

## CHAPITRE 6 - GROUPES, ANNEAUX

## Exercice 6.1

Soient  $f : G \rightarrow G'$  un isomorphisme de groupes et  $a$  un élément de  $G$  d'ordre  $n$ . Comme  $e' = f(e) = f(a^n) = (f(a))^n$ , on en déduit que  $f(a)$  est d'ordre fini, divisant  $n$ . Si  $f(a)^k = e'$ , alors  $f(a^k) = e'$  donc  $a^k = e$  car  $f$  injective, d'où  $n$  divise  $k$ . Il en résulte que  $f(a)$  est d'ordre  $n$ .

## Exercice 6.2

Dans  $\mathbb{Z}/8\mathbb{Z}$ ,  $\bar{1}$  est d'ordre 8, alors qu'aucun élément de  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$  n'est d'ordre 8, car  $4(x, y) = (\bar{0}, \bar{0})$  pour tout  $(x, y) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ . Un isomorphisme conservant l'ordre, les deux groupes ne sont pas isomorphes.

## Exercice 6.3

1. On a  $\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k!}$  mais factoriser par  $p$  n'est pas très éclairant car on ne sait pas si l'autre facteur est un entier.

Écrivons plutôt  $k! \binom{p}{k} = p(p-1)\cdots(p-k+1)$ . Par conséquent,  $p \mid k! \binom{p}{k}$ , or  $p$  est premier et  $k \in \llbracket 1; p-1 \rrbracket$ , donc  $p$  et  $k!$  sont premiers entre eux.

On déduit par le théorème de Gauss que  $p$  divise  $\binom{p}{k}$ .

2. D'après la formule du binôme de Newton :  $(a+b)^p = \sum_{k=0}^p \binom{p}{k} a^k b^{p-k}$ . D'après 1), pour  $k \in \llbracket 1; p-1 \rrbracket$ ,  $\binom{p}{k} \equiv 0 \pmod{p}$  donc, modulo  $p$ , seuls restent dans le développement le premier et le dernier terme :

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

3.  $\rightarrow$  Si  $p=2$ ,  $a^2 - a = a(a-1)$  est un nombre pair, donc  $a^2 \equiv a \pmod{2}$ .  
 $\rightarrow$  Supposons à présent  $p \geq 3$ . Démontrons par récurrence sur  $a \in \mathbb{N}$  la propriété  $\mathcal{P}_a$  suivante :  $a^p \equiv a \pmod{p}$ .  
*Initialisation* :  $a=0$ . On a bien  $0^p = 0 \equiv 0 \pmod{p}$ , donc  $\mathcal{P}_0$  est vraie.  
*Hérédité* : soit  $a \in \mathbb{N}$ . Supposons  $\mathcal{P}_a$  vraie et montrons  $\mathcal{P}_{a+1}$ .  $(a+1)^p \equiv a^p + 1^p \pmod{p}$  d'après la première question avec  $b=1$ . On en déduit avec  $\mathcal{P}_a$  que  $(a+1)^p \equiv a+1 \pmod{p}$ . En conclusion,  $a^p \equiv a \pmod{p}$  pour tout  $a \in \mathbb{N}$ . Si  $a \in \mathbb{Z}_-$ , d'après ce qui précède  $(-a)^p \equiv -a \pmod{p}$ . Comme  $p$  est impair, on conclut que  $a^p \equiv a \pmod{p}$ . En résumé,  $\forall a \in \mathbb{Z}$ ,  $a^p \equiv a \pmod{p}$ .  
 $\rightarrow$  On déduit de ce qui précède que :  $a(a^{p-1} - 1) \equiv 0 \pmod{p}$ , donc si  $p$  ne divise pas  $a$  alors, comme  $p$  est premier, il est premier avec  $a$  et par théorème de Gauss,  $p$  divise  $a^{p-1} - 1$ . Ainsi, on a bien  $a^{p-1} \equiv 1 \pmod{p}$ .

## Exercice 6.4

1. On vérifie par calcul  $\det(A(\theta)) = \det(B(\theta)) = 1$  ainsi  $G$  et  $H$  sont inclus dans  $GL_2(\mathbb{R})$ . La matrice  $I_2$  est  $A(0) = B(0)$ . Par calcul, on vérifie que  $A(\theta)A(\theta') = A(\theta + \theta') \in G$  et  $A(\theta)^{-1} = A(-\theta) \in G$  (et de même pour  $B(\theta)^{-1}$ ). On en déduit que  $G$  et  $H$  sont deux sous-groupes de  $GL_2(\mathbb{R})$ .  
 2. Soit  $A \in G$ . Il existe  $\theta \in \mathbb{R}$  tel que  $A = A(\theta)$ . On a alors  $A^2 = A(2\theta)$  et  $A^2 = I_2$  si et seulement si  $\cos(2\theta) = 1$  et  $\sin(2\theta) = 0$  soit  $\theta \in \pi\mathbb{Z}$ . Il y a donc deux matrices de  $G$  qui vérifient  $X^2 = I_2$  : la matrice  $A(0) = I_2$  et  $A(\pi) = -I_2$ . En revanche dans  $H$ , on ne trouve que  $I_2$ . S'il existait un isomorphisme  $\varphi$  entre  $G$  et  $H$ . On a, pour  $X \in G$ ,  $\varphi(X^2) = \varphi(X)^2$ . Si  $X^2 = I_2$  alors  $\varphi(X)^2 = \varphi(I_2) = I_2$ . Or  $I_2$  et  $-I_2$  sont deux matrices de  $G$  qui vérifient cela. Si  $\varphi$  est bijective,  $\varphi(I_2)$  et  $\varphi(-I_2)$  seraient deux matrices distinctes qui vérifient  $(\varphi(X))^2 = I_2$  dans  $H$  d'où une contradiction.

## Exercice 6.5

- $\rightarrow$  Les éléments inversibles de  $\mathbb{Z}/8\mathbb{Z}$  sont les classes  $\bar{p}$  avec  $p$  premier avec 8, c'est-à-dire  $\bar{1}, \bar{3}, \bar{5}$  et  $\bar{7}$ .  
 $\rightarrow$  On cherche l'ordre de chaque élément (donc le cardinal du groupe engendré par un élément). L'ordre de  $\bar{1}$  est 1, celui de  $\bar{7} = -\bar{1}$  est 2. On a  $\bar{3}^2 = \bar{5}^2 = \bar{1}$ , donc les éléments différents de 1 sont d'ordre 2. Le groupe n'est donc pas cyclique (*remarque* : on peut montrer que ce groupe des inversibles est isomorphe à  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ).

## Exercice 6.6

1. D'après le théorème de Lagrange, l'ordre d'un sous-groupe divise l'ordre du groupe. Si  $n$  est premier et  $H$  un sous-groupe de  $G = \mathbb{Z}/n\mathbb{Z}$  alors  $\text{card } H$  vaut 1 ou  $n$  donc  $H$  est  $\{0\}$  ou  $G$ . Si  $n$  n'est pas premier, il existe  $p$  et  $q$  supérieurs ou égaux à 2 tels que  $n = pq$ . Le groupe engendré par  $\bar{p}$  dans  $\mathbb{Z}/n\mathbb{Z}$  est d'ordre  $q$  où  $1 < q < n$ . Finalement  $\mathbb{Z}/n\mathbb{Z}$  est simple si et seulement si  $n$  est premier (ou  $n=1$  ?)  
 2. Si  $G$  est simple, tout élément différent du neutre engendre un sous-groupe à au moins 2 éléments donc engendre  $G$  :  $G$  est donc cyclique et donc de cardinal premier d'après la première question. Si  $G$  est cyclique d'ordre  $p$  premier alors  $G$  est isomorphe à  $\mathbb{Z}/p\mathbb{Z}$  et est donc simple.

**Exercice 6.7**

Pour tout  $(x, y) \in G^2$ ,  $f(xy) = f(x)f(y)$  car  $G$  est abélien, donc  $f$  est un morphisme. Par le théorème de Bézout, il existe deux entiers  $u$  et  $v$  tels que  $uk + vn = 1$ , d'où  $\forall x \in G$ ,  $(x^k)^u = x^{1-kn} = x$  car tout élément de  $G$  élevé à la puissance  $n$  est égal à  $e$ . Par suite, l'application  $g : x \mapsto x^u$  vérifie  $f \circ g = g \circ f = \text{Id}$ , donc  $f$  est bijective, et  $g$  est sa réciproque.

**Exercice 6.8**

- Soit  $H$  un sous-groupe de  $G$ , distinct de  $\{e\}$ . On note  $m$  le plus petit entier naturel non nul tel que  $a^m \in H$ . Comme  $H$  est un sous-groupe, le sous-groupe engendré par  $a^m$  est inclus dans  $H$ . Soit  $x \in H$ . Il existe un entier naturel  $k$  tel que  $x = a^k$ . Par division euclidienne de  $k$  par  $m$ , il existe deux entiers naturels  $j$  et  $r$  tels que  $k = mj + r$  et  $r \leq m - 1$ . Comme  $H$  est un groupe et que  $x \in H$ ,  $x(a^m)^{-j} \in H$ , c'est-à-dire  $a^r \in H$ , d'où  $r = 0$  par minimalité de  $m$ , d'où  $x = a^m j$  et  $x \in H$ . On a montré que  $H$  est cyclique engendré par  $a^m$ . Par division euclidienne de  $n$  par  $m$ , il existe deux entiers naturels  $q$  et  $s$  tels que  $n = mq + s$  et  $s \leq m - 1$ . Comme  $a^n = e$ , on obtient  $a^s = (a^m)^{-q}$ , donc  $a^s \in H$ , d'où  $s = 0$  par minimalité de  $m$ , donc  $m$  divise  $n$ .
- Comme  $d$  divise  $n$ , il existe  $m \in \mathbb{N}$  tel que  $n = dm$ . Montrons que le sous-groupe engendré par  $a^m$  est d'ordre  $d$ . On a  $(a^m)^d = e$ . S'il existe deux entiers  $k$  et  $j$  tels que  $0 \leq j < k < d$  et  $a^{km} = a^{jm}$ , alors  $(k - j)m \geq n$ , ce qui est absurde car  $k - j \leq d - 1$ . Le sous-groupe engendré par  $a^m$  est donc formé des  $d$  éléments distincts  $a^{km}$  pour  $0 \leq k \leq d - 1$ . Inversement, si  $H$  est un sous-groupe de  $G$  de cardinal  $d$ , l'étude menée à la première question montre que  $H$  est engendré par  $a^{n/d}$ .
- Nous sommes ici en notation additive. Soit  $x \in \llbracket 0; n-1 \rrbracket$ , l'élément  $\bar{x}$  est d'ordre  $d$  dans  $\mathbb{Z}/n\mathbb{Z}$  si, et seulement si  $\overline{dx} = \bar{0}$  et  $\forall k \in \llbracket 1; d-1 \rrbracket$ ,  $\overline{kx} \neq \bar{0}$ . Cela équivaut à l'existence de  $u \in \llbracket 1; d-1 \rrbracket$  premier avec  $d$  tel que  $x = \frac{n}{d}u$ . Par conséquent,  $\mathbb{Z}/n\mathbb{Z}$  possède  $\varphi(d)$  éléments d'ordre  $d$ . En partitionnant les éléments de  $\mathbb{Z}/n\mathbb{Z}$  suivant leur ordre (qui doit diviser  $n$ ), on en déduit que  $n = \sum_{d|n} \varphi(d)$ .

**Exercice 6.9**

On a  $(xy)^{pq} = x^{pq}y^{pq} = e$ . Donc l'ordre de  $xy$  est un diviseur de  $pq$ . On note  $d$  l'ordre de  $xy$ . On a  $(xy)^d = e$  et  $(xy)^{dp} = e = x^{dp}y^{dp} = y^{dp}$ . Ainsi  $y^{dp} = e$  et  $q|(dp)$ . Puisque  $p$  et  $q$  sont premiers entre eux alors  $q|d$ . De même  $p|d$ . Puisque  $p \wedge q = 1$ , on en déduit que  $pq|d$ . Finalement  $d = pq$ .

**Exercice 6.10**

- À partir de la décomposition en facteurs premiers, on peut écrire  $p$  et  $q$  sous la forme suivante :

$$p = p_1^{u_1} \cdots p_r^{u_r} p_1^{\alpha_1} \cdots p_j^{\alpha_j} p' \quad \text{et} \quad q = p_1^{u_1} \cdots p_r^{u_r} p_{j+1}^{\alpha_{j+1}} \cdots p_r^{\alpha_r} q',$$

où  $p_1, \dots, p_r$  sont des nombres premiers distincts,  $j \leq r$ ,  $p'$  et  $q'$  ne sont divisibles par aucun des  $p_i$  et sont premiers entre eux. Soit  $m$  le PPCM de  $p$  et  $q$ . Grâce à la décomposition précédente, on a

$$m = \underbrace{p_1^{u_1+\alpha_1} \cdots p_j^{u_j+\alpha_j}}_{=a} p' \underbrace{p_{j+1}^{u_{j+1}+\alpha_{j+1}} \cdots p_r^{u_r+\alpha_r}}_{=b} q',$$

donc  $m$  s'écrit  $ab$ , avec  $a|p$ ,  $b|q$  et  $a \wedge b = 1$ . Or  $x^{p/a}$  est d'ordre  $a$  et  $y^{q/b}$  est d'ordre  $b$ , et comme  $a$  et  $b$  sont premiers entre eux, leur produit est d'ordre  $m = ab$ .

- On sait que  $G$  est d'ordre  $p-1$ . On note  $s$  comme indiqué. On sait que  $G$  possède un élément d'ordre  $s$ . Il suffit de montrer que  $s = p-1$  pour montrer que  $G$  est cyclique. Par le théorème de Lagrange, l'ordre d'un élément est un diviseur de  $p-1$  donc  $s|(p-1)$ . Si  $g \in G$  alors son ordre est un diviseur de  $s$  donc  $g$  est racine du polynôme  $X^s - 1$  (dans  $\mathbb{Z}/p\mathbb{Z}$ ). Or un polynôme de  $\mathbb{K}[X]$  (où  $\mathbb{K}$  est un corps) est de degré supérieur ou égal à son nombre de racines distinctes. Il est de degré au moins  $p-1$ . On a donc  $s \geq p-1$  et finalement  $s = p-1$ .

**Exercice 6.11**

On note  $a$  un générateur de  $G$  et  $n$  son ordre. On a  $G = \{e, a, a^2, \dots, a^{n-1}\}$ . Soit  $H$  un sous-groupe de  $G$ . On note  $p = \min\{k \in \llbracket 1; n-1 \rrbracket, a^k \in H\}$ . On vérifie alors que  $H$  est le sous-groupe cyclique engendré par  $a^p$ . On a déjà  $a^p \in H$  et  $\langle a^p \rangle \subset H$ . Soit  $m \in \mathbb{N}$  tel que  $a^m \in H$ . On effectue la division euclidienne par  $p$  :  $m = qp + r$ . Or  $a^r = a^m (a^p)^{-q} \in H$  et  $r = 0$  par définition de  $p$ . On a donc  $H = \langle a^p \rangle$  et finalement l'égalité.

**Exercice 6.12**

Soit  $x \in G$ . Le sous-groupe engendré par  $x$  est d'ordre fini, sinon il serait isomorphe à  $(\mathbb{Z}, +)$  et contiendrait un nombre infini de sous-groupe (et  $G$  également).

Tout sous-groupe  $\langle x \rangle$  avec  $x \in G$  est cyclique. Le nombre de sous-groupes cycliques de  $G$  est donc fini par hypothèse. On suppose que l'ensemble de ces sous-groupes est  $\langle x_1 \rangle, \dots, \langle x_p \rangle$ . Si  $x \in G$  alors  $\langle x \rangle$  est l'un de ces sous-groupes donc  $x$  appartient à l'un des  $\langle x_i \rangle$ . Ainsi  $G$  est la réunion (pas disjointe) de ces  $p$  sous-groupes finis donc  $G$  est fini.

## Exercice 6.13

- on vérifie assez facilement que  $\mathbb{Z}[i]$  est un sous-anneau de  $\mathbb{C}$  et il reste ainsi intègre (car  $\mathbb{C}$  l'est).
- Pour déterminer les inversibles : on peut partir de  $z = a + ib \in \mathbb{Z}[i]$  et cherche  $z' = a' + ib'$  tel que  $zz' = 1$ . Un moyen efficace est de considérer l'application (norme au carré) :  $N : z = a + ib \mapsto z\bar{z} = a^2 + b^2$ . Elle vérifie  $N(zz') = zz'N(z') = N(z)N(z')$ . Ainsi si  $zz' = 1$  alors  $N(z)N(z') = 1$  (on prend le module au carré pour rester avec des valeurs entières) d'où  $N(z) = 1$ . Les seuls éléments possibles sont donc  $pm1$  et  $\pm i$  et ils conviennent.

## Exercice 6.14

- On vérifie tout d'abord qu'on a bien défini une relation d'équivalence : on a évidemment  $x\mathcal{R}x$  et si  $x\mathcal{R}y$  alors  $y\mathcal{R}x$ . De même la transitivité est immédiate. Deux éléments d'une même classe d'équivalence ont même image. Cela permet de définir une application  $\tilde{f}$ . On pourrait montrer que c'est même un morphisme de groupes (en commençant à montrer que  $G/\mathcal{R}$  a une structure de groupe mais on déborde pas mal). L'application est surjective : si  $z \in \text{Im } f$ , il existe  $x \in G$  tel que  $z = f(x)$  et alors  $\tilde{f}(\bar{x}) = z$ . Elle est injective car si  $f(\bar{x}) = f(\bar{y})$  alors  $f(x) = f(y)$  et  $x$  et  $y$  sont dans la même classe d'équivalence. L'application est bijective. On vérifie enfin que chaque classe d'équivalence comporte exactement  $|\ker f|$  éléments. Si  $f(y) = f(x)$  alors  $f(y * x^{-1}) = e_H$  et  $y * x^{-1} \in \ker f$  d'où il existe  $g \in \ker f$  tel que  $y = x * g$ . Réciproquement si  $y = x * g$  alors  $f(x) = f(y)$ . Les éléments  $x * g$  lorsque  $g$  décrit  $\ker f$  sont deux à deux distincts. Ainsi  $\bar{x}$  comporte autant d'éléments que  $\ker f$ .
- On a une partition de  $G$  par les classes d'équivalences. Il y en a  $|\text{Im } f|$  et chacune comporte  $|\ker f|$  éléments ce qui donne la formule.
- Si  $f(x) = e$  alors  $f^2(x) = f(e) = e$  donc  $\ker f \subset \ker f^2$ . De même si  $y \in \text{Im } f^2$  alors  $y \in \text{Im } f$  et  $\text{Im } f^2 \subset \text{Im } f$ . On alors les équivalences  $\ker f = \ker f^2$  si et seulement si les deux sont de même cardinal et de même pour les images. En utilisant alors  $|G| = |\text{Im } f| \cdot |\ker f| = |\text{Im } f^2| \cdot |\ker f^2|$  (puisque  $f^2$  est aussi un automorphisme de  $G$ ), on a

$$\ker f = \ker f^2 \Leftrightarrow |\ker f| = |\ker f^2| \Leftrightarrow |\text{Im } f| = |\text{Im } f^2| \Leftrightarrow \text{Im } f = \text{Im } f^2.$$

## Exercice 6.15

On note  $G = \mathbb{Z}/p\mathbb{Z}$ .

- On considère  $f$  l'application de  $(\mathbb{Z}/p\mathbb{Z}^*, \times)$  dans lui-même qui à  $x$  associe  $x^2$  (le groupe multiplicatif  $\mathbb{Z}/p\mathbb{Z}^*$  comporte  $p-1$  éléments). C'est un morphisme de groupes. On a  $x^2 = 1$  si et seulement si  $(x-1)(x+1) = 0$  donc si et seulement si  $x = 1$  ou  $x = -1$ . On a donc  $\ker f$  qui comporte deux éléments. On a alors  $|\text{Im } f| = \frac{p-1}{2}$ . On ajoute alors 0 comme dernier carré. Il y a donc  $\frac{p+1}{2}$  carrés dans  $\mathbb{Z}/p\mathbb{Z}$ .
- si  $x$  est un carré, il existe  $y \in G$  tel que  $x = y^2$  et alors  $x^{(p+1)/2} = y^{p+1} = y^{p-1}y^2$  or  $y^{p-1} = 1$  car  $p-1 = \varphi(p)$  et l'ordre de  $y$  divise  $\varphi(p)$ . Ainsi  $x^{(p+1)/2} = x$ . Puisque  $G$  est un corps, il est intègre et un polynôme de degré  $k$  admet au maximum  $k$  racines (si  $x_0$  est racine, on peut factoriser par  $(x - x_0)$ ). Le polynôme admet pour racines tous les carrés. Il sont au nombre de  $\frac{p+1}{2}$  donc toutes les racines de ce polynôme sont exactement les carrés de  $G$ .
- $-1$  est un carré si et seulement si  $(-1)^{(p+1)/2} = -1$ . On note  $p = 2q + 1$ , alors  $\frac{p+1}{2} = q + 1$  et  $-1$  est un carré si et seulement si  $q$  est pair. Finalement,  $-1$  est un carré dans  $\mathbb{Z}/p\mathbb{Z}$  si et seulement si  $p$  est un nombre premier de la forme  $4q + 1$ .
- Si  $p = 4k + 1$ , il y a  $p - 1$  solutions. Si  $p = 4k + 3$ , il y a  $p + 1$  solutions...

## Exercice 6.16

- Soit  $g = x + \sqrt{2}y \in G$ . On a  $x^2 - 2y^2 = 1 = (x + \sqrt{2}y)(x - \sqrt{2}y)$  et  $x^2 > 2y^2$ . Ainsi  $x > \sqrt{2}|y| \geq -\sqrt{2}y$ . On en déduit que  $x + \sqrt{2}y > 0$  (et aussi  $x - \sqrt{2}y$ ).
- on vérifie différente propriété :
  - $G$  est non vide car  $1 = 1 + \sqrt{2} \cdot 0 \in G$ .
  - le produit est interne : on prend  $g = x + \sqrt{2}y$  et  $g' = x' + \sqrt{2}y'$  dans  $G$  et on veut montrer que  $h = gg'$  l'est encore. Pour commencer  $h = (xx' + 2yy') + (xy' + yx')\sqrt{2}$ . On doit montrer que  $xx' + 2yy'$  est dans  $\mathbb{N}^*$ . Il est évidemment dans  $\mathbb{Z}$ . Comme au début, on a  $x > \sqrt{2}|y| \geq 0$  et  $x' > \sqrt{2}|y'| \geq 0$  donc  $xx' > 2|yy'| \geq -2yy'$ . Finalement  $xx' + 2yy' > 0$ . L'élément est bien sous la forme  $a + \sqrt{2}b$  avec  $a \in \mathbb{N}^*$  et  $b \in \mathbb{Z}$ . Il reste à prouver que  $h = a + \sqrt{2}b$  vérifie  $a^2 - 2b^2 = 1$ . On peut le faire par calcul compliqué ou simplement remarquer que  $x^2 - 2y^2 = (x - \sqrt{2}y)(x + \sqrt{2}y)$ . Si  $g = x + \sqrt{2}y$ , on note  $\bar{g} = x - \sqrt{2}y$  et on remarque que  $g\bar{g} = x^2 - 2y^2 = 1$  soit  $\bar{g} = 1/g$ . On a alors  $(g')\overline{gg'} = gg'\bar{g}\bar{g}'$  (on vérifie que  $\overline{gg'} = \bar{g}\bar{g}'$ ) et en commutant et associant on trouve 1. Ainsi  $gg'$  est dans  $G$ .
  - On a au passage montré que le symétrique de  $g$  est  $\bar{g} = \frac{1}{g}$  et qu'il est aussi dans  $G$ .
 Finalement  $G$  est un sous-groupe de  $(\mathbb{R}_+^*, \times)$ .
- On a  $(x + \sqrt{2}y)(x - \sqrt{2}y) = 1$ . Puisque  $x + \sqrt{2}y \geq 1 + \sqrt{2} > 1$ , on a  $x - \sqrt{2}y \in ]0, 1[$ .
- Les éléments de  $G \cap ]1, +\infty[$  sont ceux qui s'écrivent  $x + \sqrt{2}y$  avec  $x, y \in \mathbb{N}^*$  et  $x^2 - 2y^2 = 1$ . On détermine les premiers éléments qu'on trouve :
  - $x = 1$ , le seul élément dans  $G$  est  $1 + 0\sqrt{2} = 1$ ,
  - $x = 2$ , pas de solution puisqu'on doit avoir  $2y^2 = 3$ . Plus généralement, si  $x$  est pair  $x^2 - 2y^2$  l'est aussi donc ne peut être 1.
  - $x = 3$ , on a  $y^2 = 4$  et  $3 \pm 2\sqrt{2}$  sont dans  $G$  avec  $3 + 2\sqrt{2} > 1$ ,
  - si  $x \geq 5$  et  $y \geq 1$  alors  $x + \sqrt{2}y \geq 5 + \sqrt{2} > 3 + 2\sqrt{2}$ .
 Le plus petit élément strictement supérieur à 1 dans  $G$  est  $g_0 = 3 + 2\sqrt{2}$ .
- Considérons  $H = \langle g_0 \rangle = \{g_0^n, n \in \mathbb{Z}\}$ . C'est un sous-groupe monogène de  $G$ . Soit  $g > 1$  dans  $G$ . Puisque  $g_0 > 1$ , il existe  $n \in \mathbb{Z}$  tel que  $g_0^n \leq$

$g < g_0^{n+1}$ . On a alors  $g_0^{-n}g \in G$  et  $1 \leq g_0^{-n}g < g_0$ . Par définition de  $g_0$ , on a  $g_0^{-n}g = 1$  et  $g = g_0^n$ . En conclusion  $G = H = \langle g_0 \rangle = \{g_0^n, n \in \mathbb{Z}\}$ . On a en fait déterminé toutes les solutions entières de l'équation  $x^2 - 2y^2 = 1$  (avec  $x \in \mathbb{N}$ , mais on peut prendre les mêmes en changeant le signe de  $x$ ) : elles sont toutes obtenues à partir des puissances  $g_0^n$  pour  $n \in \mathbb{N}$  (celles avec  $n \in \mathbb{Z}$  donnent les couples  $(x, y)$  avec  $y < 0$ ).

**Exercice 6.17**

- Soient  $x, y$  dans  $G$ . On a  $(xy)^2 = xyxy = e$ . En multipliant à gauche par  $x$  et à droite par  $y$ , on a  $xxxyxy = xy$  soit  $yx = xy$ . Le groupe  $G$  est donc commutatif.
- Puisque  $a^2 = e$  et  $a \neq e$ ,  $\{e, a\} = \langle a \rangle$  sous-groupe engendré par  $a$ . Par le théorème de Lagrange, l'ordre de ce sous-groupe divise l'ordre de  $G$ . Ainsi  $G$  est d'ordre pair.
- On commence par vérifier que  $H \cap aH$  est vide : si  $x \in H \cap aH = \tilde{H}$  alors, il existe  $h_1, h_2$  dans  $H$  tels que  $x = h_1 = ah_2$ . On en déduit que  $a = h_1h_2^{-1}$  et, puisque  $H$  est un sous-groupe de  $G$ ,  $x \in H$  d'où une contradiction. On a déjà  $\text{card}(\tilde{H}) = 2\text{card}H$ . Montrons que c'est un sous-groupe de  $G$ . Soit  $x, y$  dans  $\tilde{H}$  : on a  $x = a^{\varepsilon_1}h_1$  et  $y = a^{\varepsilon_2}h_2$  avec  $h_1, h_2 \in H$  et  $\varepsilon_1$  et  $\varepsilon_2$  égaux à 0 (si dans  $H$ ) ou 1 (si dans  $aH$ ). On a alors, puisque  $G$  est commutatif et que  $a^{-1} = a$ ,  $xy^{-1} = a^{\varepsilon_1 - \varepsilon_2}h_1h_2^{-1}$ . Puisque  $\varepsilon_1 - \varepsilon_2$  vaut 0, 1 ou  $-1$ , on a bien  $xy^{-1}$  dans  $\tilde{H}$ . On a montré que  $\tilde{H}$  est un sous-groupe de  $G$ .
- On part de  $a \neq e$  et  $H_1 = \{e, a\}$ . Soit  $H_1 = G$  et c'est fini, soit ce n'est pas le cas. Il existe  $a_2 \in G$  mais pas dans  $H_1$ . On construit alors le sous-groupe  $H_2 = H_1 \cup a_2H_1$ . On procède de proche en proche : une fois construit  $H_p$  sous-groupe de cardinal  $2^p$  de  $G$ , soit  $H_p = G$  soit ce n'est pas le cas et on construit alors de même un sous-groupe de  $G$ ,  $H_{p+1} = H_p + a_{p+1}H_p$  de cardinal  $2^{p+1}$ . Puisque  $G$  est de cardinal fini, on finit par tomber sur  $G$ .  
Si on veut une version « plus propre », on peut  $\mathcal{A}$  l'ensemble des sous-groupes d'ordre une puissance de 2 de  $G$ . On considère un sous-groupe de cardinal maximal dans  $\mathcal{A}$ . Si ce n'est pas  $G$ , on peut alors en construire un autre de cardinal double d'où une contradiction. Pour les plus motivés, on peut mettre une structure de  $\mathbb{Z}/2\mathbb{Z}$  espace vectoriel sur  $G$  (réfléchir comment...), utiliser une base  $e_1, \dots, e_k$  de  $G$  pour obtenir que  $\text{card}G$  est  $2^k$ .
- Un élément de  $G$  est d'ordre 1 (le seul est  $e$ ), 2,  $p$  ou  $2p$ . Si aucun élément est d'ordre  $p$ , tous les éléments de  $G$  différents de  $e$  sont d'ordre 2 ou  $2p$ . Si  $x$  est d'ordre  $2p$  alors  $x^2$  est d'ordre  $p$  ce qu'on a exclu. Finalement tous les éléments sont d'ordre 2 (sauf  $e$ ) et  $G$  est de cardinal une puissance de 2. Si  $p$  est différent de 2 alors on a une contradiction. Il ne reste plus qu'à regarder le cas où  $p = 2$  et  $G$  d'ordre 4. L'ordre d'un élément  $x$  différent de  $e$  est 2 (c'est fini,  $p = 2$ ) ou 4 et dans ce dernier cas  $x^2$  est d'ordre  $p = 2$ .

**Exercice 6.18**

- si  $KH = HK$ . Soit  $hk, h'k' \in HK$  :  $(hk)(h'k')^{-1} = h(kk'^{-1})h'^{-1}$ . On a  $kk'^{-1} \in H$  et  $h'^{-1} \in K$  donc  $(kk'^{-1})h'^{-1} \in HK = KH$ . On peut le réécrire sous la forme  $h''k''$  et enfin  $(hk)(h'k')^{-1} = hh''k'' \in HK$  donc  $HK$  sous-groupe de  $G$ .  
→ si  $HK$  groupe. Soit  $x \in KH$ . Il existe  $k \in K$  et  $h \in H$  tel que  $x = kh$ . On a alors  $h^{-1}k^{-1} \in HK$  et l'inverse,  $kh = x$ , est encore dans  $HK$  puisque  $HK$  est un groupe. On a donc  $KH \subset HK$ . Réciproquement si  $x = hk \in HK$  alors c'est l'inverse d'un élément de  $HK$  :  $x = (x^{-1})^{-1}$ . Puisque  $x^{-1} \in HK$ , on peut l'écrire  $x^{-1} = h'k'$  et alors  $x = hk = (h'k')^{-1} = k'^{-1}h'^{-1} \in KH$ . D'où  $HK \subset KH$ . Finalement  $HK = KH$ .
- Tout d'abord il faut que  $H \times K$  et  $HK$  soient des groupes. Le premier a une structure naturelle de groupe, le second est un sous-groupe de  $G$  si et seulement si  $HK = KH$ . Supposons avoir cette condition. Si  $x = (h_1, k_1)$  et  $y = (h_2, k_2)$  sont deux éléments de  $H \times K$ , on a  $xy = (h_1h_2, k_1k_2)$  et on veut  $f(xy) = f(x)f(y)$  soit  $h_1h_2k_1k_2 = h_1k_1h_2k_2$ . Par simplification il faut et il suffit d'avoir  $h_2k_1 = k_1h_2$  et ce pour tout  $h_1 \in H$  et  $k_2 \in K$ . Une condition nécessaire et suffisante est donc  $hk = kh$  pour tout  $(h, k) \in H \times K$  (ce qui est a priori plus restrictif que  $HK = KH$  mais qui entraîne cette condition).  
Soit  $(h, k) \in H \times K$ . On a  $(h, k) \in \ker f$  si  $hk = e$  donc  $k = h^{-1}$  est dans  $H$  et  $K$ . Réciproquement tout élément  $(h, h^{-1})$  avec  $h \in H \cap K$  est dans le noyau. On en déduit que  $\ker f = \{(h, h^{-1}), h \in H \cap K\}$ . L'application est injective si et seulement si  $H \cap K = \{e\}$ . Elle est immédiatement surjective par définition de  $HK$  et dans ce cas elle est bijective.

**Exercice 6.19**

- Soient  $z$  et  $z' \in G_p$  ; il existe deux entiers  $j$  et  $k$  tels que  $z^{p^j} = 1$  et  $z'^{p^k} = 1$ , d'où  $(zz')^{p^{\max(j,k)}} = 1$  et  $(z^{-1})^{p^j} = 1$  donc  $zz'$  et  $z^{-1} \in G_p$ . Comme  $1 \in G_p$ , il en résulte que  $G_p$  est un sous-groupe de  $\mathbb{C}^*$ .
- On note  $U_k$  le groupe multiplicatif des racines  $p^{k^{\text{ièmes}}}$  de l'unité dans  $\mathbb{C}$ . On rappelle que  $U_k$  est cyclique et que  $z$  est un générateur de  $U_k$  si, et seulement si  $z$  est de la forme  $e^{2i\pi u/p^k}$  avec  $u$  premier avec  $p$ , autrement dit si, et seulement si  $z \in U_k \setminus U_{k-1}$ . On a  $G_p = \bigcup_{k \in \mathbb{N}} U_k$ , la suite d'ensembles  $(U_k)$  étant croissante pour l'inclusion. Soit  $G$  un sous-groupe propre de  $G_p$ . Si  $G$  contient un élément de  $U_k \setminus U_{k-1}$ , alors  $G$  contient  $U_k$ , donc tous les  $U_j$  pour  $j \leq k$ . Comme  $G$  n'est pas égal à  $G_p$ , l'ensemble des entiers  $k$  tels que  $G$  contienne un élément de  $U_k \setminus U_{k-1}$  est majoré, donc possède un plus grand élément  $r$ . Cet élément engendre  $U_r$ , donc  $G \supset U_r$ . Mais par définition de  $r$ ,  $G \subset U_r$ . Finalement, les sous-groupes propres de  $G_p$  sont les sous-groupes  $U_k$  ; ils sont tous cycliques, emboîtés les uns dans les autres, donc aucun n'est maximal.
- Supposons que la famille  $(z_1, \dots, z_n)$  engendre  $G_p$ . Chaque élément  $z_k$  est d'ordre  $p^{\alpha_k}$  où  $\alpha_k$  est un entier naturel. En notant  $\alpha = \max_{1 \leq k \leq n} \alpha_k$ , on a  $z_k^{p^\alpha} = 1$  pour tout  $k$ , or tout élément  $z$  de  $G_p$  est un produit d'éléments de la forme  $z_i$ , donc on a également  $z^{p^\alpha} = 1$ , d'où  $G_p \subset U_{p^\alpha}$ , ce qui est absurde.

**Exercice 6.20**

On considère un tel morphisme  $\varphi$ . On doit avoir  $\varphi(\sigma \circ \sigma') = \varphi(\sigma)\varphi(\sigma')$  pour toutes permutations  $\sigma$  et  $\sigma'$ .

→ On sait que  $\mathcal{S}_n$  est engendré par les transpositions; on va donc étudier  $\varphi$  sur ces permutations particulières.

→ si  $\tau$  est une transposition alors  $\tau^2 = \text{id}$  et  $\varphi(\tau^2) = \varphi(\tau)^2 = 1$ . On en déduit que  $\varphi(\tau) = \pm 1$ .

→ on montre que si  $\tau_1$  et  $\tau_2$  sont deux transpositions alors elles sont conjuguées : il existe  $\sigma$  telle que  $\tau_2 = \sigma\tau_1\sigma^{-1}$  (ou, ce qui est souvent plus simple pour les calculs,  $\tau_2\sigma = \sigma\tau_1$ ). On aura alors  $\varphi(\sigma\tau_1\sigma^{-1}) = \varphi(\sigma)\varphi(\tau_1)\varphi(\sigma^{-1}) = \varphi(\tau_1)$ . Ainsi toutes les transpositions ont même valeur par  $\varphi$ . Soit elles valent toutes 1 et dans ce cas  $\varphi$  est l'application constante égale à 1, soit  $\varphi$  est la signature.

*Conjugaison* : on considère deux transpositions  $\tau_{ij}$  et  $\tau_{kl}$  et on veut montrer qu'elles sont conjuguées.

→ si les deux sont à support disjoint : on pose  $\sigma = \tau_{ik}\tau_{jl}$ . On vérifie que  $\tau_{ij}\sigma = \sigma\tau_{kl}$ .

→ si on a un élément en commun dans les supports :  $\tau_{ij}$  et  $\tau_{ik}$  avec  $j \neq k$ . Avec  $\sigma = \tau_{kj}$  on a de nouveau  $\tau_{ij}\sigma = \sigma\tau_{kl}$ .

**Exercice 6.22**

On a

$$U_n = \sum_{k=1}^n \sigma(k) = \sum_{k=1}^n \left( \sum_{q|k} q \right) = \sum_{(p,q) \in \mathbb{N}^{*2}, pq \leq n} q.$$

Alors

$$U_n = \sum_{p=1}^n \left( \sum_{q \leq \frac{n}{p}} q \right) = \sum_{p=1}^n \left( \sum_{q=1}^{\lfloor \frac{n}{p} \rfloor} q \right) = \frac{1}{2} \sum_{p=1}^n \left\lfloor \frac{n}{p} \right\rfloor \left( \left\lfloor \frac{n}{p} \right\rfloor + 1 \right)$$

Or, pour tout  $x \in \mathbb{R}$ ,  $x-1 < \lfloor x \rfloor \leq x$ , donc

$$\frac{1}{2} \sum_{p=1}^n \left( \frac{n}{p} - 1 \right) \frac{n}{p} \leq U_n \leq \frac{1}{2} \sum_{p=1}^n \left( \frac{n}{p} + 1 \right) \frac{n}{p},$$

$$\frac{n^2}{2} \left( \sum_{p=1}^n \frac{1}{p^2} \right) - \frac{n}{2} \left( \sum_{p=1}^n \frac{1}{p} \right) \leq U_n \leq \frac{n^2}{2} \left( \sum_{p=1}^n \frac{1}{p^2} \right) + \frac{n}{2} \left( \sum_{p=1}^n \frac{1}{p} \right)$$

Or,  $\sum_{p=1}^n \frac{1}{p} = O(\ln n)$ ,  $\sum_{p=1}^{+\infty} \frac{1}{p^2} = \zeta(2) = \frac{\pi^2}{6}$  et  $\frac{\pi^2}{6} - \frac{1}{n} \leq \sum_{p=1}^n \frac{1}{p^2} \leq \frac{\pi^2}{6}$ , ce qui assure que  $U_n = \frac{\pi^2 n^2}{12} + O(n \ln n)$ , donc  $U_n \underset{n \rightarrow +\infty}{\sim} \frac{\pi^2 n^2}{12}$ .

**Exercice 6.23**

Si  $A$  est un sous-groupe de  $G$  et  $B$  un sous-groupe de  $H$ , alors  $A \times B$  est un sous-groupe de  $G \times H$ . Réciproquement montrons que tout sous-groupe  $T$  de  $G \times H$  est de cette forme. Comme  $p_1 : G \times H \rightarrow G, (x, y) \mapsto x$  et  $p_2 : G \times H \rightarrow H, (x, y) \mapsto y$  sont des morphismes de groupes,  $p_1(T) = A$  est un sous-groupe de  $G$  et  $p_2(T) = B$  un sous-groupe de  $H$ . Évidemment  $T \subseteq A \times B$ . Comme  $A$  et  $B$  sont images de  $T$  par des morphismes surjectifs, leurs cardinaux divisent  $|T|$ . Or  $|A|$  et  $|B|$  sont premiers entre eux, donc  $|A| \times |B|$  divise  $|T|$  et ainsi,  $T = A \times B$ . En conclusion, les sous-groupes de  $G \times H$  sont les  $A \times B$ , où  $A$  est un sous-groupe de  $G$  et  $B$  un sous-groupe de  $H$ , d'où le résultat demandé.