# **Fiche n° 2:** Morphisme, sous-groupe distingué, quotient

**Exercice 1** Soient $G$, $G'$ deux groupes et $f$ un homomorphisme de $G$ dans $G'$. Montrer que si $A \subset G$, alors $f(\langle A\rangle) = \langle f(A)\rangle$. Montrer par contre qu'il est faux que si $A' \subset G'$, alors $f^{-1}(\langle A'\rangle) = \langle f^{-1}(A')\rangle$.

**Exercice 2** Soit $G$ un groupe tel que l'application $x \to x^{-1}$ soit un morphisme. Montrer que $G$ est commutatif.

**Exercice 3** Déterminer tous les homomorphismes de groupes de $\mathbb{Z}/3\mathbb{Z}$ dans $\mathbb{Z}/7\mathbb{Z}$, de $\mathbb{Z}/3\mathbb{Z}$ dans $\mathbb{Z}/12\mathbb{Z}$, de $\mathbb{Z}/12\mathbb{Z}$ dans $\mathbb{Z}/3\mathbb{Z}$.

**Exercice 4** Soient $G$ un groupe et $n \geqslant 1$ un entier tels que l'application $x \to x^n$ soit un automorphisme de $G$. Montrer que pour tout élément $x$ de $G$, $x^{n-1}$ appartient au centre de $G$.

**Exercice 5** Montrer que le groupe des automorphismes du groupe $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ est isomorphe au groupe symétrique $S_3$.

**Exercice 6** Montrer qu'un sous-groupe d'indice 2 dans un groupe $G$ est distingué dans $G$.

**Exercice 7** Soit $G$ un groupe et $H$ un sous-groupe. On suppose que le produit de deux classes à gauche modulo $H$ est une classe à gauche modulo $H$. Montrer que $H$ est distingué dans $G$.

**Exercice 8** Soit $G$ un groupe et $\simeq$ une relation d'équivalence sur $G$. On suppose que cette relation est compatible avec la loi de groupe, c'est à dire que

$$\forall x, y \in G \quad \forall x', y' \in G \quad x \simeq x' \quad \text{et} \quad y \simeq y' \quad \text{alors} \quad xy \simeq x'y'$$

Montrer que la classe $H$ de l'élément neutre 1 est un sous-groupe distingué de $G$ et que

$$\forall x, x' \in G \quad x \simeq x' \quad \text{est} \quad \text{équivalent} \quad \text{à} \quad x'x^{-1} \in H$$

**Exercice 9** Soit $G$ un groupe et $K \subset H \subset G$ deux sous-groupes. On suppose que $H$ est distingué dans $G$ et que $K$ est caractéristique dans $H$ (i.e. stable par tout automorphisme de $H$). Montrer qu'alors $K$ est distingué dans $G$.
Donner un exemple de groupe $G$ et de deux sous-groupes $K \subset H \subset G$, $H$ étant distingué dans $G$ et $K$ étant distingué dans $H$, mais $K$ n'étant pas distingué dans $G$.

**Exercice 10** (a) Montrer que pour tous entiers $m, n > 0$ premiers entre eux, les deux groupes $(\mathbb{Z}/mn\mathbb{Z})^\times$ et $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ sont isomorphes. En déduire que $\varphi(mn) = \varphi(m)\varphi(n)$, où $\varphi$ est la fonction indicatrice d'Euler.
(b) Le groupe multiplicatif $(\mathbb{Z}/15\mathbb{Z})^\times$ est-il cyclique ? Montrer que $(\mathbb{Z}/8\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, que $(\mathbb{Z}/16\mathbb{Z})^\times \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Etudier le groupe multiplicatif $(\mathbb{Z}/24\mathbb{Z})^\times$.

**Exercice 11** (a) Montrer que si $m$ et $n$ sont des entiers premiers entre eux et qu'un élément $z$ d'un groupe $G$ vérifie $z^m = z^n = e$ où $e$ désigne l'élément neutre de $G$, alors $z = e$.
(b) Montrer que si $m$ et $n$ sont deux entiers premiers entre eux, l'application

$$\phi : \mu_m \times \mu_n \to \mu_{mn}$$

qui au couple $(s, t)$ fait correspondre le produit $st$ est un isomorphisme de groupes

**Exercice 12** Montrer que les groupes $\mu_4$ et $\mu_2 \times \mu_2$ ne sont pas isomorphes. De façon générale montrer que si $m$ et $n$ sont des entiers qui ne sont pas premiers entre eux, les groupes $\mu_{mn}$ et $\mu_m \times \mu_n$ ne sont pas isomorphes.

**Exercice 13** Soit $n$ et $d$ deux entiers tels que $d$ divise $n$. On définit une application $f : \mu_n \to \mu_d$ qui à $s$ associe $s^{n/d}$. Montrer que $f$ est un morphisme surjectif de groupes dont le noyau est $\mu_{n/d}$.

**Exercice 14** Soit $f : G \to H$ un morphisme de groupes finis. Soit $G'$ un sous-groupe de $G$. Montrer que l'ordre de $f(G')$ divise les ordres de $G'$ et de $H$.

**Exercice 15** Soit $f : G \to H$ un morphisme de groupes finis. Soit $G'$ un sous-groupe de $G$ d'ordre premier à l'ordre de $H$. Montrer que $G' \subset \ker(f)$.

**Exercice 16** Soit $G$ un groupe fini et $H$ et $K$ deux sous-groupes de $G$. On suppose que $H$ est distingué dans $G$, que $|H|$ et $|G/H|$ sont premiers entre eux et $|H| = |K|$. Montrer que $H = K$.

**Exercice 17** Soit $f$ un morphisme de groupes $f : \mathbb{Q} \to \mathbb{Q}^\times_{>0}$, $\mathbb{Q}$ étant muni de l'addition et $\mathbb{Q}^\star_{>0}$ muni de la multiplication. Calculer $f(n)$ en fonction de $f(1)$ pour tout entier $n > 0$. Montrer que les deux groupes précédents ne sont pas isomorphes.

**Exercice 18** Trouver tous les morphismes du groupe additif $\mathbb{Q}$ dans lui même.
Même question de $\mathbb{Q}$ dans $\mathbb{Z}$.
Même question de $\mathbb{Z}/m\mathbb{Z}$ dans $\mathbb{Z}$.

**Exercice 19** Etant donnés deux entiers $m, n > 0$, déterminer tous les morphismes de groupe de $\mathbb{Z}/m\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$, puis tous les automorphismes de $\mathbb{Z}/n\mathbb{Z}$.

**Exercice 20** Soit $G$ un groupe et $H$ un sous groupe distingué de $G$ d'indice $n$. Montrer que pour tout $a \in G$, $a^n \in H$. Donner un exemple de sous-groupe $H$ non distingué de $G$ pour lequel la conclusion précédente est fausse.

**Exercice 21** Soit $G$ un groupe fini et $H$ un sous-groupe distingué d'ordre $n$ et d'indice $m$. On suppose que $m$ et $n$ sont premiers entre eux. Montrer que $H$ est l'unique sous-groupe de $G$ d'ordre $n$.

**Exercice 22** Montrer que $\mathrm{SL}_n(\mathbb{R})$ est un sous-groupe distingué du groupe $\mathrm{GL}_n(\mathbb{R})$ et que le groupe quotient est isomorphe à $\mathbb{R}^\times$.

**Exercice 23** On considère les groupes suivants :

$$T = \{z \in \mathbb{C} \,|\, |z| = 1\} \quad \mu_n = \{z \in \mathbb{C} \,|\, z^n = 1\} \quad \mu_\infty = \{z \in \mathbb{C} \,|\, \exists n \quad z^n = 1\}$$

(a) Montrer les isomorphismes suivants :

$$\mathbb{R}/\mathbb{Z} \simeq T \quad \mathbb{C}^\times/\mathbb{R}^\times_{>0} \simeq T \quad \mathbb{C}^\times/\mathbb{R}^\times \simeq T \quad T/\mu_n \simeq T \quad \mathbb{C}^\times/\mu_n \simeq \mathbb{C}^\times$$

(b) Montrer que $\mu_\infty \simeq \mathbb{Q}/\mathbb{Z}$. Quels sont les sous-groupes finis de $\mu_\infty$ ?

(c) Montrer qu'un sous-groupe de type fini de $\mathbb{Q}$ contenant $\mathbb{Z}$ est de la forme $\frac{1}{q}\mathbb{Z}$. En déduire la forme des sous-groupes de type fini de $\mathbb{Q}/\mathbb{Z}$ et de $\mu_\infty$.

(d) Soit $p$ un nombre premier. Montrer que $\mu_{p^\infty} = \{z \in \mathbb{C} \,|\, \exists n \in \mathbb{N} \quad z^{p^n} = 1\}$ est un sous-groupe de $\mu_\infty$. Est-il de type fini ?

**Exercice 24** Soit $G$ un sous-groupe d'indice fini du groupe multiplicatif $\mathbb{C}^\times$. Montrer que $G = \mathbb{C}^\times$.

**Exercice 25** Soit $G$ un groupe et $H$ un sous-groupe contenu dans le centre $Z(G)$ de $G$. Montrer que $H$ est distingué dans $G$ et que, si le groupe quotient $G/H$ est cyclique, $G = Z(G)$.

**Exercice 26** Montrer qu'un groupe d'ordre $p^2$ où $p$ est un nombre premier est abélien.

**Exercice 27** Soit $G$ un groupe abélien de cardinal $pq$ où $p$ et $q$ sont deux nombres premiers distincts. Montrer que $G$ est un groupe cyclique.

**Exercice 28** (Théorème de Wilson).
Montrer qu'un nombre entier $p$ est premier ssi $(p-1)! + 1 \equiv 0$ [mod p].

**Exercice 29** (Théorème de Cauchy).
Soit $G$ un groupe abélien d'ordre $m$.
(a) Montrer que si $x^n = 1$ pour tout $x \in G$, alors $m$ divise une puissance de $n$.
(b) Soit $p$ un nombre premier divisant $m$. Montrer qu'il existe un élément de $G$ dont l'ordre est divisible par $p$.
(c) En déduire que si $p|m$, il existe un élément de $G$ d'ordre $p$.

**Exercice 30** (Indicateur d'Euler $\varphi(n)$). On considère le groupe additif $\mathbb{Z}/n\mathbb{Z}$ ($n \geqslant 2$).
(a) Montrer que pour tout $a \in \mathbb{Z}$, $\bar{a}$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$ ssi $a$ et $n$ sont premiers entre eux.
On note $\varphi(n)$ le nombre de générateurs de $\mathbb{Z}/n\mathbb{Z}$.
(b) Montrer que si $p$ est premier, $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ (où $\alpha \geqslant 1$ est un entier).
(c) Montrer que si $m$ et $n$ sont premiers entre eux, alors $\varphi(mn) = \varphi(m)\varphi(n)$. En déduire que pour $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, on a $\varphi(n) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_k})$.
(d) Montrer que pour tout entier $n \geqslant 1$, $\sum_{d|n} \varphi(d) = n$ et que cette propriété caractérise la fonction $\varphi$.

**Exercice 31** (a) Soit $G$ un groupe abélien fini d'ordre $n$. On suppose que pour tout diviseur $d$ de $n$, l'ensemble $G(d) = \{x \in G | x^d = 1\}$ a au plus $d$ éléments. Montrer qu'il y a dans $G$ exactement $\varphi(d)$ éléments d'ordre $d$.
(b) En déduire que si $K$ est un corps fini, alors le groupe multiplicatif $(K^\times, \times)$ est cyclique.

**Exercice 32** (a) Soit $p$ un nombre premier. Montrer que tout morphisme de groupes entre $\mathbb{F}_p^n$ et $\mathbb{F}_p^m$ est une application $\mathbb{F}_p$ -linéaire.
(b) Montrer que le groupe des automorphismes de $\mathbb{Z}/p\mathbb{Z}$ est isomorphe au groupe multiplicatif $\mathbb{F}_p^*$.
(c) Déterminer le nombre d'automorphismes de $\mathbb{F}_p^n$.

**Exercice 33** Déterminer le centre du groupe $GL_n(\mathbb{F}_p)$ des automorphismes de $(\mathbb{F}_p)^n$.

**Exercice 34** Soit $p$ un nombre premier. Montrer qu'un groupe abélien fini, dont tous les éléments différents de l'élément neutre sont d'ordre $p$, est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^n$.

**Exercice 35** (a) Soit $G$ un groupe et $H$ un sous-groupe distingué de $G$. On note $\varphi$ la surjection canonique $\varphi : G \to G/H$. Montrer que l'ordre d'un élément $x$ de $G$ est un multiple de l'ordre de $\varphi(x)$.
(b) Pour tout $x \in G$ on pose $\tau_x$ l'application de $G$ dans $G$ définie par $\tau_x(y) = xyx^{-1}$. Montrer que $\tau_x$ est un automorphisme de $G$ et que l'application

$$x \to \tau_x$$

est un morphisme de groupes de $G$ dans $\mathrm{Aut}(G)$. Quel est le noyau de ce morphisme ?
(c) On suppose que $G$ est fini et que $H$ est un sous-groupe distingué dont l'ordre est le plus petit nombre premier $p$ divisant l'ordre de $G$. Montrer que pour tout $x \in G$ l'ordre de la restriction à $H$ de $\tau_x$ est un diviseur de $p-1$ et de l'ordre de $G$. En déduire que $\tau_x$ restreint à $H$ est l'identité pour tout $x$ et donc que $H$ est contenu dans le centre de $G$.

**Exercice 36** Soit $G$ un groupe. On appelle groupe des commutateurs de $G$ et l'on note $D(G)$ le sous-groupe de $G$ engendré par les éléments de la forme $xyx^{-1}y^{-1}$. Montrer que $D(G)$ est distingué dans $G$ et que le quotient $G/D(G)$ est abélien. Montrer que $D(G)$ est le plus petit sous-groupe distingué de $G$ tel que le quotient de $G$ par ce sous-groupe soit abélien.

**Exercice 37** Soit $G$ un groupe d'ordre $p^3$ où $p$ est un nombre premier. Montrer que si $G$ n'est pas commutatif, $Z(G) = D(G)$ et que ce sous-groupe est d'ordre $p$.

# **Fiche n° 2:** Morphisme, sous-groupe distingué, quotient

***Indication 1*** Standard.

***Indication 2*** $(xy)^{-1} = x^{-1}y^{-1} \Rightarrow xy = yx$.

***Indication 10*** (a) est standard. En utilisant (a), on obtient $(\mathbb{Z}/15\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, lequel n'est pas cyclique puisque tous les éléments sont d'ordre 1, 2 ou 4. Le reste ne pose pas de grandes difficultés.

***Indication 11*** (a) Bezout. (b) $\phi$ est injectif et ensembles de départ et d'arrivée ont même cardinal.

***Indication 13*** $e^{2ik\pi/d} = \left(e^{2ik\pi/n}\right)^{n/d}$ $(k \in \mathbb{Z})$.

***Indication 14*** $f(G')$ est un sous-groupe de $H$ isomorphe à $G'/(\ker(f) \cap G')$.

***Indication 15*** Résulte de l'exercice 14.

***Indication 18*** Les morphismes du groupe $(\mathbb{Q}, +)$ dans lui-même sont de la forme $x \to ax$ avec $a \in \mathbb{Q}$. Les morphismes du groupe $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$ sont, parmi les précédents, ceux dont l'image est dans $\mathbb{Z}$ ; il n'y a que le morphisme nul. Les morphismes du groupe $(\mathbb{Z}/m\mathbb{Z}, +)$ dans $(\mathbb{Z}, +)$ sont déterminés par l'entier $f(1)$ qui doit vérifier $mf(1) = 0$ ; il n'y a que le morphisme nul, si $m \neq 0$.

***Indication 19*** L'ensemble $\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ des morphismes de groupe de $\mathbb{Z}/m\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ est un groupe abélien pour l'addition naturelle des morphismes. On note $\delta$ le pgcd de $m$ et $n$ et $m'$ et $n'$ les entiers $m/\delta$ et $n/\delta$. Si $p : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ désigne la surjection canonique, la correspondance associant à tout $f \in \mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ l'élément $f \circ p(1)$ induit un isomorphisme de groupe entre $\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ et le sous-groupe $n'\mathbb{Z}/n\mathbb{Z}$ du groupe additif $\mathbb{Z}/n\mathbb{Z}$, lequel est isomorphe à $\mathbb{Z}/\delta\mathbb{Z}$.
L'ensemble $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ des automorphismes de $\mathbb{Z}/n\mathbb{Z}$ est un groupe pour la composition. La correspondance précédente induit un isomorphisme entre $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ et le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ des inversibles de $\mathbb{Z}/n\mathbb{Z}$.

***Indication 22*** Le morphisme "déterminant" de $\mathrm{GL}_n(\mathbb{R})$ dans $\mathbb{R}^\times$ est surjectif et de noyau $\mathrm{SL}_n(\mathbb{R})$.

***Indication 25*** Si $\zeta$ est un élément de $G$ dont la classe modulo $H$ engendre $G/H$, alors tout élément de $G$ peut s'écrire $h\zeta^m$ avec $h \in H$ et $m \in \mathbb{Z}$.

***Indication 26*** Utiliser l'exercice 25 avec $H = Z(G)$ et le fait que le centre d'un $p$-groupe est non trivial.

***Indication 27*** Montrer d'abord que si $a$ est d'ordre $p$ et $b \in G \setminus < a >$, alors $b$ est d'ordre $q$ ou $pq$).

***Indication 29*** Pour le (a), faire une récurrence sur $m$ en introduisant le sous-groupe $H$ engendré par un élément de $G$ et le groupe quotient $G/H$. Utiliser (a) pour montrer (b), puis montrer (c).

***Indication 31*** Pour le (a), montrer d'abord que s'il existe un élément $x \in G$ d'ordre $d$, alors $\langle x \rangle = G(d)$). Pour le (b), utiliser le (d) de l'exercice précédent.

***Indication 33*** Exercice classique d'algèbre linéaire : $Z(\mathrm{GL}_n(\mathbb{F}_p)) = \mathbb{F}_p^\times \cdot \mathrm{Id}_n$ (où $\mathrm{Id}_n$ désigne la matrice identité d'ordre $n$).

***Indication 35*** Les questions (a) et (b) ne présentent aucune difficulté.

Pour la question (c), noter que, pour tout $x \in G$, on a $(\tau_x)^{|G|} = 1$, et que la restriction de $\tau_x$ à $H$ appartient à $\mathrm{Aut}(H) \simeq \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ (et utiliser l'exercice 19).

***Indication 36*** Aucune difficulté. Observer que tout conjugué d'un commutateur est un commutateur et qu'un quotient $G/H$ est abélien si et seulement si pour tous $u, v \in G$, on a $uvu^{-1}v^{-1} \in H$.

# **Fiche n° 2:** Morphisme, sous-groupe distingué, quotient

***Correction 4*** Soient $x, y \in G$ quelconques. De $(xy)^n = x^n y^n$, on déduit $(yx)^{n-1} = x^{n-1}y^{n-1}$ puis $(yx)^n = yx^n y^{n-1}$ et donc $y^n x^n = yx^n y^{n-1}$, ce qui donne $y^{n-1}x^n = x^n y^{n-1}$. Ainsi, pour tout $y \in G$, $y^{n-1}$ commute à tous les éléments de la forme $x^n$ avec $x \in G$, et est donc dans le centre de $G$, puisque l'application $x \to x^n$ est supposée surjective.

***Correction 5*** Tout automorphisme $\varphi$ du groupe $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ permute les trois éléments d'ordre 2, c'est-à-dire l'ensemble $G^*$ des trois éléments non triviaux. La correspondance qui à $\varphi \in \mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ associe sa restriction à $G^*$ induit un morphisme $\chi : \mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \to S_3$. Tout morphisme $\varphi \in \mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ étant déterminé par sa restriction à $G^*$, ce morphisme $\chi$ est injectif. De plus, tout automorphisme linéaire (pour la structure de $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$) est un automorphisme de groupes. Il y a 6 tels automorphismes (autant qu'il y a de bases). L'image de $\chi$ contient donc au moins 6 éléments. Comme c'est un sous-groupe de $S_3$, c'est $S_3$ lui-même et $\chi$ est un isomorphisme.

***Correction 6*** Le sous-groupe $H$ est à la fois la classe à gauche et la classe à droite modulo $H$ de l'élément neutre. Si $[G : H] = 2$, son complémentaire $H^c$ dans $G$ est donc l'autre classe, à droite et à gauche. Classes à droite et classes à gauche coincident donc, soit $gH = Hg$ et donc $gHg^{-1} = Hgg^{-1} = H$ pour tout $g \in G$.

***Correction 7*** D'après l'hypothèse, pour tout $x \in G$, il existe $z \in G$ tel que $xH \cdot x^{-1}H = zH$. On en déduit $xHx^{-1} \subset zH$. Cela entraine que $1 \in zH$ et donc que $z \in H$. D'où finalement $xHx^{-1} \subset H$.

***Correction 8*** Etant donnés $y, z \in H$, on a $y \simeq 1$ et $z \simeq 1$. La compatibilité de la loi donne d'une part $yz \simeq 1$, soit $yz \in H$, et d'autre part $yy^{-1} \simeq y^{-1}$ soit $y^{-1} \in H$. Cela montre que $H$ est un sous-groupe de $G$. Pour tout $x \in G$, on a aussi $xyx^{-1} \simeq x1x^{-1} = 1$ et donc $xyx^{-1} \in H$. Le sous-groupe $H$ est donc distingué.
De plus, pour $x, x' \in G$, si $x \simeq x'$, alors par compatibilité de la loi, on a $x'x^{-1} \simeq xx^{-1} = 1$, c'est-à-dire $x'x^{-1} \in H$. Réciproquement, si $x'x^{-1} \in H$, alors $x'x^{-1} \simeq 1$, et donc, par compatibilité de la loi, $x \simeq x'$.

***Correction 9*** Pour tout $g \in G$, la conjugaison $c_g : G \to G$ par $g$ induit un automorphisme de $H$ si $H$ est distingué dans $G$. Si de plus $K$ est caractéristique dans $H$, alors $K$ est stable par $c_g$. D'où $K$ est alors distingué dans $G$.

Le sous-ensemble $V_4$ du groupe symétrique $S_4$ consistant en l'identité et les trois produits de transpositions disjointes : $(1\,2)(3\,4)$, $(1\,3)(2\,4)$ et $(1\,4)(2\,3)$ est un sous-groupe (vérification immédiate) qui est distingué : cela résulte de la formule $g(i\,j)(k\,l)g^{-1} = (g(i)\,g(j))(g(k)\,g(l))$ pour $i, j, k, l \in \{1, 2, 3, 4\}$ distincts. Le sous-groupe $K$ (d'ordre 2) engendré par $(1\,2)(3\,4)$ est distingué dans $V_4$ (car $V_4$ est abélien). Mais $K$ n'est pas distingué dans $S_4$ (comme le montre encore la formule précédente).

***Correction 12*** Le groupe $\mu_{mn}$ a un élément d'ordre $mn$. En revanche tout élément $x \in \mu_m \times \mu_n$ vérifie $x^\mu = 1$ avec $\mu = \text{ppcm}(m, n)$ et est donc d'ordre un diviseur de $\mu$, lequel est $< mn$ si $m$ et $n$ ne sont pas premiers entre eux. Les groupes $\mu_{mn}$ et $\mu_m \times \mu_n$ ne peuvent donc pas être isomorphes.

***Correction 16*** Considérons la surjection canonique $s : G \to G/H$. D'après l'exercice 14, $|s(K)|$ divise $\text{pgcd}(|K|, |G/H|)$ qui est égal à $\text{pgcd}(|H|, |G/H|)$ (puisque $|H| = |K|$) et vaut donc 1. Conclusion : $s(K) = \{1\}$, c'est-à-dire $K \subset H$. D'où $K = H$ puisqu'ils ont même ordre.

***Correction 17*** On a $f(n) = f(1)^n$ pour tout entier $n > 0$. Mais on a aussi $f(1/n)^n = f(1)$ pour tout $n > 0$. Cela n'est pas possible car un nombre rationnel positif $\neq 0, 1$ ne peut être une puissance $n$-ième dans $\mathbb{Q}$ pour tout $n > 0$. (Pour ce dernier point, noter par exemple qu'être une puissance $n$-ième dans $\mathbb{Q}$ entraîne que tous les exposants de la décomposition en facteurs premiers sont des multiples de $n$). Les deux groupes $(\mathbb{Q}, +)$ et $(\mathbb{Q}_+^\times, \times)$ ne sont donc pas isomorphes.

***Correction 20*** On a $n = |G/H|$. Pour toute classe $aH \in G/H$, on a donc $(aH)^n = H$ c'est-à-dire, $a^n H = H$ ou encore $a^n \in H$. Cela devient faux si $H$ n'est pas distingué dans $G$. Par exemple le sous-groupe $H$ de $S_3$ engendré par la transposition $(1\,2)$ est d'indice 3 dans $S_3$ et, pour $a = (2\,3)$, on a $a^3 = a \notin H$.

***Correction 21*** Soit $H'$ un sous-groupe de $G$ d'ordre $n$ et d'indice $m$. Pour tout $h \in H'$, on a $h^n = 1$ et $h^m \in H$ (cf exercice ?). Puisque $n$ et $m$ sont premiers en eux, on peut trouver $u, v \in \mathbb{Z}$ tels que $um + vn = 1$. On obtient alors $h = (h^m)^u (h^n)^v \in H$. D'où $H' \subset H$ et donc $H = H'$ puisque $|H| = |H'|$.

***Correction 23*** (a) La correspondance $x \to e^{2i\pi x}$ induit un morphisme $\mathbb{R} \to T$, surjectif et de noyau $\mathbb{Z}$. D'où $\mathbb{R}/\mathbb{Z} \simeq T$. La correspondance $z \to z/|z|$ induit l'isomorphisme $\mathbb{C}^\times/\mathbb{R}_+^\times \simeq T$. Similairement $z \to z^2/|z|^2$ fournit l'isomorphisme $\mathbb{C}^\times/\mathbb{R}^\times \simeq T$. Les isomorphismes $T/\mu_n \simeq T$ et $\mathbb{C}^\times/\mu_n \simeq \mathbb{C}^\times$ s'obtiennent à partir de la correspondance $z \to z^n$.

(b) La correspondance $x \to e^{2i\pi x}$ induit un morphisme $\mathbb{Q} \to \mu_\infty$, surjectif et de noyau $\mathbb{Z}$. D'où $\mathbb{Q}/\mathbb{Z} \simeq \mu_\infty$. Si $G$ est un sous-groupe fini de $\mu_\infty$, alors il existe $m \in \mathbb{N}$ tel que $G \subset \mu_m$. Les sous-groupes du groupe cyclique $\mu_m$ sont les $\mu_n$ où $n|m$.

(c) Soit $G$ un sous-groupe de $\mathbb{Q}$ de type fini, c'est-à-dire engendré par un nombre fini de rationnels $p_1/q_1, \ldots, p_r/q_r$. On a alors $q_1 \cdots q_r G \subset \mathbb{Z}$. Soit $q$ le plus petit entier $> 0$ tel que $qG \subset \mathbb{Z}$. Le sous-groupe $qG$ est de la forme $a\mathbb{Z}$ avec $a \in \mathbb{N}$ premier avec $q$ (car l'existence d'un facteur commun contredirait la minimalité de $q$). On obtient $G = (a/q)\mathbb{Z}$. Si de plus $\mathbb{Z} \subset G$ alors $1 \in G$ et s'écrit donc $1 = ka/q$ avec $k \in \mathbb{Z}$, ce qui donne $ka = q$. Comme $\text{pgcd}(a, q) = 1$, on a nécessairement $a = 1$ et donc $G = (1/q)\mathbb{Z}$.

Soit $s : \mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$ la surjection canonique. Si $\overline{G}$ est un sous-groupe de type fini de $\mathbb{Q}/\mathbb{Z}$, alors $G = s^{-1}(\overline{G})$ est un sous-groupe de $\mathbb{Q}$, contenant $\mathbb{Z}$ et de type fini (si $p_1/q_1, \ldots, p_r/q_r$ sont des antécédents par $s$ de générateurs de $\overline{G}$, alors $1, p_1/q_1, \ldots, p_r/q_r$ engendrent $G$). D'après ce qui précède, on a $G = \frac{1}{q}\mathbb{Z}$ et donc $\overline{G} = \frac{1}{q}\mathbb{Z}/\mathbb{Z}$, qui est isomorphe à $\mathbb{Z}/q\mathbb{Z}$.

Via l'isomorphisme de la question (b), on déduit les sous-groupes de $\mathbb{Q}/\mathbb{Z}$ de type fini : ce sont les sous-groupes $\{e^{2ik\pi/q} \mid k \in \mathbb{Z}\} = \mu_q$ avec $q$ décrivant $\mathbb{N}^\times$.

(d) On vérifie sans difficulté que pour tout nombre premier $p$, $\mu_{p^\infty}$ est un sous-groupe de $\mu_\infty$. Il n'est pas de type fini : en effet le sous-groupe de $\mathbb{Q}/\mathbb{Z}$ qui lui correspond par l'isomorphisme de la question (b) est engendré par les classes de rationnels $1/p^n$ modulo $\mathbb{Z}$, $n$ décrivant $\mathbb{N}$. Un tel sous-groupe $G$ n'a pas de dénominateur commun, c'est-à-dire, il n'existe pas d'entier $q \in \mathbb{Z}$ tel que $qG \subset G$. En conséquence il ne peut pas être de type fini.

***Correction 24*** Soit $z \in \mathbb{C}$ quelconque et $\zeta \in \mathbb{C}$ une racine $n$-ième de $z$. Le sous-groupe $G$ est distingué dans $\mathbb{C}$ (puisque $\mathbb{C}$ est commutatif). Si $n$ est l'indice de $G$ dans $\mathbb{C}$, on a donc $\zeta^n = z \in G$ (cf. exercice 18). D'où $\mathbb{C} \subset G$. L'inclusion inverse est triviale.

***Correction 32*** (a) Soit $\varphi : \mathbb{F}_p^n \to \mathbb{F}_p^m$ un morphisme de groupes. Pour tout $a \in \mathbb{Z}$, on note $\overline{a} \in \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ sa classe modulo $p$. Tout élément $\overline{x} \in \mathbb{F}_p^n$ peut s'écrire $\overline{x} = (\overline{x_1}, \ldots, \overline{x_n})$ avec $x = (x_1, \ldots, x_n) \in \mathbb{Z}^n$. On a alors $\varphi(\overline{a} \cdot \overline{x}) = \varphi(\overline{ax}) = \varphi(a\overline{x}) = a\varphi(\overline{x}) = \overline{a} \cdot \varphi(\overline{x})$. Le morphisme $\varphi$ est donc compatible avec les lois externes de $\mathbb{F}_p^n$ et $\mathbb{F}_p^m$. Comme il est aussi additif, c'est une application $\mathbb{F}_p$-linéaire.

(b) Considérons l'application $V : \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) \to \mathbb{Z}/p\mathbb{Z}$ qui à tout automorphisme $\chi$ associe $\chi(1)$. Cette application est à valeurs dans $\mathbb{Z}/p\mathbb{Z}\backslash\{0\}$ (si $\chi \in \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$, alors $\ker(\chi) = \{0\}$). C'est un morphisme de $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ muni de la composition vers le groupe multiplicatif $\mathbb{Z}/p\mathbb{Z}\backslash\{0\} = \mathbb{F}_p^\times$ : en effet si $\chi, \chi' \in \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ et si on pose $\chi'(1) = \overline{c}$ (classe de $c \in \mathbb{Z}$ modulo $p$), alors $(\chi \circ \chi')(1) = \chi(\overline{c}) = c\chi(1) = \overline{c} \cdot \chi(1) = \chi'(1) \cdot \chi(1) = \chi(1) \cdot \chi'(1)$. Ce morphisme $V$ est de plus injectif puisque tout automorphisme $\chi$ de $\mathbb{Z}/p\mathbb{Z}$ est déterminé par $\chi(1)$. Enfin, pour tout $\overline{a} \in \mathbb{Z}/p\mathbb{Z}$ non nul, la correspondance $\overline{n} \to \overline{a} \cdot \overline{n}$ induit un automorphisme $\chi$ de $\mathbb{Z}/p\mathbb{Z}$ tel que $\chi(1) = \overline{a}$. L'image du morphisme $V$ est donc tout $\mathbb{F}_p^\times$. Ce qui établit l'isomorphisme demandé.

(c) D'après la question (a), il s'agit de compter le nombre d'automorphismes linéaires du $\mathbb{F}_p$-espace vectoriel $\mathbb{F}_p^n$, qui est égal au nombre de bases de $\mathbb{F}_p^n$, c'est-à-dire $(p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$.

***Correction 34*** Soit $G$ un groupe abélien fini tel que $pG = \{0\}$. Pour tout entier $n \in \mathbb{Z}$ et pour tout $g \in G$, l'élément $ng$ ne dépend que de la classe de $n$ modulo $p$ ; on peut le noter $\overline{n} \cdot g$. La correspondance $(\overline{n}, g) \to \overline{n} \cdot g$ définit une loi externe sur le groupe additif $G$ et lui confère ainsi une structure de $\mathbb{F}_p$-espace vectoriel. Cet espace vectoriel, étant fini, est de dimension finie. Il est donc isomorphe comme espace vectoriel, et en particulier comme groupe à $(\mathbb{Z}/p\mathbb{Z})^n$ pour un certain entier $n \geqslant 0$.

***Correction 37*** Le centre $Z(G)$ est ni trivial (car $G$ est un $p$-groupe) ni égal à $G$ (car $G$ non abélien). En utilisant l'exercice 25, on voit qu'il n'est pas non plus d'ordre $p^2$. Il est donc d'ordre $p$. Mais alors $G/Z(G)$ est d'ordre $p^2$ et est donc abélien (exercice 26). D'après l'exercice 36, on a alors $D(G) \subset Z(G)$. Comme $D(G) \neq \{1\}$ (sinon $G$ serait abélien), on a $D(G) = Z(G)$.