Le produit semi-direct

Préparation à l'agrégation de mathématiques
Université de Nice - Sophia Antipolis
Antoine Ducros

Octobre 2007

Ce texte est consacré, comme son titre l'indique, au produit semi-direct. Dans un premier temps, il présente une situation, analogue pour les groupes à celle que l'on rencontre en algèbre linéaire lorsque l'on croise deux sous-espaces vectoriels supplémentaires, qui conduit naturellement à la notion de produit semi-direct *interne*, c'est-à-dire de deux sous-groupes d'un même groupe. On s'inspire ensuite des formules établies à cette occasion pour définir une notion de produit semi-direct *externe*, qui s'applique à deux groupes non *a priori* plongés dans un même troisième.

La troisième section, sans doute plus délicate, est consacrée aux liens entre produits semi-directs et suites exactes. Les sous-sections 3.1 et 3.2 ont leur intérêt propre et sont relativement abordables. Les sous-sections 3.3 et surtout 3.4 ne contiennent *stricto sensu* rien de difficile, mais s'inscrivent dans la famille des mathématiques « à peu près triviales, mais qui font horriblement mal à la tête » , et il est vraisemblable qu'elles vous paraîtront au départ assez rudes ; aussi pouvez-vous contenter de les survoler (voire de les ignorer) en première lecture ; les résultats qu'elles établissent sont récapitulés sans démonstration à la sous-section 3.5 ; un exemple classique qu'il est bon de connaître, celui du groupe affine, conclut ces quelques pages.

1 Le produit semi-direct interne

1.1 Le sous-groupe engendré par une partie

Soit G un groupe et soit $\mathscr{P}$ une partie de G. L'intersection de tous les sous-groupes de G contenant $\mathscr{P}$ est un sous-groupe de G, noté $< \mathscr{P} >$, qui est de manière évidente le plus petit sous-groupe de G contenant $\mathscr{P}$, et que l'on appelle le sous-groupe de G *engendré par* $\mathscr{P}$. Il n'est pas difficile de voir (faites l'exercice) que $< \mathscr{P} >$ est exactement l'ensemble des produits finis d'éléments de $\mathscr{P} \cup \mathscr{P}^{-1}$, où $\mathscr{P}^{-1}$ désigne l'ensemble des p^{-1} pour p parcourant $\mathscr{P}$.

Remarque. L'élément neutre e de G est bien de la forme évoquée ci-dessus, puisqu'on peut le voir comme le *produit vide* d'éléments de $\mathscr{P}$. Si vous n'aimez pas cette description, vous pouvez également, *à condition que* $\mathscr{P}$ *soit non vide*, écrire e sous la forme pp^{-1}, où p est un élément quelconque de $\mathscr{P}$.

1.2 Le sous-groupe engendré par deux sous-groupes : cas général

Soient H et F deux sous-groupes de G ; appliquons ce qui précède avec $\mathscr{P} = H \cup F$. Notons pour commencer que H et F sont stables par inversion, et donc que $\mathscr{P} = \mathscr{P}^{-1}$. Le sous-groupe $< H \cup F >$ de G est en conséquence constitué des produits finis d'éléments de $H \cup F$. Puisque le produit de deux éléments de H (resp. F) appartient à H (resp. F), tout produit fini d'éléments de $H \cup F$ peut s'écrire en faisant alterner un élément de H et un élément de F. De plus, quitte à rajouter l'élément neutre (qui appartient à H et à F) au début et/ou à la fin d'un tel produit, on peut toujours supposer qu'il porte sur une famille non vide, et qu'il commence (resp. se termine) par un élément de H (resp. de F). Autrement dit, $< H \cup F >$ est l'ensemble des éléments de G qui sont de la forme $h_1 f_1 \dots h_r f_r$ où $r \geq 1$ et où h_i (resp. f_i) appartient à H (resp. F) pour tout i.

Par ailleurs, on note HF le sous-ensemble de G formé des éléments qui peuvent s'écrire comme un produit hf avec $h \in H$ et $f \in F$. On a une inclusion évidente $HF \subset < H \cup F >$, qui n'est pas stricte en général ; notez bien que HF n'a aucune raison d'être un sous-groupe de G, car il n'est *a priori* stable ni par l'inversion, ni par le produit.

1.3 Le sous-groupe engendré par deux sous-groupes : cas où l'un des deux est distingué

Lemme. *On conserve les notations introduites ci-dessus et l'on suppose de plus* H distingué *dans* G. *On a alors l'égalité* $< H \cup F >= HF$.

Démonstration. Il suffit de montrer que $< H \cup F > \subset HF$. Soit r un entier non nul et soient $h_1, \dots, h_r$ (resp. $f_1, \dots, f_r$) des éléments de H (resp. F). Nous allons prouver par récurrence sur r que $h_1 f_1 \dots h_r f_r \in HF$, ce qui établira le lemme.

Pour $r = 1$ c'est évident. On suppose donc $r > 1$ et l'assertion établie pour $r - 1$. En vertu de l'hypothèse de récurrence, $h_1 f_1 \dots h_{r-1} f_{r-1} \in HF$; il existe donc h_0 dans H et f_0 dans F tels que $h_1 f_1 \dots h_{r-1} f_{r-1} = h_0 f_0$. Dès lors

$$h_1 f_1 \dots h_r f_r = h_0 f_0 h_r f_r = h_0 f_0 h_r f_0^{-1} f_0 f_r = hf,$$

où l'on a posé $h = h_0 f_0 h_r f_0^{-1}$ et $f = f_0 f_r$. *Comme* H *est distingué dans* G, $f_0 h_r f_0^{-1} \in H$, d'où il découle que $h \in H$. Il est par ailleurs clair que $f \in F$, et $h_1 f_1 \dots h_r f_r = hf$ appartient de ce fait à HF. □

1.4 Le produit semi-direct interne

On désigne toujours par G un groupe, et par H et F deux sous-groupes de G. On suppose dans ce paragraphe que H est distingué dans G, que $H \cap F = \{e\}$, et que $< H \cup F >= G$, cette dernière hypothèse pouvant se réécrire $HF = G$ d'après le lemme précédent.

Comme $HF = G$, tout élément de G a une écriture de la forme hf avec $h \in H$ et $f \in F$. *Montrons qu'une telle écriture est unique.* Supposons donc que $h_1 f_1 = h_2 f_2$, où h_1 et h_2 appartiennent à H, et f_1 et f_2 à F. On a alors

$h_1^{-1}h_2 = f_2^{-1}f_1$. Le terme de gauche est un élément de H, celui de droite un élément de F. Comme $H \cap F = \{e\}$, ces termes sont tous deux égaux à e ; en conséquence, $h_1 = h_2$ et $f_1 = f_2$.

Tout élément de G a donc une *unique* écriture de la forme hf avec $h \in H$ et $f \in F$. On se propose maintenant de comprendre l'effet de la loi de groupe de G sur ce type de décomposition. Pour cela, il est commode d'introduire la notation suivante : si $f \in F$, on désignera par $\varphi(f)$ l'automorphisme $h \mapsto fhf^{-1}$ de H (que cette formule définisse un automorphisme de H résulte du fait que ce dernier est distingué) ; l'application φ est un morphisme de groupes de F dans $\mathsf{Aut}\, H$.

Soient $h \in H$ et $f \in F$. On peut écrire $fh = fhf^{-1}f = \varphi(f)(h)f$. Notons que $fh = hf$ si et seulement si $\varphi(f)(h) = h$. Le morphisme φ mesure donc en un sens le défaut de commutation des sous-groupes H et F de G : il est trivial (*i.e.* $\varphi(f) = \mathsf{Id}_H$ pour tout $f \in F$) si et seulement si $hf = fh$ pour tout couple $(h, f) \in H \times F$. La loi de groupe de G peut maintenant se décrire facilement. Prenons deux éléments h_1 et h_2 de H, et deux éléments f_1 et f_2 de F. De l'égalité $f_1h_2 = \varphi(f_1)(h_2)f_1$ il vient :

$$(*) \quad h_1f_1h_2f_2 = (\underbrace{h_1\varphi(f_1)(h_2)}_{\in H})(\underbrace{f_1f_2}_{\in F}).$$

On dit que G est le *produit semi-direct interne* de H et F, et que F *opère sur* H via φ. Il est immédiat, au vu des égalités ci-dessus, que φ est trivial si et seulement si l'on a $h_1f_1h_2f_2 = h_1h_2f_1f_2$ pour tout $(h_1, h_2, f_1, f_2) \in H^2 \times F^2$; si c'est le cas, on dit que G est le produit *direct* interne de H et F.

Un critère utile. Soient n et m deux entiers premiers entre eux, soit G un groupe de cardinal nm, soit H un sous-groupe distingué de G de cardinal n, et soit F un sous-groupe de G de cardinal m. *On est alors dans la situation décrite ci-dessus.* En effet, $F \cap H$ est à la fois un sous-groupe de H et un sous-groupe de F, donc son cardinal est un diviseur commun à n et m ; il est en conséquence égale à 1, ce qui signifie que $H \cap F = \{e\}$. De plus, HF est un sous-groupe de G qui contient H et F ; son cardinal est de ce fait multiple de m et de n, et partant multiple de nm puisque $\mathsf{PGCD}(n, m) = 1$. Comme le cardinal de G est égal à mn, on a nécessairement $G = HF$.

2 Le produit semi-direct externe

2.1 Introduction

Soient H et F deux groupes, et soit φ un morphisme de groupes de F dans $\mathsf{Aut}\, H$. On se propose de construire un groupe G contenant F (resp. H) comme sous-groupe (resp. comme sous-groupe distingué), tel que $H \cap F = \{e\}$, que $HF = G$, et que pour tout $(h, f) \in H \times F$ l'on ait $fh = \varphi(f)(h)f$, ou $\varphi(f)(h) = fhf^{-1}$ si l'on préfère ; l'on diposera alors de la formule $(*)$ vue au 1.4.

Remarque. L'expression « on se propose de construire un groupe G *contenant* H et F... » constitue un abus de langage. Ce que l'on va en réalité chercher à fabriquer, c'est un groupe G muni de deux morphismes *injectifs* $i : H \hookrightarrow G$ et

$j : F \hookrightarrow G$, tels que les propriétés énoncées ci-dessus soient satisfaites *modulo les identifications respectives de H à $i(H)$ et de F à $j(F)$*. Cela signifie précisément que les assertions suivantes devront être vérifiées (le lecteur conviendra aisément avec nous que le caractère rebutant de la seconde justifie l'abus commis ci-dessus) :

- $i(H)$ est distingué, $i(H) \cap j(F) = \{e\}$ et $G = i(H)j(F)$;
- pour tout $(h, f) \in H \times F$, l'on a $j(f)i(h) = i(\varphi(f)(h))j(f)$.

2.2 La construction

Pour construire G (ainsi que les injections i et j), l'on se contente essentiellement de décalquer la formule $(*)$. On définit donc G comme étant l'*ensemble* produit $H \times F$, et on le munit d'une loi interne, notée multiplicativement, en posant

$$(h_1, f_1)(h_2, f_2) = (h_1\varphi(f_1)(h_2), f_1f_2)$$

pour tout $(h_1, h_2, f_1, f_2) \in H^2 \times F^2$.

On vérifie (c'est un tout petit peu fastidieux, mais sans aucune difficulté) que l'on a bien ainsi construit un groupe ; son élément neutre est (e, e). Soit $(h_1, h_2, f_1, f_2) \in H^2 \times F^2$. Il est immédiat que $(h_1, e)(h_2, e) = (h_1h_2, e)$ et que $(e, f_1)(e, f_2) = (e, f_1f_2)$. Ceci montre que l'application i (resp. j) qui envoie un élément h de H (resp. un élément f de F) sur (h, e) (resp. (e, f)) est un morphisme de groupes, trivialement injectif. Notons que $i(H)$ (resp. $j(F)$ est l'ensemble des éléments de G de la forme (h, e) (resp. (e, f)) avec $h \in H$ (resp. $f \in F$).

Il reste à s'assurer que les conditions mentionnées ci-dessus sont remplies. Il résulte immédiatement de la définition de la loi de groupe définie sur $H \times F$ que $(h, f) \mapsto f$ est un morphisme de G dans F. Son noyau est visiblement égal à $i(H)$, lequel est par conséquent distingué ; l'égalité $i(H) \cap j(F) = \{e\}$ est triviale ; si h (resp. f) appartient à H (resp. F), alors $(h, f) = (h, e)(e, f)$ dans G, et l'on a donc bien $G = i(H)j(F)$; de plus,

$$j(f)i(h) = (e, f)(h, e) = (\varphi(f)(h), f) = (\varphi(f)(h), e)(e, f) = i(\varphi(f)(h))j(f).$$

Le groupe G (muni des injections i et j) jouit donc de toutes les propriétés requises. On l'appelle *produit semi-direct (externe)* de H et F relativement à φ, et on le note $H \rtimes_\varphi F$. Si φ est trivial, on retrouve le groupe produit habituel, que l'on note simplement $H \times F$.

Remarque. Dans un certain nombre de cas, on a réellement intérêt, pour des raisons de confort psychologique, à penser au produit semi-direct en les termes un peu abusifs utilisés au début de ce paragraphe, c'est-à-dire à oublier la construction et les injections i et j, et à le voir comme un groupe contenant H et F, dans lequel chaque élément a une unique écriture sous la formes hf, et dont la loi est décrite par la formule $(*)$ (et se retrouve à partir de l'égalité $fh = \varphi(f)(h)f$, un peu plus simple à retenir) ; toutefois dans d'autres circonstances, il peut être recommandé de travailler avec les couples (h, f) ; c'est par exemple plus prudent si $F = H$, situation dans laquelle il faut être particulièrement soigneux pour éviter toute confusion.

Liens avec le produit semi-direct interne. Redonnons-nous, comme au 1.4, un groupe G, et deux sous-groupes H et F de G tels que H soit distingué, que H et F engendrent G, et que $H \cap F = \{e\}$. Soit φ le morphisme de F dans $\mathsf{Aut}\ H$ qui envoie f sur $h \mapsto fhf^{-1}$. Les résultats du 1.4 peuvent alors, à la lumière de ce qui précède, se réécrire comme suit : *l'application* $(h, f) \mapsto hf$ *établit un isomorphisme entre* $H \rtimes_\varphi F$ *et* G .

Une différence fondamentale entre les produits semi-directs interne et externe.

- Dans le cas interne, le morphisme $\varphi : F \to \mathsf{Aut}\ H$ est imposé par la situation, il est égal à $f \mapsto (h \mapsto fhf^{-1})$.
- Dans le cas externe, le morphisme φ est donné *a priori*, et l'on construit G de sorte que $\varphi(f) = h \mapsto fhf^{-1}$ pour tout $f \in F$; d'une certaine manière, on *force* $\varphi(f)$ à être la restriction à H de l'automorphisme intérieur de G associé à f.

3 Suites exactes et produit semi-direct

3.1 Suites exactes scindées

Soient F, G et H trois groupes, et soient $u : H \to G$ et $p : G \to F$ deux morphismes. On dit que le diagramme

$$1 \longrightarrow H \xrightarrow{u} G \xrightarrow{p} F \longrightarrow 1$$

(où 1 désigne le groupe trivial) est une *suite exacte* si u est injectif, si p est surjectif, et si $\mathsf{Ker}\ p = \mathsf{Im}\ u$.

Remarque. Si

$$1 \longrightarrow H \xrightarrow{u} G \xrightarrow{p} F \longrightarrow 1$$

est une suite exacte, alors $u(H)$, qui coïncide avec le noyau de p, est un sous-groupe *distingué* de G.

Exemple 1. Soit H un sous-groupe d'un groupe G, soit i l'inclusion de H dans G et soit $\pi : G \to G/H$ le morphisme quotient. La suite

$$1 \longrightarrow H \xrightarrow{i} G \xrightarrow{\pi} G/H \longrightarrow 1$$

est exacte.

Exemple 2. Soient H et F deux groupes et soit $\varphi : F \to \mathsf{Aut}\ H$ un morphisme. Soit i le morphisme $h \mapsto (h, e)$ de H dans $H \rtimes_\varphi F$ et soit q le morphisme $(h, f) \mapsto f$ de $H \rtimes_\varphi F$ dans F ; la suite

$$1 \longrightarrow H \xrightarrow{i} H \rtimes_\varphi F \xrightarrow{q} F \longrightarrow 1$$

est exacte.

Définition. On dit qu'une suite exacte

$$1 \longrightarrow H \xrightarrow{u} G \xrightarrow{p} F \longrightarrow 1$$

est *scindée* si le morphisme p possède une *section*, c'est-à-dire un morphisme $s : F \to G$ tel que $p \circ s = \mathsf{Id}_F$.

Exemple. La suite exacte de l'exemple 2 ci-dessus est scindée ; en effet, en reprenant les notations de cette exemple, on voit facilement que $f \mapsto (e, f)$ est une section de $q : (h, f) \mapsto f$.

3.2 Description explicite des sections éventuelles lorsque F est monogène

On se donne une suite exacte

$$1 \longrightarrow H \xrightarrow{u} G \xrightarrow{p} F \longrightarrow 1$$

et l'on suppose que F est monogène, c'est-à-dire engendré par un élément f. Dans ce cas, tout morphisme de groupes défini depuis F est entièrement déterminé par sa valeur en f ; en particulier, si s est un morphisme de groupes de F dans G, alors $p \circ s = \mathsf{Id}_F \iff p(s(f)) = f$; autrement dit, s est une section de p si et seulement si $s(f)$ est un antécédent de f pour p.

- Supposons que f est d'ordre infini, auquel cas $n \mapsto f^n$ établit un isomorphisme $\mathbb{Z} \simeq F$. Dans cette situation, $s \mapsto s(f)$ définit une bijection entre $\mathsf{Hom}(F, G)$ et G ; compte-tenu de ce qui précède, on en déduit que $s \mapsto s(f)$ établit une bijection entre l'ensemble des sections de p et l'ensemble des antécédents de f pour p. *Comme f a au moins un antécédent pour p, l'ensemble des sections de p est non vide, et la suite exacte étudiée est donc scindée.*

  Remarquons que si g est un antécédent de f pour p, la section s qui lui correspond est très simple à décrire : tout élément de F a une unique écriture sous la forme f^n, avec n dans $\mathbb{Z}$; son image par s est alors précisément g^n.

- Supposons que f est d'ordre fini m, auquel cas $n \mapsto f^n$ induit un isomorphisme $(\mathbb{Z}/m\mathbb{Z}) \simeq F$. Dans cette situation, $s \mapsto s(f)$ définit une bijection entre $\mathsf{Hom}(F, G)$ et l'ensemble des élements g de G tels que $g^m = e$; compte-tenu de ce qui précède, on en déduit que $s \mapsto s(f)$ définit une bijection entre l'ensemble des sections de p et l'ensemble des antécédents g de f pour p tels que $g^m = e$. *Contrairement à ce qui se produit lorsque f est d'ordre infini, cet ensemble peut très bien être vide, comme l'atteste l'exemple ci-dessous.*

  Remarquons que si g est un antécédent de f pour p tel que $g^m = e$, la section s qui lui correspond est très simple à décrire : tout élément de F a une écriture sous la forme f^n, où n appartient à $\mathbb{Z}$ *et est uniquement déterminé modulo m* ; son image par s est alors précisément g^n, qui ne dépend bien, en vertu de l'hypothèse faite sur g, que de la classe de n modulo m.

Exemple. Nous allons exhiber une suite exacte dont le terme de droite est monogène et qui n'est pas scindée. Pour tout entier $d > 0$, on note μ_d le sous-groupe de $\mathbb{C}^*$ formé des racines d-ièmes de l'unité ; notons que μ_d est cyclique de cardinal d, il est par exemple engendré par $e^{2i\pi/d}$.

Fixons $m \in \mathbb{N}^*$. Soit u l'inclusion de μ_m dans μ_{m^2}. Soit p le morphisme de μ_{m^2} dans μ_m qui envoie un élément μ sur μ^m. Son noyau est par définition égal au sous-groupe μ_m de μ_{m^2}, et il est surjectif : tout élément de μ_m a une écriture sous la forme $e^{2ik\pi/m}$, où $k \in \mathbb{Z}$, et est ainsi l'image par p de l'élément $e^{2ik\pi/m^2}$ de μ_{m^2}. La suite

$$1 \longrightarrow \mu_m \xrightarrow{u} \mu_{m^2} \xrightarrow{p} \mu_m \longrightarrow 1$$

est donc exacte. *Si $m > 1$ elle n'est pas scindée.* Il suffit en effet, d'après ce qui a été vu plus haut, de vérifier que l'ensemble des $\mu \in \mu_{m^2}$ tels que $p(\mu) = e^{2i\pi/m}$ et tels que $\mu^m = 1$ est vide. Or si $\mu \in \mu_{m^2}$ vérifie $\mu^m = 1$, alors

$$p(\mu) = \mu^m = 1 \neq e^{2i\pi/m},$$

ce dernier fait résultant de l'hypothèse $m > 1$.

3.3 Sections et sous-groupes d'un certain type

Donnons-nous une suite exacte

$$1 \longrightarrow H \xrightarrow{u} G \xrightarrow{p} F \longrightarrow 1 \ .$$

Lemme. *Soit s une section de p. On a $u(H) \cap s(F) = \{e\}$ et $G = u(H)s(F)$. L'application s induit un isomorphisme $F \simeq s(F)$ dont la réciproque est $p_{|s(F)}$.*

Démonstration. Soit g un élément de $s(F) \cap u(H)$. Comme $u(H) = \mathsf{Ker}\ p$, l'on a $p(g) = e$. Comme g appartient à $s(F)$, il s'écrit $s(f)$ pour un certain f dans F. On a alors $f = p(s(f)) = p(g) = e$, et donc $g = s(f) = e$.

Soit maintenant g un élément de G. On a

$$p(gs(p(g))^{-1}) = p(g)p(s(p(g)))^{-1} = p(g)p(g)^{-1} = e$$

(l'avant-dernière égalité provient du fait que $p \circ s = \mathsf{Id}_F$). On peut dès lors écrire $gs(p(g))^{-1} \in \mathsf{Ker}\ p = \mathsf{Im}\ u$. Il existe donc $h \in H$ tel que $g = u(h)s(p(g))$; en conclusion, $g \in u(H)s(F)$.

Soit $f \in F$. Si $s(f) = e$, alors $f = p(s(f)) = e$ et s est donc injective. Elle induit en conséquence un isomorphisme $F \simeq s(F)$. On a $p_{|s(F)} \circ s = p \circ s = \mathsf{Id}_F$, ce qui montre que $p_{|s(F)}$ est la réciproque de l'isomorphisme $F \simeq s(F)$ défini par s. □

Lemme. *Soit Γ un sous-groupe de G tel que $\Gamma \cap u(H) = \{e\}$ et tel que $G = u(H)\Gamma$. La restriction de p à Γ induit un isomorphisme $\Gamma \simeq F$ dont la réciproque, vue comme morphisme de F dans G, est une section de p.*

Démonstration. Soit $\gamma \in \Gamma$ tel que $p(\gamma) = e$. On a alors $\gamma \in \mathsf{Ker}\ p = \mathsf{Im}\ u$; comme $\Gamma \cap u(H) = \{e\}$, on a $\gamma = e$ et $p_{|\Gamma}$ est injectif. Soit $f \in F$. Comme p est surjectif, il existe g dans G tel que $f = p(g)$. Puisque $G = u(H)\Gamma$, l'on peut écrire $g = u(h)\gamma$ avec $h \in H$ et $\gamma \in \Gamma$; dès lors $f = p(g) = p(u(h)))p(\gamma) = p(\gamma)$ puisque $u(H) = \mathsf{Ker}\ p$. En conséquence, $p_{|\Gamma}$ est surjectif, et finalement bijectif.

Soit s la réciproque de $p_{|\Gamma}$, qui va de F dans Γ et que l'on voit comme étant à valeurs dans G. Si f appartient à F, alors $p(s(f)) = p_{|\Gamma}(s(f)) = f$. On a bien démontré que $p \circ s = \mathsf{Id}_F$. □

Soit $\mathscr{S}$ l'ensemble des sections de p, et soit $\mathscr{G}$ l'ensemble des sous-groupes Γ de G tels que $\Gamma \cap u(H) = \{e\}$ et tels que $G = u(H)\Gamma$. Il résulte des deux lemmes ci-dessus que si $s \in \mathscr{S}$, alors $s(F) \in \mathscr{G}$, et que si $\Gamma \in \mathscr{G}$, alors $(p_{|\Gamma})^{-1} \in \mathscr{S}$. On a ainsi construit une application Φ de $\mathscr{S}$ dans $\mathscr{G}$ et une seconde application Ψ de $\mathscr{G}$ dans $\mathscr{S}$.

Proposition. *Les applications Φ et Ψ sont deux bijections réciproques l'une de l'autre.*

Démonstration. Soit s une section de p. Le groupe $\Phi(s)$ n'est autre que $s(F)$; la section $\Psi(\Phi(s))$ est la réciproque de $p_{|\Phi(s)} = p_{|s(F)}$; en vertu du premier des deux lemmes ci-dessus, c'est précisément s.

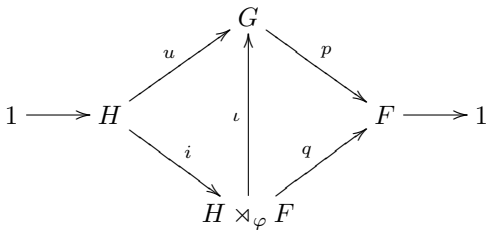
Soit $\Gamma \in \mathscr{G}$. La section $\Psi(\Gamma)$ est égale à $p_{|\Gamma}^{-1}$; comme c'est un isomorphisme de F sur Γ, son image est précisément Γ. Or cette image est par définition le groupe $\Phi(\Psi(\Gamma))$, ce qui achève la démonstration. □

3.4 Sections et produit semi-direct

Considérons une suite exacte

$$1 \longrightarrow H \xrightarrow{u} G \xrightarrow{p} F \longrightarrow 1 \ .$$

- Soit (φ, ι) un couple où φ est un morphisme de F dans $\mathsf{Aut}\ H$ et où ι est un isomorphisme entre $H \rtimes_\varphi F$ et G tel que le diagramme



  commute. Rappelons que i (resp. q) désigne l'application $h \mapsto (h, e)$ (resp. $(h, f) \mapsto f$) ; la commutativité de ce diagramme signifie donc exactement que $\iota(h, e) = u(h)$ pour tout $h \in H$ et que $p(\iota(h, f)) = f$ pour tout $(h, f) \in H \rtimes_\varphi F$.

  Soit σ la section $f \mapsto (e, f)$ du morphisme q. La composée $\iota \circ \sigma$ est une section s de p ; remarquons que le groupe $s(F)$ qui correspond à cette section n'est autre que $\iota(\{e\} \times F)$.

  À tout couple (φ, ι) comme ci-dessus on sait ainsi associer une section s de p.

- Réciproquement, soit s une section de p. On va lui associer un couple (φ, ι) comme ci-dessus. D'après le paragraphe précédent, $s(F)$ est un sous-groupe de G tel que $s(F) \cap u(H) = \{e\}$ et tel que $G = s(F)u(H)$. En vertu des résultats du 1.4, ou plus précisément de leur réinterpétation donnée au 2.2, il existe un morphisme $\psi : s(F) \to \mathsf{Aut}\ u(H)$ tel que $(a, b) \mapsto ab$ établisse un isomorphisme entre $u(H) \rtimes_\psi s(F)$ et G.

Compte-tenu du fait que u (resp. s) induit un isomorphisme entre H (resp. F) et $u(H)$ (resp. $s(F)$), il existe un morphisme φ de F vers $\mathsf{Aut}\ H$ tel que

$$(h, f) \mapsto u(h)s(f)$$

établisse un isomorphisme ι entre $H \rtimes_\varphi F$ et G.

On a en particulier $\iota(h, e) = u(h)$ et $p(\iota(h, f)) = p(s(f)) = f$ pour tout couple $(h, f) \in H \rtimes_\varphi F$, et la condition de commutativité du diagramme est ainsi satisfaite.

Commentaire. L'isomorphisme ι est défini à partir de s par une formule simple, puisqu'on vient de voir qu'il envoie tout couple (h, f) sur $u(h)s(f)$. Le morphisme φ n'admet par contre pas de description aussi agréable : il est seulement *caractérisé* par l'égalité $s(f)u(h) = u(\varphi(f)(h))s(f)$ ou, si l'on préfère, $u(\varphi(f)(h)) = s(f)u(h)s(f)^{-1}$, qui est valable pour tout (h, f).

Vérifions maintenant que les deux constructions $(\varphi, \iota) \mapsto s$ et $s \mapsto (\varphi, \iota)$ que nous venons de détailler sont réciproques l'une de l'autre.

- Partons d'un couple (φ, ι). On lui associe la section s qui envoie un élément f de F sur $\iota(e, f)$; à cette section est associé à son tour un couple (ψ, η). Le but est de montrer que $(\psi, \eta) = (\varphi, \iota)$.

  Par construction de (ψ, η), l'on a $\eta(h, e) = u(h) = \iota(h, e)$ pour tout $h \in H$ et $\eta(e, f) = s(f) = \iota(e, f)$ pour tout $f \in F$; pour tout couple (h, f) l'on a donc $\eta(h, f) = \eta(h, e)\eta(e, f) = \iota(h, e)\iota(e, f) = \iota(h, f)$ (on a utilisé le fait que $(h, f) = (h, e)(e, f)$ dans $H \rtimes_\varphi F$ aussi bien que dans $H \rtimes_\psi F$). Les applications *ensemblistes* η et ι (toutes deux définies sur *l'ensemble* $H \times F$) coïncident donc.

  Par ailleurs, ι (resp. η) est un morphisme de $H \rtimes_\varphi F$ (resp. $H \rtimes_\psi F$) vers G ; l'on a donc $\iota(f, e)\iota(e, h) = \iota(\varphi(f)(h), f)$ et $\eta(f, e)\eta(e, h) = \eta(\psi(f)(h), f)$ pour tout $h \in H$ et tout $f \in F$. Compte-tenu du fait que $\eta(h, f) = \iota(h, f)$ pour tout (h, f), et que ι et η sont injectifs, on a $\psi(f)(h) = \varphi(f)(h)$ pour tout (h, f). En conséquence, $\psi = \varphi$; comme $\eta = \iota$, on a finalement $(\psi, \eta) = (\varphi, \iota)$.

- Partons maintenant d'une section s. Il lui correspond un couple (φ, ι) ; à ce couple est associé à son tour une section t. Le but est de montrer que $t = s$.
  Par construction de t, on a pour tout $f \in F$ l'égalité $t(f) = \iota(e, f)$; mais ce dernier terme est égal, par construction de ι, à $u(e)s(f)$, soit à $s(f)$. En conséquence, $t = s$.

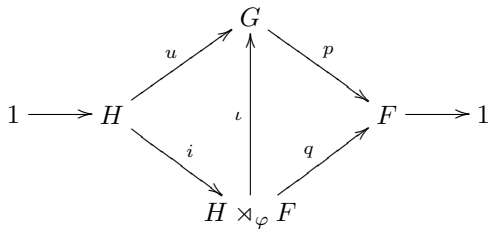
3.5 Récapitulation

Soit

$$1 \longrightarrow H \xrightarrow{u} G \xrightarrow{p} F \longrightarrow 1$$

une suite exacte. Des deux paragraphes qui précèdent, on déduit qu'il revient au même de se donner :

- une section s de p ;
- un sous-groupe Γ de G tel que $\Gamma \cap u(H) = \{e\}$ et tel que $u(H)\Gamma = G$;
- un couple (φ, ι) formé d'un morphisme $\varphi : F \to \mathsf{Aut}\ H$ et d'un isomorphisme $\iota : H \rtimes_\psi F \simeq G$ tel que le diagramme



commute.

Voici les liens entre ces objets.

i) Si la section s est donnée, Γ est simplement le groupe $s(F)$; l'isomorphisme ι envoie (h, f) sur $u(h)s(f)$, et φ est caractérisé par le fait que pour tout (h, f), on a l'égalité

$$s(f)u(h) = u(\varphi(f)(h))s(f) \text{ ou encore } u(\varphi(f)(h)) = s(f)u(h)s(f)^{-1}.$$

ii) Si Γ est donné, alors $p_{|\Gamma}$ induit un isomorphisme $\Gamma \simeq F$, et s est simplement la réciproque de cet isomorphisme, vue comme morphisme de F dans G.

iii) Si (φ, ι) est donné, alors $s(f) = \iota(e, f)$ pour tout f dans F, et le groupe Γ est simplement $\iota(\{e\} \times F)$.

Remarques.

1) Cet énoncé qui porte sur l'équivalence entre trois types d'objets ne préjuge en rien de l'existence de tels objets (rappelez-vous qu'on a vu plus haut un exemple de suite exacte non scindée). Il implique par contre que s'il existe un objet (resp. s'il n'existe pas d'objet) de l'un des trois types fixés, alors il existe un objet de chacun des deux autres types (resp. il n'existe aucun objet de l'un ou l'autre des deux autres types).

2) L'équivalence entre la donnée de s et celle du couple (φ, ι) a pour corollaire le principe suivant, dont l'énoncé est volontairement un peu vague : *toute suite exacte scindée est, à isomorphisme près, de la forme*

$$1 \longrightarrow H \xrightarrow{i} H \rtimes_\varphi F \xrightarrow{q} F \longrightarrow 1 \cdot$$

3.6 Un exemple

Soit k un corps, soit $\vec{E}$ un k-espace vectoriel et soit E un espace affine d'espace directeur $\vec{E}$. Notons τ l'application qui envoie un vecteur $\vec{u}$ sur la

translation $t_{\vec{u}}$, et l l'application qui envoie un élément du groupe affine $\mathsf{GA}(E)$ sur l'application linéaire associée, qui appartient à $\mathsf{GL}(\vec{E})$. La suite

$$1 \longrightarrow (\vec{E}, +) \xrightarrow{\tau} \mathsf{GA}(E) \xrightarrow{l} \mathsf{GL}(\vec{E}) \longrightarrow 1$$

est exacte. Soit $O \in E$. Pour toute application $\vec{f}$ appartenant à $\mathsf{GL}(\vec{E})$, on note $\vec{f}_O$ l'application affine qui fixe O et dont l'application linéaire associée est $\vec{f}$, à savoir $M \mapsto O + \vec{f}(\vec{OM})$.

Il est immédiat que $\vec{f} \mapsto \vec{f}_O$ constitue une section de l. Le sous-groupe qui lui est associé est l'image de $\mathsf{GL}(\vec{E})$ sous cette section ; c'est exactement le sous-groupe de $\mathsf{GA}(E)$ formé des bijections affines qui fixent O.

Quant au couple (φ, ι) correspondant à cette situation, il se décrit comme suit : ι envoie un couple $(\vec{u}, \vec{f})$ sur $t_{\vec{u}} \circ \vec{f}_O$; le morphisme $\varphi : \mathsf{GL}(\vec{E}) \to \mathsf{Aut}\ (\vec{E}, +)$ est tel que l'on ait pour tout couple $(\vec{u}, \vec{f})$ l'égalité $\vec{f}_O \circ t_{\vec{u}} = t_{\varphi(\vec{f})(\vec{u})} \circ \vec{f}_O$. En l'appliquant à O, l'on obtient $O + \varphi(\vec{f})(\vec{u}) = O + \vec{f}(\vec{u})$ et donc $\varphi(\vec{f})(\vec{u}) = \vec{f}(\vec{u})$; ceci vaut pour tout $(\vec{u}, \vec{f})$.

Le morphisme φ est par conséquent *l'inclusion naturelle* de $\mathsf{GL}(\vec{E})$ (groupe des bijections de $\vec{E}$ dans lui-même respectant l'addition et la multiplication par les scalaires) dans $\mathsf{Aut}\ (\vec{E}, +)$ (groupe des bijections de $\vec{E}$ dans lui-même respectant simplement l'addition).