10 Counting the elements of a finite group

July 29, 2015

10.5

1. G tel que $o(G) = 8$
2. G n'est pas cyclique

$\diamond$ $a \in G \Rightarrow a^4 = e$

Car soit $a \in G$. Alors $o(a)|o(G)$. Donc $o(a) \in \{1, 2, 4, 8\}$. Or $o(a) \neq 8$, car alors a serait un générateur et donc G serait cyclique.

Donc soit $o(a) = 1$, auquel cas il s'agit de l'identité et donc $a^4 = e^4 = e$, soit $o(a) \in \{2, 4\}$. Or, $a^4 = e$ dans un cas comme dans l'autre.

10.6

1. H, K des sous-groupes de G tel que $|H| = 12$ et $|K| = 5$

$\diamond$ $H \cap K = \{e\}$

Car supposons le contraire. Soit $a \in H \cap K$. Alors $o(a) = o(\langle a \rangle) \neq 1$ divise $|H|$ et $|K|$.

Alors $pgdc(12, 5) \neq 1$, ce qui est absurde.

10.7

1. p, q des nombres premiers et G un groupe d'ordre pq

$\diamond$ **Tout sous-groupe de G est cyclique**.

Car soit H un sous-groupe de G. Alors $o(H)|o(G)$ ie. $o(H)|pq$. On les cas où $o(H)$ est 1, p ou q.

Si $o(H) = 1$, H est triviallement cyclique. Sinon, spdg, $o(H) = q$. Alors soit $a \in H - \{e\}$. Alors l'ordre de a doit diviser l'ordre de H et n'est pas 1. Alors il doit être q. Mais alors il s'agit d'un générateur.

10.8

1. p premier et G un groupe d'ordre p^2

◇ **Il existe H un sous group de G d'ordre p**

Soit $a \in G - \{e\}$. Alors $o(a)|p^2$. Si $o(a)|p$, on a finit. Sinon, $o(a) = p^2$ et donc G est cyclique. Soit alors $b = a^p$. Alors $b \neq e$. Aussi, $b^p = (a^p)^p = a^{p^2} = e$.

Or, il doit bien s'agir de l'ordre de b, car sinon l'ordre de a serait différent. Donc $\langle b \rangle$ est un sous-groupe d'ordre p.

10.9

1. H,K des sous groupes de G tel que $|H| = 39$ et $|K| = 65$

◇ $H \cap K$ **est cyclique**

TODO Faire avec des cosets

Si $|H \cap K| = 1$, la chose est triviale. Soit alors $|H \cap K| \neq 1$. Alors il existe $a \in H \cap K$ tel que a divise 39 et 65. Or 13 est le seul diviseur commun de ces nombres. Donc $o(a) = 13$ $\forall a \in H \cap K$.

On a alors que $H \cap K$ est d'ordre 26 ou 39.

Supposons l'ordre 26. Alors $\langle a \rangle$ est un sous-groupe de $H \cap K$ d'ordre 13 et il existe $b \in H \cap K$ tel que $b \notin \langle a \rangle$. Alors $\langle b \rangle \cap \langle a \rangle = \{e\}$, car tous leurs éléments sont des générateurs (tous d'ordre 13).

Mais alors il existe $c \notin \langle a \rangle$, $c \notin \langle b \rangle$ car $\langle a \rangle$, $\langle b \rangle$ ont un élément en commun, notamment e, et donc représentent 25 des 26 éléments de $H \cap K$. Or c est d'ordre 13 et donc $\langle c \rangle$ est également un sous-groupe contenant 13 éléments distincts de ceux se trouvant dans $\langle a \rangle$ et $\langle b \rangle$. Alors la cardinalité de $H \cap K$ est d'au moins 38, ce qui est absurde.

L'argument est le même dans le cas où la cardinalité serait 39. Donc la cardinalité est 13 et il s'agit d'un groupe cyclique.

10.10

◇ **Donnez une autre preuve du théorème de Lagrange.**

Soit $H := \{h_1, h_2, \cdots h_k\}$ un sous-groupe de G où $|G| = n$. On pose $n = dk + r$.

On considère le sous-groupe aH pour $a \notin H$. Alors aH comprends k éléments distincts. Il rest alors $d(k-1) + r$ éléments desquels choisir. Soit alors $b \notin aH$. Alors il s'agit d'un autre coset possédant k éléments dinstincts. De plus, tous ses éléments sont distincts de aH.

Car sinon, $bh_i = ah_j$. Alors $bh_ih_j^{-1} = a \in bH$, car $h_ih_j \in H$. Mais alors $aH = bh_ih_j^{-1}H = bH$. Donc $b \in aH$, ce qui est absurde.

Répétant la procédure k fois, il reste finalement r éléments disponible n'appartenant à aucun des cosets précédemment construit.

Soit alors cH un coset formé à partir de ces r éléments. Alors, nécessairement, cH possède k éléments distincts où $k > r$. Alors cH doit avoir $k - r$ éléments appartenant à au moins un autre coset, disons vH. Mais alors $cH = vH$ par un argument similaire à celui présenté plus haut. Alors c était déjà dans un coset, ce qui est absurde.

Donc $r = 0$ et donc $n = dk$, ie. $|H|$ divise $|G|$.

10.13

1. G un groupe
2. H un sous-groupe
3. $\phi(Ha) = aH$

$\diamond$ **Montrez que f n'est pas nécessairement bien définie.**

On pose $G = S_3$, $H =< g >$ et alors $< g > gf =< g > f$ mais $gf < g > \neq f < g >$.

10.14

b)

1. G un groupe d'ordre 6
2. G pas cyclique

$\diamond$ G **doit contenir des éléments d'ordre 1,2,3 et au moins un de 3**

Car l'ordre des sous-groupes cycliques de G doit diviser l'ordre de G. Or, les seules diviseurs de 6 inférieurs à 6 sont 1,2,3.

Puisque tous les éléments ne peuvent pas avoir ordre 1, il doit au moins y avoir un éléments d'ordre 2. Mais puisque les 4 éléments restant ne peuvent pas tous être d'ordre 1, on suppose un deuxième élément d'ordre 2. Soit b, c ces éléments. Alors $b \neq c$ et donc $o(bc) \neq 1$.

Supposons $o(bc) = 2$. Alors $< bc >, b < bc > etc < bc >$ sont trois cosets disjoints deux à deux. Or, $b < bc >, c < bc >$ ne sont pas disjoints.

Donc bc doit être d'ordre 3.

c)

1. a un élément d'ordre 3
2. $b \notin < a >$

$\diamond$ e, a, a^2, b, ab, a^2b **décrit complètement** G

Car il existe deux cosets distincts de $< a >$, notamment $< a >$ et $< a > b$.

Or $< a >= \{e, a, a^2\}$ et $< a > b = \{b, ab, a^2b\}$.

d)

1. Même que b

$\diamond$ $o(b) = o(ab) = o(a^2b) = 2$

Puisque les cosets exhibés ci-haut sont tous les éléments de G, on a que b^2 doit être dans l'un d'eux.

Or, $b^2 \neq b$. De plus, $b^2 = ab \Rightarrow b = a$ et $b^2 = a^2b \Rightarrow b = a^2$. Or, $b \notin < a >$.

Donc b^2 n'est pas dans $< a > b$ et n'est pas a, a^2. Alors $b^2 = e$. Mais de même ab, a^2b ne sont pas dans $< a >$, la seule hypothèse dont nous disposions par rapport à b. Donc par le même raisonnement, ils sont également d'ordre 2.

e)

$\diamond$ $ba = a^2b$ **et** $ba^2 = ab$

Car $a^2b = (a^2b)^{-1} = b^{-1}a^{-2} = ba$, puisque a^2b est d'ordre 2.

De même, $ab = (ab)^{-1} = b^{-1}a^{-1} = ba^2$.

10.17

1. p premier

$\diamond$ **La multiplication sur** $G := \mathbb{Z}_p - \{0\}$ **est associative**

Premièrement, on a que l'opération de composition sur $\mathbb{Z}_p - \{0\}$ est bien définie. Car, pour chaque $x \in G$, sa factorisation première ne comprends pas p, puisque $x < p$. Alors pour tout $y \in G$, xy n'est pas divisible par p et donc $xy \in G$.

Pour $x, y, z \in G$, on pose $xyz = dp + r$, $xy = np + r_1$ et $yz = mp + r_2$. On a $(xy)z = npz + zr_1 = dp + r$ et donc $(npz + zr_1) \mod p = (dp + r) \mod p$, d'où il suit que $zr_1 = r$. De la même manière, $xr_2 = r$ et donc $xr_2 = zr_1$. Donc $(xr_2) \mod p = x \odot r_2 = (zr_1) \mod p = z \odot r_1$.

Ainsi, $(x \odot y) \odot z = r_1 \odot z = x \odot r_2 = x \odot (y \odot z)$.

10.18

1. $S_m := \{a : (a, m) = 1\}$
2. $\phi(m) := |S_m|$
3. $G := (S_m, \odot)$ où $\odot$ est la multiplication $\mod m$

$\diamond$ $\forall m \in \mathbb{N}^* \ \forall a \in S_m \ a^{\phi(m)} \equiv 1 \mod m$

Premièrement, le groupe est bien définie car m ne sera jamais diviseur de ab pour tout $a, b \in S_m$.

Soit alors $a \in G$ et donc dans S_m. Alors $a^{\phi(m)} = 1$ (**thm. 10.4**).

Donc $a^{\phi(m)} - 1 = 0 \Leftrightarrow a^{\phi(m)} (\mathrm{mod} p) - 1 (\mathrm{mod} p) = 0 \Leftrightarrow (a^{\phi m} - 1) \bmod p = 0$.

Mais alors $p|(a^{\phi(m)} - 1)$, ce qu'il fallait démontrer.

10.19 (Théorème de Wilson)

1. p premier
2. $G := (\mathbb{Z}_p - \{0\}, \odot)$

a)

$\diamond$ $(p-1)! \equiv -1 (\mathrm{mod} p)$

On a que $(p-1)^2 = (p(p-2)+1) \bmod p = 1$ et donc $(p-1)$ est son propre inverse. Mais il s'agit du seul nombre de forme $(p-i)$ $1 \leq i \leq p-1$ qui soit sont propre inverse, car $(p-i)^2 = i$, et donc i doit être identique à 1 pour pouvoir l'être.

Il suit de là que, puisque nous sommes en présence d'un groupe, chaque inverse de $(p-i)$ $1 < i \leq p-1$ doit être dans l'expression $(p-2)!$. Or, G est abelien. Donc $(p-2)! = 1$ (**Car le nombre de terme dans** $(p-2)!$ **est pair si on exclu le 1**).

Puisque l'opération de composition sur G est associative (**ex. 10.17**), on a que $(p-1) \odot (p-2) \odot \cdots \odot 2 = [(p-1) \bmod p][(p-2)! \bmod p] = (p-1) \bmod p$.

Ainsi $(p-1)! \bmod p = (p \bmod p) + (-1 \bmod p)$ et donc $((p-1)! + 1) \bmod p = 0$, c'est dire $(p-1)! \equiv -1 \bmod p$.

b)

$\diamond$ $n \geq 2$ **et** $(n-1)! \equiv -1 \bmod n$ **alors** n **est premier**

Supposons que n ne soit pas premier. Alors il existe $1 < i, j < n$ tel que

$(n-i)(n-j) = n$. Or, on a que $(n-1)! \bmod n = 1$. Mais $(n-1)!$ est divisible par n puisque $(n-i)(n-j) = n$. Alors $(n-1)! \bmod n = 0 = 1$, une contradiction. Donc n est premier.

10.20 : Double cosets

1. G un groupe et H, K sous-groupes de G
2. $HgK := \{hgk : h \in H \text{ et } k \in K\}$

$\diamond$ HgK **est l'union d'exactement** $[H : H \cap xKx^{-1}]$ **cosets gauches de** K

Car supposons $g \in G$ quelconque et $h_1, h_2, \cdots h_n$ les éléments de H. Alors $HgK = h_1gK \cup h_2gK \cup \cdots \cup h_ngK$.

Or, soit h_i, h_j tel que $h_igK = h_jgK$. Alors $h_i^{-1}h_jgK = gK$ et donc $h_i^{-1}h_jg \in gK$. Alors $h_i^{-1}h_j \in gKg^{-1}$.

Mais $h_i^{-1}h_j \in H$ et donc $h_i^{-1}h_j \in H \cap gKg^{-1}$ ssi $h_j \in h_i^{-1}(H \cap gKg^{-1})$.

Donc $h_jgK = h_igK$ ssi h_j, h_i sont dans le même coset gauche de $H \cap gKg^{-1}$. Puisqu'il existe $[H : H \cap gKg^{-1}]$ cosets gauche de ce sous-groupe, on peut déduire $HgK = h_1gK \cup \cdots \cup h_ngK = h_{i_1}gK \cup \cdots \cup h_{i_{[H:H\cap gKg^{-1}]}}gK$.

10.21 : Groupe d'ordre 77

1. G un groupe d'ordre 77

$\diamond$ **Il existe** $a, b \in G$ **tel que** $o(a) = 11$ **et** $o(b) = 7$**.**

Puisque les facteurs de 77 sont 1,7,11, on a que tout élément de G doit être de cet ordre (**thm. 10.4**). Or, puisque le seul élément d'ordre 1 est l'identité, il doit exister un élément d'ordre 7 ou un élément d'ordre 11.

Supposons qu'il n'existe pas d'élément d'ordre 11. Alors il existe 76 éléments d'ordre 7. Soit alors $a \neq e$ de G. Le sous-groupe $< a >$ d'ordre 7 est cyclique (**thm. 10.5**) et doit comprendre 6 éléments dinstincts de G. Soit alors $b \notin < a >$. Alors de même $< b >$ comprends 6 éléments de G qui ne sont pas dans $< a >$ (**Deux sous-groupes cyclique d'ordre premier doivent être disjoints**).

En répétant la procédure pour 12 éléments, on obtient 73 éléments compris dans tous les sous-groupes (**les éléments distincts et l'identité**. Il reste donc 4 éléments d'ordre 7. Mais alors les sous-groupes générés par ceux-ci doivent avoir des éléments en communs avec ceux générés précédemment, ce qui est absurde.

On peut de même supposer qu'il n'existe que des éléments d'ordre 11, pour finalement obtenir 6 éléments en reste après une décomposition en sous-groupes cycliques d'ordre 11.

10.22

1. G un groupe fini tel que $(xy)^3 = x^3y^3$ pour tout $x, y \in G$
2. $3 \not| o(G)$

a)

$\diamond$ **G est abelien.**

Car $\forall a, b \in G \quad (ab)^2 = b^2a^2$. En effet, $(ba)^3 = b^3a^3 = bababa$. Alors $b^2a^2 = abab = (ab)^2$.

Aussi, puisque $3 \not| o(G)$, alors $o(G) = 3k + r$ pour un certain $k \in \mathbb{N}$ et $r \in \{1, 2\}$.

Puisque $a^{o(G)} = e$, alors $a^{3k} = a^{-r}$. On a aussi que $(aba^{-1})^3 = a^3b^3 \Leftrightarrow ab^3a^{-1} = a^3b^3a^{-3} \Leftrightarrow b^3a^2 = a^2b^3$.

Par conséquent, pour tout $b \in G$, $(b^{-k})^3a^2 = b^ra^2 = a^2b^r$.

Supposons que $r = 1$. Alors on considère $a, b \in G$ et l'on a $a^2b^2 = b^2a^2$. Alors $(ab)^2 = b^2a^2 = abab = a^2b^2$. Or $a^2b^2 = abab \Leftrightarrow ab = ba$.

Si $r = 2$, alors on a encore $a^2b^2 = b^2a^2$.

10.24

1. $\exists g \in G$ tq $Z(g) = Z(G)$

$\diamond$ **G est abelien**

Car $g \in Z(g)$ et donc $g \in Z(G)$, c'est-à-dire que g commute avec tous les éléments de G.

Mais alors $Z(g) = G$. Or $Z(g) = Z(G)$.

10.27

1. G un groupe fini

$\diamond$ **$[G : Z(G)]$ ne peut pas être premier**

On considère $|G| = |Z(G)| + [G : Z(a_1)] + \cdots + [G : Z(a_k)]$. Alors $[G : Z(a_i)] > 1$ pour tout i (**class equation**).

Or, on a que $Z(G) \subseteq Z(a_i)$ pour tout i car $z \in Z(G) \Rightarrow za_i = a_iz$ (**def.**). Or puisque $Z(G)$ est fermé sous son opération de composition, $Z(G)$ est un sous-groupe de $Z(a_i)$ (**thm. 5.3**). Donc $|Z(G)|$ divise $|Z(a_i)|$ (**Lagrange**).

On a donc que $[G : Z(G)] = [G : Z(a_i)][Z(a_i) : Z(G)]$ (**ex. 10.15**). Soit

alors $[G : Z(G)] = p$ premier.

On a $[G : Z(a_i)] \neq 1$ car $[G : Z(a_i)] > 1$ (**ci-haut**). Donc $[Z(a_i) : Z(G)] = 1$ et $[G : Z(a_i)] = p$. Mais $[Z(a_i) : Z(G)] = 1$ implique que $|Z(G)| = |Z(a_i)|$ et donc $Z(G) = Z(a_i)$ ($Z(G) \subseteq Z(a_i)$ **groupes finis**). Mais alors G est abelien (**ex. 10.24**) et donc $[G : Z(G)] = 1$, une contradiction.

10.28

1. p un nombre premier
2. n un entier positif
3. G un groupe tq $|G| = p^n$

$\diamond$ **Utiliser la class equation pour montrer que** p **divise** $|Z(G)|$

Car on ré-arrange la class equation pour montrer

$$p(p^{n-1} + \sum_{i=1}^{k} p^{n-1}|Z(a_i)|^{-1}) = |Z(G)|$$

On a que p^{n-1} est un entier. De plus, pour tout i, $|Z(a_i)|$ divise p^{n-1}. (**Je peux le montrer sans invoquer le thm. fond. de l'artihmétique, mais c'est fastidieu et, si je l'invoque, alors je prouve également que** $|Z(G)|$ **est divisible par** p.)

10.29

1. p premier
2. G un groupe tel que $|G| = p^2$

$\diamond$ G **est abelien**

Par **ex. 10.28**, p divise $|Z(G)|$. Donc $|Z(G)| \in \{p, p^2\}$. Or $[G : Z(G)]$ n'est pas premier par **ex. 10.27**, donc $|Z(G)| \neq p$, donc est égal à p^2. Mais alors $G = Z(G)$ et donc G est abelien.

10.30

1. G un groupe fini non abelien
2. p un nombre premier
3. p divise G

$\diamond$ **Il existe un** $b \in G$ **tel que** $b \notin Z(G)$ **et** p **divise** $Z(b)$

Si p divise $|Z(G)|$, on a finit car $|Z(G)|$ est un sous-groupe de $Z(a) \forall a \in G$.

Soit alors p qui ne divise pas $|Z(G)|$.

Supposons de plus que p ne divise pas $|Z(a)|$ pour tout $a \in G$. Alors $[G : Z(a)] = \frac{|G|}{|Z(a)|} = \frac{dp}{|Z(a)|}$ et l'on peut conclure que $|Z(a)|$ divise d pour tout a (**pgdc**$(p, |Z(a)| = 1)$ **et thm 4.3**).

Alors, par la **class equation**, on a

$$pd = |Z(G)| + p\sum_{i=1}^{k} \frac{d}{|Z(a_i)|}$$

$$\Leftrightarrow$$

$$p(d - \sum_{i=1}^{k} \frac{d}{|Z(a_i)|}) = |Z(G)|$$

et donc p divise $|Z(G)|$, contrairement à ce que l'on avait supposé.

10.31

1. p un nombre premier
2. $n \in \mathbb{N}$
3. G un groupe tel que $|G| = p^n$
4. H un sous-groupe d'ordre p tel que $\forall g \in G h \in H ghg^{-1} \in H$
5. $|H|$ divise $|Z(G)|$

$\diamond$ $H \subseteq Z(G)$

Premièrement, puisque H est d'ordre p on a que H est cyclique et abelien.

Supposons alors $g \in G$ et $h \in H$. Alors

$$(ghg^{-1})(g^{-1}hg) = (g^{-1}hg)(ghg^{-1})$$

$$\Leftrightarrow$$

$$ghg^{-2}hg = g^{-1}hg^2hg^{-1}$$

$$\Leftrightarrow$$

$$g^2h(g^{-2}hg^2) = hg^2h$$

$$\Leftrightarrow$$

$$(g^{-2}hg^2)g^2h = hg^2h$$

$$\Leftrightarrow$$

$$g^{-2}hg^4h = hg^2h$$

$$\Leftrightarrow$$

$$g^{-2}hg^4 = hg^2$$

$$\Leftrightarrow$$

$$hg^2 = g^2h$$

Supposons alors $p \neq 2$. Alors tous les membres de G divisent p^n (**thm. 10.4**) et donc $o(g) = p^i$ pour $i \in \{1 \cdots n\}$, ie. $o(g)$ est impair (**thm. 4.3**).

Soit alors g un élément de G. Alors $< g >$ est un sous-groupes de G (**thm. 5.3**). Alors je dis qu'il existe un b de $< g >$ tel que $b^2 = g$. Car $o(g) = 2k + 1$ (**Euclide**). Alors $k = \frac{o(g)-1}{2}$. Or, puisque $g^{-k} \in < g >$, on a $(g^{-k})^2 = g^{-2k} = g^{1-o(g)} = g$.

On a donc montré que tout élément d'ordre impair g possède un "racine carrée" b tq $b^2 = g$. Mais on a montré plus haut que $hg^2 = g^2h$ pour tout $h \in H$. Donc si $p \neq 2$, $H \subseteq Z(G)$.

Soit alors $p = 2$. Alors $|H| = \{e, h\}$ ($|H| = p$ **hyp.**). Or $\forall g \in G \quad ghg^{-1} \in H$ (**hyp.**). Alors $ghg^{-1} = e \Leftrightarrow gh = g \Leftrightarrow h = e$, une contradiction. Alors $ghg^{-1} = h \Leftrightarrow gh = hg$ et ce pour tout g. Donc $h \in Z(G)$ et donc $H \subseteq Z(G)$.

10.32

1. G un groupe
2. X un ensemble
3. $F : G \times X \to X$ une action à gauche sur X (où $g \cdot x := F(g, x)$)
4. $orb(x) := \{g \cdot x : g \in G\}$
5. $G_x := \{g \in G : g \cdot x = x\}$

a)

1. $R \subseteq X \times X$ une relation tq $x_1 R x_2$ ssi $\exists g \in G$ tq $x_1 = g \cdot x_2$

$\diamond$ R **est une relation d'équivalence sur** X

Trivial

b)

$\diamond$ G_x **est un sous-groupe de** G

Trivial

c)

$\diamond$ $|orb(x)| = [G : G_x]$

On définit $f : orb(x) \to \{gG_x : g \in G\}$ par $f(x) = gG_x$ où $g \cdot x = y \in orb(x)$. On montre d'abord que cette fonction est bien définie.

Car soit $y \in orb(x)$ tq $g_1 x = y = g_2 x$ pour $g_1 \neq g_2$. Alors on a que $g_2^{-1} g_1 = x$, c-à-d que $g_2^{-1} g_1 \in G_x \Leftrightarrow g_2^{-1} g_1 G_x = G_x \Leftrightarrow g_1 G_x = g_2 G_x$ (**cor. 9.4**). La

fonction est donc bien définie.

Or, il est clair que la fonction est surjective, puisque pour tout gG_x, $g \cdot x \in orb(x)$ (**def.** $orb(x)$).

De plus, si $f(y) = f(z)$, alors il existe $g_1 x = z$ et $g_2 x = y$ tel que $g_1 G_x = g_2 G_x \Leftrightarrow g_2^{-1} g_1 G_x = G_x \Leftrightarrow g_2^{-1} g_1 \cdot x = x \Leftrightarrow g_1 \cdot x = g_2 \cdot x$ et donc la fonction est injective (**cor. 9.4**).

10.33

1. G un groupe fini
2. X un ensemble fini
3. $\cdot$ une action à gauche de G sur X
4. $X_g := \{x \in X : g \in G_x\}$
5. N le nombre d'orbites distinctes de X sous l'action $\cdot$ de G

$\diamond$ $N = \dfrac{1}{|G|} \sum_{g \in G} |X_g|$