Les Mathématiques pour l'Agrégation

C. Antonini
J.-F. Quint
P. Borgnat
J. Bérard
E. Lebeau
E. Souche
A. Chateau
O. Teytaud

24 avril 2002

Table des matières

Chapitre 1

Théorie des groupes

1.1 Les bases

1.1.1 Définition d'un groupe

Définition 1 *Un* **groupe** *est un ensemble G, muni d'une* **loi de composition interne** *(lci), c'est à dire une application de $G \times G \to G$, généralement notée par la concaténation ($(x, y) \mapsto xy$), vérifiant :*
• $(xy)z = x(yz)$
• $\exists 1 / \forall x\ x.1 = 1.x = x$ *; 1 est dit l'élément neutre*
• $\forall x \exists x^{-1} / xx^{-1} = x^{-1}x = 1$

Pour vérifier qu'un ensemble muni d'une loi est bien un groupe, il suffit de vérifier que les deux premiers • sont vérifiés, et que pour tout x il existe x^{-1} tel que $xx^{-1} = 1$.

Définition 2 *Un groupe G est dit* **commutatif ou abélien** *si $xy = yx$. Dans ce cas on note souvent additivement ; l'élément neutre est alors noté 0, et x^{-1} est noté $-x$.*

Définition 3 *G est un p-***groupe***, avec p premier, si G est de cardinal une puissance de p.*

1.1.2 Sous-groupe

Définition 4 (Sous-groupe) *$H \subset G$ est un* **sous groupe de** *G si et seulement si :*
• $1 \in H$
• $(x, y) \in H^2 \rightarrow xy \in H$
• $\forall x \; x^{-1} \in H$

NB : un sous-groupe est un groupe, et un groupe inclus dans un groupe (pour les mêmes lois bien sûr) est un sous-groupe de ce groupe.

On peut noter les conditions dessus plus simplement : $1 \in H \wedge HH \subset H \wedge H^{-1} \subset H$

Définition 5 *Deux sous-groupes A et B sont dits* **conjugués** *s'il existe g tel que $A = g.B.g^{-1}$.*
Etant donné H sous-groupe de G, le **normalisateur** *de H est $N_G(H) = \{g \in G / gHg^{-1} = H\}$.*
Un sous-groupe N est dit **distingué** *(ou* **normal***) si pour tout g $gNg^{-1} = N$; on note $N \lhd G$.*
Un sous-groupe N est dit **caractéristique** *si il est stable par tout automorphisme intérieur.*
Un groupe est dit **simple** *si ses seuls sous-groupes distingués sont $\{1\}$ et G.*
L'ensemble des x tels que x commute avec tout élément est appelé le **centre** *d'un groupe. Le centre est un sous-groupe. On note $Z(G)$ le centre de G.*


Il faut bien voir ce que dit la définition du normalisateur - le normalisateur de H "fait" de H un sous-groupe normal, au sens où H est normal dans son normalisateur. En fait le normalisateur est le plus grand sous-groupe contenant H dans lequel H est distingué.

Propriétés :
• Un sous-groupe est distingué si et seulement si son normalisateur est le groupe tout entier.
• Un sous-groupe est distingué si et seulement si il n'est conjugué à aucun autre sous-groupe.
• Un sous-groupe caractéristique est distingué (évident).
• Tout sous-groupe d'un groupe abélien est distingué ; par contre, en considérant H_8 le groupe des quaternions, on peut constater qu'il n'y a pas de réciproque (voir 1.10).
• $\{1\}$ et G sont toujours à la fois des sous-groupes distingués et caractéristiques.
• Le centre d'un groupe est caractéristique et distingué.

Exemples :
• $\mathbb{Z}/p\mathbb{Z}$ est simple (en effet ses seuls sous-groupes sont ses sous-groupes triviaux, donc ses seuls sous-groupes distingués sont ses sous-groupes triviaux...)
• $\mathcal{U}_n$ est simple (voir 1.10.11)

Définition 6 *On appelle* **commutateur** *de x et y l'élément $x.y.x^{-1}.y^{-1}$.*
On appelle **groupe dérivé** *d'un groupe le sous-groupe engendré[a] par les commutateurs. On note $D(G)$ le groupe dérivé de G.*

[a] Voir paragraphe 1.1.5 pour la définition de sous-groupe engendré par une partie.

Il faut bien noter que l'ensemble des commutateurs n'est pas nécéssairement un groupe ; le groupe dérivé est le sous-groupe engendré par l'ensemble des commutateurs.

Propriétés :
• $D(G)$ est distingué et même caractéristique dans G.

1.1.3 Homomorphismes

Définition 7 *On appelle* **homomorphisme** *du groupe G dans le groupe G' une fonction ϕ telle que $\phi(xy) = \phi(x)\phi(y)$. On note $Hom(G, G')$ l'ensemble des homomorphismes de G dans G'.*

On montre que pour tout tel ϕ :
• $\phi(1) = 1$
• $\phi(x^{-1}) = \phi(x)^{-1}$

La fonction constante égale à 1 est un homomorphisme de G dans G' ; éventuellement ce peut être le seul.

L'inverse d'un homomorphisme bijectif est un homomorphisme bijectif.

Proposition 8 *L'ensemble des* **automorphismes**, *i.e. des* **endomorphismes** *bijectifs, i.e. homomorphismes de G dans G bijectifs, noté $Aut(G)$, est un groupe.*

Exemples :
a) G groupe, $x \in G$
$\phi_x \in Hom(\mathbb{Z}, G)$, avec $\phi_x(n) = x^n$; le plus petit n tel que $\phi_x(n) = 1$, s'il existe est appelé ordre de x.
b) G groupe, $g \in G$
La fonction α_g, $x \mapsto gxg^{-1}$ est un automorphisme de G, dit automorphisme **intérieur** associé à g, appelée aussi **conjugaison** par g. En outre la fonction $g \mapsto \alpha_g$ est un homomorphisme de G dans $Aut(G)$. Son noyau est le centre de G.
L'ensemble des automorphismes intérieurs d'un groupe est un sous-groupe de l'ensemble des automorphismes du dit groupe.

Quelques propriétés :

Proposition 9 *(G, G') groupes, $\phi \in Hom(G, G')$*
• $Ker\ \phi := \{g \in G / \phi(g) = 1\}$
est un sous-groupe distingué de G.
• $Im\ \phi$ est un sous-groupe de G'.
• ϕ injectif $\iff Ker\phi = \{1\}$

1.1.4 Extensions

Définition 10 *On appelle* **suite exacte** *un schéma comme suit :*

$$1 \xrightarrow{} A \xrightarrow{i} B \xrightarrow{s} C \xrightarrow{} 1$$

Cela signifie que A, B et C sont des groupes, et que
• i est un homomorphisme injectif de A dans B
• s est un homomorphisme surjectif de B dans C
• $Ker\ s = Im\ i$
(on note 0 au lieu de 1 lorsque les groupes sont notés additivement)
Lorsque i et s ne sont pas précisés, cela signifie simplement que l'on peut trouver de tels i et s.
On dit alors que B est une **extension** *de A par C. Si en outre il existe $\overline{C}$ sous-groupe de B tel que la restriction de s à $\overline{C}$ est un isomorphisme, alors on dit que $\overline{C}$ est un* **relèvement**. *Cela est équivalent à dire qu'il existe un homomorphisme t de C dans B tel que $s \circ t = Id_C$. S'il y a un relèvement, l'extension est dite* **scindée**. *t est appelée* **section** *de s.*

1.1.5 Sous-groupe engendré

Proposition 11 *Soit G un groupe, X inclus dans G.*

Il existe un plus petit sous-groupe H de G contenant X. On peut le définir de deux façons :
(i) H est l'intersection de tous les sous-groupes contenant X
(ii) H est l'ensemble des produits finis d'éléments de $X \cup X^{-1}$.

Démonstration :
(i) est évident car l'intersection de deux sous-groupes est un sous-groupe.
(ii) on procède en trois points :
• K ainsi défini est un sous-groupe
• $X \subset K$ donc par (i) $H \subset K$

• $K \subset H$ est clair□

Définition 12 *On note $H =< X >$, H est appelé groupe* **engendré** *par X, et X est appelée* **partie génératrice** *de H. Si X est réduit à un seul élément x on note souvent $H =< x >$ au lieu de $H =< \{x\} >$.*
Un groupe est dit **monogène** *s'il est engendré par un seul élément. On appelle groupe* **cyclique** *un groupe monogène fini.*
On appelle **ordre d'un élément** *le cardinal du groupe engendré par cet élément.*

 Si deux homomorphismes coïncident sur une partie génératrice d'un groupe, alors ils coïncident sur l'ensemble du groupe.

 Cela sera utile pour la proposition 42.

Définition 13 *On dit que G est* **de type fini** *si $\exists X$ fini qui engendre G.*

Ainsi $\mathbb{Z}$, $\mathbb{Z}^n$ sont de type fini, et tout groupe fini est de type fini.

 tout groupe de type fini est dénombrable.
Il n'y a pas équivalence, car par exemple $(\mathbb{Q}^*, \times)$ n'est pas de type fini (preuve en considérant des générateurs et leurs décompositions en facteurs premiers)
$(\mathbb{Q}, +)$ non plus (considérer l'inf de l'intersection avec $\mathbb{R}^+$ d'un groupe de type fini, en réduisant au même dénominateur)

Proposition 14 *Le groupe engendré par un ensemble réduit à un élément x est commutatif, et est l'ensemble des x^n avec $n \in \mathbb{Z}$. Il est isomorphe à $\mathbb{Z}$ ou à $\mathbb{Z}/n\mathbb{Z}$.*

Démonstration : $\{x^n\}$ est un groupe et contient x, donc il est inclus dans $< x >$; s'il est fini alors il existe n tel que $x^p = x^{p+n}$, et donc $x^n = 1$, et donc $< x >= \{x^0, ..., x^{n-1}\}$.□

Proposition 15 *Tout sous-groupe d'un groupe cyclique est cyclique.*

Démonstration : Un tel sous-groupe H de G est évidemment fini. Notons ensuite a un générateur du groupe ; le groupe est donc de la forme $a^0, ..., a^{n-1}$. Soit $p > 0$ minimal tel que $a^p \in H$;

1.2 Groupe quotient

1.2.1 Rappel : ensemble quotient

Soit X un ensemble, et $\mathcal{R}$ une relation d'équivalence sur X ; l'ensemble des classes pour $\mathcal{R}$ est une partition de X. Cet ensemble de classes, noté $X/\mathcal{R}$, est appelé **ensemble quotient** de X par $\mathcal{R}$. La classe d'un élément est notée $\Pi(x)$, x est dit un représentant de $\Pi(x)$. Π est appelée **surjection canonique**.

Il y a en fait ainsi bijection entre l'ensemble des relations d'équivalence et l'ensemble des partitions en parties non vides. A toute relation d'équivalence $\equiv$ on peut associer une fonction f telle que $x \equiv y \iff f(x) = f(y)$ (il suffit pour le montrer de considérer la fonction Π).

Etant donnée une fonction définie sur X, on peut définir $\overline{f}$ **fonction quotient** si f est constante sur les classes d'équivalences, $\overline{f}$ étant alors définie par $\overline{f}(\Pi(x)) = f(x)$.

1.2.2 Le cas des groupes

Définition 16 *H sous-groupe de G*
On définit les **classes à gauche suivant** *H comme les xH, $x \in G$, et les* **classes à droite suivant** *H comme les Hx.*
On note G/H l'ensemble des classes à gauche, $H \setminus G$ l'ensemble des classes à droite.
On note $(G : H)$ le cardinal de G/H quand celui-ci est fini.

On travaille généralement sur G/H plutôt que sur $H \setminus G$.

Proposition 17 *Les classes à gauche déterminent une partition de G en parties non vides. Pareil pour les classes à droite.*

Proposition 18 *N sous-groupe de G, il y a équivalence entre les trois assertions suivantes :*
• *N distingué*
• *$gN = Ng$ pour tout g*
• *il existe une structure de groupe sur le quotient G/N telle que Π soit un homomorphisme.*

On voit donc que dans ce cas $G/H = H \setminus G$. Cette propriété d'un sous-groupe distingué est fondamentale : la partition en classes à droite est égale à la partition en

classes à gauche. Ce fait est caractéristique des sous groupes distingués.

Proposition 19 *G et G' deux groupes, N sous-groupe distingué de G, $\phi \in Hom(G, G')$; alors les deux assertions suivantes sont équivalentes :*
• *Il existe $\overline{\phi}$ de G/N dans G' tel que $\phi = \overline{\phi} \circ \Pi$*
• *$N \subset Ker\ \phi$*

Dans ce cas $\overline{\phi}$ est unique, et est un homomorphisme de groupes de G/N dans G'.

En particulier, $\overline{\phi}$ est une injection si $N = Ker\ \phi$, et induit un isomorphisme de $G/Ker\ \phi$ dans $Im\phi$.

Les preuves de ces faits sont faciles, et sont logiques intuitivement ; si on quotiente par quelque chose de trop gros par rapport au noyau, alors on n'a plus la précision requise pour reconstruire la fonction...

$G/D(G)$ est un groupe abélien, c'est d'ailleurs son plus grand quotient abélien, et $D(G)$ est le seul sous-groupe à avoir cette propriété.

Théorème 20 (Factorisation d'homomorphismes) *Soit G un groupe, H un sous-groupe distingué de G, ϕ un homomorphisme de G vers un groupe G'. Alors si $H \subset Ker\ \phi$, alors il existe une application $\tilde{\phi}$[a] telle que*

$$\phi = \tilde{\phi} \circ p$$

avec p la projection canonique de G sur G/H.

[a] De G/H dans G'.

Cela servira par exemple pour le théorème 48.

Démonstration : Si facile que vous le prouver serait une injure... La fonction $\tilde{\phi}$ est bien définie, car si deux éléments on même image par p alors ils ont même image par ϕ, et l'application $\tilde{\phi}$ est bien un homomorphisme car ϕ en est un (la vérification de cette implication est facile).□

1.2.3 Le théorème de Lagrange

Définition 21 *On appelle* **indice de H dans** *G, avec H un sous-groupe de G, le cardinal de G/H.*

Un théorème fondamental :

Théorème 22 (Théorème de Lagrange) *Soit G un groupe fini, et H un sous-groupe de G, alors*

$$|G| = |H|.|G/H|$$

Démonstration : Il suffit de montrer que chaque classe d'équivalence est de même cardinal, et que ce cardinal est $|H|$ (chose facile à prouver !).□

On remarque qu'il n'est absolument pas nécéssaire que H soit distingué.

1.3 Opération d'un groupe sur un ensemble

Définition 23 *Avec G un groupe et X un ensemble, on appelle* **action à gauche** *de G sur X une application α de $G \times X$ dans X telle que :*
• $\alpha(1, x) = x$
• $\alpha(g, \alpha(h, x)) = (g.h, x)$
On dit aussi que G **opère à gauche** *sur X où que G est une* **opération à gauche** *sur X. Usuellement on note plus simplement $g.x$ au lieu de $\alpha(g, x)$. Les deux conditions deviennent alors :*
• *1.x=x*
• *(g.h).x=g.(h.x)*
On définit de manière symétrique une **action à droite***. Une* **action** *sans plus de précision désigne une action à gauche. On dit que X est un G-ensemble.*

Propriétés :
• $g.x = y \iff g^{-1}.y = x$
• Etant donné x et y dans X il n'est pas du tout nécéssaire qu'il existe un g tel que $g.x = y$.
• Si G opère sur X alors tout sous-groupe H de G opère sur X pour la loi restreinte.

L'équivalence suivante est fondamentale : se donner une action de G sur X revient à se donner un homomorphisme ϕ de G dans le groupe $\sigma(X)$ des bijections de X ($g.x = \phi(g).x$).

Un exemple fondamental est l'action d'un groupe sur lui-même ; l'action est en fait simplement la loi du groupe. Il est clair que les conditions sont vérifiées.

Pour le cas des actions à droite, il faut noter que si on a une action à droite $a_1(x, g)$, alors $a_2(g, x) \to a_1(x, g^{-1})$ est une action à gauche du groupe opposé (le groupe opposé à G étant G muni de $(x, y) \to yx$). On travaillera à peu près toujours avec des classes à gauche, les résultats étant les mêmes, et puisqu'on peut reformuler le

problème en terme d'action à gauche.

Définition 24 *Etant donnés X et X' deux G-ensembles, on appelle G-***homomorphisme** *de X vers X' une application ϕ de X dans X' telle que $\phi(g,x) = g.\phi(x)$ pour tous $x \in G$ et $g \in G$. On note $Hom(X,X')$ l'ensemble des homomorphismes de X sur X'. Comme d'habitude, un* **isomorphisme** *est un homomorphisme bijectif.*

Un exemple facile et classique :
Soit G un groupe et X un G-ensemble. L'application ϕ_x pour $x \in G$ qui à g dans G associe $g.x$ est un homomorphisme de G (en tant que G-ensemble) sur X (en tant que G-ensemble).

Démonstration : Soit g dans G et y dans G (y est pris dans G en tant que G-ensemble) alors $\phi_x(g.y) = g.y.x$ et $g.\phi_x(y) = g.y.x$.□

Définition 25 *On note H_x ou G_x et on appelle* **stabilisateur** *ou* **fixateur** *de x l'ensemble des g tels que $g.x = x$. C'est un sous-groupe de G, qui n'est pas nécessairement distingué.*
On appelle **G-orbite** *de x appartenant à X (ou plus simplement* **orbite** *s'il n'y a pas de risque de confusion) et on note $\omega(x)$ ou $G.x$ la classe d'équivalence de x pour la relation $\mathcal{R}$ définie par $a\mathcal{R}b \iff \exists g \in G / g.a = b$ (il est facile de vérifier qu'il s'agit bien d'une relation d'équivalence).*
Un G-ensemble est dit **homogène** *s'il ne contient qu'une seule orbite.*
On dit que $x \in X$ est un **point fixe**, *si l'orbite de x est réduite à $\{x\}$.*
On dit que G opère **transitivement** *si $\forall x \forall y \exists g / y = g.x$.*
On dit que G opère k **fois transitivement** *si $\forall (x_i)_{i\in\{1,...,k\}} \forall (y_i)_{i\in\{1,...,k\}} (i \neq j \rightarrow x_i \neq x_j \wedge y_i \neq y_j) \rightarrow \exists g \forall i \in \{1,...,k\} / y_i = g.x_i$.*
On dit que G opère **fidèlement** *si $\forall x\ g.x = x \rightarrow g = 1$.*

Proposition 26 *Lorsque G est fini, on a pour tout x dans X, $|\omega(x)|.|H_x| = |G|$.*

Démonstration : On constatera simplement que l'application qui à $\overline{g}$ associe $g.x$ de G/H_x dans $\omega(x)$ est une bijection.□

La figure 1.1 tâche de montrer l'allure générale d'un G-ensemble.

Propriétés :
• Chaque orbite est un ensemble homogène.

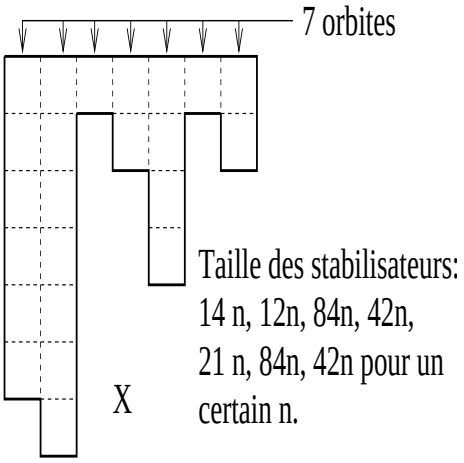

FIG. 1.1 – Exemple de G-ensemble X. Les séparations verticales sont les séparations entre les orbites, qui réalisent une partition de X. L'action n'étant pas nécessairement injective, les orbites ne sont pas nécessairement de même cardinal que G. A l'intérieur d'une même orbite, le stabilisateur est toujours le même à conjugaison près, et en particulier, les stabilisateurs dans une même orbite sont équipotents. Si le groupe et l'ensemble sont finis, le cardinal du groupe est le produit du cardinal de l'orbite par le cardinal d'un stabilisateur de cette orbite. On notera que le cardinal du groupe agissant sur cet ensemble est au moins 84 (ppcm des cardinaux des orbites).

Proposition 27 *G groupe, X et X' des G-ensembles homogènes, alors les assertions suivantes sont équivalentes :*
- $X \simeq X'$
- $\exists (x, x') \in X \times X' / H_x = H_{x'}$
- $\exists (x, x') \in X \times X' / H_x$ *est conjugué à* $H_{x'}$
- $\forall (x, x') \in X \times X' / H_x$ *est conjugué à* $H_{x'}$

Démonstration : laissée en exercice. □


Exemples classiques :

- Le groupe orthogonal $O(3, \mathbb{R})$ opère sur $\mathbb{R}^3$; les orbites sont les sphères de centre l'origine, le stabilisateur de 0 est $O(3, \mathbb{R})$ tout entier, et le stabilisateur d'un point quelconque autre que 0 est l'ensemble des rotations d'axe la droite vectorielle engendrée par ce point et des symétries par rapport à un sous-espace vectoriel passant par ce point. 0 est un point fixe.
- On peut faire opérer G sur ses sous-groupes par conjugaison, avec $g.H = gHg^{-1}$. Le stabilisateur d'un point (c'est à dire d'un sous-groupe) est alors le normalisateur de ce point (ie de ce sous-groupe).
- Si X est un espace topologique et est un G-ensemble tel que pour tout $g \in G$ l'application $y \mapsto g.y$ est un homéomorphisme, alors on dit que G **agit sur** X **par homéo-**

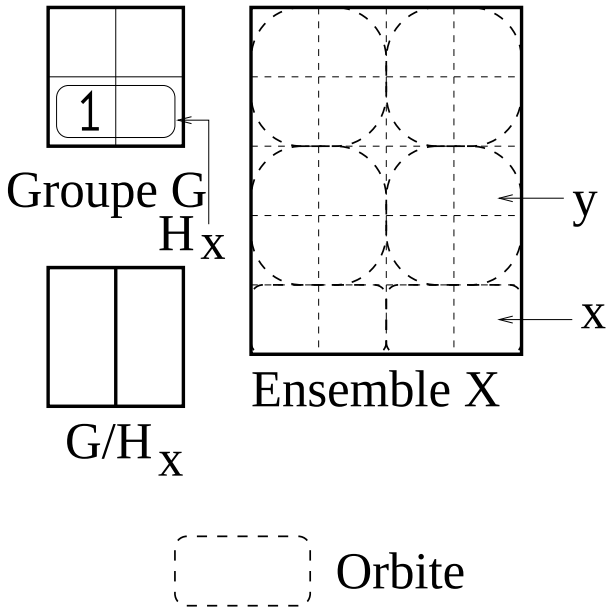

FIG. 1.2 – x est un élément de X. G est d'ordre 2, $\omega(x)$ est de cardinal 2, donc G/H_x est de cardinal 2 (il est en bijection avec $\omega(x)$), et H_x est de cardinal $\frac{4}{2} = 2$.

morphismes. La topologie quotient pour la relation d'équivalence "être dans la même orbite" vérifie des propriétés intéressantes (voir proposition **??** et théorème **??**).

Proposition 28 *Un G-ensemble homogène est isomorphe à un quotient G/H de G pour l'action de G sur G/H par translation à gauche.*

Pour bien voir l'intérêt de cette remarque, il faut se rappeler que tout G-ensemble est partitionné naturellement en orbites, qui sont des G-ensembles homogènes, et que donc on peut identifier à des actions par translation d'un groupe sur un groupe quotient.

Proposition 29 (Sur l'ensemble des points fixes) *Etant donnés G un p-groupe et X un ensemble sur lequel agit G, le cardinal de l'ensemble des points fixes de X pour G est congru au cardinal de X modulo p.*

Démonstration : Le cardinal des orbites divise le cardinal de G, donc le cardinal de l'union des orbites est congru au nombre d'orbites de cardinal 1 modulo p. Le cardinal de l'union des orbites est le cardinal de X.□

1.4 Produits

Il faut bien noter que même si de nombreuses applications des résultats ci-dessous se font avec des groupes finis, ils sont valables pour des groupes quelconques.

1.4.1 Produit direct

Définition 30 (Produit direct de deux groupes) *On appelle* **produit direct** *de deux groupes N et H et on note $N \times H$ le produit cartésien des groupes N et H muni du produit terme à terme*

$$(n, h).(n', h') = (nn', hh')$$

La fonction p_2 qui à (n, h) associe h est appelée **projection** *de $N \times H$ sur H. La fonction p_1 qui à (n, h) associe n est appelée* **projection** *de $N \times H$ sur N. On définit alors la généralisation à un produit d'un nombre quelconque de groupes par $\Pi_{i\in I}G_i$. La loi*

$$(g_i)_{i\in I}(h_i)_{i\in I} = (g_i h_i)_{i\in I}$$

muni le produit d'une structure de groupe ; on appelle ce groupe le **groupe produit**.
On définit aussi le **produit restreint** *des G_i comme étant le sous-groupe du produit des G_i des éléments $(g_i)_{i\in I}$ ne comportant qu'un nombre fini de g_i différents de l'élément neutre. S'il s'agit d'un produit d'un nombre fini de groupes il est clair que le produit restreint est égal au produit.*

Propriétés :
• p est surjective, c'est un morphisme surjectif, son noyau est distingué et isomorphe à N. On a une suite exacte

$$1 \to N \xrightarrow{i} N \times H \xrightarrow{p} H \to 1$$

avec $i(n) = (n, 1)$.
• $N \times \{1\}$ est le noyau de p, il est distingué ; et $\{1\} \times H$ est distingué aussi.

1.4.2 Produit semi-direct

Définition 31 (Produit semi-direct) *Etant donnés deux groupes N et H, et un morphisme de groupe ϕ de H dans l'ensemble des automorphismes de N ; alors on appelle* **produit semi-direct de N et H relativement à ϕ** *et on note $N \rtimes H$ le produit cartésien $N \times H$ muni de la loi $(n, h).(n', h') = (n.\phi(h)(n'), hh')$.*

On notera que formellement il faudrait préciser $N \rtimes_\phi H$.

Proposition 32 • *Le produit semi-direct $N \rtimes H$ a une structure de groupe*
• *On a une suite exacte*

$$1 \to N \xrightarrow{i} N \rtimes H \xrightarrow{s} H \to 1$$

avec $i(n) = (n, 1)$ et $s(n, h) = h$.
• *$i(N)$, c'est à dire $N \times \{1\}$ est distingué, mais pas $\{1_N\} \times H$ (contrairement au cas du produit direct).*

Démonstration : Vérification facile.□

Remarque importante :
En identifiant N et $N \times \{1\}$ d'une part, H et $\{1\} \times H$ d'autre part, on constate qu'un produit semi-direct peut toujours s'écrire comme produit semi-direct de deux sous-groupes lié au morphisme ϕ de G dans $Aut(N)$ défini par $(\phi(h))(n) = hnh^{-1}$.

1.4.3 Identifier un produit direct ou semi-direct

Cette partie est fondamentale pour ramener l'étude d'un groupe à l'étude de groupes plus petits (tâche fondamentale en théorie des groupes !).

⊡ Identification d'un produit semi-direct

Proposition 33 (Décomposition en produit semi-direct) *Si on a une suite exacte*

$$1 \to N \xrightarrow{i} G \xrightarrow{s} H \to 1$$

(c'est à dire si i est injective, si s est surjective, et si $Ker\ s = Im\ i$) et si on a un sous-groupe $\overline{H}$ de G sur lequel la restriction de s est un isomorphisme vers H [a], alors G est isomorphe à $i(N) \rtimes \overline{H}$ relativement à la loi de l'automorphisme intérieur (voir la remarque de 1.4.2).
On peut donc aussi dire que G est isomorphe à $N \rtimes H$, i étant un isomorphisme de N sur $\overline{N}$, et s étant un isomorphisme de $\overline{H}$ sur H.

[a] C'est-à-dire un relèvement, une section, voir la partie 1.4.2

Démonstration : On considère $\overline{N}$ l'image de i, et $\overline{H}$ le sous-groupe de G sur lequel la restriction de s est un isomorphisme vers H.
Puisque $\overline{N} = Ker\ s$, $\overline{N} \lhd G$ (un noyau de morphisme de groupe est toujours distingué).Il est clair que :
• $\overline{N} \cap \overline{H} = \{1\}$
• $G = \overline{N}.\overline{H}$
Le premier point est évident, du fait que s est un isomorphisme depuis $\overline{H}$, et a donc un noyau nul.

Pour le deuxième point, soit $g \in G$, alors $s(g) = s(h)$ avec $h \in H$, et $s(g.h^{-1}) = s(g).s(h)^{-1} = 1$, donc $g.h^{-1} \in N$. L'écriture d'un élément de G comme produit d'un élément de N par un élément de H est unique (facile, au vu de $\overline{N} \cap \overline{H} = \{1\}$) ; G est donc ainsi en bijection avec $\overline{N} \times \overline{H}$, par $\phi(nh) = (n, h)$. On cherche maintenant à établir une loi sur $\overline{N} \times \overline{H}$ telle que cette bijection soit un isomorphisme.
Le produit de $n.h$ par $n'h'$ est $n.h.n'h'$, que l'on doit donc exprimer comme un produit d'un élément de $\overline{N}$ par un élément de $\overline{H}$; on peut réécrire $n.h.n'.h'$ sous la forme $n.(h.n'.h^{-1}).h.h'$; puisque N est distingué, il s'agit bien du produit de $n.h.n'.h^{-1}$ (élément de $\overline{N}$) par $h.h'$ (élément de $\overline{H}$).
On vérifie facilement que la loi $(n, h).(n', h') = (n.(h.n'.h^{-1}), h.h')$ fait de cette bijection un morphisme.□

Remarque importante : L'hypothèse revient exactement à avoir une extension scindée, c'est à dire une extension munie d'un relèvement (voir 1.1.4).

Proposition 34 *Si G est un groupe, si N et H sont des sous-groupes de G, si $N \lhd\!\!\lhd G$, si $N \cap H = \{1\}$ et si $G = N.H$, alors $G \simeq N \rtimes H$.*

Démonstration : Il suffit de reprendre la preuve ci-dessus.□

⊡ Identification d'un produit direct

En fait un produit direct est un cas particulier de produit semi-direct.
En reprenant les notations de la définition du produit semi-direct et des démonstrations ci-dessus, on a équivalences entre les assertions suivantes :
• $\phi(h) = Id_N$ pour tout h
• $\overline{H}$ est distingué
• la loi de groupe sur $N \rtimes H$ est celle du produit direct

On peut aussi raisonner sur les suites exactes. Lorsque l'on a une suite exacte avec relèvement, i.e. avec une section, i.e. si l'extension est scindée, ET si $\forall (n, h) \in N \times H\ nh = hn$.

1.4.4 Quelques remarques pour éviter les gaffes

La condition de la proposition 33 est suffisante mais non nécéssaire ; on peut avoir une extension sans relèvement, c'est à dire non scindée, c'est à dire sans qu'il y ait de section, sans pour autant que le groupe ne soit pas le produit semi-direct de N par H.

On peut très bien avoir $A \times B$ (produit direct) $\simeq A \rtimes_\phi B$, avec ϕ autre que $\phi(h) = Id_N$ pour tout h ; donc il ne suffit pas de décomposer un groupe comme produit semi-direct non trivial pour conclure qu'il n'est pas un produit direct. [14] cite ainsi $\sigma_3 \times \mathbb{Z}/2.\mathbb{Z}$.

1.5 Théorèmes de Sylow. Groupes de Sylow

Les deux théorèmes de Sylow sont extraits du classique [14].

Définition 35 *On appelle p-**sous-groupe de Sylow** ou plus simplement p-**Sylow** d'un groupe G de cardinal n, un sous-groupe de G d'ordre p^r avec p premier divisant n et $n = p^r.m$ et $p \not| m$.*

Proposition 36 *Un sous-groupe P de G est un p-sous-groupe de Sylow de G si :*
- *P est un p-groupe*
- *$(G : P)$ est premier à p.*

Démonstration : Pas difficile, y'a qu'à l'écrire.□

Théorème 37 (Théorème de Sylow) *G étant un groupe fini, et p un nombre premier divisant l'ordre de G, alors G admet au moins un p-sous-groupe de Sylow.*

Démonstration : On va procéder par étapes.
• Tout d'abord un cas particulier : $\mathbb{Z}/p\mathbb{Z}$ est un corps fini puisque p est premier, et $GL(n, \mathbb{Z}/p.\mathbb{Z})$ est d'ordre $\Pi_{i=0}^{n-1}(p^n - p^i)$, comme on peut s'en convaincre en comptant les bases de $(\mathbb{Z}/p.\mathbb{Z})^n$. Le cardinal de ce groupe est donc $m.p^{n.(n-1)/2}$, avec $p \not| m$. Un p-Sylow de ce groupe est alors l'ensemble des matrices de la forme

$$\underbrace{\left\{\begin{pmatrix} 1 & * & * & \dots & * & * \\ 0 & 1 & * & \dots & * & * \\ 0 & 0 & 1 & \dots & * & * \\ \vdots & \vdots & \vdots & \ddots & * & * \\ 0 & 0 & \dots & 0 & 1 & * \\ 0 & 0 & \dots & 0 & 0 & 1 \end{pmatrix}\right.}_{n \text{ colonnes}} \left.\vphantom{\begin{pmatrix} 1 & * & * & \dots & * & * \\ 0 & 1 & * & \dots & * & * \\ 0 & 0 & 1 & \dots & * & * \\ \vdots & \vdots & \vdots & \ddots & * & * \\ 0 & 0 & \dots & 0 & 1 & * \\ 0 & 0 & \dots & 0 & 0 & 1 \end{pmatrix}}\right\} n \text{ lignes}$$

• On a maintenant besoin d'un lemme :

Lemme 38 *Soit G un groupe d'ordre $p^\alpha.m$, avec $p \not| m$ et p premier, et soit H un sous-groupe de G et S un p-Sylow de G. Alors il existe $a \in G$ tel que $a.S.a^{-1} \cap H$ soit un p-sylow de H.*

Démonstration : G opère sur G/S par translation à gauche (voir 1.9.1) ; le stabilisateur d'un élément $g.S$ est $g.S.g^{-1}$.
D'autre part H opère sur G/S par translation à gauche aussi ; le stabilisateur d'un élément $g.S$ est $g.S.g^{-1} \cap H$.
Il est clair que tout $a.S.a^{-1}$ est bien un p-groupe, il reste à en trouver un qui soit bien

un p-Sylow. Il suffit pour cela que le quotient du cardinal de H par le cardinal de $H \cap a.S.a^{-1}$ soit premier avec p ; donc il suffit que le cardinal de $H/(H \cap a.S.a^{-1})$ soit premier avec p.
Or ce cardinal est en fait le cardinal de l'orbite de $a.S$ dans G/S sous l'action de H ; or toutes ces orbites ne peuvent être de cardinal un multiple de p, sinon le cardinal de G/S serait un multiple de p, ce qui contredirait le fait que S est un p-Sylow.
Ce lemme est donc prouvé.□
• Maintenant on peut s'attaquer au cas général ; soit G un groupe vérifiant les hypothèses ; G est isomorphe à un sous-groupe de σ_n par le théorème de Cayley (voir 1.9.1). A son tour, σ_n est isomorphe à un sous-groupe de $GL(n, \mathbb{Z}/p.\mathbb{Z})$ (on considère la base canonique $(e_i)_{i\in[1,n]}$ de $(\mathbb{Z}/p.\mathbb{Z})^n$, et l'application qui à σ dans σ_n associe l'application linéaire qui à e_i associe $\sigma(e_i)$.
Par le premier point, ce groupe admet un p-Sylow ; et par le deuxième point, un sous-groupe d'un groupe admettant un p-Sylow admet un p-Sylow.□

Corollaire 39 *Si G un est groupe de cardinal $p^r.m$ avec $p \not| m$ et p premier, alors G possède des sous-groupes d'ordre p^q pour tout $q \leq r$.*

Démonstration : G contient un p-Sylow, donc un sous-groupe de cardinal p^r. On peut donc se ramener au cas des p-groupes. Le centre d'un p-groupe est non trivial, comme on le montre en 1.10.1. On considère donc G un p-groupe, et $Z(G)$ son centre, de cardinal p^r. En appliquant l'hypothèse de récurrence à $Z(G)$, on a bien des groupes d'ordre p^q, pour $q \leq r$. On considère maintenant le groupe-quotient de G par $Z(G)$, il est de cardinal p^{r-q}, on peut donc lui appliquer l'hypothèse de récurrence et y trouver un groupe de cardinal p^t pour $t \leq r - q$. En considérant l'image inverse par la projection canonique sur le groupe quotient, on obtient alors un groupe de cardinal p^{t+q}, pour $t \leq r - q$, donc pour tout cardinal p^u avec $q \leq u \leq r$. □

Théorème 40 (Deuxième théorème de Sylow) *Etant donné G un groupe, de cardinal $|G| = p^r.m$, avec $p \not| m$.*
• *Tout p-groupe inclus dans G est inclus dans un p-Sylow de G.*
• *Les p-Sylow sont tous conjugués*
• *Les p-Sylow forment une orbite de G sous l'action de G par automorphisme intérieur*
• *Un p-Sylow est distingué si et seulement si il est l'unique p-Sylow*
• *Le nombre de p-Sylow est congru à 1 modulo p et divise $|G|$*
• *Le nombre de p-Sylow divise m*

Démonstration :
• Démonstration de l'affirmation "Tout p-groupe inclus dans G est inclus dans un p-Sylow de G" :
Supposons H un p-groupe de G. Soit S un p-Sylow de G, dont l'existence est donnée par le premier théorème de Sylow. D'après le lemme 38, il existe a dans G tel que $a.S.a^{-1} \cap H$ soit un p-Sylow de H.
H étant un p-groupe, H est nécéssairement égal à $a.S.a^{-1} \cap H$. Donc H est bien inclus dans un Sylow.

• Pour montrer l'affirmation "Les p-Sylow sont tous conjugués", il suffit de faire le même raisonnement avec H un p-Sylow.
• Démonstration de l'affirmation "Les p-Sylow forment une orbite de G sous l'action de G par automorphisme intérieur" :
On a vu que les p-Sylow étaient tous conjugués ; si un autre élément leur est conjugué, c'est aussi un p-Sylow ; le résultat est donc en fait complètement évident.
• Démonstration de l'affirmation "Un p-Sylow est distingué si et seulement si il est l'unique p-Sylow" :
Si un p-Sylow est distingué et s'il n'est pas unique alors il est conjugué à l'autre... donc il n'est pas distingué.
Réciproquement si il est unique, alors s'il n'est pas distingué, alors il est conjugué à un autre p-Sylow - donc il n'est pas unique.
• Démonstration de l'affirmation "Le nombre de p-Sylow est congru à 1 modulo p et divise $|G|$" :
On rappelle que la proposition 29 affirme que le nombre de points fixes d'un ensemble X sous l'action d'un p-groupe G est congru au cardinal de X modulo p.
Il suffit alors de considérer l'ensemble des p-Sylow ; on peut faire agir dessus un p-Sylow S quelconque par conjugaison. Le nombre de p-Sylow est donc congru au nombre de points fixes de l'ensemble des p-Sylow sous l'action de S modulo p. Il reste donc à montrer qu'il y a un unique point fixe. L'existence d'un point fixe est évidente, il s'agit de S lui-même. Supposons que T soit un autre point fixe, T est donc un p-Sylow tel que pour tout s dans S, $sTs^{-1} = T$. On considère le groupe engendré par T et S, S et T sont des p-Sylow de ce groupe. Dans ce groupe toujours, T est distingué ; donc il est l'unique p-Sylow, donc il est égal à S. D'où le résultat.
• Démonstration de l'affirmation "Le nombre de p-Sylow divise m" :
Le nombre de p-Sylow est le cardinal d'une orbite, donc il divise le cardinal de G, or il est congru à 1 modulo p, donc il divise m.□

1.6 Applications des groupes de Sylow

1.6.1 Démontrer qu'un groupe n'est pas simple juste au vu de son cardinal

Cet exemple est tiré de l'excellent [14].

Proposition 41 *Un groupe d'ordre 63 ne peut être simple.*

Démonstration : on considère les 7-Sylow de G d'ordre 63 ; ce nombre de p-Sylow divise $\frac{63}{7}$ donc 9, et est congru à 1 modulo p ; donc il y a un unique 7-Sylow, donc il est distingué, donc G n'est pas simple.□

1.7 Groupes abéliens

On rappelle qu'un groupe abélien est un groupe commutatif.

Proposition 42 *Un groupe abélien G est de type fini si et seulement si il existe un homomorphisme surjectif de $\mathbb{Z}^n$ sur G pour un certain n, c'est-à-dire s'il est isomorphe à un quotient de $\mathbb{Z}^n$ par un de ses sous-groupes*[a].
Plus précisément, G est alors engendré par n éléments, si n est minimal.

[a] Notez qu'il peut s'agir du quotient de $\mathbb{Z}^n$ par n'importe quel sous-groupe, puisque $\mathbb{Z}^n$ étant commutatif, tous ses sous-groupes sont distingués

Cela nous servira pour la proposition 48.

Démonstration : En effet, supposons que G est finiment engendré, par $g_1, ..., g_n$. Considérons alors l'application de $\mathbb{Z}^n$ dans G définie par $(p_1, ..., p_n) \mapsto p_1.g_1 + ... + p_n.g_n$. Puisque G est engendré par les g_i ET G est commutatif, cette application est surjective. Il est clair que c'est un morphisme puisque G est commutatif. Donc G est isomorphe au quotient de $\mathbb{Z}^n$ par le noyau de ce morphisme, d'où le résultat.

Réciproquement, supposons que l'on ait un morphisme surjectif de $\mathbb{Z}^n$ sur G ; alors il est égal à l'homomorphisme $(p_1, ..., p_n) \mapsto p_1.g_1 + ... + p_n.g_n$, avec g_i l'image de $(0, ..., 0_{i-1\text{fois}}, 1, 0, ..., 0)$ (voir la remarque de la partie 1.1.5). Il est donc clair que G est engendré par les g_i.□

Définition 43 (Somme) *Soit $(A_i)_{i\in I}$ une famille de groupes abéliens. On note $\bigoplus_{i\in I} A_i$ l'ensemble des familles $(x_i)_{i\in I}$ avec $x_i \in A_i$ et les x_i presque tous nuls ; c'est un groupe abélien pour l'addition terme à terme ; on l'appelle* **somme** *des groupes A_i.*
Si $i_0 \in I$, on identifie A_{i_0} à l'ensemble des $(x_i)_{i\in I}$ tels que $i \neq i_0 \rightarrow x_i = 0$.
Si $\forall i\ A_i = A$ alors on note $A^{(I)} = \bigoplus_{i\in I} A_i$.

Proposition 44 (Propriété universelle des groupes abéliens) *Etant donnée une famille $(A_i)_{i\in I}$ de groupes abéliens, A' un groupe abélien, ϕ_i un homomorphisme de A_i sur A', alors il existe un unique homomorphisme de $\bigoplus A_i$ vers A' tel que la restriction de cet homomorphisme à A_i soit ϕ_i.*

Démonstration : Considérer $\phi(x) = \sum_i \phi_i(x_i)$.□

Définition 45 (Somme directe) *A étant un groupe abélien, les A_i étant des sous-groupes de A, alors :*
• les A_i sont dits en **somme directe** *si l'application canonique de $\bigoplus A_i$ dans A qui à $(x_i)_{i\in I}$ associe $\sum_i x_i$ est injective. On identifie alors son image avec $\bigoplus_{i\in I} A_i$.*
• On dit que A est **somme directe** *des A_i si l'application est bijective. On note alors (abusivement) $A = \bigoplus_{i\in I} A_i$.*

Proposition 46 *A abélien, (A_i) famille de sous-groupes, alors les A_i sont en somme directe si $\sum_i x_i = 0$ avec $x_i \in A_i$ (support fini) implique $\forall i x_i = 0$.*

Définition 47 (Groupe de torsion) *Un élément d'un groupe est dit* **élément de torsion** *s'il est d'ordre fini.*
Un groupe abélien est dit **de torsion** *si tous ses éléments sont d'ordre fini.*
Etant donné p un nombre premier, un groupe abélien est dit **de p-torsion** *si tous ses éléments sont d'ordre une puissance de p.*
Un groupe abélien est dit **libre** *s'il est isomorphe à $\mathbb{Z}^n$ pour un certain $n \in \mathbb{N}$.*
On appelle **sous-groupe de torsion** *d'un groupe abélien G le sous-groupe constitué par les éléments de torsion[a].*

[a] On vérifie facilement qu'il s'agit bien d'un sous-groupe.

Proposition 48 *Un groupe de torsion[a] et de type fini est fini.*

[a] Sous-entendu : abélien (un groupe de torsion est abélien par définition).

Démonstration : En effet, si G est de type fini et abélien, alors c'est un quotient de $\mathbb{Z}^n$, par la proposition 42.

On considère alors $ppcm$ le ppcm des ordres des n générateurs donnés par la proposition 42. L'ordre de tout élément est alors un diviseur de $ppcm$. L'homomorphisme surjectif de $\mathbb{Z}^n$ dans son quotient a pour noyau un ensemble contenant $(k\mathbb{Z})^n$. Donc il se factorise à travers $(\mathbb{Z}/k\mathbb{Z})^n$ (voir le théorème 20). Donc le groupe G est de cardinal plus petit que k^n.□

Les deux théorèmes ci-dessous sont donnés sans démonstration (laissées aux lecteurs pour exercice !).

Théorème 49 *• Tout groupe abélien sans torsion de type fini est libre.*
• Tout sous-groupe d'un groupe libre est libre.
• Deux groupes libres $\mathbb{Z}^n$ et $\mathbb{Z}^p$ sont isomorphes si et seulement si $n = p$.
• Tout groupe abélien de type fini est produit d'un groupe libre et d'un groupe de torsion. Cette décomposition est unique à isomorphisme près.

Théorème 50 *Tout groupe abélien fini G s'exprime de manière unique sous la forme*

$$\mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}$$

avec $\forall i \in [1, n-1] a_i | a_{i+1}$, et $a_1 > 1$. Les a_i sont appelés **facteurs invariants** *du groupe.*
La décomposition ainsi obtenue est appelée **décomposition cyclique** *du groupe G.*

Cette décomposition a de nombreuses conséquences :

Corollaire 51 *Soit G un groupe abélien fini ; il existe un élément d'ordre le ppcm des ordres des éléments du groupe.*

Démonstration :
• Soit G un groupe abélien fini.
• La décomposition cyclique nous permet d'écrire G sous la forme

$$\mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}$$

• On considère un élément $x = (x_1, \ldots, x_n)$ de ce produit.
• L'ordre de x est le ppcm des ordres des x_i ; or l'ordre de x_i divise a_i, qui lui-même divise a_n.
• Le ppcm des ordres est donc en fait un diviseur de a_n, donc c'est a_n lui-même.
• L'élément $(0, \ldots, 0, 1)$ convient donc (on peut remplacer 1 par n'importe quel générateur de $\mathbb{Z}/a_n\mathbb{Z}$).□
Autre conséquence :

Corollaire 52 *Soit G un groupe abélien fini. Pour tout diviseur d de $Card(G)$, il existe un sous-groupe H de G d'ordre d.*

Démonstration :
• On écrit G sous forme :

$$\mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}$$

• Décomposons d en facteurs premiers :

$$d = \Pi_{i=1}^{m} p_i$$

• Définissons :

$$d_1 = pgcd(d, a_1)$$

$$d_2 = pgcd(\frac{d}{d_1}, a_2)$$

$$d_3 = pgcd(\frac{d}{d_1 d_2}, a_3)$$

$$\ldots$$

$$d_n = pgcd(\frac{d}{d_1 \dots d_n}, a_n)$$

• Puisque $d|n$ et $n = \Pi_{i=1}^{n} a_i$, on arrive à se "débarasser" de chaque facteur premier de d dans l'un des d_i, et donc $\Pi_{i=1}^{n} d_i = d$.

• Pour tout i, d_i divise a_i.

• Dans un groupe cyclique, il existe un sous-groupe du cardinal de n'importe quel diviseur de l'ordre du groupe, donc dans $\mathbb{Z}/(a_i\mathbb{Z})$ il existe un sous-groupe H_i de cardinal d_i.

• Le produit des H_i est un sous-groupe de G de cardinal d.□

Quelques autres corollaires, sans preuve :

Corollaire 53 *Soit G un groupe abélien fini. Soit $c = p_1^{n_1} p_2^{n_2} \dots p_l^{n_l}$ la décomposition de $c = card(G)$ en facteurs premiers. Alors pour tout $i \in [1, l]$ il existe un et un seul sous-groupe H_i de G de cardinal $p_i^{n_i}$. En outre, G est isomorphe au produit des H_i.*
Les H_i, uniques, sont appelés les composantes primaires du groupe commutatif G.

1.8 Exercices sur les groupes

1.8.1 Exemples de groupes

Les objets suivants sont-ils des groupes ?
$(\mathbb{C}^*, .), (\mathbb{R}^*, .), (\mathbb{C}, +), (\mathbb{R}, +), (\mathbb{R}, .), (\mathbb{Q}, +), (\mathbb{Q}, .), (\mathbb{N}, .), (\mathbb{Z}, +)$, l'ensemble des translations du plan, l'ensemble des homothéties du plan, l'ensemble à la fois des translations et des homothéties (pour la composition) ? Ces groupes sont-ils commutatifs ?

Oui, sauf $(\mathbb{R}, .)$, $(\mathbb{Q}, .)$, $(\mathbb{N}, .)$ et l'ensemble des homothéties. Tous ces groupes sont commutatifs sauf le groupe à la fois des translations et des homothéties.□

1.8.2 Conditions réduites pour un groupe

Si G a une lci[1] associative, un élément 1 tel que $\forall g \; ge = g$, et un élément g' pour tout g tel que $gg' = 1$, alors G est un groupe.

Démonstration : On multiplie gg' par g' à gauche, et on montre que $g'g = 1$ en utilisant le g'' tel que $g'g'' = 1$. Il est facile de voir que $eg = g$ en utilisant ceci.□

1.8.3 Conditions suffisantes de commutativité

Si tout élément est son propre inverse, alors G est commutatif.

1.8.4 $\mathbb{Z}/n\mathbb{Z}$

Proposition 54 *pour $d|n$, $\mathbb{Z}/n\mathbb{Z}$ comporte un seul sous-groupe d'ordre d.*

Démonstration : Existence triviale, unicité en considérant l'ensemble des élé-

[1] lci=loi de composition interne.

ments x tels que $x^d = 1$.□

Proposition 55 *Etant donnés deux entiers n et k, on a équivalence entre les trois assertions suivantes :*
- $\overline{k}$ (dans $\mathbb{Z}/n\mathbb{Z}$) engendre $\mathbb{Z}/n\mathbb{Z}$.
- n et k sont premiers entre eux.
- $\overline{k}$ est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$.

1.8.5 Sous-groupes

• Tout sous-groupe d'un groupe cyclique est cyclique.

• G sous-groupe de $(\mathbb{R}, +) \rightarrow G$ monogène ou dense.
Démonstration : Considérer l'inf de $\mathbb{R}^+ \cap G$.□

• Il existe des sous-groupes denses de $\mathbb{R}$ de type fini.
Démonstration : $\mathbb{Z} + \sqrt{2}\mathbb{Z}$□

• L'union de deux sous-groupes est un groupe si et seulement si l'un est inclus dans l'autre.

• Le produit élément par élémentde deux sous-groupes A et B est un sous-groupe si et seulement si $AB = BA$.
Démonstration : : Supposons que AB soit un sous-groupe. Alors soit $a \in A$ et $b \in B$. $a^{-1}b^{-1} \in AB \rightarrow ba \in AB$ donc $BA \subset AB$
ab admet un inverse dans AB donc $a'b'ab = 1$, donc $b'ab = a'^{-1}$, donc $ab = b'^{-1}a'^{-1}$, donc $ab \in BA$, donc $AB \subset BA$
Réciproquement, supposons $AB = BA$, alors l'inverse de ab, $b^{-1}a^{-1}$, appartient bien à AB ; en outre il est immédiat que AB est stable par produit.□

• L'image d'un sous-groupe distingué par un homomorphisme est un sous-groupe distingué de l'image de l'homomorphisme. L'image réciproque d'un sous-groupe distingué par un homomorphisme est un sous-groupe distingué.

• L'intersection de deux sous-groupes distingués est un sous-groupe distingué.

• Tout sous-groupe d'un groupe abélien est distingué ; mais on peut avoir cette propriété sans que le groupe soit abélien ; considérer par exemple $\{1, i, j, k, -1, -i, -j, -k\}$, muni des opérations $ij = k, ji = -k, jk = i, kj = -i, ki = j, ik = -j$ (notons que ce groupe possède aussi la propriété de n'avoir que des sous-groupes propres abéliens).

1.8.6 Divers

• Dans un groupe, $(ab)^n = 1$; montrer que $(ba)^n = 1$.

• Montrer que $\mathbb{Q}$ n'est pas de type fini.

Démonstration : Considérer un nombre fini d'éléments de $\mathbb{Q}$, et un dénominateur commun de ces éléments.□

• L'ensemble des automorphismes de $\mathbb{Z}/n\mathbb{Z}$ muni de la composition est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, \times)$.

• Un sous-groupe additif de $\mathbb{R}$ est soit dense, soit de la forme $a.\mathbb{Z}$. De même, $\mathbb{R}^{+*}$ muni de la multiplication n'admet que des sous-groupes denses ou de la forme $a^{\mathbb{Z}}$.

Démonstration : Considérer la borne inf de l'intersection du sous-groupe et de $\mathbb{R}^{+*}$. Le cas multiplicatif s'obtient en considérant le log, qui est un isomorphisme de groupe, et qui préserve la densité.□

• $\mathbb{Z} + b\mathbb{Z}$ dans $(\mathbb{R}, +)$ est de la forme $a.\mathbb{Z}$ si b est rationnel, et dense si b est irrationnel.

1.9 Zoologie des opérations d'un groupe sur un ensemble

1.9.1 Opération d'un groupe G sur lui-même par translation à gauche

On associe à tout élément g de G la fonction qui à $x \in G$ associe $g.x$.

Cette opération est transitive (il y a une seule orbite) et fidèle.

Théorème 56 (Théorème de Cayley) *Si G est fini, alors G est isomorphe à un sous-groupe du groupe des permutations de G.*

Démonstration : L'application qui à g associe l'application $x \mapsto g.x$ est un homomorphisme injectif ; donc G est isomorphe à son image par cette application, qui est donc un sous-groupe du groupe des permutations de G.□

Pour "fixer les idées", on peut se représenter $\mathbb{Z}/n\mathbb{Z}$ isomorphe à l'ensemble des applications qui à $\overline{x}$ associe $\overline{x} + \overline{p}$.

1.9.2 Opération d'un groupe G sur le groupe G/H par translation à gauche

Définition 57 (Action par translation à gauche) *A g un élément et une classe $g'.H$ on associe la classe $g.g'.H$. On vérifie facilement que cette opération est bien définie et définie bien une opération d'un groupe sur un ensemble. L'opération est clairement transitive, par contre elle n'est pas fidèle en général. Le noyau de l'application ϕ associée (voir définition d'un opération d'un groupe sur un ensemble) est égal à*

$$\cap_{g\in G} g.H.g^{-1}$$

(par définition du noyau, il suffit de l'écrire)

1.9.3 Opération d'un groupe sur lui-même par automorphismes intérieurs

Définition 58 (Action par automorphismes intérieurs) *A $g \in G$ on associe l'automorphisme intérieur $x \mapsto g.x.g^{-1}$.*

Proposition 59 • *Les orbites sont exactement les classes d'équivalence pour la relation de conjugaison.* • *Le stabilisateur d'un élément x est l'ensemble des g tels que $x = g.x.g^{-1}$, c'est à dire $x.g = g.x$; c'est donc l'ensemble des éléments qui commutent avec x, on l'appelle* **centralisateur** *de x. On généralise cette définition en l'élargissant aux parties de G ; le* **centralisateur** *d'une partie est l'ensemble des éléments qui commutent avec tous les éléments de cette partie.*
• *Le centralisateur de G tout entier est donc le centre de G, c'est à dire l'ensemble des éléments qui commutent avec tous les autres.*
• *Les éléments d'une classe de conjugaison ont même ordre et même nombre de points fixes.*
On peut par exemple considérer le groupe $GL(n, \mathbb{K})$; les classes de conjugaison, c'est à dire les orbites, sont alors les classes d'équivalence pour la relation "être semblable à".

1.10 Zoologie des groupes

On trouvera une étude des groupes $\mathbb{Z}/n\mathbb{Z}$ et $(\mathbb{Z}/n\mathbb{Z})^*$ dans la partie2.5.

1.10.1 Les p-groupes

Rappelons qu'un p-groupe est un groupe de cardinal (donc d'ordre) p^r avec p un nombre premier.

Proposition 60 (Le centre d'un p-groupe non trivial est non trivial) *Si G est un p-groupe de cardinal > 1 alors son centre est de cardinal > 1.*

Démonstration : On fait agir G sur lui-même par automorphismes intérieurs, comme indiqué en 1.9.3, et on applique la proposition 1.10.1. On en déduit que le centre est de cardinal congru à p, or il est non réduit à 0.□

1.10.2 Groupe linéaire et groupe spécial linéaire

Définition 61 *Etant donné $\mathbb{K}$ un corps commutatif quelconque et E un $\mathbb{K}$-espace vectoriel de dimension finie, on appelle* **groupe linéaire** *$GL(E)$ le groupe des automorphismes de E.*

$GL(E)$ est isomorphe à $GL(n, \mathbb{K})$, groupe des matrices inversibles de taille $n \times n$, à coefficients dans $\mathbb{K}$, avec n la dimension de E.

On notera que deux matrices semblables A et B vérifient qu'il existe P tel que $A = P^{-1}.B.P$; cela revient donc à dire que A et B sont conjuguées.

Définition 62 *Le noyau de l'homomorphisme qui à f associe son déterminant est par définition l'ensemble des automorphismes de déterminant 1 ; on l'appelle* **groupe spécial linéaire** *et on le note $SL(E)$.*

$SL(E)$ est isomorphe à $SL(n, \mathbb{K})$, groupe des matrices de $GL(n, \mathbb{K})$ de déterminant 1.

Proposition 63 *On a une suite exacte :*

$$1 \to SL(E) \to GL(E) \xrightarrow{\text{dét}} \mathbb{K}^* \to 1$$

En outre, le groupe linéaire $GL(E)$ est isomorphe au produit semi-direct du groupe spécial linéaire $SL(E)$ par $\mathbb{K}^*$.

$\mathbb{K}^*$ désignant $\mathbb{K} - \{0\}$.

Démonstration : Il suffit de prendre pour injection de $SL(E)$ dans $GL(E)$ la

simple identité, et de considérer le sous-groupe H de $GL(E)$ des matrices de la forme

$$\begin{pmatrix} \lambda & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \ddots & 0 & 1 & 0 \\ 0 & 0 & \dots & 0 & 0 & 1 \end{pmatrix}$$

avec λ non nul.

Le déterminant induit bien une bijection de H sur $\mathbb{K}^*$, on a bien $H \cap SL(E)$ réduit à l'élément neutre, on a bien $SL(E).H = GL(E)$, et $SL(E)$ est clairement distingué. □

Proposition 64 (Générateurs de $GL(E)$ et $SL(E)$) • *$GL(E)$ est engendré par l'ensemble des dilatations de E.*
• *$SL(E)$ est engendré par l'ensemble des transvections de E.*

Démonstration : Je ne détaillerai pas intégralement la preuve, laborieuse, mais peu difficile. Il suffit de montrer les points suivants, dans cet ordre :

• Toute matrice de la forme $I + \lambda E_{i,j}$ pour $i \neq j$, avec $\lambda \in \mathbb{K}$ et $E_{i,j}$ la matrice définie par $(E_{i,j})_{k,l} = 1$ si $i = k$ et $j = l$ et 0 sinon, est la matrice d'une transvection. L'inverse d'une matrice de transvection, est une matrice de transvection.

• Une matrice de déterminant 1 est égale à un produit de matrices de transvections. Pour le prouver, on considère M une telle matrice, on la multiplie par des matrices de transvection pour se ramener à une matrice n'ayant qu'un seul élément non nul sur la première ligne, pour que cet élément soit l'élément en haut à gauche, et pour qu'il soit égal à 1. Il suffit alors de procéder par récurrence en considérant un produit de matrices par bloc.

(ce point est exactement le deuxième point annoncé)

• Une matrice appartenant à $GL(E)$ est le produit d'une matrice appartenant à $SL(E)$ et d'une matrice de dilatation (voir proposition 63).□

1.10.3 Groupe orthogonal et groupe spécial orthogonal

⊡ **Cas général**

Définition 65 *On appelle* **groupe orthogonal d'un espace euclidien** *E l'ensemble des automorphismes orthogonaux de E muni de la composition $\circ$; on le note $O(E)$.*
On appelle **groupe spécial orthogonal d'un espace euclidien** *E l'ensemble des automorphismes orthogonaux de E de déterminant 1 muni de la composition $\circ$; on le note $SO(E)$ ou $O^+(E)$.*
On note $O^-(E)$ le complémentaire de $SO(E)$ dans $O(E)$.
On note en outre $O_n(\mathbb{R})$ l'ensemble $O(\mathbb{R}^n)$.
On note en outre $SO_n(\mathbb{R})$ l'ensemble $SO(\mathbb{R}^n)$.

Ces espaces sont isomorphes aux espaces décrits en 1.10.4, donc je n'approfondis pas plus ici pour le moment, à part les cas spéciaux des dimensions 1, 2 et 3.

⊡ Dimension 1

Ce cas est de peu d'intérêt ; les seules transformations orthogonales sont $x \mapsto x$ et $-x \mapsto -x$...

⊡ Dimension 2

Un rapide calcul montre que les matrices des transformations orthogonales en dimension 2 sont de l'une des deux formes suivantes :

$$\begin{pmatrix} cos(\theta) & -sin(\theta) \\ sin(\theta) & cos(\theta) \end{pmatrix} \begin{pmatrix} cos(\theta) & sin(\theta) \\ sin(\theta) & -cos(\theta) \end{pmatrix}$$

La matrice de gauche représente une transformation du groupe spécial orthogonal (c'est à dire de déterminant 1, et donc dans $SO(E) = O^+(E)$), celle de droite une transformation qui n'est pas de ce groupe (c'est à dire que celle-ci est de déterminant -1, et donc dans $O^-(E)$).

(le calcul est facile, il suffit de se souvenir que $x^2+y^2 = 1 \rightarrow \exists\theta / x = cos(\theta)$ et $y = sin(\theta)$)

Définition 66 *On appelle* **rotation d'angle** θ *un endomorphisme associé à la matrice :*

$$\begin{pmatrix} cos(\theta) & -sin(\theta) \\ sin(\theta) & cos(\theta) \end{pmatrix}$$

Toujours par des calculs sans grande difficulté on montrerait que $SO_2(\mathbb{R})$ commute, et est en fait isomorphe à $\mathbb{R}/(2.\Pi.\mathbb{Z})$; les seules transformations orthogonales de déterminant 1 sont en fait les rotations. On note r_θ la rotation d'angle θ.

En étudiant la matrice de droite, on constate qu'elle est symétrique, donc diagonalisable (voir la partie **??**) ; son polynôme caractéristiques est $X^2 - 1$; elle est semblable à $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Il s'agit donc en fait d'une symétrie par rapport à un hyperplan (ici hyperplan = droite car on est en dimension 2). Ainsi les transformations orthogonales de déterminant -1 sont en fait des symétries par rapport à des droites. On note que les symétries ne commutent pas, elles. On note s_θ la symétrie correspondant θ (θ est en fait le double de l'angle de l'axe invariant avec le premier axe).

On notera que $s_\theta \circ s_{\theta'} = r_{\theta-\theta'}$.

⚠ l'angle n'est défini qu'à $2.\Pi$ près pour les rotations et les symétries.

⊡ **Dimension** 3

Proposition 67 *En dimension* 3, $O^+(E)$ *comporte :*
• *les rotations axiales*
• *l'identité, qui est un cas particulier de rotation axiale*
• *la symétrie par rapport à une droite, qui est un cas particulier de rotation axiale*
En dimension 3, $O^-(E)$ *comporte :*
• *les symétries orthogonales par rapport à un plan*
• *les composées d'une rotation autour d'un axe et d'une symétrie par rapport au plan orthogonal à cet axe*

On se donne f un endomorphisme orthogonal de E euclidien de dimension 3, et on considère I l'ensemble $\{x/f(x) = x\}$ (ensemble des invariants par f). On va classer les f possibles suivant la dimension de I.

◇ $dim\ I = 3$
Pas drôle : f est l'identité, et donc $f \in SO(E) = O^+(E)$.

◇ $dim\ I = 2$
Alors l'orthogonal de I est de dimension 1 ; la restriction de f à cet espace est un endomorphisme orthogonal (rappelons que si un espace est stable pour un endomorphisme orthogonal, alors son orthogonal aussi). Ce n'est pas l'identité puisque f n'est pas l'identité, donc il s'agit de $x \mapsto -x$ (si un endormorphisme est orthogonal, ses seules valeurs propres possibles sont 1 et -1). f est donc une symétrie par rapport à un plan. $f \in O^-(E)$.

◇ $dim\ I = 1$
La restriction de f à l'orthogonal de I (rappelons que si un espace est stable pour un endomorphisme orthogonal, alors son orthogonal aussi) est un endomorphisme orthogonal et n'a pas de vecteur invariant ; donc c'est une rotation. Donc f est une rotation autour d'un axe. Sa matrice est semblable à la matrice

$$\begin{pmatrix} cos(\theta) & -sin(\theta) & 0 \\ sin(\theta) & cos(\theta) & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

f est de déterminant 1, et donc appartient à $SO(E) = O^+(E)$.

◇ $dim\ I = 0$
En dimension 3, tout endomorphisme admet au moins une valeur propre (tout polynôme de degré impair admettant au moins une racine sur $\mathbb{R}$).
f admet donc nécéssairement une valeur propre. Or un endomorphisme orthogonal ne peut avoir pour valeur propre que 1 ou -1 ; donc -1 est valeur propre.
On va maintenant considérer O, l'ensemble des x tels que $f(x) = -x$, et on va raisonner sur la dimension de O.

$dim\ O = 3$ On a alors f la symétrie par rapport à 0 ; f est dans $O(E)$ et pas dans $SO(E)$; f est dans $O^-(E)$.

$dim\ O = 2$ **: cas impossible** Supposons $dim\ O = 2$.

Alors l'orthogonal de O est stable par f ; donc soit la restriction de f à cet orthogonal est l'identité, soit c'est moins l'identité ; puisque $dim\ I = 0$ il s'agit de moins l'identité. Donc en fait $dim\ O = 3$, d'où contradiction. Donc ce cas ne peut se produire.

$dim\ O = 1$

On considère alors la restriction de f à l'orthogonal de O. Il s'agit d'un endomorphisme orthogonal en dimension 2, sans valeur propre ; donc une rotation qui n'est pas une symétrie par rapport à un point, ni l'identité. f est de déterminant -1, et donc est dans $O(E)$ mais pas dans $SO(E)$; $f \in O^-(E)$.

1.10.4 Groupe orthogonal réel et groupe spécial orthogonal réel

Définition 68 *On appelle* **groupe orthogonal réel d'ordre** n *l'ensemble des matrices M réelles de type (n, n) telles que ${}^tM.M = I$, on le note $O_n(\mathbb{R})$; il s'agit d'un sous-groupe du groupe linéaire réel d'ordre n.*
On appelle **groupe spécial orthogonal réel d'ordre** n *l'ensemble des matrices M réelles de type (n, n) telles que ${}^tM.M = I$ et $det\ M = 1$, on le note $SO_n(\mathbb{R})$; il s'agit d'un sous-groupe du groupe orthogonal réel d'ordre n et d'un sous-groupe du groupe spécial linéaire d'ordre n.*
On appelle **matrice orthogonale** *une matrice appartenant à $O_n(\mathbb{R})$ pour un certain n.*

Proposition 69 (Propriété des matrices orthogonales réelles) *Une matrice est orthogonale si et seulement si sa transposée l'est.*
Une matrice est orthogonale si et seulement si ses vecteurs colonnes forment une famille orthonormale de $\mathbb{R}^n$.
Une matrice est orthogonale si et seulement si ses vecteurs lignes forment une famille orthonormale de $\mathbb{R}^n$.
Une matrice est orthogonale si et seulement si il s'agit d'une matrice de changement de bases orthonormales.
Une matrice orthogonale est de déterminant 1 ou -1.
Une valeur propre de matrice orthogonale est soit 1 soit -1.
Une matrice orthogonale M vérifie $com(M) = det(M).M$.

1.10.5 Groupe affine d'un espace affine

Définition 70 *On appelle* **groupe affine d'un espace affine** X *l'ensemble des applications affines bijectives de* X *dans lui-même muni de la composition ; c'est un groupe. On le note* $GA(X)$.
On appelle **groupe spécial affine d'un espace affine** X *l'ensemble des applications affines bijectives* f *de* X *dans lui-même telles que* $det\ \overrightarrow{f} = 1$, *muni de la composition ; c'est un groupe. On le note* $SA(X)$.

Le fait qu'il s'agisse d'un groupe est facile à voir. La proposition suivante est évidente :

Proposition 71 *L'application* $f \mapsto \overrightarrow{f}$ *est un morphisme de* $GA(X)$ *dans* $GL\overrightarrow{X}$.

Etudions maintenant la structure du groupe $GA(X)$.

⊡ **Générateurs de** $GA(X)$ **et** $SA(X)$

Proposition 72 • $GA(X)$ *est engendré par l'ensemble des dilatations affines de* X
• $SA(X)$ *est engendré par l'ensemble des transvections affines de* X

Démonstration : Simple conséquence de la proposition 64.□

⊡ **Sous-groupes remarquables de** $GA(X)$

◇ **Le sous-groupe des symétrie**
L'ensemble des symétries est un sous-groupe distingué de $GA(X)$. En effet, avec $s_{A,\overrightarrow{B}}$ la symétrie par rapport à A parallèlement à $\overrightarrow{B}$, on a

$$g \circ s_{Y,\overrightarrow{Z}} \circ g^{-1} = s_{g(Y),\overrightarrow{g}(\overrightarrow{Z})}$$

◇ **Le sous-groupe des translations**
L'ensemble $T(X)$ des translations de l'espace affine X est un groupe pour la composition ; ce groupe est distingué. On le voit en constatant que c'est le noyau du morphisme qui à f dans $GA(X)$ associe $\overrightarrow{f}$ dans $GL(\overrightarrow{X})$.
Le groupe quotient de X par $T(X)$ est isomorphe à $\overrightarrow{X}$.

◇ **Le sous-groupe des homothéties-translations**
L'ensemble des homothéties et des translations d'un espace affine X est stable par composition et contient l'identité ; or il est inclus dans $GA(X)$. Donc c'est un sous-groupe de $GA(X)$. Il est généré par les homothéties (toute translation s'exprime comme composée de deux homothéties de rapport inverse).
Ce sous-groupe est exactement l'ensemble des bijections de X transformant toute droite en une droite parallèle.

◇ **Le sous-groupe des applications affines bijectives de X laissant une partie donnée invariante**

On fixe une partie P de X, et on considère G l'ensemble des f appartenant à $GA(X)$ telles que $f(P) \subset P$; G est stable par composition et contient l'identité, c'est donc un sous-groupe de $GA(X)$.

◇ **En dimension finie, le sous-groupe des applications affines laissant fixe un repère**

On suppose que X est de dimension finie n. On se donne alors un repère affine $A_0, A_1, ..., A_n$.

Nécéssairement, une bijection affine f laissant invariant un repère a pour restriction à la partie $\{A_0, ..., A_n\}$ une permutation σ. Une application affine étant entièrement déterminée par l'image d'un repère affine, on en déduit que l'ensemble des applications affines bijectives laissant invariant le repère $A_0, A_1, ..., A_n$ est un groupe isomorphe à σ_{n+1}

⊡ **Le groupe affine comme produit semi-direct**

On a vu que $T(X)$, ensemble des translations de X, est distingué dans $GA(X)$, puisque noyau du morphisme $f \mapsto \overrightarrow{f}$. On a une suite exacte

$$\begin{array}{ccccc} & & f \mapsto \overrightarrow{f} & & \\ 1 \to T(X) & \to & GA(X) & \to & GL(\overrightarrow{X}) \to 1 \end{array}$$

On se donne O appartenant à X donné ; l'application $f \mapsto \overrightarrow{f}$ induit une bijection de l'ensemble des bijections affines de X laissant O invariant sur $\overrightarrow{X}$; on a donc un relèvement de $GL(\overrightarrow{X})$.

Donc $GA(X) = T(X) \rtimes GL(\overrightarrow{X})$, avec pour action de $GL(X)$ dans $T(X)$ $\overrightarrow{f}.t = f_0^{-1} \circ t \circ f_0$ avec f_0 l'application affine laissant O invariant et associée à $\overrightarrow{f}$ (ce qui revient à $\overrightarrow{f}.t_{\overrightarrow{a}} = t_{\overrightarrow{f}(\overrightarrow{a})}$, en notant $t_{\overrightarrow{u}}$ la translation de vecteur $\overrightarrow{u}$).

En considérant l'isomorphisme évident entre $T(X)$ et $\overrightarrow{X}$ (c'est-à-dire en remplaçant une translation par le vecteur de cette translation) on peut aussi écrire

$$GA(X) = \overrightarrow{X} \rtimes GL(\overrightarrow{X})$$

Et quel que soit O dans X on peut écrire toute application bijective affine f de X dans X sous la forme $f = t \circ u_0$ avec u_0 application affine bijective laissant 0 invariant.

1.10.6 Groupe projectif d'un espace vectoriel de dimension finie

Définition 73 - Proposition *On se donne E un $\mathbb{K}$-espace vectoriel de dimension finie. L'ensemble des homographies de $P(E)$ dans $P(E)$ forme un groupe pour $\circ$, appelé* **groupe projectif de** *E, noté $PGL(E)$. Ce groupe est isomorphe à $GL(E)/(\mathbb{K} \setminus \{0\}.I)$, avec I l'identité de E dans E.*
On note usuellement $PGL_n(\mathbb{K})$ pour $PGL(\mathbb{K}^n)$.

Démonstration : Seul l'isomorphisme mérite d'être détaillé.

Considérons l'application H, qui à un endomorphisme de E associe l'homographie associée à cet endomorphisme (on se donne bien entendu pour cela un repère projectif de E).

Son noyau est l'ensemble des applications linéaires de E dans E qui laissent toute droite invariante. Il faut donc montrer qu'un endomorphisme laissant toute droite invariante est une homothétie.

Lemme 74 *Un endomorphisme d'un espace vectoriel de dimension finie laissant invariante toute droite est une homothétie.*

Démonstration : On procède par récurrence sur la dimension n de l'espace vectoriel .

Pour $n = 1$ le résultat est clair.

Pour $n > 1$, on considère f un endomorphisme de E, tel que pour tout x il existe un scalaire λ_x tel que $f(x) = \lambda_x.x$.

Il est clair que si x et y de E sont liés, alors $\lambda_x = \lambda_y$.

Considérons maintenant x et y linéairement indépendants.

Alors $f(x + y) = \lambda_{x+y}.x + \lambda_{x+y}.y = f(x) + f(y) = \lambda.x + \lambda.y$, donc $\lambda_x = \lambda_{x+y} = \lambda_y$.

On a donc montré le résultat souhaité.□

Du coup, grâce à ce lemme, la preuve de la proposition est achevée.□

1.10.7 Groupe unitaire et groupe spécial unitaire d'un espace hermitien

Définition 75 *On appelle* **groupe unitaire de** E *et on note* $U(E)$ *avec* E *un espace hermitien (voir partie**??**) l'sensemble des automorphismes unitaires de* E*, c'est-à-dire des automorphismes* f *de* E *tels que* $f^{-1} = f^*$*, muni de la composition.*
On appelle **groupe spécial unitaire de** E*, et on note* $SU(E)$*, avec* E *un espace hermitien, le sous-groupe de* $U(E)$ *constitué des automorphismes unitaires de* E *de déterminant* 1.

Ces groupes sont isomorphes aux groupes dont il est question ci-dessous.

On note bien que le déterminant d'un élément de $U(E)$ peut être n'importe quelle valeur du cercle unité, et pas seulement 1 et -1 comme dans le cas des endomorphismes orthogonaux d'un espace euclidien.

1.10.8 Groupe unitaire complexe d'ordre n et groupe spécial unitaire complexe d'ordre n

Définition 76 *L'ensemble des matrices M de type (n,n) à coefficients dans $\mathbb{C}$ telles que ${}^t\overline{M}.M = I$ est un groupe pour $\circ$; on l'appelle* **groupe unitaire complexe d'ordre** *n, et on le note $U_n(\mathbb{C})$.*
L'ensemble des matrices M de type (n,n) à coefficients dans $\mathbb{C}$ telles que ${}^t\overline{M}.M = I$ et $det\ M = 1$ est un groupe pour $\circ$; on l'appelle **groupe spécial unitaire complexe d'ordre** *n ; on le note $SU_n(\mathbb{C})$, c'est un sous-groupe de $U_n(\mathbb{C})$.*

1.10.9 Groupe des similitudes d'un espace euclidien

Définition 77 *On appelle* **groupe des similitudes d'un espace euclidien** *E et on note $GO(E)$ l'ensemble des similitudes d'un espace euclidien E, muni de la composition $\circ$. On appelle* **groupe des similitudes d'un espace euclidien** *E et on note $GO(E)$ l'ensemble des similitudes d'un espace euclidien E, muni de la composition $\circ$.*

Il s'agit d'un groupe, sous-groupe de $GL(E)$ (groupe linéaire de E, ensemble des automorphismes de E.

Il est isomorphe à $\mathbb{R}_+^* \times O(E)$, avec $O(E)$ l'ensemble des automorphismes orthogonaux de E.

1.10.10 Groupe des quaternions

Définition 78 *On le note H_8. Ses éléments sont $1, -1, i, j, k, -i, -j, -k$, et la multiplication est définie par la table suivante :*

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

On peut aussi résumer la loi de multiplication par

$$ij = k, jk = i, ki = j$$

$$ji = -k, kj = -i, ik = -j$$

$$i^2 = j^2 = k^2 = -1$$

$$D(H_8) = \{1, -1\}$$

$$Z(H_8) = \{1, -1\}$$

Ce groupe n'est pas commutatif. Ses sous-groupes sont $\{1\}$, $\{1, -1\}$, $\{1, -1, i, -i\}$ et H_8 lui-même ; ils sont tous distingués. Cela montre d'ailleurs que la propriété des groupes abéliens d'avoir tous leurs sous-groupes distingués n'est pas une condition suffisante pour que le groupe soit abélien.

1.10.11 Groupe symétrique

Définition 79 *On appelle* **permutation** *d'un ensemble une bijection de cet ensemble sur lui-même.*
On appelle **support** *d'une permutation sur un ensemble tout élément de cet ensemble qui n'est pas invariant par cette permutation.*
On appelle **cycle** *d'un ensemble une bijection f telle qu'il existe $a_1, ..., a_n$ (en nombre fini et distincts) tels que $f(a_i) = a_{i+1}$ pour $i < n$, $f(a_n) = a_1$ et $f(b) = b$ si b n'est aucun des a_i. n est l'ordre du cycle ; il ne s'agit pas d'une définition, car cet ordre colle à la notion d'ordre sur les éléments d'un groupe. n est aussi appelé* **longueur** *du cycle (cette fois-ci c'est bien une définition !).*
*On appelle n-***cycle** *un cycle d'ordre n.*
On appelle **transposition** *une permutation qui «échange» deux éléments. On note (a, b) la transposition qui échange a et b. Une transposition est un cycle est longueur 2.*
On appelle **groupe symétrique** *d'un ensemble E l'ensemble des permutations de cet ensemble.*
*On note σ_n et on appelle n-***ième groupe symétrique standard** *le groupe symétrique de $\{1, 2, ..., n\}$. Tous les groupes symétriques sur des ensembles de cardinal n sont isomorphes à σ_n.*
Pour un n donné on appelle **signature** *l'unique homomorphisme ϵ de σ_n dans $\{1, -1\}$ tel que $\epsilon(\tau) = -1$ lorsque τ est une permutation.*
*On appelle n-***ième groupe alterné** *le noyau de ϵ (dans σ_n). On le note U_n.*
On appelle **matrice associée la permutation** σ **de** σ_n *la matrice M telle que $M_{i,j} = \delta_{i,\sigma(j)}$.*

Remarques et propriétés :
• On parle aussi, au lieu de n-ième groupe symétrique standard, de **groupe symétrique d'ordre** n ; il faut bien voir que ce groupe n'est *PAS* d'ordre n mais d'ordre $n!$.
• Pour bien faire il faudrait démontrer que l'on caractérise bien ici la signature. Cela serait fait dans la partie 1.10.11.

Proposition 80 • $|\sigma_n| = n!$
• $Z(\sigma_n) = 1$ *si* $n \geq 3$.
• σ_n *est engendré par les transpositions*
• σ_n *est engendré par les transpositions de la forme* $(a, a + 1)$, *avec* $a \in [1, n - 1]$.
• σ_n *est engendré par les transpositions de la forme* $(1, a)$, *avec* $a \in [1, n]$.
• σ_n *est engendré par la transposition* $(1, 2)$ *et le cycle* $(1, 2, ..., n)$.
• U_n *est engendré par les cycles d'ordre* 3.
• *Des cycles de supports disjoints commutent.*

Proposition 81 *Soit p une permutation de E fini. L'orbite d'un point x pour p est l'ensemble des $p^n(x)$ avec $n \in \mathbb{N}$. p est un cycle s'il existe une orbite et une seule qui soit de cardinal > 1.*

Démonstration : Si on a un cycle, il est clair qu'il existe une seule orbite de cardinal > 1 ; si on a une seule orbite dans ce cas, alors on considère les éléments de l'orbite, la suite est évidente.□

Théorème 82 *Toute permutation peut s'écrire comme produit de cycles de supports deux à deux disjoints. La décomposition est unique à l'ordre près des facteurs.*

Démonstration :

Considérons une permutation σ de $[1, n]$. L'unicité de sa décomposition sous la forme annoncée découle immédiatement de l'étude des orbites de l'action de $\{Id, \sigma\}$ sur $[1, n]$ (on considère ce qu'il se passe sur chaque orbite).

Pour l'existence, on se restreint aussi à une telle orbite. Il est clair que σ se comporte sur cette orbite comme un cycle. D'où le résultat.□

Proposition 83 *Le centre de σ_n est trivial dès que $n \geq 3$.*

Démonstration : Soit σ élément non neutre de σ_n. Il existe alors i tel que $\sigma(i) = j \neq i$. On prend alors k différent à la fois de i et de j, et on constate que $\sigma \circ (j\ k)(i) \neq (j\ k) \circ \sigma(i)$□

⊡ La conjugaison dans σ_n

On considère l'opération de σ_n sur σ_n par automorphisme intérieur, comme étudié en 1.9.3.

Proposition 84 • *Cette opération est transitive, et même k transitive pour tout k. Elle est fidèle pour $n \geq 3$, puisqu'alors le centre est trivial.*
• *Si on se limite à U_n, cette opération est $n-2$ fois transitive.*

Démonstration : Le premier point est évident. Pour le second, on considère $k \leq n-2$ éléments de $\{1, ..., n\}$, et on ajoute deux autres points ; on considère la permutation qui affecte nos k points correctements, et qui, si la permutation obtenue est impaire, permute les deux points supplémentaires.□

Proposition 85 • *Pour tout m, l'ensemble des cycles d'ordre m est une orbite (c'est à dire une classe de conjugaison).*
• *Si $n \geq 5$ les cycles d'ordre 3 sont conjugués dans U_n.*

Démonstration : Remarquons tout d'abord que si $f = (x_1, ..., x_k) \in \sigma_n$ et $g \in \sigma_n$, alors $g.f.g^{-1} = (g(x_1), ..., g(x_k))$. Pour montrer le premier point, il suffit alors, étant donnés deux cycles de même longueur $(x_0, ..., x_k)$ et $(y_0, ..., y_k)$ de considérer la permutation p qui à x_i associe y_i ; on a bien $p.x.p^{-1} = y$.
Le deuxième point est plus délicat, et utilise la proposition 84. Etant donnés deux 3-cycles (x_0, x_1, x_2) et (y_0, y_1, y_2), on considère la permutation p de U_n qui à x_i associe y_i ; on a bien $x = p.y.p^{-1}$.□

⊡ Les matrices de permutations

Définition 86 *L'application ϕ qui à une permutation associe la matrice associée à cette permutation est un morphisme injectif dans $GL_n(\mathbb{K})$ (ensemble des matrices inversibles de type (n, n)).*
On a la propriété $\phi(s)^{-1} = \phi(\sigma^{-1}) =^t \phi(\sigma)$.
Le déterminant de $\phi(s)$ est égal à la signature de s.

⊡ La signature

Proposition 87 (Différentes caractérisations de la signature) *On peut définir la signature ϵ sur σ_n de l'une des façons suivantes :*
1) On appelle **inversion** *d'une permutation p, une paire (i, j) d'éléments tels que $(j - i).(p(j) - p(i)) < 0$. On définit $\epsilon(p) = (-1)^{Inv(p)}$, avec $Inv(p)$ le nombre d'inversions.*
2) Il existe un unique morphisme ϵ de σ_n sur $\{-1, 1\}$ tel que $\epsilon(t) = -1$ si t est une permutation.
3) $\epsilon(p)$ est égal à $(-1)^s$ avec s le nombre de transpositions dans une décomposition de p en produit de transpositions.

Démonstration : Pas très très dur... Pour voir que 1 entraine 2 il faut voir que $\epsilon(p)$ est le produit des $\Pi_{i<j} \frac{p(j)-p(i)}{j-i}$, le reste est facile.□
Il y a en outre une caractérisation de la signature, donnée en 1.10.11.

⊡ Simplicité de U_n pour $n > 4$; conséquences

Cette preuve est tirée de [14, p. 28], fort bon livre en algèbre, pour ceux qui connaissent déjà les bases du moins.

Théorème 88 *U_n est simple (i.e. sans sous-groupe distingué non trivial) si $n \geq 5$.*

Démonstration : On procède en deux étapes :
• Le cas $n = 5$
- Le groupe U_5 se décompose en 60 éléments ; l'identité, 15 éléménts d'ordre 2, qui sont des produits de deux transpositions disjointes, 20 éléments d'ordre 3, qui sont des 3-cycles, et 24 d'ordre 5, qui sont des 5-cycles. On va se préoccuper des classes de conjugaison de U_5.
- les éléments d'ordre 2 sont conjugués (facile).
- les 3-cycles sont conjugués.
Supposons H sous-groupe de U_5, et $H \lhd U_5$, et $H \neq \{1\}$.
- S'il contient un élément d'ordre 3 il les contient tous, puisqu'il est distingué et que les éléments d'ordre 3 sont conjugués.
- S'il contient un élément d'ordre 2 il les contient tous, puisqu'il est distingué et que les éléments d'ordre 2 sont conjugués.
- S'il contient un éléments x d'ordre 5, alors il contient aussi le 5-Sylow engendré par x (voir les théorèmes de Sylow, 1.5). Les 5-Sylow étant tous conjugués, il les contient donc tous ; tout élément d'ordre 5 étant inclus dans un 5-sylow, tout élément d'ordre 5 est alors inclus dans H.
- S'il contient donc un seul type d'éléments parmi les éléments ci-dessus en plus de l'unité, alors alors son cardinal serait soit $1 + 20$, soit $1 + 24$, soit $1 + 15$; or ces nombres ne divisent pas 60. Donc il contient au moins deux types de ces éléments. Donc son cardinal est au moins $1 + 15 + 20$, et comme il divise 60, H est en fait égal à U_5. Le résultat est donc prouvé dans le cas de U_5.
• Le cas $n > 5$
- On considère $H \lhd U_n$, $H \neq \{1\}$; on considère σ dans H, $\sigma \neq 1$.
- Par hypothèse on a un certain a tel que $b = \sigma(a) \neq a$.
- on peut choisir c différent à la fois de a, de b et de $\sigma(b)$.
- on considère τ le 3-cycle (acb). $\tau^{-1} = abc$.
- On note ρ la permutation $(\tau.\sigma.\tau^{-1}).\sigma^{-1} = (acb)(\sigma.a, \sigma.b, \sigma.c)$.
- L'ensemble $\{a, b, c, \sigma.a, \sigma.b, \sigma.c\}$ ayant au plus 5 élément (car $\sigma.a = b$), on le complète par des éléments quelconques pour avoir un ensemble F de 5 éléments contenant $\{a, b, c, \sigma.a, \sigma.b, \sigma.c\}$.
- ρ est l'identité en dehors de F, et $\rho(F) = F$.
- On constate que ρ est différent de l'identité car $\rho(b) \neq b$.
- U_F, ensemble des permutations paires de F est isomorphe à U_5 ; on a un morphisme injectif ϕ de U_F dans U_n en considérant pour une permutation t de U_F la permutation dont la restriction à F est t et la restriction à F^c est l'identité.
- On considère H' l'intersection de H et de U_F.
- H' est distingué dans U_F, clairement.
- il est clair que ρ_F appartient à U_F, et que ρ_F n'est pas l'élément neutre.
- Par simplicité de U_F, on sait alors que H' est égal à U_F.
- On considère alors un 3-cycle c de F, il est dans H', donc $\phi(c)$ est dans H.
- H contient donc un 3-cycle, or puisqu'il est distingué il contient aussi sa classe de conjugaison, donc il contient tous les 3-cycles (les 3-cycles étant tous conjugués). Donc il contient le groupe engendré par les 3-cycles, c'est-à-dire U_n.

Ceci termine la preuve.□

Corollaire 89 *$D(U_n) = U_n$ pour $n \geq 5$ et $D(\sigma_n) = U_n$ pour $n \geq 2$.*

Démonstration : • Première preuve (en utilisant le théorème) :
$D(U_n)$ est distingué, donc il ne saurait être plus petit que U_n, puisque U_n est simple, donc $D(U_n) = U_n$.
$D(\sigma_n)$ est le sous-groupe engendré par les commutateurs de σ_n, or il est clair que ces commutateurs appartiennent à U_n (considérer leurs signatures). Donc $D(\sigma_n)$ est inclus dans U_n, or puisqu'il est distingué, il ne saurait être inclus strictement.
• Deuxième preuve (élémentaire) :
- on montre facilement que tout commutateur de σ_n est dans U_n.
- on en déduit que $D(U_n) \subset D(\sigma_n) \subset U_n$
- on montre alors que tout 3-cycle de U_n s'écrit comme commutateur d'éléments de U_n ; en effet avec f un tel 3-cycle, f et f^2 sont conjugués dans U_n (vrai pour toute paire de 3-cycles), donc $f^2 = t.f.t^{-1}$, et donc $f = t.f.t^{-1}.f^{-1}$.□

Corollaire 90 *Les sous-groupes distingués de σ_n sont $\{1\}, U_n, \sigma_n$.*

Démonstration : Supposons H sous-groupe distingué de σ_n.
• $H \cap U_n$ est égal à 1 ou U_n.
• Si $H \cap U_n = U_n$, alors si $H \neq U_n$, alors H contient un produit impair de transpositions ; en multipliant par l'inverse du produit des transpositions sauf une on constate que H contient une transposition. Etant données deux transpositions, on constate qu'elles sont conjuguées par les éléments de U_n ; donc H contient en fait tout σ_n.
• Si $H \cap U_n = \{1\}$, alors ϵ est un isomorphisme de H sur $\epsilon(H)$. Donc H contient en fait un seul autre élément au plus. S'il en contient deux alors soit τ l'autre élément ; il doit commuter avec n'importe quel élément puisque H est distingué et puisque τ n'est pas conjugué à l'unité ; or le centre de σ_n est trivial.□

Corollaire 91 *Sois G un sous-groupe de σ_n d'indice n. Alors G est isomorphe à σ_{n-1}.*

Démonstration : On rappelle que l'indice d'un sous-groupe, on appelle indice le cardinal du groupe quotient. Un sous-groupe d'indice n de σ_n est donc en fait un sous-groupe de cardinal $(n-1)!$.
Le cas $n \leq 4$ s'obtient facilement. Pour $n \geq 5$, on constate que σ_n ou G opère à gauche sur l'ensemble quotient (par translation à gauche, voir 1.9.2). On a donc un homomorphisme ϕ de σ_n dans l'ensemble des permutations de σ_n/H, qui est isomorphe à σ_n.Il reste maintenant à voir que cet homomorphisme est injectif (le caractère surjectif se déduisant alors des cardinaux). Son noyau est l'intersection des $a.G.a^{-1}$ pour a dans σ_n, et donc il est de cardinal au plus le cardinal de G, donc $(n-1)!$; or il est distingué, et on a montré que les seuls sous-groupes distingués de σ_n étaient $\{1\}$, U_n et σ_n ; donc il s'agit de 1, d'où le résultat. □

Admettons enfin sans preuve la proposition ci-dessous :

Proposition 92 *Si $n \neq 4$ et $n \neq 6$ tous les G vérifiant ces hypothèses sont conjugués. En fait, avec les mêmes hypothèses que ci-dessus, il existe i tel que G soit l'ensemble des permutations laissant i invariant.*

⊡ **Décomposition de** σ_n

On a une suite exacte

$$1 \to U_n \to \sigma_n \xrightarrow{\epsilon} \{-1, 1\} \to 1$$

avec ϵ la signature. Avec τ une transposition (c'est à dire une permutation de deux éléments) alors $\{Id, \tau\}$ est un groupe qui est une section pour ϵ, donc on a

$$\sigma_n \simeq U_n \rtimes \{\tau, Id\} \simeq U_n \rtimes \{-1, 1\} \simeq U_n \rtimes \mathbb{Z}/2\mathbb{Z}$$

En outre, σ_n est isomorphe à l'ensemble des automorphismes intérieurs lorsque $n \geq 3$; en effet le centre est alors trivial. On verra plus bas que l'ensemble des automorphismes intérieurs est lui-même égal à l'ensemble des automorphismes lorsque $n \neq 6$.

⊡ **Automorphismes de** σ_n

◇ **Les automorphismes intérieurs sont des automorphismes**

Les automorphismes intérieurs sont les automorphismes de la forme $t \to u.\tau.u^{-1}$, avec u une permutation quelconque. Les automorphismes intérieurs forment un sous-groupe du groupe des automorphismes, de manière évidente.

◇ **Les automorphismes sont des automorphismes intérieurs lorsque** $n \neq 6$

Proposition 93 *Un automorphisme de σ_n transformant toute transposition en transposition est un automorphisme intérieur.*

Démonstration : On considère les transpositions $t_i = (1, i)$ pour $i > 1$. Ces transpositions engendrent toutes les transpositions. Il suffit donc de montrer que ϕ, qui transforme toutes ces transpositions en transpositions, coïncident avec un automorphisme intérieur.
Pour cela on constate que :
• les $\phi(t_i)$ ne sont pas disjointes deux à deux.
• $\phi(t_i)$ et $\phi(t_j)$ ont même élément commun que $\phi(t_i)$ et $\phi(t_k)$.
• on peut donc noter $\phi(t_i)$ sous la forme (z_1, z_i).
• z est la permutation recherchée, tel que l'automorphisme intérieur correspondant corresponde à ϕ.□

Proposition 94 *On suppose $n = 1.k_1 + 2.k_2 + ... + n.k_n$ et que σ est une permutation produit de $\sum_i k_i$ cycles disjoints, k_1 d'ordre 1, k_2 d'ordre 2, k_3 d'ordre 3, ... ,k_n d'ordre k_n. Alors le cardinal du centralisateur de σ est égal à*

$$|c(s)| = \Pi_{i=1}^{n} k_i!.i^{k_i}$$

Démonstration : • Tout d'abord on montre le résultat pour un seul cycle, d'ordre n.
Le centralisateur est alors tout simplement de cardinal n ; il s'agit du sous-groupe engendré par ce cycle. Pour le voir on se ramène à un cycle $(1, 2, ..., n)$; pour que τ commute avec ce cycle, il faut que $\tau(n+1) = \tau(n)+1$, c'est-à-dire que $\tau(n+1)-\tau(n) = 1$, donc que $\tau(n) = \tau(0) + n$ (on compte modulo n) ; on a donc un élément dans le centralisateur pour tout élément de $[1, n]$.
• On le généralise ensuite à k cycles de même ordre i.
Alors en se restreignant aux permutations laissant invariants chacun des supports, on a i possibilités, on obtient donc i^k. Mais il reste la possibilité d'intervertir les supports, il faut donc multiplier par $k!$. Il est clair que toutes les permutations ainsi construites sont bien dans le centralisateur ; pour la réciproque, il suffit de supposer que a et $a + 1$ appartenant au support du même cycle (supposés de la forme $(j, j + 1, .., j + i - 1)$, et qu'ils ne sont pas envoyés dans un même support ; on constate alors que notre permutation ne saurait commuter avec notre produit de cycles.
• On le généralise enfin au cas le plus général.
Facile ! Il suffit de faire comme ci-dessus et de constater que quand deux supports ont pas la même taille il est impossible de mettre tous les éléments de l'un dans l'autre...□

Théorème 95 *Si $n \neq 6$ alors tout automorphisme de σ_n est un automorphisme intérieur.*

Démonstration : L'image d'une transposition par un automorphisme ϕ est d'ordre 2, et donc est un produit de k cycles disjoints. Par la proposition 94 le cardinal de son centralisateur est alors $2^k.k!.(n - 2.k)!$; ce cardinal est aussi le cardinal du centralisateur de notre transposition initiale, donc $2.(n - 2)!$. Si $n = 6$, on a une solution avec $n = 6$ et $k = 3$, si $n \neq 6$, on a une seule solution pour $k = 1$. Donc l'image d'une transposition par ϕ est une transposition ; donc par la proposition 93 ϕ est un automorphisme intérieur.□

1.10.12 Groupes en géométrie

⊡ **Groupe diédral** D_n

Définition 96 (Groupe diédral) *On appelle* **groupe diédral d'ordre** n *et on note* D_n *le groupe des isométries du plan conservant un polygone régulier à* n *côtés. Il contient* $2.n$ *éléments, comme on pourra s'en convaincre en distinguant le cas* n *pair et le cas* n *impair ;* n *rotations et* n *symétries.*
On note R_n *l'ensemble des* n *rotations de* D_n*.*

Proposition 97 *On a* $R_n \lhd\!\lhd D_n$*, et donc*

$$1 \to R_n \to \mathbb{D}_n \xrightarrow{p} \mathbb{Z}/2\mathbb{Z} \to 1$$

en effet D_n *étant d'ordre* $2.n$*, le quotient de* D_n *par* R_n *est d'ordre* 2*, et ne peut donc être qu'isomorphe à* $\mathbb{Z}/2.\mathbb{Z}$*.*
Etant donnée $r \in D_n \setminus R_n$*,* $\{r, Id\}$ *fournit une section ; donc on a* $D_n = R_n \rtimes \{r, Id\}$*, donc* $D_n \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$*.*

On pourra consulter la partie **??** pour plus d'informations sur le groupe diédral.

1.11 Application des groupes à la géométrie

Ci-dessous une liste non exaustive d'applications des groupes en géométrie :
- **cercle unité complexe** $(\mathbb{U}, \times)$, groupe des nombres complexes de module 1, permettant de définir les angles. Isomorphe à $O_2^+(\mathbb{R})$.
- **groupe linéaire** $GL(E)$ des applications linéaire d'un espace vectoriel dans lui-même. Voir 1.10.2.
- **groupe affine** $GA(\xi)$ des bijections affines d'un espace euclidien ξ dans lui-même. Le centre de $GA(\xi)$ est réduit à l'identité. On remarquera notamment que si le groupe additif d'un espace vectoriel agit librement et transitivement sur un ensemble ξ, celui-ci est muni par cette opération d'une structure d'espace affine. Voir 1.10.5.
- **groupe des isométries** d'un ensemble (voir partie**??**)
- **groupe des similitudes** d'un espace euclidien (voir partie 1.10.9)
- **groupe orthogonal** d'un espace euclidien, $O(E)$, voir 1.10.3.
- **groupe projectif** d'un espace vectoriel de dimension finie. Voir 1.10.6.

Chapitre 2

Anneaux

2.1 Définitions

Définition 98 (Anneau) *Un* **anneau** *est un triplet* $(A, +, \times)$ *tel que*
• A *est un ensemble non vide*
• $+$ *est une loi de composition interne (c'est à dire une application de* $A \times A$ *dans* A*), telle que* $(A, +)$ *est un groupe commutatif.*
• $\times$ *est une loi de composition interne associative, ayant un élément neutre, distributive par rapport à* $+$

On appelle **unité** *de* $(A, +, \times)$ *tout élément inversible pour* $\times$.
Si en outre $\times$ *est commutative, l'anneau est dit* **commutatif**.
On note 0 *l'élément neutre pour l'addition,* 1 *l'élément neutre pour la multiplication, le symétrique de* $a \in A$ *pour* $+$ *est noté* $-a$*, et le symétrique, lorsque* a *est une unité, de* a *pour* $\times$ *est noté* a^{-1}.

$a \times b$ *sera souvent abrégé* $a.b$ *ou même* ab.
a *et* b *appartenant à* A *sont dits* **associés** *si* $a = b.x$ *pour un certain* x *unité. La relation d'association est une relation d'équivalence.*
On dit que a **divise** b*, ou que* a *est un* **diviseur** *de* b*, ou que* b *est un* **multiple** *de* a*, pour* a *et* b *dans* A*, s'il existe* x *tel que* $b = a.x$.
On dit que a *est un* **plus grand commun diviseur** *ou* **pgcd** *des éléments* $a_1, ..., a_n$*, si pour tout* i*,* $d|a_i$ *et si pour tout* d' $\forall i$ $d'|a_i$ *implique* $d'|d$*. On dit que* a *est un* **plus petit commun multiple** *ou* **ppcm** *des éléments* $a_1, ..., a_n$*, si pour tout* i*,* $a_i|d$ *et si pour tout* d'*,* $\forall i$ $a_i|d'$ *implique* $d|d'$*.* $a \in A$ *est dit* **irréductible** *si* a *n'est pas une unité et si* $b|a$ *implique que* b *est une unité ou que* b *est associé à* a.

Les notions de ppcm et pgcd seront surtout utilisées dans le cadre d'anneaux principaux (voir partie 2.2), bien que leur définition puisse être utilisée dans un

cadre plus général.

Proposition 99 • *$a \in A$ est irréductible si et seulement si a n'est pas une unité et si $b.c = a$ implique b ou c est une unité.*
• *Dans $\mathbb{Z}$ les éléments irréductibles sont les nombres premiers.*

J'ai ici imposé l'existence d'un élément neutre pour la multiplication ; selon les terminologies ce n'est pas toujours le cas. Si l'on ne suppose pas l'existence d'un élément neutre pour la définition d'un anneau, alors un anneau vérifiant en outre cette propriété sera appelé anneau **unitaire**. Dans la vie de tous les jours, les anneaux sont toujours unitaires. L'hypothèse de commutativité est très classique, mais ici cette hypothèse sera précisée quand elle est nécessaire.

Exemples : :
• $(\mathbb{Z}, +, \times)$ est un anneau.
• $(\mathcal{P}(E), \Delta, \cap)$ est un anneau commutatif, avec Δ la différence symétrique, c'est à dire $A\Delta B = A \cup B - A \cap B$.

Propriétés :(notez que na, pour $n \in \mathbb{N}$ et $a \in A$, désigne $a + a + a + \cdots + a$ (a n fois), et a^n désigne $a \times a \times a \times \cdots \times a$ (a n fois).
• $1 \neq 0$, à moins que le cardinal de A soit 1.
• $a.0 = 0.a = 0$ pour tout $a \in A$.
• $-(a.b) = (-a).b = a.(-b)$ pour tous $(a, b) \in A^2$
• $(na).b = n.(ab) = a.(nb)$ pour tous $(a, b) \in A^2$ et $n \in \mathbb{N}$.
• L'ensemble des unités forme un groupe pour $\times$.

Proposition 100 (Formule du binôme de Newton) *Soit a et b dans un anneau A. Si a et b commutent, alors*

$$(a+b)^n = \sum_{k \in [0,n]} C_n^k a^k b^{n-k}$$

Démonstration : Par une récurrence sans difficulté, en se rappelant que $C_n^p = C_{n-1}^p + C_{n-1}^{p-1}$□

Exemple Maple
$>\ (x+y)\hat{}\,3$
$$(x+y)^3$$
$>\ expand(\%);$
$$x^3 + 3x^2y + 3xy^2 + y^3$$

Définition 101 (Diviseurs de 0, anneaux intègres, éléments nilpotents) *1.*
Un élément a est dit **diviseur à gauche de** 0 *s'il existe $b \neq 0$ tel que $b.a = 0$.*
Un élément a est dit **diviseur à droite de** 0 *s'il existe $b \neq 0$ tel que $a.b = 0$.*
Un élément est dit **diviseur de** 0 *s'il est à la fois diviseur à gauche de 0 et diviseur à droite de 0.*
Un anneau est dit **sans diviseur de** 0 *s'il n'admet pas de diviseur à gauche de 0 ou de diviseur à droite de 0 autre que 0 lui-même.*

2. *Un anneau est dit* **intègre** *si :*
   • *il est de cardinal > 1*
   • *il est commutatif*
   • *il est sans diviseur de 0*

3. *Un élément a est dit* **nilpotent** *s'il existe $n \in \mathbb{N}$ tel que $a^n = 0$. On appelle alors* **indice de nilpotence de** *a le plus petit n convenable non nul.*

Remarques :
• $(\mathbb{Z}, +, \times)$ est un anneau intègre.
• Tout anneau comporte un diviseur de 0 à gauche, un diviseur de 0 à droite, et un diviseur de 0 tout court ; il s'agit de 0 lui-même. Un anneau sans diviseur de 0 ne signifie donc pas que l'anneau ne comporte pas de diviseur de 0.
• Un anneau est sans diviseur de 0 s'il n'admet pas de diviseur à gauche de 0 autre que 0. En effet, si A n'admettant pas de diviseur à gauche de 0 admet un diviseur à droite de 0 autre que 0, alors $0 = ab$ pour a et b non nul, ce qui contredit le fait que 0 n'ait pas de diviseur à gauche.
• De même, un anneau est sans diviseur de 0 s'il n'admet pas de diviseur à droite de 0 autre que 0.
• Un anneau est sans diviseur de 0 si $ab = 0 \Rightarrow a = 0$ ou $b = 0$.

Définition 102 (Morphisme d'anneaux) *Une application f d'un anneau $(A, +, \times)$ vers un anneau $(B, +, \times)$ est un* **morphisme d'anneaux** *(ou* **homomorphisme***) si :*
• *f est un morphisme du groupe $(A, +)$ vers le groupe $(B, +)$*
• *$f(x.y) = f(x).f(y)$ pour tout $(x, y) \in A^2$*
• *$f(1_A) = 1_B$*
On appelle alors **noyau** *de f l'ensemble $ker\ f$ des $x \in A$ tels que $f(x) = 0$.*

Remarques :
• Le noyau d'un morphisme d'anneaux est le noyau du morphisme de groupes sous-jacent.

• 0 appartient au noyau de tout morphisme d'anneaux.
• L'image de l'inverse est l'inverse de l'image, pour chacune des deux lois.

Définition 103 (Produit d'anneaux) *On appelle* **produit de deux anneaux** *leur produit cartésien muni de l'addition terme à terme et de la multiplication terme à terme.*

On vérifie facilement qu'un produit d'anneaux est un anneau.

Définition 104 (Sous-anneau) *Etant donné $(A, +, \times)$ un anneau, une partie B de A est un* **sous-anneau** *de A si*
• $1 \in B$
• $(B, +)$ *est un sous-groupe de* $(A, +)$
• B *est stable par multiplication*

Propriétés :
• Un sous-anneau est un anneau, mais un anneau inclus dans un anneau n'en est pas nécessairement un sous-anneau ; en effet il faut considérer la condition $1 \in B$.
Par exemple l'ensemble des matrices de la forme

$$\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}$$

est un anneau inclus dans l'anneau des matrices 2×2, mais n'en est pas un sous-anneau.
• L'image réciproque d'un sous-anneau par un morphisme d'anneaux est un sous-anneau.
• L'image d'un sous-anneau par un morphisme d'anneaux est un sous-anneau.

Théorème 105 *Pour tout anneau $(A, +, \times)$, il existe un unique morphisme d'anneaux de $(\mathbb{Z}, +, \times)$ dans $(A, +, \times)$. Il est défini par $\phi(n) = 1_A + ... + 1_A$ n fois et $\phi(-n) = -1_A - 1_A \cdots - 1_A$ n fois pour $n > 0$.*

Démonstration : On vérifie aisément que ϕ ainsi définit est bien un morphisme d'anneau. $\phi(1)$ est nécessairement égal à 1 et $\phi(0)$ à 0. Par récurrence, les propriétés des anneaux permettent de vérifier que les autres éléments sont aussi définis de manière unique.□

Remarque : ceci montre que tout anneau contient un sous-anneau minimal qui est $\phi(\mathbb{Z})$.

2.2 Idéaux, anneaux quotients

Définition 106 (Idéal à gauche, idéal à droite) *On se donne $(A, +, \times)$ un anneau et I une partie non vide de A.*
I est un **idéal à gauche (resp. à droite)** *de $(A, +, \times)$ si*
• *I est stable pour l'addition*
• *$A.I$ est inclus dans I (resp. $I.A$ est inclus dans I)*

I est un **idéal** *(parfois on dit* **idéal bilatère***) si I est à la fois un idéal à gauche et un idéal à droite. A et $\{0\}$ sont toujours des idéaux de A ; on les appelle* **idéaux triviaux** *de A. Les autres idéaux sont appelés idéaux non triviaux (on dit parfois aussi* **idéaux propres***) de A.*

Exemples : Dans $\mathcal{M}_n(\mathbb{R})$, l'ensemble des matrices à première colonne nulle est un idéal à gauche, l'ensemble des matrices à première ligne nulle est un idéal à droite.

Propriétés :
• Un idéal contenant 1 ou toute autre unité de l'anneau est l'anneau tout entier.
• La réunion d'une suite croissante d'idéaux est un idéal.
• I idéal de A et J idéal de B ; alors $I \times J$ est un idéal de $A \times B$.
• L'intersection d'une famille d'idéaux est un idéal.

Proposition 107 • *Le noyau d'un morphisme est un idéal.*
• *L'image réciproque d'un idéal par un morphisme est un idéal.*
• *L'image d'un idéal par un morphisme est un idéal de l'image de l'anneau (et pas nécessairement de l'anneau dans lequel l'image est incluse...).*

Définition 108 *Une intersection d'idéaux étant un idéal, on peut définir l'***idéal engendré par une partie** *de A comme l'intersection de tous les idéaux contenant cette partie. C'est donc aussi le plus petit idéal contenant cette partie. On note (E) l'idéal engendré par E.*

Définition 109 *On appelle* **idéal principal** *un idéal I d'un anneau commutatif engendré un singleton $\{x\}$. On note abusivement (x) pour $(\{x\})$.*
On appelle **anneau principal** *un anneau intègre tel que tout idéal est principal.*
Un idéal I d'un anneau commutatif est dit **idéal maximal** *s'il est différent de l'anneau tout entier et si tout idéal incluant I est égal à I ou à l'anneau lui-même.*
On appelle **somme** *d'une famille d'idéaux $(I_k)_{k\in K}$ l'ensemble des $\sum_{i\in J} x_i$ avec J fini inclus dans K et $x_i \in I_i$.*
Un idéal est dit **de type fini** *s'il est somme d'un nombre fini d'idéaux principaux.*

Remarques :

• Un anneau principal est donc commutatif, non réduit à $\{0\}$, sans diviseur de 0 ; et tout idéal de cet anneau est principal.
• On notera bien qu'un idéal maximal n'est pas un idéal qui est maximal... Il est en fait maximal parmi les idéaux propres.
• Dans un anneau commutatif A, $(x) = \{x.a/a \in A\}$.
• Une somme d'idéaux est un idéal.
• La somme des idéaux I_k avec $I_k = (x_k)$ est l'idéal engendré par la famille des x_k.

Nb : Un idéal de type fini est donc un idéal engendré par un nombre fini d'éléments.

Proposition 110 *Si a et b sont associés alors $(a) = (b)$.*
Dans un anneau intègre il y a réciproque.

Démonstration : Facile au vu de la dernière remarque.□

⚠ Il n'y a pas de réciproque dans le cas général !

Théorème 111 (Théorème de Bezout) *A est supposé principal.*
• *un générateur de $I = (a_1) + (a_2) + ... + (a_n)$ est un pgcd des a_i.*
• *d, diviseur commun des a_i, est pgcd des a_i si et seulement s'il existe une famille $(\lambda_i)_{i\in[1,n]}$ tels que $d = \sum \lambda_i a_i$ (**relation de Bezout**).*
• *un générateur de $I = (a_1) \cap (a_2) \cap ... \cap (a_n)$ est un ppcm des a_i.*

Démonstration :
Le premier • est simple : un tel générateur d doit nécessairement diviser tous les a_i, et il doit nécessairement être dans l'idéal I, et donc tout élément qui divise tous les a_i, étant lui même un générateur de I, doit diviser d.

Le second • est une simple traduction du fait que d soit bien dans I et soit un générateur de I.

Pour le troisième • , donnons-nous p un tel générateur ; il appartient à I, et donc est un multiple de chaque a_i ; et si p' est un autre multiple des a_i, alors il est dans tous les (a_i), et donc appartient à I, et donc est un multiple de p.□

Dans $A = \mathbb{Z}$ ou $A = \mathbb{K}[X]$ avec $\mathbb{K}$ un corps, il est utile de disposer d'un algorithme pratique permettant de découvrir une relation de Bezout entre a et b si une telle relation existe. Pour cela, il suffit de constater que a et b ont même pgcd que a et $a - qb$, pour tout q dans A, par exemple avec q le quotient dans la division euclidienne de a par b. Si a est divisible par b, le pgcd de a et b est simplement b ; sinon, on effectue une division euclidienne. Considérons un exemple pratique, cherchons le pgcd de 42 et 30.

$$30 \not| 42$$

$$42 = 1 \times 30 + 12$$

$$12 \not| 30$$

$$30 = 2 \times 12 + 6$$

$$12|6 \text{ et } 12 = 2 \times 6$$

Donc

$$6 = 30 - 2 \times 12 = 30 - 2 \times (42 - 30) = 3 \times 30 - 2 \times 42$$

ce qui est bien la relation de Bezout attendue. Cet algorithme est appelé **algorithme d'Euclide**.

Définition 112 *Un idéal I est dit* **premier** *si et seulement si A/I est intègre. Un élément d'un anneau est dit* **premier** *si et seulement l'idéal engendré par cet élément est premier.*

Proposition 113 • *Un idéal I de A est premier si et seulement s'il est différent de A et si $a.b \in I$ implique $a \in I$ ou $b \in I$.*
• *L'image réciproque d'un idéal premier par un homomorphisme d'anneaux est un idéal premier.*

La première de ces deux propriétés est fondamentale car c'est généralement celle que l'on utilise pour montrer qu'un idéal est premier.

Proposition 114 *Un anneau commutatif est intègre si et seulement si (0) est un idéal premier.*

Démonstration :

(0) idéal premier
si et seulement si
$a.b \in (0) \rightarrow a \in (0)$ ou $b \in (0)$
si et seulement si
$a.b = 0 \rightarrow a = 0$ ou $b = 0$
si et seulement si
A intègre□

Lemme 115 *Soit A un anneau. A est un corps si et seulement si A est non réduit à $\{0\}$ et ses seuls idéaux sont $\{0\}$ et A.*

Démonstration : • Supposons que les seuls idéaux de A soient $\{0\}$ et A.
Soit x dans A, $x \neq 0$, $x.A$ est un idéal, autre que $\{0\}$, donc il contient tout A, donc en particulier il contient 1, donc il est inversible.
• Réciproquement si A est un corps, alors soit x non nul appartenant à un idéal I, alors I contient $x.A$, donc $x.x^{-1}.A$, donc A.□

Proposition 116 *Dans un anneau principal, les idéaux premiers sont (0) et (p), avec p irréductible.*

Démonstration : • Soit I un idéal premier et $p \neq 0$ un élément de A tel que $I = (p)$. Supposons que $p = a.b$. Alors $a.b \in (p)$, et donc puisque I est premier,

$a \in (p)$ ou $b \in (p)$; on suppose $a \in (p)$. Alors $a = p.a'$. On a alors $p.a'.b = p$, donc $p(1 - a'b) = 0$, or A est intègre, donc $a'.b = 1$, donc b est une unité.□

Proposition 117 *Dans un anneau principal, pour tout p irréductible, (p) est un idéal maximal.*

Démonstration : Soit $I = (p)$, avec p irréductible. Supposons $I \subset J$, avec J inclus dans A. Alors $J = (q)$, et $p = q.a$. Mais p étant irréductible, soit $q = p.x$ avec x unité, soit q est une unité. Dans le premier cas, $J = I$, et dans le deuxième cas, $J = A$. □

On va maintenant étudier la notion d'anneau quotient.
Cette notion n'est étudiée que dans le cas d'anneaux commutatifs.

Définition 118 *Etant donné I un idéal de A, on définit une relation d'équivalence $\mathcal{R}_I$ par*

$$a\mathcal{R}b \iff a - b \in I$$

Alors l'ensemble quotient pour cette relation, muni des opérations induites par les opérations sur I, est un anneau ; on l'appelle **anneau quotient** *de A par l'idéal I, et on le note A/I.*

Il convient de vérifier que la relation est bien compatible avec les opérations définies sur l'anneau (vérification aisée).

2.3 Décomposition d'un homomorphisme d'anneaux et utilisation des idéaux

Définition 119 (Factorisation d'un homomorphisme) *On dit que f homomorphisme d'un anneau A vers un anneau B se factorise par A/I avec I idéal de A si et seulement s'il existe g homomorphisme de A/I dans B tel que $f(x) = g(\overline{x})$.*

Théorème 120 *Soit f un homomorphisme d'anneaux de A vers B. Alors pour tout I idéal inclus dans $Ker\ f$, on définit $x \to \overline{x}$ la projection canonique de A sur A/I, et on a les propriétés suivantes :*
- *Il existe un unique homomorphisme g de $A/I dans B$ tel que $\forall x\ f(x) = g(\overline{x})$*
- *$Im\ f \simeq A/Ker\ f$*
- *g est injectif si et seulement si $I = Ker\ f$*
- *g est surjectif si et seulement si f est surjectif*

Proposition 121 (Image et image réciproque d'un idéal par un homomorphisme)
• *L'image réciproque d'un idéal par un homomorphisme est un idéal*
• *Si f est un homomorphisme surjectif, alors l'image d'un idéal par f est un idéal.*

Proposition 122 *Soit I idéal de A. Alors l'application ϕ qui à un idéal J avec $I \subset J \subset A$ associe la projection $\overline{J}$ de J sur A/I est une bijection de l'ensemble des idéaux de A contenant I vers l'ensemble des idéaux de A/I.*

Démonstration : • $x \mapsto \overline{x}$ étant surjectif, il est clair que ϕ associe bien un idéal à un idéal.
• Pour montrer que ϕ est bijective, on considère l'application ψ qui à un idéal K de A/I associe $\{a/\overline{a} \in K\}$. □

Proposition 123 *Un idéal I d'un anneau A est maximal si et seulement si A/I est un corps.*

Démonstration : On utilise le lemme 115 et la propriété ci-dessus.□

Corollaire 124 *Tout idéal maximal est premier.*

Démonstration : Supposons que I, idéal maximal, contient $a.b$, avec $a \notin I$ et $b \notin I$.
Alors la classe de a et la classe de b dans A/I sont non nulles, et leur produit est nul, d'où contradiction.□

Théorème 125 (Krull) *Pour tout idéal I de A, I différent de A, il existe un idéal maximal de A contenant I.*

Démonstration : Cette preuve nécéssite l'axiome du choix, via le théorème de Zorn (voir le lemme **??**).
• On considère l'ensemble des idéaux différents de A contenant I idéal de A, ordonné par l'inclusion.
• Cet ensemble est inductif. En effet étant donnée une chaîne, on considère la réunion, c'est un idéal différent de A (en effet il ne contient pas 1 par exemple).
• On peut donc considérer un élément maximal pour l'inclusion, et conclure que cet idéal est maximal.□

2.4 Anneaux commutatifs

Dans la vie de tous les jours, comme je l'écrivais un peu plus haut, les anneaux sont généralement supposés commutatifs. On va maintenant étudier des cas particuliers d'anneaux commutatifs, avec des cas de plus en plus riches. Tout d'abord les anneaux euclidiens, puis les anneaux noethériens, puis les anneaux intègres, puis les anneaux factoriels, puis les anneaux principaux. On a les implications (principal $\Rightarrow$ factoriel) et (factoriel $\Rightarrow$ intègre).

2.4.1 Anneaux euclidiens

Cette notion n'est étudiée que dans le cas d'anneaux commutatifs.

Définition 126 *Un anneau A commutatif est dit* **euclidien** *pour une application f de $A \setminus \{0\}$ dans $\mathbb{N}$, si pour tout a dans A et tout b dans $A \setminus \{0\}$ il existe $(q, r) \in A^2$ tels que $a = b.q + r$ et $r = 0$ ou $f(r) < f(b)$.*
Un anneau A commutatif est dit **euclidien** *s'il existe une application pour laquelle il est euclidien.*

Proposition 127 • *$\mathbb{Z}$ est euclidien.*
• *$\mathbb{K}[X]$ est euclidien.*

Démonstration : Considérer respectivement :
• $f(z) = |z|$
• $f(P) = deg(P)$ (voir la démonstration de la division euclidienneen 5.2)□

Proposition 128 *Etant donnée f une application multiplicative (i.e. $f(a.b) = f(a).f(b)$) de $A\setminus\{0\}$ dans $\mathbb{N}\setminus\{0\}$, avec A anneau intègre, on prolonge f multiplicativement sur le corps des fractions de A en posant $f(a/b) = f(a)/f(b)$ (f est maintenant à valeurs dans $\mathbb{Q}$). Alors A est euclidien pour f si et seulement si pour tout x dans le corps des fractions il existe a dans A tel que $f(x-a) < 1$.*

Démonstration : Facile...□

Proposition 129 *Tout anneau euclidien est principal.*

Démonstration : Soit A un tel anneau (commutatif, euclidien). On se donne P_0 dans $I \setminus \{0\}$ tel que $f(P_0)$ soit minimal. On note I' l'idéal engendré par P_0, c'est à dire l'ensemble des $P_0.P$ pour $P \in \mathbb{K}[X]$.
Pour tout P dans I, on utilise la définition $P = P_0.Q + R$; alors $P \in I$, $P_0 \in I$, donc $P_0.Q \in I$ (par définition d'un idéal), et donc $R \in I$; or $f(R) < f(P_0)$ si R est non nul, ce qui contredit la définition de P_0, donc R est nul, donc $P \in I'$, donc $I = I'$ et

donc l'anneau est principal.□

Proposition 130 *$\mathbb{Z}[i]$ et $\mathbb{Z}[\sqrt{2}]$ sont euclidiens.*

Démonstration : Dans les deux cas on utilise la caractérisation de la proposition 128.
Dans le premier cas on choisit $f(a+i.b) = |a+i.b|$ pour a et b dans $\mathbb{Q}$.
Dans le second cas on utilise $f(a+b.\sqrt{2}) = |a^2-2.b^2|$ si a et b dans $\mathbb{Z}$.
Ce second choix est particulièrement instructif ; $f(a+b.\sqrt{d}) = |a^2-d.b^2|$ sera souvent utile.□

2.4.2 Anneaux noethériens

Définition 131 (Anneau noethérien) *Un anneau commutatif dont tout idéal est de type fini est dit* **noethérien***.*

Proposition 132 *Un anneau commutatif est noethérien si et seulement si toute suite croissante d'idéaux est stationnaire à partir d'un certain rang.*

Démonstration : Trop facile pour que nous le prouvions ! Exercice pour le lecteur.□

Proposition 133 *Un anneau commutatif A est noethérien si et seulement si tout ensemble non vide d'idéaux de A admet un élément maximal pour l'inclusion.*

Démonstration : Rappelons juste qu'un élément maximal n'est pas nécessairement le plus grand élément, l'existence d'un élément maximal n'entraîne pas même celle d'un plus grand élément (voir les définitions en partie**??**).□

Proposition 134 • *Tout anneau quotient d'un anneau noethérien est noethérien.*
• *Un anneau principal est noethérien.*

Démonstration : • La proposition 122 montre qu'un idéal du quotient est la projection d'un idéal, ce dernier étant de type fini, le projeté est de type fini.
• Facile, tout idéal d'un anneau principal est engendré par un seul élément, donc par un nombre fini d'éléments.□
⚠ La propriété annoncée pour les anneaux quotients n'est pas vraie pour les sous-anneaux.

Théorème 135 (Théorème de Hilbert) *Si A est un anneau noethérien, alors pour tout n $A[X_1, ..., X_n]$ est aussi un anneau noethérien.*

Démonstration : Admis (preuve difficile).□


:

• Tout corps est un anneau noethérien, donc tout $K[x_1, \ldots, x_n]$ aussi.
• $\mathbb{Z}[x_1, \ldots, x_n]$ est noethérien.

2.4.3 Anneaux intègres

On a déjà vu les définitions, mais voici un rappel : Un anneau est dit intègre si :
• il est de cardinal > 1
• il est commutatif
• il est sans diviseur de 0

Définition 136 (Définitions dans les anneaux intègres) *a et b dans A anneau intègre sont dits* **premiers entre eux** *si*

$$\forall x \in a \; x|a \text{ et } x|b \rightarrow x \text{ est une unité}$$

De même les éléments d'une famille $(a_i)_{i\in[1,n]}$ sont dits premiers entre eux si un élément divisant tous les a_i est nécessairement une unité.

Corollaire 137 (Théorème de Bezout) *Dans un anneau principal des éléments a_i sont premiers entre eux si et seulement s'il existe une famille λ_i d'éléments de A telle que $\sum \lambda_i a_i$ soit une unité.*

Proposition 138 *Soit A un anneau intègre, et ϕ l'application qui à x dans A quotienté par la relation d'association $\mathcal{R}$ associe l'idéal engendré par x. ϕ est un isomorphisme d'ordre entre $A/\mathcal{R}$ muni de la divisibilité et l'ensemble des idéaux principaux de A muni de l'inverse de l'inclusion.*

Démonstration : • Tout d'abord il est clair que ϕ est bien définie, car deux éléments associés engendrent évidemment le même idéal.
• L'application est surjective, par définition, puisqu'on considère l'ensemble des idéaux principaux.
• Montrons que l'application est injective : si deux éléments a et b engendrent le même idéal alors $b = b'.a$ et $a = a'.b$ et donc $b = b'.a'.b$ et donc b' et a' sont des unités (car A est intègre), et donc $\overline{b} = \overline{a}$.
• Montrons qu'il s'agit d'un morphisme d'ordres :
- Si $a|b$ alors $b = a.c$ donc $b.A = a.c.A \subset a.A$ et $(b) \subset (a)$ clairement.

- Si $(b) \subset (a)$ alors $b = a.c$ pour un certain c et donc $a|b$.□

2.4.4 Anneaux factoriels

Cette notion n'est étudiée que dans le cadre d'anneaux commutatifs.

Définition 139 (Anneau factoriel) *Un anneau A est dit* **factoriel** *si :*
• *il est intègre*
• *tout a dans A s'écrit de manière unique à association près et à permutation près $a = a'.p_1.p_2.....p_n$ avec a' unité et p_i irréductible pour tout i.*

Etant donné un élément p irréductible de A un anneau factoriel, on appelle **valuation p-adique de** *A pour a dans A le nombre d'occurences d'un élément associé à p dans la décomposition de a sous forme $a = a'.p_1.....p_n$. On note généralement $v_p(A)$ la valuation p-adique de a.*

Proposition 140 *Etant donné A un anneau factoriel, on peut choisir un élément dans chaque classe d'équivalence de A pour la relation d'association $\mathcal{R}$. L'ensemble de ces éléments permet de simplifier la décomposition de $a \in A$ en $a = a'.\Pi_{i \in A/\mathcal{R}} p_i^{v_{p_i}(a)}$, le support de $i \mapsto v_{p_i}(a)$ étant fini.*

Démonstration : Evident.□

Voyons maintenant quelques propriétés intéressantes des anneaux factoriels.

Proposition 141 *Dans un anneau factoriel un élément est irréductible si et seulement s'il est premier.*

Le lemme et le théorème qui suivent se démontrent très facilement, simplement en considérant les décompositions de x, y et éventuellement z pour conclure.

Lemme 142 (lemme d'Euclide) *Si A est un anneau factoriel, alors si p est irréductible et divise $x.y$, alors p divise x ou p divise y.*

Théorème 143 (Théorème de Gauss) *Si z divise $x.y$ et si z est premier avec x alors z divise y.*

Un exemple d'application (parmi beaucoup d'autres) est le théorème 195.

Proposition 144 *Un anneau intègre noethérien vérifiant le lemme d'Euclide ou le théorème de Gauss est factoriel.*

Démonstration : Admis.□

Dans l'exemple ci-dessous on utilise le fait que $\mathbb{Z}$ est factoriel.

Exemple Maple

$> \ ifactor(200!);$

$$(2)^{197}(3)^{97}(5)^{49}(7)^{32}(11)^{19}(13)^{16}(17)^{11}(19)^{10}(23)^{8}(29)^{6}(31)^{6}(37)^{5}(41)^{4}$$
$$(43)^{4}(47)^{4}(53)^{3}(59)^{3}(61)^{3}(67)^{2}(71)^{2}(73)^{2}(79)^{2}(83)^{2}(89)^{2}(97)^{2}(101)(103)$$
$$(107)(109)(113)(127)(131)(137)(139)(149)(151)(157)(163)(167)(173)(179)$$
$$(181)(191)(193)(197)(199)$$

2.4.5 Anneaux principaux

On rappelle tout d'abord la définition d'un anneau principal : il s'agit d'un anneau intègre dont tout idéal est principal.

Je donne sans démonstration (voir [19, p156]) le résultat important suivant :

Proposition 145 *Tout anneau principal est factoriel.*

On peut préciser aussi que sur le corps des fractions rationnelles à coefficients dans un anneau principal, on dispose de la décomposition en éléments simples.

2.5 Zoologie des anneaux

2.5.1 Nilpotence (d'une somme de deux éléments nilpotents qui commutent)

Proposition 146 *La somme de deux éléments nilpotents qui commutent est nilpotente.*

Démonstration : Considérer deux tels éléments a et b, et développer par le binome de Newton 100 la puissance $(a+b)^n$ avec n la somme de leurs indices de nilpotence respectifs.□

2.5.2 $\mathbb{Z}/n\mathbb{Z}$

⊡ Généralités

Etant donné $m \in \mathbb{N}$ on note $\overline{m}$ la classe de m dans $\mathbb{Z}/n\mathbb{Z}$ (la relation d'équivalence considérée étant la congruence modulo n - x et y sont équivalents si n divise $x-y$).

Proposition 147 *On a équivalence entre les propriétés suivantes :*
• m *est premier avec* n
• $\overline{m}$ *est générateur du groupe* $(\mathbb{Z}/n\mathbb{Z}, +)$
• $\overline{m}$ *est inversible dans l'anneau* $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

Démonstration : Facile, en application du théorème de Bezout.□

Définition 148 (Fonction d'Euler) *On appelle* **fonction d'Euler** *la fonction* ϕ *telle que* $\phi(n)$ *soit le nombre d'entiers* x *tels que* $1 \leq x \leq n$ *et* $x \wedge n = 1$.

Proposition 149 • *Si* n *est premier* $\phi(n) = n - 1$ *et* $\phi(n^r) = n^{r-1}.(n-1)$ *si* $r > 0$
• $\phi(n)$ *est le nombre d'éléments inversibles de* $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

Démonstration : le premier point est clair ; il suffit de voir qu'un élément est premier avec p^n si et seulement s'il n'est pas divisible par p.
Le second point est un corollaire de la proposition précédente.□

⊡ Lemme chinois

Lemme 150 (Lemme Chinois) *Si* p *et* q *sont premiers entre eux alors*

$$(\mathbb{Z}/pq\mathbb{Z}, +) \simeq (\mathbb{Z}/p\mathbb{Z}, +) \times (\mathbb{Z}/q\mathbb{Z}, +)$$

Démonstration : Il s'agit des groupes additifs usuels. L'égalité des cardinaux montre qu'il suffit de trouver un morphisme de groupes injectif. Pour cela on associe à la classe de n dans $\mathbb{Z}/pq\mathbb{Z}$ la classe de n dans $\mathbb{Z}/p\mathbb{Z}$ et la classe de n dans $\mathbb{Z}/q\mathbb{Z}$.
Il est clair que si deux entiers ont la même classe modulo pq alors ils ont la même classe modulo p et modulo q, donc l'application est bien définie.
Le fait que cette application soit un morphisme est clair.
L'application est injective, car si deux entiers ont la même classe modulo p et q, alors ils ont la même classe modulo pq.□

Corollaire 151 *Si $n = \Pi_i p_i^{\alpha_i}$, avec les p_i premiers distincts et les $\alpha_i > 0$, alors*

$$(\mathbb{Z}/n\mathbb{Z}, +, \times) \simeq \Pi_i(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}, +, \times)$$
$$(\mathbb{Z}/n\mathbb{Z})^* \simeq \Pi_i(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^*$$
$$\phi(n) = \Pi_i\phi(p_i^{\alpha_i}) = n.\Pi_i(1 - 1/P_i)$$

Démonstration : Le premier point découle de l'utilisation récurrente du lemme chinois, le deuxième et le troisième sont des conséquences immédiates du premier.□

⊡ **Automorphismes de** $\mathbb{Z}/n\mathbb{Z}$

Proposition 152 *L'ensemble des automorphismes de $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^*$.*

Démonstration : Il suffit de considérer l'application ψ qui à un élément inversible m associe l'automorphisme $x \mapsto m.x$;
• il est clair que c'est un morphisme injectif de $(\mathbb{Z}/n\mathbb{Z})^*$ dans $Aut(\mathbb{Z}/n\mathbb{Z})$
• étant donné un automorphisme f de $\mathbb{Z}/n\mathbb{Z}$ on montre facilement qu'il est égal à $\psi(f(1))$.□

Corollaire 153 *$Aut(\mathbb{Z}/n\mathbb{Z})$ est un groupe abélien d'ordre $\phi(n)$.*

⊡ **Forme des groupes** $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$

p désigne un nombre premier.

Lemme 154 $(\mathbb{Z}/p\mathbb{Z})^* \simeq (\mathbb{Z}/(p-1)\mathbb{Z}, +)$

Démonstration : $(\mathbb{Z}/p\mathbb{Z})$ est un corps fini (voir le chapitre sur la théorie des groupes).

On sait (voir proposition 174) que le groupe multiplicatif d'un corps fini est cyclique, donc isomorphe à un certain $(\mathbb{Z}/n\mathbb{Z})$.

Il suffit donc de se rappeler que le cardinal de $(\mathbb{Z}/p\mathbb{Z})^*$ est $p-1$ pour conclure.□

Lemme 155 *Si $k > 0$, alors $(1+p)^{p^k} = 1 + \lambda.p^{k+1}$, avec $\lambda > 0$ et $\lambda \wedge p = 1$.*

Démonstration : Par récurrence sur k :
• $k = 1$
$(1+p)^p = \sum_{i=0}^{p} C_p^i p^i$

donc $(1+p)^p = 1 + p^2 + m.p^3 = 1 + p^2.(1+m.p)$
• k quelconque
On écrit $(1+p)^{p^{k+1}} = ((1+p)^{p^k})^p = (1+\lambda.p^{k+1})^p$; il suffit alors de développer en utilisant le binôme de Newton la puissance k-ième en isolant le premier et le dernier terme.□

Corollaire 156 *$1+p$ est d'ordre $p^{\alpha-1}$ dans $\mathbb{Z}/p^\alpha\mathbb{Z}$.*

Démonstration : il est d'ordre au plus $p^{\alpha-1}$ au vu du lemme précédent.
En outre $(1+p)^{p^{\alpha-2}} = 1 + \lambda.p^{\alpha-1}$, et donc ne saurait être congru à 1 modulo p^α.□

Lemme 157 *Si m et t sont premiers entre eux, et si a et b commutent, et si a est d'ordre m et b est d'ordre t, alors $a.b$ est d'ordre $m.t$.*

Démonstration : • Il est facile de voir que ab est d'ordre au plus $m.t$, puisque a et b commutent.
• Réciproquement, si $(ab)^n = 1$, alors $a^{n.t}.b^{n.t} = 1$, donc $a^{n.t} = 1$, puisque $b^{n.t} = 1$. Donc t divise l'ordre de ab. De même m divise l'ordre de ab ; donc $m.t$ divise l'ordre de ab, puisque m et t sont premiers entre eux.□

Proposition 158 *Si p premier > 2, $m \geq 2$, alors*

$$(\mathbb{Z}/p^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/\phi(p^\alpha)\mathbb{Z} \simeq \mathbb{Z}/p^{\alpha-1}.(p-1)\mathbb{Z}$$

Démonstration : On va utiliser les lemmes précédents.
• On considère tout d'abord l'application ψ définie par

$$\psi : (\mathbb{Z}/p^\alpha\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$$

ψ étant la fonction induite par l'identité (il convient de bien vérifier que ψ est bien définie et est un morphisme de groupes surjectif)
• par le lemme 154 tout élément dont l'image par ψ est non égal à $\overline{1}$ engendre $(\mathbb{Z}/p\mathbb{Z})^*$; donc son ordre est un multiple de $p-1$ (voir le lemme 154).
• étant donné x un tel élément, il existe y appartenant au groupe engendré par x tel que y est d'ordre $p-1$.
• On applique alors le lemme 157, $y.(p+1)$ est d'ordre le produit des ordres de y et de $p+1$; or y est d'ordre $p-1$ comme on vient de le voir, et $p+1$ est d'ordre $p^{\alpha-1}$ par le corollaire 156 ; $y.(p+1)$ est donc d'ordre $(p+1).p^{\alpha-1}$; le groupe engendré par y est donc nécessairement $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ tout entier, d'où le résultat.□

On vient donc par cette proposition de détailler la forme des $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ dans le cas où $p > 2$. Il convient de considérer le cas $p = 2$.

Lemme 159

$$k > 0 \rightarrow 5^{2^k} = 1 + \lambda.2^{k+2}$$

avec $\lambda \wedge 2 = 1$ *(i.e.* λ *impair)*

Démonstration : Facile, par récurrence.□

Proposition 160 $(\mathbb{Z}/2.\mathbb{Z})^* = \{1\}$, $(\mathbb{Z}/4.\mathbb{Z})^* = \{1, -1\} \simeq \mathbb{Z}/2.\mathbb{Z}$, *et ensuite (pour* $\alpha \leq 3$*)* $(\mathbb{Z}/2^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/2.\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$.

Démonstration :

• On considère le morphisme surjectif ψ induit par l'identité de $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ sur $(\mathbb{Z}/4.\mathbb{Z})^* = \{1, -1\} \simeq \mathbb{Z}/2.\mathbb{Z}$.
• Le noyau de ψ est d'ordre $2^{\alpha-2}$
• 5 appartient au noyau de ψ.
• par le lemme 159, 5 est d'ordre $2^{\alpha-2}$ (l'ordre est une puissance de 2, et $5^{2^{\alpha-3}}$ ne peut être congru à 1)
• le noyau de ψ est donc cyclique (au vu des trois affirmations précédentes)
• On a alors la suite exacte (voir chapitre sur la théorie des groupes)

$$1 \rightarrow \mathbb{Z}/2^{\alpha-2} \rightarrow (\mathbb{Z}/2^\alpha\mathbb{Z})^* \stackrel{\psi}{\rightarrow} \mathbb{Z}/2.\mathbb{Z} \rightarrow 1$$

• Le sous-groupe $\{-1, 1\}$ de $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ est une section de ψ, et il est distingué puisque notre groupe $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ est abélien. Donc on a un produit direct

$$(\mathbb{Z}/2^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/2.\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$$

ce qui conclut la preuve (précisons que le produit direct $A \times B$ est isomorphe au produit direct $B \times A$...).□

2.5.3 Idéaux étrangers

Définition 161 *Soit* A *un anneau et* c *et* d *deux idéaux bilatèresde* A*. Les anneaux* c *et* d *sont dits étrangers (ou comaximaux) si* $c + d = A$.

Exemples : deux idéaux maximaux sont toujours étrangers.

Proposition 162 *Si* $a_1, \ldots, a_n$, $b_1, \ldots, b_m$ *sont des idéaux bilatères de* A*, et si pour tout* $(i, j) \in \{1, \ldots, n\} \times \{1, \ldots, m\}$ a_i *et* b_j *sont étrangers, alors les idéaux* $a_1 \times a_2 \times \cdots \times a_n$ *et* $b_1 \times b_2 \times \cdots \times b_m$ *sont étrangers.*

Démonstration : On fait d'abord la preuve pour $m = 1$ en utilisant des égalités : $x_i + y_i = 1$ avec $x_i \in a_i$ et $y_i \in b_1$. On multiplie terme à terme. Puis on fait pareil avec $a_1, \ldots, a_n$ et chaque b_i. □

Remarque : dans $\mathbb{Z}$, a et b sont premiers entre eux si et seulement si (a) et (b) sont étrangers.

Chapitre 3

Corps

3.1 Définitions de base

Définition 163 *Un anneau $(K, +, .)$ est un* **corps** *si et seulement si le groupe des unités est $K - \{0\}$.*
Un corps est dit **commutatif** *si l'anneau sous-jacent est commutatif, c'est à dire si la multiplication est commutative.*

Propriétés :
• Un anneau commutatif non nul est un corps si et seulement si ses seuls idéaux sont les idéaux triviaux.
• Un anneau intègre fini est un corps.

3.2 Extensions de corps

Définition 164 *Un sous-anneau L de l'anneau sous-jacent à un corps K est un* **sous-corps** *de K si c'est un corps pour les lois induites.*
Si L est un sous-corps de K, on dit que K est un **sur-corps** *ou une* **extension** *de L.*
Avec L sous-corps de K, et $A \subset K$, on dit que A **engendre** *K sur L si K est le plus petit sous-corps de K contenant A et L. On note alors $K = L(A)$. Si A est fini on note $K = L(a_1, ..., a_n)$. L'extension est dite monogène si A contient un seul élément.*

Théorème 165 *Etant donné un anneau intègre A, il existe un unique corps K (à isomorphisme près) contenant un anneau intègre B isomorphe à A et tel que tout sous-corps de K contenant B soit K lui-même.*

Démonstration : On procède selon les étapes suivantes pour montrer l'existence :
• On considère les classes d'équivalences sur $A \times A$ pour la relation $\mathcal{R}$ définie par $(x,y)\mathcal{R}(x',y') \iff xy' = x'y$ (intuitivement les classes d'équivalence sont les fractions). Appelons K l'ensemble quotient ainsi obtenu.
• On considère ensuite l'addition sur ces classes, facile à retrouver au vu de la considération sur les fractions ; il s'agit de $(x,y)+(x',y') = (xy'+x'y, yy')$. De même la multiplication est définie par $(a,b).(a',b') = (aa',bb')$. Il est facile de voir que ces lois vérifient toutes les propriétés souhaitées, et qu'elles sont bien définies dans la structure quotient. On trouve un élément $(0,1)$ neutre pour l'addition, et un élément $(1,1)$ neutre pour la multiplication.
• L'application qui à x associe $(x,1)$ est un morphisme injectif de A dans K. C'est donc un isomorphisme de A sur son image A'.
• Etant donné un sous-corps de K contenant A', il contient nécéssairement les quotients d'éléments de A', et donc K tout entier.
• Il ne reste plus qu'à vérifier l'unicité de K, à isomorphisme près. Cette tâche est laissée au lecteur.□

Applications :
• Construction de $\mathbb{Q}$ à partir de $\mathbb{Z}$.
• Construction du corps des fractions rationnelles, à partir de l'anneau des polynômes.

Proposition 166 • *Si L est un sous-corps de K, alors K est un L-espace vectoriel.*
• *Si la dimension de K en tant que L-espace vectoriel est finie alors on l'appelle* **degré** *de K pour L et on le note $[K:L]$.*
• *Si K et L sont finis, alors $|K| = |L|^{[K:L]}$.*

Démonstration : Le premier point est clair.
Le second point est une définition.
Le troisième point est clair.□

Théorème 167 (Théorème des bases téléscopiques) *Si $M \subset L \subset K$ (tous trois des corps) alors si e_i est une base de K en tant que L-espace vectoriel et si f_j est une base de L en tant que M-espace vectoriel , alors $e_i.f_j$ est une base de K en tant que M-espace vectoriel . Donc $[K:M] = [K:L].[L:M]$.*

Démonstration : Facile.□

Définition 168 (Différentes extensions de corps) *Si L est une extension du corps K, alors un élément a de L est dit* **algébrique sur** *K s'il existe un polynôme P à coefficients dans K tel que $P(a) = 0$. Un nombre réel est souvent dit simplement* **algébrique** *s'il est algébrique sur $\mathbb{Q}$. L'ensemble des éléments de L algébriques sur K est appelée extension algébrique de K dans L.*
Etant donné K un corps et $P \in K[X]$, on appelle **corps de rupture de** *P un sur-corps L de K dans lequel P admet une racine a et tel que $L = K(a)$.*
Etant donné K un corps et $P \in K[X]$, on appelle **corps de décomposition de** *P un sur-corps L de K dans lequel P est scindé et $L = K(Z)$, avec Z l'ensemble des zéros de P dans L.*
Etant donné K un corps, on appelle **cloture algébrique** *de K une extension de K algébriquement close et dont tous les éléments soient algébriques sur K.*

On a existence du corps de décomposition, et existence du corps de rupture lorsque le polynôme est irréductible. Dans les deux cas, on a unicité à isomorphisme près. Le théorème de Steinitz (difficile) montre que tout corps admet une cloture algébrique, unique à isomorphisme près.

Démonstration : (de l'existence du corps de rupture) Le corps $K(X)/(P)$ convient (ie le quotient de K par l'idéal engendré par P). □

3.3 Corps finis

Proposition 169 *Un anneau intègre fini est un corps.*

Démonstration : Si un anneau est intègre, l'application $x \mapsto yx$ est bijective pour tout y. En particulier, il existe x tel que $yx = 1$.□

Théorème 170 *Un corps fini n'est jamais algébriquement clos.*

Démonstration : Facile ; il suffit de considérer le polynôme $\Pi_{k \in K}(X - k) + 1$.□

Théorème 171 *Quel que soit p premier, quel que soit n dans $\mathbb{N}$ non nul, il existe un unique corps, à isomorphisme près, de cardinal p^n. Tout corps fini est de cette forme.*

Théorème 172 (Wedderburn) *Tout corps fini est commutatif.*

Démonstration : Ces résultat, non triviaux, ne seront pas prouvés ici. On pourra consulter [14] pour une preuve compréhensible.□

Enfin deux résultats (non triviaux) donnés sans preuve :

Proposition 173 *Le groupe des automorphismes d'un corps fini de cardinal p^n est cyclique, d'ordre n, engendré par $x \mapsto x^n$.*

Proposition 174 *Le groupe multiplicatif d'un corps fini est cyclique.*

Chapitre 4

Quelques résultats supplémentaires d'arithmétique et théorie des nombres

4.1 Sous-groupes additifs de $\mathbb{R}$

Proposition 175 *Tout sous-groupe G du groupe $(\mathbb{R}, +)$ vérifie l'une et une seule des deux conditions suivantes :*

$$\exists x / G = x\mathbb{Z}$$

G est dense dans $\mathbb{R}$

Démonstration :

- On considère $\alpha = infG \cap R^{+*}$.
- On distingue les deux cas $\alpha > 0$ et $\alpha = 0$.□

4.2 Représentation p-adique des réels

Définition 176 *On se donne un entier $p > 1$. On appelle représentation p-adique du réel x la suite d'entiers $(c_n)_{n\in\mathbb{N}}$ définie par*

$$c_n = \begin{cases} E(x) \text{ si } n = 0 \\ \frac{1}{p^n} E(p^n x) - pE(p^{n-1}x) \text{ sinon} \end{cases}$$

($E(y)$ désignant la partie entière de y).

□

Théorème 177 (Caractérisation du développement p-adique) **Théorème 178** *Le développement p-adique de $x \in \mathbb{R}$ est périodique à partir d'un certain rang si et seulement si x est rationnel.*

Démonstration :

• Supposons tout d'abord le développement périodique.

Alors x est somme des $c_n p^{-n}$ pour $n \in \mathbb{N}$. Vue la périodicité, cette somme se réécrit comme somme d'un rationnel et de $\sum_{n\geq N} \frac{a}{(p^{-k})^n}$, avec a dans $\mathbb{N}$, et donc x est somme d'un rationnel et de $\frac{ap^{-kN}}{1-p^{-k}}$, et donc x est rationnel.

• Réciproquement supposons que x soit rationnel.

- On peut écrire $x = a/b$ avec a et b dans $\mathbb{N}$ (on se limite au cas $x > 0$, les autres cas étant similaires)

- On définit $x_0 = a$, et par récurrence $x_{n+1} = (x_n - bc_n)p$, avec c_n le quotient dans la division euclidienne de x_n par b.

- On montre facilement par récurrence que $0 \leq x_i < bp$ pour tout i et que les c_i sont le développement p-adique de x.

- les x_i étant bornés, on passe nécéssairement deux fois par la même valeur ; à partir de ce moment, le développement est clairement périodique.□

4.3 Fractions continues

Définition 179 (Fractions continues) *Une* **fraction continue** *est un objet de la forme suivante :*

$$[a_0, a_1, \ldots, a_n, \ldots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$$

Elle est caractérisée par une suite d'entiers qui est finie ou infinie.
On appelle **convergents** *d'une fraction continue la suite de numérateurs p_n et de dénominateurs q_n définis par :*
- $p_0 = a_0$, $q_0 = 1$
- $p_1 = a_0 a_1 + 1$, $q_1 = 1$
- $\vdots$
- ,$\vdots$
- $p_n = a_n p_{n-1} + p_{n-2}$,$q_n = a_n q_{n-1} + q_{n-2}$

Propriétés :

- A tout nombre réel on peut associer un et un seul développement en fraction continue.
- Tout nombre rationnel peut être représenté par une fraction continue finie (ex $\frac{1}{3} = 0 + \frac{1}{2+1}$).
- Seuls les nombres rationnels peuvent être représentés par une fraction continue finie.
- Un nombre est quadratique (ie solution d'une équation du second degré à coefficients dans $\mathbb{Z}$) si et seulement si son développement en fraction continue est périodique.
- Une fraction continue est liée à ses convergents par les relations $[a_0, \ldots, a_n] = p_n/q_n$ et $[a_0, \ldots, a_n, \ldots] = \lim_n \frac{p_n}{q_n}$. En outre avec

$$[a_0, \ldots, a_n] = \frac{p_n}{q_n},$$

$$|[a_0, \ldots, a_n] - [a_0, \ldots, a_n, \ldots]| < 1/q_n^2.$$

Théorème 180 (Formule d'Euler) *Supposons les a_i tous non nuls.*
Alors $1/a_1 - 1/a_2 + 1/a_3 - 1/a_4 + ... + (-1)^n/a_n =$

$$\cfrac{1}{a_1 + \cfrac{a_1^2}{a_2 - a_1 + \cfrac{a_1^2}{a_3 - a_2 + \cfrac{a_3^2}{\ddots + \cfrac{\ddots}{a_{n-1} - a_{n-2} + \cfrac{a_{n-1}^2}{a_n - a_{n-1}}}}}}}$$

Démonstration :

• Pour $n = 1$, le résultat est clair.

• Au rang 2, un calcul rapide montre que le résultat est encore valable.

• On procède ensuite par récurrence, en supposant l'égalité vraie pour $n - 1$ et les rangs inférieurs.

• Dans l'égalité pour $n - 1$, on remplace a_n par $\frac{a_n.a_{n+1}}{a_{n+1}-a_n}$

• Le résultat en découle tout seul...□

4.4 Cryptographie à clé révélée : RSA

Précisons que l'on parle aussi de clé publique .

L'objectif de la **cryptographie** est de permettre de communiquer par des messages codés, qui ne pourront être lus que par leur destinataire.

Pour cela, un "superviseur" donne à chaque receveur potentiel un "décodeur" et une "clé". La clé, comme son nom ne l'indique peut-être pas, est quelque chose qui peut être diffusé à tout le monde.

Pour envoyer un message M crypté à un individu I, il suffit de passer le message M par la moulinette de la clé correspondante à I. Cela n'est pas difficile, puisque I diffuse abondamment sa clé, à tous ses correspondants éventuels. Lorsque I reçoit un message, il peut alors utiliser son décodeur, qu'il est seul à posséder, pour transformer le message crypté en le message original.

La difficulté est que, formellement, il est toujours possible de reconstruire le message initial à partir du message crypté, pourvu que vous ayez la clé. Pour cela, il suffit de tester tous les messages possibles, l'un après l'autre (ils sont bien en bijection avec $\mathbb{N}$, comme on peut s'en convaincre facilement en considérant l'ordre lexicographique sur les messages possibles), et de les passer par la moulinette de la clé jusqu'à ce que l'on retrouve le message crypté. Mais il reste un espoir de fabriquer une cryptographie efficace, car bien sûr, cette méthode prendrait un temps énorme. La cryptographie est ainsi basée sur l'hypothèse de base que certaines tâches, faciles à faire dans un sens (le sens du cryptage par une clé), est difficile à faire dans l'autre (décryptage à l'aide d'une clé).

On note bien que la difficulté réside dans le fait que la fonction "clé" est publique. Si on cache la clé, il est très facile de réaliser des cryptographies parfaites. Par exemple, on peut utiliser le protocole suivant pour que A envoie un message à B :

- A signale à B qu'il veut lui envoyer un message, que l'on supposera constitué uniquement de 0 et de 1 (par un codage quelconque on peut facilement se ramener à cela), et de longueur 1000.

- B fournit à A une liste L de 1000 chiffres 0 ou 1, 0 et 1 étant équiprobables.

- le protocole recommence à l'étape précédente jusqu'à ce que la liste de chiffres soit passée sans être interceptée ; on tire au sort une nouvelle liste de 1000 chiffres à chaque nouvel essai.

- A transforme le message M en un message M', par $M' = M + L$ dans $\mathbb{Z}/2\mathbb{Z}$.

- A envoit M' à B ; si M' est intercepté, il ne sera pas décodable, puisque L n'est pas connu.

- B décode M' par $M = M' + L$ dans $\mathbb{Z}/2\mathbb{Z}$.

Aucune interception ne permet de décoder le message ; mais les étapes 2 et 3 peuvent prendre du temps ou n'être pas réalisables. Il est indispensable de changer de liste L à chaque nouveau message, ou du moins régulièrement - sinon, en considérant les fréquences des 0 et des 1, un observateur des différents M' pourrait finir par reconstituer L.

L'algorithme **RSA**, du nom de ses inventeurs, Rivest, Shamir et Adleman, est basé sur la difficulté de la factorisation d'un nombre entier en nombres premiers.

Supposons que A souhaite envoyer des messages cryptés RSA à B. Alors B se donne deux grands nombres premiers p et q. Maple permet aisément de construire de tels nombres, par exemple ; il suffit par exemple de tirer des nombres au sort et de recommencer jusqu'à ce qu'ils soient premiers, grâce à un algorithme permettant de dire si oui ou non un nombre est premier. En fait les algorithmes utilisés pour cela sont généralement probabilistes, c'est-à-dire qu'ils ont une probabilité non nulle de se tromper ; mais les erreurs sont extrêmement rares. La fonction Maple "isprime" permet de tester la primalité d'un nombre ; par exemple, "isprime(1234567890123456789012345678901234567)" renvoit "false", donc "1234567890123456789012345678901234567" n'est pas premier.
"nextprime(1234567890123456789012345678901234567)" renvoit
"1234567890123456789012345678901234651", qui est donc le nombre premier le plus petit plus grand que celui-ci. On constate donc que Maple permet très rapidement de trouver de grands nombres premiers ; les exemples ici fournis ne sont pas du tout à la limite du faisable, on peut aller largement au delà.

Ces deux nombres premiers seront notés p et q. La première partie de la clé publique, notée c, sera le produit de p et q. A choisit alors un nombre d, premier avec $\phi(c) = (p-1)(q-1)$, avec ϕ la fonction d'Euler, c'est-à-dire le nombre de nombres premiers plus petits que c, donc $(p-1)(q-1)$. Il est facile de choisir un nombre qui soit premier avec un autre : il suffit d'en piocher un au hasard, et de recommencer jusqu'à ce que l'algorithme de Bezout confirme que ces nombres sont premiers entre eux. On peut aussi déterminer facilement d^{-1}, inverse de d dans $(\mathbb{Z}/c\mathbb{Z})^* \simeq \mathbb{Z}/\phi(c)\mathbb{Z}$ (il y a isomorphisme car $(\mathbb{Z}/c\mathbb{Z})^* \simeq (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$ par le corollaire 151 et isomorphisme entre $(\mathbb{Z}/p\mathbb{Z})^*$ et $\mathbb{Z}/(p-1)\mathbb{Z}$ (resp. $(\mathbb{Z}/q\mathbb{Z})^*$ et $\mathbb{Z}/(q-1)\mathbb{Z}$) par le lemme 154) : il suffit d'utiliser l'algorithme de Bezout.

Cryptage :

- On suppose le message suffisamment court pour être codable par un élément inversible de $\mathbb{Z}/c\mathbb{Z}$, ce qui est possible en remplaçant le message par des tranches successives suffisamment petites (si on a un alphabet de taille α, il suffit de prendre des tranches de longueur l avec $\alpha^l < \phi(c)$). Cette méthode de codage n'a pas à être compliquée ni à être cachée. Il suffit donc d'avoir une injection de $[1, \alpha^l]$ dans $(\mathbb{Z}/c\mathbb{Z})^*$.

- chaque message de A est donc remplacé (par A) par un élément n inversible dans $\mathbb{Z}/c\mathbb{Z}$.

- A envoie alors à B le nombre $e = n^d$ dans $\mathbb{Z}/c\mathbb{Z}$.

Décryptage :

- B, qui dispose de d et de d^{-1}, effectue simplement le calcul de $e^{d^{-1}}$, qui lui donne n, et donc le message initial.

D'autres systèmes de cryptographie à clé publique font intervenir des structures plus complexes que $\mathbb{Z}/n\mathbb{Z}$, comme par exemple les courbes elliptiques.

Chapitre 5

Polynômes à une indéterminée

5.1 Généralités

Définition 181 *Soit A un anneau commutatif unitaire (resp. $\mathbb{K}$ un corps).*
L'ensemble des suites nulles à partir d'un certain rang d'éléments de A, noté $A^{(\mathbb{N})}$, est un A-module (resp. un $\mathbb{K}$-espace vectoriel) pour l'addition et la multiplication par un scalaire usuelles. En le munissant en outre du produit suivant :

$$\times : (u, v) \mapsto w \text{ avec } w_n = \sum_{i+j=n} u_i.v_j$$

On obtient une A-algèbre (resp. $\mathbb{K}$-algèbre), notée $A[X]$ (resp. $\mathbb{K}[X]$).
Les éléments de $\mathbb{K}[X]$ sont appelés **polynômes**.
Deux polynômes P et Q non nuls sont dits **associés** *s'il existe λ inversible tel que $P = \lambda.Q$.*
On identifie A $\mathbb{K}$ et l'ensemble des suites $(u_n)_{n\in\mathbb{N}}$ avec $u_n = 0$ pour tout $n > 0$, par l'isomorphisme canonique $x \mapsto (u_n)_{n\in\mathbb{N}}$ avec $u_0 = x$ et $n > 0 \to u_n = 0$.
On note X l'élément $(u_n)_{n\in\mathbb{N}}$ avec $u_0 = 0$, $u_1 = 1$, et $u_n = 0$ pour $n > 1$.
La famille des X^i pour $i \in \mathbb{N}$ constitue la base canonique du module libre $A^(\mathbb{N})$ (resp. du $\mathbb{K}$-espace vectoriel $K^{(N)}$.
Etant donné P un polynôme, on appelle **degré de** *P et on note $\deg P$ le plus grand n tel que P_n est non nul. On appelle* **coefficient dominant de** *P le coefficient de $X^{\deg P}$ (que l'on peut voir comme $X^{deg(P)^*}(P)$ si l'on travaille avec un corps, voir la partie* **??)** *; on le note $coef(P)$.*
Un polynôme non nul est dit **unitaire** *si son coefficient dominant est 1.*
On appelle **support d'un polynôme** *P l'ensemble des $n \in \mathbb{N}$ tels que $X^{n*}(P) \neq 0$. Par définition d'un polynôme, son support est fini.*
Le degré d'un polynôme P est donc aussi le sup de son support.
On appelle **valuation de** *P et on note $val(P)$ l'inf du support de P.*
On appelle **composé de deux polynômes** *P* **et** *Q et on note $P \circ Q$ le polynôme $\sum P_n Q^n$ (que l'on peut aussi voir comme $\sum_{n\in\mathbb{N}} X^{i*}(P).Q^i$ si l'on travaille avec un corps).*

Proposition 182 • 1 *est élément neutre pour la multiplication,* X *élément neutre pour* $\circ$*,* 0 *élément neutre pour l'addition.*
• *Les éléments inversibles de* $\mathbb{K}[X]$ *sont les éléments identifiés aux éléments de* $\mathbb{K} \setminus \{0\}$.
• $deg(0) = -\infty$ *et* $val(0) = +\infty$
• $deg(1) = 0$
• $deg(X^i) = i$ *et* $val(X^i) = i$
• $deg(P.Q) = deg(P) + deg(Q)$ *et* $val(P.Q) = val(P) + val(Q)$
• $deg(P + Q) \leq sup(deg(P), deg(Q))$ *avec égalité si* $deg(P) \neq deg(Q)$ *ou si les coefficients dominants de* P *et* Q *ne sont pas opposés.*
• $val(P + Q) \leq sup(val(P), val(Q))$ *avec égalité si* $val(P) \neq val(Q)$ *ou si* $P_{val(P)}$ *et* $Q_{val(Q)}$ *ne sont pas opposés.*
• *si* A *est intègre alors* $A[X]$ *est un anneau intègre ; c'est à dire que le produit de deux polynômes est nul si et seulement si l'un des deux polynômes est nul.*
• $(P+Q) \circ R = P \circ R + Q \circ R$ *mais en général* $P \circ (Q+R) \neq P \circ Q + P \circ R$

5.2 Division euclidienne

Théorème 183 (Division euclidienne) *Soient* A *et* B *deux polynômes, avec* $coef(B)$ *inversible. Alors*

$$\exists (Q, R) \text{ polynômes } / A = B.Q + R$$

avec

$$deg\ R < deg\ B$$

Démonstration : • Unicité :
Supposons $B.Q + R = B.Q' + R'$ avec les conditions données sur le degré. Alors

$$B.(Q - Q') = R' - R$$

$$deg(B) + deg(Q - Q') = deg(R' - R)$$

donc

$$deg(Q - Q') = -\infty$$

et $Q = Q'$ et $R = R'$.
• Existence :
On distingue deux cas.
- Si le degré de A est inférieur strictement au degré de B, le résultat est clair avec $Q = 0$ et $R = A$.
- Sinon on procède par récurrence sur le degré de A, en considérant

$$A - \frac{coef(A)}{coef(B)}.X^{deg(A)-deg(B)}$$

...□

Il est à remarquer que c'est par la méthode de la récurrence que l'on pratique la division euclidienne.

Définition 184 *Q est appelé* **quotient** *de A par B, et R est appelé* **reste** *de A par B.*

Un exemple en Maple :

Exemple Maple

$> \ rem(x^4+x^3+x^2+x+1, x^3, x);$

$$1+x^2+x$$

$> \ quo(x^4+x^3+x^2+x+1, x^3, x);$

$$x+1$$

Corollaire 185 *Soit $\mathbb{K}$ un corps. $\mathbb{K}[X]$ est un anneau euclidien, donc un anneau principal.*

Démonstration : La division euclidienne en est la preuve ; dans un corps, tout polynôme non nul a son coefficient dominant inversible.□

5.3 Fonction associée, racines d'un polynôme

Définition 186 *Etant donnée B une A-algèbre associative commutative et unitaire, on peut identifier P à une application de A dans A, dite* **application polynômiale associée à** *A, noté $\tilde{P}$, et définie par*

$$\tilde{P}(x) = \sum_{n\in\mathbb{N}} P_n \, x^n$$

Cela est notamment valable pour $B = A$; implicitement $\tilde{P}$ désignera généralement une fonction de A dans A.

Proposition 187 *Soit a dans A et P un polynôme appartenant à $A[X]$.*
Le reste de la division euclidienne de P par $(X-a)$ est $P(a)$.

En considérant la division euclidienne de P par $(x-a)^n$, on peut énoncer la défi-

nition suivante :

Proposition 188 - Définition
Soit P un polynôme, a un élément de A et n un entier naturel.
Les conditions suivantes sont équivalentes :
- $(X-a)^n | P$ et $(X-a)^{n+1} \not| P$
- Il existe un polynôme Q tel que $P = (X-a)^n Q$ et $\tilde{Q}(a)$ non nul.
On dit alors que a est **racine** *de P d'***ordre de multiplicité** *n.*

5.4 Cas où $A = \mathbb{K}$ est un corps

Théorème 189 *Si $\mathbb{K}$ est un corps commutatif alors $\mathbb{K}[X]$ est un anneau euclidien, donc un anneau principal, donc un anneau factoriel.*

Démonstration : Le fait que $\mathbb{K}[X]$ est un anneau euclidien a été prouvé en proposition 127.□

Proposition 190 - Définition *On dit qu'un corps $\mathbb{K}$ est* **algébriquement clos** *si et seulement si l'une des trois propositions suivantes est vérifiée :*
- tout polynôme de $\mathbb{K}[X]$ est **scindé**, *c'est-à-dire produit de polynômes de degré 1*
- tout polynôme non constant a une racine dans $\mathbb{K}$
- tout polynôme irréductible est de degré 1


Dans $\mathbb{K}[X]$ avec $\mathbb{K}$ corps algébriquement clos, tout polynôme de degré n s'écrit de manière unique à l'ordre près des facteurs sous la forme :

$$c(X-k_1)(X-k_2)\dots(X-k_n)$$

avec c inversible, et les k_i les racines (pas forcément distinctes !) du polynôme.


$\mathbb{C}$ est algébriquement clos, comme énoncé dans la proposition **??**.

Un exemple en Maple :

Exemple Maple

$> \ P := X -> x\hat{}\,4 - 1;$

$$P := X^4 - 1$$

$> \ factor(P);$

$$(x-1)(x+1)(x^2+1)$$

$> \ factor(P, complex);$

$$(x+1.)(x+1.\,I)(x-1.I)(x-1.000000000)$$

5.5 Zoologie des polynômes

En dehors des paragraphes ci-dessous, on pourra consulter la partie**??** sur l'interpolation par les polynômes de Lagrange, d'ailleurs généralisable à un cadre plus vaste que les polynômes réels, et le théorème **??**, d'approximation par les polynômes de Bernstein.

5.5.1 Relations entre les racines et les coefficients d'un polynôme - localisation des racines d'un polynôme

On se donne pour l'ensemble de cette partie un polynôme $P \in \mathbb{C}[X]$, de degré n, P non nul. On définit $P = \sum_{i=0}^{n} p_i X^i$.

⊡ Relations entre les racines et les coefficients d'un polynôme

On utilisera ici les polynômes symétriques élémentaires $\Sigma_i = \Sigma_{i,n}$ définis en partie 6.3.1.

Théorème 191 (Relations entre racines et coefficients d'un polynôme)
Notons $\sigma_i = \Sigma_i(r_1, ..., r_n)$, avec r_1,...,r_n des complexes.
On a $P = \lambda\Pi_{i=1}^{n}(X - r_i)$ pour un certain λ si et seulement si $\sigma_i = (-1)^i \frac{p_{n-i}}{p_n}$.

Démonstration : On écrit simplement l'égalité

$$\sum_{i=0}^{n} p_i X^i = \lambda\Pi_{i=1}^{n}(x - r_i)$$

On en déduit que $\lambda = p_n$, et les relations souhaitées en développant d'un côté et de l'autre du signe $=$.□

⊡ Localisation des racines d'un polynôme

◇ **Premières informations** Le théorème de Rolle **??** permet de montrer que le polynôme dérivé d'un polynôme scindé est scindé.

◇ **Méthode itérative** On peut par exemple utiliser la méthode de Newton, trouvable dans tout bon ouvrage d'analyse numérique. On pourra par exemple consulter [9]. FLEMMARD verifier

◇ **Méthode algébrique** La théorie du résultant donne quelques résultats intéressants sur la localisation de racines ; voir théorème 195.

5.5.2 Polynômes irréductibles

Définition 192 *Un polynôme P appartenant à $\mathbb{K}[X]$ est dit* **polynôme irréductible** *si il est irréductible en tant qu'élément de l'anneau $\mathbb{K}[X]$, c'est-à-dire s'il n'est pas inversible et si tout diviseur de P est une unité ou est produit de P par une unité.*

Pour plus d'informations sur la recherche de facteurs irréductibles communs à deux polynômes, on consultera le théorème 195.

Théorème 193 • *Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.*
• *Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes aX^2+bX+c, avec $a \neq 0$ et $b^2-4ac<0$.*

Démonstration : Il est évident que les polynômes considérés sont bel et bien irréductibles, dans les deux cas réel et complexe. Réciproquement, le théorème de D'Alembert-Gauss **??** donne le résultat dans le cas complexe. Dans le cas réel, on procède comme suit :

• Supposons $P \in \mathbb{R}[X]$ irréductible dans $\mathbb{R}[X]$.

• Par simplicité et sans perte de généralité, on va supposer P unitaire.

• Si x est racine de P dans $\mathbb{C}$, alors $\overline{x}$ l'est aussi, avec le même ordre de multiplicité.

• P n'a pas de racine réelle r, sinon $X-r$ diviserait P et P ne serait pas irréductible.

• P peut donc s'écrire $P=\Pi_{i=1}^{r}(X-r_i)^{n_i}(X-\overline{r}_i)^{n_i}$.

• $(X-r_i)(X-\overline{r}_i)$ est alors un polynôme réel (on le voit simplement en le développant), donc P est un produit de polynômes de discriminants négatifs strictement (là aussi il suffit de développer pour le voir). Il n'est irréductible que s'il contient un et un seul tel terme.

D'où le résultat.□

5.5.3 Résultant. Discriminant

Définition 194 *Etant donnés P et Q deux polynômes de $\mathbb{K}[X]$, on appelle* **résultant de P et Q** *le déterminant de la matrice suivante :*

$$\begin{pmatrix}
P_0 & 0 & 0 & 0 & \dots & 0 & Q_0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\
P_1 & P_0 & 0 & 0 & \dots & 0 & Q_1 & Q_0 & 0 & 0 & \dots & 0 & 0 & 0 \\
P_2 & \dots & P_0 & 0 & \dots & 0 & Q_2 & \dots & Q_0 & 0\dots & 0 & 0 & 0 & \\
P_3 & \dots & \ddots & \ddots & \ddots & 0 & Q_3 & \dots & \ddots & \ddots & \ddots & \ddots & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & Q_q & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & 0 & Q_q & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & 0 & 0 & Q_q & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & 0 & \ddots & 0 & Q_q & \vdots & \vdots & \vdots & \vdots \\
P_p & P_{p-1} & \vdots & \vdots & \vdots & \vdots & 0 & \ddots & 0 & Q_q & \vdots & \vdots & \vdots & \vdots \\
0 & P_p & \ddots & \ddots & \ddots & \ddots & 0 & \ddots & 0 & Q_q & \ddots & \ddots & \ddots & \ddots \\
0 & 0 & P_p & \ddots & \ddots & \ddots & 0 & \ddots & 0 & Q_q & \ddots & \ddots & \ddots & \ddots \\
0 & \dots & 0 & P_p & \ddots & \ddots & 0 & \ddots & 0 & Q_q & \ddots & \ddots & \ddots & \ddots \\
0 & \dots & \dots & \dots & \dots & P_p & 0 & \dots & \dots & \dots & \dots & \dots & 0 & Q_q
\end{pmatrix}$$

avec $P = \sum_{k=0}^{p} P_p X^k$ et $Q = \sum_{k=0}^{q} Q_q X^k$.
On appelle **discriminant** *d'un polynôme P le résultant de P et de P' son polynôme dérivé.*

Théorème 195 *Le résultant de P et Q est nul si et seulement si P et Q ont au moins un facteur irréductible en commun.*
Le discriminant d'un polynôme P est nul si et seulement si il a au moins un facteur irréductible en commun avec son polynôme dérivé.

Démonstration :

La deuxième affirmation n'est naturellement qu'une spécialisation de la première. On se contentera donc de prouver la première.

• Supposons tout d'abord que P et Q aient un facteur irréductible commun R.

- Alors $P = RS$ et $Q = RT$, avec $deg\ T = deg\ Q - deg\ R$ et $deg\ S = deg\ P - deg\ R$, T et S non nuls.

- $PT = QS$, ou $PT - QS = 0$. Ceci exprime très exactement l'existence d'un vecteur X tel que la matrice M donnée dans l'énoncé vérifie $MX = 0$, avec X non nul ; donc la matrice n'est pas la matrice d'une bijection, donc son déterminant est nul.

• Supposons maintenant qu'il existe X tel que MX soit nul et X soit $\neq 0$. Alors, il existe P et Q vérifiant $PT = QS$, avec $deg\ T = deg\ Q - deg\ R$ et $deg\ S = deg\ P - deg\ R$.

- Supposons alors que P et Q n'aient pas de facteur irréductible en commun. Alors, par le lemme de Gauss 143, P divise S, ce qui est impossible car $deg\ S < deg\ P$.□

En particulier, si les polynômes sont scindés, ils ont une racine commune si et seulement si leur résultant est nul. Si P est scindé, son discriminant est nul si et seulement

si il admet une racine double.

5.5.4 Division suivant les puissances croissantes

Théorème 196 (Division suivant les puissances croissantes) *Soit $n \in \mathbb{N}$, C et D des polynômes à une indéterminée sur un même anneau A commutatif et unitaire.*
On suppose que $D(0)$ (en tant qu'élément de A), est inversible.
Alors il existe deux polynômes Q et R vérifiant

$$C = DQ + X^{n+1}R$$
$$\deg Q \leq n$$

Q et R sont appelés respectivement **quotient et reste de la division suivant les puissances croissantes de C par D à l'ordre n.**

Démonstration : La preuve se fait par récurrence inverse sur la valuation de C. Si cette valuation est supérieure ou égale à $n+1$, le résultat est clair. La suite est facile...□

Cela servira notamment pour les développements limités de quotients (voir proposition **??**, ou pour la décomposition de fractions rationnelles en éléments simples (voir proposition ....).

Voyons un exemple concret, la division suivant les puissances croissantes de $X^3 + 2X^2 + 2$ par $X + 2$:

$$\begin{array}{rr|l} & X^3+2X^2+2 & X+2 \\ \cline{3-3} - & X+2 & 1 \\ \cline{2-2} & X^3+2X^2-X & \end{array}$$

Donc $X^3 + 2X^2 + 2 = (X + 2)(1) + (X^2 + 2X - 1)X$, c'est la division suivant les puissances croissantes à l'ordre 0. Continuons :

$$\begin{array}{rr|l} & X^3+2X^2+2 & X+2 \\ \cline{3-3} - & X+2 & 1-\frac{X}{2} \\ \cline{2-2} & X^3+2X^2-X & \\ - & -\frac{X^2}{2}-X & \\ \cline{2-2} & X^3+\frac{5}{2}X^2 & \end{array}$$

Donc $X^3 + 2X^2 + 2 = (X + 2)(1 - \frac{X}{2}) + (X + \frac{5}{2})X^2$, c'est la division suivant les puissances croissantes à l'ordre 1. Continuons encore :

$$\begin{array}{rr|l} & X^3+2X^2+2 & X+2 \\ \cline{3-3} - & X+2 & 1-\frac{X}{2}+\frac{5}{4}X^2 \\ \cline{2-2} & X^3+2X^2-X & \\ - & -\frac{X^2}{2}-X & \\ \cline{2-2} & X^3+\frac{5}{2}X^2 & \\ - & \frac{5}{4}X^3+\frac{5}{2}X^2 & \\ \cline{2-2} & -\frac{1}{4}X^3 & \end{array}$$

Donc, division suivant les puissances croissantes à l'ordre 2, $X^3+2X^2+2=(X+2)(1-\frac{X}{2}+\frac{5}{4}X^2)-\frac{1}{4}X^3$.

5.5.5 Polynômes orthogonaux

Définition 197 *On suppose donné $(a,b)\in\overline{\mathbb{R}}^2$, $a<b$. On suppose donnée une fonction w de $]a,b[$ dans $\mathbb{R}_+^*$ continue. Enfin on suppose que pour tout n, $\int_a^b x^n w(x)dx$ est convergente [a]. On note alors E l'ensemble des fonctions de $]a,b[$ dans $\mathbb{R}$ telles que*

$$\|f\|_2 := \sqrt{\int_a^b |f(x)|^2 w(x)dx} < \infty$$

L'ensemble des polynômes est inclus dans E, E muni du produit scalaire suivant :

$$< f,g >= \int_a^b f(x)g(x)w(x)dx$$

est un espace de Hilbert.
Il existe alors une suite de polynômes $(P_n)_{n\in\mathbb{N}}$, telle que $degP_n=n$, et telle que les P_n forment une famille orthogonale.

[a] Un cas classique est $(a,b)\in\mathbb{R}^2$ et $w=1$, ou bien a et b quelconques et $w(x)=e^{-x^2}$.

Démonstration : Le résultat découle simplement de l'orthogonalisation de Schmidt (proposition **??**) appliquée à $1,X,X^2,X^3,....$ Le fait que le degré de P_n est $\leq n$ provient simplement des propriétés de l'orthogonalisation de Schmidt, ie le fait que P_n appartient à l'espace engendré par $1,X,...,X^n$. Le fait que ce degré est $\geq n$ provient simplement du fait que s'il existait un P_n de degré $<n$, alors la famille $P_0,...,P_n$ serait une famille libre (puisqu'orthogonale) et située dans un espace de dimension n ; ce qui contredit le lemme de Steinitz **??**.

Les polynômes orthogonaux ont de multiples applications, que l'on pourra trouver par exemple dans le livre [9].

On pourra consulter l'exemple Maple qui se trouve suite à l'orthogonalisation de Schmidt (voir proposition **??**).

5.5.6 Polynômes de Tchebycheff de première espèce

Théorème 198

$$\forall n\in\mathbb{N}\exists T_n\in\mathbb{R}[X]/\deg\ T_n\leq n\wedge\forall t\cos(nt)=T_n(cos(t))$$

T_n est appelé **polynôme de Tchebycheff de permière espèce**.

Démonstration :
• Soit $n\in N$. On a

$$e^{inx} = \cos(nx) + i\sin(nx) = (\cos(x) + i\sin(x))^n = \sum_{k=0}^{n} C_n^k \cos(x)^{n_k} \sin(x)^k (i)^k$$

• En prenant les parties réelles :

$$cos(nx) = \sum_{k=0}^{k\leq n/2} C_n^{2k} cos(x)^{n-2k}(-1)^k(1-cos(x)^2)^k$$

D'où le résultat.□

Proposition 199

$$T_n = 2^{n-1}\pi_{k=0}^{n-1}(X - \cos(\frac{2k+1}{2n}\pi))$$

Démonstration : Il suffit de vérifier que le coefficient dominant est le bon, que le degré est le bon, et que les $\cos(\frac{2k+1}{2n}\pi)$ sont bien des racines.□

5.5.7 Tout polynôme positif est somme de deux carrés

Théorème 200 *Soit P un polynôme appartenant à $\mathbb{R}[X]$.*
On suppose en outre que P est positif sur $\mathbb{R}$.
Alors P est somme de deux carrés.

Démonstration : • Soit $Cool$ l'ensemble des polynômes qui s'expriment comme somme de deux carrés.

• Alors $Cool$ contient tous les polynômes de la forme $(x-a)^n$, pour n pair.

• Tout polynôme irréductible unitaire de degré 2 est dans $Cool$. En effet, $X^2 + b.X + c$ est égal à $(X - \frac{b}{2})^2 + (c - \frac{b^2}{4})$, qui est bien une somme de deux carrés si $c - \frac{b^2}{4}$

• Du coup, tout polynôme irréductible de degré 2 à coefficient dominant > 0 est dans $Cool$.

• Si P et Q sont dans $Cool$, alors PQ est dans $Cool$ ($Cool$ est stable par multiplication). En effet, avec $P = A^2 + B^2$ et $Q = C^2 + D^2$:

$$(A^2 + B^2).(C^2 + D^2) = (AD + BC)^2 + (AC - BD)^2$$

• $Cool$ contient les polynômes positifs dépourvus de racine. En effet, soit P sans racine ; il est produit de polynômes irréductibles. Le coefficient dominant est positif, au vu de l'équivalent en $\pm\infty$, donc on peut l'exprimer comme produit de polynômes irréductibles de degré 2 à coefficients dominants positifs.

• Soit P un polynôme positif. On a déjà vu que s'il n'admet pas de racine il est dans $Cool$. On suppose maintenant qu'il admet des racines, par exemple une racine a. Soit n maximal tel que $(X-a)^n$ divise P. $P = (X-a)^n Q$ est équivalent en a à $Q(a)(X-a)^n$; donc n doit être pair pour que le signe de P puisse être positif. En supposant par récurrence que pour les degrés inférieurs à celui de P le résultat est acquis, on conclut que Q et $X - a$ sont dans $Cool$, et donc que P est dans $Cool$.□

Chapitre 6

Polynômes à plusieurs indéterminées

Cette partie sera délibérément très peu détaillée ; beaucoup de démonstrations sont calquées sur le cas des polynômes à une indéterminée. Ceux qui préfèrent un cadre simple et utile peuvent se limiter à la partie5, ou l'on travaillera avec des polynômes à une seule indéterminée, et fournissant les méthodes permettant de s'attaquer à cette partie plus abstraite.

Cette partie doit être complètée par la partie5, qui par contre peut être lue indépendamment de celle-ci.

6.1 Généralités

Définition 201 *Soit A un anneau commutatif unitaire.*
On appelle **polynôme à n indéterminées à coefficients dans** *A l'ensemble des applications presques nulles de $\mathbb{N}^n$ dans A. On note $A[X_1, \ldots, X_n]$ l'ensemble des polynômes à n indéterminées à coefficients dans A.*
On dit que $P \in \mathbb{K}[X_1, \ldots, X_n]$ est **de degré** *d si d est le max des $|\nu|$ tels que P_ν est non nul (voir définition* **??** *pour les rappels sur les opérations dans $\mathbb{N}^n$).*
On dit que P est de degré d en X_i si le $\sup$ des i tels qu'il existe ν tel que ν_i est non nul est d.
On note X_i l'élément de $A[X_1, \ldots, X_n]$ nul partout sauf en $\nu = (\delta_{i,j})_{j\in[1,n]}$, avec $X_\nu = 1$.
Etant donnés P et Q deux polynômes, on note $R = P \times Q$ le **produit de P et** *Q avec*

$$R_\nu = \sum_{\alpha+\beta=\nu} P_\alpha Q_\beta$$

(pour les opérations dans N^n, voir définition **??***).*
On appelle **monôme** *un polynôme dont un seul élément est non nul.*
On appelle **dérivé formel** *d'un polynôme P par D^ν pour $\nu \in \mathbb{N}^n$ le polynôme*

$$\sum_{\alpha\in\mathbb{N}^n} \frac{(\nu+\alpha)!}{\alpha!} P_{\alpha+\nu}$$

On note parfois $\frac{\delta}{\delta X_i}$ D^ν avec $\nu_j = (\delta_{i,j})_{j\in[1,n]}$.

Proposition 202 *On identifie $A[X_1, \ldots, X_n]$ à $A[X_1, \ldots, X_{n-1}][X_n]$, ainsi que $A[X_1, \ldots, X_p][X_{p+1}, \ldots, X_n]$ à $A[X_1, \ldots, X_n]$.*
$A[X_1, \ldots, X_n]$ est intègre si et seulement si A est intègre.
$A[X_1, \ldots, X_n]$ est muni naturellement d'une structure de A-module. Muni de la multiplication définie plus haut, il s'agit d'une A-algèbre.
L'ensemble des monômes unitaires est une base de $A[X_1, \ldots, X_n]$.
Etant donnée B une A-algèbre associative commutative unitaire, $P \in A[X_1, \ldots, X_n]$ et $x_1, ..., x_n$ n éléments de B, on appelle **valeur de P en** *$(x_1, \ldots, x_n)$ l'élément de B $\sum_{\nu\in\mathbb{N}^n} P_\nu x_1^{\nu_1} x_2^{\nu_2} \ldots x_n^{\nu_n}$. On note cet élément $\tilde{P}(x_1, \ldots, x_n)$. On constate ainsi qu'un polynôme P s'identifie naturellement à une application $\tilde{P}$ de B^n dans B. On note $A[x_1, \ldots, x_n]$ l'ensemble des $P(x_1, \ldots, x_n)$ pour $P \in A[x_1, \ldots, x_n]$.*
Si $(x_1, \ldots, x_n)$ vérifie $\tilde{P}(x_1, \ldots, x_n) = 0$, on dit que $(x_1, \ldots, x_n)$ est un zéro de P.
Etant donné $(x_1, \ldots, x_n)$ n éléments de B, l'ensemble des polynômes P vérifiant $P(x_1, \ldots, x_n) = 0$ est un idéal de $A[X_1, \ldots, X_n]$, engendré par les $(X_i - a_i)$ pour $i \in [1, n]$.

6.2 Si A est un corps $\mathbb{K}$

Proposition 203 *Si $\mathbb{K}$ est un corps, $\mathbb{K}[X_1, \ldots, X_n]$ est naturellement muni d'une structure de $\mathbb{K}$-espace vectoriel .*
Formule de Taylor, si $\mathbb{K}$ est un corps de caractéristique nulle : soit $P \in \mathbb{K}[X]$, alors

$$P = \sum_{\nu \in \mathbb{N}^n} \frac{1}{\nu!}(D^\nu P)(0) X^\nu$$

6.3 Zoologie des polynômes à plusieurs indéterminées

6.3.1 Polynômes symétriques

⚠ A est supposé ici anneau commutatif et unitaire.

Définition 204 *Soit $P \in A[X_1, \ldots, X_n]$. P est dit* **polynôme symétrique** *si et seulement si pour tout σ permutation de $[1, ..., n]$, $P(X_1, ..., X_n) = P(X_{\sigma(1)}, X_{\sigma(2)}, ..., X_{\sigma(n)})$.*
On appelle **polynômes symétriques élémentaires** *les polynômes de la forme*

$$\Sigma_{k,n} = \sum_{1 \leq a_1 \leq a_2 \leq \ldots \leq a_k \leq n} X_{a_1} X_{a_2} ... X_{a_k}$$

pour $1 \leq k \leq n$.
*On appelle k-***ième polynôme de Newton** *le polynôme $N_k = \sum_{i=1}^n X_i^k$.*

Les polynômes symétriques élémentaires sont de la forme suivante, dans le cas $n = 3$:

$$\Sigma_{1,3} = X_1 + X_2 + X_3$$
$$\Sigma_{2,3} = X_1X_2 + X_2X_3 + X_1X_3$$
$$\Sigma_{3,3} = X_1X_2X_3$$

Je ne donnerai pas ici de preuve des résultats énoncés ; on pourra se référer à [19]. On a les propriétés suivantes :

• Les polynômes symétriques élémentaires sont symétriques (évident)

• Les polynômes de Newton sont symétriques (évident)

• Si Q est un polynôme, alors $P = Q(\Sigma_{1,n}, \Sigma_{2,n}, ..., \Sigma_{n,n})$ est un polynôme symétrique (facile)

• Si $P \in A[X_1, ..., X_n]$ est symétrique, alors il existe un polynôme Q tel que $P = Q(\Sigma_{1,n}, \Sigma_{2,n}, ..., \Sigma_{n,n})$ (pas évident du tout, récurrence sur le nombre d'indéterminées et sur le degré du polynôme.

• **Relations de Newton** : Si $1 \leq k \leq n$ on a

$$N_k = \sum_{i=1}^{k-1} (-1)^i N_{k-i} \Sigma_{i,n} + (-1)^k k \Sigma(k, n)$$

Si $n \leq k$ on a

$$N_k = \sum_{i=1}^{n} (-1)^i N_{k-i} \Sigma_{i,n}$$

Bibliographie

[1] P. BARBE, M. LEDOUX, *Probabilité*, BELIN, 1998.

[2] H. BRÉZIS, *Analyse fonctionnelle*, MASSON, 1983.

[3] H. CARTAN, *Calcul différentiel*, FLEMMARD.

[4] A. CHAMBERT-LOIR, S. FERMIGIER, V. MAILLOT, *Exercices de mathématiques pour l'agrégation, Analyse 1*, MASSON, 1997.

[5] A. CHAMBERT-LOIR, S. FERMIGIER, *Exercices de mathématiques pour l'agrégation, Analyse 2*, MASSON, 1995.

[6] A. CHAMBERT-LOIR, S. FERMIGIER, *Exercices de mathématiques pour l'agrégation, Analyse 3*, MASSON, 1996.

[7] P.G. CIARLET, *Introduction à l'analyse numérique matricielle et à l'optimisation*, DUNOD, 1998.

[8] F. COMBES *Algèbre et géométrie*, BRÉAL, 1998. <

[9] J.-P. DEMAILLY, *Analyse numérique et équations différentielles*, PRESSES UNIVERSITAIRES DE GRENOBLE, 1996.

[10] W. GIORGI, *Thèmes mathématiques pour l'agrégation*, MASSON, 1998.

[11] A. GRAMAIN, *Intégration*, HERMANN 1988, PARIS.

[12] J.-L. KRIVINE, *Introduction to axiomatic set theory*, D. REIDEL PUBLISHING COMPANY, DORDRECHT-HOLLAND.

[13] S. LANG, *Real analysis*, ADDISON-WESLEY PUBLISHING COMPANY, 1969.

[14] D. PERRIN, *Cours d'algèbre*, ELLIPSES 1996.

[15] A. POMMELLET, *Cours d'analyse*, ELLIPSES 1994.

[16] W. RUDIN, *Analyse réelle et complexe*, MASSON 1992.

[17] R. SMULLYAN, *Théorie de la récursion pour la métamathématique*, FLEMMARD.

[18] Y.G. SINAI *Probability theory - An introduction course*, SPRINGER TEXTBOOK, 1992.

[19] P. TAUVEL, *Mathématiques générales pour l'agrégation*, MASSON, 1997.

[20] J. VAUTHIER, J.J. PRAT, *Cours d'analyse mathématiques de l'intégration*, MASSON, 1994.

[21] D. WILLIAMS, *Probability with martingales*, CAMBRIDGE UNIVERSITY PRESS, 1991.

[22] C. ZUILY, H. QUEFFÉLEC, *Eléments d'analyse pour l'intégration*, MASSON, 1995.