Université de Rennes 1
Préparation à l'agrégation
de mathématiques
Auteur du document :

A. Ducros

A propos des objets caractérisés par une propriété universelle

Antoine Ducros

Octobre 2003

Introduction

Le but de ce texte est de détailler la manière d'utiliser les objets caractérisés par ce que l'on appelle une *propriété universelle* ; vous en avez rencontré sans doute essentiellement en algèbre (quotients divers, algèbres de polynômes...) et en topologie (complété d'un espace métrique, espace topologique quotient...). Pour bien les comprendre, et éviter de se laisser noyer dans la technique et le formalisme, il convient de bien distinguer trois types de questions :

- l'*intuition* qu'il faut se faire de ces objets : c'est évidemment absolument essentiel pour arriver à travailler avec ;
- la *construction* des objets, souvent technique et laborieuse mais sans vraie difficulté ;
- l'*utilisation précise* de la propriété universelle qui les caractérise.

Après avoir dit quelques mots sur chacun de ces points on reviendra sur les exemples mentionnés ci-dessus.

L'aspect intuitif

On est amené, *grosso modo*, à introduire une propriété universelle à chaque fois que l'on souhaite **forcer** un objet à satisfaire certaines contraintes, et **seulement ces contraintes**, sans en imposer d'autres : on cherche donc à construire l'objet qui, parmi tous ceux satisfaisant les contraintes en question, est le plus général, celui pour lequel on n'a rajouté aucune autre spécification. C'est le fait, exprimé **naïvement**, d'être "le plus général", que l'on traduit **rigoureusement** par la satisfaction d'une propriété universelle. Donnons quelques exemples :

Le quotient d'un anneau A par un idéal I. Il s'agit essentiellement de construire un anneau en partant de A, puis en décrétant que les éléments de I sont nuls et en n'imposant rien de plus que ce qui découle de cette nullité et des propriétés générales des anneaux.

L'algèbre de polynômes à n indéterminées $A[X_1, \ldots, X_n]$. Elle doit être vue comme *la A-algèbre la plus générale engendrée par n éléments.*

La construction de $\mathbb{C}$ à partir de $\mathbb{R}$. Elle consiste mathématiquement à considérer $\mathbb{R}[X]/()X^2 + 1$, mais intuitivement elle vise à adjoindre de force à $\mathbb{R}$ un élément que l'on oblige à avoir un carré égal à -1 (et l'on se débrouille avec ces contraintes et elles seules).

Les quotients d'anneaux de polynômes. Plus généralement si A est un anneau et (P_i) une famille de polynômes en n indéterminées $X_1, \ldots, X_n$ sur A alors $A[X_1, \ldots, X_n]/(P_i)$ doit être vu comme *l'algèbre la plus générale engendrée par n éléments en lesquels s'annulent les P_i.*

Le quotient d'un espace topologique par une relation d'équivalence. On cherche intuitivement à forcer tout point à coïncider avec tous les autres points de sa classe d'équivalence, et seulement avec ceux-ci.

La construction

Lorsque vous pensez à un objet défini par une propriété universelle il vaut mieux se fonder sur la description intuitive donnée ci-dessus que sur la construction elle-même. Celle-ci est cependant utile pour deux raisons :

- elle permet tout d'abord de **s'assurer de l'existence** de l'objet satisfaisant la propriété universelle en question, existence qui n'est pas évidente *a priori* (reportez vous ainsi au paragraphe intitulé *contre-exemple* à la fin de ce texte). Pour les objets que vous avez rencontrés jusque là l'existence ne pose pas de réels problèmes, et la construction, quoique technique, est en général élémentaire : on se contente le plus souvent de faire "ce qu'il faut" pour que la propriété souhaitée soit vérifiée. Mais il y a en mathématiques des théorèmes d'existence d'objets satisfaisant une propriété universelle qui sont extrêmement difficiles à démontrer.

-elle permet ensuite d'établir certains faits importants concernant l'objet construit **qui ne découlent pas directement de la propriété universelle**. Par exemple le fait que le morphisme quotient $A \to A/I$ soit surjectif et de noyau I se démontre à l'aide de la définition précise du quotient comme ensemble des classes d'équivalence. De même le fait que dans $A[X_1, \ldots, X_n]$ tout élément ait une unique écriture sous la forme $\sum a_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}$ découle de la construction de $A[X_1, \ldots, X_n]$.

La propriété universelle elle-même

Elle se présente toujours sous la même forme : si l'on appelle B l'objet satisfaisant la propriété universelle celle-ci consiste à fournir une *bijection explicite*

pour tout objet C de même nature entre l'ensemble des morphismes de B vers C (ou parfois de C vers B) et un certain autre ensemble.

Ainsi la propriété universelle du quotient d'un anneau A par un idéal I peut être énoncée comme suit : *si p désigne le morphisme quotient $A \to A/I$ et si C est un anneau alors $g \mapsto g \circ p$ établit une bijection entre l'ensemble des morphismes d'anneaux de A/I vers C et l'ensemble des morphismes d'anneaux de A vers C s'annulant sur I.*

Remarque. On peut se demander ce qui se passe si l'on remplace I par une partie quelconque de A qui ne soit pas forcément un idéal. Plus précisément si P est un sous-ensembke de A on peut chercher à construire un objet B et un morphisme $p : A \to B$ satisfaisant la propriété suivante : *si C est un anneau alors $g \mapsto g \circ p$ établit une bijection entre l'ensemble des morphismes d'anneaux de B vers C et l'ensemble des morphismes d'anneaux de A vers C s'annulant sur P.* Un tel couple (B, p) existe effectivement : il suffit de prendre pour B le quotient $A/(P)$ où (P) est *l'idéal engendré par P.* La flèche $p : A \to A/(P)$ est surjective et de noyau (P).

En termes imagés si l'on force les éléments de P à être nuls alors tous ceux de (P) le deviennent également.

Remarque. Bien que l'on vienne de l'étendre à tous les sous-ensembles de A la notion de quotient *par un idéal* reste très utile : en effet même si P est une partie quelconque de A l'objet satisfaisant la propriété universelle correspondante est construit comme un quotient par un idéal.

Utilisation de la propriété universelle

Vous devez utiliser **systématiquement** les propriétés universelles pour définir des morphismes depuis (ou parfois vers) les objets qu'elles caractérisent. **Elles doivent être connues par cœur et s'en servir doit devenir un automatisme.** Par exemple à chaque fois que vous devez construire un morphisme d'un quotient A/I vers un anneau C vous devez d'abord avoir le **réflexe** de dire : "cela revient à construire un morphisme de A vers C s'annulant sur I". C'est seulement ensuite que vous devez commencer à réfléchir.

L'unicité à unique isomorphisme près

Le cas général

La propriété universelle permet également de montrer que l'objet construit est **unique à unique isomorphisme près** (l'isomorphisme en question devant être "compatible à la propriété universelle" dans un sens que le lecteur est invité à préciser dans chaque cas). Le procédé est toujours le même ; résumons-le grossièrement : on se donne deux objets B et B' satisfaisant tous deux une certaine propriété universelle. Le fait que B la satisfasse assure l'existence d'un unique morphisme f de B vers B' compatible à la propriété universelle, le fait

que B' la satisfasse assure l'existence d'un unique morphisme g de B' vers B compatible à la propriété universelle. L'application gf est un morphisme de B dans lui-même, compatible à la propriété universelle, et comme c'est aussi le cas de l'identité la partie "unicité" (ou "injection") dans la définition de la propriété universelle permet de conclure que gf est l'identité ; on montre de même que fg est l'identité. En conséquence f est un isomorphisme, et on a vu qu'il était unique.

Un exemple

Voyons plus précisément comment cela fonctionne, par exemple avec un anneau de polynômes à une variable. On se donne donc un anneau A, une A-algèbre B munie d'un élément X telle que pour toute A-algèbre C l'application $f \mapsto f(X)$ soit une bijection entre $\mathrm{Hom}_A(B, C)$ et C ; de même on se donne une A-algèbre B' munie d'un élément Y telle que pour toute A-algèbre C l'application $f \mapsto f(Y)$ soit une bijection entre $\mathrm{Hom}_A(B', C)$ et C. On veut montrer qu'il existe un unique isomorphisme de A-algèbres de B vers B' qui envoie X sur Y (c'est ici le sens à donner à l'expression "compatible à la propriété universelle"). La propriété universelle de B entraîne l'existence d'un unique morphisme de A-algèbres f de B vers B' qui envoie X sur Y ; de même celle de B' entraîne l'existence d'un unique morphisme de A-algèbres g de B' vers B qui envoie Y sur X. On en déduit que gf est un morphisme de A-algèbres de B dans lui-même qui envoie X sur X ; comme c'est le cas de l'identité la partie "injection" de la propriété universelle de B assure que gf est l'identité ; on le montre de même pour fg. Les applications f et g sont donc toutes deux des isomorphismes, et "sont uniques".

A titre d'exercice le lecteur est invité à énoncer puis à prouver l'unicité à unique isomorphisme près du quotient d'un anneau par un idéal.

Exemples détaillés

Dans ce qui suit on se propose de donner, pour toute une série d'objets définis par des propriétés universelles, les renseignements suivants :

-l'intuition qu'il convient de se faire de cet objet.

-l'énoncé précis de sa propriété universelle.

-éventuellement certains résultats intéressants que l'on ne déduit pas directement de la propriété universelle, et que l'on établit grâce à la construction de l'objet en question.

-l'énoncé de la propriété universelle comprend toujours la description d'une bijection : on donnera explicitement la bijection réciproque.

Le quotient d'un anneau A par l'idéal (P) engendré par une partie P de A.

Description intuitive

On fabrique à partir de A un anneau dans lequel tous les éléments de P sont décrétés nuls ; on ne rajoute aucune autre contrainte que celles liées à cette nullité et aux propriétés générales des anneaux.

Enoncé de la propriété universelle

Le quotient $A/(P)$ est un anneau muni d'un morphisme $p : A \to A/(P)$ tel que pour tout anneau C l'application $g \mapsto g \circ p$ établisse une bijection entre l'ensembles des morphismes d'anneaux de $A/(P)$ vers C et l'ensemble des morphismes d'anneaux de A vers C s'annulant sur P.

Propriétés obtenues grâce à la construction de $A/(P)$

La flèche $p : A \to A/(P)$ est surjective de noyau (P). On en déduit que si $A \to B$ est un morphisme s'annulant sur P alors le morphisme $A/(P) \to B$ correspondant a même image que $A \to B$, et qu'il est injectif si et seulement si le noyau de $A \to B$ est exactement (P). En particulier tout morphisme d'anneaux $\varphi : A \to B$ induit un isomorphisme $A/\mathrm{Ker}\,\varphi$ et $\mathrm{Im}\,\varphi$.

Réciproque de la bijection

Soit $f : A \to C$ un morphisme d'anneaux s'annulant sur P. Soit x appartenant à $A/(P)$. Comme p est surjectif il existe y appartenant à A tel que $p(y) = x$; si z est un autre élément de A tel que $p(z) = x$ alors $p(y-z) = 0$ donc $y - z$ appartient à (P) d'où il découle que $f(y) = f(z)$; la valeur commune de f sur tous les antécédents de x est notée $g(x)$. L'application g ainsi construite est telle que $g \circ p = f$ (et c'est la seule).

L'algèbre de polynômes $A[X_1, \ldots, X_n]$

Description intuitive

C'est la A-algèbre la plus générale engendrée par n éléments.

Enoncé de la propriété universelle

Pour toute A-algèbre B l'application $f \mapsto (f(X_1), \ldots, f(X_n))$ établit une bijection entre l'ensemble des morphismes de A-algèbres de $A[X_1, \ldots, X_n]$ vers B et l'ensemble B^n.

Propriétés obtenues grâce à la construction de $A[X_1, \ldots, X_n]$

Tout élément de $A[X_1, \ldots, X_n]$ a une unique écriture sous la forme

$$\sum a_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}$$

avec les $a_{i_1,\ldots,i_n}$ dans A.

Réciproque de la bijection

Soit $(b_1, \ldots, b_n)$ un élément de B^n. L'unique morphisme f de $A[X_1, \ldots, X_n]$ vers B qui vaut b_i en X_i est donné par la formule $f(\sum a_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}) = \sum a_{i_1,\ldots,i_n} b_1^{i_1} \ldots b_n^{i_n}$.

Remarque. Le morphisme f ci-dessus est souvent noté $P \mapsto P(b_1, \ldots, b_n)$ et est appelé *évaluation de P en $(b_1, \ldots, b_n)$*.

Un quotient $A[X_1, \ldots, X_n]/(P_i)$ d'une algèbre de polynômes (combinaison des deux cas précédents)

Description intuitive

C'est la A-algèbre la plus générale engendrée par n éléments en lesquels les P_i s'annulent.

Enoncé de la propriété universelle

Pour toute A-algèbre B l'application $f \mapsto (f(\overline{X_1}), \ldots, f(\overline{X_n}))$ établit une bijection entre l'ensemble des morphismes de A-algèbres de $A[X_1, \ldots, X_n]/(P_i)$ vers B et le sous-ensemble de B^n formé des n-uplets en lesquels les P_i s'annulent.

Propriétés obtenues grâce à la construction de $A[X_1, \ldots, X_n]/(P_i)$

Tout élément de $A[X_1, \ldots, X_n]/(P_i)$ a une écriture sous la forme

$$\sum a_{i_1,\ldots,i_n} \overline{X_1}^{i_1} \ldots \overline{X_n}^{i_n}$$

avec les $a_{i_1,\ldots,i_n}$ dans A ; deux telles écritures

$$\sum a_{i_1,\ldots,i_n} \overline{X_1}^{i_1} \ldots \overline{X_n}^{i_n}$$

et

$$\sum b_{i_1,\ldots,i_n} \overline{X_1}^{i_1} \ldots \overline{X_n}^{i_n}$$

sont égales si et seulement si le polynôme

$$\sum (a_{i_1,\ldots,i_n} - b_{i_1,\ldots,i_n}) X_1^{i_1} \ldots X_n^{i_n}$$

appartient à l'idéal (P_i).

Réciproque de la bijection

Soit $(b_1, \ldots, b_n)$ un élément de B^n en lequel tous les P_i s'annulent. Si

$$\sum a_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}$$

appartient à (P_i) alors $\sum a_{i_1,\ldots,i_n} b_1^{i_1} \ldots b_n^{i_n}$ est nul. On en déduit que la valeur de $\sum a_{i_1,\ldots,i_n} b_1^{i_1} \ldots b_n^{i_n}$ ne dépend que de la classe de $\sum a_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}$ modulo (P_i), et donc que de $\sum a_{i_1,\ldots,i_n} \overline{X_1}^{i_1} \ldots \overline{X_n}^{i_n}$; on peut donc désigner sans ambiguïté cette valeur par la notation $f(\sum a_{i_1,\ldots,i_n} \overline{X_1}^{i_1} \ldots \overline{X_n}^{i_n})$. L'application f ainsi construite est l'unique morphisme de $A[X_1, \ldots, X_n]/(P_i)$ vers B tel que $f(\overline{X_i}) = b_i$ pour tout i.

Module libre M de base $(e_i)_{i \in I}$ sur un anneau A

Description intuitive

C'est le A-module le plus général engendré par une famille d'éléments indexée par I.

Enoncé de la propriété universelle

Pour tout A-module N l'application $f \mapsto (f(e_i))$ établit une bijection entre l'ensemble des applications A-linéaires de M vers N et l'ensemble N^I des familles d'éléments de N indexés par I.

Propriété obtenue grâce à la construction de M

Tout élément de M a une unique écriture sous la forme $\sum a_i e_i$ où les a_i appartiennent à A et sont tous nuls sauf un nombre fini.

Réciproque de la bijection

Soit N un A-module et soit (n_i) une famille indexée par I d'éléments de N. L'unique application A-linéaire de M vers N qui envoie e_i sur n_i pour tout i est celle qui associe à un élément m de M la somme $\sum a_i m_i$, où (a_i) est l'unique famille de scalaires telle que $m = \sum a_i e_i$.

Le complété $\widehat{X}$ d'un espace métrique X

Description intuitive

On rend X complet en lui adjoignant de force les limites de toutes ses suites de Cauchy.

Enoncé de la propriété universelle

L'espace $\widehat{X}$ est muni d'une isométrie $i : X \hookrightarrow \widehat{X}$. Pour tout espace métrique complet Y l'application $f \mapsto f \circ i$ établit une bijection entre l'ensemble des isométries de $\widehat{X}$ vers Y et l'ensemble des isométries de X vers Y.

Propriété obtenue grâce à la construction de $\widehat{X}$

L'isométrie i identifie X à un sous-espace dense de $\widehat{X}$.

Réciproque de la bijection

Soit φ une isométrie de X vers un espace complet Y et soit x un point de $\widehat{X}$. Comme X est dense dans $\widehat{X}$ le point x est limite d'une suite (x_n) d'éléments de X nécessairement de Cauchy puisque convergente. Comme φ est une isométrie la suite $(\varphi(x_n))$ est de Cauchy et donc converge vers un certain y puisque Y est complet. On vérifie que y ne dépend pas de la suite (x_n) choisie, et l'application $f : x \mapsto y$ est l'unique isométrie de $\widehat{X}$ vers Y telle que $f \circ i = \varphi$.

Le quotient d'un espace topologique X par une relation d'équivalence $\mathscr{R}$

Description intuitive

On veut forcer tout point de X à coïncider avec les autres points de sa classe d'équivalence, et seulement avec ceux-ci.

Enoncé de la propriété universelle

Le quotient $X/\mathscr{R}$ est muni d'une application continue $p : X \to X/\mathscr{R}$. Pour tout espace topologique Y l'application $f \mapsto f \circ p$ établit une bijection entre les applications continues de $X/\mathscr{R}$ vers Y et les applications continues de X vers Y constantes sur les classes de $\mathscr{R}$.

Propriétés obtenues grâce à la construction de $X/\mathscr{R}$

La flèche $X \to X/\mathscr{R}$ est surjective ; deux points x et y ont même image dans $X/\mathscr{R}$ si et seulement si $x\mathscr{R}y$. Une partie de $X/\mathscr{R}$ est ouverte si et seulement si son image réciproque par p est ouverte.

Bijection réciproque

Soit Y un espace topologique et soit φ une application continue de X vers Y constante sur les classes de $\mathscr{R}$. Soit x un point de $X/\mathscr{R}$. Comme p est surjective il existe y tel que $p(y) = x$. Si z est un point de X tel que $p(z) = x$ alors $z\mathscr{R}y$ d'après ce qui précède, et donc $\varphi(z) = \varphi(y)$. Notons $f(x)$ la valeur commune de φ sur tous les antécédents de x ; l'application f ainsi définie est l'unique application continue de $X/\mathscr{R}$ vers Y telle que $f \circ p = \varphi$.

Exemples d'utilisation du quotient

i) Soit A un anneau et soit f un élément de A. Montrons comment prouver qu'il existe un isomorphisme entre $A[X]/fA[X]$ et $(A/fA)[X]$. Notons pour commencer que la propriété universelle de la A-algèbre $A[X]$ assure l'existence d'un unique morphisme de $A[X]$ vers $(A/fA)[X]$ qui prolonge $A \to A/fA$ et envoie X sur X. Ce morphisme envoie par construction $\sum a_i X^i$ sur $\sum \overline{a_i} X^i$. Il est surjectif puisque $A \to A/fA$ l'est. Son noyau est l'ensemble des polynômes de la forme $\sum a_i X^i$ avec $\overline{a_i} = 0$ pour tout i, c'est-à-dire exactement $fA[X)$. En effet si un polynôme s'écrit $\sum a_i X^i$ avec $\overline{a_i} = 0$ pour tout i alors pour tout i l'élément a_i de A appartient à fA et donc s'écrit fb_i pour un certain b_i ; on voit alors que P s'écrit $f \sum b_i X^i$. Réciproquement un polynôme appartenant à $fA[X]$ a par construction tous ses cœfficients multiples de f, donc nuls modulo fA.
On déduit de tout ceci que la flèche construite induit un isomorphisme entre $A[X]/fA[X]$ et $(A/fA)[X]$. Notez que cette flèche envoie $\overline{X}$ sur X.

ii) Soit A un anneau et soient f et g deux éléments de A. Montrons que $A/(f,g)$ est isomorphe à $(A/(f))/(\overline{g})$. Considérons la flèche composée $A \to A/(f) \to (A/(f))/(\overline{g})$. Comme $A \to A/(f)$ et $(A/(f))/(\overline{g})$ sont des surjections elle est surjective. Son noyau est l'ensemble des a appartenant à A tel que l'élément $\overline{a}$ de $A/(f)$ soit nul modulo $\overline{g}$, autrement dit c'est l'ensemble des a pour lesquels il existe b appartenant à A tel que $\overline{a} = \overline{bf}$. C'est encore l'ensemble des a appartenant à A tels qu'il existe b et c dans A vérifiant l'égalité $a = bf + cg$. C'est donc exactement l'idéal (f,g) de A. On en déduit que la flèche ainsi construite établit un isomorphisme entre $A/(f,g)$ et $(A/(f))/(\overline{g})$.

Remarque. Les deux preuves ci-dessus utilisent aussi bien les propriétés universelles (des quotients et des polynômes) que celles fournies par les constructions. Si cela vous amuse, vous pouvez, à titre d'exercice, essayer de construire les isomorphismes souhaités *en utilisant uniquement les propriétés universelles.* Mais c'est un peu plus long, comme vous le constaterez...

Appliquons ces résultats à l'anneau $(\mathbb{Z}/p\mathbb{Z})[X]/(X^2+\overline{1})$, où p est un nombre premier. Il est isomorphe d'après le *i*) à $(\mathbb{Z}[X]/p\mathbb{Z}[X])/(\overline{X}^2+\overline{1})$ et donc encore, d'après le *ii*), à $\mathbb{Z}[X]/(p, X^2+1)$. En appliquant à nouveau le *ii*) on voit que ce dernier est isomorphe à $\mathbb{Z}[X]/(X^2+1)/(\overline{p})$. Or l'unique application de $\mathbb{Z}[X]$ dans *l'anneau* $\mathbb{Z}[i]$ *des entiers de Gauss* qui envoie X sur i, application dont l'existence est assurée par la propriété universelle de $\mathbb{Z}[X]$, est surjective et a pour noyau l'idéal engendré par X^2+1 (prouvez-le!). Il en découle que $\mathbb{Z}[X]/(X^2+1)$ est isomorphe à $\mathbb{Z}[i]$.

On en déduit que $\mathbb{Z}[X]/(X^2+1)/(\overline{p})$ est isomorphe à $\mathbb{Z}[i]/p$. On a finalement établi l'existence d'un isomorphisme entre $(\mathbb{Z}/p\mathbb{Z})[X]/(X^2+1)$ et $\mathbb{Z}[i]/p$. En

particulier ces deux anneaux sont ou bien tous deux intègres, ou bien tous deux non intègres. Or le premier est intègre si et seulement si $X^2+\overline{1}$ est irréductible dans $(\mathbb{Z}/p\mathbb{Z})[X]$ c'est-à-dire, puisqu'il est de degré 2, si et seulement si il n'a pas de racines dans $\mathbb{Z}/p\mathbb{Z}$, donc si et seulement si -1 n'est pas un carré modulo p. Quant à $\mathbb{Z}[i]/p$ il est intègre, $\mathbb{Z}[i]$ étant factoriel (et même principal !) si et seulement si p est irréductible dans $\mathbb{Z}[i]$. *On a finalement prouvé que $\mathbb{Z}[i]/p$ est intègre si et seulement si -1 n'est pas un carré modulo p.*

Groupes et propriétés universelles

Ce qui suit est plus difficile (bien que sur le principe ce soit dans la lignée de ce qui précède) et doit être vu comme un complément culturel pour celles et ceux qui sont déjà à l'aise avec le reste.

Groupe quotient d'un groupe par une partie quelconque

Soit G un groupe et soit P une partie de G. On cherche à construire un groupe F et un morphisme $p : G \to F$ tel que pour tout groupe H l'application $f \mapsto f \circ p$ établisse une bijection entre l'ensemble des morphismes de groupes de F vers H et l'ensemble des morphismes de groupes de G vers H s'annulant sur P.

Un tel couple (F, p) existe effectivement (et est unique à unique isomorphisme près). On peut prendre par exemple (la démonstration est laissée au lecteur !) pour F le quotient de G par *le plus petit sous-groupe distingué de G contenant* P et pour p la flèche quotient.

Remarques. Si P est lui-même un sous-groupe distingué on retrouve la notion classique de quotient. Si P est un sous-groupe non distingué faites très attention : **le quotient défini ci-dessus n'est pas le quotient habituel G/P** ; ce dernier satisfait une propriété universelle qui concerne les applications de G vers tous les ensembles (et pas seulement les morphismes de G vers les groupes) et ne peut être muni d'une structure de groupe faisant de la flèche $G \to G/P$ un morphisme.

Groupes libres

Intuitivement on se fixe un entier n et l'on souhaite construire le groupe le plus général engendré par n éléments. On va traduire rigoureusement ce souhait par la recherche d'un groupe G muni de n éléments $g_1, \ldots, g_n$ satisfaisant la propriété universelle suivante : pour tout groupe H l'application $f \mapsto (f(g_1), \ldots, f(g_n))$ établit une bijection entre l'ensemble des morphismes de groupes de G vers H et l'ensemble H^n.

Un tel groupe existe, est unique à unique isomorphisme près (précisez le sens de cette formule dans ce contexte !) et est appelé le *groupe libre à n générateurs*. Expliquons brièvement sa construction : G s'identifie à l'ensemble des *mots*

réduits en les $2n$ *lettres* $g_1, \ldots, g_n, g_1^{-1}, \ldots, g_n^{-1}$, c'est-à-dire des suites finies d'éléments de $\{g_1, \ldots, g_n, g_1^{-1}, \ldots, g_n^{-1}\}$ ne comportant aucune sous-suite de deux termes consécutifs de la forme $g_i g_i^{-1}$ ou $g_i^{-1} g_i$. La loi interne consiste à concaténer deux suites puis à réduire le résultat obtenu, c'est-à-dire à supprimer successivement toutes les sous-suites de deux de termes consécutifs de la forme $g_i g_i^{-1}$ ou $g_i^{-1} g_i$ qui apparaissent. La suite vide est l'élément neutre de G.

Par exemple dans le groupe libre à 3 générateurs le produit des mots

$$g_1 g_2 g_2 g_3^{-1} g_1^{-1} \text{ et } g_1 g_3 g_3 g_2$$

est égal à

$$g_1 g_2 g_2 g_3 g_2.$$

Si l'on se donne un groupe H et n éléments $h_1, \ldots, h_n$ de H l'unique morphisme de G vers H valant h_i en g_i a une description très simple : il envoie tout mot réduit $\mathscr{R}$ sur l'élément de H déduit de $\mathscr{R}$ en y substituant h_i (resp. h_i^{-1}) à g_i (resp. g_i^{-1}) pour tout i. L'élément de H en question sera noté $\mathscr{R}(h_1, \ldots, h_n)$.

Groupes définis par générateurs et relations (combinaison des deux cas précédents)

On se fixe n et on se donne une famille $(\mathscr{R}_j)$ de mots réduits en $2n$ lettres $g_1, \ldots, g_n, g_1^{-1}, \ldots, g_n^{-1}$. On cherche à construire le groupe le plus général engendré par n éléments en lesquels chacun des $\mathscr{R}_j$ (auquel on pense comme à une relation) s'annule. On traduit cette exigence en terme d'une propriété universelle : on cherche un groupe Γ muni de n éléments $\gamma_1, \ldots, \gamma_n$ tel que pour tout groupe H l'application $f \mapsto (f(\gamma_1), \ldots, f(\gamma_n))$ établisse une bijection entre l'ensemble des morphismes de groupes de Γ vers H et le sous-ensemble de H^n formé des n-uplets en lesquels chacun des $\mathscr{R}_j$ s'annule.

Soit G le groupe libre à n générateurs $g_1, \ldots, g_n$. Désignons par F le plus petit sous-groupe distingué de G contenant les $\mathscr{R}_j$, par Γ le groupe quotient G/F et par γ_i la classe de g_i modulo F pour tout i. Alors Γ muni des γ_i répond au problème posé (il suffit d'appliquer les propriétés universelles mentionnées aux deux paragraphes précédents) ; on l'appelle le *groupe défini par les générateurs* $\gamma_1, \ldots, \gamma_n$ *et les relations* $\mathscr{R}_j(\gamma_1, \ldots, \gamma_n)$.

Exercice : on fixe un entier n et on note H le groupe défini par deux générateurs x et y et par les relations x^2, y^n et $xyx^{-1}y$. Prouvez que H est isomorphe au groupe diédral D_n.

Contre-exemple

Considérons la propriété universelle de l'algèbre des polynômes en une variable sur un anneau A : c'est une algèbre B munie d'un élément X telle que pour toute A-algèbre C l'application $f \mapsto f(X)$ établisse une bijection entre l'ensemble $\mathrm{Hom}_A(B, C)$ et l'ensemble C.

Le but est de montrer qu'il n'y a pas d'analogue de cette algèbre lorsqu'on travaille avec des corps. Plus précisément soit k un corps ; rappelons qu'une *k-extension* est simplement une k-algèbre qui est un corps. Question : peut-on trouver une k-extension L munie d'un élément T qui satisfasse la propriété suivante : *pour toute k-extension F l'application $f \mapsto f(T)$ établit une bijection entre l'ensemble* $\mathrm{Hom}_k(L, F)$ *et l'ensemble F* ?

La réponse est négative. En effet supposons que ce soit le cas. On est alors dans l'une des deux situations suivantes :

- T est transcendant sur k. Dans ce cas $T - 1$ est inversible dans L. Soit Y son inverse et soit φ l'unique k-morphisme de L dans k valant 1 en T. Comme $Y(T-1) = 1$ on a $\varphi(Y)(\varphi(T) - 1) = 1$ mais comme $\varphi(T) = 1$ on obtient $0 = 1$ ce qui est absurde (un corps est toujours non nul !).

- T est algébrique sur k. Soit P son polynôme minimal et soit φ l'unique k-morphisme de L dans $k(Z)$ (où Z est une indéterminée) qui envoie T sur Z. Comme P est à cœfficients dans k et comme φ est un k-morphsime on a l'égalité $\varphi(P(T)) = P(\varphi(T))$. Il vient

  $$0 = \varphi(0) = \varphi(P(T)) = P(\varphi(T)) = P(Z)$$

  ce qui est absurde puisque P est non nul.