ALGÈBRE GÉNÉRALE

JEAN-PAUL CALVI

Références

[1] Burn, R.P. *Groups, a path to geometry*, Cambridge university press, Cambridge, 1985.
[2] Kargapolov, M. et Merzliakov I. *Eléments de la théorie des groupes*, Mir, Moscou, 1985.
[3] Kostrikin, A. *Introduction à l'algèbre*, Mir, Moscou, 1981.
[4] Kurosh, A. *Cours d'algèbre supérieure*, Mir, Moscou, 1973.

1. Introduction à la théorie des groupes

§ 1. La structure de groupe.

1.1. *Lois internes.*

1.2. *Associativité, commutativité.* Exemple de loi non associative, non commutative.

1.3. *À quoi sert l'associativité ? la commutativité ?*

Théorème 1.1. *Lorsque la loi $*$ sur E est* associative*, on peut écrire les produits sans qu'il soit nécessaire de placer les parenthèses (autrement dit le résultat ne dépend pas de la manière dont sont placées les parenthèses). En particulier, pour $a \in E$ et $n \in \mathbb{N}^\star$, on peut définir*

$$a^n =_{def} \underbrace{a * a * \cdots * a}_{n \text{ fois}}$$

et on a les relations

$$\begin{cases} a^n * a^m &= a^{n+m} \qquad (n,m \in \mathbb{N}^\star) \\ (a^n)^m &= a^{nm} \qquad (n,m \in \mathbb{N}^\star) \end{cases}$$

Date: 3 avril 2006.

Merci de signaler les erreurs et les imprécisions en écrivant à *calvi@picard.ups – tlse.fr*.

Enfin, si, en plus d'être associative, la loi $*$ est aussi commutative *on peut permuter les éléments de $a_1 * a_2 * \cdots * a_n$ de manière arbitraire sans modifier le résultat.*

1.4. *Elément neutre pour une loi interne.* Soit $*$ une loi interne sur un ensemble (non vide) E. On dit qu'un élément $e \in E$ est **élément neutre** (pour $*$) si

$$\forall a \in E \qquad a * e = e * a = a.$$

Par exemple 0 est élément neutre de l'addition dans $\mathbb{N}$.

Théorème 1.2. *Une loi interne admet au plus un élément neutre.*

1.5. *Définition d'un groupe.* Un ensemble G muni d'une loi interne $*$ est appelé groupe si

(i) La loi $*$ est associative et admet un élément neutre, noté e — ou, s'il faut préciser, e_G.
(ii) Pour tout $g \in G$, il existe un élément $y \in G$, appelé **élément symétrique** de g tel que

$$g * y = y * g = e.$$

On parle alors du **groupe** $(G,*)$ ou — lorsqu'il n'y a pas d'ambiguïté sur la loi $*$ — simplement du groupe G. Lorsque la loi $*$ est commutative on dit que $(G,*)$ est un **groupe commutatif** ou encore un **groupe abélien**. Lorsque G contient un nombre infini d'éléments, on dit que G est infini. Dans le cas contraire, on dit que G est fini. Le **cardinal** (c'est-à-dire le nombre d'éléments) d'un groupe G, appelé **ordre**, est noté $\mathrm{card}(G)$ ou $o(G)$ ou $|G|$.

1.6. *L'élément symétrique.*

Théorème 1.3. *Dans un groupe tout élément admet toujours un* unique *élément symétrique.*

L'unique élément symétrique de g est noté g^{-1}. On a

(i) $e^{-1} = e$. L'élément neutre est son propre symétrique.
(ii) $(g^{-1})^{-1} = g$.
(iii) $(g * g')^{-1} = g'^{-1} * g^{-1}$. Le symétrique d'un produit est le produit *inverse* des symétriques.
(iv) Plus généralement $(g_1 * g_2 * \cdots * g_n)^{-1} = g_n^{-1} * g_{n-1}^{-1} * \ldots g_1^{-1}$.

En particulier on a $(g^n)^{-1} = (g^{-1})^n$ $(n \in \mathbb{N}^\star)$. On note alors

$$g^{-n} =_{def} (g^n)^{-1}$$

ce qui permet de définir g^m pour $m \in \mathbb{Z}$ en convenant $g^0 = e$. Dans ces conditions on a les relations.

$$(g^m)^{m'} = g^{mm'} \quad \text{et} \quad g^m * g^{m'} = g^{m+m'} \qquad (m,m' \in \mathbb{Z}).$$

1.7. *Sept exemples de groupes.*

a) (**U**,.). C'est l'ensemble des nombres complexes de module 1 muni de la *multiplication des nombres complexes*. L'élément neutre est 1. C'est un groupe abélien infini.

b) ($\mathbb{Z}$,+). L'ensemble des entiers relatifs muni de *l'addition (habituelle)*. L'élément neutre est 0, le symétrique d'un élément est son opposé. C'est un groupe abélien infini.

c) ($\mathbf{U}_n$,.) où $n \in \mathbb{N}^\star$. L'ensemble des racines n-ième de l'unité (dans $\mathbb{C}$). L'élément neutre est 1. C'est un groupe abélien fini. Il contient n éléments.

d) ($\mathbf{GL}_n(\mathbb{K})$,.). L'ensemble des matrices inversibles à n lignes et n colonnes à coefficients dans $\mathbb{K} = \mathbb{C},\mathbb{R}$ ou $\mathbb{Q}$, muni de l*a multiplication des matrices*. L'élément neutre est la matrice identité. L'élément symétrique est la matrice inverse. C'est un groupe non abélien (dès que $n > 1$) infini.

e) ($\mathbf{S}(\Omega)$,$\circ$). Ω est un ensemble quelconque non vide et $\mathbf{S}(\Omega)$ est l'ensemble des bijections de Ω sur Ω muni de *la composition des fonctions*. L'élément neutre est l'application identité, le symétrique est la bijection réciproque. C'est un groupe infini lorsque Ω est infini et il a pour cardinal $n!$ lorsque Ω est formé de n éléments. Il est non abélien dès que $\mathrm{card}(\Omega) > 2$. Ce groupe est étudié en détail par la suite.

f) ($\mathbf{Is}(P)$,$\circ$). L'ensemble des isométries affines du plan euclidien P muni de la composition des fonctions. C'est un groupe infini non abélien contenant en particulier les translations, les rotations, les réflexions (symétries orthogonales).

g) **Produit de 2 groupes** Soient $(G_1,*_1)$ et $(G_2,*_2)$ deux groupes. On définit une loi $\star_3$ sur $(G_1 \times G_2)$ par la relation suivante :

$$(g_1,g_2) *_3 (g_1',g_2') = (g_1 *_1 g_1',g_2 *_2 g_2').$$

Alors $(G_1 \times G_2,*_3)$ est un groupe, appelé le produit (ou produit direct) de $(G_1,*_1)$ par $(G_2,*_2)$. Lorsque $(G_1,*_1) = (G_2,*_2)$ on parle du groupe G^2 et on garde pour la loi de G^2 la même notation que pour la loi de G. On peut plus généralement former le produit de n groupes et lorsque tous les groupes coïncident on obtient G^n.

1.8. *Notation additive, notation multiplicative.*

§ 2. **Sous-Groupes.**

2.1. *Définition et notations.* Soient $(G,*)$ un groupe et H un sous-ensemble *non vide* de G. On dit que H est un sous-groupe de G si

(i) Pour tous $x,y \in H$ on a $x * y \in H$

(ii) Pour tout $x \in H$, $x^{-1} \in H$

(Cela signifie que la restriction de $*$ à $H \times H$ donne une loi interne de H et que $(H,*)$ est alors lui-même un groupe.) Les deux conditions ci-dessus peuvent être remplacées par

(iii) Pour tous $x,y \in H$ on a $x * y^{-1} \in H$

La notation $H < G$ est employée pour dire *H est sous-groupe de G*. Lorsqu'on n'exclut pas la possibilité que H soit égal à G on écrit $H \leq G$.

2.2. *Six exemples de sous-groupes.*

a) $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < (\mathbb{C},+)$.

b) $m\mathbb{Z} < (\mathbb{Z},+)$.

c) $\mathbf{U}_n < \mathbf{U} < (\mathbb{C}^\star,.)$.

d) $\mathbf{GL}_n(\mathbb{Q}) < \mathbf{GL}_n(\mathbb{R}) < (\mathbf{GL}_n(\mathbb{C}),\cdot)$.

e) $\mathbf{T} < \mathbf{Is}(P) < (\mathbf{S}(P),\circ)$ où $\mathbf{T}$ l'ensemble des **translations** du plan euclidien.

f) $\mathcal{R}_A < (\mathbf{Is}(P),\circ)$ où $\mathcal{R}_A$ l'ensemble des **rotations** de centre A du plan euclidien.

2.3. *Intersections de sous-groupes.*

Théorème 1.4. *Soient $(G,*)$ un groupe et $\mathcal{F}$ une famille non vide de sous-groupes de G ($\mathcal{F}$ peut contenir un nombre fini ou infini de sous-groupes). Si I est l'intersection de tous les éléments de $\mathcal{F}$, autrement dit $I = \cap_{H\in\mathcal{F}} H$ alors I est lui-même un sous-groupe de G.*

2.4. *Sous-groupe engendré par une partie.* Soit $(G,*)$ un groupe et A un sous-ensemble *non vide* de G. On appelle sous-groupe engendré par A le sous-groupe

$$\langle A\rangle = \cap_{H\in\mathcal{S}} H$$

où $\mathcal{S}$ est l'ensemble de tous les sous-groupes de G qui contiennent A. Cet ensemble n'est pas vide car il contient G lui-même et la formule ci-dessus est par conséquent bien définie.

Théorème 1.5. *Le sous-groupe $\langle A\rangle$ est le plus petit sous-groupe de G contenant A. Autrement dit, $\langle A\rangle$ est caractérisé par les deux conditions suivantes*

(i) *$\langle A\rangle$ est un sous-groupe de G contenant A.*

(ii) *Si H est un autre sous-groupe de G contenant A on a $\langle A\rangle \subset H$*

2.5. *Description des éléments d'un sous-groupe engendré.*

Théorème 1.6. *Soient $(G,*)$ un groupe, A un sous-ensemble non vide de G et $x \in \langle A\rangle$. Il existe $n \in \mathbb{N}^\star$ et des éléments $y_1,y_2,\ldots,y_n$ avec $y_i \in A$ ou $y_i^{-1} \in A$ pour $i = 1,2,\ldots n$ tels que $x = y_1 * y_2 * \cdots * y_n$.*

Pour bien des questions, on considère qu'on a déjà acquis une bonne connaissance du groupe G si on a pu exhiber un ensemble générateur *le*

plus petit possible car on peut alors décrire par la formule assez simple ci-dessus tous les éléments du groupe.

2.6. *Groupes cycliques, ordre d'un élément.* On dit qu'un groupe $(G,*)$ est cyclique s'il est engendré par un ensemble réduit à un seul élément i.e. $G = \langle\{a\}\rangle$. On note aussi pour simplifier $G = \langle a\rangle$.

Théorème 1.7. *Soit $(G,*)$ un groupe cyclique engendré par $a \in G$. Il y a deux possibilités.* Ou bien *a est d'ordre fini $d \in \mathbb{N}^\star$ et on a $G = \{a^i, i = 0,1,\dots d-1\}$* ou bien *$a$ n'est pas d'ordre fini (on dit alors qu'il est d'ordre infini) et $G = \{a^m, m \in \mathbb{Z}\}$. Dans chaque cas les éléments des ensembles indiqués sont deux à deux distincts.*

On remarquera que l'ordre d'un élément est égal au cardinal du groupe qu'il engendre. Les groupes cycliques sont tous abéliens[1].

2.7. *Quatre exemples de sous-groupes engendrés.*
a) $\langle m\rangle = m\mathbb{Z}$.
b) $\langle m,n\rangle = pgcd(m,n)\mathbb{Z}$.
c) $\mathbf{U}_n = \langle \exp(2i\pi/n)\rangle$.
d) On démontre en géométrie que toute isométrie du plan s'écrit comme la composée d'au plus *trois* réflexions (symétries orthogonales) on a donc

$$\mathbf{Is}(p) = \langle s_D : D \text{ droite du plan}\rangle.$$

§ 3. Morphismes.

3.1. *Definition.* Soit $(G,*)$ et $(G',\circ)$ deux groupes et φ une application de G dans $G' : \varphi : G \to G'$. On dit que φ est un **morphisme de groupe** (ou simplement un **morphisme**) lorsqu'elle vérifie

$$\varphi(a * b) = \varphi(a) \circ \varphi(b) \qquad (a,b \in G) \tag{1}$$

Terminologie...

(i) Les morphismes sont aussi appelés **homomorphismes**.
(ii) Lorsque le groupe de départ et le groupe d'arrivée sont les mêmes on parle d'**endomorphisme**.
(iii) Un morphisme bijectif est un **isomorphisme**.
(iv) Un isomorphisme de G dans lui-même s'appelle un **automorphisme**.

Si $\varphi : G \to G'$ est un isomorphisme alors l'application réciproque $\varphi^{-1} : G' \to G$ (qui existe puisque φ est bijective) est un isomorphisme.

Théorème 1.8. *L'image de l'élément neutre du groupe de départ par un morphisme est l'élément neutre du groupe d'arrivée.* $[\varphi(e_G) = e_{G'}]$.

1. Beaucoup d'auteurs appellent **groupe monogène** ce que nous avons appelé groupe cyclique infini et garde la dénomination de cyclique au seuls groupes finis.

Théorème 1.9. *Par un morphisme l'image du symétrique d'un élément est le symétrique de l'image de cet élément.* $[\varphi(g^{-1}) = [\varphi(g)]^{-1}.]$

Théorème 1.10. *Soient φ un morphisme de G dans G' et H un sous-groupe de G alors $\varphi(H)$ est un sous-groupe de G'. En particulier $\varphi(G)$ est un sous-groupe de G'.* $[H \leq G \Rightarrow \varphi(H) \leq G'.]$

3.2. *Morphismes et image des sous-groupes.*

Théorème 1.11. *Soient φ un morphisme de G dans G' et H un sous-groupe de G alors $\varphi(H)$ est un sous-groupe de G'. En particulier $\varphi(G)$ est un sous-groupe de G'.* $[H \leq G \Rightarrow \varphi(H) \leq G'.]$

Rappelons que $\varphi(H) \stackrel{\text{def}}{=} \{\varphi(h) : h \in H\}$ et s'appelle l'**image** de H par φ.

3.3. *Le noyau.* Soit φ un morphisme de $(G,*)$ dans $(G',\circ)$. On appelle **noyau** de φ et on note $\ker\varphi$ l'ensemble

$$\ker\varphi =_{def} \{g \in G \ : \ \varphi(g) = e_{G'}\} \tag{2}$$

Théorème 1.12. *Le noyau d'un morphisme est un sous-groupe du groupe de départ.* $[\ker\varphi \leq G]$.

Théorème 1.13. *Pour qu'un morphisme soit injectif il faut et il suffit que son noyau se réduise à l'élément neutre.* $[\varphi : G \stackrel{\text{morph.}}{\longrightarrow} G'$ injective $\Leftrightarrow \ker\varphi = \{e_G\}.]$

Corollaire. *Soient G et G' deux groupes finis de* même cardinal *et φ un morphisme de G dans G'. Pour que φ soit un isomorphisme il faut et il suffit que* $\ker\varphi$ *soit réduit à l'élément neutre.*

3.4. *Cinq exemples de morphismes.*

a)
$$\exp : \begin{array}{ccc}(\mathbb{R},+) & \longrightarrow & (\mathbb{R}^{\star+},.) \\ x & \longmapsto & \exp x.\end{array}$$

b)
$$\exp : \begin{array}{ccc}(\mathbb{R},+) & \longrightarrow & (\mathbf{U},.) \\ x & \longmapsto & \exp ix.\end{array}$$

c)
$$\det : \begin{array}{ccc}\mathbf{GL}_n(\mathbb{K}) & \longrightarrow & (\mathbb{K}^{\star},.) \\ A & \longmapsto & \det A\end{array}$$

d) Soit $(G,.)$ un groupe et $x \in G$. L'application
$$\phi_x : \begin{array}{ccc}(G,.) & \longrightarrow & (G,.) \\ g & \longmapsto & x^{-1}gx.\end{array}$$

est un automorphisme. Les automorphismes construits de cette manière s'appellent des **automorphismes intérieurs**. L'ensemble des automorphismes intérieurs, noté $\mathbf{Int}(G)$, forme lui-même un groupe lorsqu'on le munit de la loi de composition des applications.

e) Soit $(G,*)$ un groupe quelconque et $g \in G$. L'application suivante est un morphisme de groupe.

$$p_g : \begin{array}{ccc} (\mathbb{Z},+) & \longrightarrow & (G,*) \\ m & \longmapsto & g^m. \end{array}$$

§ 4. Relation d'équivalence définie par un sous-groupe.

4.1. *Définition.* Soient $(G,*)$ un groupe et H un sous-groupe de G. On définit la relation $\Re_H$ sur G par

$$x \Re_H y \overset{def}{\iff} x^{-1} * y \in H.$$

Théorème 1.14. *La relation $\Re_H$ est une relation d'équivalence sur G.*

Rappelons que la classe d'équivalence de $x \in G$, notée $\mathbf{cl}(x)$ ou $\overline{x}$ ou $\dot{x}$ est l'ensemble des éléments de G qui sont en relation avec x

$$\mathbf{cl}(x) = \{g \in G : x \,\Re_H\, g\}.$$

L'ensemble de toutes les classes d'équivalence est noté G/H et est appelé le **quotient** de G par H. Lorsque $y \in \mathbf{cl}(x)$, on dit que y est un **représentant** de $\mathbf{cl}(x)$. On a toujours que x est un représentant de $\mathbf{cl}(x)$ mais, en général, $\mathbf{cl}(x)$ admet beaucoup d'autres représentants.

4.2. *Description des classes d'équivalence (à gauche).* Dans la relation $\Re_H$ définie ci-dessus on a

$$\mathbf{cl}(x) = x * H$$

où $x * H = \{x * h : h \in H\}$.

4.3. *Le théorème de Lagrange.*

Théorème 1.15. *Soit $(G,*)$ un groupe fini et H un sous-groupe de G. Le cardinal de H divise le cardinal de G autrement dit $o(H)|o(G)$.*

Corollaire (de la démonstration)**.** *Sous les mêmes hypothèses, on a plus précisément*

$$\mathrm{card}(G) = \mathrm{card}(G/H) \times \mathrm{card}(H)$$

Corollaire. *Dans un groupe fini, l'ordre de tout élément divise l'ordre du groupe.* $[\forall x \in G, o(x)|o(G)]$

4.4. *Application à la caractérisation des groupes d'ordre premier.*

Théorème 1.16. *Tout groupe d'ordre premier $p > 1$ est cyclique et il est engendré par n'importe lequel de ses éléments différents du neutre.* $[\forall x \in G/\{e\}, G = \langle x \rangle]$

§ 5. **Groupes quotients.**

5.1. *Sous-groupes distingués.* Soit $(G,*)$ un groupe et H un sous-groupe de G. On dit que H est **distingué** dans G (ou **normal** dans G, ou encore **invariant**) s'il vérifie la propriété suivante

$$\forall x \in G \quad x^{-1} * H * x \subset H, \tag{3}$$

c'est-à-dire

$$\forall x \in G, \forall h \in H \quad x^{-1} * h * x \in H.$$

En réalité la condition (3) est équivalente à

$$\forall x \in G \quad x^{-1} * H * x = H, \tag{4}$$

qui est en apparence plus forte.

La notation $H \triangleleft G$ signifie que H est un sous-groupe distingué de G. Lorsqu'on n'exclut pas que H soit égal à G on écrit $H \trianglelefteq G$

5.2. *Trois exemples de sous-groupes distingués.*

a) Si $(G,*)$ est abélien alors n'importe lequel de ses sous-groupes est distingué dans G.

b) Si φ est un morphisme de $(G,*)$ dans $(T,\circ)$ alors $\ker\varphi$ est un sous-groupe distingué de G. [$\ker\varphi \trianglelefteq G$.]

c) Soit $H = \{\lambda Id : \lambda \in \mathbb{R}^\star\}$ où Id est la matrice identité dans $\mathbf{GL}_n(\mathbb{R})$. On a $H \trianglelefteq \mathbf{GL}_n(\mathbb{R})$.

5.3. *Compatibilité de $\Re_H$ avec la loi de G lorsque $H \trianglelefteq G$.* Soit $(G,*)$ un groupe et $H \trianglelefteq G$. La relation d'équivalence $\Re_H$ définie par le sous-groupe distingué H a la propriété remarquable d'être **compatible** avec la loi $*$. Cela signifie que, pour $g_1,g_2,r_1,r_2 \in G$,

$$\left.\begin{array}{ccc} g_1 & \Re_H & g_2 \\ r_1 & \Re_H & r_2 \end{array}\right\} \Rightarrow g_1 * r_1 \ \Re_H \ g_2 * r_2.$$

5.4. *Opération sur l'ensemble des classes. Groupe quotient. Projection canonique.* Soit $(G,*)$ un groupe et H un sous-groupe distingué de G. On rappelle que G/H désigne l'ensemble des classes d'équivalence de $\Re_H$. On peut définir une loi $\overline{*}$ sur G/H comme suit

$$\overline{*} : \begin{array}{ccc} G/H \times G/H & \longrightarrow & G/H \\ (\mathcal{C}_1\,,\mathcal{C}_2) & \longmapsto & \mathbf{cl}\left(\begin{array}{c}\text{n'importe quel}\\ \text{représentant de } \mathcal{C}_1\end{array} * \begin{array}{c}\text{n'importe quel}\\ \text{représentant de } \mathcal{C}_2\end{array}\right) \end{array} \tag{5}$$

Théorème 1.17. *Soit $(G,*)$ un groupe et $H \trianglelefteq G$, $(G/H,\overline{*})$ est un groupe.*

Théorème 1.18. *Soit $(G,*)$ un groupe et $H \trianglelefteq G$. L'application s définie par*

$$s : \begin{array}{ccc} (G,*) & \longrightarrow & (G/H,\overline{*}) \\ x & \longmapsto & \mathbf{cl}(x). \end{array}$$

est un morphisme de groupe. Il est surjectif. Son noyau est égal à H.

Le morphisme s s'appelle la **surjection** (ou **projection**) **canonique** de G sur G/H. On note parfois $s = s_H$.

5.5. *Le groupe $\mathbb{Z}/n\mathbb{Z}$.* Définition. Propriétés élémentaires.

Théorème 1.19. *Soit $n > 1$ et $a \in \mathbb{N}$. Pour que $\overline{a} = \mathbf{cl}(a)$ engendre $\mathbb{Z}/n\mathbb{Z}$ (i.e. $\mathbb{Z}/n\mathbb{Z} = \langle\overline{a}\rangle$) il faut et il suffit que a et n soient premiers entre eux.*

5.6. *Théorème d'isomorphisme.*

Théorème 1.20. *Soient G_1 et G_2 deux groupes et ϕ un homomorphisme de G_1 dans G_2. Il existe un* isomorphisme ν *de $G_1/\ker\phi$ sur $\phi(G_1)$ tel que $\phi = \nu \circ s$ où s est la surjection canonique de G_1 sur $G_1/\ker\phi$. On a donc*

$$G_1/\ker\phi \simeq \phi(G_1).$$

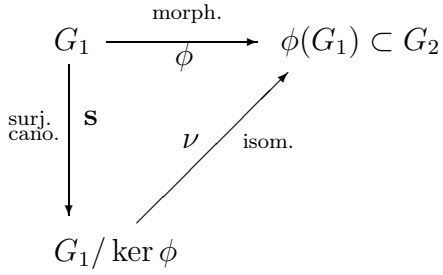

FIG. 1. *Schéma du théorème d'isomorphisme $\varphi = \mathbf{s} \circ \nu$*

5.7. *Trois exemples d'application du théorème d'isomorphisme.*
a) $\mathbb{R}/2\pi\mathbb{Z} \simeq \mathbf{U}$.
b) $\mathbf{GL}_n(\mathbb{K})/\mathbf{SL}_n(\mathbb{K}) \simeq \mathbb{K}^\star$.
c) Tout groupe cyclique fini d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

§ 6. **Le groupe symétrique.**

6.1. *Définitions.* Soit $\Omega = \{1,2,\ldots,n\}$. Une bijection de Ω sur Ω s'appelle une **permutation**. L'ensemble des permutations de Ω est noté $\mathbf{S}_n$. un élément f de $\mathbf{S}_n$ est souvent représenté sous la forme d'un tableau à 2 lignes et n colonnes :

$$f = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ i_1 & i_2 & i_3 & \ldots & n \end{pmatrix}$$

où la seconde ligne donne les images des éléments correspondant sur la première ligne. On munit $\mathbf{S}_n$ de la loi de composition des applications que l'on note cependant ici par un point $(\cdot)$ plutôt que par $\circ$.

Théorème 1.21. $(\mathbf{S}_n,\cdot)$ *est un groupe (non commutatif dès que $n > 2$) d'ordre $n!$.*

$(\mathbf{S}_n,\cdot)$ s'appelle le (n-ième) **groupe symétrique**.

6.2. *Cycles.* Soit $f \in \mathbf{S}_n$. S'il existe $k \in \{2,\ldots n\}$ et $a_1,a_2,\ldots,a_k$ dans Ω tels que

$$\begin{cases} f(a_i) = a_{i+1} & i = 1,\ldots,k-1 \\ f(a_k) = a_1 & \\ f(b) = b & b \notin \{a_1,\ldots,a_k\} \end{cases},$$

autrement dit, si f est de la forme

$$\begin{pmatrix} \boxed{\text{Id}} & \begin{matrix} a_1 \\ a_2 \end{matrix} & \boxed{\text{Id}} & \begin{matrix} a_2 \\ a_3 \end{matrix} & \boxed{\text{Id}} & \ldots & \boxed{\text{Id}} & \begin{matrix} a_{k-1} \\ a_k \end{matrix} & \boxed{\text{Id}} & \begin{matrix} a_k \\ a_1 \end{matrix} \end{pmatrix}$$

alors on dit que f est un **cycle**, ou, plus précisément un k-**cycle** et on note

$$f = (a_1\, a_2\, \ldots\, a_k).$$

Les 2-cycles sont appelés **transpositions**. L'ensemble $\{a_1,\ldots,a_k\}$ s'appelle le **support** du cycle f.

Théorème 1.22. *Si deux cycles ont des supports disjoints alors ils commutent. De manière précise, si $\{a_1,\ldots,a_k\} \cap \{b_1,\ldots,b_r\} = \emptyset$ alors*

$$(a_1\, a_2\, \ldots\, a_k) \cdot (b_1\, b_2\, \ldots\, b_r) = (b_1\, b_2\, \ldots\, b_r) \cdot (a_1\, a_2\, \ldots\, a_k).$$

Théorème 1.23. *Si f est un k-cycle alors f est d'ordre k (c-a-d $f^k = Id$ et $f^{k-1} \neq Id$.)*

Théorème 1.24. *Toute permutation se décompose en un produit de cycles disjoints. Cette décomposition est unique à l'ordre près des facteurs.*

On a les propriétés suivantes :

$$\begin{aligned} (a_1\, a_2\, a_3\, \ldots\, a_k) &= (a_1\, a_2) \cdot (a_2\, a_3)\, \ldots\, (a_{k-1}\, a_k) \\ (a_1\, a_2) &= (1\, a_1) \cdot (1\, a_2) \cdot (1\, a_1). \end{aligned}$$

6.3. *Signature.* Soit $f \in \mathbf{S}_n$. On définit $\epsilon(f)$ par la relation

$$\epsilon(f) = \prod_{1 \le i < j \le n} \frac{f(j) - f(i)}{j - i}.$$

Quelle que soit f, on a toujours $\epsilon(f) \in \{-1,1\}$. le nombre $\epsilon(f)$ s'appelle la **signature** de f.

Théorème 1.25. *Si $f = (1\,k)$ alors $\epsilon(f) = -1$.*

Théorème 1.26. *L'application $\epsilon : (\mathbf{S}_n,\cdot) \to (\{-1,1\},\cdot)$ est un morphisme de groupe. Autrement dit, quelles que soient f et g dans $\mathbf{S}_n$ on a*

$$\epsilon(f \cdot g) = \epsilon(f) \cdot \epsilon(g).$$

Corollaire. *La signature d'une transposition quelconque est égale à -1*

Corollaire. *La signature d'un cycle de longueur k est égale à $(-1)^{k-1}$.*

Corollaire. *L'ensemble $A_n := \{f \in \mathbf{S}_n \,:\, \epsilon(f) = 1\}$ est un sous-groupe distingué de $\mathbf{S}_n$. On l'appelle le n-ième **groupe alterné**.*

---

2. Introduction aux anneaux et corps

§ 1. La structure d'anneau.

1.1. *Définitions.* Un ensemble non vide A muni de deux lois internes — que l'on notera toujours, pour simplifier, $+$ et $\cdot$ — est un **anneau** si

(i) $(A,+)$ est un groupe commutatif,

(ii) la loi $\cdot$ est associative et elle est **distributive** par rapport à la loi $+$, c-a-d

$$\forall x,y,z \in A \quad \begin{cases} x \cdot (y+z) = (x \cdot y) + (x \cdot z) \\ (y+z).x = (y \cdot x) + (z \cdot x) \end{cases}.$$

On parle alors de l'anneau $(A, +, \cdot)$. La loi $+$ est appelée **l'addition** de A et la loi . est appelée le produit (ou **la multiplication**) de A. L'élément neutre de $(A,+)$ est toujours noté 0 — ou, s'il faut être précis, 0_A — et le symétrique de $x \in A$ pour la loi $+$ est noté $-x$. On rappelle que la notation $y - x$ signifie $y + (-x)$.

Théorème 2.1. *Soit $(A, +, \cdot)$ un anneau.*

(i) *$\forall a \in A$, $a \cdot 0 = 0 = 0 \cdot a$. (On dit parfois que le neutre de la loi $+$ est un élément **absorbant**.)*

(ii) *$\forall a,b \in A$, $(-a) \cdot b = a \cdot (-b) = -(ab)$.*

1.2. *Différents types d'anneaux.* Anneaux commutatifs, anneaux unitaires, anneaux intègres.

1.3. *Sous-anneaux.* Soit $(A, +, \cdot)$ un anneau et B un sous-ensemble non vide de A, B est un **sous-anneau** de A si

(i) $\forall a,b \in B$, $a - b \in B$

(ii) $\forall a,b \in B$, $a \cdot b \in B$.

1.4. *Trois exemples d'anneaux.*

a) $(\mathbb{Z}, +, \cdot)$ est un anneau commutatif, unitaire et intègre.

b) $(M_n(\mathbb{K}), +, \cdot)$ ($\mathbb{K} = \mathbb{Q},\mathbb{R},\mathbb{C}$) est un anneau unitaire non commutatif et non intègre.

c) Soient I un intervalle de $\mathbb{R}$ et $\mathcal{F}(I)$ l'ensemble des fonctions définies sur I à valeurs réelles alors $(\mathcal{F}(I), +, \cdot))$ est un anneau commutatif unitaire non intègre. (Ici les lois $+$ et $\cdot$ sont l'addition et le produit habituel des fonctions.) L'ensemble $\mathcal{C}(I)$ des fonctions continues sur I est un sous-anneau de $\mathcal{F}(I)$.

1.5. *Morphismes d'anneaux.* Soient $(A, +, \cdot)$ et $(B, +, \cdot)$ deux anneaux et f une application de A dans B. On dit que f est un **morphisme d'anneau** si

(i) $\forall\ a,a' \in A\ f(a + a') = f(a) + f(a')$,

(ii) $\forall\ a,a' \in A\ f(a \cdot a') = f(a) \cdot f(a')$,

Attention, lorsque A et B sont *unitaires*, on rajoute la condition

(iii) $f(1_A) = 1_B$,

Pour qu'un morphisme d'anneau soit injectif, il faut et il suffit que son noyau soit réduit au neutre 0_A.

§ 2. **Elements inversibles d'un anneau unitaire. Corps.**

2.1. *Le groupe des éléments inversibles.* Soit $(A, +, \cdot)$ un anneau unitaire. Un éléments $a \in A$ est dit inversible s'il existe $b \in A$ tel que

$$a \cdot b = b \cdot a = 1.$$

Cet élément b, s'il existe, est unique. On le note a^{-1}. Il y a toujours au moins un élément inversible, le neutre 1 lui-même, pour lequel $1^{-1} = 1$. On note A^* l'ensemble des éléments inversibles de l'anneau A. Naturellement, puisque $(a^{-1})^{-1} = a$, si $a \in A^*$ alors $a^{-1} \in A^*$.

Théorème 2.2. *L'ensemble A^* des éléments inversibles d'un anneau unitaire $(A, +, \cdot)$ est un groupe lorsqu'on le munit de la loi $\cdot$.*

2.2. *Définition d'un corps.* Un anneau unitaire $(F, +, \cdot)$ tel que $1_F \neq 0_F$ pour lequel $F^* = F/\{0_F\}$ s'appelle un **corps**.

Une partie non vide L de F est un **sous-corps** de F si

(i) $\forall x,y \in L$, $x - y \in F$

(ii) $\forall x,y \in L/\{0\}$, $x \cdot y^{-1} \in F$

Isomorphismes de corps...

Dans un *corps commutatif* on écrit souvent $\frac{a}{b}$ à la place de $a.b^{-1}$. On a alors les règles de calcul suivantes :

(i) $\frac{a}{b}.\frac{c}{d} = \frac{a.b}{b.d}$

(ii) $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$

2.3. *Exemples de corps.*

§ 3. L'anneau $\mathbb{Z}/n\mathbb{Z}$.

3.1. *Construction.* Définition du produit sur $\mathbb{Z}/n\mathbb{Z}$.

Théorème 2.3. *Quel que soit $n \in \mathbb{N}$, $n \geq 2$, $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau commutatif unitaire.*

3.2. *Le cas premier.*

Théorème 2.4. *Quel que soit $p \in \mathbb{N}$, p* premier*, $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ est un corps commutatif.*

3.3. *Application à l'arithmétique.*

Théorème 2.5 (Petit théorème de Fermat)**.** *Soient p premier et $a \in \mathbb{Z}$ tel que $p \not| a$. On a toujours*

$$a^{p-1} \equiv 1 \quad [p].$$

Autrement dit p divise toujours $a^{p-1} - 1$ dès lors qu'il ne divise pas p.

§ 4. Idéaux d'un anneau commutatif. Anneaux quotient.

4.1. *Définition.*

4.2. *Exemple : idéaux principaux.*

Théorème 2.6. *$(\mathbb{Z}, +, \cdot)$ est un anneau principal.*

4.3. *Exemple : noyau des morphismes.*

4.4. *Anneaux quotients.* Soit $(A, +, \cdot)$ un anneau commutatif et I un idéal de A. Puisque, en particulier, I est un sous-groupe de $(A,+)$, on peut former le groupe quotient A/I (il faut que I soit un sous-groupe distingué mais puisque $(A,+)$ est commutatif, tous ses sous-groupes sont distingués). Les éléments de A/I sont de la forme $\mathcal{C} = \mathbf{cl}(a) = a + I = \{a + h : h \in I\}$ et la loi $+$ (précédemment notée $\overline{+}$) sur A/I vérifie

$$\mathbf{cl}(a) + \mathbf{cl}(b) = \mathbf{cl}(a + b)$$

et plus généralement

$$\underset{\substack{\uparrow \\ \text{loi } + \text{ dans } A/I}}{\mathcal{C}_1 + \mathcal{C}_2} = \mathbf{cl}\Big(\underset{\text{représentant de } \mathcal{C}_1}{\text{n'importe quel}} + \underset{\text{représentant de } \mathcal{C}_2}{\text{n'importe quel}} \Big). \qquad \nearrow \text{ loi } + \text{ dans A}$$

Nous allons voir que grâce au fait que I est un idéal, on peut aussi définir un produit sur A/I comme suit

$$\begin{array}{rccl} \cdot\ : & A/I \times A/I & \longrightarrow & A/I \\ & (\mathcal{C}_1\,,\mathcal{C}_2) & \longmapsto & \mathbf{cl}\left(\begin{array}{c}\text{n'importe quel}\\ \text{représentant de } \mathcal{C}_1\end{array}\ \cdot\ \begin{array}{c}\text{n'importe quel}\\ \text{représentant de } \mathcal{C}_2\end{array}\right). \end{array}$$

Théorème 2.7. *Soit $(A,+,\cdot)$ un anneau commutatif et I un idéal de A alors $(A/I,+,\cdot)$ où $+$ et $\cdot$ sont définies comme ci-dessus est un anneau commutatif. Si A est unitaire alors A/I est aussi unitaire et on a $1_{A/I} = \mathbf{cl}(1_A)$.*

Théorème 2.8. *Soient $(A,+,\cdot)$ et $(B,+,\cdot)$ deux anneaux commutatifs et $f : A \to B$ un morphisme d'anneaux. Il existe un (unique) isomorphisme $\gamma : A/\ker f \to f(A)$ tel que $f = \gamma \circ s$ où s est la surjection canonique de A sur $A/\ker f$. On a donc*

$$\frac{A}{\ker f} \simeq f(A).$$

§ 5. **Anneaux de Polynômes.**

5.1. *Définitions.* Construction (par les suites à support fini) de $A[X]$, A étant un anneau commutatif unitaire. Définition de X. Addition et produit des polynômes. Calcul de X^n.

Théorème 2.9. *Soit $P \in A[X]$. Il existe $n \in \mathbb{N}$ et des éléments a_0,a_1,…,$a_n \in A$ tels que P s'écrive*

$$P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n = \sum_{i=0}^{n} a_iX^i.$$

De plus si

$$P = \sum_{i=0}^{n} a_iX^i \quad et \quad P = \sum_{i=0}^{m} b_iX^i$$

sont deux écritures de $P \in A[X]$, avec disons $n \leq m$, alors nécessairement

$$a_i = b_i \text{ pour } 0 \leq i \leq n \text{ et } b_i = 0_A \text{ pour } n < i \leq m.$$

Cela signifie que, si on enlève les termes nuls inutiles, l'écriture $P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ est unique.

Théorème 2.10. *Soit $(A,+,\cdot)$ un anneau commutatif unitaire. $(A[X],+,\cdot)$ est un anneau commutatif unitaire avec $0_{A[X]} = 0_A$ et $1_{A[X]} = 1_A$.*

Monômes, coefficients, coefficient dominant (dom), degré (deg).

Si P,$T \in A[X]$ $\deg(P+T) \leq \max(\deg(P), \deg(Q))$ et l'égalité a lieu à moins que P et Q soient de même degré et que $\mathrm{dom}(P) = -\mathrm{dom}(Q)$.

Théorème 2.11. *Si l'anneau commutatif unitaire A est intègre alors $A[X]$ est aussi intègre et on a*

$$\deg(PT) = \deg(P) + \deg(T). \tag{6}$$

Avec la convention $\deg(0) = -\infty$, la formule (6) ci-dessus reste vraie lorsque $P = 0$ ou $Q = 0$.

5.2. *Polynômes et fonctions polynomiales.* Soit A un anneau commutatif unitaire. A tout polynôme $P \in A[X]$, $P = a_0 + a_1X + \cdots + a_nX^n$, on fait correspondre une fonction polynomiale $\tilde{P} : A \to A$ définie par

$$(\forall t \in A) \quad \tilde{P}(t) = a_0 + a_1t + \cdots + a_nt^n.$$

Par exemple, au polynôme nul $P = 0$ correspond la fonction constante nulle et au polynôme $P = X$ correspond la fonction identité de A. Notant $\mathcal{F}(A)$ l'anneau des fonctions de A dans A. L'application

$$\mathrm{F}_A : \begin{array}{ccc} A[X] & \longrightarrow & \mathcal{F}(A) \\ P & \longmapsto & \tilde{P} \end{array}$$

est un morphisme d'anneau.

On note souvent $P(t)$ plutôt que $\tilde{P}(t)$. C'est un raccourci auquel il faut prendre garde.

5.3. *Division euclidienne des polynômes.*

Théorème 2.12. *Soient A un anneau commutatif unitaire intègre et $P \in A[X]$ un polynôme dont le coefficient dominant est inversible (i.e.* $\mathrm{dom}(P) \in A^*$*). Quel que soit $T \in A[X]$, il existe un et un seul couple de polynômes (Q,R) tels que*

$$\begin{cases} \deg R < \deg P \\ T = QP + R \end{cases}.$$

On dit que Q est ***le quotient*** *de la division euclidienne de T par P et R est* ***le reste****.*

Exemple de division.

5.4. *L'anneau principal $\mathbb{K}[X]$.*

Théorème 2.13. *Si $\mathbb{K}$ est un corps alors l'anneau $\mathbb{K}[X]$ est principal.*

5.5. *Racines des polynômes.* Soit A un anneau commutatif unitaire intègre et $P \in A[X]$. On dit qu'un élément $a \in A$ est un **zéro** de P (ou bien une **racine** de P) si $P(a) = 0$ autrement dit, plus précisément, si la fonction polynomiale $\tilde{P}$ associée à P s'annule en a.

Théorème 2.14. *Pour que a soit racine de P il faut et il suffit que le polynôme $X - a$ divise P, c'est-à-dire qu'il existe $Q \in A[X]$ tel que $P = (X - a)Q$.*

Le théorème précédent suggère de définir la multiplicité d'une racine de la manière suivante. On dit que a est une racine (un zéro) **d'ordre** k (**de multiplicité** k) lorsque $(X - a)^k$ divise P (i.e. $P = (X - a)^k Q$ pour un certain $Q \in A[X]$) mais $(X - a)^{k+1}$ ne divise pas P.

Théorème 2.15. *Soient A un anneau commutatif unitaire et $P \in A[X]$. Si A est intègre et si a_1,a_2,...,a_r sont des zéros de P alors*

$$P = (X - a_1)^{k_1}(X - a_2)^{k_2} \dots (X - a_r)^{k_r} Q$$

où k_i est la multiplicité de a_i ($1 \leq i \leq r$) et aucun des a_i n'est racine de $Q \in A[X]$.

Corollaire. *Si A est un anneau (commutatif unitaire) intègre alors tout polynôme $P \in A[X]$ non nul admet au plus* $\deg(P)$ *racines en tenant compte de la multiplicité. Autrement dit si P admet m racines a_i ($i \in \{1,2,\dots,m\}$) chacune de multiplicité s_i alors on a nécessairement $s_1 + s_2 + \cdots + s_m \leq \deg(P)$.*

Ce résultat n'est plus vrai si A n'est pas supposé intègre.

Corollaire. *Si A est un anneau commutatif unitaire intègre de cardinal infini alors l'application* F_A *qui a tout polynôme fait correspondre sa fonction polynomiale associée est injective.*

§ 6. **Le corps des fractions d'un anneau intègre.** Soit A un anneau (commutatif unitaire) intègre. On note $A^0 =_{def} A/\{0_A\}$. Sur l'ensemble $(A \times A^0)$ on définit la relation $\Re$ par

$$(a,b)\Re(c,d) \overset{def}{\iff} ad - bc = 0.$$

Le relation $\Re$ est une relation d'équivalence. La classe d'équivalence d'un élément $(a,b) \in A \times A^0$ est notée $\frac{a}{b}$, $Q(A)$ désigne l'ensemble de toutes les classes d'équivalence, i.e.

$$Q(A) =_{def} \left\{ \frac{a}{b} : a \in A, b \in A^0 \right\}.$$

Sur $Q(A)$ on montre qu'on peut définir de manière consistante les deux lois $+$ et $\cdot$ comme suit

$$\frac{a}{b} + \frac{c}{d} =_{def} \frac{ad + bc}{bd} \quad \text{et} \quad \frac{a}{b} \cdot \frac{c}{d} =_{def} \frac{ac}{bd}.$$

Théorème 2.16. $(Q(A), +, \cdot)$ *est un corps commutatif avec* $0_{Q(A)} = \frac{0}{1}$ *et* $1_{Q(A)} = \frac{1}{1}$. *De plus* A *devient un sous-anneau de* $Q(A)$ *si l'on identifie tout élément* $a \in A$ *avec* $\frac{a}{1} \in Q(A)$. *Le corps* $Q(A)$ *s'appelle le* ***corps des fractions*** *de l'anneau intègre* A.

Exemple. Corps des fractions rationnelles.

LABORATOIRE DE MATHÉMATIQUES E. PICARD, UNIVERSITÉ PAUL SABATIER 31062 TOULOUSE CEDEX 4 FRANCE.

E-mail address: calvi@picard.ups-tlse.fr