Université d'Avignon - Faculté des sciences — Année 2015-2016
S5 - Algèbre générale

CH 1) Groupes

1. Définitions

Définition 1.1. *Un groupe est la donnée d'un ensemble G et d'une loi de composition interne $*$, c'est-à-dire une application $G \times G \to G$ qui à deux éléments x, y associent $x * y$, telle que :*

– (associativité) : $x * (y * z) = (x * y) * z$ pour tout x, y, z dans G.

–(existence d'un élément neutre) : il existe un élément e de G tel que pour tout x dans G on a $e * x = x * e = x$.

– (tout élément a un inverse) : pour tout x dans G il existe un élément x' dans G (appelé un inverse de x) tel que $x * x' = x' * x = e$.

L'opération $*$ est appelée *loi du groupe.*

L'associativité permet d'enlever les parenthèses dans l'écriture d'un "produit" de trois termes sans qu'il n'y ait ambigité de sens :

$$x * y * z = x * (y * z) = (x * y) * z$$

L'élément neutre est unique, et l'inverse de chaque élément est unique.

Définition 1.2. *Un groupe $(G, *)$ est **commutatif** (on dit aussi **abélien**) si l'ordre des éléments dans le produit n'a aucune importance, i.e. :*

$$\forall x, y \in G, \quad x * y = y * x$$

Enfin, il sera aussi pertinent de s'intéresser au cardinal du groupe (i.e., lorsque le groupe est fini en tant qu'ensemble, le nombre de ses éléments).

Définition 1.3. *Le cardinal du groupe $(G, *)$ est appelé **ordre** du groupe.*

Il y a aussi une contraction de langage usuelle et pratique :

Définition 1.4. *Un groupe **fini** est un groupe dont l'ordre est fini.*

Définition 1.5. *Soient $(G, *)$, $(G', *')$ deux groupes. Une application $f : G \to G'$ est un **(homo)morphisme de groupes** si :*

$$\forall x, y \in G, \ f(x * y) = f(x) *' f(y)$$

*Un morphisme bijectif est un **isomorphisme.** Si $(G, *) = (G', *')$, un morphisme $f : G \to G$ est un **endomorphisme.** Un endomorphisme bijectif est un **automorphism.***

*Le **noyau** de f, noté $\mathrm{Ker}(f)$, est l'image réciproque $f^{-1}(\{1\})$ de l'élément neutre de G'.*

Proposition 1.6. *f est injective si et seulement si son noyau $\mathrm{Ker}\, f$ est trivial, i.e. réduit à $\{1\}$.* □

2. Des exemples de groupe :

2.1. **Les nombres.** Chacune des données $(G, *)$ suivantes est un groupe commutatif de loi $*$:

(1) $(\mathbb{Z}, +)$
(2) $(\mathbb{Q}, +)$
(3) $(\mathbb{R}, +)$
(4) $(\mathbb{C}, +)$
(5) $(\mathbb{Q} \setminus \{0\}, \times)$
(6) $(\mathbb{R} \setminus \{0\}, \times)$
(7) $(\mathbb{C} \setminus \{0\}, \times)$

2.2. **Matrices inversibles.** Pour tout entier n, soit $\mathrm{GL}(n, \mathbb{R})$ (respectivement $\mathrm{GL}(n, \mathbb{C})$) l'ensemble des matrices à coefficient réel (respectivement complexe) à determinant non-nul. Alors, $\mathrm{GL}(n, \mathbb{R})$ et $\mathrm{GL}(n, \mathbb{C})$ muni de la loi de multiplication des matrices est un groupe, dont l'élément neutre est la matrice identité : la matrice diagonale n'ayant que des 1 sur la diagonale.

2.3. **Groupe des permutations.** Il s'agit du groupe $(\mathcal{S}(E), \circ)$ des bijections d'un ensemble E dans lui-même, muni de la loi de composition des fonctions.

3. Groupes arithmétiques

Soit n un entier. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des entiers modulo n.

Prosaïquement, on peut définir dans un premier temps $\mathbb{Z}/n\mathbb{Z}$ comme étant l'ensemble des entiers compris entre 0 et $n-1$. On définit alors la loi suivante sur $\mathbb{Z}/n\mathbb{Z}$: le "produit" entre deux éléments i et j est l'entier $i \bar{+} j$, reste modulo n de $i + j$.

Lemme 3.1. *La loi $\bar{+}$ sur $\mathbb{Z}/n\mathbb{Z}$ est associative.*

Démonstration. Soient i, j, k trois éléments de $\mathbb{Z}/n\mathbb{Z}$. Il existe deux entiers q_{ij} et q_{jk} tels que :

$$i + j = nq_{ij} + i \bar{+} j \text{ et } j + k = nq_{jk} + j \bar{+} k$$

Notons r_1 l'élément $(i \bar{+} j) \bar{+} k$ de $\mathbb{Z}/n\mathbb{Z}$. Il est défini par le fait qu'il est compris entre 0 et $n-1$, et que $(i \bar{+} j) + k - r_1$ est divisible par n. Donc $(i + j - nq_{ij}) + k - r_1 = (i + j + k) - r_1 - nq_{ij}$ est divisible par n. On en déduit que r_1 est le reste de la division de $i + j + k$ par n.

De la même manière, r_2 est le reste modulo n de $i + (j \bar{+} k) = i + j + k - nq_{jk}$, et donc aussi le reste modulo n de $i + j + k$. Il est donc égal à $i \bar{+} (j \bar{+} k)$. □

Il est par ailleurs facile de voir que 0 est un élément neutre de $\mathbb{Z}/n\mathbb{Z}$ (et donc l'élément neutre de $\mathbb{Z}/n\mathbb{Z}$), et que pour tout i dans $\mathbb{Z}/n\mathbb{Z}$, la différence $n - i$, qui est bien comprise entre 0 et $n - 1$, est un/l' inverse de i pour la loi $\bar{+}$. Celle-ci est donc bien une loi de groupe.

Définition 3.2. *On appelle groupe cyclique d'ordre n le groupe $(\mathbb{Z}/n\mathbb{Z}, \bar{+})$.*

Nous verrons plus tard le sens du mot *cyclique*, pour l'instant, voyons-le comme un simple adjectif dans la dénomination de $(\mathbb{Z}/n\mathbb{Z}, \bar{+})$.

Exercice 3.3. *Montrer que $(\mathbb{Z}/n\mathbb{Z}, \bar{+})$ est commutatif.*

4. Table de multiplication dans un groupe

Pour les groupes finis il y a un moyen commode de représenter la loi de groupe sous la forme d'un tableau, dont les colonnes et les lignes sont indexées par les éléments du groupe, et où la case de la ligne x et de la colonne y contient le produit $x * y$.

Voici en exemple la table associée au groupe $(\mathbb{Z}/4\mathbb{Z}, \bar{+})$:

$\bar{+}$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Remarque 4.1. *On omet souvent les lignes et colonnes indexées par l'élément neutre e, puisque leur contenu est sans surprise.*

On peut remarquer qu'un groupe est commutatif si et seulement si le tableau correspondant est symétrique par rapport à la diagonale.

Exercice 4.2. *On voit dans cet exemple que tout élément de G apparaît une et une seule fois dans chaque colonne, ainsi que dans chaque ligne. Est-ce un hasard ?*

5. Quelques conventions d'écriture

5.1. **Sur l'écriture de la loi de groupes.** Rappelons qu'un groupe est un ensemble G muni d'une loi (de groupe) que nous avons noté $*$ dans la feuille précédente. Mais une fois la notion acquise, lorsqu'il n'y a pas d'ambiguité à craindre, il est avantageux d'omettre le signe $*$, et de prendre l'habitude de noter tout simplement xy le produit $x * y$. On note alors 1 l'élément neutre, x^{-1} l'inverse d'un élément x du groupe.

5.2. **Parenthèses et puissances.** Nous avons déjà observé que l'associativité de la loi de groupe permet de laisser tomber les parenthèses lorsqu'on écrit le produit de trois éléments :

$$x(yz) = (xy)z = xyz$$

Ceci s'étant à un produit quelconque de n éléments du groupe : si x_1, x_2, ... , x_n sont n éléments du groupe, $x_1(x_2(...(x_{n-1}x_n)...))$ est égal à $((...((x_1x_2)x_3)....)x_n)$, ainsi qu'à toutes les expressions obtenus en insérant des parenthèses de manière convenable. Par exemple, pour $n = 4$:

$$x(y(zt)) = (xy)(zt) = ((xy)z)t = (x(yz))t = x((yz)t)$$

On peut donc toujours omettre les parenthèses et noter tout simplement $x_1x_2...x_n$ le produit de n éléments du groupe : le résultat sera le même, quelque soit la manière de placer des parenthèses (par contre, on ne peut pas modifier l'ordre d'apparition des termes x_i, sauf dans le cas particulier des groupes abéliens).

Lorsque tous les x_i sont égaux, on note sobrement x^n le produit de x par lui-même n fois :

$$x^n = xx...x$$

On l'appelle **puissance n-ième de x.**

Remarquons que cette notation s'étend aux n entiers négatifs : tout d'abord, nous avons déjà convenu que x^{-1} désigne l'inverse de x ; ensuite, on définit pour n entier strictement positif x^{-n} comme étant $(x^{-1})^n$. Pour le cas $n = 0$, on pose $x^0 = 1$.

Exercice 5.1. *Montrer (par récurrence) que pour tout entier n, x^{-n} est l'inverse de x^n.*

Exercice 5.2. *Montrer que pour toute paire d'entiers p, q, et tout x dans le groupe G on a :*

$$x^p x^q = x^{p+q} \text{ et } (x^p)^q = x^{pq}$$

5.3. **Groupes abéliens.** Quand le groupe est abélien, il est pertinent d'adopter la convention suivante : on note 0 l'élément neutre (au lieu de 1), et on note + la loi de groupe. L'inverse d'un élément x est alors noté $-x$, et sa puissance n-ième est notée nx (ceci inclut donc le cas $n < 0$, ainsi que le cas $n = 0 : 0x$ est par convention l'élément neutre 0).

6. Sous-groupes

6.1. **Définition.** Soit G un groupe.

Définition 6.1. *Soit H une partie non vide de G. On dit que H est un sous-groupe de G si :*

- *H est stable par multiplication : si x, y sont deux éléments de H, alors xy appartient à H,*
- *H est stable par inversion : si x est un élément de H, son inverse x^{-1} est aussi un élément de H.*

Soit H un sous-groupe de G. Comme H est non-vide, il contient un élément x. Comme il est stable par inversion, x^{-1} appartient à H, et comme il est stable par composition, il contient aussi l'élement neutre 1 (car $1 = xx^{-1}$).

Proposition 6.2. *Si $f : G \longrightarrow G'$ est un morphisme de groupes alors son noyau $Kerf$ est un sous-groupe de G.*

Lemme 6.3. *Soit H un sous-groupe de G. Pour tout x dans H et tout entier n, la puissance x^n appartient à H.*

Démonstration. Récurrence sur n pour les entiers n positifs. Pour les entiers n négatifs, appliquer à l'inverse x^{-1}. □

Proposition 6.4. *Soit H un sous-groupe de G. Muni de la même opération que G, H est un groupe.*

Démonstration. L'opération dans H est bien définie puisque H est stable par multiplication ; elle est associative puisqu'elle l'est déjà dans G. Nous avons déjà vu que l'élément neutre 1 de G appartient à H, et il continue d'y jouer le rôle d'élément neutre ! Enfin, pour tout x dans H, l'inverse x^{-1}, qui est dans H, est un inverse de x dans H. □

Proposition 6.5. *Soient H, H' deux sous-groupes de G. Alors, si elle est non vide, l'intersection $H \cap H'$ est un sous-groupe de G.*

Démonstration. Soient x, x' deux éléments de $H \cap H'$. Comme ils appartiennent tous les deux au sous-groupe H, on a $xy \in H$ et $x^{-1} \in H$. De même, comme ils apprtiennent à H', $xy \in H'$ et $x^{-1} \in H'$. Donc xy et x^{-1} appartiennent à $H \cap H'$. □

Exercice 6.6. *$H \cap H'$ est-il un sous-groupe de H ?*

6.2. **Exemples.** Beaucoup d'exemples de groupes s'obtiennent en tant que sous-groupe d'un groupe plus gros. Celà permet de s'épargner la fastidueuse vérification de l'associativité de la loi d'opération : si G est un groupe, alors pour vérifier qu'une partie H de G soit un (sous-)groupe, il "n'y a plus qu'à" vérifier qu'elle est stable par produit et inversion.

6.2.1. *Réels positifs.* Nous avons déjà observé que $(\mathbb{R} \setminus \{0\}, \times)$ est un groupe. Or, le produit de deux nombres réels positifs est positif, et l'inverse $1/x$ d'un nombre réel positif est positif. Donc, $(]0, +\infty[, \times)$ est un groupe, puisqu'un sous-groupe de $(\mathbb{R} \setminus \{0\}, \times)$.

6.2.2. *Nombres complexes de module* 1 *(le cercle).* Nous savons que $(\mathbb{C} \setminus \{0\}, \times)$ est un groupe. Soit $\mathbb{U}$ l'ensemble des nombres complexes z de module $|z|$ égal à 1. Alors, si z, z' appartiennent à $\mathbb{U}$, le produit zz' et l'inverse $|1/z|$ appartiennent l'un et l'autre à $\mathbb{U}$. En effet : $|zz'| = |z||z'| = 1.1 = 1$, et $|1/z| = 1/|z| = 1/1 = 1$. Donc $\mathbb{U}$ est un (sous-)groupe.

Remarquons que l'inverse d'un élément z de $\mathbb{U}$ est le conjugué $\bar{z}$ puisque $z\bar{z} = |z|^2 = 1$.

6.2.3. *Racines de l'unité.* Pour tout entier $n \geq 2$, soit $\mathbb{U}_n$ l'ensemble des racines n-ième de l'identité, c'est à dire l'ensemble des nombres complexes z tels que $z^n = 1$. Si $z \in \mathbb{U}_n$, alors $|z|^n = 1$, donc $|z| = 1$. Il s'ensuit que $\mathbb{U}_n$ est une partie de $\mathbb{U}$. De plus, si x et y sont deux éléments de $\mathbb{U}_n$, alors $(xy)^n = x^n y^n = 1$ et $(1/x)^n = 1/x^n = 1$, donc xy et x^{-1} appartiennent à $\mathbb{U}_n$. Ainsi, $\mathbb{U}_n$ est un sous-groupe de $\mathbb{U}$.

Notons que les éléments de $\mathbb{U}_n$ sont les nombres complexes $x = re^{i\theta}$ tels que $1 = x^n = r^n e^{ni\theta}$. Donc $r = 1$ (c'est à dire que x appartient à $\mathbb{U}$, ce qu'on avait déjà remarqué), et $n\theta$ est un multiple de 2π. Ainsi, les éléments de $\mathbb{U}_n$ sont les nombres complexes de la forme $e^{i2k\pi/n}$ avec $k \in \{0, 1, ..., n-1\}$. En particulier, $\mathbb{U}_n$ est d'ordre fini n.

On remarque aussi que $e^{i2k\pi/n}$ est la puissance k-ième de $e^{i2\pi/n}$. En d'autres termes, si on pose $\zeta = e^{i2\pi/n}$, les éléments de $\mathbb{U}_n$ sont 1, ζ, ζ^2, ... , ζ^{n-1}.

Exercice 6.7. *Montrer que l'application de $\mathbb{Z}/n\mathbb{Z}$ vers $\mathbb{U}_n$ qui envoie k sur $e^{i2k\pi/n}$ est un isomorphisme de groupes.*

6.2.4. *Le groupe spécial linéaire.* Dans la feuille précédente, nous avons vu le groupe des matrices inversibles $\mathrm{GL}(n, K)$ pour $n \geq 2$, où K désigne $\mathbb{R}$ ou $\mathbb{C}$. Soit $\mathrm{SL}(n, K)$ la partie de $\mathrm{GL}(n, K)$ formé des éléments de déterminant 1 (rappelons que $\mathrm{GL}(n, K)$ est l'ensemble des matrices de déterminant **non nul**. Alors, si A, B sont deux éléments de $\mathrm{SL}(n, K)$:

$$\det(AB) = \det(A)\det(B) = 1.1 = 1,$$

et

$$\det(A^{-1}) = 1/\det(A) = 1.$$

Donc $\mathrm{SL}(n, K)$ est un sous-groupe de $\mathrm{GL}(n, K)$.

6.2.5. *Sous-groupes de* $(\mathbb{Z}, +)$. Soit p un entier naturel, et $n\mathbb{Z}$ l'ensemble des entiers divisibles par n. On considère $(\mathbb{Z}, +)$ comme un groupe abélien, on note donc l'opération de groupe par $+$, et l'élément neutre est bien 0. Si n divise les entiers x et y, alors il divise leur somme $x + y$ ainsi que l'"inverse" (pour la loi de groupe) $-x$. Donc $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

Théorème 6.8. *Tout sous groupe de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$ avec $n \in \mathbb{Z}$.* □

6.3. **Sous-groupe engendré par une partie.** Soit G un groupe, et A une partie de G. Ce n'est pas forcément un sous-groupe. Cependant :

Proposition 6.9. *Il existe un sous-groupe $\langle A \rangle$ de G tel que :*
- *$\langle A \rangle$ contient A,*
- *Tout sous-groupe de G qui contient A contient aussi $\langle A \rangle$.*

Démonstration. Il suffit de prendre l'intersection de tous les sous-groupes de G contenant A. □

Définition 6.10. *$\langle A \rangle$ est appelé le sous-groupe engendré par A.*

Il existe une autre manière de définir $\langle A \rangle$, beaucoup moins abstraite :

Lemme 6.11. *Le sous-groupe engendré par A est l'ensemble des produits d'éléments de A ou d'inverses d'éléments de A.* □

Corollaire 6.12. *Le sous-groupe engendré par un élément g est l'ensemble des puissances de g :*

$$\langle g \rangle = \{g^n \ / \ n \in \mathbb{Z}\}$$

7. Quotient par un sous-groupe

Soit $(G, *)$ un groupe, et $H \subset G$ un sous-groupe.

Définition 7.1. *Une **classe à gauche de** $(G, *)$ **modulo** H est un sous-ensemble de G de la forme :*

$$gH = \{gh \ / \ h \in H\}$$

*où g est un élément de G. Une **classe à droite de** $(G, *)$ **modulo** H est un sous-ensemble de G de la forme :*

$$Hg = \{hg \ / \ h \in H\}$$

Lemme 7.2. *L'ensemble des classes à gauche modulo H est une partition de G.* □

En d'autres termes :

Lemme 7.3. *La relation $\sim_H$ sur G définie par :*

$$(g \sim_H g') \Leftrightarrow (gH = g'H) \Leftrightarrow g^{-1}g' \in H)$$

est une relation d'équivalence. □

Exemple 7.4. *Si $G = \mathbb{Z}$ et $H = n\mathbb{Z}$, alors :*

$$(k \sim_H l) \Leftrightarrow k \equiv l[n]$$

Dans ce cas, une classe à gauche (ou à droite !) est une classe de congruence modulo n.

On note G/H l'espace quotient, *i.e.* l'ensemble des classes à gauche.

Cet espace admet parfois une structure naturelle de groupe.

En fait, $G \times G$ admet une relation d'équivalence naturelle, la loi produit, définie par :

$$(g_1, g_2) \approx_H (g_1', g_2') \Leftrightarrow [(g_1 \sim_H g_1') \text{ et } (g_2 \sim_H g_2')]$$

Lemme 7.5. *L'application $* : G \times G \to G$ est **compatible** avec les relations d'équivalence $\approx_H$ et $\sim_H$ si et seulement si H est un **sous-groupe distingué** de G, i.e. si et seulement si :*

$$\forall h \in H, \ \forall g \in G, \ ghg^{-1} \in H$$

Démonstration. Dire que $* : G \times G \to G$ est compatible avec $\approx_H$ et $\sim_H$ signifie que, si $(g_1, g_2) \approx_H (g_1', g_2')$, alors $g_1 g_2 \sim_H g_1' g_2'$. Or :

– *Si H est distingué dans G :* soit g_1, g_2, g_1', g_2' dans G tels que $(g_1, g_2) \approx_H (g_1', g_2')$. Alors, il existe h_1, h_2 dans H tels que $g_1' = g_1 h_1$ et $g_2' = g_2 h_2$. On a :

$$g_1' g_2' = g_1 h_1 g_2 h_2 = g_1 (g_2 g_2^{-1}) h_1 g_2 h_2 = g_1 g_2 (g_2^{-1} h_1 g_2) h_2 = g_1 g_2 h_3$$

où $h_3 = (g_2^{-1} h_1 g_2) h_2$. Comme H est distingué dans G, $h' = g_2^{-1} h_1 g_2$ appartient à H, et comme H est un sous-groupe, $h_3 = h' h_2$ est dans H. Donc $g_1 g_2 \sim_H g_1' g_2'$.

– *Si $*$ est compatible :* Soient $h \in H$;, $g \in G$. Alors $(1, g^{-1}) \approx_H (h, g^{-1})$. Comme $*$ est compatible, on a $g^{-1} = 1 * g^{-1} \sim_H hg^{-1}$, donc $ghg^{-1} \in H$. □

Notation : l'écriture $H \lhd G$ signifie que H est un sous-groupe distingué de G (on dit aussi **sous-groupe normal de G.**

Proposition 7.6. *Si $H \lhd G$, alors l'application induite $*' : G/H \times G/H \to G/H$ est une loi de groupe. De plus, la surjection canonique $p_H : G \to G/H$ est un morphisme de groupes.* □

Exercice 7.7. *On considère le cas où G est le groupe $\mathbb{Z}$ et H le sous-groupe $n\mathbb{Z}$ avec $n \in \mathbb{N}^*$.*
- *Montrer : $H \lhd G$.*
- *Montrer que G/H est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

Théorème 7.8 (Factorisation canonique)**.** *Soit $(G, *)$ un groupe, soit $H \lhd G$ un sous-groupe distingué, $(G', *')$ un groupe et $f : G \to G'$ un morphisme de groupes. Alors, il existe un morphisme de groupes $g : G/H \to G'$ tel que $f = g \circ p_H$ si et seulement si $H \subset \operatorname{Ker} f$.*

Dans ce cas, g est unique et est appelé ***passage au quotient de f modulo H.***

7.1. Ordre de sous-groupes.

Théorème 7.9 (de Lagrange)**.** *Soit $H \subset G$ un sous-groupe. On suppose que l'ordre de G est fini. Alors, l'ordre de H divise l'ordre de G.*

Démonstration. On a la formule :

$$|G| = |H|[G : H]$$

où $[G : H]$ (indice de H dans G) est le cardinal de l'ensemble quotient G/H. En effet, les classes à gauche, qui forment une partition de G, ont toutes le même nombre $|H|$ d'éléments. □

Corollaire 7.10. *Dans un groupe fini, l'ordre d'un élément g (i.e. l'ordre du sous-groupe $\langle g \rangle$) divise $|G|$.*

On rappelle que l'ordre d'un élément est aussi :
- le plus petit entier k tel que $g^k = 1$,
- le seul entier qui divise tous les entiers k tels que $g^k = 1$.