Chapitre 1

Groupes et actions de groupes

1.1 Rappels

1.1.1. Un *groupe* est la donnée d'un ensemble G muni d'une application notée $(x, y) \to xy$ de $G \times G$ vers G vérifiant les trois axiomes suivants :

(a) associativité : $(xy)z = x(yz)$ pour tous $x, y, z \in G$;

(b) élément neutre : il existe $1 \in G$ tel que $1x = x1 = x$ pour tout $x \in G$;

(c) inverse : pour tout $x \in G$, il existe $x^{-1} \in G$ tel que $xx^{-1} = x^{-1}x = 1$.

On dit que le groupe est *commutatif*, si $xy = yx$ pour tous $x, y \in G$.

Un *sous-groupe* de G est une partie $H \subset G$ telle que *(a)* pour tous $x, y \in H$, $xy \in H$, *(b)* $1 \in H$, et *(c)* pour tout $x \in H$, $x^{-1} \in H$.

1.1.2. Soient G, G' deux groupes. Un *homomorphisme* de G vers G' est une fonction $\varphi : G \to G'$ telle que $\varphi(x, y) = \varphi(x)\varphi(y)$ pour tous $x, y \in G$. Il est clair que la composée de deux homomorphismes est encore un homomorphisme. Un peu moins évidente est la proposition suivante :

1.1.3 Proposition. — *Soit $\varphi : G \to G'$ un homomorphisme* bijectif. *Alors φ^{-1} est encore un homomorphisme, de G' vers G.*

Démonstration. — Laissée au lecteur.

1.1.4. On notera $\mathrm{Hom}\,(G, G')$ l'ensemble des homomorphismes de G vers G' ; on notera que $\mathrm{Hom}\,(G, G')$ n'est jamais vide, puisqu'il contient toujours l'homomorphisme *trivial* φ défini par $\varphi(x) = 1$ pour tout $x \in G$. Un homomorphisme bijectif sera appelé *isomorphisme* de G sur G'.

Pour tout groupe G, on note $\mathrm{Aut}\,(G)$ l'ensemble des isomorphismes de G vers lui-même ; il résulte de la proposition 1.1.3 que $\mathrm{Aut}\,(G)$ est à nouveau un groupe, appelé *groupe des automorphismes* de G.

1.1.5 Exemples. — *(a)* Soit G un groupe, et soit $x \in G$. On définit une fonction $\varphi_x : \mathbf{Z} \to G$ par la formule

$$\varphi_x(n) = \begin{cases} x \dots x \quad (n \text{ fois}) & \text{si } n > 0 \\ 1 & \text{si } n = 0 \\ x^{-1} \dots x^{-1} \quad (|n| \text{ fois}) & \text{si } n < 0 \end{cases} \tag{1.1}$$

Alors on vérifie facilement que φ_x est un homomorphisme du groupe additif $(\mathbf{Z}, +)$ vers G ; on notera souvent x^n au lieu de $\varphi_x(n)$.

(b) Soit G un groupe. Pour tout $g \in G$ fixé, on définit $\gamma_g : G \to G$ par $\gamma_g(x) = gxg^{-1}$. Alors on vérifie facilement que $\gamma_g \in \mathrm{Aut}\,(G)$; on dit que γ_g est l'*automorphisme intérieur* de G défini par g. De plus, il est facile de vérifier que l'application $g \to \gamma_g$ est un *homomorphisme* de G vers $\mathrm{Aut}\,(G)$.

On dit qu'un sous-groupe N de G est *distingué*, si $\gamma_g(N) \subset N$ pour tout $g \in G$ (on a alors en fait $\gamma_g(N) = N$ pour tout $g \in G$.)

1.1.6 Proposition. — *Soient G, G' deux groupes, $\varphi \in \mathrm{Hom}\,(G, G')$.*

(i) $\mathrm{Im}\,\varphi$ *est un sous-groupe de* G'.
(ii) $\mathrm{Ker}\,\varphi := \{x \in G \mid \varphi(x) = 1\}$ *est un sous-groupe distingué de* G.
(iii) φ *est injective si et seulement si* $\mathrm{Ker}\,\varphi = \{1\}$.

Démonstration. — Laissée au lecteur.

1.1.7 Définition. — (sous-groupe engendré) Soit G un groupe, et soit S une partie de G. Ordonnons l'ensemble des sous-groupes de G par l'inclusion. Alors il existe un plus petit sous-groupe $\langle S \rangle$ de G, nécessairement unique, contenant S ; on dit que c'est le sous-groupe de G *engendré* par S. On peut le décrire de deux façons :

(a) $\langle S \rangle$ est l'intersection de tous les sous-groupes de G contenant S ;
(b) $\langle S \rangle$ est l'ensemble des produits finis $x_1 \dots x_s$, $s \in \mathbf{N}$ (nous ferons toujours la convention que le produit vide, correspondant à $s = 0$, est égal à 1), où $x_1, \dots, x_s$ appartiennent à $S \cup S^{-1}$.

En effet, il est clair que l'intersection d'une famille de sous-groupes de G est encore un sous-groupe de G, d'où la caractérisation *(a)*. D'autre part, soit $H = \{x_1 \dots x_s\}$, $s \in \mathbf{N}$, $x_1, \dots, x_j \in S \cup S^{-1}$. Clairement, $1 \in H$, et H est stable par produit ; comme $(x_1 \dots x_s)^{-1} = x_s^{-1} \dots x_1^{-1}$, H est également stable par prise d'inverses. Donc H est un sous-groupe de G contenant S, d'où $\langle S \rangle \subset H$; mais clairement tout sous-groupe de G contenant S contient S^{-1} et tous les produits finis $x_1 \dots x_s$, donc on a $H \subset \langle S \rangle$, et $H = \langle S \rangle$.

1.1.8 Exemple. — Soit $x \in G$. Alors $\langle x \rangle = \{x^n\}_{n \in \mathbf{Z}} = \mathrm{Im}\,\varphi_x$; en particulier, $\langle x \rangle$ est un sous-groupe *commutatif* de G. Deux cas se présentent :

(a) φ_x est injective ; alors $\langle x \rangle \simeq \mathbf{Z}$, et on dit que x est d'ordre infini.

(b) φ_x n'est pas injective. Alors si $N \subset \mathbf{Z}$ est le noyau de φ_x, on sait qu'il existe un unique $d > 0$ tel que $N = d\,\mathbf{Z}$. Donc $x^n = x^m$ si et seulement si n et m ont même reste modulo d, et $\langle x \rangle$ s'identifie au groupe additif $\mathbf{Z}/d\mathbf{Z}$; l'entier d est aussi le plus petit $n > 0$ tel que $x^n = 1$, et on dit que c'est l'*ordre* de x dans G.

1.2 Ensembles quotient

1.2.1. Soit X un ensemble. On appelle *relation* sur X toute partie de $X \times X$, ou de façon équivalente, toute fonction R de $X \times X$ vers $\{0,1\} = \{\text{faux}, \text{vrai}\}$. On notera xRy pour exprimer que $R(x,y) = \text{vrai}$. Souvent aussi on associe à R un symbole tel que $\equiv$, $\sim$, ou $\sim_R$ s'il faut préciser R, ou encore $\leq$, $\leq_R$ (le choix du symbole sera guidé par les propriétés attendues de la relation). Si par exemple le symbole choisi est $\sim$, on notera $x \sim y$ au lieu de xRy .

1.2.2 Définition. — On appelle *relation d'équivalence* sur X toute relation $\sim$ telle que :

(a) $x \sim x$ pour tout $x \in X$ (réflexivité) ;
(b) $x \sim y$ implique $y \sim x$ (symétrie) ;
(c) $x \sim y$ et $y \sim z$ impliquent $x \sim z$ (transitivité).

1.2.3 Exemples. — *(a)* Sur tout ensemble X, l'égalité est une relation d'équivalence.
(b) Fixons un entier $d > 0$, et notons $\sim$ la relation sur $\mathbf{Z}$ définie par $x \sim y$ si et seulement si d divise $x - y$. Alors on vérifie aussitôt que $\sim$ est une relation d'équivalence, dite relation de congruence modulo d.
(c) Soient X et X' deux ensembles, $f : X \to X'$ une fonction. Alors la relation $\sim$ sur X définie par $x \sim y$ si et seulement si $f(x) = f(y)$ est une relation d'équivalence.

1.2.4. Une *partition* de X est une famille $\mathcal{P}$ de parties deux à deux disjointes de X de réunion égale à X. En d'autres termes, on a :

(a) $Y, Y' \in \mathcal{P}$ et $Y \cap Y' \neq \emptyset$ impliquent $Y = Y'$;
(b) $\bigcup_{Y \in \mathcal{P}} Y = X$.

On ecrit alors $X = \coprod_{Y \in \mathcal{P}} Y$. Si $\emptyset \notin \mathcal{P}$, on dit que $\mathcal{P}$ est une partition de X en parties non-vides. Remarquons que suivant cette définition, l'ensemble vide possède exactement deux partitions : la famille vide, et la famille réduite à l'ensemble vide ; et exactement une partition en parties non-vides, la famille vide.

1.2.5 Théorème. — *(équivalence entre relations d'équivalence et partitions) (i) Soit X un ensemble, $\sim$ une relation d'équivalence sur X. Pour tout $x \in X$, notons $\pi(x) = \{y \in X \mid x \sim y\}$, et disons que $\pi(x)$ est la* classe d'équivalence *de x modulo $\sim$. Alors les classes d'équivalence forment une partition de X en parties non-vides, et l'on a $x \sim y$ si et seulement si $\pi(x) = \pi(y)$.*

(ii) Réciproquement, soit $\mathcal{P}$ une partition de X en parties non-vides. Pour tout $x \in X$, notons $\pi(x)$ l'unique $Y \in \mathcal{P}$ tel que $x \in Y$, et notons $\sim$ la relation sur X définie par

$x \sim y$ si et seulement si $\pi(x) = \pi(y)$. Alors $\sim$ est une relation d'équivalence, et pour tout $x \in X$, la classe d'équivalence de x est $\pi(x)$.

Démonstration. — *(i)* Soit $y \in \pi(x)$, et montrons que $\pi(y) = \pi(x)$. Pour toute $z \in \pi(y)$, on a $y \sim z$, donc $x \sim z$ par transitivité de $\sim$, et $z \in \pi(x)$. Ainsi, $\pi(y) \subset \pi(x)$; mais comme on a aussi $y \sim x$ par symétrie de $\sim$, on peut échanger les rôles de x et y et conclure que $\pi(x) \subset \pi(y)$, d'où l'égalité. Ceci prouve déjà que $x \sim y$ si et seulement si $\pi(x) = \pi(y)$. Supposons maintenant que $\pi(x) \cap \pi(y) \neq \emptyset$, et soit $z \in \pi(x) \cap \pi(y)$. Alors $\pi(x) = \pi(z)$ d'après ce qui précède, et de même $\pi(y) = \pi(z)$; donc $\pi(x) = \pi(y)$, ce qui prouve que les classes d'équivalence forment bien une partition.

(ii) Evident.

1.2.6 Remarque. — Il est clair d'après le théorème que les deux constructions qui à une relation d'équivalence associent l'ensemble de ses classes d'équivalence, et à une partition la relation $\pi(x) = \pi(y)$, sont des bijections réciproques l'une de l'autre de l'ensemble des relations d'équivalence sur X, sur l'ensemble des partitions de X en parties non-vides. De plus, le théorème montre en passant que *toutes* les relations d'équivalence sur X peuvent être obtenues par la construction de l'exemple 1.2.3*(c)*, avec $X' = \mathcal{P}(X)$.

1.2.7. Soit $\sim$ une relation d'équivalence sur X. On note alors $X/\sim$ l'ensemble des classes d'équivalence modulo $\sim$, et on dit que $X/\sim$ est l'*ensemble quotient* de X par la relation $\sim$. La surjection $\pi : X \to X/\sim$ est appelée *surjection canonique* (ou parfois projection canonique) de X sur $X/\sim$. Les classes d'équivalence sont aussi appelées les *fibres* de la surjection canonique π ; cette terminologie est d'ailleurs utilisée pour toutes les surjections $f : X \to X'$: les fibres de f sont les $f^{-1}(y)$, $y \in X'$.

1.2.8 Proposition. — *(propriété universelle des quotients) Soient X, X' deux ensembles, $f : X \to X'$ une fonction, $\sim$ une relation d'équivalence sur X. Alors il existe une fonction $\overline{f} : X/\sim \to X'$ telle que $f = \overline{f} \circ \pi$, si et seulement si f est constante sur chaque classe d'équivalence. La fonction $\overline{f}$ est alors unique ; on dit que c'est la fonction définie par f par passage au quotient.*

Démonstration. — Supposons que $\overline{f}$ existe ; alors pour tout $x \in X$ on a :

$$\overline{f}(\pi(x)) = f(x) \qquad (*)$$

ce qui prouve que $\overline{f}$ est entièrement déterminée, d'où l'unicité de $\overline{f}$ sous réserve d'existence. De plus, f est alors constante sur chaque classe d'équivalence, puisque π l'est. Pour que la formule $(*)$ soit une définition correcte de $\overline{f}(\pi(x))$, il faut prouver que le membre de droite ne dépend que de la *classe* de x ; mais c'est évidemment le cas lorsque f est constante sur chaque classe.

1.2.9 Remarque. — En pratique, il faut éviter de penser à $X/\sim$ comme à un ensemble de parties de X. Il faut plutôt considérer les éléments de $X/\sim$ comme les points d'un nouvel ensemble dont la nature importe peu ; ce qui compte, c'est la surjection $\pi : X \to X/\sim$ dont les fibres sont les classes d'équivalence. D'ailleurs, si $f : X \to X'$ est

n'importe quelle autre surjection avec cette propriété, l'application $\overline{f} : X/\sim \to X'$ définie par f par passage au quotient est *bijective* ; cela permet d'identifier $X/\sim$ et X'. Ceci permet souvent de donner des réalisations concrètes d'ensembles quotient. Nous nous astreindrons par la suite à utiliser uniquement la surjection π, et non pas la réalisation explicite de $X/\sim$ en termes de parties de X.

1.2.10 Exemple. — Définissons une relation d'équivalence $\sim$ sur $\mathbf{R}$ par $x \sim y$ si et seulement si $x-y \in 2\pi\mathbf{Z}$; l'ensemble quotient est noté $\mathbf{R}/2\pi\mathbf{Z}$ (cet ensemble se rencontre fréquemment dans la théorie des séries de Fourier ; on peut d'ailleurs remarquer qu'une fonction $f : \mathbf{R} \to \mathbf{C}$ est périodique de période 2π si et seulement si elle passe au quotient par $\sim$ au sens de la proposition 1.2.8). Alors la fonction $x \to e^{ix}$ est une surjection de $\mathbf{R}$ vers le cercle unité $\mathbf{U} \subset \mathbf{C}$, dont les fibres sont exactement les classes d'équivalence de $\sim$; ceci donne l'identification habituelle entre $\mathbf{R}/2\pi\mathbf{Z}$ et $\mathbf{U}$.

1.3 Actions de groupes

1.3.1 Définition. — Soient G un groupe, X un ensemble. Une *action* (à gauche) de G sur X est la donnée d'une fonction $\alpha : G \times X \to X$, notée en général $(g, x) \to gx$, telle que :

(a) $(gh)x = g(hx)$ pour tous $g, h \in G$, $x \in X$;
(b) $1x = x$ pour tout $x \in X$.

Nous appellerons *G-ensemble* tout ensemble muni d'une action de G.

1.3.2 Remarques. — *(a)* On définirait de même la notion d'action *à droite* : c'est la donnée d'une fonction $(x, g) \to xg$ de $X \times G$ vers G telle que $x(gh) = (xg)h$ pour tous $x \in X$ et $g, h \in G$ et $x1 = x$ pour tous $x \in X$. Mais si l'on s'est donné une action à droite, on en déduit une action *à gauche* de G sur X en posant $\alpha(g, x) = xg^{-1}$; cela permet de ramener l'étude des actions à droite à celle des actions à gauche (et réciproquement). Donc, chaque résultat que nous démontrerons sur les actions à gauche aura un analogue pour les actions à droite, dont nous laisserons l'explicitation au lecteur. Bien entendu, en pratique il ne faut pas hésiter à écrire les actions du côté où cela semble le plus naturel.

Si le groupe G est commutatif, c'est encore plus simple : dans ce cas, toute action à droite *est* aussi directement une action à gauche, sans qu'il soit nécessaire d'introduire d'inverses. Pour un groupe non commutatif, les deux notions sont distinctes.

(b) La donnée d'une action de G sur X est équivalente à la donnée d'un homomorphisme $g \to \alpha_g$ de G vers $\mathfrak{S}_X$ (groupe des bijections de l'ensemble X vers lui-même) (exercice : le vérifier).

(c) Il arrive souvent que l'ensemble X porte une structure supplémentaire, et que les α_g soient des isomorphismes pour cette structure (par exemple : X est un groupe, et les α_g sont dans $\mathrm{Aut}\,(X)$; X est un espace vectoriel sur un corps k, et les α_g sont dans $\mathbf{GL}(X)$; X est un espace topologique et les α_g sont des homéomorphismes, ...) ; on parlera alors d'action de G sur X *par automorphismes de groupes*, ou *par applications linéaires*, ou *par homéomorphismes*, ...

1.3.3 Exemples. — Ils abondent :

(a) Pour tout groupe G, on définit trois actions de G sur lui-même : l'action *régulière gauche* σ définie par $\sigma(g,x) = gx$; l'action *régulière droite* τ définie par $\tau(x,g) = xg$ (attention ! elle est écrite ici comme action à droite) ; et l'action *par conjugaison* γ définie par $\gamma(g,x) = gxg^{-1}$. L'action γ est particulièrement riche, car c'est une action par automorphismes de groupes.

(b) Le groupe $\mathfrak{S}_n$ des bijections de l'ensemble $X = \{1,\dots,n\}$ agit évidemment sur X, mais aussi sur tous les ensembles déduits de X de façon "ensembliste" : les puissances X^m, $m \in \mathbf{N}$; l'ensemble $\mathcal{P}(X)$ des parties de X ; l'ensemble $\mathcal{F}(X,X)$ des fonctions de X vers lui-même ; l'ensemble des partitions de X ; l'ensemble des recouvrements de X ; ... De plus, ces actions préservent les notions ensemblistes comme l'appartenance, l'inclusion, la complémentation, etc., au sens ou par exemple $gx \in gA$ si $x \in A$; il est essentiel de s'entraîner à reconnaître ces phénomènes de "transport de structure".

(c) De même, l'action de G sur lui-même par conjugaison définit des actions sur tous les ensembles définis à partir de G de façon "groupiste" : par exemple, l'ensemble des sous-groupes de G, l'ensemble des parties génératrices de G, l'ensemble des éléments d'ordre m de G (m entier ≥ 1), ...

(d) Soit k un corps commutatif, et soit V un k-espace vectoriel de dimension finie n. Alors le groupe $\mathbf{GL}(V)$ agit sur V, mais aussi sur les bases de V, sur les sous-espaces vectoriels de V, sur les endomorphismes de V, sur le dual V^*, ...

(e) On peut définir une action de tout groupe G sur tout ensemble X en posant $gx = x$ pour tous $g \in G$, $x \in X$; cette action (*a priori* pas très intéressante) est appelée *triviale*. Elle n'est pourtant pas sans importance ; d'ailleurs, il y a des cas où c'est la seule action possible.

(f) Soient X et Y deux G-ensembles. On définit alors une action de G sur l'ensemble $\mathcal{F}(X,Y)$ de toutes les fonctions de X vers Y en posant $(gf)(x) = g.f(g^{-1}x)$. C'est comme cas particulier de cette définition que sont définies les actions de $\mathbf{GL}(V)$ sur $\mathrm{End}\,(V)$ et sur V^* dans *(d)* : on a $(gu)(x) = g.u(g^{-1}x) = (g \circ u \circ g^{-1})(x)$ pour $u \in \mathrm{End}\,(V)$, et $(g\lambda)(x) = \lambda(g^{-1}x)$ pour tout $\lambda \in V^*$; dans ce dernier cas, on a donc fait agir trivialement le groupe G sur k.

1.3.4 Définition. — Soient X, X' deux G-ensembles. On appelle *G-morphisme* (ou parfois *entrelacement*) de X vers X' toute fonction $\varphi : X \to X'$ telle que $\varphi(gx) = g\varphi(x)$ pour tous $g \in G$, $x \in X$. On note $\mathrm{Hom}_G(X,X')$ l'ensemble des G-morphismes de X vers X'.

1.3.5 Exemple. — Soit X un G-ensemble, et soit $x \in X$. Pour tout $g \in G$, on pose $\varphi_x(g) = gx$; alors on vérifie immédiatement que φ_x est un G-morphisme de (G,σ) vers X. On démontre d'ailleurs facilement que toute $\varphi \in \mathrm{Hom}_G((G,\sigma),X)$ est entièrement déterminée par la donnée de $\varphi(1)$, et que φ_x est donc le seul $\varphi \in \mathrm{Hom}_G((G,\sigma),X)$ tel que $\varphi(1) = x$.

1.3.6 Définition. — Soit X un G-ensemble.

(a) Pour tout $x \in X$, on pose $G_x := \{g \in G \mid gx = x\}$; on dit que G_x est le *stabilisateur* de x dans G.

(b) Pour tout $x \in X$, on pose $Gx := \{gx, g \in G\}$; on dit que Gx est l'*orbite* de x sous G (on trouve aussi des notations telles que $\mathcal{O}_x$, C_x, etc.).

(c) On dit qu'une partie $Y \subset X$ est *stable* sous l'action de G, si $gy \in Y$ pour tous $g \in G$, $y \in Y$.

(d) On dit que $x \in X$ est *point fixe* pour l'action de G, si $gx = x$ pour tout $g \in G$; cela équivaut à $G_x = G$, et aussi à $Gx = \{x\}$. On note X^G l'ensemble des points fixes de X pour G.

1.3.7 Proposition. — *Soit X un G-ensemble. Alors les orbites de G dans X forment une* partition *de X. On note X/G l'ensemble quotient correspondant (*i.e. *l'ensemble des orbites de G dans X).*

Démonstration. — Il suffit de prouver que la relation $\sim$ sur X définie par $x \sim y$ si et seulement si $y \in Gx$ est une relation d'équivalence ; en effet, il est clair que les G-orbites sont alors les classes d'équivalence pour cette relation. Or il est clair que $x = 1.x \in Gx$, donc $\sim$ est réflexive ; si $y = gx \in Gx$, on a $x = g^{-1}y \in Gy$, donc $\sim$ est symétrique ; enfin si $y = gx \in Gx$ et $z = hy \in Gy$, on a $z = hgx \in Gx$, donc $\sim$ est transitive.

1.3.8 Exemples. — *(a)* Soit $G = \mathfrak{S}_n$, $X = \{1, \ldots, n\}$. Alors $Gx = X$ pour tout $x \in X$, et G_x est isomorphe à $\mathfrak{S}_{n-1}$ (exercice). Si on fait agir G sur $\mathcal{P}(X)$ (cf. ex. 1.3.3*(b)*), il y a $n+1$ orbites, définies par la cardinalité (exercice : le démontrer ; pouvez-vous décrire le stabilisateur de $Y \subset X$?)

(b) Soit V un k-espace vectoriel de dimension finie n, $G = \mathbf{GL}(V)$. Alors il y a deux orbites : $V \backslash \{0\}$, et $\{0\}$ (exercice).

(c) Soit G un groupe, et faisons agir G sur lui-même par conjugaison. Les orbites pour cette action s'appellent les *classes de conjugaison* de G. Le stabilisateur de $x \in G$ pour l'action par conjugaison s'appelle le *centralisateur* de x dans G, et se note $Z_G(x)$.

(d) De même, si on considère l'action de G sur l'ensemble de ses sous-groupes, déduite de l'action par conjugaison, le stabilisateur d'un sous-groupe H est appelé *normalisateur* de H dans G, et noté $N_G(H)$. Par définition, c'est l'ensemble des $g \in G$ tels que $gHg^{-1} = H$ (d'où la terminologie) ; il contient H comme sous-groupe distingué, et c'est le plus grand sous-groupe de G avec cette propriété. Un sous-groupe est point fixe pour cette action, si et seulement si c'est un sous-groupe distingué de G.

(e) Soient X, X' deux G-ensembles. Alors les points fixes de l'action de G sur $\mathcal{F}(X, X')$ définie en 1.3.3*(f)* sont exactement les G-morphismes de X vers X' (exercice).

1.3.9 Proposition. — *Soit X un G-ensemble, $x \in X$.*

(i) *G_x est un sous-groupe de G.*

(ii) *Pour tout $g \in G$, $G_{gx} = gG_xg^{-1}$; en particulier, les stabilisateurs des divers points d'une orbite sont tous conjugués entre eux.*

(iii) *Soit X' un autre G-ensemble, $\varphi \in \mathrm{Hom}_G(X, X')$. Alors $G_x \subset G_{\varphi(x)}$*

Démonstration. — Laissée au lecteur.

1.4 Quotient d'un groupe par un sous-groupe

1.4.1 Définition. — Soient G un groupe, H un sous-groupe de G, et soit $x \in G$. On appelle *classe à gauche* (resp. *classe à droite*) de x modulo H l'ensemble $xH \subset G$ (resp. $Hx \subset G$) ; ce sont aussi les orbites de x sous la restriction à H de l'action régulière droite (resp. gauche). On note G/H (resp. $H\backslash G$) l'ensemble des classes à gauche (resp. à droite) modulo H, et on dit que c'est le quotient de G par H à droite (resp. à gauche).

1.4.2 Proposition. — *Soient G et H comme dans la déf. 1.4.1. Les classes à gauche (resp. à droite) modulo H forment une partition de G en parties non-vides. La relation d'équivalence correspondante est donnée par $x \sim y$ si et seulement si $x^{-1}y \in H$ (resp. $yx^{-1} \in H$).*

Démonstration. — Laissée au lecteur.

1.4.3 Proposition. — *(cas d'un sous-groupe distingué) Soit G un groupe, H un sous-groupe de G. Les assertions suivantes sont équivalentes :*

(i) H est distingué dans G ;
(ii) les classes à gauche et les classes à droite définies par H sont les mêmes, i.e. *$xH = Hx$ pour tout $x \in G$;*
(iii) il existe une structure de groupe sur l'ensemble G/H telle que la surjection canonique $\pi : G \to G/H$ soit un homomorphisme.

La structure de groupe de (iii) est alors unique ; on dit que G/H muni de cette structure est le groupe quotient *de G par H.*

Démonstration. — *(i) $\Longrightarrow$ (ii)* C'est clair : comme H est distingué, on a $xHx^{-1} = H$ pour tout $x \in G$, donc $xH = Hx$.
(ii) $\Longrightarrow$ (iii) Supposons qu'il existe une structure de groupe sur G/H telle que π soit un homomorphisme. Alors pour tous $x, y \in G$, on a

$$\pi(x)\pi(y) = \pi(xy) \qquad (*)$$

ce qui prouve déjà l'unicité de la loi de groupe sous réserve d'existence, puisqu'il n'y a qu'une seule valeur possible pour $\pi(x)\pi(y)$. Pour que la formule $(*)$ puisse servir de *définition* de $\pi(x)\pi(y)$, il faut vérifier que si $x', y' \in G$ sont tels que $\pi(x') = \pi(x)$, $\pi(y') = \pi(y)$, alors on a $\pi(x'y') = \pi(xy)$. Or il existe alors $h, k \in H$ tels que $x' = xh$, $y' = yk$; et comme par hypothèse on a $Hy = yH$, on a aussi $h'(= y^{-1}hy) \in H$ tel que $hy = yh'$. Donc on peut écrire :

$$x'y' = xhyk = xy.h'k$$

ce qui prouve bien que $\pi(x'y')\pi(xy)$. Ainsi, sous l'hypothèse de *(ii)*, la formule $(*)$ définit de manière cohérente une loi de composition sur G/H ; la vérification de l'associativité de cette loi, du fait que $\pi(1)$ est élément neutre, et du fait que $\pi(x^{-1})$ est inverse de $\pi(x)$ pour tout $x \in G$, sont immédiates, car ces propriétés sont aussitôt "héritées" des propriétés analogues de la loi de groupe sur G.
(iii) $\Longrightarrow$ (i) C'est clair : s'il existe une loi de groupe comme en *(iii)*, on a $H = \pi^{-1}(\pi(1)) = \operatorname{Ker}\pi$, donc H est distingué d'après 1.1.6 *(ii)*.

1.4.4 Remarque. — On a ainsi une réciproque à la prop. 1.1.6 : *tout* sous-groupe distingué de G peut apparaître comme noyau d'un homomorphisme $\varphi : G \to G'$.

1.4.5 Exercice. — Soit G un groupe, et soit $\sim$ une relation d'équivalence sur G, *a priori* arbitraire. On suppose qu'il existe une structure de groupe sur $G/\sim$ telle que la surjection canonique $\pi : G \to G/\sim$ soit un homomorphisme. Montrer alors que $\sim$ est la relation définie par un sous-groupe distingué $N \subset G$.

1.4.6 Proposition. — *Soient G, G' deux groupes, $\varphi : G \to G'$ un homomorphisme ; soit N un sous-groupe distingué de G. Alors φ passe au quotient en une fonction $\overline{\varphi} : G/N \to G'$ si et seulement si $N \subset \operatorname{Ker}\varphi$; $\overline{\varphi}$ est alors un homomorphisme de groupes de G/N vers G', et $\operatorname{Ker}\overline{\varphi} = \pi(\operatorname{Ker}\varphi)$.*

Démonstration. — Si φ passe au quotient par N, elle est constante sur chaque classe modulo N ; en particulier, φ est constante sur $1.N = N$. Mais $1 \in N$ et $\varphi(1) = 1$, donc $f(x) = 1$ pour tout $x \in N$, ce qui prouve bien que $N \subset \operatorname{Ker}\varphi$. Réciproquement, si $N \subset \operatorname{Ker}\varphi$, on a $\varphi(xh) = \varphi(x)\varphi(h) = \varphi(x)$ pour tous $x \in G$ et $h \in N$, donc φ passe au quotient par N.

Il est immédiat de vérifier que $\overline{\varphi}$ est un homomorphisme de groupes. Soit $\pi(x) \in G/N$ tel que $\overline{\varphi}(\pi(x)) = 1$; comme $\overline{\varphi} \circ \pi = \varphi$, on a $\varphi(x) = 1$, donc $x \in \operatorname{Ker}\varphi$. Ainsi, le noyau de $\overline{\varphi}$ est l'image par π de $\operatorname{Ker}\varphi$.

1.4.7 Corollaire. — *Tout homomorphisme de groupes $G \to G'$ passe au quotient en un homomorphisme* injectif *$G/\operatorname{Ker}\varphi \to G'$ et en un isomorphisme $G/\operatorname{Ker}\varphi \to \operatorname{Im}\varphi$. En particulier, tout homomorphisme* surjectif *$\varphi : G \to G'$ passe au quotient en un isomorphisme $G/\operatorname{Ker}\varphi \simeq G'$.*

Démonstration. — C'est clair : si on prend $N = \operatorname{Ker}\varphi$, le noyau de $\overline{\varphi}$ est $\pi(N) = \{1\}$.

1.4.8 Exemple. — Si H est un sous-groupe *quelconque* de G, $\pi(H)$ s'identifie à $H/(H \cap N)$. En effet, on a $\operatorname{Ker}(\pi|_H) = \operatorname{Ker}\pi \cap H = N \cap H$, et on applique le corollaire.

1.5 Relèvements et produits semidirects

1.5.1. On va maintenant s'intéresser aux questions de relèvements de quotients. Soit G un groupe, et soit N un sous-groupe distingué de G. Appelons *supplémentaire* de N dans G tout sous-groupe H de G tel que *(a)* $N \cap H = \{1\}$ *(b)* N et H engendrent G.

1.5.2 Proposition. — *Soient G et N comme ci-dessus, et soit H un supplémentaire de N dans G. Alors l'application $(x, y) \to xy$ est une bijection de l'ensemble $N \times H$ vers G (en d'autres termes, tout élément $g \in G$ admet une* unique *écriture comme produit $g = xy$, $x \in N$, $y \in H$).*

Démonstration. — Tout d'abord, si $xy = x'y'$, avec $x, x' \in N$, $y, y' \in H$, on a aussi $x'^{-1}x = y'y^{-1} \in N \cap H$, donc $x'^{-1}x = y'y^{-1} = 1$, d'où $x = x'$ et $y = y'$. Ainsi, l'application $(x, y) \to xy$ est injective.

Pour montrer qu'elle est surjective, il suffira de montrer que l'ensemble K des produits xy, $x \in N$, $y \in H$, est un sous-groupe de G ; en effet, il est clair que K contient N et H, donc il contiendra alors le sous-groupe engendré par N et H, qui est G par hypothèse. Or, il est clair que $1 = 1.1$ appartient à K. Si xy et $x'y'$ sont dans K, on peut écrire $xyx'y' = xyx'y^{-1}.yy'$, et comme $xyx'y^{-1} \in N$, $yy' \in H$, on voit que $xyx'y'$ est bien de la forme voulue. De même on écrit : $y^{-1}x^{-1} = y^{-1}x^{-1}y.y^{-1}$, avec $y^{-1}x^{-1}y \in N$, $y^{-1} \in H$.

1.5.3 Proposition. — *Soit G un groupe, et soit N un sous-groupe distingué de G. Alors N possède un supplémentaire dans G si et seulement si il existe $\sigma \in \mathrm{Hom}\,(G/N, G)$ tel que $\pi \circ \sigma = \mathrm{Id}_{G/N}$. On dit que σ (ou parfois le sous-groupe $\sigma(G/N)$ de G) est un* relèvement *de G/N dans G.*

Démonstration. — Supposons que N posséde un supplémentaire H. Alors le noyau de $\pi|_H$ est $N \cap H = \{1\}$, donc π se restreint en une injection de H vers G/N. Mais si $g \in G$, et si l'on écrit $g = xy$, avec $x \in N$ et $y \in H$ comme à la prop. 1.5.2, on a $\pi(g) = \pi(x)\pi(y) = \pi(y)$, ce qui prouve que π est également surjective de H vers G/N. Donc $\pi|_H$ est un isomorphisme, et son inverse $\sigma = (\pi|_H)^{-1}$ vérifie $\pi \circ \sigma = \mathrm{Id}_{G/N}$.

Réciproquement, si σ existe, posons $H = \sigma(G/N)$, et montrons que H est un supplémentaire de N dans G. Si $x \in N \cap H$, on a $x = \sigma(z)$, avec $z \in G/N$. Mais alors $1 = \pi(x) = \pi(\sigma(z)) = z$, donc $z = 1$ et $x = \sigma(z) = 1$. D'autre part, si $g \in G$, posons $y = \sigma(\pi(g))$, et $x = gy^{-1}$. Alors $g = xy$, $y \in H$ par construction, et $\pi(x) = \pi(g)\pi(y)^{-1}$; mais $\pi(y) = (\pi \circ \sigma \circ \pi)(g) = \pi(g)$ puisque $\pi \circ \sigma = \mathrm{Id}_{G/N}$, donc $\pi(x) = 1$, et on a bien $NH = G$, donc *a fortiori* N et H engendrent G.

1.5.4 Exemple. — L'exemple le plus simple de sous-groupe distingué ne possédant pas de supplémentaire est obtenu en prenant pour G le groupe $\mathbf{Z}/4\mathbf{Z}$, et pour N l'unique sous-groupe d'ordre 2 de G, engendré par $\overline{2}$. Nous laisserons la démonstration en exercice (instructif !) au lecteur.

1.5.5. Définissons maintenant la notion abstraite de produit semidirect. Soient N et H deux groupes, et supposons donné un homomorphisme $y \to \tau_y$ de H vers $\mathrm{Aut}\,(N)$. On pose alors, pour (x, y) et (x', y') dans $N \times H$:

$$(x, y).(x', y') = (x\tau_y(x'), yy')$$

On vérifie facilement (exercice) que l'on obtient ainsi une loi de groupe sur l'ensemble $N \times H$, d'élément neutre $(1, 1)$. On note $N \rtimes H$ (ou $N \rtimes_\tau H$ s'il convient de préciser τ) ce groupe, et on dit que c'est le *produit semidirect* de N par H défini par τ.

L'ensemble des $(x, 1)$, $x \in N$, est un sous-groupe de $N \rtimes H$ isomorphe à N, et que nous identifierons à N ; de même, l'ensemble des $(1, y)$, $y \in H$, est un sous-groupe de $N \rtimes H$ identifié à H, et pour tous $x \in N$, $y \in H$ on a $(x, 1)(1, y) = (x, y)$. On vérifie facilement que le sous-groupe N est *distingué* dans $N \rtimes H$; de plus, un calcul élémentaire montre que $(1, y)(x, 1)(1, y)^{-1} = (\tau_y(x), 1)$, ce qui prouve que τ_y est la restriction à N de l'automorphisme intérieur $\gamma_{(1,y)}$.

Donc, si on note $G = N \rtimes H$, on voit que N est distingué dans G, et que H est un supplémentaire de N dans G. Réciproquement, si on se donne un groupe G, un sous-groupe distingué N de G et un supplémentaire H de N (supposé exister), les formules écrites dans la démonstration de la prop. 1.5.2 prouvent que G s'identifie au produit semidirect de N par H défini à l'aide de l'action adjointe de H sur N.

1.5.6. Parmi tous les produits semidirects possibles de N par H, il y en a un particulier : c'est celui correspondant à l'homomorphisme *trivial* de H vers $\mathrm{Aut}\,(N)$. On dit alors que le produit correspondant est le produit *direct* de N et H, et on le note $N \times H$. Dans ce cas, la formule du produit est simplement donnée par :

$$(x, y)(x', y') = (xx', yy')$$

pour tous $x, x' \in N$, $y, y' \in H$. On notera que dans ce cas, les sous-groupes N et H sont *tous deux* distingués dans $N \times H$: la symétrie est rétablie.

1.5.7 Exercice. — Montrer que si dans un produit semidirect $N \rtimes H$ les sous-groupes N et H sont tous deux distingués, alors le produit est direct.

1.5.8 Proposition. — *(propriété universelle du produit) Soient N, H, G' trois groupes, $\varphi \in \mathrm{Hom}\,(N, G')$, $\psi \in \mathrm{Hom}\,(H, G')$. Alors il existe un homomorphisme $\vartheta : N \times H \to G'$ tel que $\vartheta|_N = \varphi$, $\vartheta|_H = \psi$ si et seulement si $\varphi(x)\psi(y) = \psi(y)\varphi(x)$ pour tous $x \in N$, $y \in H$ (autrement dit, si et seulement si les deux sous-groupes $\varphi(N)$ et $\psi(H)$ de G' commutent entre eux) ; l'homomorphisme ϑ est alors unique.*

Démonstration. — Laissée au lecteur.

1.6 G-ensembles homogènes

1.6.1 Définition. — Soit X un G-ensemble. On dit que X est *homogène* sous l'action de G, ou encore que l'action de G sur X est *transitive*, si l'action de G dans X possède exactement une orbite (en particulier, X doit être non-vide).

1.6.2 Exemples. — *(a)* Nous avons vu que l'action de $\mathfrak{S}_n$ sur $X = \{1, \ldots, n\}$ est transitive ; de même, son action sur l'ensemble des parties $Y \subset X$ de cardinalité fixée est transitive.

(b) Pour tout groupe G, (G, σ) est un G-ensemble homogène.

(c) Soit $G = \mathbf{O}(n)$ le groupe des transformations orthogonales en dimension n. Alors la sphère unité de $\mathbf{R}^n$ est un G-ensemble homogène (dans ce cas, on parlera de G-*espace homogène*, car la topologie de la sphère, et même sa structure de sous-variété différentielle de $\mathbf{R}^n$, est préservée par l'action de G) ; si $n \geq 2$, c'est même un espace homogène sous l'action du groupe $\mathbf{SO}(n)$.

(d) Soit X un G-ensemble quelconque, et soit $x \in X$. Alors l'orbite Gx de x sous G est de manière évidente un G-ensemble homogène ; c'est d'ailleurs la plus petite partie G-stable de X contenant x. On voit donc qu'il y a abondance de G-ensembles homogènes.

1.6.3 Proposition. — *Soient X, X' deux G-ensembles homogènes.*

(i) Toute $\varphi \in \mathrm{Hom}_G(X, X')$ est surjective.

(ii) Soient $x \in X$, $x' \in X'$. Alors il existe $\varphi \in \mathrm{Hom}_G(X, X')$ telle que $\varphi(x) = x'$ si et seulement si $G_x \subset G_{x'}$; le morphsime φ est alors unique.

Démonstration. — *(i)* C'est évident : soit $x \in X$, et $y = \varphi(x)$. Si z est un autre point de X', il existe un $g \in G$ tel que $z = gy$; mais alors $z = \varphi(gx)$.
(ii) La nécessité provient de la prop. 1.3.9*(iii)*. Pour la suffisance, montrons que l'on peut définir $\varphi \in \mathrm{Hom}_G(X, X')$ en posant $\varphi(gx) = gx'$. Il s'agit de vérifier que si $gx = g'x$, alors $gx' = g'x'$; l'application φ sera alors correctement définie. Or si $gx = g'x$, on a $g^{-1}g'x = x$, donc $g^{-1}g' \in G_x$; puisque $G_x \subset G_{x'}$ par hypothèse, on a alors aussi $g^{-1}g'x' = x'$, donc $gx' = g'x'$. La vérification du fait que la fonction φ ainsi définie est un G-morphisme est immédiate, ainsi que l'unicité de φ, puisque si $y \in X$ on peut écrire $y = gx$, $g \in G$, d'où $\varphi(y) = g\varphi(x)$, ce qui prouve que la donnée de $\varphi(x)$ détermine entièrement φ.

1.6.4 Théorème. — *(i) Soit G un groupe, H un sous-groupe de G. Alors il existe une unique action de G sur G/H telle que la surjection canonique $\pi : (G, \sigma) \to G/H$ soit un G-morphisme. Pour cette action, G/H est un G-ensemble homogène.*
(ii) Réciproquement, soit X un G-ensemble homogène, et soit $x \in X$. Alors le G-morphisme canonique $\varphi_x : (G, \sigma) \to X$ passe au quotient en un isomorphisme $G/G_x \to X$.

Démonstration. — *(i)* Si l'action existe, on doit avoir

$$g\pi(x) = \pi(gx) \qquad (*)$$

pour tous $g \in G$, $x \in X$; ceci prouve déjà l'unicité sous réserve d'existence. Pour que $(*)$ soit une définition correcte de $g\pi(x)$, il faut prouver que le membre de droite ne dépend que de $\pi(x)$. Or si $\pi(x) = \pi(x')$, il existe $h \in H$ tel que $x' = xh$; alors $gx' = (gx)h$, et $\pi(gx') = \pi(gx)$, ce qui prouve notre assertion. Il reste à vérifier que ceci définit bien une action de G sur G/H, mais ceci est comme d'habitude une vérification immédiate que nous laisserons au lecteur.

(ii) C'est le même raisonnement que dans la prop. 1.6.3*(ii)* (on pourrait d'ailleurs s'y ramener) : il est clair que $\varphi_x(gh) = ghx = gx$ si $h \in G_x$; donc φ_x passe au quotient par G_x en un morphisme $\overline{\varphi}_x : G/G_x \to X$. Si $\overline{\varphi}_x(\pi(g)) = \overline{\varphi}_x(\pi(g'))$, on a $\varphi_x(g) = \varphi_x(g')$, donc $gx = g'x$ et $g^{-1}g'x = x$, ce qui prouve que $g^{-1}g' \in G_x$ et donc que $\pi(g) = \pi(g')$. Ainsi, le morphisme $\overline{\varphi}_x$ défini par φ_x par passage au quotient est bijectif.

1.6.5 Définition. — On dit qu'un sous-groupe H est d'*indice fini* dans G, si l'ensemble G/H est fini ; on note alors $[G : H] = |G/H|$, et on dit que $[G : H]$ est l'indice de H dans G. Il est clair que les sous-groupes d'indice fini sont exactement les stabilisateurs des points des G-ensembles finis.

1.6.6 Exercice. — *(a)* Soient H, K deux sous-groupes de G. Montrer que les conditions suivantes sont équivalentes :

(i) H agit transitivement sur G/K ;
(ii) K agit transitivement sur G/H ;
(iii) G agit transitivement sur $G/H \times G/K$.

(b) Montrer que si H et K sont d'indice fini dans G, $H \cap K$ aussi, et

$$[G : H \cap K] \leq [G : H][G : K]$$

(c) Sous l'hypothèse de *(b)*, montrer que les conditions *(i)*, *(ii)*, *(iii)* de *(a)* sont encore équivalentes à

(iv) $[G : H \cap K] = [G : H][G : K]$.

(d) Montrer que l'on a toujours $[G : H \cap K] \geq \max\{[G : H], [G : K]\}$. Donner des exemples où $[G : H \cap K] = [G : H][G : K]$, $[G : H \cap K] = \max\{[G : H], [G : K]\}$, et aussi un exemple où $[G : H \cap K]$ ne divise pas $[G : H][G : K]$.

1.6.7 Théorème. — *(classification des G-ensembles homogènes) Soient X, X' deux G-ensembles homogènes. Les assertions suivantes sont équivalentes :*

(i) $X \simeq X'$;
(ii) il existe $x \in X$, $x' \in X'$ tels que $G_x = G_{x'}$;
(iii) il existe $x \in X$, $x' \in X'$ tels que G_x soit conjugué à $G_{x'}$;
(iv) pour tous $x \in X$, $x' \in X'$, G_x est conjugué à $G_{x'}$;

Démonstration. — *(i)* $\Longrightarrow$ *(ii)* : si φ est un isomorphisme de X sur X', et si $x \in X$, on a clairement $G_x = G_{\varphi(x)}$.

(ii) $\Longrightarrow$ *(iii)* : évident.

(iii) $\Longrightarrow$ *(iv)* : cela résulte de la prop. 1.3.9*(ii)*

(iv) $\Longrightarrow$ *(i)* : choisissons $x \in X$, $x' \in X'$. Si $G_{x'} = gG_xg^{-1}$, on a $G_{gx} = G_{x'}$, donc quitte à remplacer x par gx, on peut supposer que $G_x = G_{x'} = H$. Alors les morphismes canoniques φ_x, $\varphi_{x'}$ passent au quotient en des isomorphismes $G/H \to X$, $G/H \to X'$, ce qui prouve bien que X et X' sont isomorphes car isomorphes à un même troisième.

1.6.8 Exercice. — Soit X un G-ensemble homogène, $x \in X$. Montrer que le groupe $\mathrm{Aut}_G(X)$ s'identifie canoniquement au groupe *opposé* du groupe $N_G(G_x)/G_x$ (on pourra commencer par le cas $X = (G, \sigma)$).

1.7 Groupes résolubles, groupes nilpotents

Dans toute cette section, G désigne un groupe.

1.7.1 Définition. — Pour tous $x, y \in G$, on appelle *commutateur* de x et y, et on note $[x, y]$, l'élément $xyx^{-1}y^{-1}$ de G. Si H et K sont deux sous-groupes de G, nous noterons $[H, K]$ le sous-groupe de G *engendré* par les $[x, y]$, $x \in H$, $y \in K$ (remarquons que la relation $[y, x] = [x, y]^{-1}$, qui résulte immédiatement des définitions, entraîne que $[H, K] = [K, H]$). En particulier, notons $D(G) = [G, G]$; on dit que $D(G)$ est le *groupe dérivé* de G.

1.7.2 Proposition. — *Soit G' un groupe, $\varphi \in \mathrm{Hom}\,(G, G')$.*

(i) *Pour tous $x, y \in G$, $\varphi[x, y] = [\varphi(x), \varphi(y)]$.*
(ii) *$\varphi(D(G)) \subset D(G')$.*
(iii) *Si φ est* surjective, *$\varphi(D(G)) = D(G')$.*

Démonstration. — *(i)* et *(ii)* sont immédiats. Pour *(iii)*, il suffit de remarquer que si $x', y' \in G'$, on peut écrire $x' = \varphi(x)$, $y' = \varphi(y)$, donc $[x', y'] = \varphi[x, y]$ d'après *(i)*, ce qui prouve bien que $D(G') \subset \varphi(D(G))$.

1.7.3 Proposition. — *Si H et K sont deux sous-groupes distingués de G, le sous-groupe $[H, K]$ est encore distingué, et contenu dans $H \cap K$.*

Démonstration. — Soient $x \in H$, $y \in K$. Alors en écrivant $[x, y] = xyx^{-1}.y^{-1}$ on voit que $[x, y] \in K$, et en l'écrivant $x.yx^{-1}y^{-1}$ on voit qu'il est dans H ; donc $[x, y] \in H \cap K$, et en passant au sous-groupe engendré on a bien $[H, K] \subset H \cap K$. De plus, si $g \in G$ et si γ_g est l'automorphisme intérieur défini par g, on a $\gamma_g[x, y] = [\gamma_g(x), \gamma_g(y)] \in [H, K]$, donc $\gamma_g[H, K] \subset [H, K]$ en passant au sous-groupe engendré.

1.7.4 Corollaire. — *$D(G)$ est un sous-groupe distingué de G.*

1.7.5 Corollaire. — *Si $H \cap K = \{1\}$, H et K commutent.*

1.7.6 Proposition. — *Le groupe quotient $G/D(G)$ est abélien, et si A est un groupe abélien quelconque, toute $\varphi \in \mathrm{Hom}\,(G, A)$ passe au quotient par $D(G)$. On dit que $G/D(G)$ est le* plus grand quotient abélien, *ou encore l'*abélianisé, *de G.*

Démonstration. — Il est clair qu'un groupe G' est abélien si et seulement si tous les commutateurs dans G' sont égaux à 1. Or si $G' = G/D(G)$, et si $x' = \pi(x)$ et $y' = \pi(y)$ sont deux éléments de G', on aura $[x', y'] = \pi[x, y] = 1$ puisque $[x, y] \in D(G)$. Donc $G/D(G)$ est abélien. Si $\varphi \in \mathrm{Hom}\,(G, A)$ avec A abélien, on aura $\varphi[x, y] = [\varphi(x), \varphi(y)] = 1$ pour tous $x, y \in G$, donc φ passe au quotient par $D(G)$.

1.7.7 Définition. — On appelle *suite dérivée* (resp. *suite centrale descendante*) de G la suite de sous-groupes de G (distingués d'après 1.7.3) définie par :

$$\begin{aligned} &D^0(G) = G, \qquad D^n(G) = [D^{n-1}(G), D^{n-1}(G)] \qquad (n > 0) \\ &C^1(G) = G, \qquad C^n(G) = [G, C^{n-1}(G)] \qquad (n > 1) \end{aligned}$$

On dit que G est *résoluble* (resp. *nilpotent*), s'il existe $n \geq 0$ tel que $D^n(G) = \{1\}$ (resp. $n \geq 1$ tel que $C^n(G) = \{1\}$). Le plus petit $n \geq 0$ tel que $D^n(G) = \{1\}$ (resp. le plus petit $n \geq 1$ tel que $C^{n+1}(G) = \{1\}$) s'appelle la *classe de résolubilité* (resp. *classe de nilpotence*) de G.

Comme on a clairement $D^n(G) \subset C^{n+1}(G)$ pour tout $n \geq 0$, tout groupe nilpotent est résoluble (mais la réciproque est fausse).

1.7.8 Proposition. — *Le groupe G est résoluble si et seulement si il existe une suite de sous-groupes*

$$G_0 = G \supset G_1 \supset \ldots \supset G_n = \{1\}$$

avec G_j distingué dans G_{j-1} et G_{j-1}/G_j abélien pour tout $j \in \{1, \ldots, n\}$.

Démonstration. — Si G est résoluble, $G_j = D^j(G)$ convient. Réciproquement, supposons que la suite $(G_j)_{0 \leq j \leq s}$ existe. Alors l'image de $D(G)$ par la surjection canonique $G \to G/G_1$ est réduite à $\{1\}$ d'après 1.7.6, puisque G/G_1 est abélien ; donc $D(G) \subset G_1$. Par une récurrence évidente, $D^j(G) \subset G_j$ pour $1 \leq j \leq s$. Donc $D^s(G) \subset G_s = \{1\}$.

1.7.9 Proposition. — *(i) Tout sous-groupe et tout quotient d'un groupe résoluble (resp. nilpotent) est résoluble (resp. nilpotent).*
(ii) Soit N un sous-groupe distingué de G. Alors G est résoluble si et seulement si N et G/N le sont.

Démonstration. — *(i)* Exercice.

(ii) Si G est résoluble, N et G/N le sont d'après *(i)*. Réciproquement, supposons N et G/N résolubles, et soit $\pi : G \to G/N$ la surjection canonique. Alors par une récurrence immédiate à partir de 1.7.2*(iii)*, on voit que π induit une surjection $D^j(G) \to D^j(G/N)$ pour tout $j \geq 0$. Si $k \in \mathbf{N}$ est tel que $D^k(G/N) = \{1\}$, on a donc $\pi(D^k(G)) = \{1\}$, d'où $D^k(G) \subset N$, et $D^{k+j}(G) \subset D^j(N)$ pour tout $j \geq 0$, donc $D^n(G) = \{1\}$ pour n assez grand.

1.7.10 Définition. — On appelle *centre* de G, et l'on note $Z(G)$, l'ensemble des éléments z de G tels que $gz = zg$ pour tout $g \in G$ (ou encore, tels que $\gamma_z = \mathrm{Id}_G$). Il est clair que $Z(G)$ est un sous-groupe distingué commutatif de G.

1.7.11 Proposition. — *(i) Soit G un groupe nilpotent de classe de nilpotence n. Alors $C^n(G) \subset Z(G)$; en particulier on a $Z(G) \neq \{1\}$ si $G \neq \{1\}$.*
(ii) Soit N un sous-groupe de $Z(G)$. Alors N est distingué dans G, et G est nilpotent si et seulement si G/N l'est.

Démonstration. — *(i)* C'est clair, car (si $G \neq \{1\}$) $C^n(G) \neq \{1\}$, et $[G, C^n(G)] = \{1\}$, donc tout élément de $C^n(G)$ commute avec tout élément de G.

*(ii)*Il est clair que tout sous-groupe de $Z(G)$ est distingué dans G. Si N est un tel sous-groupe, on sait d'après 1.7.9*(i)* que si G est nilpotent, G/N l'est aussi. Réciproquement, supposons G/N nilpotent, et soit $\pi : G \to G/N$ la surjection canonique. Comme en 1.7.9*(ii)*, on voit que π induit une surjection $C^j(G) \to C^j(G/N)$ pour tout $j \geq 1$. Donc si n est l'ordre de nilpotence de G/N, $\pi(C^{n+1}(G)) = \{1\}$, d'où $C^{n+1}(G) \subset N \subset Z(G)$, et $C^{n+2}(G) \subset [G, Z(G)] = \{1\}$. Donc G est nilpotent de classe $\leq n+1$ ($\geq n$).