UNIVERSITÉ DE LORRAINE

L3 Mathématiques – Site Nancy, S5 – 2021/22

Algèbre 2 – Feuille 3

Groupes finis, groupes cycliques

Exercice 1. *Déterminer les générateurs du groupe additif $\mathbb{Z}/12\mathbb{Z}$ et ceux du groupe multiplicatif $\mathbb{U}_{18}$.*

Solution de l'exercice 1. Les deux groupes sont cycliques engendrés respectivement par $\overline{1}$ et $\zeta = e^{i\frac{2\pi}{18}} = e^{i\frac{\pi}{9}}$. Les générateurs de $\mathbb{Z}_{12}$ sont donc les $\overline{k}$ avec $\text{pgcd}(k, 12) = 1$, soit : $\overline{1}, \overline{5}, \overline{7}, \overline{11}$ et ceux de $\mathbb{U}_{18}$ sont $\zeta, \zeta^5, \zeta^7, \zeta^{11}, \zeta^{13}$ et ζ^{17}.

Exercice 2. *Déterminer les éléments d'ordre 6 et ceux d'ordre 5 dans le groupe $\mathbb{U}_{30}$.*

Solution de l'exercice 2. Le groupe $G = \mathbb{U}_{30}$ est cyclique engendré par $\zeta = e^{i\frac{\pi}{15}}$, il existe donc un unique sous groupe $H = \langle \zeta^{\frac{30}{6}} \rangle = \langle \zeta^5 \rangle$ d'ordre 6 de G. Tous les éléments d'ordre 6 se trouvent dans H qui admet $\varphi(6) = 2$ générateurs. Il n'y a donc que deux éléments d'ordre 6 qui sont ζ^5 et ζ^{25}.

Pour déterminer les éléments d'ordre 5, on adopte une autre méthode : $G = \mathbb{U}_{30}$ est cyclique engendré par $\zeta = e^{i\frac{\pi}{15}}$. Soit $\zeta^k \in G$, avec $k \leq 0 \leq 29$. On a

$$\begin{aligned} o(\zeta^k) = 5 &\iff \frac{o(\zeta)}{\text{pgcd}(o(\zeta), k)} = 5 \\ &\iff \frac{30}{\text{pgcd}(30, k)} = 5 \\ &\iff \text{pgcd}(30, k) = 6 \\ &\iff k \in \{6, 12, 18, 24\} \end{aligned}$$

Ainsi les éléments d"ordre 5 de $\mathbb{U}_{30}$ sont $\zeta^6, \zeta^{12}, \zeta^{18}$ et ξ^{24}, où $\zeta = e^{i\frac{\pi}{15}}$.

Exercice 3. *Déterminer les sous-groupes de $\mathbb{Z}/20\mathbb{Z}$ et les sous-groupes de $\mathbb{U}_{12}$.*

Solution de l'exercice 3. $\mathbb{Z}_{20}$ est cyclique d'ordre 20 engendré par $\overline{1}$, tous ses sous groupes sont donc les $H_d = \langle \overline{(\frac{20}{d})} \rangle$ lorsque d décrit l'ensemble des diviseurs de 20.

$\mathbb{U}_{12}$ est cyclique d'ordre 12 engendré par $\zeta = e^{2i\pi/12} = e^{i\pi/6}$, tous ses sous groupes sont donc les $H_d = \langle \zeta^{\frac{12}{d}} \rangle$ lorsque d décrit l'ensemble des diviseurs de 12.

Exercice 4. *Montrer qu'un groupe G est d'ordre premier si, et seulement si, il est cyclique et simple (c-à-d que $\{e\}$ et G sont les seuls sous-groupes distingués de G).*

Solution de l'exercice 4. Si G est d'ordre premier p alors tout élément x de $G \setminus \{e\}$ vérifie : $o(x) \neq 1$ et $o(x)$ divise p (Théorème de Lagrange), donc $o(x) = p$ et comme on a déjà $< x > \subseteq G$, l'égalité des cardinaux conclut : $G = \langle x \rangle$ est cyclique. Enfin tout sous groupe H de G, qu'il soit distingué ou non, a pour cardinal 1 ou p (toujours avec le théorème de Lagrange) donc $H = \{e\}$ ou G.

Réciproquement si $G = \langle x \rangle$ est cyclique, notons $p = o(x)$. Soit d un diviseur de p. Il existe alors un unique sous groupe H d'ordre d. Comme G est abélien, H est distingué dans G donc $H = \{e\}$ ou G et par suite $d = 1$ ou p. Les seuls diviseurs de p sont 1 et lui même donc p est premier.

Exercice 5. *Soient G un groupe fini, K et M deux sous-groupes de G d'ordres k et m. Montrer que si, k et m sont premiers entre eux, alors $K \cap M = \{e\}$.*

Solution de l'exercice 5. $K \cap M$ est à la fois un sous-groupe de K et à la fois un sous-groupe de M. Son ordre divise donc à la fois k et m respectivement, et donc leur pgcd : 1. C'est un groupe de cardinal 1, il est réduit au neutre.

Exercice 6. *Soit G un groupe fini d'ordre $2n$, d'élément neutre e. On suppose qu'il existe deux sous-groupes distincts H, H' de G d'ordre n, tels que $H \cap H' = \{e\}$. Montrer que $n = 2$ et dresser la table de G.*

Solution de l'exercice 6. Comme $H \neq H'$ sont deux groupes de cardinal n on a $n \geq 2$. Ensuite $\text{card}(H \cup H') = 2n - 1$, il existe donc un unique $a \in G \setminus (H \cup H')$. On note $H_1 = H \setminus \{e\}$ et $H'_1 = H' \setminus \{e\}$ de sorte que $G = H_1 \cup H'_1 \cup \{e, a\}$ soit une réunion disjointe. Pour $x \in H_1$ et $y \in H'_1$, le produit xy ne saurait être dans H_1, sinon $y \in H \setminus \{e\} = H_1$ ce qui est impossible. Donc xy n'est pas non plus dans H'_1 pour le même raisonnement. Enfin l'inverse de x est dans H_1 (car H est un groupe) donc $xy \neq e$. Il ne reste que $xy = a$ ce qui prouve que :

$$H_1 H'_1 \subseteq \{a\}$$

On conclut en remarquant que l'application $H_1 \times H_1' \to H_1H_1'$, $(x,y) \mapsto xy$ est bijective. Donc :

$$(n-1)^2 = |H_1||H_1'| = |H1H_1'| \leq 1$$

donc $n = 1$ ou 2 et $n \geq 2$: $n = 2$.

	e	x	y	a
e	e	x	y	a
x	x	e	a	y
y	y	a	e	x
a	a	y	x	e

Exercice 7. *Soit G un goupe d'ordre $2p$, avec $p > 2$ premier. Montrer qu'il existe dans G des sous-groupes H et K d'ordres p et 2 et que l'on a $G = HK$, H distingué dans G et $H \cap K = \{e\}$.*

Solution de l'exercice 7. D'après le théorème de Cauchy, il existe $a, b \in G$ tels que $o(x) = p$ et $o(b) = 2$. Les sous-groupes $H = \langle a \rangle$ et $H = \langle b \rangle$ sont donc respectivement d'ordre p et 2.

On a $H \cap K$ est un sous-groupe de H et K, donc son ordre $|H \cap K|$ divise p et 2. Il est donc égal à 1 et $H \cap K = \{e\}$.

Comme $[G : H] = \frac{|G|}{|H|} = 2$, H est distingué dans G.

On en déduit que HK est un sous-groupe de G. Mais H et K sont des sous-groupes de HK, donc p et 2 divisent $|HK|$ et par suite $2p$ divise $|HK|$. Cela montre que $G = HK$.

Exercice 8. *Soit $f : G \to G'$ un morphisme de groupes. Montrer que si $x \in G$ est d'ordre fini n, alors $f(x)$ est d'ordre fini et son ordre divise n.*
Application : trouver tous les morphismes de $\mathbb{Z}/3\mathbb{Z}$ dans $\mathbb{Z}/7\mathbb{Z}$

Solution de l'exercice 8. Puisque f est un morphisme, $f(x)^n = f(x^n) = f(e) = e'$ où e est le neutre de G et e' est le neutre de G'. On déduit de cette formule que $f(x)$ est d'ordre fini et que son ordre divise n.

Application : si f est un tel morphisme, f est complètement déterminé par la donnée de $f(\overline{1})$. $o(\overline{1}) = 3$ et $f(\overline{1}) \in \mathbb{Z}_7$ donc $o(f(\overline{1}))$ divise 3 d'après le premier point et divise aussi 7, il divise donc leur pgcd qui vaut 1. Ainsi $f(\overline{1})$ est la classe nulle de $\mathbb{Z}_7$ et le seul morphisme de groupe et le morphisme nul.

Exercice 9. *Soient G et G' deux groupes cycliques d'ordres n et m. Combien existe-t-il de morphismes de G dans G' ?*
Donner l'expression de tous les morphismes de $\mathbb{Z}/21\mathbb{Z}$ dans $\mathbb{Z}/6\mathbb{Z}$, de $\mathbb{Z}/18\mathbb{Z}$ dans $\mathbb{Z}/6\mathbb{Z}$.

Solution de l'exercice 9. G est cyclique engendré par un $x \in G$. D'après l'exercice précédent, la donnée de $f(x)$ suffit à déterminer entièrement f et on sait aussi que son ordre divise $\text{pgcd}(n,m)$. Il s'agit donc, pour chaque diviseur d de $\text{pgcd}(n,m)$, de déterminer le nombre d'éléments de G' d'ordre d. Mais G' est cyclique, on sait qu'il existe un unique sous groupe d'ordre d pour d divisant $\text{pgcd}(n,m)$ et donc m. Chacun de ces sous groupes admet $\varphi(d)$ générateurs : c'est le nombre d'éléments d'ordre d dans G'. En conclusion : Il y a $\sum_{d|\text{pgcd}(n,m)} \varphi(d)$ choix possibles pour $f(x)$, c'est le nombre de morphismes de G dans G'. Nous verrons dans l'exercice 15 que ce nombre vaut
mathrmpgcd(n,m).

- *$21 \wedge 6 = 3$, il y a 3 choix pour $f(\overline{1})$: les classes de 0, de 2 et de 4.*
- *$18 \wedge 6 = 6$: on choisit ce qu'on veut pour la valeur de $f(\overline{1})$.*

Exercice 10. *Montrer que le groupe $\text{Aut}(\mathbb{Z}/5\mathbb{Z})$ est cyclique. Expliciter ses éléments et donner ses générateurs.*

Solution de l'exercice 10. On note $f_k : \overline{x} \to \overline{kx}$. D'après l'exercice précédent il y a 5 morphismes au total, si on se restreint aux morphismes bijectifs il n'y en a plus que 4, il sont en bijection avec les générateurs du groupe cyclique $\mathbb{Z}/5\mathbb{Z}$. On note que $f_2^2 = f_4$, $f_2^3 = f_3$, $f_2^4 = Id$. Donc G est cyclique engendré par f_2 et $f_2^3 = f_3$ car $\text{pgcd}(3,4) = 1$. Ses éléments sont f_1, f_2, f_3 et f_4.

Exercice 11. *Soient G un groupe fini et H un sous-groupe distingué de G.*

(a) Soit K un sous-groupe de G tel que $[G : H]$ et $|K|$ soient premiers entre eux. Montrer que $K \subset H$.

(b) Si $[G : H]$ et $|H|$ sont premiers entre eux, montrer que le seul sous-groupe de G d'ordre m est H.

Solution de l'exercice 11. (a) Soit $x \in K$. Notons $k = |K|$. On a alors $n = o(x)$ qui divise k. De plus G/H est un groupe car H est distingué dans G, on a alors $o(\overline{x})$ divise $[G : H]$, où $\overline{x}$ désigne la classe modulo H de x. Or on remarque que $\overline{x}^n = \overline{x^n} = \overline{e}$ donc $o(\overline{x})$ divise $n = o(x)$ qui divise k. Ainsi $o(\overline{x})$ divise le pgcd de k et $[G : H]$, c'est-à-dire 1. Cela signifie que $\overline{x} = \overline{e} = H$ donc que $x \in H$. Ainsi, $K \subseteq H$.

(b) Si K est un autre sous groupe d'ordre $m = |H|$ premier avec $[G : H]$, la question précédente prouve que $K \subseteq H$ et l'égalité des cardinaux conclut quant à l'égalité des ensembles.

Exercice 12. *(a) Montrer que tout grope d'ordre p^n où p est un nombre premier et $n \in \mathbb{N}^*$, a un centre non réduit à $\{e\}$.*

(b) Soit G un groupe ; montrer que si $G/Z(G)$ est cyclique, alors G est abélien.

(c) Soit p un nombre premier et soit G un groupe d'ordre p^2. Montrer que G est abélien.

Solution de l'exercice 12. (a) On fait agir G sur lui-même par conjugaison. L'équation des classes s'écrit :

$$|G| = \sum_{i=1}^{r} |G \cdot x_i| = |Fix(G)| + \sum_{\substack{i=1 \\ |G\cdot x_i|\geq 2}}^{r} \frac{|G|}{|G_{x_i}|} = |Z(G)| + \sum_{\substack{i=1 \\ |G\cdot x_i|\geq 2}}^{r} \frac{|G|}{|G_{x_i}|}$$

où r est le nombre d'orbites. Pour tout $i \in \{1, \cdots, r\}$, G_{x_i} est un sous groupe de G, son cardinal est donc une puissance de p. Lorsque $\frac{|G|}{|G_{x_i}|} |G \cdot x_i| \geq 2$, on en déduit que $\frac{|G|}{|G_{x_i}|}$ est un multiple de p pour chaque $i \in \{1, \cdots, r\}$. Ainsi

$$|Z(G)| \equiv |G| \mod p \equiv 0 \mod p$$

$e \in Z(G)$ donc $|Z(G)| \geq 1$ et $|Z(G)|$ est un multiple de p impliquent donc que $|Z(G)| \geq p \geq 2$. Le centre de G n'est pas réduit à $\{e\}$.

(b) Supposons que $G/Z(G)$ est cyclique engendré par $\overline{z}$. Soient $x, y \in G \times G$. Il existe donc k et l deux entiers tels que $\overline{x} = \overline{z}^k$ et $\overline{y} = \overline{z}^l$. Cela signifie qu'il existe s et t dans $Z(G)$ tels que $x = z^k s$ et $y = z^l t$.

Comme s commute avec tout les éléments de G : $xy = z^{k+l} st$.

Il en va de même pour t : $yx = z^{l+k} ts = z^{k+l} st = xy$.

Ce qui prouve que G est abélien.

(c) Par le théorème de Lagrange $|Z(G)|$ divise p^2 et par la question (a), $|Z(G)| \geq p$. Les seules valeurs possibles pour $|Z(G)|$ sont alors p et p^2. Supposons par l'absurde que le centre de G a pour cardinal p. Le groupe $G/Z(G)$ a donc pour cardinal $[G : Z(G)] = p$ premier. Un groupe de cardinal premier est cyclique donc d'après la question (b) G est abélien et par suite $G = Z(G)$. Ceci contredit le fait que G a pour cardinal p^2 et son centre a pour cardinal p. Ainsi on a $|Z(G)| = p^2 = |G|$. Ce qui prouve que G est abélien.

Exercice 13. *Soit p un nombre premier et soit G un groupe d'ordre p^2.*

(a) Quels sont les ordres possibles des éléments de G ? Montrer que si G possède un élément d'ordre p^2, alors $G \simeq \mathbb{Z}/p^2\mathbb{Z}$.

(b) On suppose que G ne possède pas d'élément d'ordre p^2.

(i) Montrer que, pour tout $x \in G \setminus \{e\}$, $\langle x \rangle \simeq \mathbb{Z}/p\mathbb{Z}$.

(ii) Montrer que si H et K sont deux sous-groupes de G distincts d'ordre p, alors $H \cap K = \{e\}$ et $HK = G$. En déduire que $G \simeq (\mathbb{Z}/p\mathbb{Z})^2$.

Solution de l'exercice 13. Tout d'abord, d'après le théorème 3.7 du chapitre 2, G est abélien.

(a) Si $x \in G$ alors d'après le théorème de Lagrange $o(x)$ divise p^2. On a donc $o(x) \in \{1, p, p^2\}$. Si G admet un élément d'ordre $p^2 = |G|$, cet élément est générateur de G donc G est cyclique. Un groupe cyclique d'ordre p^2 est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$, ce qui conclut.

(b)(i) Soit $x \in G \setminus \{e\}$. D'après la question (a) et l'hypothèse faite on a $o(x) = p$. Ainsi $\langle x \rangle$ est un groupe cyclique d'ordre p donc isomorphe à $\mathbb{Z}_p$.

(b)(ii)

- *$H \cap K$ est un sous-groupe de H de cardinal p, donc d'après Lagrange $|H \cap K|$ vaut 1 ou p. Mais si $|H \cap K| = p = |H| = |K|$ on aura alors $H = H \cap K = K$ ce qui est faux. Donc $|H \cap K| = 1$ et $H \cap K = \{e\}$.*
- *$HK \subseteq G$ est clair. Il est aussi claire que HK est un sous-groupe de G, puisque G est abélien. Considérons l'application $f : H \times K \to HK$, $(h, k) \mapsto hk$. Comme G est abélien f est un morphisme de groupes, surjectif par construction. De plus $(h, k) \in \ker f$ si, et seulement si, $hk = e$ ou encore $h = k^{-1} \in H \cap K = \{e\}$. Donc $(h, k) = (e, e)$ et f est injectif. Il s'ensuit que les deux groupes HK et $H \times K$ sont isomorphe, d'où $|HK| = |H \times K| = |H| \times |K| = p^2$. Le sous-groupe HK a donc le même ordre que G et par conséquent $HK = G$.*
- *D'après la question précédente, $G = KH$ et KH est isomorphe à $H \times K$. Donc $G \simeq H \times K$. Mais comme H et K sont d'ordre p, il sont isomorphe chacun à $\mathbb{Z}_p$. Ainsi $G \simeq \mathbb{Z}_p \times \mathbb{Z}_p$.*

Exercice 14. *Soi G un groupe d'ordre pq où p et q ont deux nombres premiers distincts. On veut montrer que G possède au moins un élément d'ordre p et au moins un élément d'ordre q sans utiliser le théorème de Cauchy. Pour cela on suppose que G ne possède aucun éléments d'ordre q.*

(a) Montrer que tout élément de $G \setminus \{e\}$ est d'ordre p.

(b) Soit $x \in G \setminus \{e\}$ et soit $H = \langle x \rangle$.

(1) Montrer que si H est distingué dans G, alors le quotient G/H est cyclique d'ordre q ; soit alors $y \in G$ tel que $G/H = \langle \bar{y} \rangle$. En raisonnant sur $o(y)$ et $o(\bar{y})$ trouver une contradictions et en déduire que H n'est pas distingué dans G.

(2) Montrer que $N_G(H) = H$.

(3) Montrer que H possède exactement q conjugués aHa^{-1} quand a décrit G ; en déduire que la réunion R des conjugués de H a $1 + q(p-1)$ éléments.

(4) Montrer que $R \neq G$. On peut donc choisir $y \in G \setminus R$.

(5) Soit $K = \langle y \rangle$ et soit S la réunion des conjugués de K. Montrer que S a $1 + q(p-1)$ éléments.

(6) Montrer que $S \cap R = \{e\}$. En déduire que $\text{card}(S \cup R) = 1 + 2q(p-1)$.

(7) Conclure.

Solution de l'exercice 14. On suppose que G ne possède pas d'éléments d'ordre q. (a) Soit $x \in G$ tel que $o(x) \neq 1$. D'après le théorème de Lagrange, $o(x))$ divise $|G| = pq$. Donc $o(x) = q$ puis que x ne peut pas être d'odre q par hypothèse.

(b) Soit $x \in G \setminus \{e\}$ et posons $H = \langle x \rangle$. D'après la question précédente $o(x) = p$ et $|H| = p$.

(1) Si H est distingué, alors G/H est un groupe et son ordre est $\frac{|G|}{|H|} = \frac{pq}{p} = q$ est premier, donc cyclique. Soit $\bar{y}$ un de ses générateurs, $G/H = \langle \bar{y} \rangle$, avec $o(\bar{y}) = q$. On $\overline{y^q} = \bar{y}^q = \bar{e} = H$, donc $y^p \in H$ et d'après le théorème de Lagrange, $(y^q)^p = e$ ou encore $(y^p)^q = e$, ce qui entraîne que $o(y^p)$ divise q. Mais comme q est premier, on a $y^p = e$ ou $o(y^p) = q$. Comme G n'a pas d'éléments d'ordre q, on déduit que $y^p = e$, ce qui entraîne que $o(y)$ divise p et et par suite $y = e$ ou $o(y) = p$. D'où une contradiction avec $o(\bar{y}) = q$. En conclusion H n'est pas distingué dans G.

(2) Il est claire que $H \lhd N_G(H) \leq G$. On a $[G : H] = q$. Or $[G : H] = [G : N_G(H)] \times [N_G(H) : H]$, donc $[G : N_G(H)] = 1$ ou $[G : N_G(H)] = q$. Mais si $[G : N_G(H)] = 1$, alors $G = N_G(H)$ et cela veut dire que H est distingué dans G ce qui n'est pas. Par conséquent $[G : N_G(H)] = q$ et par suite $[N_G(H) : H] = 1$, d'où $N_G(H) = H$.

(3) On considère l'action de G sur l'ensemble des sous-groupes de G par

$$(g, K) \mapsto g \cdot K = gKg^{-1}$$

Le stabilisateur de H pour cette action est

$$\begin{aligned} G_H &:= \{g \in G \mid g \cdot H = H\} \\ &= \{g \in G \mid gHg^{-1} = H\} \\ &= N_G(H) \end{aligned}$$

L'orbite de H pour la même action

$$\begin{aligned} G \cdot H = \mathrm{Orb}(H) &= \{g \cdot H \mid g \in G\} \\ &= \{gHg^{-1} \mid g \in G\} \quad \text{classes de conjugaison de } H \\ &= \text{ensemble des conjugués de } H \end{aligned}$$

Mais G/G_H est en bijection avec $Orb(H)$, donc

$$\mathrm{card}\,(Orb(H)) = \frac{|G|}{|N_G(H)|} = [G : N_G(H)] = q$$

En conclusion H admet exactement q conjugués.

Posons

$$R = \bigcup_{g \in G} gHg^{-1}$$

la réunion de tous les conjugués de H. Il y en a exactement q. Les conjugués gHg^{-1} sont tous des sous-groupes d'ordre p (comme H). Donc conjugués $g_1Hg_1^{-1}$ et $g_2Hg_2^{-1}$ sont ou bien d'intersection réduite à $\{e\}$ ou bien sont égaux (Théorème de Lagrange). On en déduit que

$$\mathrm{card}(R) = 1 + q(p-1)$$

(4) Si $R = G$, alors $\mathrm{card}(R) = \mathrm{card}(G) = |G|$, d'où $pq = 1 + q(p-1)$ ce qui est absurde. Ainsi $R \neq G$.

(5) Soit alors $y \in G \setminus R$ et posons $K = \langle .y \rangle$. Soit S la réunion de conjugués de K. On montre de même que S admet $1 + q(p-1)$ éléments.

(6) Sit $z \in R \cap S$, alors il existe $n, m \in \mathbb{N}$, $a, b \in G$ tels que $z = ax^na^{-1} = by^mb^{-1}$, d'pù $y^m = (b^{-1}a)x^n(b^{-1}a)^{-1} \in R$. On en déduit que p divise m et que $z = e$ et que $R \cap S = \{e\}$. Par conséquent

$$card(S \cup R) = (1 + q(p-1) + (1 + q(p-1)) - 1 = 1 + 2q(p-1) > pq$$

D'où une contradiction.

(7) En conclusion, nous avons montré par l'absurde que G admet au moins un élément d'ordre p.

Comme p et q jouent le même rôle, G admet au moins un élément d'ordre q.

est

Exercice 15. *Pour tout entier $n \geq 2$, on note $\varphi(n)$ le cardinal de l'ensemble des entiers tels que $0 \leq k \leq n-1$ et $k \wedge n = 1$. On convient que $\varphi(1) = 1$. La fonction φ de $\mathbb{N}^*$ dans $\mathbb{N}^*$ ainsi définie est appelée la fonction d'Euler. L'entier $\varphi(n)$ est aussi le nombre de générateurs de tout groupe cyclique d'ordre n.*

(a) Déterminer $\varphi(2), \varphi(3), \varphi(4)$ et $\varphi(5)$.

(b) Montrer que $\varphi(p) = p - 1$ si et seulement si p est premier.

(c) Soit $n \in \mathbb{N}^*$. Montrer que $n = \sum_{d|n} \varphi(d)$.

(d) Soient $m, n \in \mathbb{N}^*$ tels que $m \wedge n = 1$. Montrer que $\varphi(mn) = \varphi(m)\varphi(n)$.

(e) Montrer que si la décomposition en facteurs premiers de $n \geq 2$ est $n = p_1^{s_1} \cdots p_k^{s_k}$, alors $\varphi(n) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_k})$.

(f) En déduire que pour tout $m, n \in \mathbb{N}^*$, $\varphi(mn) = \varphi(m)\varphi(n)\frac{d}{\varphi(d)}$, où $d = \mathrm{pgcd}(m, n)$.

(g) Soit $n \geq 3$. Montrer que $\varphi(n)$ est pair.

(h) Montrer que $\varphi(2n) = \varphi(n)$ si n est impair et que $\varphi(2n) = 2\varphi(n)$ si n est pair.

Solution de l'exercice 15. *(a) $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$.*

(b) Supposons p premier. Les entiers qui ne sont pas premiers avec p sont les multiples de p. Il existe donc $p-1$ éléments dans $[0, p-1]$ qui sont premiers avec p, qui sont $1, \ldots, p-1$. Réciproquement, si $\varphi(p) = p-1$, comme 0 n'est pas premier avec p, nécessairement les $p-1$ autres éléments $1, \ldots, p-1$ sont premiers avec p. Ils ne divisent donc pas p. Cela signifie que p est premier (principe du crible d'Eratosthène)

(c) D'après le th. de Lagrange, l'ordre de tout élément de $\mathbb{U}_n$ divise n. On a donc une partition $\mathbb{U}_n = \underset{d|n}{U} \Lambda_d$, où pour tout diviseur d de n on pose $\Lambda_d = \{x \in \mathbb{U}_n \mid o(x) = d\}$. Or, si d divise n, il existe dans le groupe cyclique $\mathbb{U}_n$ un unique sous-groupe d'ordre d. C'est $\mathbb{U}_d$ car $\mathbb{U}_d \subset \mathbb{U}_n$. Chacun des $\varphi(d)$ générateurs de $\mathbb{U}_d$ est un élément de Λ_d. Réciproquement, si $x \in \mathbb{U}_n$ est d'ordre d, alors $\langle x \rangle$ est un sous-groupe d'ordre d de $\mathbb{U}_n$. Il est donc égal à $\mathbb{U}_d$ d'après l'unicité du sous-groupe d'ordre d dans $\mathbb{U}_n$. Ainsi, x est un générateur de $\mathbf{U}_d$. Finalement, Λ_d est l'ensemble des générateurs de $\mathbb{U}_d$ et on a card $(\Lambda_d) = \varphi(d)$ d'où la relation.

$$n = \text{card}\,(\mathbb{U}_n) = \sum_{d|n} \text{card}\,(\Lambda_d) = \sum_{d|n} \varphi(d)$$

(d) Pour $m \geq 2$, notons Δ_m l'ensemble des générateurs du groupe $\mathbb{Z}/m\mathbb{Z}$. Supposons $m \wedge n = 1$. D'après la proposition, $\Delta_m \times \Delta_n$ est l'ensemble des générateurs de $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ et ce groupe cyclique est isomorphe à $\mathbb{Z}/mn\mathbb{Z}$ donc

$$\varphi(m)\varphi(n) = \text{card}\,(\Delta_m \times \Delta_n) = \text{card}\,(\Delta_{mn}) = \varphi(mn)$$

(e) Supposons que $k = 1$, soit $n = p^s$, avec p premier. Les éléments de $[0, n-1]$ qui ne sont pas premiers avec n, sont $0, p, 2p, \cdots, \left(p^{s-1} - 1\right) p$. On a donc $\text{card}\,(\Delta_n) = p^s - p^{s-1} = p^s \left(1 - \frac{1}{p}\right)$. Supposons $k \geq 2$, d'où $n = p_1^{s_1} \cdots p_k^{s_k}$. D'après (i) on a :

$$\varphi(n) = \varphi\left(p_1^{s_1}\right) \cdots \varphi\left(p_k^{s_k}\right) = p_1^{s_1} \left(1 - \frac{1}{p_1}\right) \cdots p_k^{s_k} \left(1 - \frac{1}{p_k}\right)$$

(f) Les facteurs premiers de mn sont les facteurs premiers de m seul (qui ne sont pas facteurs de n), les facteurs premiers de n seul et les facteurs premiers communs à m et n qui sont les facteurs premiers du pgcd d. Si on applique (ii) à m et n, on voit que $\varphi(m)\varphi(n)$ contient tous les termes de $\varphi(mn)$ mais que $\prod_{p|d} \left(1 - \frac{1}{p}\right) = \frac{\varphi(d)}{d}$ est compté deux fois. En divisant $\varphi(m)\varphi(n)$ par ce terme, on obtient bien $\varphi(mn)$.

(g) Si $n = 2^k$, avec $k \geq 2$, alors $\varphi(n) = 2^k - 2^{k-1} = 2^{k-1}$ est pair. Si n a un facteur premier impair p, de multiplicité k, on a $n = p^k m$ avec $p^k \wedge m = 1$ Alors $\varphi(n) = \varphi\left(p^k\right)\varphi(m) = (p-1)p^{k-1}\varphi(m)$ est pair car $p-1$ est pair.

(h) Si n est impair, comme $2 \wedge n = 1$ on a $\varphi(2n) = \varphi(2)\varphi(n) = (2-1)\varphi(n) = \varphi(n)$. Si n est pair, il existe m impair et $k \geq 1$ tels que $n = 2^k m$. Comme 2^k et 2^{k+1} sont premiers avec m, on a

$$\varphi(n) = \varphi\left(2^k m\right) = \varphi\left(2^k\right)\varphi(m) = \left(2^k - 2^{k-1}\right)\varphi(m)$$
$$\varphi(2n) = \varphi\left(2^{k+1} m\right) = \varphi\left(2^{k+1}\right)\varphi(m) = \left(2^{k+1} - 2^k\right)\varphi(m) = 2\varphi(n)$$

Généralisation. On montre de même, que pour tout $s \in \mathbb{N}^*$ on a $\varphi\left(2^s n\right) = 2^{s-1}\varphi(n)$ pour n impair et $\varphi\left(2^s n\right) = 2^s \varphi(n)$ pour n pair.

Autre généralisation. Soit p un nombre premier. Si n n'est pas divisible par p, on a $\varphi(pn) = (p-1)\varphi(n)$. Si n est divisible par p, on a $\varphi(pn) = p\varphi(n)$.

Exercice 16. *Soit G un groupe fini d'ordre n. Soit p le plus petit nombre premier qui divise n. On suppose que H est un sous-groupe de G d'indice p. Montrer que H est distingué dans G.*

Solution de l'exercice 16. *On fait agir à gauche H sur G/H, ce dernier étant un ensemble de cardinal p. On obtient un morphisme de H dans $\mathcal{S}_p$. Or, H stabilise la classe de l'élément neutre puisque $H \cdot H = H$. Donc permute les $p-1$ classes restantes. On en déduit un morphisme de H vers le sous-groupe isomorphe à $\mathcal{S}_{p-1}$ qui stabilise la classe du neutre. Mais aucun diviseur de $|H|$ ne divise $|\mathcal{S}_{p-1}| = (p-1)!$. Donc, le morphisme est trivial. On vient de montrer que pour tout g de G, $H \cdot gH = gH$. Cela signifie que $g^{-1}1Hg = H$. Donc,H est distingué.*