

Vocabulaire de base sur les groupes

1^{er} octobre 2009

En cours, nous avons dit que $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$ était un groupe pour la multiplication ; de même que \mathbb{C}^* l'ensemble des nombres complexes non nuls. On a même parlé de groupe multiplicatif (pour faire référence à la loi \times). Et puisque $\mathbb{U} \subset \mathbb{C}^*$, on a dit que \mathbb{U} était un sous-groupe de \mathbb{C}^* .

De même, nous avons dit que \mathbb{R} était un groupe pour l'addition. On a parlé dans ce cas de groupe additif (pour faire référence à la loi $+$). On ne l'a pas dit, mais $2\pi\mathbb{Z}$ est un sous-groupe du groupe additif \mathbb{R} . Ceci sera expliqué plus loin.

En attendant ...

I ... COMMENÇONS PAR LA DÉFINITION

1. *Motivation*

C'est un principe général : mettre de la structure là où il n'y en pas. Par exemple, $\mathbb{Z}[i]$ que nous avons déjà croisé a une addition et une multiplication ce qui fait de lui un *anneau* (on dira plus tard ce que c'est). Il s'avère que cet anneau $\mathbb{Z}[i]$ est un anneau avec des propriétés très surprenantes. Ce sont ces propriétés surprenantes qui ont permis de répondre à la question suivante : *À quelles conditions un entier peut s'écrire comme la somme de deux carrés ?*

Il faut se dire que ces structures dont nous parlons ici sont apparues tardivement en comparaison à la pratique double-millénaire des mathématiques.

Le premier à parler de groupe fût Évariste Galois¹, mais il considérait une situation particulière : celle des groupes de permutation (voir plus loin). Il les utilisa pour donner des conditions permettant d'exprimer les racines d'un polynôme en fonction des coefficients du polynôme (avec quelques restrictions notables : seules les extractions de racines ; des additions ; multiplications et divisions étaient « autorisées »). Ces conditions portent sur un groupe associé au polynôme appelé depuis groupe de Galois.

Depuis lors, les groupes ont été amplement utilisés dans de nombreuses situations : en géométrie ; en théorie des nombres ; pour la résolution d'équations différentielles ; etc ... et dans la vie de tous les jours pour les échanges sécurisés (cryptosystème R.S.A ; El Gamal ; log discret).

Pour avoir une vision esthétique de la notion de groupe, vous pouvez jeter un oeil² aux jolies illustrations dues à Escher³ sur les différentes manière de paver un plan (ou une terrasse si on a une surface restreinte) à l'aide d'un motif de départ (si possible différent du morne carreau).

2. *Définition*

Ici, il s'agit de multiplier (ou d'additionner) des éléments entre eux. Mais il faut quelques règles pour pouvoir le faire. Ce sont ces quelques règles qui permettront de dire s'il s'agit d'un groupe (ou pas).

¹Mathématicien français (1811-1832). Voir sa notice sur <http://www-groups.dcs.st-and.ac.uk/~history/index.html>

²<http://mcescher.frloup.com/affichediapo.php?cat=6> et pour des explications <http://xavier.hubaut.info/coursmath/doc/pavages.htm>

³Escher Mauritz Cornelius (1898-1972). Graveur et dessinateur néerlandais. Célèbre pour son travail sur les paradoxes (perspectives impossibles ; auto-référence) et les pavages.

Avant de parler de groupe, parlons de loi de composition interne.

Définition 1 Soit E un ensemble. Une loi de composition interne \star sur E est une application $\star : E \times E \rightarrow E$.

On voit donc la loi $+$ définie sur \mathbb{R} (ou sur \mathbb{C}) comme une application de $\mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$. À $(x, y) \in \mathbb{R}^2$ est associé $x + y$ qui appartient bien à \mathbb{R} . Il s'agit donc d'une loi de composition interne sur \mathbb{R} .

De même la loi \times est une loi de composition interne pour \mathbb{R}_+^* . En effet à $(x, y) \in \mathbb{R}_+^* \times \mathbb{R}_+^*$ est associé $x \times y$ qui est bien un élément de \mathbb{R}_+^* .

Remarque : Le terme interne est donc là pour dire que tout reste dans l'ensemble E considéré ; le terme loi se comprenant comme une règle bien définie ; composition car on considère deux éléments.

On peut enfin définir la notion de groupe :

Définition 2 Un ensemble G muni d'une loi de composition interne \star (on note en général (G, \star) ; G étant l'ensemble et \star la loi de composition interne sur G) est un groupe si les propriétés suivantes sont vérifiées.

1. (associativité) $\forall (x, y, z) \in G^3, (x \star y) \star z = x \star (y \star z)$;
2. (existence d'un élément neutre) $(\exists e \in G) (\forall x \in G : x \star e = e \star x)$;
3. (existence d'un symétrique ou inverse) $(\forall x \in G) (\exists y \in G : x \star y = y \star x = e)$.

Prenons le cas de $(\mathbb{R}, +)$: il s'agit bien d'un groupe.

1. Tout d'abord $2 + (3 + 5)$ c'est la même chose que $(2 + 3) + 5$: la loi $+$ est associative⁴
2. Il y a bien un élément neutre : c'est 0.
3. Enfin tout élément a un symétrique (synonyme : inverse ou opposé). Le symétrique de π c'est $-\pi$.

La définition soulève quelques questions (que je soulève pour vous) :

- Existence d'un élément neutre. D'accord, mais y-a-t-il plusieurs éléments neutres ?
- Existence d'un symétrique. D'accord, mais y-a-t-il plusieurs symétriques possibles pour un même élément ?

La réponse est NON. Si élément neutre il y a, il est unique. Si symétrique il y a, il est unique. Voici pourquoi (ceci peut être sauté en première lecture)

Démonstration. —

- Considérons tout d'abord deux éléments neutres e_1 et e_2 .
Puisque e_1 est neutre, $e_1 \star e_2 = e_1$.
Puisque e_2 est neutre, $e_1 \star e_2 = e_2$.
On conclut que $e_1 = e_2$. Ce qui signifie qu'il n'y a qu'un seul élément neutre ! On le note e .
- Considérons maintenant $x \in G$. Supposons qu'il existe $y_1 \in G$ et $y_2 \in G$ tels que :

$$x \star y_1 = y_1 \star x = e ; x \star y_2 = y_2 \star x = e.$$

On va calculer $(x \star y_1) \star y_2$. de deux manières

1. $(x \star y_1) \star y_2 = e \star y_2 = y_2$ (on a utilisé successivement le fait que y_1 est un symétrique de x puis que e est neutre).
2. $(x \star y_1) \star y_2 = (y_1 \star x) \star y_2 = y_1 \star (x \star y_2)$ (on a utilisé successivement $x \star y_1 = y_1 \star x$ puis l'associativité).
Mais $y_1 \star (x \star y_2) = y_1 \star e = y_1$ (on a utilisé successivement le fait que y_2 est un symétrique de x puis que e est neutre).

On a donc $y_1 = (x \star y_1) \star y_2 = y_2$. Ce qui signifie que x n'a qu'un seul symétrique.

□

Dorénavant, on parlera donc de l'**élément neutre** d'un groupe (G, \star) . On le notera e_G (parfois e , parfois autrement selon le contexte). Et si $x \in G$, on parlera de son symétrique et qu'on note x^{-1} (parfois $-x$ selon le contexte, mais de préférence au format multiplicatif).

Remarque : Soit (G, \star) un groupe.

⁴Ne pas croire qu'un exemple particulier vaut preuve de l'associativité. Dans le cas de la loi $+$ définie sur \mathbb{R} , cela fait partie des propriétés admises.

1. On a $(x \star y)^{-1} = y^{-1} \star x^{-1}$. On pourra remarquer l'analogie avec la formule donnant la réciproque de la composée de deux bijections (voir plus loin) ;
2. Si pour tous x et y dans le groupe G

$$x \star y = y \star x,$$

on dit que le groupe G est **commutatif** (ou abélien⁵).

3. Quelques exemples

Bijections d'un ensemble Soit E un ensemble vide. On note $\text{Bij}(E)$ l'ensemble des bijections de E dans E .

$\text{Bij}(E)$ muni de la composition d'applications \circ est un groupe.

Tout d'abord, il faut vérifier que \circ est une loi de composition interne. Mais si f et g sont des bijections de E dans E alors $f \circ g$ est une bijection de E dans E .

1. la loi \circ est associative. Soient f, g et h des bijections de E dans E . Par définition, l'application $(f \circ g) \circ h$ associe à $x \in E$ l'élément $(f \circ g)(h(x))$ soit $f(g(h(x)))$.
De même, l'application $f \circ (g \circ h)$ associe à $x \in E$ l'élément $f((g \circ h)(x))$ soit $f(g(h(x)))$.
Par conséquent, pour tout $x \in E$, $((f \circ g) \circ h)(x) = (f \circ (g \circ h))(x)$. Ce qui signifie que $(f \circ g) \circ h = f \circ (g \circ h)$, et on a donc établi l'associativité.
2. Il y a un élément neutre : il s'agit de l'application identité Id_E .
Par définition $f \circ \text{Id}_E$ est l'application qui à $x \in E$ associe l'élément $f(\text{Id}_E(x)) = f(x)$. Par conséquent $f \circ \text{Id}_E = f$.
On trouve de la même manière $\text{Id}_E \circ f = f$.
3. Tout élément $f \in \text{Bij}(E)$ possède un symétrique : il s'agit de la réciproque de f (ce qui explique d'une part la notation f^{-1} et d'autre part le terme « loi de composition interne »). On a bien $f \circ f^{-1} = \text{Id}_E$ et $f^{-1} \circ f = \text{Id}_E$.

En général $\text{Bij}(E)$ n'est pas un groupe commutatif.

Groupe des permutations d'un ensemble fini Si E est un ensemble fini, le groupe des permutations de E , noté $\sigma(E)$ est le groupe des bijections de E dans E (on ne parle pas de bijection mais de permutation dans ce contexte). Si $E = \{1, \dots, n\}$, son groupe de permutations est noté σ_n . En général $\sigma(E)$ et σ_n ne sont pas des groupes commutatifs.

Le groupe σ_n est un exemple de groupe fini (il possède un nombre fini d'éléments). Son cardinal⁶ est égal à $n! = n \times (n-1) \times \dots \times 1$.

Groupe des isométries du plan Ceci peut être sauté en première lecture.

Une application f du plan euclidien \mathcal{P} est une isométrie si pour tous points M et N du plan

$$f(M)f(N) = MN.$$

Par exemple, une rotation, une translation, une symétrie axiale sont des exemples d'isométrie du plan, puisque chacune d'elles préserve les distances. En revanche une homothétie de rapport 2 n'est pas une isométrie. Elle a plutôt tendance à multiplier les distances par 2.

On peut établir que si f est une isométrie du plan, alors f est une bijection. L'ensemble $\text{Isom}(\mathcal{P})$ est alors un groupe pour la composition (donc pour la loi \circ).

En fait $\text{Isom}(\mathcal{P})$ est un *sous-groupe* du groupe $(\text{Bij}(\mathcal{P}), \circ)$ et en tant que sous-groupe, c'est un groupe.

Le groupe $\text{Isom}(\mathcal{P})$ n'est pas commutatif.

⁵En l'honneur de Niels Abel. **Abel** Niels (1802-1829). Mathématicien norvégien

⁶Le cardinal d'un ensemble fini E se note $|E|$. Ici, on a donc $|\sigma_n| = n!$. Ne pas confondre avec la valeur absolue !

4. Sous-groupe d'un groupe

Définition 3 Soit (G, \star) un groupe. Un sous-groupe H de G est un sous-ensemble de G ayant les propriétés suivantes.

1. $e_G \in H$.
2. $\forall (x, y) \in H^2, x \star y^{-1} \in H$.

On peut remplacer la propriété 2. par les deux propriétés suivantes.

2. (a) $\forall (x, y) \in H^2, x \star y \in H$;
- (b) $\forall y \in H, y^{-1} \in H$.

Propriété 1 Soient (G, \star) un groupe et H un sous-groupe. Alors H muni de la loi \star est un groupe.

EXEMPLE :

- \mathbb{Z} est un sous-groupe de $(\mathbb{R}, +)$: en effet
 1. $0 \in \mathbb{Z}$;
 2. Si m et n appartiennent à \mathbb{Z} alors $n - m$ également.
- Plus généralement, $a\mathbb{Z}$ (avec $a \geq 0$) est un sous-groupe de $(\mathbb{R}, +)$. En particulier $2\pi\mathbb{Z}$ est un sous-groupe de $(\mathbb{R}, +)$.
- \mathbb{R}_+^* est un sous-groupe de (\mathbb{R}^*, \times) .
- \mathbb{U} est un sous-groupe de (\mathbb{C}^*, \times) .
- L'ensemble des isométries du plan qui préservent l'orientation⁷ est un sous-groupe de $\text{Isom}(\mathcal{P})$. On l'appelle le groupe des déplacements du plan et on le note $\text{Isom}^+(\mathcal{P})$.
- L'ensemble des isométries du plan qui préservent le carré $ABCD$ avec $A(1, 0)$; $B(0, 1)$; $C(-1, 0)$; $D(0, -1)$ est un sous-groupe de $\text{Isom}(\mathcal{P})$. C'est un groupe fini à 8 éléments.

Exercice.

1. Discuter de la commutativité des sous-groupes et groupes mentionnés auparavant. Dans le cas de la non-commutativité du groupe (G, \star) considéré, on exhibera deux éléments x et y tels que $x \star y \neq y \star x$.
2. Déterminer les 8 éléments du groupe des isométries du carré.
3. Soit (G, \star) . Montrer que $\{e_G\}$ et G sont des sous-groupes de G .

II MORPHISME DE GROUPES

1. Définition

Définition 4 Soient (G_1, \star_1) et (G_2, \star_2) deux groupes d'élément neutre respectif e_1 et e_2 . Une application ϕ de G_1 dans G_2 est un morphisme si ϕ vérifie les propriétés suivantes.

1. $\phi(e_1) = e_2$;
2. $\forall (x, y) \in G \times G, \phi(x \star_1 y) = \phi(x) \star_2 \phi(y)$.

Remarque :

- On pourrait se passer de la première propriété. En effet $\phi(e_1 \star_1 e_1) = \phi(e_1)$ et dans le même temps $\phi(e_1 \star_1 e_1) = \phi(e_1) \star_2 \phi(e_1)$. D'où $\phi(e_1) = \phi(e_1) \star_2 \phi(e_1)$. En simplifiant on a donc automatiquement $\phi(e_1) = e_2$ grâce à la propriété 2. Malgré cela, on vérifiera systématiquement 1. pour établir qu'une application donnée est un morphisme.
- La propriété 2. entraîne également la propriété suivante.

$$\forall y \in G, \phi(y^{-1}) = \phi(y)^{-1}.$$

⁷On parle alors d'isométrie directe ou de déplacement.

2. Exemples

Exemple de l'exponentielle réelle L'application réelle \exp est un morphisme de $(\mathbb{R}, +)$ vers (\mathbb{R}_+^*, \times) . En effet :

1. $\exp(0) = 1$ (le neutre de $(\mathbb{R}, +)$ a pour image le neutre de (\mathbb{R}_+^*, \times));
2. $\forall (x, y) \in \mathbb{R}^2, \exp(x + y) = \exp(x) \times \exp(y)$.

morphismes de (\mathbb{R}_+^*, \times) vers $(\mathbb{R}, +)$ On en connaît déjà un : \ln . En effet :

1. $\ln(1) = 0$ (le neutre de (\mathbb{R}_+^*, \times) a pour image le neutre de $(\mathbb{R}, +)$);
2. $\forall (x, y) \in \mathbb{R}_+^* \times \mathbb{R}_+^*, \ln(x \times y) = \ln(x) + \ln(y)$.

Y-en a-t-il d'autres ? OUI. Il y en a même beaucoup. Si parmi ceux-là, on s'intéresse à ceux⁸ qui sont des applications continues de \mathbb{R}_+^* vers \mathbb{R} , on a le résultat suivant.

Théorème 1 Soit ϕ un morphisme continu du groupe multiplicatif \mathbb{R}_+^* vers le groupe additif \mathbb{R} . Alors, il existe $\lambda \in \mathbb{R}$ tel que

$$\forall x \in \mathbb{R}_+^*, \phi(x) = \lambda \ln(x).$$

Traduction. Soit ϕ une application continue de \mathbb{R}_+^* vers \mathbb{R} . Si pour tous x et y dans \mathbb{R}_+^* ,

$$\phi(x \times y) = \phi(x) + \phi(y)$$

alors ϕ est de la forme $\lambda \ln$ avec $\lambda \in \mathbb{R}$.

3. noyau et image

Soit ϕ un morphisme d'un groupe (G_1, \star_1) vers un groupe (G_2, \star_2) . Le noyau de ϕ , noté $\ker(\phi)$ est le sous-ensemble suivant de G_1 .

$$\ker(\phi) = \{x \in G_1 : \phi(x) = e_2\}.$$

Quant à l'image, il s'agit de l'image d'une application :

$$\text{Im}(\phi) = \{y \in G_2 : (\exists x \in G_1)(y = \phi(x))\}.$$

Propriété 2 Soit ϕ un morphisme d'un groupe (G_1, \star_1) vers un groupe (G_2, \star_2) . Alors

1. $\ker(\phi)$ est un sous-groupe de G_1 ;
2. $\text{Im}(\phi)$ est un sous-groupe de G_2 .

C'est un cas particulier d'une situation générale.

Exercice. Soit ϕ un morphisme d'un groupe (G_1, \star_1) vers un groupe (G_2, \star_2) . Soient H_1 un sous-groupe de G_1 ; H_2 un sous-groupe de G_2 . Etablir les propriétés suivantes.

1. $\phi^{-1}(H_2)$ est un sous-groupe de G_1 ;
2. $\phi(H_1)$ est un sous-groupe de G_2 .

En quoi est-ce une situation plus générale que celle décrite dans la propriété précédente ?

EXEMPLE :

1. Soit $\phi : \mathbb{R} \rightarrow \mathbb{R}$ définie par $\phi(x) = 2\pi x$. L'application ϕ est un morphisme de $(\mathbb{R}, +)$ vers $(\mathbb{R}, +)$ (le vérifier). De plus $\phi(\mathbb{Z}) = 2\pi\mathbb{Z}$. On retrouve à l'aide de l'exercice précédent le fait que $2\pi\mathbb{Z}$ est un sous-groupe de \mathbb{R} .
2. Soit $\phi : \mathbb{C} \rightarrow \mathbb{C}^*$ définie par

$$\phi(z) = \exp(\text{Re}(z)) (\cos(\text{Im}(z)) + i \sin(\text{Im}(z))).$$

L'application ϕ est un morphisme de $(\mathbb{C}, +)$ vers (\mathbb{C}^*, \times) . De plus, $\ker(\phi) = 2\pi\mathbb{Z}$ et $\text{Im}(\phi) = \mathbb{C}^*$.

Ainsi, ϕ est surjective et on trouve que $2\pi\mathbb{Z}$ est un sous-groupe de $(\mathbb{C}, +)$.

⁸on dit alors que le morphisme est continu

4. *isomorphisme*

La détermination du noyau caractérise l'injectivité. Plus précisément.

Propriété 3 Soit ϕ un morphisme d'un groupe (G_1, \star_1) vers un groupe (G_2, \star_2) . Les propriétés suivantes sont équivalentes.

1. ϕ est injective.
2. $\ker(\phi) = \{e_1\}$.

Définition 5 Un isomorphisme ϕ d'un groupe (G_1, \star_1) vers un groupe (G_2, \star_2) est un morphisme bijectif de (G_1, \star_1) vers (G_2, \star_2) .

Propriété 4 Soit ϕ un isomorphisme d'un groupe (G_1, \star_1) vers un groupe (G_2, \star_2) . Alors la réciproque ϕ^{-1} est un isomorphisme de (G_2, \star_2) vers (G_1, \star_1) .

EXEMPLE : L'application \exp est un isomorphisme de $(\mathbb{R}, +)$ vers (\mathbb{R}_+^*, \times) . On en déduit que la réciproque de \exp est un isomorphisme de (\mathbb{R}_+^*, \times) vers $(\mathbb{R}, +)$. On retrouve ainsi que \ln est un (iso)morphisme du groupe (\mathbb{R}_+^*, \times) vers le groupe $(\mathbb{R}, +)$.