(x \star y) \star z$.

4. 0 est un élément neutre pour la loi $\star$. En effet,

$$x \star 0 = 0 \star x = \frac{x + 0}{1 + 0} = x.$$

5. Tout élément $x \in G$ est inversible, d'inverse $-x$. En effet, on a

$$x \star (-x) = (-x) \star x = \frac{x - x}{1 - x^2} = 0.$$

 De plus, le groupe est clairement abélien.

6. Il est clair que $\star$ est une loi de composition interne sur $\mathbb{R}^2$. De plus, <ul class="rien">
7. cette loi est associative :

$$\begin{aligned} (x, y) \star \big((x', y') \star (x'', y'')\big) &= (x, y) \star (x' + x'', y'e^{x''} + y''e^{-x'}) \\ &= (x + x' + x'', ye^{x'+x''} + y'e^{x''}e^{-x} + y''e^{-x'}e^{-x}) \\ &= (x + x' + x'', ye^{x'+x''} + y'e^{-x+x''} + y''e^{-x-x'}). \end{aligned}$$

De même,

$$\begin{aligned} \big((x, y) \star (x', y')\big) \star (x'', y'') &= (x + x', ye^{x'} + y'e^{-x}) \star (x'', y'') \\ &= (x + x' + x'', (ye^{x'} + y'e^{-x})e^{x''} + y''e^{-x-x'}) \\ &= (x + x' + x'', ye^{x'+x''} + y'e^{-x+x''} + y''e^{-x-x'}) \end{aligned}$$

et donc on a bien $(x, y) \star \big((x', y') \star (x'', y'')\big) = \big((x, y) \star (x', y')\big) \star (x'', y'')$.

8. $(0, 0)$ est un élément neutre de G :

$$(x, y) \star (0, 0) = (x + 0, ye^0 + 0e^{-x}) = (x, y)$$

$$(0, 0) \star (x, y) = (0 + x, 0e^x + ye^{-0}) = (x, y).$$

9. Tout élément $(x, y) \in G$ admet un inverse donnée par $(-x, -y)$. En effet,

$$(x, y) \star (-x, -y) = (x - x, ye^{-x} - ye^{-x}) = (0, 0),$$

$$(-x, -y) \star (x, y) = (-x + x, -ye^x + ye^x) = (0, 0).$$

 De plus, le groupe n'est pas abélien, car

$$(1, 0) \star (0, 1) = (1, e^{-1}) \text{ tandis que } (0, 1) \star (1, 0) = (1, e^1).$$

Exercice 8.

On note $GL_n(\mathbb{Z})$ l'ensemble des matrices de $\mathcal{M}_n(\mathbb{R})$, à coefficients dans $\mathbb{Z}$, qui sont inversibles et dont l'inverse est à coefficients dans $\mathbb{Z}$.

1. Démontrer que si M est à coefficients dans $\mathbb{Z}$, alors $M \in GL_n(\mathbb{Z})$ si et seulement si $\det(M) = \pm 1$.
2. En déduire que $GL_n(\mathbb{Z})$ est un sous-groupe de $GL_n(\mathbb{R})$.

Correction.

1. Prenons d'abord $M \in GL_n(\mathbb{Z})$. Alors on a
$$\det(M) \times \det(M^{-1}) = \det(MM^{-1}) = \det(I_n) = 1$$
et de plus $\det(M)$ et $\det(M^{-1})$ sont des éléments de $\mathbb{Z}$. Ceci n'est possible que si $\det(M)$ et $\det(M^{-1})$ sont égaux à 1 ou -1. Réciproquement, si $\det(M) = \pm 1$, alors les formules de Cramer nous disent que
$$M^{-1} = \frac{1}{\det M}(\text{comat } M)^T.$$
La comatrice d'une matrice à coefficients dans $\mathbb{Z}$ étant à coefficients dans $\mathbb{Z}$ et $\det(M)$ valant ± 1, on a bien que M^{-1} est une matrice à coefficients entiers.
2. On remarque d'abord que $I_n \in GL_n(\mathbb{Z})$. Ensuite, si $A, B \in GL_n(\mathbb{Z})$, des formules
$$\det(A^{-1}) = \frac{1}{\det(A)}$$
et
$$\det(AB) = \det(A)\det(B)$$
on déduit facilement que $\det(A^{-1})$ et $\det(AB)$ sont éléments de $\{-1, 1\}$ et donc A^{-1}, AB sont éléments de $GL_n(\mathbb{Z})$.

Exercice 9.

Montrer que $H = \{x + y\sqrt{3};\ x \in \mathbb{N},\ y \in \mathbb{Z},\ x^2 - 3y^2 = 1\}$ est un sous-groupe de $(\mathbb{R}_+^*, \times)$.

Correction.

La première chose à remarquer est que $H \subset \mathbb{R}_+^*$. Pour $x + y\sqrt{3} \in H$, puisque $x^2 - 3y^2 > 0$ et $x \in \mathbb{N}$, on a $x > \sqrt{3}|y|$ et donc $x + y\sqrt{3} > 0$. On remarque ensuite que $1 = 1 + 0\sqrt{3}$ est bien un élément de H. Soient $a = x + y\sqrt{3}$ et $b = u + v\sqrt{3}$ deux éléments de H. Alors :
$$(x + y\sqrt{3})(u + v\sqrt{3}) = (xu + 3yv) + \sqrt{3}(xv + yu).$$
On remarque ensuite que
$$\begin{aligned}(xu + 3yv)^2 - 3(xv + yu)^2 &= x^2u^2 + 9y^2v^2 - 3x^2v^2 - 3y^2u^2 \\ &= x^2(u^2 - 3v^2) + 3y^2(3v^2 - u^2) \\ &= x^2 - 3y^2 \\ &= 1.\end{aligned}$$

De plus, il est clair que $xu+3yv$ et $xv+yu$ sont éléments de $\mathbb{Z}$. Il reste à voir que $xu+3yv$ est élément de $\mathbb{N}$. Mais c'est clair car $x \geq \sqrt{3}|y|$ et $u \geq \sqrt{3}|v|$. Ainsi, $ab \in H$. Démontrons finalement que H est bien stable par passage à l'inverse. On a

$$\frac{1}{a} = \frac{1}{x+y\sqrt{3}} = \frac{x-y\sqrt{3}}{x^2-3y^2} = x - y\sqrt{3} \in H$$

puisque $x^2+3(-y)^2 = 1$. Ainsi, H est bien un sous-groupe de $(\mathbb{R}_+^*, \times)$.

Exercice 10.

Soit $(G, \cdot)$ un groupe fini et A, B deux sous-groupes de G. On note $AB = \{ab;\ a \in A,\ b \in B\}$. Montrer que AB est un sous-groupe de G si et seulement si $AB = BA$.

Correction.

Supposons d'abord que $AB = BA$. Alors AB est un sous-groupe de G car :

1. $e \in AB$, car $e = ee$ avec $e \in A$ et $e \in B$ (ce sont des sous-groupes) ;
2. AB est stable par passage au produit. En effet, si $x = ab \in AB$ et $y = a'b' \in AB$, alors $xy = aba'b'$. Or, ba' est un élément de BA, c'est donc aussi un élément de AB et donc $ba' = a''b''$ avec $a'' \in A$ et $b'' \in B$. On en déduit que

   $$xy = aa''b''b \in AB$$

   puisque $aa'' \in A$ et $bb'' \in B$.
3. AB est stable par passage à l'inverse. En effet, si $x = ab \in AB$, alors $x^{-1} = b^{-1}a^{-1}$ est élément de BA et $BA = AB$.

Réciproquement, supposons que AB est un sous-groupe de G et prouvons que $AB = BA$. Soit d'abord $x = ab \in AB$. Alors $x^{-1} = b^{-1}a^{-1} \in AB$ et donc $b^{-1}a^{-1} = a'b'$ avec $a' \in A$ et $b' \in B$. On passe à l'inverse :

$$ab = b'^{-1}a'^{-1} \in BA.$$

De même, si $y = ba \in BA$, alors $y^{-1} = a^{-1}b^{-1} \in AB$, et donc $y = (y^{-1})^{-1} \in AB$.

Exercice 11.

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

Correction.

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 $a^2 > 0$. D'où $1 = a^2 = f(i^2) = f(-1)$ et $1 = f(1)$. f ne peut pas être injectif, on a obtenu une contradiction.

Exercice 12.

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.

Correction.

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. Procédons en deux temps. 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 $v = \phi(u)$. Alors puisque ϕ est un morphisme, on a $v^n = h$ et h est divisible. Pour conclure, il suffit donc de prouver que $(\mathbb{Q}_+^*, \cdot)$ n'est pas divisible. Mais par exemple, pour $g = 2$ et $n = 2$, il n'existe par de rationnel u tel que $u^2 = 2$ (car $\sqrt{2}$ est irrationnel). Les deux groupes ne sont donc pas isomorphes.

3. Exercices d'approfondissement

Exercice 13.

Soit H un sous-groupe strict d'un groupe $(G, \cdot)$. Déterminer le sous-groupe engendré par le complémentaire de H.

Correction.

Notons K le complémentaire de H et fixons a un élément de K (rappelons que 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 (ce qui entraîne que $a^{-1} \in L$ et que le produit $a^{-1}ax$ est aussi dans L).

Exercice 14.

Soit $(G, \cdot)$ un groupe fini et H un sous-groupe de G.

1. Montrer que pour tout $a \in G$, H et $aH = \{ah;\ h \in H\}$ ont le même nombre d'éléments.
2. Soient $a, b \in G$. Démontrer que $aH = bH$ ou $aH \cap bH = \varnothing$.
3. En déduire que le cardinal de H divise le cardinal de G.

Correction.

1. Soit $f : H \to aH$ définie par $f(h) = ah$. Il s'agit clairement d'une surjection de H sur aH. De plus, si $ah_1 = ah_2$, alors $h_1 = h_2$ car a est inversible, et donc f est aussi injective. f est donc une bijection de H sur aH ; ces deux ensembles ont le même nombre d'éléments.
2. Supposons que $aH \cap bH \neq \varnothing$ et prouvons que $aH = bH$. Par symétrie, il suffit de prouver que $aH \subset bH$. Soit $x \in aH \cap bH$, $x = ah_1 = bh_2$. Prenons $y = ah \in aH$. Alors $a = bh_2h_1^{-1}$ et donc $y = bh_2h_1^{-1}h \in bH$.
3. La réunion des ensembles aH est clairement égale à G (si $x \in G$, il est dans xH). On ne garde que les aH deux à deux disjoints et par les deux questions précédentes, on réalise ainsi une partition de G avec des ensembles qui ont tous le même cardinal, à savoir le cardinal de H. Si k est le nombre d'ensembles nécessaires pour réaliser cette partition, on a

   $$k\mathrm{card}(H) = \mathrm{card}(G)$$

   et donc le cardinal de H divise celui de G.

Exercice 15.

Soit f un morphisme d'un groupe fini $(G, \cdot)$ dans $(\mathbb{C}^*, \cdot)$. Calculer $\sum_{x\in G} f(x)$.

Correction.

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

$$\sum_{x\in G} f(ax) = \sum_{x\in G} f(x).$$

Mais d'autre part, puisque f est un morphisme de groupes, on a aussi

$$\sum_{x\in G} f(ax) = \sum_{x\in G} f(a)f(x) = f(a)\sum_{x\in G} f(x).$$

Ainsi, il vient

$$\big(f(a) - 1\big) \times \sum_{x\in G} f(x) = 0.$$

Puisque $f(a) \neq 1$, on en déduit que $\sum_{x\in G} f(x) = 0$.

Exercice 16.

Soit G le groupe des isométries du plan affine euclidien qui laissent invariant un triangle équilatéral Δ. Démontrer que G est isomorphe à S_3.

Correction.

Notons $T = \{A, B, C\}$ les trois sommets du triangle. Il suffit de construire un isomorphisme de G sur S_T. Considérons $\phi : G \to S_T,\ g \mapsto g_{|T}$ et prouvons que ϕ est un isomorphisme. Remarquons d'abord que ϕ est bien définie. En effet, les sommets du triangle sont bien envoyés par un élément g de G sur eux-mêmes (pourquoi !!!!), et g étant bijective, sa restriction à l'ensemble fini T ne peut être que bijective. Il est alors clair que ϕ est un morphisme de groupe. Elle est injective. En effet, si g est l'identité sur les $\{A, B, C\}$, ceci signifie que g est une isométrie du plan ayant au moins trois points fixes. Ainsi, g ne peut être que l'identité. Prouvons enfin que ϕ est surjective. Les transpositions engendrant S_3, il suffit de démontrer que les transpositions sont dans l'image de ϕ. Mais la transposition $(A\ B)$ est dans l'image de ϕ. Il suffit en effet de considérer pour g la symétrie orthogonale à la médiatrice de $[AB]$ (cette droite passe donc par C), qui échange les points A et B tout en gardant C fixe.