Compléments sur les groupes

1 Quelques théorèmes

Soit $f : G \longrightarrow G'$ un homomorphisme de groupes surjectif. Nous allons désigner par $S(G')$ l'ensemble des sous-groupes de G' et par $S_f(G)$ celui des sous-groupes de G contenant $Ker(f)$.

Théorème Il existe une bijection de $S(G')$ sur $S_f(G)$.

Démonstration Soit φ l'application de $S(G')$ dans $S_f(G)$ qui associe à H' le sous-groupe $f^{-1}(H')$ de G. φ est injective, car nous avons

$$\begin{aligned}\left[\varphi(H') = \varphi(K')\right] &\Longrightarrow \left[f^{-1}(H') = f^{-1}(K')\right] \\ &\Longrightarrow \left[f\left(f^{-1}(H')\right) = f\left(f^{-1}(K')\right)\right] \\ &\Longrightarrow \left[H' = K'\right]\end{aligned}$$

vu que f est surjective. D'un autre côté, si $H \in S_f(G)$, alors

$$H' = f(H) \in S(G') \text{ et } \varphi(H') = f^{-1}(H') = H$$

car nous avons

$$\begin{aligned}\left[x \in f^{-1}(f(H))\right] &\Longrightarrow \left[f(x) \in f(H)\right] \\ &\Longrightarrow (\exists y \in H)\left[f(x) = f(y)\right] \\ &\Longrightarrow \left[x - y \in Ker(f) \subseteq H\right] \\ &\Longrightarrow \left[x \in H\right]\end{aligned}$$

D'où $f^{-1}(f(H)) \subseteq H$. L'autre inclusion est évidente. Ainsi φ est surjective.

Théorème La bijection φ est croissante.

Démonstration Si $H' \subseteq K'$, alors

$$\begin{aligned}\left[x \in \varphi(H')\right] &\Longrightarrow \left[x \in f^{-1}(H')\right] \\ &\Longrightarrow \left[f(x) \in H'\right] \\ &\Longrightarrow \left[f(x) \in K'\right] \\ &\Longrightarrow \left[x \in f^{-1}(K') = \varphi(K')\right]\end{aligned}$$

D'où $\varphi(H') \subseteq \varphi(K')$.

Théorème H' est un sous-groupe distingué de G' si, et seulement si, le sous-groupe $H = \varphi(H')$ de G est distingué.

Démonstration Si H' est un sous-groupe distingué de G', alors nous avons

$$\begin{aligned}[x \in G, y \in H] &\Longrightarrow \left[f(x) \in G',\ f(y) \in H'\right] \\ &\Longrightarrow \left[f\left(x^{-1}yx\right) = f(x)^{-1} f(y) f(x) \in H'\right] \\ &\Longrightarrow \left[x^{-1}yx \in f^{-1}\left(H'\right) = H\right]\end{aligned}$$

Réciproquement, si le sous-groupe H de G est distingué, alors H' est un sous-groupe distingué de G'. En effet, si $x' \in G'$ et $y' \in H'$, alors il existe $x \in G$ et $y \in H$ tels que $x' = f(x)$ et $y' = f(y)$ ($H' = f\left(f^{-1}(H')\right) = f(H)$ car f est surjective). Nous avons

$$\left(x'\right)^{-1} y' x' = f(x)^{-1} f(y) f(x) = f\left(x^{-1}yx\right) \in f(H) = H'$$

car $x^{-1}yx \in H$.

Théorème Si H' est distingué dans G' et $H = \varphi(H')$, alors G'/H' est isomorphe à G/H.

Démonstration L'application

$$g; G \xrightarrow{f} G' \xrightarrow{p'} G'/H'$$

où p' est la surjection canonique qui est un homomorphisme de groupes. Il est surjectif et son noyau est H car

$$[x \in Ker(g)] \Longleftrightarrow \left[p'(f(x)) = g(x) = \overline{e'}\right] \Longleftrightarrow \left[f(x) \in H'\right] \Longleftrightarrow [x \in H]$$

D'où $G'/H' = \mathrm{Im}(g) \simeq G/H$.

2 Chaînes normales

Soient G_1 et G_2 deux sous-groupes de G tels que $G_1 \subseteq G_2$.

Définition On appelle **chaîne normale** de G entre G_2 et G_1 toute chaîne de sous-groupes de G

$$G_1 = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = G_2$$

telle que chaque H_i soit un sous-groupe distingué de son successeur H_{i+1}. Les groupes quotients $F_i = H_{i+1}/H_i$ pour $i = 0,1,...,n-1$ sont appelés les **facteurs** de la chaîne.

Définition On appelle **chaîne normale** du groupe G toute chaîne normale de G entre $\{e\}$ et G.

Exemple Soit S_3 le groupe des permutations de l'ensemble $\{1,2,3\}$ et A_3 le groupe alterné d'ordre 3. La chaîne

$$\{i\} \subseteq A_3 \subseteq S_3$$

est une chaîne normale du groupe S_3.

Théorème Si $f;G\longrightarrow G'$ est un homomorphisme surjectif, alors f transforme toute chaîne normale

$$\{e\}=H_0\subseteq H_1\subseteq\cdots\subseteq H_n=G$$

de G en une chaîne normale

$$\left\{e'\right\}=H_0'\subseteq H_1'\subseteq\cdots\subseteq H_n'=G'$$

de G' et il existe un homomorphisme surjectif u_i du facteur $F_i=H_{i+1}/H_i$ sur le facteur $F_i'=H_{i+1}'/H_i'$ pour $i=0,1,...,n-1$.

Démonstration L'homomorphisme f transforme la chaîne

$$\{e\}=H_0\subseteq H_1\subseteq\cdots\subseteq H_n=G$$

en la chaîne

$$\left\{e'\right\}=H_0'\subseteq H_1'\subseteq\cdots\subseteq H_n'=G'$$

où $H_i'=f(H_i)$ pour $i=0,1,...,n-1$. Cette chaîne est normale, car l'image d'un sous-groupe distingué par un homomorphisme surjectif est un sous-groupe distingué. D'un autre côté, L'application u_i définie par

$$u_i(p_i(x))=p_i'(f(x))$$

est bien définie, car nous avons

$$\begin{aligned}[p_i(x)=p_i(y)]&\Longrightarrow\left[xy^{-1}\in H_i\right]\\&\Longrightarrow\left[f(x)f(y)^{-1}=f\left(xy^{-1}\right)\in f(H_i)=H_i'\right]\\&\Longrightarrow\left[p_i'(f(x))=p_i'(f(y))\right]\end{aligned}$$

où p_i et p_i' sont les surjections canoniques. Il est facile de vérifier que u_i est un homomorphisme de groupes surjectif.

Théorème Si $f;G\longrightarrow G'$ est un homomorphisme injectif, alors toute chaîne normale

$$\left\{e'\right\}=H_0'\subseteq H_1'\subseteq\cdots\subseteq H_n'=G'$$

de G' est transformée par f^{-1} en une chaîne normale

$$\{e\}=H_0\subseteq H_1\subseteq\cdots\subseteq H_n=f^{-1}(G)=G$$

de $f^{-1}(G)$ et il existe un homomorphisme injectif v_i du facteur $F_i=H_{i+1}/H_i$ dans le facteur $F_i'=H_{i+1}'/H_i'$ pour $i=0,1,...,n-1$.

Démonstration Soit $H_i=f^{-1}(H_i')$ pour $i=0,1,...,n-1$. Les sous-groupes H_i de G forment une chaîne

$$\{e\}=H_0\subseteq H_1\subseteq\cdots\subseteq H_n=f^{-1}(G)=G$$

où $H_0 = f^{-1}(H_0') = f^{-1}(e') = Ker(f) = \{e\}$. Cette chaîne est normale car nous avons

$$\begin{aligned}[x \in H_{i+1}, y \in H_i] &\Longrightarrow \left[f(x) \in H_{i+1}',\ f(y) \in H_i'\right] \\ &\Longrightarrow \left[f\left(x^{-1}yx\right) = f(x)^{-1} f(y) f(x) \in H_i'\right] \\ &\Longrightarrow \left[x^{-1}yx \in H_i\right]\end{aligned}$$

L'application v_i est définie comme l'application u_i du théorème précédent. C'est un homomorphisme de groupes. Il est injectif car nous avons

$$\begin{aligned}\left[v_i(p_i(x)) = \overline{e'}\right] &\Longrightarrow \left[p_i'(f(x)) = \overline{e'}\right] \\ &\Longrightarrow \left[f(x) \in H_i'\right] \\ &\Longrightarrow \left[x \in f^{-1}\left(H_i'\right) = H_i\right] \\ &\Longrightarrow \left[p_i(x) = \overline{e}\right]\end{aligned}$$

Théorème Si chaque facteur d'une chaîne normale de G possède une chaîne normale, alors nous obtenons une chaîne normale de G en concaténant les différentes chaînes des facteurs. Les facteurs de la nouvelle chaîne sont isomorphes aux facteurs des chaînes des différents facteurs.

Démonstration Soit

$$\{e\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = G$$

une chaîne normale de G et soit

$$\{\overline{e}\} = K_{i,0} \subseteq K_{i,1} \subseteq \cdots \subseteq K_{i,n_i} = F_i$$

une chaîne normale du facteur F_i pour $i = 1,2,...,n-1$. La surjection canonique $p_i; H_{i+1} \longrightarrow F_i$ transforme cette chaîne en une chaîne normale de G entre H_i et H_{i+1}

$$H_i = L_{i,0} \subseteq L_{i,1} \subseteq \cdots \subseteq L_{i,n_i} = H_{i+1}$$

où $L_{ij} = p_i^{-1}(K_{ij})\ L_{i,j}/H_i \approx K_{i,j}$. Il en résulte que la chaîne

$$\begin{aligned}\{e\} = H_0 = L_{0,0} \subseteq L_{0,1} \subseteq \cdots \subseteq L_{0,n_0} = H_1 \subseteq \cdots \subseteq H_{n-1} \\ = L_{n-1,0} \subseteq L_{n-1,1} \subseteq \cdots \subseteq L_{n-1,n_i} = H_n = G\end{aligned}$$

est une chaîne normale de G. Il nous reste à prouver que le facteur $L_{i,j+1}/L_{i,j}$ est isomorphe au facteur $K_{i,j+1}/K_{i,j}$ et ceci pour $j = 0,1,...,n_i - 1$ et pour $i = 0,1,...,n-1$. La restriction de p_i à $L_{i,j+1}$ est un homomorphisme surjectif de $L_{i,j+1}$ sur $K_{i,j+1}$. Le dernier théorème de la section précédente nous donne l'isomorphisme recherché (prendre $G' = K_{i,j+1}$, $H' = K_{i,j}$ et $H = L_{i,j}$).

3 Groupes résolubles

Définition On dit qu'un groupe G est résoluble si, et seulement si, il possède une chaîne normale dont les facteurs sont abéliens.

Exemple Le groupe symétrique S_3 est résoluble.

Théorème Tout groupe abélien est résoluble.

Démonstration Il suffit de prendre la chaîne $\{e\} \subseteq G$.

Théorème Tout groupe cyclique est résoluble.

Démonstration Car un groupe cyclique est abélien.

Théorème Toute image par un homomorphisme d'un groupe résoluble est un groupe résoluble.

Démonstration Si G' est une image homomorphe du groupe résoluble G, alors il existe un homomorphisme surjectif $f;G \longrightarrow G'$. Si

$$\{e\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = G$$

est une chaîne normale de G à facteurs abéliens, alors la chaîne

$$\left\{e'\right\} = H_0' \subseteq H_1' \subseteq \cdots \subseteq H_n' = G'$$

où $H_i' = f(H_i)$ pour $i = 0,1,...,n-1$ est normale et ses facteurs sont des images homomorphes de ceux de la chaîne de G (par l'homomorphisme u_i). Il en résulte que la chaîne G' est une chaîne normale à facteurs abélien. Ceci prouve que G' est résoluble.

Corollaire Tout groupe quotient d'un groupe résoluble est un groupe résoluble.

Démonstration En effet, un groupe quotient de G est une image homomorphe de G par la surjection canonique.

Théorème Si $f;G \longrightarrow G'$ est un homomorphisme injectif et si G' est résoluble, alors G est résoluble.

Démonstration Si G' est résoluble, alors il possède une chaîne normale

$$\left\{e'\right\} = H_0' \subseteq H_1' \subseteq \cdots \subseteq H_n' = G'$$

à facteurs abéliens. La chaîne

$$\{e\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = G$$

où $H_i = f^{-1}(H_i')$ pour $i = 0,1,...,n$ est une chaîne normale et il existe homomorphisme injectif $v_i;H_{i+1}/H_i \longrightarrow H_{i+1}'/H_i'$. Il en résulte que les facteurs de la chaîne de G sont

tous abéliens, ce qui prouve que G est résoluble.

Corollaire Tout sous-groupe K d'un groupe résoluble est un groupe résoluble.

Démonstration Il suffit d'appliquer le théorème précédent à l'injection canonique.

Théorème Si G possède une chaîne normale dont les facteurs sont des groupes résolubles, alors G est résoluble.

Démonstration Soit

$$\{e\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = G$$

une chaîne normale de G telle que tous les facteurs $F_i = H_{i+1}/H_i$ sont résolubles. Nous avons démontré que l'on peut utiliser ces chaînes normales des facteurs pour construire une chaîne normale de G dont les facteurs sont isomorphes aux facteurs des différentes chaînes normales des facteurs. Mais les chaînes des F_i peuvent être choisies à facteurs abéliens, il en résulte que les facteurs de la chaîne concaténée sont tous abéliens et G est résoluble.

Théorème Soit H un sous-groupe distingué de G. G est résoluble si, et seulement si, H et G/H sont résolubles.

Démonstration Si G est résoluble, alors H et G/H sont résolubles comme nous l'avons vu. Réciproquement, si H et G/H sont résolubles, alors

$$\{e\} \subseteq H \subseteq G$$

est une chaîne normale de G dont les facteurs $F_1 = H/\{e\} \approx H$ et $F_2 = G/H$ sont résolubles. Il en résulte que G est résoluble.

Dans la suite, nous allons prouver que G est résoluble si, et seulement si, G possède une chaîne normale dont les facteurs sont des groupes cycliques d'ordres premiers. Il est clair que si G satisfait cette condition, alors G est résoluble. Pour démontrer la réciproque, nous démontrons les théorèmes préliminaires suivants :

Théorème Si p est un facteur premier de l'ordre d'un groupe cyclique fini G, alors G possède un élément d'ordre p.

Démonstration Si a est un générateur de G, alors l'élément $b = a^{\frac{n}{p}}$ est d'ordre p, car $b^p = e$ et p est premier.

Théorème Si p est un facteur premier de l'ordre d'un groupe abélien fini G, alors G possède un élément d'ordre p.

Démonstration Par récurrence sur l'ordre n de G. Si $n = 1$, le théorème est vrai. Supposons le théorème vrai pour tous les groupes finis d'ordre $< n$ et démontrons-le pour les groupes finis d'ordre n. Soit G un tel groupe. Si G est cyclique, alors on

est ramené au théorème précédent. Sinon, G possède un élément h d'ordre m tel que $1 < m < n$. Soit $H = gr(h)$ le sous groupe de G engendré par h. Le groupe quotient G/H est d'un ordre $< n$. Deux cas sont possibles :

1. p divise m : dans ce cas, p divise l'ordre du groupe H qui est d'ordre $m < n$. Ainsi H contient un élément d'ordre p.
2. p ne divise pas m : p divise l'ordre de G/H car $n = m \times ord(G/H)$ et p est premier. Il existe $\overline{y} \in G/H$ d'ordre p. L'élément $x = y^m$ vérife $x \neq e$ (sinon $\overline{y}^m = \overline{e}$ et p divise $m = Ord(\overline{y})$) et $x^p = (y^m)^p = (y^p)^m = e$ car $y^p \in H$ ($\overline{y}^p = \overline{e}$) et m est l'ordre de H. On en déduit que p est l'ordre de x car p est premier.

Corollaire Si G est un groupe abélien fini d'ordre non premier, alors G possède un sous-groupe propre(c.a.d distint de $\{e\}$ et G.

Démonstration Si p est un facteur premier de l'ordre de G, alors G possède un élément d'ordre p. Le sous-groupe $H = gr(a)$ qui est le sous groupe de G engendré par a est un sous-groupe propre de G.

Théorème Si G est un groupe résoluble, alors G possède une chaîne normale dont les facteurs sont des groupes cycliques d'ordres premiers.

Démonstration Soit

$$\{e\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = G$$

une chaîne normale à facteurs abéliens. Nous supposons que cette chaîne est la plus longue des chaînes normales de G à facteurs abéliens. Si un facteur F_i n'était pas un groupe cyclique d'ordre premier, alors F_i possède un sous-groupe propre et G possède un sous-groupe H tel que $H_i \subseteq H \subseteq H_{i+1}$. H est distingué dans H_{i+1}, car si $x \in H_{i+1}$ et $y \in H$, alors $\overline{x}^{-1}\overline{yx} = \overline{y}$ (F_i est abélien). Il en résulte $x^{-1}yxy^{-1} \in H_i \subseteq H$ et $x^{-1}yx = \left(x^{-1}yxy^{-1}\right)y \in H$. D'un autre côté, H/H_i est abélien (sous-groupe de F_i) et H_{i+1}/H est abélien car nous avons

$$H_{i+1}/H \simeq (H_{i+1}/H_i)/(H/H_i)$$

et $(H_{i+1}/H_i)/(H/H_i)$ est abélien car c'est un quotient du groupe abélien F_i. Ainsi, si nous insérons H entre H_i et H_{i+1} nous obtenons une chaîne normale à facteurs abéliens plus longue que la plus longue des telles chaînes.

4 Groupe dérivé

Définition Soit G un groupe distinct de $\{e\}$. Pour tout $(a,b) \in G \times G$, l'élément $a^{-1}b^{-1}ab$ sera noté $[a,b]$ et appelé le **commutateur** de a et b.

Théorème Les propriétés suivantes sont vraies :

1. $[G$ est abélien$] \Longleftrightarrow [[a,b] = e$ pour tout $(a,b) \in G \times G]$.
2. L'inverse d'un commutateur est un commutateur.
3. Si c est un commutateur, alors $x^{-1}cx$ est un commutateur pour tout $x \in G$.

Démonstration Ces propriétés sont faciles à vérifier.

Définition Le sous-groupe de G engendré par tous les commutateurs $[a,b]$, $(a,b) \in G \times G$, sera appelé **groupe dérivé** du groupe G. Il sera noté G'.

Théorème Le groupe dérivé G' de G est l'ensemble des produits finis de commutateurs.

Démonstration Soit H l'ensemble des produits finis de commutateurs. H est un sous-groupe de G et il contient tous les commutateurs. Il est le plus petit sous-groupe de G qui contient tous les commutateurs car si un sous-groupe K de G contient tous les commutateurs, alors K contient tous les produits finie de commutateurs. Ainsi $H \subseteq K$ et $H = G'$.

Théorème Le groupe dérivé G' de G est un sous-groupe distingué de G.

Démonstration Car, si $y \in G'$, alors y est un produit fini de commutateurs, soit $y = c_1 \cdots c_t$. Il en résulte

$$x^{-1}yx = x^{-1}c_1 \cdots c_t x = \left(x^{-1}c_1x\right)\left(x^{-1}c_2x\right) \cdots \left(x^{-1}c_tx\right) \in G'$$

car le conjugué d'un commutateur est un commutateur.

Théorème Si H est un sous-groupe distingué de G, alors G/H est abélien si, et seulement si, $G' \subseteq H$.

Démonstration Si $c = a^{-1}b^{-1}ab$ est un commutateur, alors

$$\overline{c} = \overline{a^{-1}b^{-1}}\overline{a}\overline{b} = \overline{a}^{-1}\overline{b}^{-1}\overline{a}\overline{b} = \overline{e}.$$

Il en résulte $c \in H$ qui prouve $G' \subseteq H$. Réciproquement, si $G' \subseteq H$, alors nous avons pour tout $\left(\overline{a},\overline{b}\right) \in G/H \times G/H$

$$\overline{a}^{-1}\overline{b}^{-1}\overline{a}\overline{b} = \overline{a^{-1}b^{-1}}\overline{a}\overline{b} = \overline{a^{-1}b^{-1}ab} = \overline{e}$$

et par suite G/H est abélien.

Corollaire Soit G' le groupe dérivé du goupe G. G/G' est abélien.

Définition On définit, par récurrence, le **groupe dérivé d'ordre** i comme étant le groupe dérivé du groupe $G^{(i-1)}$: $G^{(i)} = \left(G^{(i-1)}\right)'$. On définit $G^{(0)}$ comme étant le groupe G.

Nous avons :

Théorème Si G est un groupe résoluble, et si

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{e\}$$

est une chaîne normale à facteurs abéliens, alors $G^{(i)} \subseteq G_i$ pour $i = 0,1,...,n$.

Démonstration Par récurrence . Si $i = 0$, nous avons $G_0 = G = G^{(0)}$. Supposons avoir $G^{(i)} \subseteq G_i$. Nous avons $G^{(i+1)} = \left(G^{(i)}\right)' \subseteq G_i'$. Comme G_i/G_{i+1} est abélien, on a $G_i' \subseteq G_{i+1}$ et par suite

$$G^{(i+1)} = \left(G^{(i)}\right)' \subseteq G_i' \subseteq G_{i+1}.$$

Théorème G est résoluble si, et seulement si, $G^{(n)} = \{e\}$ pour certains n.

Démonstration Si G est résoluble et si

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{e\}$$

est une chaîne normale à facteurs abéliens, alors $G^{(n)} \subseteq G_n = \{e\}$, d'où $G^{(n)} = \{e\}$. Réciproquement, si $G^{(n)} = \{e\}$ pour un entier naturel n, alors la chaîne

$$G = G^{(0)} \supseteq G' = G^{(1)} \supseteq \cdots \supseteq G^{(n)} = \{e\}$$

est une chaîne normale à facteurs abéliens car $G^{(i)}/G^{(i+1)}$ est abélien car $G^{(i+1)} = \left(G^{(i)}\right)'$. Ainsi G est résoluble.

Théorème Le groupe alterné A_n n'est pas résoluble pour $n \geq 5$.

Démonstration Nous allons démontrer que A_n' contient tous les cycles de longueur 3. Si (abc) est un tel cycle, alors

$$(abc) = (adc)(bec)(acd)(bce) = (acd)^{-1}(bce)^{-1}(acd)(bce) \in A_n'$$

où d et e des éléments distincts et distinct de a,b,c ($n \geq 5$). Il en résulte que A_n, engendré par les cycles de longueur 3, est égal à son groupe dérivé A_n'. Ceci prouve que A_n n'est pas résoluble pour $n \geq 5$, car son groupe dérivé de n'importe quel ordre est distinct de $\{i\}$.

Corollaire Le groupe symétrique S_n n'est pas résoluble pour $n \geq 5$.

Démonstration Sinon, A_n serait résoluble.

Théorème Le groupe symétrique S_n est résoluble pour $n \in \{1,2,3,4\}$.

Démonstration Ceci est claire pour $n = 1,2,3$. Pour $n = 4$, nous avons la chaîne

$$\{i\} \subseteq W \subseteq V \subseteq A_4 \subseteq S_4$$

où V est le groupe

$$V = \{i, (12)(34), (13)(24), (14)(23)\}$$

et W est un sous-groupe d'ordre 2 de V. Cette chaîne est normale. La seule vérification à faire est que V est un sous-groupe distingué de A_4. Mais V est distingué dans S_4. Ainsi la chaîne est normale. Les facteurs sont tous d'ordre 2 ou 3, ils sont abéliens. Il en résulte que S_4 est résoluble.