I. GÉNÉRALITÉS SUR LES GROUPES,

groupes finis, groupe symétrique

0. Rappels.

Nous supposons connues les notions de groupe, groupe abélien (ou commutatif), de sous-groupe, d'homomorphisme de groupes.
Nous noterons généralement multiplicativement : $(g,h) \mapsto gh$ les lois de groupe, l'élément neutre sera alors noté 1, l'inverse de g sera noté g^{-1}. Cette règle aura dans ce livre une exception majeure, celle du groupe $\mathbf{Z}$, ses sous-groupes et ses quotients, ainsi que des groupes additifs des corps et des espaces vectoriels qui seront bien entendu notés additivement.

Le cardinal d'un groupe fini est aussi appelé son ***ordre***. Si p est un nombre premier, on appelle p-groupe un groupe dont le cardinal est une puissance de p. Si g est un élément de G, l'ordre de g est le plus petit entier $n > 0$ (s'il en existe) qui vérifie $g^n = 1$. C'est aussi l'ordre du sous-groupe engendré par g, cf. § 1 ci-dessous.

Le ***noyau*** d'un homomorphisme $f : G \to H$ est le sous-groupe de G défini par :

$$\operatorname{Ker} f = \{g \in G \mid f(g) = 1\}.$$

L'image de f est aussi un sous-groupe de H, noté $\operatorname{Im} f$. Un isomorphisme est un homomorphisme de groupes bijectif. Un ***automorphisme*** d'un groupe G est un isomorphisme de G sur G. Un exemple d'automorphisme est fourni par les ***automorphismes intérieurs***. Un tel automorphisme i_g est donné, pour $g \in G$, par la formule $i_g(x) = gxg^{-1}$.

Si H est un sous-groupe d'un groupe G on appelle ***classe à gauche*** de l'élément $a \in G$ relativement à H le sous-ensemble

$$aH = \{g \in G \mid g = ah, \quad h \in H\}$$

et on définit de même les classes à droite Ha. Les classes à gauche forment une partition de G. Leur ensemble est noté G/H. Ce n'est pas un groupe en général. Le cardinal de G/H est appelé l'***indice*** de H dans G et noté $(G : H)$.
Lorsque le groupe est fini, la considération des classes à gauche conduit au théorème suivant :

Théorème 0.1 (Lagrange).
Si H est un sous-groupe du groupe fini G, l'ordre de H et l'indice de H dans G divisent l'ordre de G. Précisément, on a

$$|G| = |H|\,|G/H| = |H|(G : H).$$

En particulier l'ordre d'un élément $g \in G$ divise l'ordre de G.

Le groupe des bijections (ou permutations) d'un ensemble E s'appelle le ***groupe symétrique*** de E et est noté $\mathfrak{S}(E)$. Si E et E' ont même cardinal les groupes symétriques associés sont isomorphes. Lorsque l'on a $E = \{1, 2, \ldots, n\}$ avec $n \in \mathbf{N}$ on pose $\mathfrak{S}(E) = \mathfrak{S}_n$ et on parle du groupe symétrique standard. Le cardinal de ce groupe est $n!$.

Le groupe symétrique contient des permutations remarquables : les ***cycles*** d'ordre k. Un tel cycle est noté $\sigma = (a_1, a_2, \ldots, a_k)$ avec les $a_i \in E$, distincts et la notation signifie que l'on a $\sigma(a) = a$ si a n'est pas l'un des a_i et $\sigma(a_i) = a_{i+1}$ (où l'indice est pris modulo k). Un tel cycle est un élément d'ordre k (i.e. vérifie $\sigma^k = 1$). Pour $k = 2$ on parle de ***transpositions***.

Le groupe $\mathfrak{S}_n$ est muni d'un homomorphisme surjectif, appelé signature, et noté $\varepsilon : \mathfrak{S}_n \to \{1, -1\}$, que l'on peut définir de multiples façons (cf. par exemple [L]) mais dont nous retiendrons les propriétés suivantes :
a) si τ est une transposition on a $\varepsilon(\tau) = -1$, plus généralement,
b) si σ est un cycle d'ordre k on a $\varepsilon(\sigma) = (-1)^{k+1}$.
Le noyau de ε est formé des permutations paires (i.e. celles qui vérifient $\varepsilon(s) = 1$). C'est un groupe de cardinal $n!/2$, appelé groupe ***alterné*** et noté $\mathfrak{A}_n$.

Enfin, le lecteur est supposé avoir une certaine familiarité avec quelques d'objets élémentaires comme les groupes additifs $\mathbf{Z}/n\mathbf{Z}$ des congruences modulo n ou le groupe de Klein $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}, \ldots$

1. Générateurs d'un groupe.

Proposition-définition 1.1.
Soient G un groupe et $A \subset G$ une partie de G. Il existe un plus petit sous-groupe H de G contenant A. On dit que H est le sous-groupe engendré par A, ou que les éléments de A sont des ***générateurs*** *de H. On note $H = <A>$.*

Démonstration. L'existence de H peut se voir de deux manières :
a) par « l'extérieur » : on considère tous les sous-groupes de G contenant A (il y a au moins G tout entier) et leur intersection convient ;
b) par « l'intérieur » : on suppose A non vide (sinon on a $H = \{1\}$), on pose $A^{-1} = \{x \in G \,|\, x^{-1} \in A\}$, puis $H = \{a_1 \ldots a_n \,|\, n \in \mathbf{N},\ a_i \in A \cup A^{-1}\}$. Alors H est un groupe, contient A et est évidemment le plus petit possible.

Exemples 1.2.

1) Groupes monogènes et cycliques.

Un groupe G engendré par un élément a, est dit ***monogène***. Il est isomorphe à $\mathbf{Z}$ ou $\mathbf{Z}/n\mathbf{Z}$, pour un $n \in \mathbf{N}$ (considérer l'homomorphisme surjectif $\varphi : n \mapsto a^n$, de $\mathbf{Z}$ dans G). Dans le second cas, G est dit ***cyclique***. En particulier, si $|G| = p$ est un nombre premier, G n'a pas de sous-groupe non trivial (en vertu du théorème de Lagrange), donc si $a \in G$ et $a \neq 1$, G est égal à $<a>$, donc cyclique et on a $G \simeq \mathbf{Z}/p\mathbf{Z}$.

2) Groupes symétrique $\mathfrak{S}_n$ et alterné $\mathfrak{A}_n$.

a) Les transpositions engendrent $\mathfrak{S}_n$, on peut même se limiter aux transpositions $(1,2)$, $(1,3),\dots(1,n)$ ou encore $(1,2)$, $(2,3),\dots(n-1,n)$ comme on le voit aisément par récurrence sur n.
Le lecteur montrera, à titre d'exercice, que la transposition (1,2) et le n-cycle (1,2,...,n) engendrent $\mathfrak{S}_n$ (cf. 4.10 ci-dessous).

b) Les cycles d'ordre 3 engendrent $\mathfrak{A}_n$, pour $n \geq 3$. En effet, $\mathfrak{A}_n$ est engendré par les produits pairs de transpositions et on a les formules :

$$(a,b)(b,c) = (a,b,c),$$

$$(a,b)(a,c) = (a,c,b)$$

(ce qui prouve au passage que tous les cycles d'ordre 3 sont dans $\mathfrak{A}_n$),

$$(a,b)(c,d) = (a,b)(a,c)\ (a,c)(c,d) = (a,c,b)(a,c,d).$$

Nous verrons, à propos des groupes classiques, de nombreux autres exemples de générateurs.

2. Sous-groupes distingués.

Définition 2.1.
Soit G un groupe et H un sous-groupe de G. On dit que H est ***distingué*** *dans G s'il est invariant par automorphisme intérieur i.e. si on a :*

$$\forall a \in G,\ \forall h \in H,\ aha^{-1} \in H.$$

On note alors : $H \lhd G$.

Remarques 2.2.
0) La condition ci-dessus équivaut à dire que pour tout $a \in G$ on a $aH = Ha$, i.e. l'égalité des classes à droite et à gauche modulo H.
1) Si $f : G \longrightarrow G'$ est un homomorphisme, son noyau $\operatorname{Ker} f$ est un sous-groupe distingué de G.
2) Réciproquement, si on a $H \lhd G$, le quotient G/H, ensemble des classes à gauche (ou à droite) est muni d'une structure de groupe et on a un homomorphisme surjectif $p : G \longrightarrow G/H$, de noyau H.
Dans la situation de 1) on a, de plus, un isomorphisme :

$$\operatorname{Im} f \simeq G/\operatorname{Ker} f.$$

3) Enfin on définit une ***suite exacte*** :

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{p} H \longrightarrow 1.$$

Dans cette écriture, N, G, H sont des groupes, i, p des homomorphismes et la suite est dite exacte si : 1) i est injectif, 2) p est surjectif, 3) on a $\operatorname{Im} i = \operatorname{Ker} p$.
Lorsque les groupes sont abéliens et notés additivement on écrit les suites exactes avec des 0 :

$$0 \to N \to G \to H \to 0.$$

Exemples 2.3.

1) $\{1\}$ et G sont toujours des sous-groupes distingués (dits triviaux).

2) Si G est abélien, tout sous-groupe de G est distingué. Pour la réciproque, cf. Exercice B.3.

3) Étudions le groupe $\mathfrak{S}_3$ qui a 6 éléments :
$1 = \mathrm{Id}$, $\tau_c = (a,b)$, $\tau_b = (a,c)$, $\tau_a = (b,c)$, $\sigma = (a,b,c)$, $\sigma^2 = \sigma^{-1} = (a,c,b)$.
Le groupe $\mathfrak{S}_3$ contient un sous-groupe distingué d'ordre 3, $<\sigma>= \{1, \sigma, \sigma^2\} = \mathfrak{A}_3$, isomorphe à $\mathbf{Z}/3\mathbf{Z}$ et on a une suite exacte :

$$1 \longrightarrow \mathbf{Z}/3\mathbf{Z} \longrightarrow \mathfrak{S}_3 \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow 1.$$

En revanche les sous-groupes $<\tau_a>= \{1, \tau_a\}$ ... ne sont pas distingués, on a :

$$\sigma\tau_a\sigma^{-1} = \tau_{\sigma(a)} = \tau_b.$$

Définition 2.4.
Un groupe $G \neq \{1\}$ est dit ***simple*** *si ses seuls sous-groupes distingués sont $\{1\}$ et G.*

Exemples 2.5.

1) $\mathbf{Z}/p\mathbf{Z}$ est simple si et seulement si p est premier.

2) $\mathfrak{A}_n$ est simple pour $n \geq 5$ (cf. § 8).

2.6 Commentaire.

L'intérêt des sous-groupes distingués est de permettre le « dévissage » des groupes : si G est un groupe et si on a un sous-groupe distingué $H \lhd\!\!\lhd G$, on peut essayer de ramener l'étude de G à celle de H et de G/H (si G est fini, ces groupes sont de cardinal plus petit). Nous verrons des exemples de dévissages aux § 6 et § 7. Les groupes simples, eux, sont indévissables d'où l'intérêt particulier qu'on leur porte. La classification des groupes simples finis a été achevée en 1981, cf. [Pu].
Là encore, les groupes classiques nous fourniront beaucoup d'exemples de groupes simples.

3. Centre et commutateurs.

Nous exhibons maintenant deux sous-groupes distingués d'un groupe G, qui existent toujours, mais peuvent être triviaux : le centre et le groupe dérivé.

a) Le centre.

Définition 3.1.
Le ***centre*** *du groupe G est le sous-groupe de G formé des éléments qui commutent avec tous les autres :*

$$Z(G) = \{a \in G \mid \forall g \in G,\ ag = ga\}.$$

On a $Z(G) \lhd\!\!\lhd G$, ($Z(G)$ est même un sous-groupe ***caractéristique*** de G, i.e. invariant par tout automorphisme).

Exemples 3.2.

1) Si G est commutatif, on a $Z(G) = G$.

2) Si $G = \mathfrak{S}_n$, avec $n \geq 3$, on a $Z(G) = \{1\}$. En effet, soit $\sigma \in G$, $\sigma \neq 1$. Pour un certain i, on a $\sigma(i) = j \neq i$. Soit $k \neq i, j$ et $\tau = (j, k)$. Alors on a $\sigma\tau(i) = \sigma(i) = j$, $\tau\sigma(i) = \tau(j) = k$, donc $\sigma\tau \neq \tau\sigma$ et $\sigma \notin Z(G)$.

3) Soit $\mathbf{H}_8 = \{\mp 1, \mp i, \mp j, \mp k\}$ le groupe des quaternions (cf. Chapitre VII). (La multiplication est définie par la règle des signes et les formules

$$i^2 = j^2 = k^2 = -1;\ ij = -ji = k;\ jk = -kj = i;\ ki = -ik = j.)$$

Alors $Z(\mathbf{H}_8) = \{1, -1\}$ est non trivial, (cf. 4.15)

b) Les commutateurs.

Définition 3.3.

Le **groupe dérivé** $D(G)$ *est le sous-groupe* **engendré** *par les commutateurs de G, i.e. les éléments de la forme $xyx^{-1}y^{-1}$ avec $x, y \in G$.*(1)

Le groupe $D(G)$ est parfois appelé improprement groupe des commutateurs.
On a $D(G) \lhd G$, et même $D(G)$ caractéristique. En effet, si $\varphi \in \mathrm{Aut}\, G$, on a $\varphi(xyx^{-1}y^{-1}) = \varphi(x)\varphi(y)\varphi(x)^{-1}\varphi(y)^{-1}$, donc les commutateurs sont conservés. Notons que $G/D(G)$ est abélien. C'est même le plus grand quotient abélien de G, et ceci caractérise $D(G)$.

Exemples 3.4.

1) Si G est commutatif on a $D(G) = \{1\}$.
2) Si $G = \mathfrak{S}_3$ on a $D(G) = \{1, \sigma, \sigma^2\}$.
3) Si $G = \mathbf{H}_8$ on a $D(G) = \{1, -1\}$.
4) Si $G = \mathfrak{A}_5$ on a $D(G) = \mathfrak{A}_5$ (cf. § 8).

4. Opération d'un groupe sur un ensemble.

Définition 4.1.

Soit G un groupe, X un ensemble, on dit que G **opère** *sur X si on s'est donné une application :*

$$\begin{aligned} G \times X &\longrightarrow X \\ (g, x) &\longmapsto g.x \end{aligned}$$

vérifiant les axiomes suivants :
1) $\forall g, g' \in G,\ \forall x \in X,\ g.(g'.x) = (gg').x$
2) $\forall x \in X,\ 1.x = x$.

Il revient au même de se donner un homomorphisme $\varphi : G \longrightarrow \mathfrak{S}(X)$, où $\mathfrak{S}(X)$ désigne le groupe des bijections de X (on pose alors : $g.x = \varphi(g)(x)$).

4.2 Commentaire.

C'est une notion essentielle ! D'abord, c'est la situation que l'on rencontre dans toute géométrie (affine, avec le groupe affine, projective, avec $PGL(n, k)$ cf. Chapitre IV, euclidienne avec le groupe des isométries, hyperbolique avec le groupe de Lorentz etc), ensuite, parce qu'au delà de l'intérêt de l'opération pour l'étude

(1) *Le commutateur de x et y, $xyx^{-1}y^{-1}$, est appelé ainsi car il vaut 1 si et seulement si x et y commutent. On le note parfois $[x, y]$.*

de l'ensemble X, elle permet souvent en retour d'obtenir des renseignements sur le groupe G comme nous le verrons au paragraphe suivant.
Nous appellerons « géométriques » les propriétés d'un élément de G relatives à une opération (points fixes ...) par opposition aux propriétés « algébriques » (ordre d'un élément, commutation ...).

Définition 4.3.
a) On dit que G opère ***transitivement*** *sur X si on a :*

$$\forall x \in X,\ \forall y \in X,\quad \exists g \in G,\quad g.x = y.$$

b) On dit que G opère ***fidèlement*** *si $\varphi : G \longrightarrow \mathfrak{S}(X)$ est injectif i.e. si $g.x = x$ pour tout $x \in X$ implique $g = 1$.*

Notons que $G/\mathrm{Ker}\,\varphi$ opère fidèlement sur X. Ainsi, si E est un espace vectoriel, le groupe $GL(E)$ opère non fidèlement sur l'ensemble $\mathbf{P}(E)$ des droites vectorielles de E mais son quotient $PGL(E)$ opère fidèlement (cf. IV, 2.8).

Si G n'opère pas transitivement, on introduit la relation d'équivalence suivante :

$$x \mathcal{R} y \Longleftrightarrow \exists\, g \in G,\ y = g.x,$$

qui mesure le défaut de transitivité. Les classes pour cette relation sont les ***orbites*** de X sous G. L'orbite de $x \in X$ est notée $\omega(x)$. On notera que G opère transitivement sur $\omega(x)$.
Par exemple, les orbites du groupe orthogonal $O(n, \mathbf{R})$ dans son opération naturelle sur $\mathbf{R}^n$ sont les sphères de centre l'origine.

Exemple 4.4. Décomposition d'une permutation en produit de cycles disjoints.
Le groupe $\mathfrak{S}_n$ opère sur $X = \{1, 2, ..., n\}$. Soit $\sigma \in \mathfrak{S}_n$ et $<\sigma>$ le groupe cyclique engendré par σ qui opère aussi sur X. Soient $F_1, F_2, \ldots, F_r$ les orbites de X sous $<\sigma>$. Alors, les permutations σ_i définies par :

$$\sigma_i(x) = \begin{cases} x & \text{si } x \notin F_i \\ \sigma(x) & \text{si } x \in F_i \end{cases}$$

sont des cycles, d'ordre $|F_i|$, deux à deux permutables, et on a $\sigma = \sigma_1 \ldots \sigma_r$.
Par exemple si $X = \{1, \ldots, 8\}$ et

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 4 & 5 & 1 & 8 & 7 & 2 \end{pmatrix},$$

on a $\sigma = (1\,3\,4\,5)\,(2\,6\,8)\,(7) = (1\,3\,4\,5)\,(2\,6\,8)$, (en général, les cycles d'ordre 1 sont omis dans l'écriture de σ).

Définition 4.5.
Si G opère sur X et si $x \in X$, on définit $H_x = \{g \in G \mid g.x = x\}$.
C'est un sous-groupe de G (non distingué en général) appelé le ***stabilisateur*** *(ou encore fixateur) de x.*

Exemple 4.6. Dans l'opération de $\mathfrak{S}_n$ sur $X = \{1, ..., n\}$, le stabilisateur d'un point est isomorphe à $\mathfrak{S}_{n-1}$.

Orbites et stabilisateurs sont liés par la remarque évidente suivante (cf. aussi ci-dessous Exemple C) :

Proposition 4.7.
L'application $\overline{g} \mapsto g.x$ de G/H_x (ensemble des classes à gauche) dans $\omega(x)$ est bien définie et est une bijection.

Lorsque G est fini, on a donc $|\omega(x)| = |G|/|H_x|$, en particulier $|\omega(x)|$ divise $|G|$. Lorsque G et X sont munis de structures supplémentaires (par exemple topologiques) on peut souvent préciser la proposition. Ainsi, par exemple, on peut montrer que l'espace quotient $O(n, \mathbf{R})/O(n-1, \mathbf{R})$ est homéomorphe à la sphère unité $\mathbf{S}^{n-1}$ de $\mathbf{R}^n$.

4.8 Quelques exemples d'opérations.

Nous donnons ici seulement des exemples en théorie des groupes, les situations géométriques seront étudiées dans les chapitres suivants.

Exemple A.

On peut faire opérer G sur G par ***translation à gauche.***
On pose pour $g, a \in G$, $g.a = ga$. (Attention l'application $a \mapsto ga$ n'est pas un automorphisme de groupes).
On remarque que G opère alors simplement transitivement i.e.

$$\forall a, b \in G,\ \exists!\, g \in G,\ g.a = b \qquad (\text{on prend } g = ba^{-1}).$$

A fortiori, G opère donc fidèlement et on a un homomorphisme injectif

$$\varphi :\ G \longrightarrow \mathfrak{S}(G).$$

En particulier on en déduit le théorème de Cayley :

Théorème 4.9.
Si G est fini de cardinal n, G est isomophe à un sous-groupe de $\mathfrak{S}_n$.

Exemple B.

On peut aussi faire opérer G sur lui-même par ***automorphisme intérieur*** en posant $g.a = gag^{-1}$. Les orbites s'appellent alors ***classes de conjugaison*** et si $a' = gag^{-1}$, a' est un conjugué de a.
Le stabilisateur de a s'appelle ***centralisateur*** :

$$H_a = \{g \in G \mid gag^{-1} = a\} = \{g \in G \mid ga = ag\}.$$

On définit de même le centralisateur d'une partie de A de G :

$$C_G(A) = \{g \in G \mid \forall a \in A,\ ga = ag\}.$$

En particulier $C_G(G)$ est le centre de G. Dans le cas du groupe symétrique, on a la proposition suivante :

Proposition 4.10.
1) Si $\sigma \in \mathfrak{S}_n$ est un cycle d'ordre p, $\sigma = (a_1, \ldots, a_p)$ et si $\tau \in \mathfrak{S}_n$, on a

$$\tau\sigma\tau^{-1} = (\tau(a_1), \ldots, \tau(a_p)).$$

2) Dans $\mathfrak{S}_n$ tous les cycles d'ordre p sont conjugués.
3) Si $n \geq 5$ les cycles d'ordres 3 sont conjugués dans $\mathfrak{A}_n$.

Démonstration.
1) Si $x \notin \{\tau(a_1), \ldots, \tau(a_p)\}$, $\tau^{-1}(x) \notin \{a_1, \ldots, a_p\}$ et donc :

$$\tau\sigma\tau^{-1}(x) = \tau\tau^{-1}(x) = x.$$

Si $x = \tau(a_i)$, $\tau\sigma\tau^{-1}(x) = \tau\sigma(a_i) = \tau(a_{i+1})$ (les indices sont pris modulo p).

Il faut retenir de cet exemple ce qu'on peut appeler le **principe de conjugaison**. Il se résume en deux idées essentielles :

a) Si $g \in G$ est un élément « d'un certain type » $g' = \tau g \tau^{-1}$ est un élément « de même type ». Par exemple si g est d'ordre k, g' aussi ; si g a k points fixes, g' aussi ; en géométrie si g est une symétrie hyperplane, g' aussi ...

b) Si g est caractérisé « géométriquement » par un certain ensemble Y (ici, c'est l'ensemble des points fixes de g), l'ensemble Y' correspondant pour $g' = \tau g \tau^{-1}$ s'obtient en transportant Y par τ : $Y' = \tau(Y)$.
Nous retrouverons très souvent ce principe dans la suite.

Nous reprenons la démonstration de 4.10 :

2) Soient $\sigma = (a_1, \ldots, a_p)$, $\tau = (b_1, \ldots, b_p)$ et soit $g \in \mathfrak{S}_n$ tel que $g(a_i) = b_i$ pour tout i (il existe évidemment un tel g, même si $p = n$, on dit que $\mathfrak{S}_n$ est n-fois transitif). Alors on a $\tau = g\sigma g^{-1}$ en vertu du principe énoncé ci-dessus.

3) On a besoin du

Lemme 4.11.
Le groupe $\mathfrak{A}_n$ est $n-2$ fois transitif sur $\{1, \ldots, n\}$ i.e., si on a $a_1, \ldots a_{n-2}$ distincts et $b_1, \ldots b_{n-2}$ distincts, il existe $\sigma \in \mathfrak{A}_n$ tel que $\sigma(a_i) = b_i$.

En effet, on écrit :

$$\{1, \ldots, n\} = \{a_1, \ldots, a_{n-2}, a_{n-1}, a_n\} = \{b_1, \ldots, b_{n-2}, b_{n-1}, b_n\}$$

et on considère $\sigma \in \mathfrak{S}_n$ telle que $\sigma(a_i) = b_i$ pour tout $i = 1, \ldots, n$. Si σ est paire c'est terminé, sinon on compose σ avec la transposition (a_{n-1}, a_n).

Le même raisonnement qu'en 2) montre alors que pour $n \geq 5$, les 3-cycles sont conjugués dans $\mathfrak{A}_n$.

Remarque 4.12. Si $n = 3$ ou 4 l'assertion précédente est fausse. En effet, pour $n = 3$ le groupe $\mathfrak{A}_3$ est abélien donc la conjugaison y est triviale. Pour $n = 4$ il y a 8 cycles d'ordre 3 et ils ne peuvent être tous conjugués dans $\mathfrak{A}_4$ sinon ils formeraient une orbite dont le cardinal devrait diviser 12 en vertu de 4.7.

Exemple 4.13. Soit k un corps commutatif, $GL(n, k)$ le groupe des matrices carrées d'ordre n inversibles à coefficients dans k. Alors, pour $A, B \in GL(n, k)$:
A, B conjuguées $\iff \exists P \in GL(n, k)$, $B = P^{-1}AP \iff A, B$ semblables.

4.14 Une application aux p-groupes.

Rappelons que si p est un nombre premier, on appelle p-groupe un groupe dont le cardinal est une puissance de p. On a alors la proposition suivante :

Proposition 4.15.
Le centre d'un p-groupe distinct de $\{1\}$ n'est pas réduit à $\{1\}$.

Démonstration. On prouve d'abord le lemme suivant :