Cours de mathématiques

TOME IV

ALGÈBRE GÉNÉRALE

Mathématiques générales

France $\sim$ 2024

Écrit et réalisé par Louis Lascaud

Chapitre 1

Structures algébriques

Résumé

Les considérations sur les groupes, les anneaux, les corps, les espaces vectoriels, les modules... étant reléguées à des chapitres/tomes distincts, nous nous intéressons à trois choses en particulier : les structures très faibles (magmas, magmas associatifs, demi-groupes), la structure de monoïde et la question des mots, et nous continuons les développements sur les quotients maintenant dans le monde algébrique.

1.1 Magmas

Quelques petits rappels terminologiques pour la fluidité du discours qui suit.

Définition. ***(Magma)***

Un *magma* est un ensemble muni d'une loi de composition interne.

Définition. ***(Magma associatif)***

Un *magma associatif* $(E, \star)$ est un magma dont la loi de composition est associative, c'est-à-dire vérifie :

$$\forall a,b,c \in E \quad (a \star b) \star c = a \star (b \star c).$$

Autrement dit, on peut supprimer les parenthèses pour l'opération.

Propriété. ***(Associativité des puissances)***

Tout magma associatif est associatif des puissances, *i.e.*

$$\forall a \in E \quad a \star (a \star a) = a \star (a \star a),$$

ce qui n'a rien d'immédiat.

Exercice 1

Combien y a-t-il a priori de façons de parenthéser un produit à n facteurs dans un magma non associatif (on ne demande pas de preuve) ? Réaliser ce maximum dans un magma simple.

Définition. ***(Magma commutatif)***

Un *magma commutatif* est un magma dont la loi de composition est commutative, c'est-à-dire vérifie :

$$\forall a,b \in E \quad a \star b = b \star a \ .$$

Autrement dit, l'ordre n'a pas d'importance pour l'opération.

Propriété. ***(Commutativité généralisée)***

Soit E un magma commutatif. Soient $n \in \mathbb{N}$ et $a_1,...,a_n \in E$. Soit $\sigma \in \mathfrak{S}_n$. Alors

$$\sum_{i=1}^{n} a_{\sigma(i)} = \sum_{i=1}^{n} a_i.$$

Définition. ***(Magma unifère (latéral))***

Un *magma unifère* est un magma admettant un élément neutre. Un *magma unifère à gauche* est un magma admettant un élément neutre à gauche. Un *magma unifère à droite* est un magma admettant un élément neutre à droite.

Définition. ***(Élément absorbant (latéral))***

Dans un magma unifère (à gauche), un *élément absorbant (à gauche)* est un élément dont le produit (à gauche) avec un élément quelconque vaut toujours le neutre.

Exercice 2

1. Montrer qu'un élément neutre d'un magma unifère est unique.
2. Un magma peut-il être unifère à gauche et à droite mais pour deux éléments neutres distincts ?
3. Que dire pour un élément absorbant ?

Définition. ***(Inverse (latéral))***

Dans un magma unifère (latéral), un *inverse (à gauche)* d'un élément est un élément dont le produit (à gauche) avec cet élément vaut toujours le neutre.

Remarque. On peut également définir des éléments absorbants ou des inverses à droite, même si le magma est unifère est gauche.

Exercice 3

1. Montrer que les inverses dans un magma unifère sont uniques pour un élément fixé.
2. Peut-on trouver plusieurs inverses à droite dans un magma unifère ?
3. Donner un exemple d'inverse seulement à droite dans un magma unifère seulement à gauche.
4. Peut-on trouver à la fois plusieurs inverses à droite et plusieurs inverses à gauche dans un magma unifère, qui soient distincts les uns les autres ? Et dans un magma unifère à gauche et à droite d'éléments neutres distincts (voir exercice précédent) ?

1.2 Monoïdes

Définition. ***(Monoïde)***

Un *monoïde* est un magma unifère associatif.

Exercice 4

Un *demi-groupe* est un magma associatif. Donner des exemples de demi-groupes et de monoïdes non simplifiables à gauche.

Exercice 5

(Axiomes faibles du groupe) Soit un magma unifère à gauche (resp. à droite) tel que tout élément admette au moins un inverse à gauche (resp. à droite). Montrer que c'est un groupe.

1.3 Structures algébriques quotients élémentaires

Principe. ***(Théorème fondamental de l'algèbre)***

Je peux quotienter (souvent)[a].

[a] Même pas zéro. Même si ça ne sert à rien.

On introduit maintenant les mêmes concepts que précédemment, avec la notion algébrique de loi en supplément. On se rend compte que cela ne change rien aux résultats, et qu'ils sont très stables même compte tenu de l'absence de structure élaborée pour les espaces considérés. Tout d'abord, une équivalence peu utile en pratique mais structurellement fondamentale.

Propriété. ***(Compatibilité d'une loi à une relation et morphisme projection)***

Soit $(E,*)$ un magma qui soit également de façon sous-jacente un ensemble muni d'une relation d'équivalence $\mathcal{R}$. Alors $*$ est compatible avec $\mathcal{R}$ (*i.e.* pour tous éléments x,y,x',$y' \in E, (x \sim x' \text{ ET } y \sim y') \implies x*y \sim x'*y'$) si et seulement s'il existe une unique loi dite *loi quotient* notée ici $\diamond$ telle que π soit un morphisme de $(E,*)$ dans $(E/\mathcal{R},\diamond)$.

▷ On va plus rapidement que pour le théorème de factorisation, puisque les arguments sont les mêmes. D'une part, si la loi $*$ est compatible, alors pour analyse, on doit poser pour tous x,$y \in E$ $\overline{x} \diamond \overline{y} = \overline{x*y}$ (expression de ce que π soit morphisme), ce qui est licite par compatibilité même de la loi pour la relation d'équivalence et définit de manière unique $\diamond$ sur $E/\mathcal{R}$. La synthèse est immédiate comme précédemment. Réciproquement, s'il existe (une unique) loi quotient qui rende la projection π un morphisme, alors si l'on prend dans E $x \sim x'$ et $y \sim y'$ quatre éléments, on a $\pi(x) = \pi(x')$ et $\pi(y) = \pi(y')$ par définition de la projection canonique puis $\pi(x*y) = \pi(x) \diamond \pi(y) = \pi(x') \diamond \pi(y') = \pi(x'*y')$, les première et dernière égalité étant la propriété hypothétique de morphisme. Ainsi $x*y \sim x'*y'$, donc $*$ est compatible avec $\mathcal{R}$ par définition. ■

VOC On dit aussi que la relation compatible est une *congruence*.

Exercice 6

Que connaissez-vous comme famille dénombrable de relations compatibles avec les deux lois de l'anneau $\mathbb{Z}$?

Heuristique

Il faut tenter de ne pas mettre au même ordre cette propriété avec celle du théorème de factorisation, mais plutôt avec la définition de la projection canonique, quoiqu'elle ne soit pas théorème de son côté.

On précise la notion de compatibilité par une subtilité qui ne sera utile que dans la section suivante.

Définition. ***(Compatibilité à gauche, à droite d'une loi à une relation)***

Soit $(E,*)$ un magma qui soit également de façon sous-jacente un ensemble muni d'une relation d'équivalence $\mathcal{R}$. On dit que $*$ est *compatible à gauche* avec $\mathcal{R}$ si pour tous éléments x,y,$y' \in E, y \sim y' \implies x*y \sim x*y'$. On définit de même la compatibilité à droite.

Propriété. ***(Compatibilité et compatibilité latérale)***

Une loi est compatible avec une relation d'équivalence si et seulement si elle est compatible à gauche et à droite avec cette relation.

▷ Ce n'est pas aussi évident que certaines choses... D'abord, il est clair qu'une relation compatible est latéralement compatible, par réflexivité : si $x \sim x'$, $y \sim y$ donc la compatibilité donne $x * y \sim x' \sim y$, de même à gauche. Réciproquement, supposons que la relation soit compatible à gauche et compatible à droite. Soient $x \sim x'$ et $y \sim y'$ quatre éléments de E. Alors par compatibilité à gauche, $x * y \sim x' * y$ et par compatibilité à droite, $x' * y \sim x' * y'$. Par transitivité, on a $x * y \sim x' * y'$. ■

Remarque. Dans le cas d'une loi de magma commutative, ces compatibilité latérales partielles sont équivalentes et donc équivalentes chacune à la compatibilité tout court, ce qui permet d'affaiblir légèrement les hypothèses.

Exercice 7

Soit $\equiv$ une relation d'équivalence sur $\mathbb{M}$. On suppose que $(\mathbb{M}, \cdot\ )$ est un magma et que la relation est compatible avec la loi interne (où seulement compatible à gauche, voir ce qui précède).

1. Démontrer que, pour tous $x \equiv y$ dans $\mathbb{M}$, pour tout $n \in \mathbb{N}$, $x^n \equiv y^n$.
2. On suppose ce magma unifère à gauche. Soient x,y deux éléments équivalents admettant des inverses à gauche. Montrer que $-x \equiv -y$.
3. *(Peu utile)* Que dire de cette dernière propriété si la loi n'avait été que compatible à droite ?

Propriété. ***(Héritage des lois quotients)***

Si la loi de base a pour propriétés ou éléments caractéristiques les suivants, la loi quotient également, et dans ce dernier cas pour les classes de ces éléments :

- l'associativité ;
- la commutativité ;
- les éléments neutres (latéraux) ;
- les éléments absorbants (latéraux) ;
- les inverses (latéraux) ;
- en présence d'un magmas muni de deux lois dont l'une est distributive par rapport à l'autre, la distributivité ;
- le quotient d'un monoïde est un monoïde, d'un groupe, d'un anneau est un monoïde, un groupe, un anneau, d'un corps, d'une algèbre, est un anneau, un corps, une algèbre.

▷ En faire quelques-uns soi-même est un bon exercice de clarté mentale. ■

La régularité seule n'est pas conservée dans la loi quotient. Par exemple, si 2 est bien régulier dans $(\mathbb{Z}, \times)$, il ne l'est plus dans $(\mathbb{Z}/4\mathbb{Z}, \times)$ muni de la loi quotient, que l'on note de la même manière abusivement.

La dernière propriété et la relativement grande stabilité des quotients algébriques semble de loin terminer la théorie des espaces quotients. C'est vrai, en ce sens qu'elle la permet ; mais les sections suivantes vont préciser la nature des relations d'équivalence compatibles pour les lois algébriques : modulo un sous-groupe distingué pour les groupes, pour un idéal dans un anneau unitaire, par exemple.

Semblablement à la section précédente, on peut représenter les théorèmes par des diagrammes commutatifs, en précisant profitablement les lois impliquées.

$$\begin{array}{ccc} (E,*) & & \\ \downarrow{\scriptstyle \pi} & & \\ (E/\mathcal{R},\overline{*}) & & \end{array}$$

Des diagrammes comme thème universel

En 1942, dans leur essai *General theory of natural equivalences*, les chercheurs Samuel Eilenberg and Saunders MacLane introduisent les notions de catégorie, de foncteur, de transformation naturelle dans le cadre de leurs travaux en topologie algébrique. Ces constructions étaient la suite logique de celle de sa professeur Emmy Noether, notamment connue pour ses travaux en algèbre abstraite (les anneaux noethériens portent son nom). Le mathématicien Stanislaw Ulam écrit que de telles idées germaient déjà en Pologne dans les années num1930. Il semble, plus généralement, que la formalisation de la théorie des catégories ait été en partie une réaction aux vacillations de la théorie des ensembles à cette époque, quoiqu'elle ait davantage servie à justifier une assise globale des domaines mathématiques qu'à leurs résolutions.

Maintenant, on énonce le parallèle du théorème de factorisation, non plus seulement pour les applications, mais pour les morphismes de magmas, définis exactement de la même manière que les morphismes de groupe du cours. Pour fixer les notations, $(E,*)$ est un magma qui soit également de façon sous-jacente un ensemble muni d'une relation d'équivalence $\mathcal{R}$; on suppose que la loi est compatible avec la relation (sinon, on ne peut rien faire comme on l'a vu) et que la loi quotient est notée $\overline{*}$. On introduit également un autre magma quelconque $(F,\diamond)$.

Théorème. ***(Théorème de factorisation pour les morphismes)***

Soit f un **morphisme** de E dans F. Alors f est compatible **avec** $\mathcal{R}$ au même sens que dans la section ensembliste si et seulement s'il existe un unique **morphisme** $\tilde{f}$ tel que $f = \tilde{f} \circ \pi$ (se qui se réécrit $f(x) = \tilde{f}(\overline{x})$ pour tout $x \in E$). Dans ce cas de compatibilité,

on dit toujours qu'on *passe au quotient* dans le morphisme f.

▷ Par rapport au théorème de factorisation pour les applications, il suffit de vérifier que l'application quotient est un morphisme et on établit les connexions logiques annoncées automatiquement avec ce seul annexe. Or : $\tilde{f}(\overline{x}*\overline{y}) = \tilde{f}(\overline{x*y}) = f(x*y) = f(x) \diamond f(y) = \tilde{f}(\overline{x}) \diamond \tilde{f}(\overline{y})$. ■

Exercice 8

(Une formulation plus faible des théorèmes de factorisation) Vérifier que l'énoncé précédent reste vrai si l'on remplace *morphisme* par simplement *application*.

Remarque. Ne mélangeons pas tout. Il faut prendre garde par exemple à ne pas confondre compatibilité de l'application avec la relation sur l'espace de départ et celle de la loi de l'espace de départ avec cette relation également.

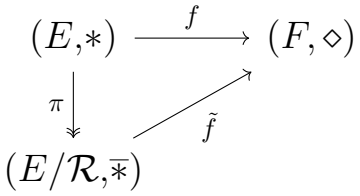
Méthode. ***(Recette pour passer au quotient dans les morphismes)***

J'ai un morphisme φ d'une structure quotient Q dans F une même structure quelconque.

1. J'identifie la relation d'équivalence qui quotiente : $Q = E/\mathcal{R}$ et E la structure initiale.
2. Je vérifie que $\mathcal{R}$ est une relation d'équivalence pour justifier mon propos.
3. **Je vérifie que la loi de E structuré est compatible avec $\mathcal{R}$.**
4. e pose un morphisme f de E dans F définie sans aucun problème et qui devra, une fois passée au quotient, retomber sur φ.
5. Je montre que pour tous éléments x,y de E, si $x\mathcal{R}y$, alors $f(x)$ et $f(y)$ sont égaux.
6. Je peux maintenant définir un morphisme $\varphi = \tilde{f} : Q \longrightarrow F$ sans trouble, telle que pour tout $\overline{x} \in Q$, $\tilde{f}(\overline{x}) = f(x)$, et j'insiste bien sur ce que cette construction n'est possible que grâce aux deux compatibilités vérifiées précédemment.

Si je veux une propriété d'injectivité, de surjectivité, voire de bijectivité pour mon application, je me réfère au résultat de l'exercice déjà étudié..

Voilà le diagramme correspond à ce nouveau théorème de factorisation dans sa version algébrique. Par rapport au précédent, on précise les lois pour garder les idées claires. Par contre, on ne précise pas que les flèches sont toutes des morphismes de magmas, ce qui est automatique lorsqu'on se donne de tracer de tels diagrammes. Ceux-ci prennent essor dans la théorie des catégories : dans la catégorie des ensembles, où les objets sont les ensembles, les flèches sont tout simplement les applications ; dans la catégorie des magmas, où les objets sont les magmas, les flèches sont les morphismes de magmas.



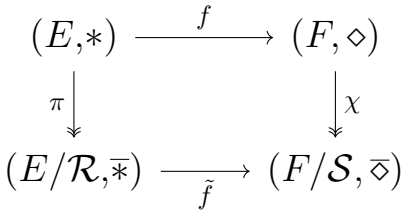
Le théorème de factorisation pour les morphismes établit à son tour la commutation de ce diagramme. Notons par surcroît que les caractérisations de monomorphisme, épimorphisme, isomorphisme (morphismes injectifs, surjectifs, bijectifs), sont les mêmes que dans l'exercice sur ce sujet de la section précédente ; de même pour le théorème qui suit.

De la même manière, on dispose d'un théorème carré corollaire, encore moins excitant que le premier. Là, le magma d'arrivée du morphisme $(F,\diamond)$ est muni de façon sous-jacente d'une relation d'équivalence $\mathcal{S}$ que l'on note aussi $\equiv$, ses classes $\widehat{\cdot}$, compatible avec la loi de magma et l'on note χ le morphisme projection canonique.

Théorème. ***(Théorème de factorisation carré pour les morphismes)***

Soit f un morphisme de E dans F. Alors f est compatible avec $\mathcal{R}$ au même sens que dans la section ensembliste si et seulement s'il existe un unique morphisme $\tilde{f}$ tel que $\chi \circ f = \tilde{f} \circ \pi$ (se qui se réécrit $f\hat{(}x) = \tilde{f}(\overline{x})$ pour tout $x \in E$). Dans le cas de compatibilité, on dit encore qu'on passe au quotient dans f.

▷ C'est tout simplement la conjonction du théorème carré de factorisation pour les applications et du théorème de factorisation pour les morphismes. ■



Le diagramme illustratif est similaire a ce qui a déjà été vu.

Exemple fondamental

Soient n, m deux entiers premiers entre eux et l'application

$$\begin{array}{rccc} f : & \mathbb{Z}/nm\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ & \overline{k}_{\equiv nm} & \longmapsto & (\overline{k}_{\equiv n}, \overline{k}_{\equiv m}). \end{array}$$

On vérifie que c'est une bijection : en effet, par cardinalité, il suffit de montrer l'injectivité qui découle de la primalité relative de n et m. En réalité, nous devons montrer d'abord que f est bien définie, ce qui découle de la compatibilité de f avec la congruence modulo mn : en effet, si $k \equiv k' \ [nm]$, $k = k' + qnm$ donc $k \equiv k' \ [n]$ et $k \equiv k' \ [m]$ ce qui donne le même couple $f(k) = f(k') = (\overline{k}_{\equiv_n}, \overline{k}_{\equiv_m}) = (\overline{k'}_{\equiv_n}, \overline{k'}_{\equiv_m})$. De plus, l'application quotient est encore un morphisme donc l'application f est un isomorphisme, ce qui constitue le théorème chinois. Pour titre de compréhension, la relation $\mathcal{S}$ en reprenant les notations précédentes, qui n'intervient pas dans aucune hypothèse, est la relation produit $\equiv_n \times \equiv_m$ sur $\mathbb{Z}^2$ le groupe produit.

On laisse le soin au lecteur de se rendre compte à partir de la définition pourquoi le produit de deux relations sur un produit cartésien est une relation (*ouf*, murmure le SQL).

Ce n'est pas parce qu'on établit l'existence d'un isomorphisme qu'il faut confondre cet exemple avec le théorème d'isomorphisme qui suit !

Théorème. ***(Théorème d'isomorphisme pour les magmas)***

Soit f une application de $(E,*)$ dans $(F,\diamond)$ deux magmas quelconques. On considère la relation d'équivalence $\mathcal{R}$ sur E définie par $x \sim y \iff f(x) = f(y)$. Dans ce cas, f est compatible avec $\mathcal{R}$, $(\mathrm{Im}(f),\diamond)$ est un magma et l'application quotient de f par cette relation réalise un isomorphisme de $(E/\mathcal{R},\overline{*})$ sur $(\mathrm{Im}(f),\diamond)$.

▷ Il n'y a pas grand-chose à faire. Précisons toutefois pour être rigoureux :

- La compatibilité de l'application f avec la relation d'équivalence des fibres a déjà été établie dans le théorème de bijection quotient. On se rappelle son extrême trivialité.
- Le théorème de bijection quotient établit que l'application quotient est une bijection sur $\mathrm{Im}(f)$.
- La bijection quotient est un morphisme d'après le théorème de factorisation pour les morphismes (de magmas).
- Il faut seulement montrer que $(\mathrm{Im}(f),\diamond)$ est un magma, c'est-à-dire que la partie $\mathrm{Im}(f)$ est stable sous la loi $\diamond$ dont on note la restriction à $\mathrm{Im}(f) \times \mathrm{Im}(f)$ de la même manière abusivement. C'est facile : si $y,y' \in \mathrm{Im}(f)$, $y = f(x)$ et $y' = f(x')$ et f est un morphisme donc $f(x * x') = f(x) \diamond f(x') = y \diamond y' \in \mathrm{Im}(f)$, car $x * x' \in E$, $(E,*)$ étant stable par $*$ en tant que magma.

Ainsi $\tilde{f}$ est un isomorphisme de magmas de $(E/\mathcal{R},\overline{*})$ dans $(\mathrm{Im}(f),\diamond)$. ■

$$\begin{array}{ccc} (E,*) & \xrightarrow{\ f\ } & \mathrm{Im}(f) \\ {\scriptstyle\pi}\downarrow & \nearrow_{\tilde{f}} & \\ (E/\mathcal{R},\overline{*}) & & \end{array}$$

D'après la propriété d'héritage de la structure de monoïde et de groupe, on établit les deux mêmes théorèmes pour des monoïdes et des groupes. Il est en fait un peu moins trivial de les vérifier pour des morphismes de monoïdes, qui sont définis non seulement par la préservation de la loi mais aussi par l'image du neutre qui doit être le neutre d'arrivée, ce qui n'est pas automatique comme dans le cas connu des morphismes de groupe.

Exercice 9

1. Énoncer et justifier ces trois derniers théorèmes pour des groupes.
2. Énoncer et justifier ces trois derniers théorèmes pour des monoïdes.

Principe. ***(Théorèmes de factorisation)***

Le phénomène général est celui-ci : étant donné une structure aussi munie d'une relation d'équivalence, si la structure quotientée est également structurée (compatibilité de la structure avec la relation d'équivalence), alors un morphisme quotient partant de cette structure est compatible avec la relation d'équivalence si et seulement s'il se quotiente en morphisme.

Principe. ***(Théorèmes d'isomorphisme)***

Étant donné une structure, étant donné un morphisme quelconque partant de cette structure, son image, qui a systématiquement la même structure, est isomorphe à la structure quotient par la relation d'équivalence des fibres (sa structuration étant systématique).

Chapitre 2

Théorie élémentaire des groupes

Résumé

Voici une longue partie sur les groupes. Nous nous attardons sur des sujets divers de la théorie élémentaire de cette structure : après quelques considérations amusantes sur les bases, on s'attarde aux théorèmes classiques sur l'arithmétique des groupes, les groupes de symétrie usuels, suivis d'un cours sur les quotients de groupes dont on a choisi qu'il intègre les principaux développements de théorie de groupe classiques de l'Agrégation. On continue avec la théorie des actions, les théorèmes de Sylow, le théorème de Kronecker, la notion de résolution et celle de groupe libre-présentation par gén & rel.

2.1 Définition

2.1.1 Inversion dans un groupe

Voilà une propriété intéressante qui ne permet de vérifier simplement que l'on est en présence d'un inverse.

Propriété. ***(Inverses latéraux dans un groupe)***

Soit G un groupe et $x \in G$. Si y est un inverse à gauche de x, alors c'est l'inverse de x. De même, si y est un inverse à droite de x, alors c'est l'inverse de x.

▷ Si $yx = e$, comme $x^{-1}x = e$, $x^{-1}x = yx$. En inversant à droite par x, on a $y = x^{-1}$. ■

Autrement dit, le phénomène d'inverse latéral est évincé dans un groupe au profit de l'inversibilité générale.

2.2 Groupes abéliens

Propriété. ***(Sous-groupes d'un groupe abélien)***

Les sous-groupes d'un groupe abélien sont abéliens.

2.2.0.1 Théorème 5/8

Lemme. ***(Lemme 1/4)***

Soit G un groupe fini non abélien. Alors $|\mathcal{Z}(G)| \leqslant \frac{|G|}{4}$.

▷ Si $|G : \mathcal{Z}(G)] = 1$, $\mathcal{Z}(G) = G$, exclu. Si $[G : \mathcal{Z}(G)] = 2$, $G/\mathcal{Z}(G) \simeq \mathbb{Z}/2\mathbb{Z}$ cyclique donc G est abélien, exclu. De même si $[G : \mathcal{Z}(G)] = 3$. Ainsi $[G : \mathcal{Z}(G)] \geqslant 4$, d'où le résultat. ■

Théorème. ***(Théorème 5/8)***

Dans un groupe abélien fini, la probabilité que deux éléments commutent est $\leqslant \frac{5}{8}$.

▷ On utilise le lemme et la remarque suivante : si $g \notin \mathcal{Z}(G)$, son centralisateur $C(g)$ est un sous-groupe strict de G, donc $|C(g)| \leqslant \frac{|G|}{2}$ par le théorème de Lagrange.

On cherche à majorer $p(G) \leqslant \frac{1}{|G|^2}\{(g,g') \in G^2 \mid gg' = g'g\}$. On note C cet ensemble. Alors clairement $\mathrm{Com}(A) = \bigcup_{g\in G} \{g\} \times C(g)$. Ainsi, $|\mathrm{Com}(A)| \leqslant \sum_{g\in\mathcal{Z}(G)} |C(g)| + \sum_{g\notin\mathcal{Z}(G)} |G| \leqslant |\mathcal{Z}(G)||G| + (|G| - |\mathcal{Z}(G)|)\frac{|G|}{2} = \frac{|\mathcal{Z}(G)|G||}{2} + \frac{|G|^2}{2}$. Ainsi $p(G) \leqslant \frac{1}{2} + \frac{|\mathcal{Z}(G)|}{2|G|} = \frac{1}{2} + \frac{1}{8} = \frac{5}{8}$. ■

Remarque. Cette borne est atteinte, par exemple dans le groupe diédral d'ordre 8.

2.3 Sous-groupe

2.3.0.1 Sous-groupes triviaux

Définition. ***(Sous-groupe triviaux)***

Soit G un groupe. On appelle :

- *sous-groupe trivial*, tout sous-groupe égal à $\{e\}$ ou G ;
- *sous-groupe nul*, le sous-groupe $\{e\}$;
- *sous-groupe grossier*, le sous-groupe G ;
- *sous-groupe propre*, tout sous-groupe qui n'est pas G.

2.4 Morphisme de groupes

2.4.1 Noyau d'un morphisme

Propriété. ***(Deux éléments ont la même image par un morphisme)***

Soit $f : G \longrightarrow G'$ un morphisme de groupes. Soient $x, y \in G$. Alors $f(x) = f(y)$ si et seulement si $x - y \in \mathrm{Ker}(f)$.

2.4.2 Groupe des automorphismes

Propriété. ***(Automorphismes remarquables d'un groupe abélien)***

Soit G un groupe abélien de cardinal $n \geqslant 3$. Alors $\mathrm{Aut}(G) \neq \{id\}$.
Plus précisément, si n est l'exposant de G et k un entier premier avec l'exposant de G. Alors $x \longmapsto kx$ est un automorphisme de G.

▷ La donnée de cet automorphisme est bien sûr inspirée des automorphismes des groupes cycliques dont on donnera une description exhaustive dans la section consacrée. Avec les notations de l'énoncé, il existe u,v des coefficients de Bézout pour $ku + nv = 1$. Ainsi $x \longmapsto uv$ est une réciproque de l'application proposée. Comme c'est un morphisme de groupes sans problème, on a un automorphisme non trivial si $k \neq 1$.

Remarquons également que pour tout $n \geqslant 3$, il existe un entier inférieur à n, plus grand que 1, premier à n, donné par $n - 1$: si $d \mid n$,$n - 1$, $d \mid n - (n - 1) = 1$. ■

2.5 Ordre d'un élément dans un groupe, génération

2.5.1 Définition et caractérisation

Formellement, étant donné un élément $g \in G$ d'un groupe, l'exponentiation par un entier définit un morphisme ϕ de $\mathbb{Z}$ dans G dont le noyau est un idéal de $\mathbb{Z}$ Ainsi $\mathbb{Z}/\mathrm{Ker}(\phi) \simeq \langle g \rangle$, qui est donc cyclique. Son ordre est l'ordre de ce groupe cyclique ; s'il est d'ordre nul, on dira donc aussi qu'il est d'ordre infini.

2.5.2 Notion de génération

2.5.2.1 Système de générateurs

Remarques.

1. Tout groupe admet un système de générateurs : si G est un groupe, $\{x, x \in G\}$ convient. Cette trivialité se révèle utile dans le cas des groupes abéliens finis par l'écriture :

$$|G| = |\langle x_1 \rangle \dots \langle x_n \rangle|.$$

2.5.2.2 Sous-groupe engendré

Propriété. ***(Sous-groupe engendré par le complémentaire)***

Soient G un groupe et H un sous-groupe strict de G. Alors le sous-groupe engendré par $\complement_G H$ est G tout entier.

▷ On note K le complémentaire de H. Soit $x \in G$. Si $x \in K$, c'est terminé. Sinon, $x \in H$. Or on sait que K est non vide, car H est strict, donc il contient a. On a donc $ax \in K$, car sinon, $axx^{-1} = a \in H$. Or $a^{-1} \in K$, car sinon son inverse $a \in H$. Ainsi, $(a^{-1})(ax) = x \in \langle K \rangle$. Voilà. ■

2.5.3 Théorème de Lagrange et conséquences

Propriété. ***(Majoration des cardinaux d'un sous-groupe)***

Soit G un groupe fini et H un sous-groupe de G. Alors $\text{card}(H) \leqslant \frac{\text{card}(G)}{2}$.

▷ Conséquence de la majoration des diviseurs d'un entier. ■

Remarque. Cette majoration est maximale comme en témoigne le groupe alterné dans le groupe symétrique de n'importe quel ordre $n \geqslant 2$, par exemple $n = 3$.

2.5.3.1 Groupes de cardinaux pairs, impairs

Propriété. ***(Groupe de cardinal impair)***

Dans un groupe fini de cardinal impair, tout élément admet une racine carrée.

▷ Soit G un groupe fini de cardinal $2n+1$. Soit $x \in G$. Alors $x^{2n+1} = 1$, donc $(x^n)^2 = x^{-1}$. Quitte à avoir pris x^{-1}, on a une racine carrée de x. ■

Lemme. ***(Lemme de l'involution)***

Toute involution sur un ensemble de cardinal impair admet au moins un point fixe.

▷ Supposons que f agisse sur E sans point fixe. Soient x_1,...,x_n les éléments de E. Alors $f(x_1) = x_{i_0}$, deux éléments. Prenons le prochain x_i non cité. Alors $f(x_i) = x_{i_1}$ deux éléments, où x_{i_0} n'a pas été cité, car f est une involution, donc deux autres éléments. Ainsi on forme des paires d'éléments de E. À quelque étape que l'on s'arrête, on a un nombre pair d'éléments ; absurde. ■

Propriété. ***(Groupe de cardinal pair)***

Dans un groupe fini de cardinal pair, il existe au moins un élément d'ordre 2.

▷ Découle directement du lemme de l'involution rappelé ci-dessus appliqué à l'inversion sur le groupe $Gprive\,\{e\}$. ■

2.5.4 Théorème de Cauchy

Théorème. ***(Théorème de Cauchy)***

Soit G un groupe fini et p un facteur premier de l'ordre de G. Alors G contient (au moins) un élément d'ordre p, c'est-à-dire, G contient un groupe premier d'ordre p.

On donne trois preuves, deux dans des cas plus ou moins particuliers.

▷ *(Preuve dans le cas $G = 2p$.)* Alors le cardinal de G est pair, donc par le lemme de l'involution, il admet un élément d'ordre 2. Il reste à montrer que G admet un élément d'ordre p. Si ce n'est pas le cas, alors par Lagrange, tous les éléments sont d'ordre 2. C'est un groupe d'exposant 2 : il est donc de cardinal 2^d. Si $d = 2$, $p = 2$ et il n'y a rien à faire. Sinon, absurde. Donc il y a aussi un élément d'ordre p. ■

▷ *(Preuve dans le cas commutatif.)* Soient $x_1,...,x_r$ les éléments de G. Alors clairement $G = \langle x_1\rangle ... \langle x_r\rangle$ donc $|G| = |\langle x_1\rangle ... \langle x_r\rangle|$ divise $\mathrm{ord}(x_1)...\mathrm{ord}(x_r)$ d'après la formule du produit. Si p divise $|G|$, il divise donc ce produit d'ordres. Par lemme d'Euclide, il divise $\mathrm{ord}(x_i)$ pour un certain i. Soit k le diviseur conjugué de p pour $\mathrm{ord}(x_i)$. Alors $(x_i^k)^p = x_i^{\mathrm{ord}(x_i)} = 1$ et x^k est d'ordre $\mathrm{ord}(x_i)$. ■

▷ *(Preuve (McKay) dans le cas général.)* Soit G un groupe de cardinal n et p un diviseur premier de son ordre ; on fait agir (voir la section sur les actions de groupe) $\mathbb{Z}/p\mathbb{Z}$ sur l'ensemble $E = \{(x_1,...,x_p) \in G^p, x_1...x_p = 1\}$. Cet ensemble est de cardinal n^{p-1} : étant donné $(x_1,...,x_{p-1})$ $p-1$-uplet de G, il existe un et un seul $x_p = (x_1...x_{p-1})^{-1}$ tel que $x_1...x_p = 1$. On écrit l'équation aux classes : puisque p divise n, pour un certain q, $pq = \sum_T |O(x)|$ ou, puisque p est premier, une orbite a pour cardinal 1 ou p. Or $(e,...,e)$ a une orbite de cardinal 1. Le nombre d'orbites de cardinal 1 est donc un multiple non nul de p, autrement l'équation donnerait une absurdité de divisibilité. En particulier, il y a au moins un tel élément. Un tel élément est par définition de l'action de la forme $(x,...,x)$ où x est non trivial, et par définition de E, $x^p = 1$. D'où le résultat. ■

Remarque. Il y a donc au moins $p-1$ éléments distincts dans G qui soient d'ordre p, puisque tous les éléments non triviaux d'un groupe premier l'engendrent.

2.5.5 Ordre dans un produit

2.5.6 Propriétés opératoires de l'ordre

Propriété. ***(Ordre d'une image)***

Soit $f : G \longrightarrow G'$ un morphisme de groupes et $x \in G$. Alors $\text{ord}(f(x))$ divise $\text{ord}(x)$.

2.5.6.1 IMPORTANT : ordre d'une puissance

Lemme

Soit G un groupe et a un élément d'ordre n fini. Soit k un entier premier avec n. Alors l'élément a^k est encore d'ordre n.

▷ Reprenons les notations de l'énoncé. Soit p un entier tel que $(a^k)^p = 1$. Alors $a^{kp} = 1$ donc par caractérisation de l'ordre, l'ordre de a, n divise kp. Seulement, n et k sont premiers entre eux donc d'après le théorème de Gauss, n divise p. Ceci vaut pour tout p, donc par caractérisation de l'ordre, n est l'ordre de a^k. ■

Propriété. ***(Ordre d'une puissance)***

Soit G un groupe et a un élément d'ordre n fini. Soit k un entier quelconque. Alors a^k est d'ordre $\frac{n}{n \wedge k}$.

▷ Nous n'utilisons pas le lemme proprement dit, mais l'idée du lemme. Soit p un entier tel que $(a^k)^p = 1$. Alors $a^{kp} = 1$ donc par caractérisation de l'ordre, l'ordre de a, n divise kp. On sait qu'il existe n' et k' deux entiers premiers entre eux tels que $n = (n \wedge k)n'$ et $k = (n \wedge k)k'$, ce qui permet d'écrire $(n \wedge k)n' \mid p(n \wedge k)k'$. Puisqu'un PGCD n'est jamais nul, $n' | pk'$. Mais puisque n' et k' sont premiers entre eux, n' divise p. Puisque ceci vaut pour tout entier p, n' est l'ordre de a^k, et par définition $n' = \frac{n}{n \wedge k}$. ■

Reformulation pratique. ***(Cas additif)***

Dans le cas additif, cela signifie que l'élément ka a pour ordre additif $\frac{n}{n \wedge k}$ ($\frac{n}{n \wedge k} ka = 0$).

Remarque. Il est immédiat, d'après le corollaire du théorème de Lagrange, de vérifier que cette quantité est bien divisée par l'ordre, autrement dit, que c'est une puissance annulatrice de l'élément a^k.

2.5.6.2 Ordre d'un produit

Cette propriété n'est absolument pas généralisable : si x et y ne commutent pas, ce n'est plus vrai ; si les ordres de x et y ne sont pas premiers entre eux, même s'ils commutent, l'ordre du

produit n'est pas le ppcm des ordres. Voici deux contre-exemples illustrant ces faits, intéressants en eux-mêmes.

Propriété. ***(Symétrie de l'ordre)***

Soit G un groupe. Alors $\text{ord}(xy) = \text{ord}(yx)$ pour tous $x,y \in G$.

▷ Soit $k \in \mathbb{Z}$. Alors $(xy)^k = (xy)...(xy) = x(yx)...(yx)y = x(yk)^{k-1}y$. Ainsi $(xy)^k = 1$ si et seulement si $(yk)^{k-1} = x^{-1}y^{-1} = (yx)^{-1}$ soit $(yk)^k = 1$. ■

2.5.6.3 Ordre d'une somme

Propriété. ***(Ordre d'une somme)***

Soit G un groupe. Soient $x,y \in G$ tels que $\text{ord}(x) \wedge \text{ord}(y) = 1$. Alors $\text{ord}(x+y) = \text{ord}(x) \times \text{ord}(y)$.

▷ Remarquons d'abord que si $\langle x \rangle \cap \langle y \rangle = \{0\}$, alors $\text{ord}(x+y) = \text{ppcm}(\text{ord}(x),\text{ord}(y))$. En effet, $k(x+y) = 0$ si et seulement si $kx = -ky$, donc par hypothèse, si et seulement si $kx = ky = 0$.

Il suffit de remarquer que l'hypothèse de la propriété précédente implique la condition donnée ci-dessus. On note $p = \text{ord}(x), q = \text{ord}(y)$. Si $kx \in \langle y \rangle$ où $k \in [\![1,p]\!]$, alors $(qk)x = 0$, donc $p \mid kq$, donc par lemme de Gauss $p \mid k$, donc $kx = 0$. ■

2.5.7 Exposant d'un groupe

Définition. ***(Exposant d'un groupe)***

Soit G un groupe (de torsion). On appelle *exposant* de G, et l'on note $\exp(G)$, le plus grand des ordres des éléments de G, éventuellement infini.
Reformulons. L'exposant est, s'il existe, autrement on dit qu'il est infini, le plus petit entier strictement positif n tel que $\forall g \in G \quad g^n = e$.

Remarque. L'exposant est bien défini dans tout groupe fini où tout élément est d'ordre fini et par convention dans un groupe où un élément à un ordre infini.

Attention ! L'exposant peut être infini dans un groupe infini où tous les éléments sont d'ordre fini, par exemple, l'entonnoir infini $\prod_{n=1}^{\infty} \mathbb{Z}/n\mathbb{Z}$.

Lemme

L'exposant d'un groupe d'exposant fini est le ppcm des ordres de ses éléments.

▷ Soit N l'exposant du groupe G. Il s'agit de montrer que l'ordre de tout élément divise N. Remarquons que N est de torsion. On suppose qu'il existe un élément $x \in G$ d'ordre k qui ne divise pas N. Alors il existe un nombre premier tel que $a = v_p(k) > b = v_p(N)$. On écrit $k = p^a k_0$ et $x = p^b N_0$. Alors $k_0 x$ est d'ordre p^a et $p^b g$ est d'ordre N_0 où g est un élément d'ordre N ; en effet, il y en a un par hypothèse d'absurde. Alors $k_0 x + p^b g$ est d'ordre $p^a N_0$, ce qui est absurde, car on a $p^a N_0 > N$. ■

Exemples. ***(Exposants de groupe)***

1. L'exposant du groupe cyclique $\mathbb{Z}/n\mathbb{Z}$ est clairement n. Ainsi, pour tout $n \in \mathbb{N}$, il existe un groupe fini d'ordre n.
2. L'exposant d'un groupe est invariant par puissance (ne pas se laisser porter par le vocabulaire !). Ainsi, si G est d'exposant r, alors G^d est encore d'exposant r.
3. Le même constant reste vrai pour des exponentiations infinies : ainsi $(\mathbb{Z}/n\mathbb{Z})^{\mathbb{N}}$ est d'exposant n. Par suite, pour tout n, il existe un groupe infini d'exposant n.
4. **Tout groupe d'exposant fini est de torsion.** Attention, comme dit précédemment, la réciproque est fausse.
5. L'exposant de $\mathfrak{A}_3$ est 6, bien que $\mathfrak{A}_3$ n'ait aucun élément d'ordre 6, car $2 \vee 3 = 6$. Ce phénomène n'a plus cours dans les groupes abéliens.

Propriété. ***(Théorème de l'exposant)***

Dans un groupe fini G, tout facteur premier de l'ordre de G divise l'exposant.

▷ Soit $G = \{x_1,...,x_n\}$. Alors $|G|$ divise $|\{x_1\}|...|\{x_n\}|$ d'après la formule du produit, et tout élément a son ordre qui divise l'exposant r de G, donc si p divise $|G|$, p divise r^n, donc p divise r. ■

Propriété. ***(Exposant d'un groupe abélien fini)***

Dans un groupe abélien fini, l'exposant est toujours atteint.

Pour démontrer ce théorème, on aura besoin des deux lemmes suivants.

Lemme

Soient G un groupe et $x,y \in G$ deux éléments qui commutent. Alors $\mathrm{ord}(xy) = \mathrm{ppcm}(\mathrm{ord}(x),\mathrm{ord}(y))$.

Lemme

Soient $a,b \in \mathbb{Z}$. Alors il existe a',b' tels que $a' \mid a$, $b' \mid b$, $a' \wedge b' = 1$ et $a'b' = a \vee b$.

2.6 Groupes monogènes et groupes cycliques

2.6.1 Définition

On énonce deux résultats de propagation de structure, par ailleurs très élémentaires, simplement pour qu'il figure dans cette section par un souci d'exhaustivité.

Propriété. ***(Quotient d'un groupe monogène)***

Tout quotient d'un groupe monogène est monogène.

Propriété. ***(Quotient d'un groupe cyclique)***

Tout quotient d'un groupe cyclique est cyclique.

Pour une preuve, on se référera à la partie sur les quotients de groupe.

On notera également que cette dernière propriété aurait pu être établi, sans moins d'effort, de façon constructive à partir des quotients de $\mathbb{Z}/n\mathbb{Z}$ et du théorème général que nous énonçons dès maintenant.

2.6.2 Théorème de classification

Théorème. ***(Théorème fondamental de classification des groupes monogènes)***

Tout groupe monogène est isomorphe au groupe additif $\mathbb{Z}$ ou à un certain $\mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N}^*$.

Heuristique

Étudier un groupe cyclique revient donc à étudier $\mathbb{Z}/n\mathbb{Z}$, ce qui se ramène inévitablement à des raisonnements arithmétiques. Deuxième exemple d'intervention hégémonique de l'arithmétique dans la théorie des groupes, après le théorème de Lagrange.
On aurait pu se demander pourquoi ne pas considérer à la place des $\mathbb{Z}/n\mathbb{Z}$, les groupes des racines n-ième de l'unité (ce qui aurait eu un avantage, le groupe multiplicatif d'un corps fini étant toujours cyclique, on aurait pu l'identifier à un autre groupe *multiplicatif*).
Ce groupe multiplicatif est en vérité beaucoup moins intuitif au niveau des opérations, et de toute manière, équivalent à $\mathbb{Z}/n\mathbb{Z}$ en ce qu'il est grosso-modo son image par un morphisme, l'exponentielle complexe.

2.6.3 Groupes finis d'ordres premiers

Quelques considérations sur les groupes finis d'ordres premiers, appelés ici *groupes premiers* même si cette appellation est loin d'être œcuménique. La plupart sont des corollaires du premier point, lui-même seule conséquence directe du théorème de Lagrange, mais celui-là explique pourquoi nous n'abordons ce sujet que dans cette section.

Propriété. ***(Cyclicité des groupes premiers)***

Tout groupe fini d'ordre premier est cyclique.

▷ Soit G un groupe fini d'ordre p premier Soit x un élément non trivial, qui existe, car $p > 1$ donc G n'est pas nul. Soit H le sous-groupe engendré par x. L'ordre de H divise p, donc l'ordre de H égale 1 ou p. Mais il n'est pas 1, puisque H n'est pas nul, puisque x ne l'est pas. Donc x génère un sous-groupe de G d'ordre p l'ordre de G, donc $H = G$, donc x génère G. Donc G est engendré par un élément, donc cyclique. ■

Corollaire. ***(Commutativité des groupes premiers)***

Tout groupe fini d'ordre premier est commutatif.

▷ Tout groupe cyclique est commutatif. ■

Propriété. ***(Générateurs des groupes premiers)***

Tout groupe fini d'ordre premier est engendré par n'importe lequel de ses éléments non neutres.

▷ Il suffit de jeter un coup d'œil sur la preuve précédente pour comprendre le résultat. ■

Propriété. ***(Simplicité des groupes premiers)***

Les sous-groupes quelconques d'un groupe fini d'ordre premier sont triviaux.

▷ Soit G un groupe premier d'ordre p. Soit H un sous-groupe de G. Par le grand théorème de Lagrange, $|H|$ divise p premier, donc $|H| = 1$ ou p. Si H est nul, c'est terminé. Sinon, $|H| \neq 1$ donc H est un sous-groupe de G de cardinal p donc $H = G$. Dans tous les cas, H est trivial (nul ou impropre). ■

Remarque. On en déduit que tout groupe premier est simple, puisque commutatif.

2.6.4 Structure des groupes cycliques

Les groupes cycliques (c'est-à-dire, essentiellement, les anneaux modulaires), héritent d'une certaine rigidité quant à leur structure et notamment à leurs sous-structures. En particulier, on montre dans le cadre des groupes cycliques une réciproque au théorème de Lagrange.

2.6.4.1 Sous-groupes d'un groupe cyclique

Avant de démontrer le résultat général sur les groupes cycliques, on démontre une propriété moins forte, qu'il convient de connaître à petit niveau (mais qui n'est pas vraiment plus facile à

démontrer !). Néanmoins, sa connaissance est requise pour la preuve de l'unicité dans le théorème suivant.

Propriété. ***(Cyclicité des sous-groupes d'un groupe cyclique)***

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

▷ Soit G un groupe cyclique. Soit H un sous-groupe de G. On applique une méthode similaire à celle pour montrer que tout sous-groupe de $\mathbb{N}$ est de la forme $n\mathbb{Z}$, ce qui naturel, car cette preuve établit que tous les sous-groupes d'un groupe monogène infini sont également monogènes.

Si H est le sous-groupe nul, alors il est cyclique puisque engendré par 1 et engendré par 1. Supposons donc $H \neq \{1\}$ et $h \in H$, $h \neq 1$. Soit a un générateur de G. On considère $psa = \{a^k, k \in \mathbb{N}\}$. Puisque a génère $G \ni 1$, il existe un $k \in \mathbb{N}^*$ tel que $a^k = h \in H$; k est non nul, car h n'est pas neutre. L'ensemble des $k \in \mathbb{N}^*$ tel que $a^k \in H$ est donc une partie non vide de $\mathbb{N}^*$. Soit donc k_0 son minimum. Alors a^{k_0} engendre H. En effet, soit $x \in H$ quelconque. Alors $x \in G$, et a génère g, donc $x = a^n$ pour au moins un $n \in \mathbb{N}$. On effectue la division euclidienne de n par k_0 : $n = qk_0 + r$ où $0 \leqslant r < k_0$. Alors $a^n = a^{qk_0+r} = a^{k_0 q} a^r = (a^{k_0})^q a^r$, et $a^{k_0} \in H$ par hypothèse, donc $(a^{k_0})^q$ également. Ainsi, puisque $x \in G$, $a^r = x(a^{k_0})^{-q} \in H$ sous-groupe de G. Mais c'est absurde, car alors $a^r \in H$ où $r < k_0$ ce qui contredit la minimalité de k_0 si $r \neq 0$. Ainsi $r = 0$, d'où $x = (a^{k_0})^q$, donc x est généré par a^{k_0} pour tout $x \in H$. Ceci termine la preuve. ■

Corollaire. ***(Générateur d'un sous-groupe d'un groupe cyclique)***

Tout sous-groupe H d'un groupe cyclique généré par x est généré par x^k où k est la plus petite puissance non nulle telle que $x^k \in H$.

▷ C'est l'objet de la preuve précédente, constructive. ■

Astuce !

Puisque tout sous-groupe H d'un groupe cyclique G est cyclique, et que l'on connaît les générateurs d'un groupe cyclique dès que l'on en connaît un (voir sous-section suivante), on connaît tous les générateurs d'un sous-groupe d'un groupe cyclique : étant donné x un générateur du groupe cyclique de départ G, ce sont les $x^{kk'}$ où k est la plus petite puissance non nulle telle que $x^k \in H$ et les k' sont les entiers de $[\![1,k]\!]$ premiers avec k.

Théorème. ***(Sous-groupes d'un cyclique)***

Soit G un groupe cyclique d'ordre $n \in \mathbb{N}$. Alors pour tout diviseur d de n dans $\mathbb{N}$, il existe un sous-groupe de G d'ordre d. De plus, ce sous-groupe est littéralement unique.

Remarque. L'assertion « littéralement unique » signifie que le sous-groupe considéré est unique et pas seulement *essentiellement unique*, c'est-à-dire unique à isomorphisme près.

Preuve.

▷ Remarquons que la proposition est immédiate pour le groupe cyclique nul. Soit donc G un groupe cyclique d'ordre $n \neq 0$ et soit d un diviseur naturel de n ; on a $d \neq 0$ par force. Soit m le diviseur associé, de sorte que $m = \frac{n}{d}$. Alors x^m est un élément de G d'ordre $\frac{n}{n \wedge m} = \frac{n}{m} = d$. Soit donc $H = \{1, x^m, x^{2m}, ..., x^{(d-1)m}\}$ le sous-groupe engendré par lui. Il est évidemment de cardinal d, donc H convient.

Montrons que c'est l'unique sous-groupe de G qui convient à la propriété énoncée. Soit H' un sous-groupe de G d'ordre d. D'après la proposition précédente, H' est cyclique. D'après son corollaire, on a même $H' = psx^{m'}$ où m' est la plus petite puissance non nulle de x telle que $x^{m'} \in H'$. L'ordre de $x^{m'}$ est donc d. Ainsi $x^{m'd} = 1$. De plus, l'ordre de x est bien $m'd$. En effet, puisque m' est minimal pour l'appartenance à H', $x^u \neq 1$ pour $1 < u < m'$. De plus aucun des $(x^{m'})^v$, $v < d$, n'égale 1 car sinon l'ordre de $x^{m'}$ ne serait pas d. Si maintenant $x^{m'v+i} = 1$, $1 < i < m'$, alors $x^{m'v}x^i \in H'$ puis $x^i = x^{-m'v} \in H'$ ce qui contredit la minimalité de m'. Par suite, $m'd = n$. Puisque $md = n$, on a $m = m'$ puis $H = H'$. ■

2.6.5 Élément primitif d'un groupe cyclique

Définition. ***(Élément primitif d'un groupe monogène)***

On appelle *primitif* d'un groupe G, tout générateur de G.

Exemple fondamental. ***(Racines primitives de l'unité)***

Soit n un entier naturel. On appelle *racine n-ième primitive de l'unité*, tout générateur du groupe cyclique $\mathbb{U}_n$. L'ensemble des racines n-ièmes primitives de l'unité n'est a priori pas un groupe, pour la bonne raison que leur nombre $\varphi(n)$ n'a aucune raison de diviser l'entier n.
Curieusement, dans le cadre des éléments primitifs d'un groupe cyclique, on préfère le formalisme multiplicatif ; sans doute à cause du lien fondamental avec la définition des polynômes cyclotomiques.

Propriété. ***(Générateurs d'un groupe cyclique (en fonction d'un donné))***

Soit G un groupe cyclique d'ordre n et x un générateur de G. Alors les générateurs de G sont donnés par les x^k où k sont les entiers de $[\![1,n]\!]$ premiers à n.

▷ L'ensemble des éléments de G est, par hypothèse, décrit par $\{x^k, k \in [\![1,n]\!]\}$. Considérons pour chacun des éléments de G le sous-groupe qu'il engendre. Remarquons également que x^k engendre G si et seulement s'il engendre x ; en effet, s'il engendre G, a fortiori, il engendre x, et réciproquement, s'il engendre x, il engendre tout élément engendré par x (car $x^n = x^{kn}$) donc G car x génère G. Ainsi, $G = psx^k$ si et seulement s'il existe un entier r tel que $x = x^{kr}$, soit $x^{kr-1} = 1$. Puisque x est d'ordre n, par caractérisation de l'ordre, ceci a lieu si et seulement s'il existe également un entier s tel que

$kr-1=sn$. Ainsi, $G=\left\langle x^k\right\rangle$ si et seulement s'il existe deux entiers r,s tels que $kr+sn=1$, c'est-à-dire si et seulement si k et n sont premiers entre eux d'après le théorème de Bézout. ■

Corollaire. ***(Nombre d'éléments primitifs d'un groupe cyclique)***

Un groupe cyclique d'ordre n possède exactement $\varphi(n)$ générateurs, où φ est l'indicatrice d'Euler.

▷ Par la proposition suivante et la définition formelle de l'indicatrice d'Euler. ■

2.6.6 Morphismes entre groupes cycliques

Propriété. ***(Morphismes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$)***

Soient n,m deux entiers naturels. Alors les morphismes de groupes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$ sont exactement les $\overline{x}\mapsto\overline{kx}$ où $k=q\frac{m}{\text{pgcd}(n,m)}$, $q\in[\![1,\text{pgcd}(n,m)]\!]$. En particulier, $\text{card}(\text{Hom}(\mathbb{Z}/n\mathbb{Z},\mathbb{Z}/m\mathbb{Z}))=\text{pgcd}(n,m)$.

▷ Soit f un tel morphisme. Alors pour tout $x\in\mathbb{Z}$, $f(\overline{x})=xf(\overline{1})$ donc par monogénéité, f est déterminé par $f(\overline{1})$. On a $f(\overline{1})=\overline{k}$ pour au moins un $k\in[\![1,m]\!]$. Alors $f(\overline{n})=f(0_n)=0_m=nf(\overline{1})=n\overline{k}=\overline{nk}$, d'où m divise nk. On note $d=\text{pgcd}(n,m)$ et on décompose $m=dm'$ et $n=dn'$, où m' et n' sont premiers entre eux. Alors $dm'\mid dn'k$ d'où $m'\mid n'k$ d'où $m'\mid k$ par le lemme de Gauss. Ainsi k est un multiple de $\frac{m}{\text{pgcd}(n,m)}$. Remarquons au passage que $q\frac{m}{\text{pgcd}(n,m)}\leqslant m$ d'où $q\leqslant\text{pgcd}(n,m)$. Réciproquement, on vérifie que si k est un multiple de $\frac{m}{\text{pgcd}(n,m)}$, alors pour tous x,$y\in\mathbb{Z}$, si $\overline{x}_n=\overline{y}_n$, alors $\overline{kx}_m=\overline{kx}_m$, et donc l'application $x\mapsto kx$ de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$ est bien définie. En effet, si n divise $x-y$, alors $k=q\frac{m}{\text{pgcd}(n,m)}=q\frac{\text{ppcm(n,m)}}{n}$ d'où $q\text{ppcm}(n,m)$ divise $k(x-y)$. Mais m divise $\text{ppcm}(n,m)$. Il est immédiat qu'elle définit alors un morphisme de groupes par opération usuelle. ■

Corollaire

Si n et m sont premiers entre eux, le seul morphisme de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$ est l'identité.

Corollaire

Le seul morphisme d'anneaux de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$ est l'identité.

2.6.7 Automorphismes d'un groupe cyclique

On établit une correspondance subtile entre les automorphismes du groupe additif $\mathbb{Z}/n\mathbb{Z}$ et les inversibles de l'anneau modulaire $\mathbb{Z}/n\mathbb{Z}$ qui sert également de pont entre l'arithmétique des anneaux et la théorie des groupes.

Propriété. ***(Description des automorphismes $\mathbb{Z}/n\mathbb{Z}$)***

Soit n un entier naturel. Les automorphismes du groupe additif $\mathbb{Z}/n\mathbb{Z}$ sont les $x \longmapsto cx$ où c est un entier naturel premier avec n.

Reformulation pratique

Dans le cadre d'un groupe cyclique G, noté multiplicativement, ses automorphismes sont donc les $x \longmapsto x^c$ où c est un entier naturel premier avec n.

▷ Soit f un automorphisme de $\mathbb{Z}/n\mathbb{Z}$. Puisque le groupe de départ est cyclique, le morphisme est déterminé par l'image de 1. En effet, si $k \in \mathbb{Z}$, $f([k]_n) = kf([1]_n) = [k]_n f([1]_n)$. Puisque f est bijectif, donc surjectif, il existe $k \in \mathbb{Z}$ tel que $[1]_n = [k]_n f([1]_n)$. Ainsi, $f([1]_n)$ est un inversible de $\mathbb{Z}/n\mathbb{Z}$, monoïde commutatif pour le produit. Ainsi, $f : x \longmapsto cx$ où c est un élément de $\mathbb{Z}/n\mathbb{Z}$ inversible. Ainsi, $c = [k]_n$ où k est premier avec n. Ainsi, $f : x \longmapsto [k]_n x = kx$ où k est un entier naturel premier avec n. ■

Remarque. Remarquer que cette propriété découle aisément de la description des morphismes de groupes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$, (n,m) quelconques, que l'on a déjà menée plus haut.

Théorème. ***(Automorphismes d'un groupe cyclique)***

Le groupe des automorphismes d'un groupe cyclique d'ordre n est isomorphe au groupe multiplicatif des inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z})^*$.

▷ Soit G un groupe cyclique d'ordre n. Il est donc isomorphe à $\mathbb{Z}/n\mathbb{Z}$, et immédiatement, $\mathrm{Aut}(G)$ est isomorphe à $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}$ (c'est une composition !). Il suffit donc de montrer le résultat pour $\mathbb{Z}/n\mathbb{Z}$. Pour tout $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^*$, k est premier avec n. Ainsi l'application $f_k : x \longmapsto kx$ est un automorphisme de $\mathbb{Z}/n\mathbb{Z}$ d'après la proposition précédente. Soit $f : (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ qui à $[k]$ fait correspondre f_k. Il est immédiat que cette application est bien définie, car si k et k' sont congrus modulo n, soit $k = k' + qn$, il définissent le même morphisme : pour $x \in \mathbb{Z}/n\mathbb{Z}$, $f_k(x) = kx = (k' + nq)x = k'x + q(nx) = k'x = f_{k'}(x)$, car $nx = 0$ dans $\mathbb{Z}/n\mathbb{Z}$. Montrons que f est un isomorphisme, ce qui garantira que $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ et $\mathbb{Z}/n\mathbb{Z}s$ sont isomorphes. L'application f est un morphisme, car pour tous $k,k' \in \mathbb{Z}/n\mathbb{Z}$, pour tout $x \in \mathbb{Z}/n\mathbb{Z}$, $f(kk')(x) = f_{kk'}(x) = (kk')x = k(k'x) = kf_{k'}(x) = f_k(f_{k'}(x))$, d'où $f(kk') = f_k \circ f_{k'}$. Montrons maintenant que f est bijective. D'après la proposition précédente, elle est surjective. Montrons qu'elle est injective. Soient $k,k' \in \mathbb{Z}/n\mathbb{Z}$. Supposons $f(k) = f_k = f(k') = f_{k'}$. Alors en particulier, $f_k(1) = k = f_{k'}(1) = k'$ dans $\mathbb{Z}/n\mathbb{Z}$. Donc $f : k \longmapsto f_k$ est injective, et c'est terminé. ■

On en déduit deux faits subtils, à retenir dans un coin de sa tête.

Corollaire

Le groupe des automorphismes d'un groupe monogène est commutatif.

▷ Le seul automorphisme de $(\mathbb{Z},+)$ est l'identité, donc dans le cas d'un groupe monogène infini G, $\mathrm{Aut}(G)$ est trivial. Le cas cyclique découle immédiatement de ce qui précède. ■

Corollaire

Le groupe des automorphismes d'un groupe premier est cyclique.

▷ Conséquence directe du théorème et de ce que le groupe multiplicatif d'un corps fini est cyclique. ■

2.6.8 Classification des groupes d'ordre *pq*

Les groupes d'ordre pq, $p < q$ deux nombres premiers distincts, sont presque cycliques, comme on va le voir. On rappelle que si $p = q$, le groupe est encore abélien, mais il n'est pas forcément cyclique.

Propriété. ***(Groupes abéliens d'ordre*** pq***)***

Soient p,q deux nombres premiers distincts. Alors tout groupe **abélien** d'ordre pq est cyclique.

▷ Simple application du théorème de Kronecker et du théorème des restes chinois. ■

Théorème. ***(Classification des groupes d'ordre*** pq***)***

Soient p,q deux nombres premiers distincts avec $p < q$.
Si p ne divise pas $q-1$, alors tout groupe d'ordre pq est cyclique.
Sinon, il y a deux groupes d'ordre pq non isomorphes : le groupe cyclique et un produit semi direct $\mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/q\mathbb{Z}$.

▷ Soit G un tel groupe. D'après le théorème de Sylow, G admet un q-Sylow et le nombre de ses conjugués et $k \mid p$ et $k \equiv 2 \ [q]$ où $q > p$, donc $k = 1$. Ainsi ce sous-groupe Q est distingué dans G. Par ailleurs, soit P un p-Sylow de G. Alors $P \cap Q$ est trivial, car son ordre divise à la fois p et q. Par conséquent, $PQ = G$. En particulier, G est produit semi-direct de Q et P : $G \simeq \mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$. Il reste donc à caractériser les morphismes possibles de $\mathbb{Z}/p\mathbb{Z}$ dans $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \simeq \mathbb{Z}/(q-1)\mathbb{Z}$.

Si $p \nmid q-1$, alors $p \wedge (q-1) = 1$ donc il n'y a que le morphisme trivial. Le produit est donc direct, $G \simeq \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ puis par le lemme chinois, $G \simeq \mathbb{Z}/pq\mathbb{Z}$ le groupe cyclique.

Dans le deuxième cas maintenant, alors $\mathbb{Z}/(q-1)\mathbb{Z}$ possède un unique sous-groupe Γ d'ordre p. Puisque l'image de φ divise nécessairement l'ordre de $\mathbb{Z}/p\mathbb{Z}$, son cardinal est 1, et c'est alors le morphisme nul, donc $G \simeq \mathbb{Z}/p\mathbb{Z}$, ou c'est un isomorphisme. Par suite, φ est nécessairement un isomorphisme de $\mathbb{Z}/p\mathbb{Z}$ sur Γ, déterminé par le choix de $\varphi(1)$ parmi les $p-1$ générateurs de Γ. Si ψ est un autre isomorphisme de $\mathbb{Z}/p\mathbb{Z}$ sur Γ, alors $\psi^{-1} \circ \varphi$ est un automorphisme de $\mathbb{Z}/p\mathbb{Z}$; il existe donc un isomorphisme de $Q \rtimes_\psi P$ sur $Q \rtimes_\varphi P$, donc ce produit semi-direct est unique à isomorphisme près. ■

2.7 Groupes de symétrie

Les groupes de symétrie sont des exemples particuliers de groupes ; la théorie des groupes trouve notamment des applications dans son étude appliquée aux groupes de symétrie. Le groupe étant en mathématiques la réalisation de la notion de symétrique, il n'est pas étonnant que tout groupe se réalise comme sous-groupe de l'un d'entre eux *(théorème de Cayley)*.

2.7.1 Groupes symétriques

Propriété. ***(Centre du groupe symétrique)***

Soit $n \geqslant 2$. Alors $\mathcal{Z}(\mathfrak{S}_n)$ est trivial.

2.7.1.1 Éléments remarquables du groupe symétrique

Propriété. ***(Inverse d'un cycle)***

L'inverse d'un cycle est son écriture de gauche à droite.

Un élément d'ordre 2, c'est-à-dire une involution de $\mathfrak{S}_n$, c'est pas forcément une transposition ! Par exemple, une *double transposition* comme $(1,2)(3,4)$ dans $\mathfrak{S}_4$ est d'ordre 2 mais n'est pas une transposition (pourquoi) ?

Exercice 10

Peut-on trouver dans un cas particulier dans $\mathfrak{S}_n$ une permutation d'ordre n (resp. $n!$) qui n'est pas un n-cycle (resp. $n!$-cycle) ?

▷ **Éléments de réponse.**

La seconde question est un test : évidemment que non, autrement $\mathfrak{S}_n$ serait cyclique mais en général il n'est pas commutatif, donc il y a peu de chances. Pour répondre à la première question, il faut aller jusqu'à $\mathfrak{S}_{10}$ dans lequel $(1,2,3,4,5)(6,7)$ est une permutation d'ordre $2 \times 5 = 10$ qui n'est pas un 10-cycle, ni un cycle d'ailleurs.

2.7.1.2 Signature

Propriété. ***(Conservations de la signature)***

La signature est un morphisme de groupes.

▷ Soient σ, σ' deux permutations. Alors

$$\varepsilon(\sigma\circ\sigma') = \prod_{1\leqslant i<j\leqslant n} \frac{\sigma\circ\sigma'(j)-\sigma\circ\sigma'(i)}{j-i} = \prod_{1\leqslant i<j\leqslant n} \frac{\sigma\circ\sigma'(j)-\sigma\circ\sigma'(i)}{\sigma'(j)-\sigma'(i)} \prod_{1\leqslant i<j\leqslant n} \frac{\sigma'(j)-\sigma'(i)}{j-i}$$
$$= \prod_{1\leqslant i<j\leqslant n} \frac{\sigma(i)-\sigma(i)}{j-i} \prod_{1\leqslant i<j\leqslant n} \frac{\sigma'(i)-\sigma'(i)}{j-i} = \varepsilon(\sigma)\times\varepsilon(\sigma')$$

puisque σ' est une bijection de $[\![1,n]\!]$ sur lui-même. ■

Théorème. ***(Caractérisation de la signature)***

La signature est l'unique morphisme de groupes non trivial de $\mathfrak{S}_n$ dans $\mathbb{C}^*$, pour tout entier naturel n.

▷ Toutes les transpositions de $\mathfrak{S}_n$ sont conjuguées donc elles ont la même image par ε, notons la c. Soit $t = (1,2)$ une transposition au pif. Alors $\varepsilon(t^2) = \varepsilon(id) = 1 = c^2$. Si $c = 1$, puisque toute permutation est un produit de transposition, alors $\varepsilon = 1$, exclu. Sinon, $c = -1$. Soit σ une permutation paire ; alors σ est le produit d'un nombre pair de transpositions, donc $\varepsilon(\sigma) = +1$. Soit σ une permutation impaire ; alors σ est le produit d'un nombre impair de transpositions, donc $\varepsilon(\sigma) = -1$. On reconnaît la signature. ■

Propriété. ***(Expression de la signature par les inversions)***

Soient $n \in \mathbb{N}$ et $\sigma \in \mathfrak{S}_n$. Alors $\varepsilon(\sigma) = (-1)^N$ où N est le nombre d'inversions de σ.

2.7.1.3 Présentations du groupe symétrique

Soit n un entier naturel.

Théorème

Les cycles engendrent $\mathfrak{S}_n$.

Théorème

Les transpositions engendrent $\mathfrak{S}_n$.

On peut faire encore mieux.

Propriété

Les transpositions de la forme $(1,i)$, $i \in [\![2,n]\!]$, engendrent $\mathfrak{S}_n$.

▷ En effet, $(i,j) = (1,i)(1,j)(1,i)$. ■

Remarque. Ce système de générateurs par des transpositions est minimal ; on ne peut pas trouver de système à moins de $n-1$ éléments composé uniquement de transpositions.

▷ La preuve est simple. ■

Propriété

Les transpositions de la forme $(i,i+1)$, $i \in [\![1,n-1]\!]$, engendrent $\mathfrak{S}_n$.

▷ Par récurrence à partir de ce qui précède : pour $(1,2)$, il n'y a rien à faire ; ensuite, on écrit pour $(1,k+1) = (k,k+1)(1,k)(k,k+1)$. ■

Propriété

Le couple $(1,2,\ldots,n)$ et $(1,2)$ engendre $\mathfrak{S}_n$. Plus généralement, si $i \in [\![1,n-1]\!]$, le couple $(1,2,\ldots,n)$ et $(i,i+1)$ engendre $\mathfrak{S}_n$.

▷ Il suffit d'itérer l'action par conjugaison de ce cycle sur cette permutation pour voir qu'ils engendrent le système précédent. ■

Remarque. Ce système est évidemment minimal, puisque le groupe symétrique n'est pas monogène.

Attention ! $(1,2,3,4) \in S_4$ et $(1,3) \in S_4$ engendrent un groupe diédral $|H| = 8$. On pourra voir un critère sous le quel un n-cycle et une transposition engendrent S_n.

2.7.1.4 Sous-groupe alterné

Propriété. *(Cardinal du groupe alterné)*

Soit n un entier naturel $\geqslant 2$. Alors $\text{card}(\mathfrak{A}_n) = \frac{n!}{2}$.

▷ Soit τ une transposition, par exemple $(1,2)$. Alors $\sigma \mapsto \sigma \circ \tau$ est une bijection de $\mathfrak{A}_n$ sur son complémentaire dans $\mathfrak{S}_n$. ■

Propriété. *(Cardinal du groupe alterné)*

Soit n un entier naturel $\geqslant 2$. Alors $\mathfrak{A}_n$ est l'unique sous-groupe de $\mathfrak{S}_n$ d'ordre $\frac{n!}{2}$.

▷ Il s'agit de se rappeler qu'un tel sous-groupe H est d'indice 2 donc respecte donc la règle des signes. Puisque toute permutation se décompose en produit de transpositions, soit H contient toutes les permutations paires, soit H contient toutes les permutations impaires. Or H contient l'identité qui est paire, donc $H = \mathfrak{A}_n$ par définition. ■

Propriété. ***(Centre du groupe alterné, du groupe symétrique)***

Pour tout entier naturel $n \geqslant 3$, $\mathcal{Z}(\mathfrak{A}_n) = \mathcal{Z}(\mathfrak{S}_n) = \{id\}$.

▷ On le vérifie jusqu'à $n = 5$ à partir duquel on invoque la simplicité du groupe alterné. La deuxième égalité en découle. ■

2.7.1.5 Propriétés calculatoires des cycles

Une puissance d'un cycle n'est pas nécessairement un cycle !

Propriété. ***(Puissance d'un cycle)***

Soient n,p,k des entiers naturels et $c = (a_1,...,a_p) \in \mathfrak{S}_n$ un p-cycle, $a_1,...,a_p \in [\![1,n]\!]$.
Alors c^k est le produit de $k \wedge p$ cycles de longueur $\frac{p}{p \wedge k}$.

▷ Pour trouver la décomposition d'une permutation, on reprend la preuve du théorème fondamental : on étudie l'action du groupe engendré par c^k sur $[\![1,n]\!]$. Soit donc un élément dans le support de c^k, soit $i \in [\![1,p]\!]$; on note $w(a_i)$ l'orbite de a_i, soit $w(a_i) = \{a_{i+mk}, m \in \mathbb{N}^*\}$ où les indices sont pris modulo p. On cherche donc le plus petit m non nul tel que $mk \equiv 0\ [p]$. Il est clair par une technique classique que ce $m = \frac{p}{p \wedge k}$. L'orbite est donc de cardinal $\frac{p}{p \wedge k}$. Puisqu'il y a p éléments dans le support de c, la réunion de ces orbites est de cardinal p, donc il doit y avoir $p \wedge k$ tels cycles, d'où le résultat. ■

Lemme. ***(Lemme fondamental des cycles)***

Soient $n \in \mathbb{N}$, $\sigma \in \mathfrak{S}_n$ et $a_1,...,a_s \in [\![1,n]\!]$, $s \in \mathbb{N}$. Alors :

$$\sigma(a_1, ..., a_s)\sigma^{-1} = (\sigma(a_1),..., \sigma(a_s)).$$

Attention à ne pas inverser le sens de la conjugaison.

Propriété. ***(Classes de conjugaison dans $\mathfrak{S}_n$)***

Deux permutations sont conjuguées si et seulement si elles ont le même type.

▷ Il est clair que si σ, σ' sont conjuguées par τ, elles ont le même type par le lemme fondamental des cycles : $\sigma' = \tau c_1 c_2 ... c_m \tau^{-1} = \tau c_1 \tau^{-1} ... \tau c_m \tau^{-1}$ où $\sigma = c_1 ... c_m$. Réciproquement, soient σ, σ' deux permutations de même type : $\sigma = \alpha_1,..., \alpha_r$ et $\sigma' = \beta_1, ..., \beta_r$ de mêmes longueurs dans

l'ordre. Alors pour conjuguer σ à σ', on choisit pour chaque cycle i une permutation qui marche avec le lemme fondamental. Comme tous ces cycles sont à supports disjoints, on peut prendre une seule et même conjugatrice qui fonctionne pour tous ; en réécrivant comme précédemment, on obtient une formule de conjugaison. ■

2.7.1.6 Propriétés combinatoires des cycles

2.7.1.7 Propriétés matricielles des permutations

Théorème. ***(Théorème de Brauer)***

Soit K un corps de caractéristique nulle. Soit n un entier naturel. Soient $\sigma, \tau \in \mathfrak{S}_n$. Alors σ, τ sont conjugués dans $\mathfrak{S}_n$ si et seulement si P_σ et P_τ sont K-semblables.

▷ Le sens direct est immédiat par le fait que $\sigma \mapsto P_\sigma$ soit un morphisme de groupes : si $\sigma = \gamma\tau\gamma^{-1}$, alors $P_\sigma = P_\gamma P_\tau P_\gamma^{-1}$ dans $\mathfrak{M}_n(\mathbb{K})$. On montre le sens réciproque.

Supposons que P_σ,P_τ sont semblables sur K. On sait d'après le lemme fondamental sur les cycles que deux permutations sont conjuguées si et seulement si elles ont le même type, c'est-à-dire si elles ont le même nombre c_p de p-cycles dans la décomposition en produit de cycles à supports disjoints pour tout $p \in [\![1,n]\!]$. Montrons donc qu'il existe $B \in GL_n(K)$ tel que $Bx = 0$ où $x = (c_1(\sigma)-c_1(\tau),...,c_p(\sigma)-c_p(\tau))$.

Soit $\gamma \in \mathfrak{S}_n$. On pose $V_\gamma = \mathrm{Ker}(P_\gamma - I_n)$. Soit $y \in \mathbb{R}^n$. Alors $y \in V_\gamma$ ssi $P_\gamma y = y$ ssi $\forall k \in \mathbb{N} P_\gamma^k y = y$ ssi $\forall k \in \mathbb{N}, \forall i \in [\![1,n]\!]$, $y_{\gamma^k(i)} = y_i$, donc $y \in V_\gamma$ si et seulement si $y_i = y_j$ dès que i et j sont dans la même orbite sous l'action de $\langle\gamma\rangle$. On en déduit que $\dim(V_\gamma) = \sum_{p=1}^{n} c_p(\gamma)$ est le nombre d'orbites de $[\![1,n]\!]$ sous l'action de $\langle\gamma\rangle$.

Puisque P_σ et P_τ sont semblables, pour tout $k \in \mathbb{N}$, P_σ^k et P_τ^k le sont également. Par suite, V_{σ^k} et V_{τ^k} sont clairement isomorphes, donc de même dimension ; ainsi σ^k et τ^k ont le même nombre de cycles dans leurs décompositions. D'après le lemme sur le nombre de cycles dans la décomposition de la puissance d'un cycle, on a $\sum_{p=1}^{n}(k \wedge p)c_p(\sigma) = \sum_{p=1}^{n}(k \wedge p)c_p(\tau)$ d'où $\sum_{p=1}^{n}(k \wedge p)[c_p(\sigma) - c_p(\tau)] = 0$. Ainsi $B = (i \wedge j)_{i,j \in [\![1,n]\!]^2}$ convient.

Reste à montrer que B est inversible. Or on vérifie par le calcul (très agréable) que si $A = (a_{ij})_{i,j}$ est la matrice telle que $a_{ij} = 1$ si i divise j et 0 sinon, si φ est l'indicatrice d'Euler, alors d'après la formule $m = \sum_{d|m} \varphi(d)$, $A^T Diag(\varphi(1),...,\varphi(n))A = B$, donc puisque A est triangulaire supérieure avec seulement des 1 sur la diagonale, A est inversible, donc B également. ■

2.7.1.8 Sous-groupes transitifs du groupe symétrique

Définition. ***(Sous-groupe transitif)***

Soit n un entier naturel. Soit H un sous-groupe de $\mathfrak{S}_n$. Le groupe H est dit *transitif*, si l'action naturelle de $\mathfrak{S}_n$ sur $[\![1,n]\!]$ induite sur H est transitive.

Lemme

n divise l'ordre de tout sous-groupe transitif de $\mathfrak{S}_n$.

▷ Soit S le stabilisateur de 1. Alors $\text{card}(H) = \text{card}(S)\text{card}(\Omega_1)$. Mais il n'y a qu'une seule orbite, donc $\text{card}(\Omega_1) = n$, puisque $\Omega_1 = [1,n]$. ■

Théorème

Pour p premier, les sous-groupes transitifs de $\mathfrak{S}_p$ sont exactement les sous-groupes contenant un p-cycle.

▷ Soit H un sous-groupe transitif de $\mathfrak{S}_p$. Alors d'après le lemme, p divise H, donc H peut contenir un p-cycle. Réciproquement, un sous-groupe de $\mathfrak{S}_p$ est bien transitif. ■

Proposition

Tout conjugué d'un groupe transitif est transitif.

▷ Soit H un sous-groupe transitif. Soient $g \in \mathfrak{S}_n$ et $x \in [1,n]$. Par transitivité, il existe $h \in H$ tel que $hg^{-1}(1) = g^{-1}(x)$. Donc $ghg^{-1}(1) = x$, donc gHg^{-1} est transitif. ■

Théorème. ***(Sous-groupes transitifs de $\mathfrak{S}_4$)***

Les sous-groupes transitifs de $\mathfrak{S}_4$ sont lui-même, son sous-groupe alterné, et les conjugués de $\langle(13),(1234)\rangle$, $\langle(13)(24),(12)(34)\rangle$ et $\langle(1234)\rangle$.

▷ Les sous-groupes transitifs de $\mathfrak{S}_4$ sont d'ordre 4, 8 ou 12. Dans le dernier cas, on a un sous-groupe distingué. S'il contient une transposition, il les contient toutes, donc c'est $\mathfrak{S}_4$ entier, absurde. Donc H est dans $\mathfrak{A}_4$. Donc $H = \mathfrak{A}_4$. Autrement, on remarque que D_8 agit fidèlement sur l'ensemble des sommets du carré, $D_8 \hookrightarrow \mathfrak{S}_4$ donc son image est un 2-Sylow de $\mathfrak{S}_4$ isomorphe au groupe diédral d'ordre 4. On observe que les sous-groupes transitifs de ce dernier sont lui-même, le groupe engendré par sa rotation et $\{1,r^2,sr,sr^3\}$. D'après les théorèmes de Sylow, H est conjugué à un sous-groupe de ce groupe diédral. ■

2.7.2 Groupes diédraux

Les groupes diédraux sont les groupes de symétrie des polygones réguliers du plan.

2.7.2.1 Définition

Soit $n \in \mathbb{N}$ tel que $n \geqslant 3$; avant cela, le groupe diédral est mal défini et n'a pas d'interprétation géométrique. On se place dans le plan complexe et on considère l'unique polygone régulier convexe dont les sommets sont les éléments de $\mathbb{U}_n$.

On rappelle qu'une isométrie affine est une application du plan complexe dans notre cas dans lui-même conservant les distances, c'est-à-dire, le produit scalaire usuel. L'ensemble $\mathrm{Isom}(\mathbb{C})$ des isométries du plan est un groupe pour la loi de composition des applications.

On utilisera le lemme suivant :

Théorème

Une isométrie du plan est déterminée par l'image d'un point non nul.

▷ En effet, $f(X) = AX + B = AX + f(0)$. Ainsi, si $X_0 = (x,y)$ est non nul, on a $AX = f(X_0) - f(0) = (\cos(\theta)x - \sin(\theta)y, \sin(\theta)x + \cos(\theta)y)$. En sommant et en faisant la différence, ceci permet de trouver l'angle θ. ■

Fait

L'ensemble des isométries affines de $\mathbb{C}$ opère sur $\mathbb{C}^m$ par $f \cdot (x_1,...,x_m) = (f(x_1),...,f(x_m))$.

Définition. ***(Groupe diédral)***

On appelle *groupe diédral* d'ordre n, ou de degré n, et l'on note D_n, le **groupe** stabilisateur de $\mathbb{U}_n$ pour l'action définie précédemment.
C'est-à-dire : le groupe diédral d'ordre n est l'ensemble des isométries affines laissant invariant le polygone régulier à n côtés.

Remarque. La formulation curieuse de la définition précédente est justifiée par le fait qu'on vérifie facilement, vu qu'une isométrie affine préserve les distances, qu'un élément de D_n va en vérité préserver *n'importe quel polygone régulier* à n côtés du plan complexe. Ceci justifie également que l'on se limite à $\mathbb{U}_n$.

Autre remarque. Par définition, D_n est un groupe. C'est un sous-groupe de $\mathrm{Isom}(\mathbb{C})$.

Heuristique

On comprend que cette condition de fixation va drastiquement diminuer le nombre d'isométries la satisfaisant, jusqu'à un nombre fini. On comprend également que le groupe symétrique ne va pas suffire, puisqu'à priori, il n'est pas possible de permuter isométriquement les côtés d'un polygone à $n \geqslant 4$ côtés.

Nous allons préciser la structure de D_n tout le long de cette partie.

Prendre $\mathbb{U}_n$ en particulier à l'intérêt suivant.

Lemme

Toute isométrie affine préservant $\mathbb{U}_n$ préserve l'origine, autrement dit, est une isométrie vectorielle.

▷ La somme des racines n-ièmes de l'unité est nulle. Puisqu'une application affine préserve les barycentres, elle préserve leur barycentre, qui est zéro, d'où le résultat. ■

On rappelle qu'une isométrie vectorielle est une application linéaire de $\mathbb{R}^2$ dans lui-même préservant le produit scalaire, *i.e.* les distances, qui est de plus inversible et de norme 1. Matriciellement, son inverse égale sa transposée. On note $Oj(\mathbb{C})$ l'ensemble des isométries vectorielles du plan complexe, groupe pour la composition, topologiquement compact. Une isométrie vectorielle est de déterminant ± 1 et envoie toute base orthonormée sur une base orthonormée, propriété qui les caractérise ; dans le plan, la classification des isométries est largement simplifiée : on appellera *rotation* toute isométrie positive, dont le sous-groupe est noté $\mathcal{SO}_n(\mathbb{R}^2)$, et *réflexion* toute isométrie négative, dont l'ensemble, complémentaire du précédent, est noté $\mathcal{O}_-(\mathbb{R}^2)$. Le sous-groupe $\mathcal{SO}_n(\mathbb{R})$ est d'indice 2. On connaît la forme matricielle exacte des isométries du plan ; on renvoie au cours d'Algèbre linéaire ou de Géométrie pour leur description exhaustive.

On s'intéresse maintenant à la structure de D_n, sous-groupe (que l'on va montrer fini) de $\mathcal{O}(\mathbb{C})$.

On remarque que :

Propositions

- D_n contient un sous-groupe cyclique d'ordre 2, à savoir $\{id, s\}$ où s est la réflexion d'axe (OI) où I est le point d'affixe 1 (car $\mathbb{U}_n$ est stable par conjugaison).
- D_n contient un sous-groupe cyclique d'ordre n, à savoir $\langle r \rangle$ où r est la rotation d'angle $\frac{2\pi}{n}$, soit $z \mapsto e^{\frac{2i\pi}{n}} z$.

Proposition

$srsr = 1$.

▷ L'application r^{-1} est la rotation de centre O et d'angle $-2\pi/n$. De plus, en observant le déterminant, srs est une rotation. Il suffit de regarder l'image de I. Il est clair que $s(I) = I$, puisque $sr(I)$ est le conjugué de I, d'où le résultat. ■

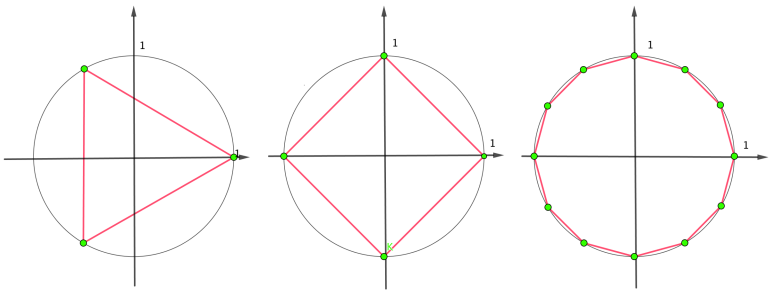


FIGURE 2.7.1 : *Les premiers ensembles sur lesquels les groupes diédraux agissent de façon stabilisatrice* —

Corollaire. ***(Commutativité de D_n)***

On voit par cette propriété que D_n n'est jamais abélien (pour $n \geqslant 3$).

Théorème

D_n est généré par r et s.

▷ On note A_k le point d'affixe $e^{\frac{2ik\pi}{n}}$ pour $k \in [\![0,n-1]\!]$. Soit $f \in D_n$. Alors f est soit une réflexion, soit une rotation.

S'il existe k tel que $f(A_k) = A_k$, alors par caractérisation des isométries du plan, f est la réflexion d'axe (OA_k). Or $s \circ r^{n-2k}(A_k) = s(A_{n-k}) = A_k$, donc $f = s \circ r^{n-2k}$.

Si maintenant f n'a pas d'autre point fixe que O, supposons que f soit une rotation. Soient tout de même k,m tels que $f(A_k) = A_m$. Alors f est d'angle $(\vec{OA_k}, \vec{OA_m}) = \arg(\frac{e^{\frac{2ik\pi}{n}}}{e^{\frac{2im\pi}{n}}})$, soit $f = r^{k-m}$.

Supposons enfin que f soit une réflexion sans point fixe. Notons Δ son axe. Alors $O \in \Delta$ et il existe bien évidemment $k \in [\![0,n-1]\!]$ tel que Δ coupe $[A_k, A_{k+1}]$; de plus $f \in D_n$, donc forcément f coupe ce segment en son milieu. Alors $f = s \circ r^{n-2k-1}$. En effet, en regardant le déterminant $s \circ r^{n-2k-1}$ est une réflexion. De plus, $s \circ r^{n-2k-1}(A_k) = A_{k+1}$. Donc $f = s \circ r^{n-2k-1}$.

Ainsi, tout élément de D_n est dans $\langle s,r \rangle$, ce qu'il fallait montrer. ■

De là, on va déduire une description exhaustive du groupe diédral de degré n.

Lemmes

1. Pour tout $k \in [\![0,n-1]\!]$, $sr^k s = b^{-k}$.
2. s n'est pas une puissance de r.

▷ Immédiats. ■

Proposition. ***(Description de D_n)***

$D_n = \{1, s, r, ..., r^{n-1}, sr, ..., sr^{n-1}\}$. De plus, tout groupe engendré par deux éléments a,b d'ordre respectifs 2 et n tels que $abab = 1$, est isomorphe à D_n.

Proposition. ***(Cardinal (et pré-structure) de D_n)***

Pour tout $n \geqslant 3$, $\text{card}(D_n) = 2n$ et D_n est constitué de n rotations formant un sous-groupe cyclique d'indice 2 de D_n et de n réflexions, son complémentaire.

Nous utilisons dans cette article la convention : D_n est le sous-groupe des isométries laissant invariant un polygone régulier d'ordre n. Certains auteurs veulent que le cardinal de D_n égale son ordre ; dans ce cas, ce groupe devient $*D_{2n}$; nous n'utilisons pas cette convention.

Exemples. ***(Groupes diédraux de petits ordres)***

1. Pour $n = 0$, $\mathbb{U}_n$ n'est pas défini sur $\mathbb{U}$. On peut raisonnablement fixer $D_0 = \{id\}$, mais attention à l'initialisation si l'on fait une récurrence sur les cardinaux des groupes diédraux à la commencer à 1.
2. Pour $n = 1$, le groupe D_1 est l'ensemble des isométries fixant un point ; il contient l'identité et la réflexion d'axe l'axe des abscisses ; on a donc $D_1 \simeq C_2$ le groupe cyclique d'ordre 2.
3. Pour $n = 2$, le groupe D_2 est l'ensemble des isométries fixant un segment ; il contient l'identité, la rotation d'angle π, la réflexion par rapport à l'axe des abscisses et l'antirotation d'angle π. Il est isomorphisme au groupe de Klein $\mathcal{K} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Ces deux groupes sont les seuls groupes diédraux abéliens.
4. Pour $n = 3$, le groupe D_3 est l'ensemble des isométries qui fixe un triangle équilatéral. Il est isomorphe à $\mathfrak{S}_3$ le groupe symétrique d'ordre 3, en particulier, il n'est pas commutatif.

Méthode. ***(Construire en un temps record le groupe diédral)***

Soit D_n l'ensemble des isométries affines du plan complexe qui fixent le polygone régulier d'ordre n donné par les racines de l'unité. Une isométrie affine est déterminée par l'image d'un point ; par hypothèse, l'image d'un des segments du polygone considéré par un élément de D_n est un autrement segment ; or il y a n segments. En tenant compte de l'orientation, on trouve $|D_n| = 2n$. D'autre part, il existe un sous-groupe de D_n noté D_n^+ uniquement composé de rotations : c'est le noyau du déterminant $D_n \longrightarrow \{\pm 1\}$. Puisque D_n contient au moins une rotation (d'angle $2\pi/n$ et au moins une réflexion (par rapport à l'axe (Ox), le premier théorème d'isomorphisme donne que $|D_n^+| = n$. On voit immédiatement qu'il est engendré par la rotation choisie en exemple à la phrase précédente.

Proposition. ***(Ordre des réflexions)***

Tout élément de D_n^- est d'ordre 2. De plus, en le notant s', on a $D_n = \langle r,s \rangle$.

▷ Une réflexion (ici dans le plan) est une symétrie, donc involutive. On peut vérifier qu'un couple d'éléments vérifie les axiomes de caractérisation d'un groupe diédral, puisque r engendre un groupe cyclique d'ordre n, c'est le groupe diédral d'ordre n. ■

Exercice 11

Montrer qu'il n'y a aucune inclusion non triviale entre les groupes diédraux finis.

▷ **Éléments de réponse.**

Si les racines de l'unité peuvent se recouper, toutes les isométries de $D_n \supseteq D_m$ fixent-elle vraiment le m-gone ?

Proposition

$I_p \circ I_q = T_{p-q}$.

2.7.3 Groupes de symétrie de l'espace

2.8 Quotients de groupe

L'austérité de la section précédente sut les structures quotients en algèbre générale élémentaire doit s'effacer devant une partie plus sexy sur les quotients de groupe. On doit introduire d'abord la notion adjacente de sous-groupe distingué, aussi appelé sous-groupe normal. On rappelle aussi cette propriété claire de la partie précédente :

Propriété. ***(Groupe quotient)***

Si $(G, \times)$ est un groupe, $\mathcal{R}$ une relation d'équivalence sur G compatible avec $\times$, alors $G/\mathcal{R}$ muni de la loi quotient est un groupe d'élément neutre $\overline{e}$; si $x \in G$, $\overline{x}^{-1} = \overline{x^{-1}}$.

▷ On pouvait voir aussi que le quotient est l'image d'un groupe par π, surjective, qui est un morphisme de magmas. ■

2.8.1 Distinction de sous-groupes

2.8.1.1 Notion de distinction ou normalité

On introduit une relation d'équivalence dans les groupes, très utile, liée au concept de conjugaison : deux éléments a et b d'un groupe sont dits *conjugués* s'il existe g dans ce groupe

tel que $gag^{-1} = b$, ou autrement dit $ga = bg$. Pour toute la suite, on se fixe $(G, \times)$ un groupe, non nécessairement commutatif. Soit H un sous-groupe de G muni de sa loi induite.

Propriété. ***(Classes à gauches, classes à droite)***

Les relations $\sim_d$ et $\sim_g$ définies sur G par $a \sim_g b \iff a^{-1}b \in H \iff b \in aH$ et $a \sim_d b \iff ba^{-1} \in H \iff b \in Ha$ sont deux relations d'équivalences. Leurs classes sont respectivement appelées *classes à gauche modulo* H et *classes à droite modulo* H.

▷ Facile (le faire !). ■

⟶ **Convention.** On ne considère plus que les classes à gauche, quitte à considérer le groupe opposé : $(G, \times')$ où pour tous x,$y \in G$, $x \times' y = y \times x$. La relation d'équivalence des classes à droite pour le groupe G est alors celle des classes à gauche sur son groupe opposé. Cette relation d'équivalence, on pourra appeler systématiquement *relation d'équivalence des classes à gauche*, l'autre, *relation d'équivalence des classes à droite*. Lorsque les classes à gauche et les classes à droite coïncident, on dira tout simplement *classes*, ce dont on va voir que cela correspond exactement au cas où le sous-groupe modulo est distingué. Ce n'est pas la même relation que la conjugaison évoquée plus haut.

Exercice 12

1. Montrer que toutes les classes à gauche par H sont équipotentes à H.
2. *(Théorème de Lagrange)* On suppose G fini. Montrer que $\mathrm{card}(H)$ divise $\mathrm{card}(G)$. *La quantité* $\frac{\mathrm{card}(G)}{\mathrm{card}(H)}$*, notée* $[G : H]$ *(ou* $(G : H)$ *dans le contexte de la théorie des corps où ce premier note le degré), est appelée indice de* H *dans* G *; elle peut être définie même si le groupe n'est pas fini.*

Exercice 13

Soit $(u_n)_{n\in\mathbb{N}}$ une suite dans un espace métrique et p un entier naturel. Justifier de deux manières que $(u_n)_{n\in\mathbb{N}}$ converge si et seulement si pour tout $k \in [\![0,p-1]\!]$, les $(u_{np+k})_{n\in\mathbb{N}}$ convergent vers la même limite.

Avant de poursuivre, il est conseillé de reprendre la notion succincte de compatibilité latérale.

Propriété. ***(Caractérisation des relations d'équivalence compatibles à gauche avec les lois de groupe)***

On a que la relation d'équivalence des classes à gauche est compatible à gauche avec la loi de groupe $\times$. Réciproquement, toute relation d'équivalence compatible avec elle est une relation de classes à gauche modulo un certain sous-groupe.

▷ On fait systématiquement l'abus de ne pas préciser les lois de groupe, puisqu'il n'y en a qu'une et ses restrictions. Soit G un groupe et H un sous-groupe, $\sim$ la relation d'équivalence des

classes à gauche. Montrons qu'elle est compatible à gauche : soient x,y,y' dans G tels que $y \sim y'$, et montrons $xy \sim xy'$. L'hypothèse se récrit $y^{-1}y' \in H$, et montrons $(xy)^{-1}xy' \in H$, soit $y^{-1}x^{-1}xy' \in H$ par inverse d'un produit ; ces notations sont univoques par associativité. Or $x^{-1}x = e$ donc cela revient à montrer $y^{-1}y' \in H$, ce qui exactement l'hypothèse, donc c'est immédiat.

Réciproquement, soit $\sim$ une relation d'équivalence sur G compatible à gauche avec la loi de groupe. On pose $H = \overline{e}$ comme on s'y attend. Dans ce cas, $a \sim b \iff a^{-1}a \sim a^{-1}b \iff e \sim a^{-1}b \iff a^{-1}b \in \overline{e} \iff a^{-1}b \in H$; justifions la première équivalence : le sens direct est la compatibilité à gauche, le sens réciproque est la régularité dans le groupe G. Enfin, il faut vérifier que H est bien un sous-groupe (et oui, petit scarabée). Il contient le neutre par réflexivité, il est stable par circularité de $\sim$ (conjonction de la transitivité et de la symétrie) et stable par passage à l'inverse, car si $x \in H$, $\overline{x} = \overline{e}$ et l'on a justifié que $\overline{x^{-1}} = \overline{e^{-1}} = \overline{e}$ soit $x^{-1} \in H$. ■

Exercice 14

Donner un exemple de groupe et de sous-groupe où les classes à gauche et les classes à droite ne coïncident pas.

⟶ **Notation.** Étant donné une relation d'équivalence G compatible avec la loi de groupe, on note H le sous-groupe dont elle est relation d'équivalence des classes à gauche ; il existe toujours d'après ce qui précède. On note alors G/H le groupe quotient de G par ladite relation. Pour les classes à droite, ce qui consiste à remplacer par le mot *droite* toutes les occurrences de *gauche* dans le théorème précédent, on note $H \setminus G$.

Exercice 15

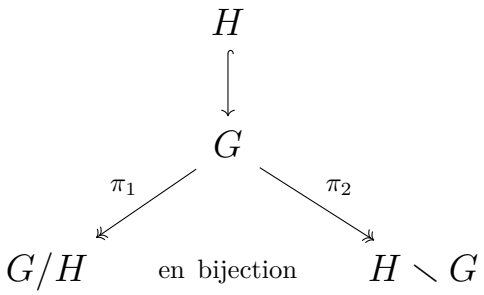
Cette notation est-elle raisonnable ?

Propriété. ***(Dénombrement des classes à gauche et à droite)***

Pour tout groupe G, pour tout sous-groupe H de G, G/H et $H \setminus G$ ont le même cardinal.

▷ La bijection à exhiber est celle qui à une partie de G, associe la partie composée des inverses d'éléments de G : $X \longmapsto X^{-1} = \{x^{-1} \mid x \in X\}$. ■

Pour l'instant, on dispose seulement du schéma suivant :



L'injection de H dans G est canonique, car c'est même une inclusion.

Exercice 16

1. *(Passage fondamental du monde des classes au monde des éléments)* Montrer que pour tout $a \in G$, $aH = H$ si et seulement si $a \in H$.
2. Montrer que pour tous a,$b \in G$, $aH = bH$ si et seulement si $aH \subseteq bH$ et que cette condition est elle-même équivalente à l'équivalence de a et b.
3. Montrer que pour tous a,$b \in G$, $aH = Hb$ si et seulement si $aH \subseteq Hb$. Cette condition est elle équivalente à l'équivalence de a et b ?

L'origine des classes à gauche et classes à droite

La théorie des groupes est élaborée en grande partie dans la première moitié du XIX^{e} siècle par Évariste Galois, mathématicien français, élève au lycée Louis-le-Grand, deux fois emprisonné, mort en 1832 à vingt ans à la suite d'un duel causé par « une infâme coquette ». La veille, le num29 mai, il écrit un lettre adressée à Auguste Chevalier qui constitue son testament mathématique. Il lui demande en fin d'article : « Tu prieras publiquement Jacobi ou Gauss de donner leur avis, non sur la vérité mais sur l'importance des théorèmes. » Dans cette lettre, centrée sur la résolution des équations, il écrit : *Dans les deux cas, le groupe de l'équation se partage par l'adjonction en groupes tels, que l'on passe de l'un à l'autre par une même substitution ; mais la condition que ces groupes aient les mêmes substitutions n'a lieu certainement que dans le second cas. Cela s'appelle la décomposition propre.*

En d'autre termes, quand un groupe G en contient un autre H, le groupe G peut se partager en groupes, que l'on obtient chacun en opérant sur les permutations de H une même substitution ; en sorte que

$$G = H + HS + HS' + ...$$

Et aussi il peut se décomposer en groupes qui ont tous les mêmes substitutions, en sorte que

$$G = H + TH + T'H + ...$$

Ces deux genres de composition ne coïncident pas ordinairement. Quand ils coïncident, la décomposition est dite propre. Et l'on voit combien le groupe Bourbaki a apporté au formalisme mathématique dans les années 1940.

On introduit maintenant la terminologie fondamentale de cette partie.

Définition. ***(Sous-groupe normal, sous-groupe distingué)***

Un sous-groupe H du groupe G est dit *normal*, ou *distingué*, ou *invariant*, s'il est stable par automorphismes intérieurs (ou actions par conjugaison, pour tous les élements de G). On note alors $H \triangleleft G$.

Remarques.

1. Par définition, $H \triangleleft G \iff \forall a \in G \quad aHa^{-1} \subseteq H$, ou ce qui est équivalent (dire pourquoi), $a^{-1}Ha \subseteq H$.
2. On dit sous-groupe normal, ou sous-groupe distingué de façon tout à fait indistincte, comme on dit abélien et commutatif indifféremment. On dit plutôt *invariant* dans la théorie des représentations.

Propriété. ***(Caractérisations des sous-groupes normaux)***

Les conditions suivantes sont équivalentes :

(i) $H \triangleleft G$;

(ii) pour tout $a \in G$, $aHa^{-1} = H$ (H est son seul conjugué) ;

(iii) pour tout $a \in G$, $a^{-1}Ha = H$;

(iv) pour tout $a \in G$, $aH = Ha$;

(v) $\sim_d = \sim_g$;

(vi) la relation d'équivalence des classes à gauche modulo H est compatible avec la loi de groupe de G ;

(vii) il existe une loi $\diamond$ définie sur G/H telle que pour tous $a,b \in G$, $aH \diamond bH = (ab)H$.

▷ Les conditions *(ii)* et *(iii)* sont équivalentes, comme on a demandé au lecteur de le justifier précédemment. Cela vient de ce que $G = \{a^{-1} \mid a \in G\}$, la symétrisation étant une permutation dans un groupe. On établit facilement par double inclusion l'équivalence entre *(ii)* et *(iv)*. Pour établir l'équivalence de *(i)* et *(ii)*, il suffit de montrer l'implication $aHa^{-1} \subseteq H \implies aHa^{-1} = H$ pour tout a dans G. Elle est bien vraie, car l'inclusion $H \subseteq aHa^{-1}$ est toujours vraie si $aHa^{-1} \subseteq H$; en effet, si $h \in H$, alors cette hypothèse appliqué à a^{-1} donne $a^{-1}ha \in H$. On pose donc $h' = a^{-1}ha$ et dans ce cas $h = ah'a^{-1} \in aHa^{-1}$ (avouons qu'il faut avoir la tête reposée).

Les conditions *(v)* et *(vi)* sont équivalentes. En effet, si $\sim_d = \sim_g$, alors $\sim_g$ est compatible à gauche en tant que relation de classes à gauche mais également à droite puisqu'elle égale $\sim_d$; elle est donc compatible. Réciproquement, si $\sim_g$ est compatible, elle est compatible à droite et l'on peut prendre un sous-groupe H' dont elle est relation modulo à droite. Or on a vu dans la preuve que H' était la classe du neutre, et le neutre à gauche égale le neutre à droite dans un groupe, donc $H = H'$. D'autre part, l'équivalence *(vi)* $\iff$ *(vii)* est l'expression du théorème de factorisation : on a vu que l'unicité de la loi quotient était superfétatoire dans l'équivalence, et l'identité $aH \diamond bH = (ab)H$ exprime que la projection est un morphisme.

Il ne reste plus qu'à faire le lien entre ces deux groupes de propositions équivalentes. On le fait par *(iv)* $\iff$ *(v)*. Si les classes à gauche égalent les classes à droite pour le même élément, la partition par les classes à gauche et les classes à droite est la même, et donc définit la même relation d'équivalence, soit $\sim_d = \sim_g$. Réciproquement, si $\sim_d = \sim_g$ et $a \in G$, $aH = \overline{a}_{\sim_g} = \overline{a}_{\sim_d} = Ha$. ■

Remarque. Pour la loi $\diamond$, on a alors également pour tous $a,b \in G$,

$$aH \diamond bH = \{x \times y \mid x \in aH, y \in bH\}.$$

C'est très commode. Le lecteur avancé pourra remarquer que les classes à gauche sont aussi les orbites pour l'action de translation à droite de H sur G. Comme on appelle parfois *transversale* un système de représentants, une *transversale d'un sous-groupe* est une transversale de la relation d'équivalence des classes à gauche.

▷ Il faut et suffit donc de montrer : pour tous $a,b \in G$, $(ab)H = \{ahbh' \mid h,h' \in H\}$. Puisque H est distingué dans G, $Hb = bH$ donc cet ensemble se récrit $\{abhh' \mid h,h' \in H\}$. Or on vérifier par double inclusion facile que $H = \{hh' \mid h,h' \in H\}$ (l'une est la stabilité magmatique, l'autre la présence du neutre) et l'on peut récrire cet ensemble $(ab)H$, ce que l'on voulait. ■

Mise au point. Nous avons montré que les relations d'équivalences compatibles avoir la loi dans le cas des groupes étaient celles définies par classes modulo un sous-groupe, ce qui est spécifique à la catégorie des groupes et permet de reformuler les théorèmes de quotient. Avec la caractérisation précédente, on montre que la relation d'équivalence de classes à gauche est compatible si et seulement si le sous-groupe considéré est distingué. La conjonction de ses deux résultats permet de réduire l'étude des groupes quotients à celle des quotients par sous-groupes distingués. Étant donné $H \triangleleft G$, G/H est donc un groupe muni de la loi quotient et la projection canonique est un morphisme de groupes (et si H n'est pas normal, ces deux dernières propositions sont aussi infirmées).

Le schéma triangulaire de tout à l'heure peut donc se simplifier, mais dans le cas seul des sous-groupes distingués :

$$H \xhookrightarrow{\triangleleft} G \xrightarrow{\pi} G/H = H \backslash G$$

2.8.1.2 Sous-groupes distingués classiques et théorèmes opératoires

Les quelques propriétés suivantes, quoique capitales, ne sont pas essentielles. On peut donc se référer au chapeau de la section suivante sur les groupes quotients pour se clarifier l'esprit.

Exemples

1. **Les sous-groupes triviaux sont distingués** dans G. On peut donc noter $\{e\} \triangleleft G$ et $G \triangleleft G$. Les relations d'équivalence des classes latérales (classes à gauches, classes à droite) sont donc compatibles avec la loi de groupe, mais c'était facilement prévisibles, car ce sont respectivement (le re-vérifier) la relation d'égalité et la relation pleine, c'est-à-dire pour laquelle tous les points du groupe sont en relation.
   On en déduit que $G/G = \{g\}$ et que $G/\{e\} = \{\{g\} \mid g \in G\}$. Si l'on avait choisi de représenter les ensembles quotients par des systèmes de représentants (*confer* la remarque associée), on aurait eu $G/\{e\} = G$. Dans les deux cas, $[G : G] = \mathrm{card}(G)$ et $[G : \{e\}] = 1$.
2. Un
3. sous-groupe caractéristique est un sous-groupe qui soit un point fixe de l'action canonique de Aut sur G *(voir section sur les actions de groupe plus bas)*, autrement dit un sous-groupe stable par tout automorphisme de G. Puisque les automorphismes intérieurs sont des automorphismes, tout sous-groupe caractéristique est distingué. De surcroît, on peut aisément se convaincre que tout sous-groupe caractéristique d'un sous-groupe normal est normal dans l'absolu. La caractérisation est bien sûr transitive pour l'inclusion des sous-groupes.

Exercice 17

On considère Φ l'ensemble des sous-groupes de G et la relation $\triangleleft$ définie sur Φ. Montrer que c'est un relation réflexive antisymétrique partielle. Quelle est sa clôture transitive ? Est-ce un ordre total ?

Propriété. ***(Intercalation de distinction)***

Soient K un sous-groupe de H un sous-groupe de G. Si $K \triangleleft G$, alors $K \triangleleft H$.

▷ C'est une simple manipulation de la définition. ■

On donnera davantage de théorèmes d'opérations, qui sont peu nombreux. Pour l'instant, on peut retenir que **la distinction n'est pas transitive** mais que **tout sous-groupe intermédiaire dans une relation de distinction en induit une**. De plus, la distinction ne s'étend pas : en général, si $K \triangleleft H$, on n'a pas $K \triangleleft G$ (contre-exemple classique : $\{id, (1,2)(3,4)\}, \mathfrak{A}_4, \mathfrak{S}_4$).

Propriété. ***(Sous-groupes distingués d'un groupe commutatif)***

Tout sous-groupe d'une groupe commutatif est distingué dans ce groupe.

▷ La relation d'équivalence des classes à gauche a la même expression que celle des classes à droite, ce qui permet d'utiliser la caractérisation $\sim_d = \sim_g$. ■

Cette remarque ne rend pas caduque la notion de groupe quotient dans le cas commutatif, mais elle la simplifie considérablement : tous les sous-groupes sont des sous-groupes distingués ce qui permet de définir systématiquement la relation d'équivalence modulo ce sous-groupe de façon univoque. De plus, on avait que les compatibilités opératoires sont équivalentes aux compatibilités latérales, et de toute façon vraies par distinction.

Exemple

On considère le groupe $(\mathbb{Z}, +)$. Soit $n \in \mathbb{N}$, alors $n\mathbb{Z}$ est un sous-groupe additif de $\mathbb{Z}$. De plus, $n\mathbb{Z} \triangleleft \mathbb{Z}$ automatiquement puisque $(\mathbb{Z}, +)$ est commutatif. On peut donc définir le groupe quotient $\mathbb{Z}/n\mathbb{Z}$ de façon unique ; une classe (à gauche, mais le concept est exactement le même qu'à droite par commutativité) selon $n\mathbb{Z}$ est un élément de la forme $k + n\mathbb{Z}$ où $k \in \mathbb{Z}$, ce qui correspond bien aux classes de congruences déjà connues et à la description du cours : $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\}$. Ne pas confondre la notation $n\mathbb{Z}$, qui correspond au « H » des développements précédents, et le $k + H$ qui correspond au « aH » mais en notation additive.

Exercice 18

On appelle *groupe de Dedekind* un groupe dans lequel tout sous-groupe est distingué. On appelle *groupe hamiltonien* un groupe de Dedekind non abélien.

1. Pourquoi introduire le concept de groupe hamiltonien ?
2. Montrer que le groupe des quaternions, ou *groupe quaternionique*, $Q = \{1, -1, i, -i, j, -j, k, -k\}$, où les quatre premiers sont complexes et $i^2 = j^2 = k^2 = ijk = -1$, est hamiltonien. (Remarquer qu'alors, $ij = k$.)

Certains sous-groupes classiques généralement définis dans les groupes sont automatiquement distingués. On en voit quelques-uns.

Propriété. *(Distinction des centres)*

Le centre d'un groupe en est un sous-groupe distingué.

Ou, plus généralement, tout sous-groupe du centre d'un groupe est distingué. Dans la même veine : le centralisateur d'un sous-groupe en est un sous-groupe distingué.

▷ On peut plus fortement montrer qu'il est caractéristique. Le centre du groupe G est $\mathcal{Z}(G) = \{x \in G \mid \forall g \in G \quad gx = xg\} = \{x \in G \mid \forall g \in G \quad gx = xg\}$, l'ensemble des éléments du groupe qui commutent avec tous les autres ; on laisse au lecteur le soin de montrer que c'est bien un sous-groupe de G. Soit $\phi \in \mathrm{Aut}(G)$. Soit $x \in \mathcal{Z}(G)$. Soit $g \in G$. $g\phi(x)g^{-1} = \phi(t)\phi(x)\phi(t^{-1})$, car ϕ est un automorphisme donc surjectif. Par morphisme, on le récrit $g\phi(x)g^{-1} = \phi(txt^{-1}) = \phi(x)$, car x est central, ce qui conclut. ■

Propriété. ***(Distinction des cœurs)***

Le cœur d'un sous-groupe d'un groupe est un sous-groupe distingué de ce dernier.

▷ Pour un sous-groupe H de G, son cœur dans G est $cr_G(H) = H_G = \bigcap_{g\in G} gHg^{-1}$; on laisse au lecteur le soin de montrer que c'est bien un sous-groupe de G. Il est contenu dans H, car cette intersection est contenue dans son terme pour $g = e$ qui est H. Montrons maintenant la distinction dans G, dont découle par ailleurs la distinction dans H. Soit $a \in H$. Alors :

$$\begin{aligned} aH_Ga^{-1} = a\bigcap_{g\in G} gHg^{-1}a^{-1} & \\ &= \{ata^{-1} \mid t \in \bigcap_{g\in G} gHg^{-1}\} \\ &= \{ata^{-1} \mid t \in G, \forall g \in G \quad t \in gHg^{-1}\} \\ &= \{ata^{-1} \mid t \in G, \forall g \in G \quad t \in agHg^{-1}a^{-1}\} \\ &= \{t \in G \mid \forall g \in G \quad t \in gHg^{-1}\} \\ &= \bigcap_{g\in G} gHg^{-1}. \end{aligned}$$

L'avant-dernière égalité vient de ce que $(g \longmapsto ag) \in S(G)$. Ainsi $H_G \triangleleft G$. ■

On peut définir plus généralement le cœur d'une partie d'un groupe. Le cœur d'un sous-groupe est doté de propriétés encore meilleures[1].

Enfin, un exemple de haute importance, puisqu'on va voir dans la suite qu'il donne exactement les sous-groupes distingués. C'est par lui que nous formulerons en particulier le théorème de factorisation pour les groupes.

Propriété. ***(Distinction des noyaux)***

Le noyau d'un morphisme de groupe est un sous-groupe distingué du groupe de départ.

▷ On le vérifie très aisément : si $x \in \mathrm{Ker}(f)$ un morphisme de G dans G' deux groupes quelconques, si $g \in G$, alors $f(gxg^{-1}) = f(g)f(x)f(g^{-1}) = f(g)e_{G'}f(g^{-1}) = f(g)f(g^{-1}) = f(gg^{-1}) =$

[1] Quelques suppléments intéressants. D'abord, remarquons que le cœur d'un sous-groupe H de G contient tous les sous-groupes que H qui sont normaux dans G ; en effet, si K est un sous-groupe de H normal dans G, si $g \in G$, $K = gKg^{-1} \subseteq gHg^{-1}$ donc $K \subseteq H_G$. C'est donc le plus grand sous-groupe normal dans G contenu dans H au sens de l'inclusion.

Théorème. ***(Structure du quotient par le cœur)***

Soit H un sous-groupe quelconque de G. Alors G/H_G est isomorphe à un sous-groupe de $S(G/H)$.

▷ On opère à gauche sur G/H par $(g,X) \longmapsto gX$. Le noyau de cette action est le cœur de H dans G. Ainsi, d'après le théorème de factorisation pour les groupes, son quotient est injectif. Sa co-restriction est donc un isomorphisme sur un sous-groupe de $S(G/H)$. ■

$f(e_G) = e_{G'}$, donc $\mathrm{Ker}(f)$ est stable par automorphismes intérieurs soit $\mathrm{Ker}(f) \triangleleft G$. ■

Exemples. ***(Noyaux distingués)***

1. On retrouve que les centres sont distingués en tant qu'intersection des noyaux de tous les automorphismes intérieurs de G.
2. $SL_n(\mathbb{K}) = \mathrm{Ker}(\det) \triangleleft GL_n(\mathbb{K})$ où $(\mathbb{K}, +, \times)$ est corps commutatif ; de même pour un espace vectoriel de dimension finie ;
3. $\mathcal{SO}_n = \mathrm{Ker}(\det) \triangleleft \mathcal{O}_n(\mathbb{R})$ (bien sûr le morphisme déterminant n'est plus défini sur le même groupe) ; de même pour un espace vectoriel réel de dimension finie ;
4. $SU_n = \mathrm{Ker}(\det) \triangleleft U(n)$; de même pour un espace vectoriel complexe de dimension finie ;
5. $\mathfrak{A}_n = \mathrm{Ker}(\varepsilon) \triangleleft \mathfrak{S}_n$; de même pour les permutations d'un ensemble fini.
6. On se souvient que si K est un sous-groupe de H, et $K \triangleleft G$, alors $K \triangleleft H$. N'allez pas pourtant écrire que la première propriété découle de $SL_n(\mathbb{K}) \triangleleft \mathfrak{M}_n(\mathbb{K})$, ce qui n'a aucun sens puisque $\mathfrak{M}_n(\mathbb{K})$ n'a pas de structure de groupe. Pour plus d'informations, appelez l'exercice de la section complémentaire sur le sujet.

Exemples. ***(Sous-groupes distingués)***

1. On considère $G = \mathfrak{S}_3$ et $H = \langle\sigma\rangle = \{1, \sigma, \sigma^2\}$ où $\sigma = (1,2,3)$. On a que H est distingué dans G puisqu'il est d'indice 2. Alors :

$$H \simeq \mathbb{Z}/3\mathbb{Z} \text{ et } G/H \simeq \mathbb{Z}/2\mathbb{Z}$$

   mais G n'est pas abélien.
2. Soient $G = \mathfrak{S}_4$, H son sous-groupe alterné et $K = \{id, (1,2)(3,4)\}$. Alors K est clairement un sous-groupe de H, puisque $((1,2)(3,4))^2 = id$, et le produit de deux transpositions est pair. Alors on sait que H est distingué dans G. De même, K est distingué dans H ; on peut le vérifier à la main en remarquant que toute permutation paire du groupe alterné d'ordre 4 est le produit de deux transpositions. Puisque pour les éléments de K, c'est évident, on a jamais que 10 petites choses à vérifier. Pourtant, K n'est pas distingué dans G : $(1,3)(1,2)(3,4)(1,3)$ fait correspondre 1 à 4, ce qui n'est le cas d'aucun des deux éléments de K.

On a cette dernière caractérisation des sous-groupes normaux, moins pratique, mais qui donne une première importance aux Ker parmi les sous-groupes.

Propriété. ***(Caractérisation de la normalité par noyaux)***

Un sous-groupe d'un groupe est distingué si et seulement si c'est le noyau d'un morphisme de groupes.

▷ On a déjà vu dans la propriété précédente la proposition réciproque. Soit maintenant $H \triangleleft G$. Alors le groupe quotient G/H est défini de manière univoque et c'est bien un groupe. On pose $\pi : G \longrightarrow G/H$ le morphisme projection canonique. Alors $\mathrm{Ker}(\pi) = \{x \in G \mid \pi(x)\} = \overline{x} = \overline{e}\} = \{x \in G \mid x \in \overline{e} = H\} = H$. ■

Exercice 19

(Groupe dérivé) On appelle *groupe dérivé* d'un groupe, le groupe engendré par les commutateurs d'éléments de G (on dit qu'un élément est commutateur s'il s'écrit sous la forme $aba^{-1}b^{-1}$ où a,$b \in G$). Montrer que le groupe dérivé est caractéristique et que c'est le plus petit sous-groupe normal au sens de l'inclusion pour lequel le groupe quotient est abélien. *Ce groupe quotient est appelé l'abélianisé de G.*

Pour clore cette partie, quelques théorèmes opératoires sur la normalité, dont on rappelle le caractère intrinsèque.

Exercice 20

Soit H sous-groupe normal de G. Donner un sous-groupe de H ni normal dans G, ni normal dans H.

Propriété. ***(Intersection de sous-groupes normaux)***

Une intersection quelconque de sous-groupes normaux est sous-groupe normal.

▷ On considère G un groupe et $(G_i)_{i\in I}$ une famille quelconque de ses sous-groupes distingués. Il n'est pas forcé de distinguer le cas I vide, quoique évident. Soit $x \in \bigcap_{i\in I} G_i$. Soit $g \in G$. Pour tout $i \in I$, $x \in G_i$ donc $gxg^{-1} \in G_i$ par distinction de G_1 donc $gxg^{-1} \in \bigcap_{i\in I} G_i$ et c'est terminé. ■

Remarque. La borne inférieure pour l'ordre inclusif étant l'intersection, on peut donc définir le sous-groupe distingué engendré par une partie d'un groupe, comme l'intersection de tous les sous-groupes distingués contenant cette partie. C'est exactement le même raisonnement que pour un sous-groupe engendré, une tribu engendré, un sous-espace vectoriel engendré, l'adhérence d'une partie d'un espace topologique... Le phénomène général est seulement lié à la stabilité par intersection : si un truc est stable par intersection quelconque, alors on peut définir le truc engendré par un machin.

Exercice 21

Que dire d'une réunion de sous-groupes normaux ?

Propriété. ***(Génération par des sous-groupes normaux)***

Un sous-groupe engendré par une famille quelconque de sous-groupes normaux est sous-groupe normal.

▷ Soit $(G_i)_{i\in I}$ une famille quelconque de groupes normaux dans G. Soit H le groupe généré par elle. Soit $x \in H$: $x = a_1...a_n$ avec les a_i dans les G_j. Si $g \in G$, $gxg^{-1} = ga_1...a_ng^{-1} = (ga_1g^{-1})(ga_2g^{-1})(ga_3...g^{-1})(ga_ng^{-1})$, car $gg^{-1} = e$. Or chacun des termes ainsi parenthésés de ce produit est dans l'un des G_j puisque ceux-ci sont normaux. Le produit est donc dans le groupe généré par eux, ce qui conclut. ■

Exercice 22

Que dire du produit direct de deux sous-groupes normaux ?

Exercice 23

Quel est le sous-groupe normal engendré par les $(i,i+2)$ dans $\mathfrak{S}_{2n+1}$?

Exercice 24

Montrer que si H_1, H_2 sont deux sous-groupes normaux de G, H_1H_2 est normal dans G. La normalité d'un seul suffit-elle ?

Propriété. ***(Image directe d'un sous-groupe normal par un morphisme)***

Soient G,G' deux groupes munis de lois quelconques et f un morphisme de G dans G'. Si H est distingué dans G, alors $f(H)$ est distingué dans $f(G)$.

▷ Soit $y \in f(H)$, d'où $y = f(x), x \in G$ et $g \in f(G)$. Dans ce cas $g = f(t), t \in G$ et $g^{-1} = f(t^{-1}$. Alors $gyg^{-1} = f(t)f(x)f(t^{-1} = f(txt^{-1})$ par morphisme. Mais H est distingué dans G donc $txt^{-1} \in H$, d'où $gyg^{-1} \in f(H)$ ce qui termine la preuve. ■

Remarque. C'est faux si l'on remplace $f(G)$ par G' dans la proposition précédente. On laisse le lecteur faire l'effort fort formateur de produire un contre-exemple.

Propriété. ***(Image réciproque d'un sous-groupe normal par un morphisme)***

Soient G, G' deux groupes munis de lois quelconques et f un morphisme de G dans G'. Si H est distingué dans $f(G)$, alors $f^{-1}(H)$ est distingué dans G.

▷ Soit $x \in f^{-1}(H')$. Soit $g \in G$. Alors $f(gxg^{-1}) = f(g)f(x)f(g^{-1})$ par morphisme. Mais $f(x) \in H'$ par hypothèse et $f(g) \in f(G)$ donc comme H' est normal dans $f(G)$, ce triple produit appartient encore à H'. ainsi $gxg^{-1} \in f^{-1}(H')$, ce qui termine la preuve. ■

Exercice 25

Montrer que pour tout $n \in \mathbb{N}^*$, un groupe de type fini, c'est-à-dire généré par une partie finie, n'a qu'un nombre fini de sous-groupes normaux d'indice n.

Propriété. ***(Distinction par un conjugué du sous-groupe)***

Soit H un sous-groupe de G. H est distingué dans G si et seulement l'un de ses conjugués est distingué dans G.

▷ Et même si et seulement si tous ses conjugués sont distingués dans G. (Un conjugué d'un sous-groupe H est un sous-groupe gHg^{-1}, parfois noté H^g, pour un élément g de G donné.) En effet, on traite l'équivalence en se rappelant la caractérisation : un sous-groupe est distingué si et seulement s'il est son seul conjugué. De plus, H fait partie de ses conjugués par l'action de e. ■

Exercice 26

On appelle *sous-groupe normal minimal*, un élément minimal pour l'inclusion de l'ensemble des sous-groupes normaux non triviaux de G. On rappelle qu'un élément minimal d'un ensemble ordonnée $(E, \leq)$ est un élément m tel que $\forall x \in E \quad (x \leq m \implies x = m)$. Montrer que tout groupe fini non trivial admet au moins un sous-groupe normal minimal. Que dire dans un groupe quelconque ? Discuter le cas des sous-groupes normaux maximaux.

2.8.1.3 Sous-groupe d'indice 2

Propriété. ***(Distinction des sous-groupes d'indice 2)***

Tout sous-groupe d'indice 2 d'un groupe quelconque est distingué.

▷ On a $G = H \sqcup gH$ pour n'importe quel $g \notin H$. De même à droite, $G = H \sqcup Hg$. Ainsi $gH = GpriveH = Hg$, donc H est distingué dans G ; en effet, si $g \in H$, alors $gH = H = Hg$. ■

Propriété. ***(Règle des signes dans les sous-groupes d'indice 2)***

Tout sous-groupe d'indice 2 d'un groupe respecte la règle des signes, autrement dit, en notant G notre groupe, H un sous-groupe d'indice 2 et $K = GpriveH$, on a :

- $\star$ $\forall x,y \in H \quad xy \in H$;
- $\star$ $\forall x \in H, y \in K \quad xy \in K$;
- $\star$ $\forall x,y \in K \quad xy \in K$.

▷ La première propriété découle de la définition de sous-groupe. La seconde est universelle à tout sous-groupe, on la laisse vérifier au lecteur. Pour la dernière, on a $K = x^{-1}H$ pour tout $x \in K$, car $x^{-1} \in K$. En effet, $G = H \sqcup xH$. Ainsi, pour tout $y \in K$, $y = x^{-1}h$ pour un $h \in H$, donc $xy = h \in H$. ■

Remarque. On retrouve alors que tout sous-groupe d'indice 2 est distingué.

Exemples. *(Groupes d'indice 2)*

1. Le sous-groupe alterné d'ordre n vérifie la règle des signes dans $\mathfrak{S}_n$.
2. Le groupe spécial orthogonal d'ordre n vérifie la règle des signes dans $\mathcal{O}_n(\mathbb{R})$.

2.8.2 Groupes quotients

On peut, avec toutes les considérations précédentes, fixer les notations du cadre le plus général possible : on prend $(G, \times)$ un groupe et H un sous-groupe distingué dans G. On note $\mathcal{R}$ la relation d'équivalence des classes à gauche modulo H, aussi notée $\equiv$ et appelée congruence modulo H ; dans ce cas, $G/\mathcal{R} = G/H$, et c'est le même ensemble si l'on avait pris les classes à droite, ce qui permet de noter aussi $\overline{G}$ ou $\frac{G}{H}$. De plus, la projection canonique π est un morphisme d'après la section précédente sur les magmas. Muni de la loi quotient, que l'on note multiplicativement, G/H a la structure de groupe. Son élément neutre est $\overline{e} = eH = H$ et si aH est un élément de G/H, où l'on a pris $a \in G$, son inverse est $a^{-1}H$: on peut le reformuler en voyant que $a^{-1}H \cdot aH = (aa^{-1})H = eH = H$ et de même $aH \cdot a^{-1}H = H$. Enfin, ce cadre est justifié par ce qu'il n'existe de groupe quotient (pour lequel la projection canonique soit quotient, ce que l'on veut à chaque fois) que si la relation d'équivalence considérée est compatible avec la loi de groupe, et ces relations sont exactement les relations de classes, indifféremment prises à gauche ou à droite, modulo les sous-groupes distingués.

Exercice 27

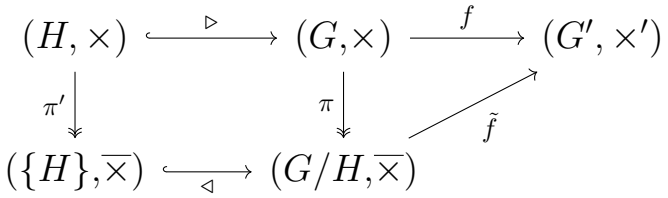
Test : quelles sont les parties X de G telles que G/X, muni de la loi quotient, soit un groupe ?

Pour clarté mentale, on énonce le théorème de factorisation établi plus haut en exercice avec sa formulation nouvelle.

Propriété. *(Théorème de factorisation pour les groupes, version mal dite)*

Soit f un morphisme de groupes de G dans G' un autre groupe quelconque muni d'une loi passée sous silence. Alors l'application f est compatible avec la congruence modulo H si et seulement s'il existe un unique morphisme $\tilde{f}$ tel que $f = \tilde{f} \circ \pi$ (se qui se réécrit $f(g) = \tilde{f}(\overline{g})$ pour tout $g \in G$). Dans ce cas de compatibilité, on dit toujours qu'on *passe au quotient* dans le morphisme f.

▷ Normalement, c'est déjà fait. ■



Dans le diagramme ci-dessous, l'application π', inutile, est la restriction à H de π. Elle est donc constamment égale à $H = \overline{e} = \overline{h}$ pour tout $h \in H$. Le groupe en bas à gauche est distingué dans le groupe quotient puisque c'est son sous-groupe trivial.

Exercice 28

(Insolite) π' peut-elle être la dérivée de π ?

Propriété

Si G est un groupe abélien et $H \triangleleft G$, G/H est abélien.

▷ C'est une conséquence directe de l'expression de la loi quotient établie en remarque précédemment : pour tous $a,b \in G$, $aH \cdot bH = (ab)H = (ba)H = bH \cdot aH$. ■

Propriété. *(Monogénéité du groupe quotient)*

Si G est un groupe monogène et $H \triangleleft G$, G/H est monogène.

▷ Il s'agit simplement de remarquer que le caractère de générateur est conservé par passage à la structure quotient ; c'est au lecteur de le vérifier. ■

Remarque. Plus généralement : si g génère G, $\overline{g}$ génère G/H ; si G est généré par A, G/H est généré par $\pi(A)$; en particulier, si G est de type fini, G/H également.

Propriété. *(Cyclicité du groupe quotient)*

Si G est un groupe cyclique et $H \triangleleft G$, G/H est cyclique.

▷ Puisqu'un groupe est cyclique si et seulement s'il est monogène et fini, par rapport à la propriété précédente, il n'y a qu'à justifier que le groupe quotient est également fini si G est fini. C'est le cas, par surjectivité de la projection canonique, $\mathrm{card}(G/H) \leqslant \mathrm{card}(G) < \infty$. ■

Remarque. Plus généralement : si G est fini, G/H est fini, de cardinal inférieur. Peut-être doit-on rappeler que, dans tous les cas, fondamentalement, $\mathrm{card}(E/\mathcal{R}) \leqslant \mathrm{card}(E)$, et donc si E est fini, tout quotient de E est également fini. De plus, il y a égalité des cardinaux, dans le cas fini, si et seulement si $\mathcal{R}$ est l'égalité de E.

Théorème. ***(Commutativité d'un groupe quotient)***

Un groupe quotient selon un groupe distingué est commutatif si et seulement si celui-ci contient tous les commutateurs.

▷ Voir l'exercice sur les groupes dérivés de la partie précédente. ■

Exercice 29

Soit $n \neq 4$. Quels sont les sous-groupes distingués des $\mathfrak{S}_n$?

Après ces quelques remarques structurelles, il est temps de passer aux choses sérieuses. On introduit un groupe $(G', *)$.

Théorème. ***(Théorème de factorisation pour les groupes)***

Soit f un morphisme de groupes de G dans G'. H est dans $\mathrm{Ker}(f)$ si et seulement s'il existe un unique morphisme $\tilde{f}$ tel que $f = \tilde{f} \circ \pi$ (se qui se réécrit $f(g) = \tilde{f}(\overline{g})$ pour tout $g \in G$).

▷ D'abord, la condition $H \subseteq \mathrm{Ker}(f)$ équivaut à la compatibilité de f avec la relation d'équivalence des classes à gauche, c'est-à-dire : $\forall a,b \in G \quad a^{-1}b \in H \implies f(a) = f(b)$. En effet, si f est un morphisme, $\forall x \in H \implies \mathrm{Ker}(f) \iff \forall a^{-1}b \in H \; f(a^{-1}b) = e_{G'}$: les éléments de H sont exactement les éléments de la forme $a^{-1}b$ qui sont dans H, équivalence logique qui se montre aisément comme on a déjà pu le faire, et $f(a^{-1}b) = e_{G'} \iff f(a)^{-1}f(b) = e_{G'} \iff f(a) = f(b)$. C'est donc une reformulation du théorème de factorisation. ■

Exercice 30

Donner un exemple de cas où un sous-groupe distingué n'est pas inclus dans le noyau.

Exercice 31

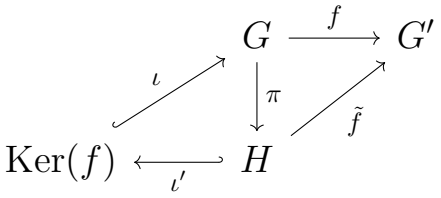
Peut-on trouver un contre-exemple où le sous-groupe n'est pas distingué, et où il y aurait factorisation sans inclusion dans le noyau ?

Exercice 32

Dans le théorème précédent, montrer que :

1. $\mathrm{Ker}(\tilde{f}) = \mathrm{Ker}(f)/H$ et $\tilde{f}$ est injective si et seulement si $H = \mathrm{Ker}(f)$;
2. $\mathrm{Im}(\tilde{f}) = \mathrm{Im}(f)$ et $\tilde{f}$ est surjective si et seulement si f est surjective ;
3. $\tilde{f}$ est un isomorphisme si et seulement si f est surjective et $H = \mathrm{Ker}(f)$.

Une illustration du théorème de factorisation.



Méthode. ***(Recette pour passer au quotient dans les morphismes de groupes)***

1. Je vérifie que je dispose de deux groupes G, G', d'un morphisme f entre les deux, et d'un sous-groupe H du groupe de départ G.
2. **Je vérifie que H est distingué dans G.** J'en déduis cette affirmation, que le quotient existe dans toute sa splendeur d'ensemble quotient univoquement défini par une relation de congruence et a la structure de groupe.
3. **Je vérifie maintenant que H est inclus dans $\mathrm{Ker}(f)$.** Si je veux, pour crâner, je précise que c'est une condition nécessaire et suffisante à la compatibilité de f avec la congruence, car je connais même la preuve de mon théorème de factorisation sur les groupes.
4. Je peux maintenant définir un morphisme $= \tilde{f} : G/H \longrightarrow G'$ sans trouble, telle que pour tout $\overline{g} \in G/H$, $\tilde{f}(\overline{g}) = f(g)$, et j'insiste bien sur ce que cette construction n'est possible que grâce aux deux hypothèses vérifiées précédemment.

i je veux une propriété d'injectivité, de surjectivité, voire de bijectivité pour mon application, je me réfère aux résultats habituels que nous avons déjà vus.

Exercice 33

Expliquer pourquoi, pour tout morphisme d'un groupe G dans un groupe abélien G', on peut le factoriser en un morphisme de l'abélianisé de G dans G'.

Exercice 34

(Rigolo) Soient H, K deux sous-groupes d'un groupe. Montrer que $HK = KH$ si et seulement si $H = K$ ou $H = -K$.

Maintenant, nous énonçons les trois théorèmes d'isomorphisme pour les groupes qui sont l'adaptation du théorème d'isomorphisme pour la structure magmatique, dont découle ensuite deux corollaires. On peut avoir à l'esprit que c'en sont toujours des cas particuliers.

Avec eux, nous retrouvons des « règles de calcul », avec lesquelles il faut bien sûr être toujours très prudent de ne pas écrire d'absurdités, mais qui rendent la notion de quotient bien plus intuitive qu'elle ne l'a été depuis une vingtaine de pages : on fait le quotient de groupes par des groupes, même si ce doivent être des sous-groupes, et distingués, et ils présentent des

isomorphismes à la place des identités algébriques élémentaires des petites classes.

Théorème. ***(Premier théorème d'isomorphisme)***

Soit f un morphisme de groupes de G dans G', deux groupes quelconques. Alors $\mathrm{Ker}(f)$ est distingué dans G et $G/\mathrm{Ker}(f)$ est isomorphe à $\mathrm{Im}(f)$. Plus précisément, il existe un unique isomorphisme de groupes qui pour tout élément de x de G, applique la classe de x selon $\mathrm{Ker}(f)$ sur $f(x) \in \mathrm{Im}(f)$.

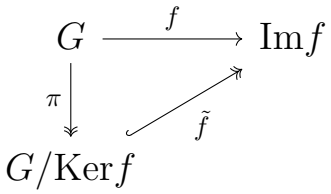
▷ Tout est déjà fait, et l'on voit que c'est la formulation du théorème d'isomorphisme pour les magmas, pour les groupes. L'isomorphisme est bien sûr la corestriction du morphisme quotient $\tilde{f}$, et tout cela est possible, car $\mathrm{Ker}(f)$ est distingué. On peut voir que l'injectivité vient de ce que $\mathrm{Ker}(\tilde{f})$ est $\mathrm{Ker}(f)$ (pourquoi ?) qui est l'élément neutre du groupe quotient $G/\mathrm{Ker}(f)$, ce qui caractérise l'injectivité pour les morphismes. ■

Ce théorème est fondamental ; sa preuve n'est pas pour autant compliquée, comme on demande de s'en rendre compte dans l'exercice suivant : la longueur relative des développements faits, l'accumulation des concepts et du vocabulaire, ne doit pas occulter que ce résultat n'a que l'apparence de l'écueil. L'empêtrement précédent n'est dû qu'à la volonté d'exhaustivité, quitte à étudier ce qui n'est pas fondamental. Nous pensons que le lecteur saura voir ce qui l'est.

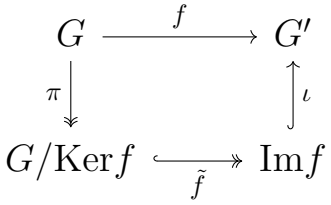
Exercice 35

Redémontrer le théorème d'isomorphisme calmement, en allant droit au but.

Voilà en images le premier théorème d'isomorphisme.



On trouve parfois la précision suivante, ι étant l'injection canonique qui retranscrit une inclusion. Le symbole ι pour une injection canonique est très classique.



Exercice 36

Montrer que, H étant un groupe quelconque, il existe un homomorphisme surjectif de G sur H si et seulement si H est un quotient de G (c'est-à-dire : H est isomorphe à un quotient de G).

Exercice 37

Soit f un morphisme de groupes de G dans G'. On suppose que G est de cardinal fini. On veut montrer que $\text{card}(G) = \text{card}(\text{Ker}(f)).\text{card}(\text{Im}(f))$; en particulier, l'ordre de $\text{Im}(f)$ divise l'ordre de G, ce que ne fournit pas le théorème de Lagrange.

1. Déduire ce résultat du théorème d'isomorphisme.

2. Le redémontrer naïvement grâce au lemme des bergers.

D'après le théorème d'isomorphisme, nous avons donc l'opportunité, dans tous les cas, d'exhiber un groupe isomorphe à un groupe quotient donné G/H. En effet, tout sous-groupe distingué (ici H) est le noyau d'un morphisme de groupe f, et en appliquant le théorème d'isomorphisme, on obtient que G/H est isomorphe à $\text{Im}(f)$.

Exercice 38

1. Donner un groupe facile isomorphe à $GL_n(\mathbb{K})/SL_n(\mathbb{K})$.

2. Donner un groupe facile isomorphe à $\mathcal{O}_n(\mathbb{R})/\mathcal{SO}_n$.

3. Donner un groupe facile isomorphe à $\mathfrak{S}_n/\mathfrak{A}_n$.

4. Donner des groupes faciles isomorphes à $\mathbb{R}/\mathbb{Z}$, sa torsion *(voir ci-bas)*, puis $\mathbb{R}/\mathbb{Q}$.

5. À quel groupe est isomorphe $G/\mathcal{Z}(G)$?

Exercice 39

Un exemple récréatif, les groupes de torsion : un élément d'un groupe est dit *de torsion* s'il est d'ordre fini ; la *torsion* d'un groupe est l'ensemble de ses éléments de torsion.

1. Montrer que la torsion d'un groupe abélien en est un sous-groupe. Donner un contre-exemple dans le cas non commutatif.

2. Donner un exemple de groupe *sans torsion*, c'est-à-dire dont la torsion est réduite au neutre.

3. Quelle est la torsion de $\mathbb{R}/\mathbb{Z}$?

4. Un *groupe de torsion* est un groupe égal à sa torsion. Donner un exemple de groupe de torsion infini.

Exercice 40

On considère le *tore rationnel* $\mathbb{Q}/\mathbb{Z}$.

1. Montrer que le tore rationnel est de torsion.

2. Quels sont les éléments d'ordre d du tore rationnel.

▷ **Éléments de réponse.**

Il est clair que le tore rationnel est de torsion d'après l'exercice précédent. On montre aisément que les éléments d'ordre d de $\mathbb{Q}/\mathbb{Z}$ sont les $\frac{n}{d}+\mathbb{Z}$ où $n \in \mathbb{Z}$.

Exercice 41

Soit H un sous-groupe distingué de G et X une partie de G. Soit K un sous-groupe de G contenant H.

1. Montrer que $\pi^{-1}(\pi(X)) = XH$.

2. Montrer que $\pi^{-1}(\pi(K)) = K$.

Nous énonçons à présent le théorème de correspondance, résultat intermédiaire aux théorèmes d'isomorphisme, très riche puisque composé de beaucoup de propositions. Nous préférons le donner dans sa forme complexe classique plutôt que d'en délier les parties, avec la contrepartie d'enjoindre le lecteur de s'y attarder pesamment ainsi que sa preuve.

Théorème. ***(Théorème de correspondance)***

Soit H un sous-groupe distingué de G. Alors $K \longmapsto K/H$ définit une bijection de l'ensemble des sous-groupes de G contenant H sur l'ensemble des sous-groupes de G/H ; elle applique les sous-groupes normaux de G contenant H sur les sous-groupes normaux de G/H ; elle est croissante pour l'inclusion, de réciproque également croissante, préserve l'indice, et enfin, A est normal dans B si et seulement si l'image de A est normale dans l'image de B.

▷ Procédons point par point.

⋆ On considère l'application $K \longmapsto K/H$ définie sur E l'ensemble des sous-groupes de G contenant H. Soit K un sous-groupe de G contenant H, H étant distingué dans G. Alors la propriété d'intercalation de sous-groupe distingué donne que H est distingué dans K, donc K/H existe, et c'est un sous-groupe de G/H : en effet, la loi sur K/H est induite de celle sur G/H, car si a,$b \in K$ ont peut classes deux éléments aH, bH, ce sont des éléments de G qui ont pour classes ces mêmes. L'application est donc bien à valeurs dans F l'ensemble des sous-groupes du groupe quotient.

⋆ On peut donner une autre expression à cette application : c'est tout simplement π, l'application projection qui est définie sur l'ensemble des parties de G (pour toute application de E dans F, on peut canoniquement définir une application de $\mathcal{P}(E)$ dans $\mathcal{P}(F)$). Comme c'est au sens strict du terme, une autre application, nous la notons Π. Vérifions que si G' est un sous-groupe de G contenant H, alors $\Pi(G') = \pi(G') = \{\overline{x} \mid x \in G'\} = G'/H$. C'est en fait immédiat, car l'ensemble défini précédemment est G'/H par surjection de la projection canonique (et on rappelle bien que le point précédent nous donne la possibilité de parler de groupe quotient pour la congruence modulo H, pour G').

Remarque. Dans la littérature, on voit $\Pi(G') = \overline{G'}$. Cette notation est tout à fait licite, car la barre supérieure est l'une des notations (notation infixe) de la projection canonique.

Cependant, nous sommes convaincus que c'est un pas en arrière dans la compréhension du concept : la quantité $\pi(G')$ est une image directe et non pas l'image de G' par une application, mais nous pouvons définir l'application Π sur une partie de l'ensemble des parties de G, en l'occurrence l'ensemble des sous-groupes contenant H, et dans ce cas $\pi(G')$ désigne aussi, incidemment, l'image d'un élément par une application, Π. Il est également très important que comprendre que Π n'est pas un morphisme, il n'est pas même défini sur une structure algébrique !

- ⋆ Montrons que l'application Π est une bijection ; pour cela, on exhibe sa bijection réciproque Φ qui à tout sous-groupe de G/H, prenons en un G', envoie $\pi^{-1}(G')$, qui est un sous-groupe de G contenant H. En effet, si $h \in H$, alors $\pi(h) = \overline{e}$ est le neutre de G/H qui appartient à G' puisque c'est un sous-groupe, donc $\pi^{-1}(G')$ contient H. La structure de groupe vient de celle d'image réciproque par un morphisme. Montrons que $\Pi \circ \Phi = id_F$ et que $\Phi \circ \Pi = id_E$.
  - ⁕ Soit G' un sous-groupe de G contenant H. L'inclusion $G' \subseteq \pi^{-1}(\pi(G'))$ est vérifiée pour toute partie de G' quelle que soit même π, soit $G' \subseteq \Phi \circ \Pi(G')$. Montrons l'inclusion réciproque. Soit $x \in \pi^{-1}(\pi(G'))$, c'est-à-dire tel que $\pi(x) = \overline{x} \in \pi(G')$. Cela signifie qu'il existe $x' \in G'$ tel que $pi(x) = p(x')$. Mais d'après un résultat anonyme que l'on a pris soin de rappeler en même temps que la notion de relation d'équivalence, on a donc $x \sim x'$, soit $xx'^{-1} = h \in H$. Ainsi $x = hx'$ produit de deux éléments de G', car H est dans G', donc x est dans G'. On en déduit $G' = \pi^{-1}(\pi(G'))$ pour tout G' dans E, d'où $\Phi \circ \Pi = id_E$.
  - ⁕ Soit B un sous-groupe de G/H. Il est connu (puisqu'on a demandé au tout début de revoir les bases sur les ensembles, et notamment sur les opérations entre images et images réciproques) que puisque π est surjective, l'égalité $B = \pi \circ \pi^{-1}(B)$ est vérifiée pour en fait n'importe quelle partie de B. On a donc $\Pi \circ \Phi = id_F$. Ceci conclut pour la bijectivité de Π, de bijection réciproque Φ.
- ⋆ Justifions que Π est un isomorphisme d'ensembles ordonnés, c'est-à-dire une bijection croissante dont la réciproque est également croissante, pour les ordres partiels d'inclusion sur E et F. Avec l'expression de Π par π et de Φ par π^{-1}, c'est une propriété de cours : en effet, image et image réciproque sont deux applications croissantes sur les ensembles de parties du départ et de l'arrivée. C'est inchangé par restriction et corestriction.
- ⋆ Vérifions que Π préserve l'indice, c'est-à-dire que l'indice de A dans B est l'indice de $f(A)$ dans $f(B)$. D'abord, ceci a du sens, car $\Pi(A) = A/H$ et $\Pi(B) = B/H$ sont des images de groupes par le morphisme π donc des groupes, et $\Pi(A) \subseteq \Pi(B)$ donc $\Pi(A)$ est un sous-groupe $\Pi(B)$[1]. Il s'agit de montrer que $[B/H : A/H] = [B : A]$, c'est-à-dire que $\text{card}\left(\frac{A/H}{B/H}\right) = \text{card}\left(\frac{A}{B}\right)$. C'est une conséquence du troisième théorème d'isomorphisme, puisque $\frac{A/H}{B/H}$ et $\frac{A}{B}$ sont isomorphes donc en particulier ils ont le même cardinal ; on laisse le soin au lecteur de vérifier que le troisième théorème d'isomorphisme n'utilise pas de résultat découlant de cette affirmation.
- ⋆ Montrons que pour tous A,B sous-groupes de G contenant H, $\Pi(A) = \pi(A) = A/H$ est normal dans $\Pi(B) = \pi(B) = B/H$ si et seulement si A est normal dans B. D'une part, si

[1] Rappelons que, pour définir l'indice, il n'y a besoin que de la structure de sous-groupe et pas forcément de sous-groupe distingué, car de toute manière, l'indice à gauche et l'indice à droite coïncident.

$A \triangleleft B$, alors si $x \in B/H$, si $a \in A/H$, $xax^{-1} \in A/H$; pour s'en convaincre, il suffit d'écrire ces classes comme des représentants et tout s'illumine. D'autre part, si $A/H \triangleleft B/H$, alors si $a \in A$ et $x \in B$, $xax^{-1} \in A$. En effet, de même que précédemment, en passant aux classes, $\overline{xax^{-1}} = \overline{x}.\overline{a}.\overline{x^{-1}} \in A/H$ par distinction, d'où $a \in A$ par définition.

⋆ Nous devons enfin justifier que la restriction de l'application aux sous-groupes normaux dans G a pour image l'ensemble des sous-groupes normaux de G/H. D'une part, si G' (contenant H toujours) est normal dans G, alors $f(G')$ est normal dans $f(G) = G/H$ par surjectivité. D'autre part, si un sous-groupe B de G/H en est un sous-groupe distingué, alors par surjectivité il existe G' dans G contenant H un sous-groupe (c'est-à-dire un élément de E) tel que $\Pi(G') = B$, et $\Pi(G')$ est normal dans $\Pi(G) = G/H$ donc d'après l'équivalence du paragraphe précédent, G' est normal dans G, et il contient H. Ainsi Π envoie l'ensemble des sous-groupes normaux de G contenant H sur l'ensemble des sous-groupes normaux de G/H exactement ; cette restriction et corestriction est donc bien évidemment surjective, et injective en tant que restriction d'une injection ; ces deux ensembles sont en bijection.

Tout a ainsi été justifié. ■

Le théorème de correspondance donne un peu de licence pour travailler sur le groupe quotient, en voyant ses opérations comme des projections de celles sur le groupe d'origine, par l'intermédiaire de la projection canonique. Notamment, elle donne un moyen d'expliciter les sous-groupes d'un groupe quotient en fonction de ceux du groupe de départ : pour un exemple concret, le lecteur peut se référer à la section suivante.

Exercice 42

Si H est distingué dans G, et K un sous-groupe de H distingué dans G, G/K est-il un sous-groupe de G/H ?

Exercice 43

(Une conséquence du théorème de correspondance) Montrer que, si H est normal dans G, H est un sous-groupe normal maximal si et seulement si G/H est simple.

Corollaire. ***(Correspondance des sous-groupes normaux avec ceux du quotient)***

Soit H un sous-groupe distingué de G. Alors il existe une bijection explicite entre les sous-groupes normaux de G contenant H et les sous-groupes normaux de G/H.

▷ Relire les dernières lignes de la démonstration du théorème de correspondance. ■

Exercice 44

Soient H, K deux sous-groupes d'un groupe.

1. Montrer que HK est un sous-groupe du groupe si et seulement si $HK = KH$.

2. Montrer qu'il suffit que H soit normal dans le groupe.

3. Sous quelle condition HK est-il normal ?

Théorème. ***(Second théorème d'isomorphisme)***

Soient G un groupe, $K \triangleleft G$ et H un sous-groupe de G. Alors $K \cap H \triangleleft H$, HK est un groupe et $K \triangleleft HK$, et $\frac{H}{K \cap H} \simeq \frac{HK}{K}$. Plus précisément, il existe un unique isomorphisme de $H/(H \cap K)$ sur HK/K tel que pour tout élément x de H, $f(x(H \cap K)) = xK$.

▷ On a déjà montré dans l'exercice précédent que HK est un sous-groupe de G, l'un des deux, à savoir K, étant normal dans G. De plus, si $x \in H \cap K$, alors si $a \in H$, $axa^{-1} \in H$ comme produit d'éléments de H et appartient à K, car K est distingué dans G, et $a \in G$: on a donc la distinction de $H \cap K$ dans H. D'autre part, si $x \in K$, si $a = hk \in HK$, alors $axa^{-1} = hkx(hk)^{-1} = h(kxk{-}1)h{-}1$. Or K est distingué dans H donc $kxk^{-1} = k' \in K$. Ainsi $axa^{-1} = hk'h^{-1} \in K$, car K est distingué dans H ; ainsi, K est distingué dans HK ; nous sommes donc tranquilles pour passer à la partie intéressante du théorème. K étant distingué dans G, on considère la projection canonique $\varphi : G \longrightarrow G/K$. Note ψ la restriction de φ à H. (Le noyau de ψ est $H \cap K$ et l'on retrouve que $H \cap K$ est distingué dans H.) L'image de ψ est l'ensemble des classes d'éléments de H suivant K par définition de la projection et de la restriction. On remarque que cet ensemble est HK/K, sous-groupe de G/K. L'énoncé résulte donc du premier théorème d'isomorphisme appliqué à ψ. ■

Remarque importante. Nous enjoignons le lecteur à vérifier que le second théorème d'isomorphisme se généralise légèrement en changeant l'hypothèse « $K \triangleleft G$ » par « H normalise K » *(voir les compléments deux sections plus bas)*.

Exercice 45

1. Quels sont les sous-groupes de $GL_n(\mathbb{K})$, $\mathbb{K}$ un corps, contenant $SL_n(\mathbb{K})$?

2. Quels sont les sous-groupes de $\mathfrak{S}_n$ contenant $\mathfrak{A}_n$?

=

Exercice 46

(Identité de Dedekind) Soient G un groupe, U et V deux parties de G telles que $UV = G$. Soient H un sous-groupe de G contenant U et K un sous-groupe de G contenant V. Montrer que $H = U(V \cap H)$ et que $K = (U \cap K)V$.

Le troisième théorème d'isomorphisme établit une égalité qui rappelle la simplification en haut et en bas des numérateur et dénominateur d'une fraction.

Théorème. ***(Troisième théorème d'isomorphisme)***

Soient G un groupe, H un sous-groupe de G, K un sous-groupe de H, avec H, K normaux dans G. Alors $H/K \triangleleft G/K$ et $\frac{G/K}{H/K} \simeq \frac{G}{H}$.

▷ Premier réflexe : K est normal dans H (par intercalation). Ainsi, on a $K \triangleleft H \triangleleft G$ et $K \triangleleft G$, ce qui permet de parler de H/K, de G/K et de G/H. Nous savons déjà également que H/K est un sous-groupe distingué de G/H : on l'a montré dans le théorème de correspondance (et ce n'est pas ce pourquoi l'on a appelé le troisième théorème d'isomorphisme dans la même preuve !). Or, toute classe X de G suivant K est contenue dans une et une seule classe selon H : en effet, X est de la forme xK, $x \in G$, donc $X = xK \subseteq xH$ classe suivant H, et la classe de x suivant H qui contient X est unique, par disjonction des classes d'équivalence. À toute classe X selon K, faisons correspondre cette unique classe selon H contenant X par une application f de G/K dans G/H. Ainsi, pour tout élément $x \in G$, $f(xK) = xH$. On vérifie très vite que f est un morphisme de groupes surjectif de noyau H/K. (On retrouve que H/K est distingué dans G/K.) On conclut par premier théorème d'isomorphisme. ■

Exercice 47

En déduire (mais c'était déjà conséquence du premier théorème d'isomorphisme) que la relation $A \preccurlyeq B \iff A$ est isomorphe à un quotient de B est un ordre.

Exercice 48

Deux sous-groupes isomorphes d'un même groupe sont-ils nécessairement égaux ?

Avant de terminer sur les quotients de groupe, une variante du premier théorème d'isomorphisme.

Propriété. ***(Quatrième théorème d'isomorphisme)***

Soient G un groupe, H un autre groupe et L un sous-groupe normal de G. On note π la surjection canonique de G sur G/L. Alors $\mathrm{Hom}(G/L, H)$ est en bijection avec l'ensemble des morphismes de G dans H dont le noyau contient L, par l'application $g \longmapsto g \circ \pi$.

▷ C'est une reformulation du théorème de factorisation pour les groupes ! On peut la voir, au choix, de cette manière, ou comme une généralisation du premier théorème d'isomorphisme, ou encore étudier $G/N \to G/K \to H$ où le premier morphisme est défini comme dans la démonstration du troisième théorème d'isomorphisme. De cette façon, on voit l'intrication des quatre théorèmes précédents. ■

Nous énonçons un résultat connexe, qui introduit pudiquement la notion de suite exacte.

Propriété

Si $f : G \longrightarrow G'$ est un morphisme de groupes, G, G' deux groupes quelconques, alors il existe une suite exacte (c'est-à-dire une suite de morphismes dont l'image de l'un est égale au noyau du suivant) donnée par $G \to G' \to G'/\mathrm{Im}(f) \to 1$.

▷ Les morphismes à considérer sont, dans l'ordre : f, la projection canonique sur $\mathrm{Im}(f)$, le morphisme trivial toujours égal au neutre. ■

2.8.2.1 Application : le cas des anneaux modulaires

On appelle anneaux modulaires, les $\mathbb{Z}/n\mathbb{Z}$ pour n parcourant l'ensemble des entiers naturels. Comme on le sait depuis le lycée, ce sont des anneaux unitaires, mais on peut se contenter pour l'instant de considérer la structure de groupe additif qui renferme déjà beaucoup des subtilités de la structure. Nous proposons au lecteur de démontrer les quelques résultats suivants en exercice : ce sont des conséquences du théorème de correspondance.

Exercice 49

Montrer que si G est un groupe et H un sous-groupe de G d'indice fini n. Soit $x \in G$. Montrer que $x^n \in H$.

Exercice 50

1. Montrer que, si G est un groupe cyclique, alors tout sous-groupe de G est lui-même cyclique (exercice classique de spé).
2. Justifier que tout groupe monogène est isomorphe à $\mathbb{Z}$ ou à un certain $\mathbb{Z}/n\mathbb{Z}$, pour $n \in \mathbb{N}^*$. En déduire que tout sous-groupe d'un groupe monogène est monogène.
3. Soit $n \in \mathbb{N}^*$. Montrer que $\mathbb{Z}/n\mathbb{Z}$ est fini, de cardinal n.
4. Montrer que les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont exactement les $d\mathbb{Z}/n\mathbb{Z}$, pour d diviseur de n, et qu'il y en a donc $\varphi(n)$.
5. Quel est le cardinal de $d\mathbb{Z}/n\mathbb{Z}$, pour d divisant n ? En déduire qu'il est isomorphe à $\mathbb{Z}/l\mathbb{Z}$, où l est le diviseur associé à d de n.
6. Montrer que $\frac{\mathbb{Z}/n\mathbb{Z}}{d\mathbb{Z}/n\mathbb{Z}}$ est isomorphe à $\mathbb{Z}/d\mathbb{Z}$.
7. Soit G un groupe cyclique d'ordre n. Montrer que pour tout diviseur d de n, G admet un unique sous-groupe d'ordre d, que tous les sous-groupes de G sont ainsi décrits, que ce groupe H est cyclique, et que G/H est également cyclique.
8. Montrer que, si G est un groupe cyclique d'ordre n et d un diviseur naturel de n, le sous-groupe d'ordre d de n est l'ensemble des éléments x de G tels que $x^d = 1$.
9. En déduire que les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont, à isomorphismes près, les $\mathbb{Z}/d\mathbb{Z}$ pour d divisant n.

Exercice 51

On souhaite montrer que le groupe multiplicatif d'un corps $\mathbb{K}$ est cyclique. On note, pour tout entier naturel a, l'endomorphisme de $\mathbb{K}^*$ défini par $f_a : x \longmapsto x^a$. Soient a,b deux entiers naturels tels que $ab = n - 1$. On note $N_a = \text{card}(\text{Ker}(f_a))$.

1. Expliquer pourquoi $N_a \leqslant a$.
2. Montrer que $\text{Im}(f_a) \subseteq \text{Ker}(f_b)$.
3. En déduire que $N_a = a$ et $N_b = b$.
4. Montrer par récurrence sur a, diviseur de $n - 1$, que le nombre d'éléments de $\mathbb{K}^*$ d'ordre a est égal à $\varphi(a)$.
5. Conclure.

2.8.2.2 Retour post-traumatique sur la distinction

Exercice 52

On rappelle qu'un sous-groupe maximal est un élément maximal pour l'inclusion de l'ensemble des sous-groupes propres d'un groupe.

1. Redémontrer la formule des indices.
2. Montrer que tout sous-groupe d'indice fini premier d'un groupe est maximal.
3. Montrer que, dans un groupe fini, tout sous-groupe propre est contenu dans au moins un sous-groupe maximal.
4. Montrer que le résultat persiste dans un groupe de type fini. Qu'a-t-on utilisé ?
5. Montrer que tout sous-groupe maximal aussi normal est d'indice fini premier.
6. Montrer qu'un sous-groupe est divisible si et seulement s'il n'a pas de sous-groupe maximal.

Exercice 53

(Théorème de Frobenius/lemme d'Ore) Montrer que dans un groupe fini G, tout sous-groupe d'indice le plus petit nombre premier divisant G est distingué.

▷ **Éléments de réponse.**

Soit H un tel sous-groupe. On fait agir H sur G/H par translation à gauche : pour $(h,xH) \in G \times G/H$, on pose $h \cdot xH = hxH$. La formule des orbites donne que le cardinal de G/H, soit p, est la somme des cardinaux des orbites sous cette action. L'orbite d'un élément $x \in G/H$ sous l'action de H est en bijection avec H/St_x où St_x est un sous-groupe de H. Comme p est le plus entier premier divisant l'ordre de G et $\text{card}(G/H) = p$, on en déduit que $\text{card}(H)$ est un produit de nombres entiers supérieurs ou égaux à p. Par le théorème de Lagrange, $\text{card}(H/St_x) = \text{card}(\Omega_x)$ vaut ainsi soit 1, soit un produit d'entiers supérieurs à p. Puisque l'élément H de G/H a une orbite réduite au neutre, et $p \geqslant 1 + q$ où $q \geqslant p$ est impossible, l'équation aux classes s'écrit $p = 1 + 1 + ...$, donc elle est triviale. Ainsi $HxH = xH$ pour tout $x \in G$, donc H est distingué dans G (l'écrire).

Définition. ***(Normalisateur)***

Si H est un sous-groupe de G, on dit qu'un élément g de G normalise H si $gHg^{-1} = H$, ou, ce qui est équivalent (le vérifier), $g^{-1}Hg = H$ (ou encore avec seule l'inclusion directe). L'ensemble des de H est appelé *normalisateur* de H et est noté $N_G(H)$.

Propriété. ***(Structure du normalisateur)***

Si H est un sous-groupe de G, $N_G(H)$ est le plus grand sous-groupe de G contenant H dans lequel H est normal.

▷ Les vérifications sont simples, et laissées au lecteur. Il s'agit de voir, successivement que : le normalisateur est un groupe, qu'il contient H, qu'il est normal, et qu'il contient tout sous-groupe de G dans lequel H est normal. ■

Corollaire. ***(Caractérisation de la normalité par le normalisateur)***

Si H est un sous-groupe de G, H est distingué dans G si et seulement s'il égale son normalisateur.

▷ C'est trivial avec ce qui précède. ■

Exercice 54

On généralise un résultat démontré en exercice en préambule du second théorème d'isomorphisme. Soit H un sous-groupe de G et K un sous-groupe de G normalisant H, c'est-à-dire inclus dans son normalisateur.

1. Montrer que HK est un sous-groupe.
2. Montrer que $H \cap K$ est distingué dans H. L'est-il dans K ?

Remarque. Le normalisateur d'un sous-groupe H dans G contient le centralisateur de H dans G, donc a fortiori, le centre de G. Pour se rendre compte de ce fait, le lecteur peut se reporter aux définitions de centralité sur les actions de groupe.

Propriété. ***(Caractérisation des normalisateurs par génératrices)***

Si H est un sous-groupe de G généré par une partie X, un élément g de G normalise H si et seulement si $g^{-1}Xg$ et gXg^{-1} sont tous deux contenus dans H.

▷ En exercice. ■

On termine avec un résultat important. Dans son *Group theory*, William Raymond Scott, docteur mathématicien diplômé en 1947 de l'Université de l'État de l'Ohio, écrit que ce théorème, presque trivial, est d'une grande importance dans la théorie des groupes en général.

Propriété. ***(Lemme N/C)***

Soient G un groupe, H un sous-groupe de G. Alors $C_G(H) \triangleleft N_G(H)$ et $N_G(H)/C_G(H)$ est isomorphe à un sous-groupe de $\mathrm{Aut}(G)$.

▷ Montrons d'abord la distinction, pour pouvoir parler de groupe quotient. Soit g un élément de $N_G(H)$. $f_g : x \longmapsto gxg^{-1}$ induit un automorphisme sur H par définition du normalisateur. On définit donc un morphisme (le vérifier) φ de $N_G(H)$ dans $\mathrm{Aut}(H)$ qui à g fait correspondre f_g. Or le noyau de ce morphisme est $C_G(H)$, qui est donc distingué dans $N_H(G)$. Enfin, d'après le premier théorème d'isomorphisme, $C_G(H) \triangleleft N_G(H)$ et $N_G(H)/C_G(H)$ est isomorphe à un sous-groupe de $\mathrm{Aut}(G)$; c'est $\mathrm{Im}(\varphi)$. ■

2.8.3 Exercices complémentaires à ce sujet

Exercice 55

On appelle *groupe de* $\mathfrak{M}_n(\mathbb{K})$, $\mathbb{K}$ un corps commutatif, ou *groupe de matrices* toute partie de $\mathfrak{M}_n(\mathbb{K})$ stable pour la loi multiplicative induite et qui, muni d'elle, soit un groupe.

1. Montrer que tout groupe de $\mathfrak{M}_n(\mathbb{K})$ dans $GL_n(\mathbb{K})$ est un sous-groupe de ce dernier.
2. Y a-t-il d'autres groupes de $\mathfrak{M}_n(\mathbb{K})$ que ceux-ci ?
3. Justifier que tout groupe de matrices est un sous-groupe du groupe linéaire ou est constitué uniquement de matrices non inversibles.
4. Montrer que les groupes de $\mathfrak{M}_n(\mathbb{K})$ sont exactement les sous-groupes des conjugués des groupes de la forme : $\left\{ \begin{pmatrix} M & O_{n-r} \\ O_{n-r} & O_{n-r} \end{pmatrix} \mid M \in GL_r(\mathbb{K}) \right\}$, $r \in [\![0,n]\!]$.
5. Quels sont les éléments neutres des groupes de $\mathfrak{M}_n(\mathbb{K})$?

Exercice 56

Montrer qu'un sous-groupe non trivial d'un groupe est d'indice 2 si et seulement s'il respecte la règle des signes. En déduire qu'un tel sous-groupe est toujours normal.

Exercice 57

1. Quel est le conjugué d'un cycle par une permutation σ ?
2. *(Cette question utilise l'exercice précédent.)* Montrer que pour tout $n \in \mathbb{N}$, $\mathfrak{A}_n$ est le seul sous-groupe de $\mathfrak{S}_n$ de cardinal $\frac{n!}{2}$.
3. Montrer que ε est le seul morphisme de groupe de $(\mathfrak{S}_n, \circ)$ dans $(\mathbb{C}^*, \times)$.

Exercice 58

Montrer que le groupe diédral d'ordre 3 noté D_6 (groupe des isométries du plan qui conservent les 3-gones, c'est-à-dire les triangles) est isomorphe au groupe symétrique $\mathfrak{S}_3$ mais que c'est le seul groupe diédral à être isomorphe à un groupe symétrique entier. Montrer cependant qu'il se plonge toujours dans un $\mathfrak{S}_{\frac{n}{2}}$.

Exercice 59

Un groupe est *simple*, si tous ses sous-groupes distingués sont triviaux.

1. Quels sont les groupes commutatifs simples ?

2. Montrer que $\mathcal{SO}_n(\mathbb{R})$ est simple si et seulement si n est impair.

3. *(Thème pour l'agrégation : simplicité du groupe alterné)* Montrer que $\mathfrak{A}_n$ est simple si et seulement si $n \neq 2$ ou 4.

Exercice 60

1. Montrer que $\mathfrak{A}_n$ est son propre dérivé.

2. Montrer que $\mathfrak{A}_n$ est le dérivé du groupe symétrique d'ordre n.

Exercice 61

Un sous-groupe d'un groupe est *strictement caractéristique* s'il est stable par tout endomorphisme caractéristique. Il est *pleinement caractéristique* s'il est stable par tout endomorphisme. Caractériser la caractérisation du centre d'un groupe.

2.9 Actions de groupes

En mathématiques, la notion d'action d'un groupe[1], ou *loi de composition externe,* sur un ensemble, rassemble un phénomène de grande ampleur : sur ensemble quelconque, les structures de groupes usuelles vont permuter les éléments de façon conservative, de sorte que les théorèmes sur les groupes vont être utilisables. On verra très rapidement que la donnée d'une action d'un élément d'un groupe sur un ensemble revient de façon équivalente à celle d'une permutation de l'ensemble.

Parmi les actions de groupe, celle d'un groupe sur lui-même permettent une prise de recul sur le point de vue purement algébrique des groupes. En particulier, l'équation aux classes associée à l'action intérieure par conjugaison nous fournira un outil pour démontrer les théorèmes de Sylow, donnant une réciproque partielle au théorème de Lagrange en quantifiant l'existence de p-sous-groupes d'un groupe quelconque.

[1] La notion d'action de groupes est la raison d'être des groupes.

De façon beaucoup plus puissante, on comprend rapidement que l'on peut étudier les groupes mêmes relativement aux actions dans lesquelles ils se réalisent. Cette remarque est assez perturbante, car le groupe fondamental, premier groupe à émerger historiquement, n'agit a priori sur aucun ensemble (mais en fait si ; de quelle manière[1] ?).

Ainsi, les actions de groupes sont un point de vue fondamental en théorie des groupes, sinon le principal.

2.9.1 Opération d'un groupe sur un ensemble : définition

Définition. ***(Opération d'un groupe sur un ensemble, action de groupe)***

Soient $(G,\times)$ un groupe quelconque et E un ensemble sans structure particulière. On dit que G *agit* sur E, ou *opère* sur E, par l'*action* ou *opération* $\cdot : G\times E \longrightarrow E$, souvent notée de façon infixe $\cdot$, si :

- ⋆ *(Action du neutre)* $\forall x\in E \quad e_G\cdot x = x$;
- ⋆ *(Compatibilité)* $\forall g,g'\in G\ \forall x\in E \quad g\cdot(g'\cdot x) = (gg')\cdot x$.

Certains auteurs parlent respectivement de *respect de la neutralité* et d'*associativité*. Nous n'adoptons pas cette terminologie.

Remarque. On a toujours $G\cdot E\subseteq E$. En effet, une action est en particulier une application. Attention à ne pas se mélanger les pinceaux : on arrive dans l'ensemble et non dans le groupe. Il n'y a priori aucunes lois définies sur X.

Proposition. ***(Point de vue représentatif des actions de groupe)***

Le groupe G opère sur l'ensemble E si et seulement s'il existe un morphisme de groupes $\phi : G\longrightarrow S_E$ le groupe symétrique de E, appelé *représentation* du groupe G, ou *morphisme structurel*, lié à l'action par :

$$\forall g\in G\ \forall x\in E \quad g\cdot x = (\phi(g))(x).$$

Autrement dit, lorsqu'un groupe agit sur un ensemble, un quotient de ce groupe se plonge dans le groupe symétrique de cet ensemble ! S'il est possible de revisser G, on peut donc décrire G à travers son action, car S_E est connu.

▷ La compatibilité puis l'action du neutre donne que $\phi(g^{-1})$ est application réciproque de $\phi(g)$ donc ϕ est bien à valeurs dans S_E. C'est bien un morphisme de groupes, grâce à la compatibilité. Réciproquement, la propriété de morphisme et le fait qu'un morphisme envoie le neutre sur, ici, l'identité, donnent les deux propriétés de compatibilité et d'action du neutre de l'action. Ceci explicite une bijection entre l'ensemble des actions de G sur E et $\mathrm{Hom}(G,S_E)$. ■

[1] Indice : ça commence par un M.

VOC On dit que :

- un élément $g \in G$ *agit* sur E s'il existe une bijection $\phi(g)$ de E, définie au moyen de g ;
- le groupe $g \in G$ agit sur E si tous les éléments de G agissent sur E, le neutre de façon identique, et chacun de façon deux à deux compatible.

Remarque. Les actions ainsi définies devraient s'appeler en toute rigueur *actions à gauche*. On peut considérer les actions à droite $(g,x) \mapsto x \cdot g$; c'est tout à fait inutile, puisque les actions à droite sont en bijection avec les actions à gauche par l'introduction du groupe opposé au groupe symétrique d'un ensemble (la loi étant alors contravariante). Cette notation est parfois commode dans des cas que nous n'aborderons pas tout de suite.

Définition. ***(Actions équivalentes)***

Soit G un groupe opérant sur un ensemble X et d'autre part sur une ensemble Y. On dit que ces deux opérations sont *équivalentes* s'il existe une bijection f de X dans Y telle que pour tout $g \in G$, pour tout $x \in X$, $f(g \cdot_X x) = g \cdot_Y f(x)$.

Remarque. Un groupe opérant sur deux ensembles ne peut le faire de façon équivalente que si ces deux ensembles sont déjà en bijection. Cela revient alors à prendre deux fois la même action, à isomorphisme près au sens de la catégorie des ensembles.

Définition. ***(Actions quasi-équivalentes)***

Soit G un groupe opérant sur un ensemble X et un groupe G' opérant sur un ensemble Y. On dit que ces deux opérations sont *quasi-équivalentes* s'il existe une bijection f de X dans Y et un isomorphisme σ de G dans G' tel que pour tout $g \in G$, pour tout $x \in X$, $f(g \cdot_{G,X} x) = \sigma(g) \cdot_{G',Y} x$.

Remarquer que ces deux notions ne s'appliquent pas aux mêmes objets. On peut seulement dire que deux opérations d'un même groupe sont quasi-équivalentes si et seulement si elles sont équivalentes, ce qui a peu d'intérêt.

2.9.2 Exemples fondamentaux d'actions de groupe

Avant de parler des propriétés fondamentales des actions, on souhaite fournir un grand nombre d'exemple qui serviront grandement pour illustrer les considérations suivantes.

Exemples. ***(Actions d'un groupe sur un ensemble)***

1. L'*action triviale* d'un groupe G sur un ensemble X quelconques est donnée par $g \cdot x = x$ pour tous $g \in G$, $x \in X$. En effet, c'est celle associée au morphisme trivial, soit l'élement neutre de $\mathrm{Hom}(G,S_X)$.
2. $\mathbb{Z}$ agit sur tout groupe par l'itération $(k,g) \mapsto n.k =\mapsto k^n$; cette action munit le

groupe G de la structure de $\mathbb{Z}$-module. Si tout élément du groupe G est d'ordre 2, cette application passe au quotient et munit G de la structure de $\mathbb{Z}/2\mathbb{Z}$ espace vectoriel.

3. Si un groupe G agit sur un ensemble X par $\cdot_0$, alors tout sous-groupe H agit naturellement par induction sur X par :

$$\begin{aligned} H \times X &\longrightarrow X \\ (h,x) &\longmapsto h \cdot_0 x. \end{aligned}$$

4. *(Important)* Tout groupe G agissant sur un ensemble X agit naturellement par induction sur $\mathcal{P}(X)$ l'ensemble de ses parties par :

$$\begin{aligned} G \times \mathcal{P}(X) &\longrightarrow \mathcal{P}(X) \\ (g,A) &\longmapsto g \cdot A = \{g \cdot a,\ a \in A\}. \end{aligned}$$

5. *(Action de McKay)* Soient n un entier naturel et X un ensemble. Alors le groupe $\mathbb{Z}/n\mathbb{Z}$ agit naturellement sur l'ensemble des n-uplets à valeurs dans X, noté X^n, par :

$$\overline{1} \cdot (x_1,...,x_n) = (x_n,x_1,x_2,...,x_{n-1}) \overline{2} \cdot (x_1,...,x_n) = (x_{n-1},x_n,x_1,...,x_{n-2})$$

et ainsi de suite. On vérifie qu'elle est bien définie et que c'est une action de groupes compatible.

6. On sait que le groupe symétrique $\mathfrak{S}_n$, $n \in \mathbb{N}$, agit sur l'ensemble $[\![1,n]\!]$ de façon canonique par $(\sigma, k) \mapsto \sigma(k)$. L'étude des orbites des éléments sous cette action donne le théorème de décomposition d'une permutation en produit de cycles.

7. Plus généralement, tout ensemble E est opéré par son groupe des permutations par

$$\begin{aligned} S_E \times E &\longrightarrow E \\ (f,x) &\longmapsto f(x). \end{aligned}$$

On vérifie aisément que c'est bien une action de groupes, associé au morphisme identité de $S_E \longrightarrow S_E$ pour représentation.

Exemples. ***(Actions matricielles)***

1. *(Exemple concret d'action)* L'*action de Steiniz*, pour un corps $\mathbb{K}$ et n,m deux entiers naturels, est définie par :

$$\begin{aligned} \pi : \ GL_n(\mathbb{K}) \times GL_m(\mathbb{K}) &\longrightarrow \mathfrak{M}_{n,m}(\mathbb{K}) \\ (P,Q) \cdot M &\longmapsto PMQ^{-1}. \end{aligned}$$

2. Le groupe orthogonal (resp. unitaire) d'un espace euclidien (resp. hermitien) opère sur sa sphère unité :

$$\begin{aligned} \mathcal{O}(E) \times S &\longrightarrow S \\ (u,x) &\longmapsto u(x) \end{aligned}$$

(resp.

$$\begin{aligned} U(E) \times S &\longrightarrow S \\ (u,x) &\longmapsto u(x) \end{aligned} \quad).$$

3. Le groupe $GL_n(k)$ agit sur $\mathfrak{M}_{n,p}(k)$ par translation à gauche :

$$\begin{aligned} GL_p(k) \times \mathfrak{M}_{n,p}(k) &\longrightarrow \mathfrak{M}_{n,p}(k) \\ (P,M) &\longmapsto PM. \end{aligned}$$

4. Le groupe $GL_p(k)$ agit sur $\mathfrak{M}_{n,p}(k)$ par translation et inversion à droite :

$$\begin{aligned} GL_p(k) \times \mathfrak{M}_{n,p}(k) &\longrightarrow \mathfrak{M}_{n,p}(k) \\ (P,M) &\longmapsto MP^{-1}. \end{aligned}$$

5. Le groupe $GL_n(k)$ agit sur $\mathfrak{M}_n(k)$ par translation et inversion à droite :

$$\begin{aligned} GL_n(k) \times \mathfrak{M}_n(k) &\longrightarrow \mathfrak{M}_n(k) \\ (P,M) &\longmapsto PMP^{-1}. \end{aligned}$$

C'est la composée des deux actions précédentes au même point du groupe.

6. En particulier, $\mathcal{O}_n(\mathbb{R})$ agit sur $\mathfrak{M}_n(\mathbb{R})$ par conjugaison.

7. Le groupe $GL_n(k)$ agit sur $\mathcal{S}_n(k)$ par congruence :

$$\begin{aligned} GL_n(k) \times \mathcal{S}_n(k) &\longrightarrow \mathcal{S}_n(k) \\ (P,M) &\longmapsto PM\,{}^tP. \end{aligned}$$

Exemples. ***(Actions d'un groupe lui-même/actions intérieures)***

1. L'*action par conjugaison* ou *action par automorphismes intérieurs* d'un groupe G sur lui-même est donnée par :

$$\begin{aligned} c_g : \quad G \times G &\longrightarrow G \\ (g,x) &\longmapsto gxg^{-1} \end{aligned}$$

ou, ce qui est essentiellement pareil,

$$fonctionc_gG \times GG(g,x)g^{-1}xg$$

selon les auteurs. Notons que la deuxième est celle de la formule du changement de base dans l'espace des matrices carrées tandis que la première est celle de la formule de conjugaison des cycles du groupe symétrique.

2. L'*action par translations à gauche* d'un groupe G sur lui-même est donnée par :

$$\begin{aligned} c_g : \quad G \times G &\longrightarrow G \\ (g,x) &\longmapsto gx. \end{aligned}$$

L'*action par translations à droite* d'un groupe G sur lui-même est donnée par :

$$\begin{aligned} c_g : \quad G \times G &\longrightarrow G \\ (g,x) &\longmapsto xg. \end{aligned}$$

Remarquer que, contrairement au cas de l'action par conjugaison où la représentation associée à l'action est carrément à valeurs dans $\mathrm{Aut}(G)$, la fonction de x à g fixé n'est pas un morphisme de groupe.

3. L'action par conjugaison d'un groupe G sur lui-même induit une action de G sur l'ensemble de ses sous-groupes $H(G)$ donnée par

$$\begin{aligned} G \times \mathcal{H}(G) &\longrightarrow \mathcal{H}(G) \\ (g,H) &\longmapsto gHg^{-1}. \end{aligned}$$

4. Plus généralement, le groupe des automorphismes d'un groupe G agit sur l'ensemble de ses sous-groupes par :

$$\begin{aligned} \mathrm{Aut}(G) \times \mathcal{H}(G) &\longrightarrow \mathcal{H}(G) \\ (f,H) &\longmapsto f(H). \end{aligned}$$

Cette action est appelée *action canonique par automorphismes* de G.

5. Le groupe des automorphismes intérieurs d'un groupe G agit sur l'ensemble de ses sous-groupes par :

$$\begin{aligned} \mathrm{Int}(G) \times \mathcal{H}(G) &\longrightarrow \mathcal{H}(G) \\ (\phi,H) &\longmapsto \phi(H). \end{aligned}$$

Cette action est équivalente à l'action par conjugaison d'un groupe sur l'ensemble de ses sous-groupes.

Contre-exemple. ***(Opération qui n'est pas une action)***

L'application de $\mathbb{Z} \times \mathbb{Z}$ dans $\mathbb{Z}$ qui à (k,x) fait correspondre $x+1$ n'est pas une action de groupes. Elle est compatible, mais ne respecte pas le neutre. De même, l'application qui à (k,x) fait correspondre $x+k^2$ n'est pas une action de groupes. Elle respecte le neutre,

mais n'est pas compatible.
L'application de $\mathbb{Z} \times \mathbb{Z}$ dans $\mathbb{Z}$ qui à (k,x) fait correspondre kx n'est pas une action de groupes : elle n'est ni compatible, ni ne respecte le neutre. □

2.9.3 Orbites, stabilisateurs, points fixes, etc.

Dans toute cette partie, on se fixe un G un groupe, X un ensemble et une action de G sur X notée comme usuellement.

Toutes les notions suivantes s'appliquent évidemment aux actions d'un groupe sur lui-même, mais il est important de les manipuler d'abord dans le cas général afin de savoir où elles se situent : dans l'ensemble ou dans le groupe.

2.9.3.1 Orbites

Définition. ***(Orbite d'un élément)***

L'*orbite* d'un élément $x \in X$ est l'ensemble $\{g \cdot x,\ g \in G\}$. On le note au choix Ω_x, $\mathcal{O}_x$, $\mathrm{orb}(x)$, $G \cdot x$.

Propriété. ***(Structure des orbites)***

L'ensemble des orbites des éléments d'un ensemble sous l'action de G forme une partition de X.

▷ Considérer la relation $x \in \Omega_y$, symétrique, car on est dans un groupe. ■

2.9.3.2 Stabilisateurs, centralisateurs, normalisateurs

Définition. ***(Stabilisateur d'un élément)***

Le *stabilisateur* d'un élément $x \in X$ est l'ensemble $\{g \in G,\ g \cdot x = x\}$. On le note au choix St_x, $\mathrm{stab}(x)$, Stab_x, G_x.

Propriété. ***(Structure des stabilisateurs)***

Le stabilisateur d'un élément de X est un sous-groupe de G.

▷ Clair au vu des hypothèses sur l'action de groupes. ■

Attention ! Les stabilisateurs d'une action en général n'ont aucune raison d'être distingués ! On peut quand même définir le quotient de G par un stabilisateur. Il n'est pas muni de structure de groupe et ne coïncide pas forcément avec le quotient $St_x priveG$.

Exercice 62

1. Donner un exemple.
2. Donner un contre-exemple.

2.9.3.3 Stabilisateur d'une partie

Définition. ***(Stabilisateur d'une partie)***

Le *stabilisateur* d'une partie $A \subseteq X$ est l'ensemble $\{g \in G,\ g \cdot A = A\}$. On le note St_A, $\mathrm{stab}(A)$ ou d'autres manières intuitives encore.

Remarque. Le stabilisateur d'une partie n'est autre que le stabilisateur pour l'action naturelle sur l'ensemble des parties.

Attention, le stabilisateur d'une partie n'a aucune raison d'être un sous-groupe de G, même si l'action considérée est intérieure et A est un sous-groupe de $X = G$ (exemple ?).

2.9.3.4 Fixateurs

Définition. ***(Points fixes par l'action d'un élément)***

L'ensemble des *points fixés* par un élément $g \in G$ est l'ensemble $\{x \in X,\ g \cdot x = x\}$. On le note Fix_g.

2.9.4 Équation aux classes, formule de Burnside

Propriété. ***(Relation entre orbites et stabilisateurs)***

Pour tout $x \in X$, $\Omega_x \simeq G/St_x$ au sens des ensembles.

▷ On pose $\varphi : g \cdot x \mapsto gSt_x$. Cette fonction est bien définie et c'est une bijection (pas un isomorphisme de groupes). ■

Ce constat est fondamental et constitue la simplification primordiale de l'équation aux classes.

Théorème. ***(Formule des orbites)***

Soit G un groupe agissant sur un ensemble X. Alors :

$$\mathrm{card}(X) = \sum_{x \in X} \mathrm{card}(\Omega_x).$$

▷ Tout simplement parce que les orbites partitionnent X. ■

Corollaire

Si toutes les orbites sous l'action de G ont le même cardinal (par exemple : l'action par translation), alors le cardinal d'une orbite divise le cardinal de X.

Cette formule préliminaire se simplifie grâce au lemme précédent pour donner la plus utile *équation aux classes*. On détaillera un cas particulier extrêmement important dans le cas de l'action par conjugaison d'un groupe sur lui-même.

Théorème. ***(Formule des classes)***

Soit G un groupe agissant sur un ensemble *fini* X. Soit X_0 l'ensemble des points fixes sous cette action et notons $\mathcal{T}$ une *transversale*, c'est-à-dire un système de représentants des orbites non réduites à un élément. Alors :

$$\operatorname{card}(X) = \operatorname{card}(X_0) + \sum_{x\in\mathcal{T}} \frac{\operatorname{card}(X)}{\operatorname{card}(\mathrm{St}_x)}.$$

▷ D'après le lemme, $\operatorname{card}(\Omega_x) = [G : \mathrm{St}_x] = \frac{\operatorname{card}(X)}{\operatorname{card}(\mathrm{St}_x)}$. ■

Dans le cas de l'action par conjugaison, la formule se réécrit d'une façon drastiquement différente.

Théorème. ***(Équation aux classes)***

Soit G un groupe. Soit $\mathcal{T}$ une transversale pour l'action par conjugaison de G sur lui-même. Alors

$$\operatorname{card}(G) = \operatorname{card}(\mathcal{Z}(G)) + \sum_{\substack{x\in\mathcal{T}\\ x\notin\mathcal{Z}(G)}} \frac{\operatorname{card}(G)}{\operatorname{card}(C(x))}.$$

De plus, aucun des termes de la somme à droite n'est égal à 1.

L'équation aux classes sert donc à calculer le cardinal d'un groupe : il suffit de connaître le cardinal de son centre, puis de déterminer une transversale et de calculer le centralisateur de chaque élément de celle-ci[1].

[1] C'est une blague ! Bien sûr que non, l'équation aux classes est complètement inutile pour calculer des cardinaux. Calculer le centre d'un groupe est un exercice parfois redoutable ; bonjour pour ensuite recommencer l'opération pour trouver des commutants pour chaque élément d'une transversale dont l'existence est elle-même donnée par ni plus ni moins que l'axiome du choix.

L'équation aux classes permet des raisonnements arithmétiques sur le centre des groupes, notamment ceux des p-groupes où la manipulation est facilitée ; on en verra de nombreux exemples, qui sont les principales applications de cette formule, dans la section sur le Théorème de Sylow.

On montre avant de terminer la formule de Burnside. On commence avec un lemme utile.

Propriété. ***(Conjugué d'un stabilisateur)***

Soient $x \in X$ et $g \in G$. Alors

$$St_g \cdot_x = gSt_xg^{-1}.$$

▷ Soit $g' \in St_g \cdot_x$. Alors $g' \cdot (g \cdot x) = x$, d'où $(g'g) \cdot x = x$. Posons $y = g^{-1}g'$. Alors $g' \in St_xg \cdot x$ donc $g'^{-1} \in St_g \cdot_x$, donc $g'^{-1}g = y^{-1} \in St_x$, d'où $y \in St_x$, d'où $g' = gy$ où $y \in St_x$. Ainsi $gSt_g \cdot_x \subseteq gSt_x$. L'autre inclusion se montre de la même manière par inversion dans G. ■

Par conséquence :

- les stabilisateurs sont isomorphes, donc équipotents ;
- et donc tous les stabilisateurs ont le même indice.

Théorème. ***(Formule de Burnside)***

Soit G un groupe fini agissant sur un ensemble X. Soit N le nombre d'orbites sous cette action. Alors :

$$\mathrm{card}(G) = \frac{1}{N}\sum_{g\in G}\mathrm{card}(\mathrm{Fix}_g).$$

▷ On va calculer le cardinal de $S = \{(g,x) \in G \times X \mid g \cdot x = x\} = \{(g,x) \in G \times X,\ g \in St_x\}$ de deux manières différentes. Clairement, $S = \bigsqcup_{x\in X}\{x\} \times St_x$, d'où $\mathrm{card}(S) = \sum_{x\in X}\mathrm{card}(St_x)$. D'autre part, $\bigsqcup_{g\in G}\mathrm{Fix}_g \times \{g\}$, donc $\mathrm{card}(S) = \sum_{g\in G}\mathrm{card}(\mathrm{Fix}_g)$. Fixons T une transversale pour la partition de X en orbites ; alors $\mathrm{card}(T) = N$. On a $\sum_{x\in X}\mathrm{card}(St_x) = \sum_{x\in T}\sum_{y\in\Omega_x}\mathrm{card}(St_y)$. Or on a vu que $\mathrm{card}(St_y) = \frac{\mathrm{card}(G)}{\mathrm{card}(\Omega_y}$ et si $y \in \Omega_x$, $\Omega_y = \Omega_x$. Ainsi, $\sum_{x\in X}\mathrm{card}(St_x) = \sum_{x\in T}\sum_{y\in\Omega_x}\frac{\mathrm{card}(G)}{\mathrm{card}(\Omega_x)} = \mathrm{card}(G)\sum_{x\in T}\sum_{y\in\Omega_x)} fr1\mathrm{card}(\Omega_x) = \mathrm{card}(T)\mathrm{card}(G) = N\mathrm{card}(G)$, d'où le résultat. ■

Exemple fondamental. ***(Application au dénombrement des coloriages)***

On cherche le nombre de façons de colorier un cube avec trois couleurs.
Il y a a priori 3^6 façons de colorier ; cependant, certains coloriages sont équivalents à rotation près du cube. On introduit donc le groupe G des rotations du cube qui agit sur l'ensemble X des faces du cubes. Le groupe G des rotations du cube est isomorphe à $\mathfrak{S}_4$; il est donc de cardinal 24.
Pour chaque élément de G, on dénombre le nombre de coloriages invariants. Pour l'identité, tous les coloriages le sont. Pour les rotations passant par des sommets opposés, d'angles $\pm 2\pi/3$, il y a 3^2 coloriages invariants. Pour les rotations d'axe les centres des faces opposées et d'angle $\pm\pi/2$, il y a 3^3 coloriages invariants. Pour les rotations d'axe les centres des

faces opposées et d'angle $\pm\pi$, il y a 3^4 coloriages invariants. Pour les rotations d'axe les centres des côtés opposées et d'angle $\pm\pi$, il y a 3^3 coloriages invariants. En sommant, on obtient $\sum_{g\in G} \mathrm{Fix}_g = 1368$.
Par suite, le nombre d'orbites est $\frac{1368}{24} = 57$. C'est le nombre cherché.

2.9.5 Propriétés des actions de groupe

On rappelle qu'à une action $G \times X \longrightarrow X$ est associé un unique morphisme T de G dans S_X, qui à g fait correspond $(x \to g \cdot x)$, de réciproque $(x \to g^{-1} \cdot x)$.

Définition. ***(Action transitive)***

Soit G un groupe opérant sur un ensemble X. On dit que G opère *transitivement* sur X, ou que l'action est *transitive*, si deux éléments de X sont toujours dans une même orbite, autrement dit, s'il n'y a qu'une seule orbite.
Une action est transitive, si et seulement si, l'application T_x qui à $g \in G$ fait correspondre $g \cdot x$ est surjective pour tout $x \in X$.

Propriété

Si T est surjective, l'action est transitive.

▷ Soient $(x,y) \in X^2$. On considère la transposition (x,y) dans S_X. Puisque T est surjective, il existe g tel que $(x \mapsto g \cdot x)$ soit égal à cette transposition ; g convient alors. ■

La réciproque est fausse ! Dans la preuve précédente, on comprend bien que la condition est beaucoup trop forte : cela voudrait dire que toute permutation de X se réalise comme l'action d'un élément de G sur X. Par exemple, le groupe $Z/3\mathbb{Z}$ opère transitivement par translation à gauche sur son groupe de permutation $\mathfrak{S}_3$. Mais il n'existe pas de surjection d'un ensemble à 3 éléments sur un ensemble à 6 éléments... Plus généralement, T n'a aucune chance d'être surjective dans le cas de l'action d'un groupe sur lui-même, car pour tout groupe G (fini ou non), $G < S_G$ au sens du cardinal.

Définition. ***(Action fidèle)***

Soit G un groupe opérant sur un ensemble X. On dit que G opère *fidèlement* sur X, ou que l'action est *fidèle*, si seul l'élément neutre fixe tous les éléments de X, autrement dix, si l'intersection de tous les stabilisateurs est réduite au neutre.
Une action est fidèle, si et seulement si, l'application T est injective.

Contre-exemple. ***(Opération qui agit non fidèlement)***

Soit $H \leqslant G$ groupes. Alors G opère sur l'ensemble G/H par translation à gauche :

$$\begin{aligned} G \times G/H &\longrightarrow G/H \\ (g,xH &\longmapsto gxH. \end{aligned}$$

Cette opération est transitive comme toute translation à gauche ; elle n'est pas fidèle en général. **À retenir** : elle est fidèle, si et seulement si, H est trivial ou n'est pas distingué dans G.
En effet, $\mathrm{Ker}(T) = \bigcap_{x\in H} xHx^{-1}$. Si H est distingué dans G, alors $\mathrm{Ker}(T) = H$. Si H n'est pas trivial, alors T n'est pas injective. Si H n'est pas distingué dans G, alors cette intersection a au moins deux termes et ils sont tangents au neutre, donc $\mathrm{Ker}(T) = \{e\}$, donc T est injective. □

Propriété. ***(Fidélisation d'une action par quotient)***

Soit une action de G sur X et T le morphisme associé. Alors $G/\mathrm{Ker}(T)$ agit fidèlement sur X.

On donne également deux autres notions simples et liées au précédentes.

Définition. ***(Action libre)***

Soit G un groupe opérant sur un ensemble X. On dit que G opère *librement* sur X, ou que l'action est *libre*, si tout élément différent du neutre agit sans point fixe.
Autrement dit, $\forall x \in X,\ St_x = \{e\}$.

Propriété

Une action libre est en particulier fidèle.

▷ Qui peut le moins, peut le encore moins. ■

Contre-exemple. ***(Action fidèle non libre)***

Dans un groupe non abélien dont le centre est réduit au neutre, comme $\mathfrak{S}_{112}$, l'action par conjugaison n'agit pas librement ; certains éléments ont des commutants non triviaux. En revanche, l'intersection de tous est le centre de G donc l'action est fidèle. □

Définition. ***(Action simplement transitive)***

Soit G un groupe opérant sur un ensemble X. On dit que l'action est *(simplement) transitive*, si deux éléments quelconques du groupe sont envoyés l'un sur l'autre par un et

un seul élément du groupe, soit $\forall x,y \in X,\ \exists! g \in G,\quad y = g \cdot x$.
Autrement dit, une action simplement transitive est une action transitive et libre.

Remarque. Dans la formule précédente, $x = g^{-1} \cdot y$.

Contre-exemple. ***(Action transitive non simplement)***

Le groupe général linéaire de dimension $n = 12$ agit sur l'ensemble des matrices diagonales de manière transitive immédiatement ; la matrice de passage d'une à l'autre n'est pas unique, si les matrices diagonales ont plusieurs valeurs propres distinctes. □

Il est donc immédiat par définition qu'un action simplement transitive est fidèle.

Propriété. ***(Condition suffisante de simple transitivité)***

Une action fidèle et transitive *d'un groupe abélien* est simplement transitive.

▷ Soit G un groupe commutatif et X un ensemble. On suppose avec les notations usuelles que G agisse fidèlement et transitivement sur X. On note ϕ le morphisme structurel. Soient $(g,x) \in G \times X$ tels que $\phi(g)(x) = x$. Montrons que $g = e$. Puisque l'action est transitive, pour tout $y \in X$, il existe un g_y tel que $y = \phi(g_y)(x)$, de sorte que

$$\phi(g)(y) = \phi(g)(\phi(g_y)(x)) = \phi(gg_y)(x) = \phi(g_y g)(x) = \phi(g_y)(\phi(g)(x)) = \phi(g_y)(x) = y.$$

Par suite, $\phi(g)$ est l'identité, donc $g = e$. C'est terminé. ■

Propriété. ***(Transitivité dans le cas fini)***

Une action transitive d'un groupe fini G sur un ensemble X est simplement transitive si et seulement si X ont le même cardinal.

▷ Facile. ■

On ne conseillera jamais assez aux étudiants de vérifier si chacune de ces propriétés sont vérifiées pour les actions définies précédemment. Par exemple, on pourra montrer que l'action par conjugaison n'est jamais libre (sauf pour le groupe trivial), et est fidèle si et seulement si le centre du groupe est trivial.

2.9.6 Actions d'un groupe sur lui-même

2.9.6.1 Actions par conjugaison et équation aux classes de conjugaison

Remarque. L'action par conjugaison n'a d'intérêt que dans un groupe non abélien.

	Actions en général	**Conjugaison = automorphismes intérieurs**	**Translations à gauche**
Expression	$G \times E \to E$ $(g,x) \mapsto g.x$	$G \times G \to G$ $(g,x) \mapsto gxg^{-1}$ ET f_g est un **automorphisme**	$G \times G \to G$ $(g,x) \mapsto gx$ ET f_g est une **bijection (mais pas un morphisme)**
Orbite d'un élément	Les $O_x = \Omega_x$ $= \{y \in E, \exists g \in G \ y = g.x\}$ partitionnent E **(ne sont pas des sous-groupes** sauf cas trivial)	**Classe de conjugaison** C_x = ensemble des **conjugués** de x *(les gxg^{-1} pour g parcourant G)*	Il n'existe qu'une seule orbite : on dit que l'action est **transitive**
Stabilisateur/Sous-groupe d'isotropie d'un élément	$G_x = St_x$ $= \{g \in G, g.x = x\}$ **(sous-groupe)**	**Centralisateur** de x noté $Z_x = C(x) = C_G(x)$: ensemble des éléments qui commutent avec x	Tous triviaux par régularité (« l'action agit sans point fixe ») : on dit qu'elle est **libre** Libre et transitive = **simplement transitive** L'intersection de tous les stabilisateurs est réduite au neutre : on dit que l'action est **fidèle**. On en déduit le théorème de Cayley.
Stabilisateur d'une partie	$Stab(A)$ $= \{g \in G, gA = A\}$ **(a priori pas un sous-groupe)**	Centralisateur d'une partie : **définition alternative** comme l'ensemble des éléments qui commutent avec tous les éléments de x **(sous-groupe)** $C(G) = Z(G)$ le centre de G *(donc s.-g. **distingué**)*	Rien de spécial
Équation aux classes	Soit T famille de représentants pour la partition par les orbites. $card(E) = \sum_{x \in T} \frac{card(G)}{card(G_x)}$	$card(G)$ $= card(Z(G))$ $+ \sum_{x \in T, x \notin Z(G)} \frac{card(G)}{card(Z_x)}$	Aucun intérêt, il n'y a qu'une orbite
		Normalisateur d'une partie X : $N_G(X) = \{g \in G, gXg^{-1} = X\}$ • Sous groupe • Si X sous-groupe, plus grand sous-groupe dans lequel X est normal • $C(X)$ normal dans $N(X)$	

FIGURE 2.9.1 : *Quelques caractéristiques sur les actions d'un groupe sur lui-même —*

Propriété. ***(Action par conjugaison)***

Soit G un groupe et $g \in G$. L'application $c_g : x \mapsto gxg^{-1}$ de G dans lui-même est un automorphisme de groupes, appelé *automorphisme intérieur* de G associé à g.

Remarque. On aurait pu définir l'automorphisme intérieur sous la forme $g^{-1}xg$. Cela ne définit pas le même élément, et donc pas le même morphisme, mais globalement, l'ensemble des automorphismes intérieurs de G est défini par l'ensemble des éléments de cette forme, ou ceux de la première.

Définition. ***(Automorphismes intérieurs)***

Soit G un groupe. On note $\mathrm{Int}(G)$ l'ensemble des automorphismes intérieurs de G, ou *intérieur* de G.

Propriété. ***(Structure de l'intérieur)***

Soit G un groupe. Alors $\mathrm{Int}(G)$ est un sous-groupe distingué de $\mathrm{Aut}(G)$.

▷ Pour tout $g \in G$, $c_{g^{-1}} = (c_g)-1$. ■

Remarque. Si G est cyclique, alors $\mathrm{Int}(G)$ est commutatif en tant que sous-groupe d'un groupe commutatif. Cependant, G est commutatif donc il est clair que son intérieur est vide. Si G est premier, on en déduit que son intérieur est cyclique, mais de même, il est trivial.

Définition. ***(Classe de conjugaison)***

Soit G un groupe et x. On appelle *classe de conjugaison* de G, et on note $C_x = C(x)$, l'orbite de x sous l'action de G. C'est l'ensemble des *conjugués* de x, soit les $c_g(x) = gxg^{-1}, g \in G$.

Théorème. ***(Géométrie des classes de conjugaison d'un groupe fini)***

Un sous-groupe strict d'un groupe fini ne peut couper toutes les classes de conjugaison.

▷ La classe de conjugaison de $x \in G$ est $G = \{gxg^{-1}, g \in G\}$. Soit H un sous-groupe strict de g. Alors $gxg^{-1} \in H$ si et seulement si $x \in g^{-1}Hg$. Montrons donc que $G \neq \bigcup_{g \in G} gHg^{-1}$. On raisonne par cardinalité.

On remarque que si $gH = g'H$, alors $g'g^{-1} = h \in H$ d'où $g' = hg$ puis $gHg^{-1} = g'Hg'^{-1}$. On peut donc réduire cette union à un système de représentants des classes selon H à gauche $g_1,...,g_s$ où $s = [G : H]$. Dans ce cas, $x \in g^{-1}Hg$. Donc $\left|\bigcup_{g \in G} gHg^{-1}\right| = \left|\bigcup_{i=1}^{s} g_iHg_i^{-1}\right| = \sum_{i=1}^{s} \left|g_iHg_i^{-1}\right| \leqslant \sum_{i=1}^{s} |H| = s\,|H| = G$, puisque $|g_iH| = |H|$ donc $\left|g_iHg_i^{-1}\right| \leqslant g_iH$. Cette majoration n'est pas concluante.

On peut l'affiner. En effet, tous les $g_i H g_i^{-1}$ ont l'élément neutre en commun, d'où $\left|\bigcup_{g\in G} gHg^{-1}\right| \leqslant \sum_{i=1}^{s} |H| - (s-1) \leqslant |G| - (s-1)$. Puisque H est un sous-groupe strict, $s \geqslant 2$ donc $-(s-1) \leqslant -1$ d'où $\left|\bigcup_{g\in G} gHg^{-1}\right| < |G|$. ■

Contre-exemple. ***(Classes de conjugaison infinies)***

Ce théorème ne vaut plus pour les groupes infinis. On sait en effet que toute matrice de $GL_n(\mathbb{C})$ est trigonalisable, ce qui veut dire que le sous-groupe strict des matrices triangulaires supérieures coupe toutes les classes de conjugaison.
Ceci est cohérent avec le fait qu'un corps fini ne peut être algébriquement clos, *i.e.* toute matrice à coefficient dans lui ne peut être trigonalisable. □

On peut décrire l'intérieur d'un groupe grâce au théorème d'isomorphisme.

Propriété. ***(L'intérieur est un quotient)***

Soit G un groupe. Alors $\mathrm{Int}(G) \simeq G/\mathcal{Z}(G)$.

▷ L'application de G dans $\mathrm{Aut}(G)$ a pour image $\mathrm{Int}(G)$ et se quotient en une application injective sur le quotient par son noyau $\mathcal{Z}(G)$. En effet, $gxg^{-1} = x$ pour tout g ssi $x \in \mathcal{Z}(G)$. ■

Corollaire

$\mathrm{Int}(G)$ n'est pas cyclique sauf si G est commutatif.

Définition. ***(Normalisateur)***

Soit G un groupe et X une partie de G. On note $N(X)$ le *normalisateur* de X, le stabilisateur de X par l'action par conjugaison.

Propriété. ***(Structure des normalisateurs)***

Pour toute partie X de G, $N(X)$ est un sous-groupe de G.

Formule. ***(Formule du normalisateur)***

Le nombre de sous-groupes conjugués à H est égal à l'indice du normalisateur de H.

Définitions. ***(Centralisateurs)***

Soit G un groupe et X une partie de G. On note $C(X)$ le *centralisateur* de X, l'ensemble des éléments de G qui commute avec tous les éléments de X.

- Si $X = \{x\}$, on note $C(x)$ le *centralisateur de* x. On a $C(x) = \mathrm{St}_x$ pour la conjugaison.
- Si X est une partie quelconque de G, on note comme précédemment. C'est son stabilisateur pour l'action par conjugaison induite sur l'ensemble des parties.
- Si $X = G$, on note $C(G) = \mathcal{Z}(G)$ le *centre* de G.

Propriété. ***(Structure des centralisateurs)***

Dans tous les cas, un centralisateur est un sous-groupe de G.

2.9.6.2 Le théorème de Cayley

Théorème. ***(Théorème de Cayley)***

Tout groupe est isomorphe à un groupe de permutations, c'est-à-dire, un sous-groupe d'un groupe des permutations d'un certain ensemble.

▷ En effet, l'action par translations à gauche est fidèle. La représentation associée fournit donc un morphisme injectif de G sur son image, qui est un sous-groupe de S_G. On pourra le reformuler à profit à la main. ■

2.10 Théorèmes de Sylow

2.10.1 Notion de p-groupe

Dans toute la suite, on fixe $p \in \mathcal{P}$.

Définition. ***(p-groupe)***

Soit p un nombre premier. On appelle p-groupe, tout groupe non trivial G dont l'ordre = le cardinal est une puissance de p, soit :

$$existsk \in \mathbb{N}^* \quad \mathrm{card}(G) = p^k.$$

En particulier, les groupes premiers sont des p-groupes.

L'exposant d'un p-groupe n'a aucune raison d'être $\log_p(|G|)$. Mais peut-on trouver un lien ?

Propriété. ***(Sous-groupe d'un p-groupe)***

Tout sous-groupe d'un p-groupe est un p-groupe.

▷ Théorème de Lagrange. ■

VOC En toute logique, un sous-p-groupe est un sous-groupe d'un p-groupe. Par contre, un p-sous-groupe est un sous-groupe d'un groupe quelconque qui est un p-groupe. Les sous-p-groupes sont donc en particulier des p-sous-groupes, mais par convention, la réciproque est fausse.

On rappelle le théorème suivant, qui peut se voir comme un précédent aux théorèmes de Sylow :

Théorème. ***(Lemme de Cauchy)***

Soit G un groupe d'ordre $n = p_1^{\alpha_1}...p_r^{\alpha_r}$. Alors pour tout $i \in [\![1,r]\!]$, il existe un sous-groupe premier de G d'ordre p_i. En particulier, tout groupe admet un sous-groupe premier.

Exercice 63

Soient $p,q \in \mathcal{P}$. Montrer qu'un groupe d'ordre pq non abélien n'est jamais simple.

▷ **Éléments de réponse.**

Si $p = q$, on a un p-groupe résoluble. Il n'est pas abélien, donc pas simple. Sinon, soit un q-groupe dans ce groupe donné par le premier théorème de Sylow que nous allons verrons. Son indice est le plus premier dans la décomposition de l'ordre, donc il est distingué. On rappelle par ailleurs qu'il y a seulement deux groupes abéliens dans les deux cas.

Exercice 64

On s'intéresse aux groupes finis dont tous les éléments sont d'ordre p, pour p un nombre premier.

1. Donner un exemple de groupe infini pour lequel cette propriété est vérifiée toutefois.
2. Soit G un groupe fini dont tous les éléments sont d'ordre 2, c'est-à-dire, au demeurant, prenons un groupe d'exposant 2. Montrer que G est abélien, puis que $G \simeq (\mathbb{Z}/2\mathbb{Z})^a$ pour un certain $a \in \mathbb{N}^*$.
3. Soit G un groupe fini dont tous les éléments sont d'ordre 3. Montrer que G est abélien, puis que $G \simeq (\mathbb{Z}/3\mathbb{Z})^b$ pour un certain $b \in \mathbb{N}^*$.
4. On suppose G est un groupe abélien fini et que tous ses éléments sont d'ordre p. Montrer que $G \simeq (\mathbb{Z}/p\mathbb{Z})^d$ pour un certain $d \in \mathbb{N}^*$. En déduire que G est un p-groupe.
5. Exhiber un contre-exemple dans le cas non abélien.

▷ **Éléments de réponse.**

L'idée de preuve est toujours la même : on montre que la loi externe de module passe au quotient ce qui munit G de la structure de $\mathbb{Z}/p\mathbb{Z}$-module et donc d'espace vectoriel. Puisque G est fini, il est de dimension finie.

Pour un contre-exemple, on peut penser au groupe $U_3(\mathbb{F}_p)$.

L'équation aux classes donne des renseignements précieux sur le centre d'un p-groupe.

Propriété. ***(Centre d'un p-groupe)***

Le centre d'un p-groupe n'est jamais trivial.

▷ Soit G un p-groupe, de cardinal p^k. Supposons que son centre soit trivial. Dans l'équation aux classes, aucun élément de la transversale choisi et n'étant pas dans le centre de G n'a un centralisateur égal à G ; ainsi, l'équation donne $p^k = 1 + \alpha_1 p + ...\alpha_k p^k$. Puisque G n'est pas abélien, les α_i ne sont pas tous nuls. En faisant la différence, on trouve, puisque $k \geqslant 1$, on a p divise 1, absurde. ■

Pour les p-groupes de petits ordres, on a plus fort, ce qui se révèle très utile pour la classification des groupes de petits ordres :

Propriété. ***(Groupes d'ordre p^2)***

Tout groupe d'ordre p, p^2 est abélien.

▷ On sait que tout groupe premier est cyclique donc abélien. Soit un groupe d'ordre p^2. Son centre est d'ordre p ou p^2, puisqu'il n'est pas trivial. Supposons qu'il soit d'ordre p. Alors $G/\mathcal{Z}(G)$ est d'ordre p, donc premier, donc cyclique, et l'on sait qu'alors G est abélien. ■

Contre-exemple. ***(Groupe d'ordre p^3 non abélien)***

Ceci ne fonctionne plus à l'ordre $k \leqslant 3$. On exhibe un groupe d'ordre $2^3 = 8$ non abélien. Le groupe D_8 des symétries du carré convient. □

En fait, plus généralement, on se rend compte que :

Propriété. ***(Groupes d'ordre p^2)***

Soit G un p-groupe opérant sur un ensemble fini E. Le nombre de points fixes de cette opération est congru au cardinal de E modulo p.

▷ Immédiat avec la formule des classes. ■

On peut se demander, dans un p-groupe, s'il existe toujours des sous-groupes d'ordre p^s. C'est le cas. On peut également redémontrer plus simplement le théorème de Cauchy dans ce cas particuleir.

Propriété

Dans un p-groupe, il existe toujours au moins un élément d'ordre p (et donc au moins $p-1$ éléments d'ordre p, puisque tous les éléments d'un groupe premier, celui engendré par lui, l'engendrent).

▷ Soit G un p-groupe. Soit $x \in G$ non trivial, puisque G est non trivial. Il est d'ordre p^r par le théorème de Lagrange. Ainsi $x^{p^{r-1}}$ est d'ordre $\frac{p^r}{p^r \wedge p^{r-1}} = p$. ■

Théorème. ***(Structure des sous-groupes d'un p-groupe)***

Si G est un p-groupe d'ordre p^a, alors pour tout $m \in [\![0,a]\!]$, G admet un sous-groupe d'ordre p^m (non nécessairement unique).

▷ On raisonne par récurrence sur a. Pour $a = 1$, on parle d'un groupe premier, il n'y a rien à faire. Supposons alors le résultat vrai au rang a et montrons-le au rang $a+1$. Soit G un groupe d'ordre p^{a+1}. Soit $m \in [\![1,a+1]\!]$. Si $m = a+1$, il suffit de prendre G lui-même. Sinon, $m \in [\![1,a]\!]$. Il existe un élément $x$de G d'ordre p. En regardant la preuve en détail, on peut même le prendre dans le centre de G, puisque le centre d'un p-groupe n'est pas trivial. On note $H = \langle x \rangle$ qui est donc distingué dans G. On considère $C = G/H$ qui est un groupe d'ordre p^a. On peut lui appliquer l'hypothèse de récurrence ; il existe donc un sous-groupe D de C d'ordre p^{m-1}, si $m \geqslant 1$; si $m = 0$, il suffisait de prendre le sous-groupe trivial. Par structure des sous-groupes du groupe quotient, il existe un sous-groupe K de G tel que $D = K/H$. On a alors $|H| = |D||H| = p.p^{m+1} = p^m$. Le résultat est ainsi démontré. ■

Ce sous-groupe n'a aucune raison d'être unique : dans le groupe diédral d'ordre 8, il y a au moins deux involutions distincts.

2.10.2 Les trois théorèmes de Sylow

Ces considérations vont en fait se généraliser dans le cas d'un groupe quelconque d'ordre fini. Pour tout diviseur premier de l'ordre de G, on va montrer qu'il existe un sous-groupe de G d'ordre $p^{v_p(|G|)}$ (et donner des caractéristiques liant les différents sous-groupes de cette sorte). Ce groupe est donc un sous-p-groupe, d'ordre maximal qui plus est ; en lui appliquant le théorème précédent, on obtient l'existence de nombreux sous-groupes d'un groupe fini quelconque *tant que l'on ne mélange pas les diviseurs premiers entre eux*, ce qui était tout de même licite, rappelons-le, pour les groupes cycliques.

Définition. ***(p-Sylow)***

Soit G un groupe fini d'ordre $p_1^{\alpha_1}...p_r^{\alpha_r}$. On appelle p_1-Sylow de G, tout sous-p-groupe de G d'ordre $p_1^{\alpha_1}$.

Fait

p ne divise pas le cardinal de G/S pour tout S où S est un p-Sylow de G.

Théorème. ***(Premier théorème de Sylow)***

Soient G un groupe fini et p un nombre premier divisant $|G|$.
Il existe au moins un p-Sylow dans G.

Une première démonstration repose sur l'application du théorème de Cauchy par récurrence.

▷ En particulier, G n'est pas trivial. Montrons le résultat par récurrence sur l'ordre de G. Pour l'ordre 2, c'est évident, qu'il n'y a qu'un seul groupe, d'ailleurs premier, de cet ordre. Supposons maintenant que G est d'ordre n et que la propriété est vraie pour tout groupe d'ordre $< n$.

Premier cas, il existe un sous-groupe strict de G tel que p ne divise pas $|G/H|$. Alors on applique l'hypothèse de récurrence à H ; il existe donc un p-Sylow de H. Mais puisque, en reprenant les notations précédentes, $|G/H| = p_2^{\alpha_2}...p_r^{\alpha_r}$, un p-Sylow de H est bien un p-sous-groupe de H d'ordre $p_1^{\alpha_1}$; c'est donc un p-Sylow de G.

Sinon, pour tout sous-groupe strict de G, p divise $[G : H]$. On exploite cette information à partir de l'équation aux classes. On a donc :

$$\mathrm{card}(G) = \mathrm{card}(\mathcal{Z}(G)) + \sum_{x \in \mathcal{T}, x \notin \mathcal{Z}(G)}^{[} G : C(x)]$$

avec les notations habituelles. On rappelle que $C(x)$ est un sous-groupe de G, strict pour tout $x \notin C(x)$. Par différence, $\mathcal{Z}(G)$ est d'ordre divisible par p ; par le théorème de Cauchy, ici même dans le cas abélien, il admet un élément d'ordre p engendrant un sous-groupe H, normal dans G par intercalation. On considère le quotient G/H. Il est d'ordre $p_1^{\alpha_1 - 1}s$ en notant $s = p_2^{\alpha_2}...p_r^{\alpha_r}$. Puisque ce nombre est $< n$, par hypothèse de récurrence, il admet un $p = p_1$-Sylow, c'est-à-dire un p-sous-groupe d'ordre $p_1^{\alpha_1 - 1}$. Ce groupe est de la forme K/H où G est donc un sous-groupe de $\mathcal{Z}(G) \leqslant G$ d'ordre $p_1^{\alpha_1}$, et le théorème est démontré. ■

On peut également donner une preuve constructive du p-Sylow de G. Elle repose sur le théorème de Cayley généralisé qui plonge tout groupe fini dans un sous-groupe du groupe général linéaire d'un corps fini.

Remarque. Ce théorème est plus fort que le théorème de Cauchy, et redonne l'existence d'un élément d'ordre p dans tout groupe dont l'ordre est divisible par p.

Théorème. ***(Second théorème de Sylow)***

Soient G un groupe fini et p un nombre premier divisant $|G|$.
Alors :

- tous les p-Sylow de G sont conjugués, sachant que le conjugué d'un p-Sylow est

un p-Sylow ; autrement dit, les p-Sylow de G sont exactement les conjugués d'un p-Sylow donné ;
- tout p-sous-groupe de G est contenu dans un p-Sylow de G ; autrement dit, les p-Sylow de G sont exactement les p-sous-groupes maximaux de G.

Lemme

Soit H un sous-groupe de G et S un p-Sylow de G. Alors il existe un sous-groupe conjugué à S intersectant H en un p-Sylow de H.

▷ Considérons l'action de H sur G/S par translation à gauche (sur un ensemble). Le stabilisateur d'une classe aS, $a \in G$, est clairement $aSa^{-1} \cap H$. En effet, si $h \in H$ vérifie $haS = aS$, alors $ha = as$ pour un certain $s \in S$ d'où $h \in aSa^{-1}$ et la réciproque est triviale. Notons a_1S,...,a_tS un système de représentants des orbites sous l'action considérée. En notant $X = \{a_1,...,a_t\}$, on a, par la formule des orbites, $\text{card}(G/S) = \sum_{x \in X} \frac{\text{card}(H)}{\text{card}(xSx^{-1} \cap H)}$. Comme S est un p-Sylow de G, p ne divise pas le cardinal de G/S. Il existe donc au moins un $x \in X$ tel que p ne divise par $\frac{\text{card}(H)}{\text{card}(xSx^{-1} \cap H)}$. Autrement dit, la valuation p-adique du cardinal de H est la valuation p-adique du cardinal de $xSx^{-1} \cap H$). Puisque clairement, par Lagrange, $xSx^{-1} \cap H$) est un sous-p-groupe de H, c'est alors un p-Sylow de H. ■

On reprend la preuve du théorème.

▷ Soit H un sous-groupe de G et S un p-Sylow de G. Alors d'après le lemme, il existe $g \in G$ tel que $gSg^{-1} \cap H$ soit un p-Sylow de H. En l'appliquant pour $H = G$, on trouve que gSg^{-1} est un p-Sylow de G (on ne s'en sert que dans la deuxième partie de la preuve). Soit S' un p-Sylow de G. En l'appliquant pour $H = S'$, on trouve que $S' = gSg^{-1}$ pour un certain g. S et S' étant arbitraires, tous les p-Sylow de G sont conjugués, ce qu'il fallait démontrer. Si maintenant H est un p-groupe quelconque, alors puisque H est l'unique p-Sylow de H, donc forcément dans le lemme précédent H est inclus dans gSg^{-1} qui est un p-Sylow de G, ce qu'il fallait démontrer. ■

Théorème. *(Troisième théorème de Sylow)*

Soient G un groupe fini et p un nombre premier divisant $|G| = p^m s$ où s est étranger à p. On note n_p le nombre de p-Sylow de G. Alors :
- n_p divise s,
- $n_p \equiv 1 \ [p]$.

▷ Le premier théorème de Sylow garantit qu'il existe au moins un p-Sylow S de G. Le deuxième théorème assure que l'ensemble des p-Sylow de S est l'ensemble des conjugués de S. C'est donc l'indice du normalisateur de S dans G ; il divise $|G|$ par le théorème de Lagrange. Remarquons que si nous montrons

$$n_p \equiv 1 \ [p]$$

, alors p est premier avec n_p, donc par le lemme de Gauss, n_p divise s. Montrons donc le second point.

Soit X l'ensemble des p-Sylow de G. Alors G agit sur X par conjugaison ; par restriction, S agit sur X par conjugaison. Or le cardinal d'une orbite divise le cardinal de S. Ainsi le cardinal d'une orbite est une puissance de p. Si elle n'est pas réduite au neutre, p le divise. Soit T un p-Sylow de G, fixe par l'action de S sur X. Soit H le sous-groupe engendré par S et T. T étant invariant sous l'action de S, on a $ST = TS$, d'où $H = TS = ST$ puis d'après la formule du produit, $|H||S \cap T| = |S||T| = p^{2m}$. Donc l'ordre de H divise p^{2m}. Puisque $|H| \geqslant p^m$, H est d'ordre une puissance de p. Or par le théorème de Lagrange, l'ordre de H divise $n = p^m s$ donc $|H| = p^m$ et d'ailleurs H est un p-Sylow de G. Ainsi $\text{card}(S \cap T) = p^m$, donc $S = T$. Ainsi, S est l'unique p-Sylow fixé par l'action par conjugaison de S. Alors l'équation aux classes pour cette action montre que $\text{card}(X) \equiv 1 \ [p]$. ■

Méthode. ***(Exhiber un sous-groupe distingué grâce à Sylow)***

On peut, grâce à l'utilisation conjointe des trois théorèmes de Sylow, exhiber des sous-groupes distingués d'un groupe de cardinal quelconque. On choisit l'un des facteurs premiers de la décomposition de son ordre ; le premier théorème fournit l'existence d'un sous-groupe H d'ordre $p^{v_p(|G|)}$. Grâce au second théorème, on sait que les p-Sylow de G sont exactement ses conjugués. Le troisième théorème donne des informations sur le nombre de ces conjugués en fonction d'une congruence et du produit des autres facteurs premiers de $|G|$ à leur bonne valuation. Si l'on arrive à en déduire que ce nombre est 1, alors H n'a qu'un seul conjugué, il est donc distingué dans G.

Exercice 65

1. Montrer que tout groupe d'ordre 15 est cyclique.
2. Montrer qu'un groupe d'ordre 350 ne peut être simple.

▷ **Éléments de réponse.**

On applique la méthode précédente. Dans le premier cas, on obtient un sous-groupe d'ordre 3 qui est normal et un sous-groupe d'ordre 5. Puisque 3 et 5 sont premiers entre eux, leur intersection est réduite au neutre. Ainsi G est isomorphe à leur produit, qui est cyclique. Dans le deuxième cas, on écrit $350 = 2 \times 5^2 \times 7$ et l'on regarder les 5-Sylow de G.

Remarque. Dans la méthode ci-dessous, on a intérêt à choisir un facteur premier qui élevé à la bonne valuation donne un diviseur petit (et donc un complémentaire petit et une congruence étroite).

2.11 Théorème de structure des groupes abéliens finis

Astuce !

Les théorèmes de classification, quels qu'ils soient, permettent de trouver la structure d'un groupe à partir de son cardinal ; on laisse méditer la puissance de ce raisonnement.

2.11.1 Exposé du théorème de classification

Théorème. ***(Classification des groupes abéliens de type fini, Kronecker)***

Soit G un groupe abélien de type fini. Alors il existe un unique entier naturel n et une unique suite $(a_1,...,a_k)$, $k \in \mathbb{N}$, d'entiers > 1 tels que :

$$G \simeq \mathbb{Z}^n \times \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times ... \times \mathbb{Z}/a_k\mathbb{Z},$$

où a_{i+1} divise a_i pour tout $i \in [\![1,k-1]\!]$.
Réciproquement, un tel groupe est un groupe abélien de type fini.

On montre l'unicité d'une telle décomposition.

▷ Exercice du Cassini. ■

Ce théorème n'a que peu d'intérêt sans sa démonstration qui permet de construire la décomposition.

2.11.2 Démonstration de l'existence du théorème de classification

Soit $(A,+)$ un groupe abélien et p un nombre premier.

Définition. ***(Partie p-primaire de A, torsion p-primaire de A)***

On note $A(p)$ le sous-groupe des éléments de A dont l'ordre est une puissance de p. On l'appelle *partie p-primaire* ou *torsion p-primaire* de A, car toute partie primaire est évidemment un groupe de torsion.

Proposition

Si A est fini, alors $A(p)$ est un p-groupe (c'est-à-dire, par définition, que son cardinal est une puissance de p).

Théorème

Si A est un groupe abélien fini, alors $A = \prod_{p \in \mathcal{P},\ p \mid \mathrm{ord}(A)} A(p)$.

▷ On raisonne par récurrence sur l'exposant de G noté d. Par définition, d est le plus petit entier tel que pour tout $x \in A$, $\alpha x = 0$. En particulier, l'exposant divise l'ordre. Si d est une puissance de p, alors $A = A(p)$ et il n'y a rien à démontrer. Supposons donc que $d = mm'$ avec m et $m' > 1$ et $(m,m') = 1$ (notation pour : premiers entre eux). Par l'identité de Bézout, il existe deux entiers r et s tels que $rm + rm' = 1$. Donc $A = (rm + sm')A = rmA + sm'A \subseteq mA + m'A \subseteq A$ d'où $A = mA + m'A$. Montrons que cette somme est directe : soit $x \in mA \cap m'A$. Alors $m'x = mx = 0$ donc $x = (rm + sm')x = 0$. Ainsi A est le produit direct de mA et $m'A$.

Soit $A_m = \{x \in A \mid mx = 0\}$. Alors $A_m = m'A$. En effet, $A_m \supseteq m'A$ car $d = mm'$ est l'exposant de G, et inversement, si $x \in A_m$, alors $x = (rm + sm')x = m'sx \in m'A$ d'où l'égalité. Symétriquement $A_{m'} = mA$. Or l'ordre de A_m est plus petit que m, et celui de $A_{m'}$ est plus petit que m'. On applique l'hypothèse de récurrence à ses deux groupes, donc $A_m = A(p_1) \times ... \times A(p_n)$, p_1,...,p_n les facteurs premiers de ord(A_m) et $A_{m'} = A(q_1) \times ... \times A(q_r)$, q_1,...,q_r les facteurs premiers de ord$(A_{m'})$ et il est évident que, par primalité relative, aucun des p n'égale un q. ■

Remarque. Joint avec la proposition précédente, ce théorème est cohérent avec le théorème fondamental de l'arithmétique.

Exemple. ***(Une illustration triviale)***

On considère $\mathbb{Z}/2022\mathbb{Z}$. Puisque $2022 = 2 \times 3 \times 337$, on peut poser $m = 6$ et $m' = 337$. Ainsi $A = A_6 \times A_{337}$. Or $A_6 = 337A = 337\mathbb{Z}/2022\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z}$ et $A_{337} = 6A = 6\mathbb{Z}/2022\mathbb{Z} \simeq \mathbb{Z}/337\mathbb{Z}$. On recommence avec $\mathbb{Z}/6\mathbb{Z}$ et l'on obtient que $\mathbb{Z}/2022\mathbb{Z} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/337\mathbb{Z}$, ce qui était donné immédiatement par le théorème chinois.

On aura donc utilisé les deux lemmes suivants dont on laisse la démonstration au lecteur :

Lemme

Si $n = p_1^{\alpha_1}...p_r^{\alpha_r}$, alors

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times ... \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}.$$

Lemme

Pour tous entiers n,m, on a :

$$n\mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/(\frac{m}{n \wedge m})\mathbb{Z}.$$

Ce théorème et ces propriétés décomposer ainsi tous les groupes cycliques. Nous voulons étendre ces raisonnements à tous les groupes abéliens finis d'un certain ordre quelconque *(voir les exercices)*.

Poussons maintenant plus loin la décomposition.

Définition. ***(Groupe de type*** $(p_1^{r_1},...,p_s^{r_s})$***)***

Un groupe A est dit de type $(p_1^{r_1},...,p_s^{r_s})$ s'il est isomorphe à un produit de p-groupes cycliques d'ordre p^{r_i}, soit $A \simeq \mathbb{Z}/p_1^{r_1}\mathbb{Z} \times ... \times \mathbb{Z}/p_s^{r_s}\mathbb{Z}$.

Théorème

Tout p-groupe abélien fini est isomorphe à un produit de p-groupes cycliques. S'il est de type $(p^{r_1},...,p^{r_s})$ avec $r_1 \geqslant ... \geqslant r_s \geqslant 1$, alors la suite $(r_1,...r_s)$ est unique.

▷ On procède en plusieurs étapes.

Lemme

Soit A un p-groupe abélien fini et $b \in A prive \{0\}$. Supposons que $pb,p^2b,...,p^kb$ sont non nuls et soit p_n l'ordre de p^kb. Alors b a pour ordre p^{k+m}.

▷ L'ordre de $p^kb \in A$ est bien une puissance de p d'après le théorème de Lagrange, A étant un p-groupe. Par hypothèse, $p^{k+m}b = p^m(p^kb) = 0$. Si $p^nb = 0$, alors tout d'abord $n > k$ par hypothèse sur les p^ib, $i \leqslant k$. Ensuite $n - k \geqslant m$ puisque sinon l'ordre de p^kb serait plus petit que p^m, puisque $p^np^kb = p^kp^nb = 0$. Ceci caractérise l'ordre de b. ■

Exercice 66

Expliciter l'exemple $A = \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$, $p = 3$, $|A| = 3^6$ et $b = (3,1)$.

▷ Nous allons maintenant prouver l'existence du produit désiré par récurrence sur l'ordre de A. Soit a_1 un élément d'ordre maximal. Soit $A_1 = \langle a_1 \rangle$, disons d'ordre p^{r_1}. ■

Lemme

Soit $\overline{b} \in A/A_1$ d'ordre p^r. Alors il existe un représentant a de $\overline{b}$ dans A ayant le même ordre p^r.

▷ Soit b un représentant de $\overline{b}$ dans A. Alors $p^rb \in A_1$. Donc $p^rb = na_1$ avec $n = p^kn \geqslant 0$ où p ne divise pas n. On peut supposer $k < r_1$, car sinon $p^rb = 0$ et b serait d'ordre p^r $(\text{ord}(\overline{b}) \leqslant \text{ord}(na_1))$ est aussi un générateur du p-groupe cyclique A_1. na_1 est donc d'ordre p_1^r. ■

2.12 Groupes résolubles

2.12.1 Un mot sur les groupes simples

Un sous-groupe d'un groupe simple n'est pas nécessairement simple (oui.)
Voici un argument marteau. Si c'était le cas, alors, tout groupe serait simple ou un groupe de permutations, et c'est faux, prendre $\mathbb{Z}/4\mathbb{Z}$. En effet (Cayley), tout groupe est isomorphe à un sous-groupe d'un groupe de permutations. Si ce n'est pas ce groupe, c'est donc le groupe alterné, qui est simple, ou un sous-groupe, qui serait donc simple.

2.12.2 Commutateurs, groupe dérivée, abélianisé

Définition. ***(Commutateur)***

Soit G un groupe. On appelle *commutateur* de G tout élément de la forme $[x,y] = xyx^{-1}y^{-1}$ où $x,y \in G$.

Définition. ***(Groupe dérivé)***

Soit G un groupe. On appelle *groupe dérivé* de G, et l'on note $D(G)$ ou G' ou $[G,G]$, le sous-groupe de G engendré par les commutateurs.

Remarque. Parfois l'ensemble des commutateurs est un groupe, parfois non.

Propriété. ***(Abélianisé)***

G' est distingué dans G. On appelle *abélianisé* de G le quotient $G/G' = G^{ab}$. Alors G' est le plus petit sous-groupe distingué de G tel que G/H soit abélien, au sens suivant : si G/H est abélien, et H est distingué dans G, alors $H \supseteq G'$.

▷ En effet, par propriété universelle, tout morphisme de G vers un groupe abélien se factorise à travers $G/G' = Ab(G)$. ■

Méthode. ***(Non-isomorphie par les dérivés)***

Soient G,H deux groupes. Si G' et H' ne sont pas isomorphes, alors G et H ne sont pas isomorphe (le montrer).

2.12.2.1 Propriétés opératoires de la dérivation de groupes

Propriété. ***(Dérivée d'une somme directe)***

Le groupe dérivé d'une somme directe de groupes G_i est la somme directe des groupes dérivées $D(G_i)$.

Propriété. ***(Dérivée d'un produit direct)***

Le groupe dérivé d'un produit direct de groupes G_i est le sous-groupe constitué des éléments g pour lesquels il existe $n_g \in \mathbb{N}$ tel que, pour tout i, la composante g_i de g soit le produit de n_g commutateurs.

Propriété. ***(Dérivée d'un produit semi-direct)***

Soit $G = H \rtimes K$. Alors $D(G) = (D(H)[H,K]) \rtimes D(K)$.

▷ En effet, $D(G)$ est le sous-groupe engendré par la réunion des trois sous-groupes $D(H)$, $[H,K]$, inclus dans H, et $D(K)$, or l'ensemble $D(H)[H,K]$ est un sous-groupe de H, stable par l'action de K donc par celle du groupe $D(K)$. ■

2.12.2.2 Dérivation d'ordre supérieur

2.12.2.3 Compléments

Définition. ***(Groupe carré)***

Soit G un groupe. On pose $C(G) = C = G^2 = \langle x^2, x \in G \rangle$.

Lemme

$D(G) \subseteq C(G)$.

▷ $xyx^{-1}y^{-1} = x^2(x^{-1}y)(x^{-1}y)(y^{-1})^2$ produit de carrés. ■

Propriété. ***(Groupe carré dérivé)***

Soit G un groupe engendré par ses involutions. Alors $C = D$.

▷ Soit $x \in G$. Alors par hypothèse $x = x_1...x_p$ des éléments d'ordre 2. En particulier $x = x_1...x_px_1...x_p$. Pour $p = 1$, $x^2 = e$. Pour $p = 2$, $x^2 = x_1x_2x_1^{-1}x_2^{-1}$. Par récurrence, si le produit de $p-1$ involutions a son carré dans D, alors $x_1...x_px_1...x_p = x_1(x_2...x_p)x_1(x_2...x_p)-1(x_2...x_p)^2$ est le produit d'un commutateur et de quelque chose dans D par hypothèse. Ainsi $x^2 \in D$. On a le résultat. ■

Application. ***(Théorème du groupe carré dérivé)***

1. Le groupe symétrique est engendré par les transpositions. Il est clair que son carré est $\mathfrak{A}_n$. On en déduit que le dérivé de $\mathfrak{S}_n$ est $\mathfrak{A}_n$.
2. Soit $G = O_2(\mathbb{Q})$ le groupe multiplicatif des matrices 2×2 à coefficients dans $\mathbb{Q}$. Comme G est engendré par les symétries, $D(G) = C(G)$. Alors D est un sous-groupe de $\mathcal{SO}_2(\mathbb{R})$, car engendré par les carrés qui sont des matrices de déterminant 1. On peut même montrer que D est un sous-groupe strict de $\mathcal{SO}_2(\mathbb{R})$.

2.12.3 Résolubilité

Définition. ***(Groupe résoluble)***

Un groupe G est dit *résoluble* s'il existe $n \in \mathbb{N}$ et $\{e\} \subseteq G_0 \subseteq G_1 \subseteq .. \subseteq G_n = G$ une suite de sous-groupes de G tels que $G_i \triangleleft G_{i+1}$ et G_{i+1}/G_i est abélien pour tout $i \in [\![1, n[\![$. Une telle suite est appelée *suite de résolubilité*.

Intuitivement, les groupes résolubles sont des groupes qui sont proches d'être abéliens ; ils se reconstruisent par morceaux de groupes abéliens.

Propriété. ***(Résolubilité des groupes abéliens)***

Tout groupe abélien est résoluble.

▷ La suite $\{e\} \triangleleft G$ convient. En effet, $G \simeq G/\{e\}$ est abélien. ■

On comprend avec le fait précédent, que dans le cas des groupes abéliens, on va pouvoir obtenir des groupes abéliens *en sautant moins haut*, en rajoutant des échelons à l'échelle.

Fait. ***(Lien entre simplicité et résolubilité)***

Un groupe simple (il n'y a pas d'échelons) est résoluble si et seulement s'il est abélien. En particulier, un groupe simple non abélien est non résoluble.

Propriété. ***(Condition suffisante de résolubilité)***

Soit G un groupe et $\{e\} \subseteq G_1 \subseteq ... \subseteq G_n \subseteq G$ une suite de sous-groupes tous distingués dans G. Alors pour tout i, G_i est distingué dans G_{i+1} et si G_{i+1}/G_i est abélien pour tout i, alors G est résoluble.

▷ Conséquence de la propriété d'intercalation. ■

On verra qu'en fait, cette condition est nécessaire.

La résolution d'un groupe se reformule à l'aide de la suite des groupes dérivés (revoir donc la notion de Dérivation aux ordres supérieurs à 1).

Propriété. ***(Caractérisation de la résolubilité)***

Un groupe G est résoluble si et seulement si la suite des groupes dérivés $D^n(G)$, $n \in \mathbb{N}^*$ est stationnaire à $\{e\}$.

▷ Si c'est le cas, on a directement une suite de résolution donnée, si N est l'ordre de stationnarité de $(D^n(G))_n$, par $\{e\} \subseteq D^{N-1}(G) \subseteq ... \subseteq D(D(G)) \subseteq D(G) \subseteq G$. C'est la réciproque qu'il faut démontrer : elle montre que cette condition est nécessaire, donc pas trop forte. On a $\{e\} G_n \subseteq ... \subseteq G_0 = G$ une suite de sous-groupes vérifiant la condition de résolubilité. Puisque G/G_1 est abélien, $D(G) \subseteq G_1$. De même, puisque G_1/G_2 est abélien, $D^2(G) = D^1(G)' \subseteq G_1' \subseteq G_2$. Puisque G_2/G_3 est abélien, $D^3(G) = D^2(G)' \subseteq G_2' \subseteq G_3$, et ainsi de suite. Par suite, pour tout $i \in [\![1,n]\!]$, $D^i(G) \subseteq G_i$. Ainsi $D^n(G) \subseteq \{e\}$ soit $D^n(G) = \{e\}$. ■

Corollaire

Si G est résoluble, il existe une suite de sous-groupes

$$\{e\} \subseteq G_0 \subseteq G_1 \subseteq ... \subseteq G_n = G$$

avec $G_i \triangleleft G$ pour tout i et G_{i+1}/G_i abélien.

▷ Il suffit de choisir la suite des sous-groupes dérivés. En effet, pour tout i, $D^i(G) \triangleleft G$. En effet, le sous-groupe des commutateurs est pleinement caractéristique. En effet, pour tout automorphisme σ de G, $\sigma[x,y] = [\sigma(x), \sigma(y)]$ donc $\sigma(G') = G'$. Par récurrence immédiate, $\sigma(D^i(G)) = D^i(G)$. ■

Dans le cas des groupes *finis*, on peut demander encore plus fort sur la forme des quotients successifs.

Corollaire. ***(Résolubilité dans le cas fini)***

Si G est résoluble et fini, il existe une suite de sous-groupes

$$\{e\} \subseteq G_0 \subseteq G_1 \subseteq ... \subseteq G_n = G$$

avec $G_i \triangleleft G$ pour tout i et G_{i+1}/G_i premier (donc cyclique, donc abélien), soit de la forme $\mathbb{Z}/p_i\mathbb{Z}$.
Une telle suite de résolubilité est dite *maximale*.

▷ Disons qu'une suite telle que précédemment est *maximale* si l'on ne peut pas la raffiner avec par exemple $G_i \subseteq H \subseteq G_{i+1}$ avec H distinct de G_i et G_{i+1} et G_{i+1}/H, H/G_i abéliens. Comme G est fini, il n'y a qu'un nombre fini de sous-groupes, donc il existe une telle suite maximale : en

effet, à partir d'une séquence de résolubilité, on raffine chaque portion jusqu'à épuiser le nombre de sous-groupes. Si G_{i+1}/G_i n'est pas de la forme $\mathbb{Z}/p\mathbb{Z}$ pour un certain nombre premier p, il contient un sous-groupe non trivial H'. Il est donc de la forme H/G_i où H est un sous-groupe de G_{i+1} contenant G_i, soit $G_i \subsetneq H \subsetneq G_{i+1}$. En particulier, G_i est distingué dans H par intercalation et H/G_i est abélien par sous-groupe d'un groupe abélien ; de plus, H est distingué dans G_{i+1} et G_{i+1}/H est abélien : en effet, le troisième théorème d'isomorphisme donne $\frac{G_{i+1}/G_i}{H/G_i} \simeq G_{i+1}/H$ qui est donc un groupe, donc H est distingué, et abélien comme quotient d'un groupe abélien. ■

2.12.4 Propriétés opératoires de la résolubilité

On énonce quelques propriétés opératoires sur les groupes résolubles. La seconde permet de scinder les problèmes de résolubilité en problèmes plus petit.

Proposition. ***(Sous-groupe d'un groupe résoluble)***

Soient G un groupe et $H \subseteq G$ un sous-groupe de G. Si G est résoluble, alors H est résoluble.

▷ Soit une suite $G_n = \{e\} \subseteq G_{n-1} \subseteq ... \subseteq G_1 \subseteq G_0 = G$ avec $G_{i+1} \triangleleft G_i$ et G_{i+1}/G_i abélien. On introduit $H_i = H \cap G_i$ pour tout i. Alors les H_i forment une suite de sous-groupes de la même forme que précédemment, avec $H_{i+1} \triangleleft H_i$ pour tout i. Puisque clairement l'homomorphisme $H_i \longrightarrow G_i \longrightarrow G_i/G_{i+1}$ a pour noyau H_{i+1}, on a un plongement $H_i/H_{i+1} \longrightarrow G_i/G_{i+1}$, ce qui prouve que H_i/H_{i+1} est abélien. ■

Lemme

Soient G un groupe et $H \leqslant G$. Si G est abélien, alors H et G/H sont abéliens.

Proposition. ***(Théorème de recomposition)***

Soient G un groupe et $H \subseteq G$ un sous-groupe distingué de G. Alors G est résoluble si et seulement si H est résoluble et G/H est résoluble.

▷ Gardons les notations précédentes et notons $s : G \longrightarrow G/H$ la projection canonique. On obtient la suite de sous-groupes $s(G_n) = \{e\} \subseteq s(G_{n-1}) \subseteq ... \subseteq s(G_1) \subseteq s(G_0) = G/H$ et l'on a que $s(G_{i+1}) \triangleleft s(G_i)$, car l'image d'un sous-groupe distingué par un homomorphisme est un sous-groupe distingué de l'image de cet homomorphisme. De plus, la flèche $G_i \longrightarrow s(G_i) \longrightarrow s(G_i)/s(G_{i+1})$ est surjective et a pour noyau un sous-groupe de G_i contenant G_{i+1}. Il induit donc un homomorphisme surjectif $G_i/G_{i+1} \longrightarrow s(G_i)/s(G_{i+1})$. Par suite, $s(G_i)/s(G_{i+1})$ est abélien, comme quotient du groupe abélien G_i/G_{i+1}. Ainsi la condition n'est pas trop forte.

Inversement, supposons H et G/H résolubles. On a donc deux suites de sous-groupes $G'_n = \{e'\} \subseteq G'_n \subseteq G'0 = G/H$ et $H_m = \{e\} \subseteq H_{m-1} \subseteq H_0 = H$ avec chaque sous-groupe distingué dans le suivant et tous quotients abéliens. Introduisons pour tout i qui existe, $G_i = s(G'_i)$. On obtient la suite de

sous-groupes $G_n = H \subseteq G_{n-1} ... \subseteq G_1 \subseteq G_0 = G$ avec immédiatement $G_{i+1} \triangleleft G_i$. L'homomorphisme de groupes $G_i = s^{-1}(G'_i) \longrightarrow G'_i \longrightarrow G'_i/G'_{i+1}$ est surjectif de noyau $G_{i+1} = s^{-1}(G'_{i+1})$; on en déduit un isomorphisme $G_i/G_{i+1} \simeq G'_i/G'_{i+1}$ et le fait que G_i/G_{i+1} est abélien. Il suffit de raccorder ces deux suites pour obtenir la résolution de G. ■

Le corollaire suivant sert à la construction des groupes résolubles dans la classification des groupes.

Propriété. ***(Résolubilité grossière)***

Si G est un groupe fini non simple, et si tout groupe d'ordre strictement inférieur à celui de G est résoluble, alors G est résoluble.

▷ En effet, soit G un tel groupe et H un sous-groupe distingué non trivial ; il en existe, car G est supposé non simple. Alors H est de cardinal strictement inférieur et G/H est de cardinal strictement inférieur par Lagrange. On applique donc l'hypothèse puis on recolle par le théorème précédent. ■

Exercice 67

Soit p un nombre premier. Montrer que tout p-groupe est résoluble, et que l'on peut choisir une suite de résolubilité descendant d'un point dans la puissance de son cardinal à chaque sous-groupe.

▷ **Éléments de réponse.**

Soit G un groupe d'ordre p^n. On raisonne par récurrence sur n. Pour $n = 1$, le groupe est premier, donc abélien. Pour l'hérédité, le centre d'un p-groupe n'étant pas trivial, on a $H = \mathcal{Z}(G)$ distingué dans G et G/H est, par Lagrange, un p-groupe d'ordre $< n$. Or $\mathcal{Z}(G)$ est abélien donc résoluble, et par hypothèse, G/H est résoluble. Ainsi G est résoluble.

On montre dans la section suivant qu'en rajoutant un facteur premier dans la décomposition de l'ordre, on obtient encore des groupes résolubles : il faudra donc au moins trois facteurs premiers dans $|G|$ pour que le groupe G soit non résoluble.

Proposition. ***(Produit de groupes résolubles)***

Le produit de deux groupes résolubles est résoluble si et seulement si chacun des facteur l'est.

2.12.5 Résolution des petits groupes

Théorème. ***(Théorème de Burnside)***

Tout groupe n'ayant que deux facteurs premiers dans la décomposition de son ordre est résoluble.

▷ On raisonne par l'absurde. Soit G un tel groupe non résoluble. Puisque $\mathbb{N}$ est bien ordonné, on peut supposer que G est d'ordre minimal $p^n q^m$.

Alors G est non nul. De plus, G est un groupe simple. En effet, si G admettait un sous-groupe distingué H non trivial, alors H et G/H seraient résolubles par minimalité de G, leurs ordres ne comportant par théorème de Lagrange que des puissances de p ou de q. Par recollement, G serait résoluble. De plus, ni n, ni m ne sont nuls, autrement, si n est nul, G est un q-groupe, donc résoluble. Enfin, G n'est pas abélien, car sinon résoluble, donc par simplicité, son centre, qui en est un sous-groupe distingué, est réduit au nul.

Le premier théorème de Sylow assure l'existence d'un sous-groupe S de G d'ordre p^n. Comme S est un p-groupe non trivial, son centre $Z(S)$ est non trivial ; soit g dedans non trivial. Le nombre de conjugués de g est égal à l'indice du centralisateur de g, qui divise l'indice q^m de son sous-groupe S. Ce nombre est donc de la forme q^d. De plus, g est supposé non central dans G car différent de 1 donc $d > 0$.

Soit $(\chi_i)_{i\in[\![1,h]\!]}$ la famille des caractères sur $\mathbb{C}$ irréductibles de G, où ici χ_1 désigne le caractère trivial. Comme g n'est pas dans la même classe de conjugaison que 1, la relation d'orthogonalité sur les colonnes de la table des caractères donne $0 = \sum_{i=1}^{h} \chi_i(1)\chi_i(g) = 1 + \sum_{i=2}^{h} \chi_i(1)\chi_i(g)$. Or les $\chi_i(g)$ sont des entiers algébriques, comme sommes de racines de l'unité. Si tous les caractères irréductibles non triviaux qui ne s'annulent pas en g prenaient en 1 une valeur multiple de q, on en déduirait que le nombre $-\frac{1}{q} = \sum_{i>2,\chi_i(g)\neq 0} \frac{\chi_i(1)}{q}\chi_i(g)$ est un entier algébrique comme combinaison linéaire à coefficients dans $\mathbb{Z}$ d'entiers algébriques, ce qui est absurde. Ainsi, il existe un caractère irréductible χ non trivial, tel que l'entier $\chi(1)$ ne soit pas divisible par q et que le complexe $\chi(g)$ soit non nul.

Soit u l'élément de l'algèbre du groupe G sur les nombres complexes égal à la somme des q^d éléments de la classe de conjugaison c_g de g. Alors on sait que le complexe suivant est un entier algébrique : $\frac{1}{\chi(1)} \sum_{s\in G} u_s\chi(s) = \frac{1}{\chi(1)} \sum_{s\in c_g} \chi(g) = \frac{q^d\chi(g)}{\chi(1)}$. Puis, q étant premier avec $\chi(1)$, le théorème de Bézout donne a,$b \in \mathbb{Z}$ tels que $aq^d + b\chi(1) = 1$. Donc $\frac{\chi(g)}{\chi(1)} = a\frac{q^d\chi(g)}{\chi(1)} + b\chi(g)$. La valeur $\chi(g)/\chi(1)$ est donc combinaison linéaire à coefficients entiers d'entiers algébriques, donc elle est algébrique.

L'image de g par la représentation ρ de caractère χ, est une homothétie. En effet, notons ζ le nombre complexe $\chi(g)/\chi(1)$. C'est un entier algébrique, non nul, donc sa norme $N(\zeta)$, produit de ses conjugués, c'est-à-dire des racines de son polynôme minimal sur $\mathbb{Q}$, est un entier relatif non nul. Or ζ est moyenne arithmétique de racines de l'unité : les valeurs propres de $\rho(g)$, donc ses conjugués aussi, donc tous sont de module $\leqslant 1$. Comme leur produit est de module $\geqslant 1$, tous sont en fait de module 1, en particulier ζ, ce qui signifie que les valeurs propres de $\rho(g)$ sont égales, donc que $\rho(g)$ est une homothétie.

Concluons ; soit N le noyau de ρ. L'homothétie $\rho(g)$ est bien évidemment centrale dans $\mathrm{Im}(g)$ qui est canoniquement isomorphe à G/N, alors que g n'est pas central dans G. Par conséquent, le sous-groupe normal N du groupe simple G est non trivial, donc égal à G, si bien que la représentation ρ est triviale, ce qui contredit le choix de χ. ■

Exercice 68

Montrer que tout groupe d'ordre < 60 est résoluble.

▷ **Éléments de réponse.**

On utilise les théorèmes de Sylow. D'après le lemme de Burnside, si G est un groupe d'ordre < 60 doit être non résoluble, il admet au moins trois facteurs premiers distincts dans sa décomposition en facteurs premiers. Avec la condition de majoration, seuls $30 = 2 \times 3 \times 5$ et $42 = 2 \times 3 \times 7$ conviennent. Or dans le premier cas, G admet 10 3-Sylow deux à deux disjoints et 6 5-Sylow deux à deux disjoints, donc 10.2 éléments d'ordre 3 et 6.4 éléments d'ordre 5, ce qui est impossible, car $20 + 24 > 30$. Dans le deuxième cas, G admet un 7-Sylow et le nombre de ses conjugués divise 6 et est congru à 1 modulo 7, même conclusion. Dans tous les cas, G admet un sous-groupe distingué, et ni G, ni G/H ne sont égaux à 30 ou 42, donc sont résolubles. Par recollement, G est résoluble.

On voit dans la section suivante que le plus petit groupe non résoluble est exactement d'ordre 60.

2.12.6 Simplicité du groupe alterné

Théorème. ***(Simplicité du groupe alterné)***

Pour $n \geqslant 5$, $\mathfrak{A}_n$ est simple.
Ainsi, $\mathfrak{A}_n$ est simple si et seulement si $n = 2{,}3$ ou $n \geqslant 5$.

▷ On observe que si $n \geqslant 5$, tous les 3-cycles sont conjugués dans $\mathfrak{A}_n$. On sait déjà que si σ est un 3-cycle, il existe $\rho \in \mathfrak{S}_n$ telle que $\sigma = \rho(1,2,3)\rho^{-1} = \rho(4,5)(1,2,3)(4,5)^{-1}\rho^{-1} = \rho'(1,2,3){\rho'}^{-1}$. On a $\varepsilon(\rho) = -\varepsilon(\rho')$, donc ρ ou $\rho' \in \mathfrak{A}_n$. Ainsi les 3-cycles forment une unique classe de conjugaison dans $\mathfrak{A}_n$.

Remarquons également que si H, sous-groupe distingué de $\mathfrak{A}_n$, contient un 3-cycle, alors il les contient tous par distinction dans $\mathfrak{A}_n$ = stabilité par conjugaison. Comme $\mathfrak{A}_n$ est engendré par les 3-cycles, on en déduit $H = \mathfrak{A}_n$.

On montre que $\mathfrak{A}_n$ est simple par récurrence sur $n \geqslant 5$.

Montrons que $\mathfrak{A}_5$ est simple. Soit $\{id\} \neq H \triangleleft \mathfrak{A}_5$. On veut montrer $H = \mathfrak{A}_5$. On observe par un

simple exercice de combinatoire[1], on observe que $\mathfrak{A}_5$ est la réunion disjointe de l'identité, les doubles transpositions, les 3-cycles et les 5-cycles. S'il existe un 3-cycle dans H, alors c'est terminé. S'il existe une double transposition dans H, disons, pour fixer les idées, $\tau = (1,2)(3,4) \in H$, pour $\rho \in \mathfrak{A}_5$, $\rho\tau\rho^{-1} = (\rho(1),\rho(2))(\rho(3),\rho(4))$, en choisissant ici $\rho = (3,4,5) \in \mathfrak{A}_5$, alors $\rho\tau\rho^{-1} = (1,2)(4,5) \in H$, donc $\tau(\rho\tau\rho^{-1}) = (3,4)(4,5) \in H$. Mais c'est un 3-cycle en puissance, donc c'est terminé. Il reste à montrer le cas où H contient un 5-cycle. Prenons $\sigma = (1,2,3,4,5)$ pour exemple : on calcule $\sigma^{-1}\rho\sigma\rho^{-1} = (5,4,3,2,1)(1,2,5,3,4) = (2,4,5)$ à la main. Dans tous les cas, H contient un 3-cycle est c'est terminé.

Montrons enfin que pour tout $n \geqslant 6$, si $\mathfrak{A}_n$ est simple, alors $\mathfrak{A}_{n+1}$ est simple. Soit $\{id\} \neq H \triangleleft \mathfrak{A}_n$. Introduisons $G_i = \{\sigma \in \mathfrak{A}_n \mid \sigma(i) = i\}$. Alors clairement $G_i \simeq \mathfrak{A}_{n-1}$ de même que $\{\sigma \in \mathfrak{S}_n \mid \sigma(i) = i\} \simeq \mathfrak{S}_{n-1}$. Or par intercalation, $H \cap G_i \triangleleft G_i$, et comme par hypothèse de récurrence, G_i est simple, $H \cap G_i = id$ ou G_i. S'il existe i avec $G_i \cap H \neq \{id\}$, alors $G_i \subseteq H$, mais G_i contient clairement un 3-cycle, car $n \geqslant 4$, donc H qui lui est égal aussi, donc $H = \mathfrak{A}_n$. Montrons simplement que $G_i \cap H = \{i\}$ $\forall i \in [\![1,n]\!]$ ne peut. Soit $\sigma \in Hprive\{id\}$. Supposons $\forall i, \sigma \notin G_i$. On a $\sigma(1) = i \neq 1$, i ainsi défini ; choisissons $j \notin \{1,i\}$. Alors $\sigma(j) = k$ avec $k \neq j$. Choisissons l,m distincts $\notin \{1,i,j,k\}$, ce qui est possible, car $n \geqslant 6$. Posons $\rho = (j,l,m)$. Alors $\tau = (\rho^{-1}\sigma^{-1}\rho)\sigma \in H$, $k,1,i \notin \text{support}(\rho)$. Ainsi $\tau(1) = \rho^{-1}\sigma^{-1}\rho\sigma(1) = \rho^{-1}\sigma^{-1}\rho(i) = \rho^{-1}\sigma^{-1}(i) = \rho^{-1} = 1$, d'où $\tau \in G_1$. De même, $\tau(j) = \rho^{-1}\sigma^{-1}\rho\sigma(j) = \rho^{-1}\sigma^{-1}\rho(k) = \rho^{-1}\sigma^{-1}(k) = \rho^{-1}(j) = m \neq j$, donc $\tau \neq id$. ■

Corollaire. ***(Non-résolubilité du groupe alterné)***

Pour $n \geqslant 5$, $\mathfrak{S}_n$ n'est pas résoluble.
Ainsi, $\mathfrak{S}_n$ est résoluble si et seulement si $n \leqslant 5$.
Plus précisément, les sous-groupes distingués de $\mathfrak{S}_n$ sont les sous-groupes triviaux, le sous-groupe alterné, et le groupe de Klein si $n = 4$.

▷ En effet, s'il l'était, tous ses sous-groupes le seraient. Or $\mathfrak{A}_k$ est simple non abélien, donc n'est pas résoluble. Plus explicitement, si $H \triangleleft \mathfrak{S}_n$, alors $H \cap \mathfrak{A}_n \triangleleft \mathfrak{A}_n$ donc ou bien $H \cap \mathfrak{A}_n = \mathfrak{A}_n$, donc $\mathfrak{A}_n \subseteq H \subseteq \mathfrak{S}_n$ donc $H = \mathfrak{A}_n$ ou $\mathfrak{S}_n$ par cardinalité, ou bien $H \cap \mathfrak{A}_n = \{e\}$, d'où $|H| \leqslant 2$, car $H \hookrightarrow \mathfrak{S}_n \longrightarrow \mathfrak{S}_n/\mathfrak{A}_n = \{\pm 1\}$. Mais si $H = \{id, \tau\}$ avec $\tau^2 = id$, donc et bien H n'est pas distingué dans $\mathfrak{S}_n$. ■

Remarque. On **retrouve** ce résultat. En effet, $\mathfrak{A}_n$ est engendré par les 3-cycles, dont on

[1] En effet,

$$\begin{aligned} 5 &= 5 \\ &= 4+1 \\ &= 3+1+1 \\ &= 3+2 \\ &= 2+2+1 \\ &= 2+1+1+1 \\ &= 1+1+1+1+1. \end{aligned}$$

déduit que $\mathfrak{A}_n$ est son propre dérivé pour $n \geqslant 5$. Ainsi, $\mathfrak{A}_n$ est le dérivé de $\mathfrak{S}_n$ et la suite des dérivés successifs n'est pas stationnaire au neutre. Ainsi $\mathfrak{S}_n$ n'est pas résoluble.

2.12.6.1 Cas des plus petits ordres : $\mathfrak{S}_n$ pour $n = 1,2,3,4$

Définition. ***(Groupe de Klein de permutations)***

On appelle *représentation dans* $\mathfrak{S}_4$ *du groupe de Klein*, le groupe :

$$\mathcal{K} = \mathbb{V}_4 = \{id, (12)(34), (13)(24), (14)(23)\}.$$

Lemme. ***(Distinction de*** $\mathbb{V}_4$***)***

$\mathcal{K}$ est un sous-groupe distingué de $\mathfrak{S}_4$ isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$.

▷ L'ensemble $\mathcal{K}$ consistant en l'identité et les trois doubles transpositions de $\mathfrak{S}_4$, il est stable par conjugaison, car le conjugué d'une double transposition (à supports disjoints) est une double transposition. On vérifie en se salissant les mains que le produit de deux éléments de $\mathbb{V}_4 prive\{id\}$ est égal au troisième. Ceci suffit à montrer, puisque toutes sont des involutions, que c'est un sous-groupe distingué de $\mathfrak{A}_n$ isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. ■

Remarque. *(Conjugaison des 3-cycles dans* $\mathfrak{A}_4$*)* Tous les 3-cycles ne sont pas conjugués dans $\mathfrak{A}_4$! Il y a même exactement trois classes de conjugaison.

▷ Les 3-cycles sont tous conjugués dans $\mathfrak{S}_4$, si bien que le centralisateur d'un 3-cycle est le sous-groupe cyclique C_3 qu'il engendre. Il en résulte que la classe de conjugaison d'un 3-cycle dans $\mathfrak{A}_4$ est de cardinal 4. Un examen rapide des déplacements du tétraèdre régulier montre que deux 3-cycles son conjugués dans $\mathfrak{A}_4$ si et seulement si, l'arête commune est parcourue dans des sens opposés. En particulier, un 3-cycle et son inverse ne sont pas conjugués dans $\mathfrak{A}_4$.

Par exemple, la classe de (1,2,3) sont (1,2,3), (2,1,4), (3,4,1) et (432). ■

Le groupe $\mathfrak{A}_4$ n'est pas simple (il y en a d'autres...) !

Propriétés. ***(Simplicité du groupe alterné aux petits ordres)***

1. Pour $n = 1$, $\mathfrak{S}_n = \mathfrak{A}_n$ est trivial, abélien, donc résoluble. On ne parle pas de simplicité.
2. Pour $n = 2$, $\mathfrak{A}_n$ est trivial. Il est simple. Le groupe $\mathfrak{S}_n$ est résoluble, car abélien.
3. Pour $n = 3$, $\mathfrak{A}_n$ est abélien et simple, car de cardinal 3. Son dérivé est $\{e\}$, donc $\mathfrak{S}_n$ est résoluble (non abélien).

2.13 Groupes libres, présentation par générateurs et relations

2.13.1 Groupe libre

Définition-propriété. ***(Groupe libre)***

Soit S un ensemble. On appelle *groupe libre* sur S, le groupe $F(S)$, unique à isomorphisme près, universel pour la propriété suivante : pour tout groupe G, pour toutes applications $f : S \longrightarrow G$ et $g : S \longrightarrow F(S)$, il existe un unique morphisme de groupes $h : F(S) \longrightarrow G$ tel que $g \circ h = f$, soit :

$$\begin{array}{ccc} S & \xrightarrow{f} & G \\ {\scriptstyle g}\downarrow & \nearrow_{h} & \\ F(S) & & \end{array}$$

On peut donner une description simple des groupes libres.

Propriété. ***(Groupe libre sur un ensemble fini)***

Soit $S = \{x_1,...,x_n\}$ un ensemble. On note $F(S) = F_n$. Alors F_n est le quotient de l'ensemble des mots, *i.e.* des suites finies de symboles $w = x_1x_2x_2^{-1}x_1x_3...x_{n-2}$, sur l'alphabet $\{x_1,...,x_n,x_1^{-1},...,x_n^{-1}\}$, où les x_i^{-1} sont simplement des copies des x_i (et la notation inverse simplement une notation), qui forme un monoïde (associatif) pour la concaténation, d'élément neutre le *mot vide* $\emptyset := 1 := e$, par la relation : pour tous mots U,V, $Ux_ix_i^{-1}V \sim Ux_i^{-1}x_iV \sim UV$.

VOC On dit *libre*, car l'on peut choisir librement les images des éléments de la base[1] x_i, x_i^{-1}.

Exemples. ***(Groupes libres)***

1. Soit S un ensemble à 1 élément. Alors $F_S := F_1 = \mathbb{Z}$. Si G est n'importe quel groupe, $g \in G$, il existe $\rho : \mathbb{Z} \longrightarrow G$ qui à $1 \longmapsto g = \rho(1)$.

[1] En effet, on peut écrire tout élément de $F(S)$ sous la forme $a_1^{\varepsilon_1}...a_r^{\varepsilon_r}$ où $a_i = x_j$ et $\varepsilon_i = \pm 1$.

2.13.2 Présentation d'un groupe par générateurs et relations

Définition. ***(Présentation d'un groupe)***

Une *présentation d'un groupe* G est l'écriture $G = \langle S, R\rangle$ où $S \subseteq G$ est un ensemble, les *générateurs* de G, et R un ensemble d'éléments de $F(S)$ tel que $F(S)/\langle\langle R\rangle\rangle \xrightarrow{\sim} G$.

Heuristiquement, de même que le groupe libre est le groupe le plus général qui ne vérifie aucune relation du tout, le groupe donné par présentation par générateurs et R est le plus général qui vérifie R.

Exemples. ***(Groupes présentés par générateurs et relations)***

1. Posons $\mathbb{Z}_n = \langle x \mid x^n = 1\rangle$. Si $g \in G$, $g^n = 1$, alors il existe $\mathbb{Z}_n \longrightarrow G$, $x \mapsto g$, et $\mathbb{Z}_n = F_1 = \mathbb{Z}/\langle x^n\rangle$.

Remarque. On peut voir les choses ainsi :

- ⋆ Si $S \subseteq G$, alors clairement par construction $F(S) \longrightarrow G$.
- ⋆ Si $\langle S\rangle = G$, alors ce morphisme est surjectif.
- ⋆ Soit K son noyau. On sait que $F(S)/K \simeq G$.
- ⋆ On écrit $K = \langle\langle R\rangle\rangle$ le sous-groupe normal engendré, c'est-à-dire engendré par les éléments de R et de leurs conjugués.

Chapitre 3

Généralités sur les anneaux

Résumé

L'étude des anneaux trouve son origine dans l'école allemande du XIX^{e} siècle. Elle est développée par les mathématiciens Dedekind, Hilbert, Fraenkel et Noether. Elle naît de l'étude des équations algébriques, des nombres algébriques et de la recherche d'une démonstration du grand théorème de Fermat. Elle conduira à un développement important de l'algèbre générale et de la géométrie algébrique. Contrairement à la théorie élémentaire des groupes, la théorie des anneaux essaime de façon non linéaire : intervention rapide de la notion d'idéal, algèbres sur un anneau, théorie des corps, anneaux de polynômes, arithmétique dans les anneaux, théorie des modules, etc. Il est donc beaucoup moins aisé d'exposer les notions de base sur les anneaux sans tomber dans un aller-retour constant, dû à la nécessité d'une marche pédagogique homogène, entre des blocs pourtant cohérents pris séparément. Nous nous efforçons ainsi de regrouper les connaissances en les ordonnant par complexité croissante. Techniquement parlant, l'anneau est un structure qui enrichit celle du groupe en rajoutant une seconde loi qui interagit avec la première par *distributivité* : de cet axiome fondamental, on déduit une certaine rigidité de la structure, notamment grâce à la similitude à $\mathbb{Z}$ qui ne sera pas mise en défaut avant les tentatives de généralisation de l'arithmétique de cet ensemble. On demande également la commutativité de l'addition pour disposer d'un objet aussi intuitif qu'on le souhaite. Un problème sous-jacent de l'algèbre de la structure anneaux est l'impossibilité a priori de simplifier par un élément non nul. En effet, lorsque les anneaux et corps de nombres que nous connaissons permettent de régulariser un produit par les éléments différents de 0, il est possible que, dans un anneau, un produit de facteurs non nul soit nul, une propriété que nous appellerons *non-intégrité*. En cherchant à inverser les éléments non nuls d'un anneau, on parvient très vite à la notion de corps dont l'étude d'exemples pathologiques est au cœur de la recherche mathématique actuelle.

3.1 Notions générales sur les anneaux

One Ring to rule them all, One Ring to find them, One Ring to bring them all and in the darkness bind them.

J. R. R. Tolkien, *The Fellowship of the Ring*

3.1.1 Définitions élémentaires

Définition. ***(Anneau (unitaire))***

Un *anneau* ou *anneau unitaire* $(A, +, \times)$ est la donnée d'un groupe commutatif $(A, +)$ et d'une loi de composition interne $\times$ sur A associative, possédant un élément neutre et distributive à gauche et à droite sur $+$.

Reformulation pratique

La propriété de distributivité à gauche équivaut à ce que l'application :

$$\begin{aligned} (A,+) &\longrightarrow (A,+) \\ y &\longmapsto x \times y \end{aligned}$$

soit un morphisme de groupes abéliens pour tout $x \in A$. De même, la propriété de distributivité à droite équivaut à ce que l'application :

$$\begin{aligned} (A,+) &\longrightarrow (A,+) \\ x &\longmapsto x \times y \end{aligned}$$

soit un morphisme de groupes abéliens pour tout $y \in A$.

⟶ **Convention.** Dans cette définition de l'objet d'anneau, on pourra bénignement remplacer anneau par **anneau unitaire** puisque nous supposons dans les axiomes l'existence d'un élément neutre additif. Ce n'est pas le cas dans la définition annexe suivante.

Définition. ***(Pseudo-anneau)***

Un *pseudo-anneau* $(A, +, \times)$ est la donnée d'un groupe commutatif $(A, +)$ et d'une loi de composition interne $\times$ sur A associative et distributive à gauche et à droite sur $+$.

Dans la littérature, surtout venant des vieilles croûtes, on pourra trouver parfois *anneau* à la place de *pseudo-anneau*. Il faut prendre garde à cet ambiguïté de définition pour la raison suivante.

Contre-exemple. ***(Tout pseudo-anneau n'est pas un anneau)***

L'objet $(2\mathbb{Z}, +, \times)$ qui réunit les entiers relatifs pairs est un pseudo-anneau (le vérifier !) mais aucun élément n'est neutre, donc ce n'est pas un anneau. □

⟶ **Convention.** Dans toute cette partie, on procèdera au même abus que pour toute structure algébrique élémentaire (voir dans la section Magmas, Groupes...) en se permettant d'identifier, lorsque les lois sont intuitives ou simplement n'interviennent pas nommément, l'anneau $(A, +, \times)$ et l'ensemble sous-jacent A.

Exercice 69

Donner un exemple pour lequel l'abus précédent casse fortement la tête.

▷ **Éléments de réponse.**

Exhiber deux sets de lois d'anneau différentes sur un même ensemble qui génèrent des propriétés tout à fait différentes.

Propriété. ***(Absorbance du zéro d'un anneau)***

Soit $(A, +, \times)$ un anneau. Alors pour tout $x \in A$, $0_A \times A = A \times 0_A = 0_A$.

▷ On a l'identité de Toto : $0_A + 0_A = 0_A$. Multiplions par x, et, par distributivité, on obtient : $x0_A + x0_A = x0_A$. Puisque $x0_A$ est bien sûr symétrisable pour l'addition, on le retranche à droite et à gauche, de sorte que $x0_A = 0_A$. La distributivité à droite assure l'autre égalité. ■

Définition. ***(Anneau nul, anneau trivial)***

Un anneau est dit *nul* ou *trivial* dès que $A = \{0\}$.

Propriété. ***(Anneau trivial)***

Tout anneau trivial est un anneau.

Remarque. On remarque que **tous les anneaux triviaux sont isomorphes** au sens des anneaux *(voir dans la suite la définition de morphisme d'anneaux)*, ce qui permet de parler de **l'**anneau trivial (avec l'article défini) dans la suite.

Propriété. ***(Caractérisation de l'anneau trivial)***

Un anneau A est trivial si et seulement si $0_A = 1_A$.

▷ Le sens direct est immédiat. Pour la réciproque, soit $x \in A$. Alors $x1_A = x$ mais $1_A = 0_A$ donc $x1_A = x0_A = 0_A$ par absorption d'où $x = 0_A$. ■

Exemples. ***(Anneaux)***

1. Si $(M,+)$ est un groupe abélien, alors $(\mathrm{End}(M),+,\circ)$ est un anneau non commutatif. Attention ! $(\mathrm{Aut}(M),+\circ)$ n'est absolument rien du tout (mais $(\mathrm{Aut}(M),\circ)$ est un groupe) !

3.1.2 Commutativité

3.1.3 Sous-anneau

Propriété. ***(Intersection de sous-anneaux)***

Toute intersection (quelconque) de sous-anneaux d'un anneau en est un sous-anneau.

Définition-propriété. ***(Sous-anneau engendré)***

Soit A un anneau et P une partie de A. Alors il existe un plus petit sous-anneau de A contenant P.

3.1.4 Morphisme d'anneaux

Propriété. ***(Consistance de la notion de sous-anneau)***

Soit $B \subseteq A$ et $i : B \hookrightarrow A$ l'inclusion canonique. Il existe une unique structure d'anneaux sur B telle que i soit un morphisme.

▷ C'est quasi tautologique. Il est clair que si l'on munit B des lois induites, l'injection canonique est un morphisme. De même, si l'injection canonique est un morphisme, alors on voit que $a \times_B b = i(a) \times_A i(b) = a \times_A b$ pour tous a,$b \in B$, donc $\times_B = \times_A$; de même, $+_B = +_B$ et $1_A = 1_B$, ce qui caractérise les sous-anneaux, donc B est muni des lois induites. ■

3.1.5 Inversibles d'un anneau

Définition. ***(Inversible, unité)***

On appelle *inversible* ou *unité* d'un anneau $(A,+,\times)$ tout élément qui soit symétrisable pour la loi $\times$.

L'exercice suivant explique l'appellation moins répandue d'*unité* pour désigner les symétrisables multiplicatifs.

Exercice 70

Quels sont les inversibles de $\mathbb{Z}$?

▷ **Éléments de réponse.**

Il faut écrire la définition calculatoire d'inversibilité.

Calmons-nous quand même.

Exercice 71

Trouver un anneau muni d'une norme, tel qu'un élément unitaire ne soit pas inversible.

Définition. ***(Ensemble des inversibles, ensemble des unités)***

On note A^* ou $A^\times$ l'ensemble des *inversibles* ou *unités* de A.

On peut se poser la question suivante :

Exercice 72

Soit un anneau A ayant exactement deux éléments inversibles : 1 et -1, en supposant que $1 \neq -1$. A-t-on forcément une bijection de A sur $\mathbb{Z}$ (ce qui serait un premier pas pour dire que A et $\mathbb{Z}$ se comportent de la même manière) ?

▷ **Éléments de réponse.**

On répond par la négative. On considère A l'ensemble des restes d'entiers par la division modulo 3. On montre que c'est un anneau qui satisfait à l'hypothèse demandée, mais il n'a que trois éléments. Ce ne peut donc pas être $\mathbb{Z}$ à isomorphisme près.

Proposition. ***(Image d'un inversible par un morphisme)***

Soient A,B deux anneaux et $f : A \longrightarrow B$ un **morphisme d'anneaux**. Alors $f(A^*) \subseteq B^*$.

3.1.5.1 Inverses latéraux dans un anneau

Proposition. ***(Inverse latéral dans un anneau)***

Soient A un anneau et $x \in A$. On suppose que $yx = 1_A$.

1. Si A est commutatif, y est inverse de x.
2. Si A est un corps, même conclusion.
3. Si $A = \mathrm{End}(E)$ où E est un espace-vectoriel de dimension finie, même conclusion.
4. En général, on ne peut pas conclure.

▷ Si A est commutatif, $yx = xy$. Si A est un corps, il suffit d'appliquer le résultat sur les groupes à $\mathbb{K}^*$ après avoir exclu le cas nul. Si $A = \mathrm{End}(E)$, le résultat sera prouvé dans le cours sur les matrices à coefficient dans un corps. Donnons un contre-exemple dans le cas général. On considère les endomorphismes de dérivation et d'intégration à partir de zéro dans $\mathcal{C}^\infty(\mathbb{R})$. ■

3.1.6 Intégrité, division du zéro

Définition. ***(Diviseur de zéro)***

Soit A un anneau. Un élément $a \in A$ est dit *diviseur de zéro* s'il existe un élément $b \in A$ **non nul** tel que $ab = 0_A$.
On note $\mathrm{Div}_0(A)$ l'ensemble des diviseurs de zéro de A.

Ne pas confondre avec la divisibilité, qui présente une incohérence de langage dans le cas des éléments nuls. Ainsi :

- Tout entier divise zéro, mais seul l'entier nul est un diviseur de zéro.

Remarque. D'après la définition, dans l'anneau nul, il n'y a aucun diviseur de zéro, car il n'y a aucun élément non nul !

Propriété. ***(Division de zéro par zéro)***

Dans un anneau non nul, 0 est un diviseur de 0.

Propriété. ***(Diviseurs de zéro et nilpotents)***

Si A est non nul, $\mathrm{Div}_0(A) \supseteq \mathrm{Nil}(A)$.

Propriété. ***(Diviseurs de zéro et inversibles)***

Si A est non nul, $\mathrm{Div}_0(A) cap A^* = \emptyset$.

Propriété. ***(Diviseurs de zéro d'un corps)***

Soit K un corps. Alors $\mathrm{Div}_0(K) = \emptyset$.

Remarque. On retrouve qu'alors $\mathrm{Nil}(K) = \emptyset$.

Définition. ***(Intégrité)***

Un anneau A est dit *intègre* s'il est commutatif, non trivial et sans diviseur de zéro autre que zéro lui-même. Autrement dit, A est commutatif, non nul et pour tous a,$b \in A$,

$$ab = 0 \text{ si et seulement si } a = 0 \text{ ou } b = 0.$$

Propriété. ***(Sous-anneau d'un anneau intègre)***

Tout sous-anneau non nul d'un anneau intègre est intègre.

3.1.7 Corps

Proposition. ***(Caractérisation pratique des morphismes de corps)***

Dans un corps, l'axiome des morphismes d'anneaux $\varphi(1) = 1$ est automatiquement vérifié dès que φ est non nul.

▷ On a $\varphi(1^2) = \varphi(1) = \varphi(1)^2$ d'où $\varphi(1)(1 - \varphi(1)) = 0$. Ainsi soit $\varphi(1) = 0$, soit $\varphi(1) = 1$. Or si $\varphi(1) = 0$, pour tout x, $\varphi(x) = \varphi(1 \times x) = \varphi(1)\varphi(x) = 0$ par absorption, donc φ est identiquement nul, ce qui est exclu. ■

Remarque. En fait, c'est vrai dès que l'on est dans un anneau intègre.

Proposition. ***(Image d'un corps par un morphisme)***

L'image d'un corps par un morphisme d'anneaux est un corps.

Remarque. La phrase : *l'image d'un corps par un morphisme de corps est un corps*, est curieuse. On ne suppose pas dans l'énoncé que l'arrivée est elle-même un corps.

▷ L'image d'un anneau par un morphisme d'anneaux est un anneau. Soit $f : K \longrightarrow A$ un morphisme d'anneaux, K un corps. Soit $x \in f(K)$ non nul. Alors $x = f(t)$ où $t \in K$ est non nul, autrement $x = f(0) = 0$. Ainsi t admet un inverse t'. Puisque $f(t') = f(t)^{-1}$, x est inversible d'inverse $f(t')$. ■

3.1.8 Algèbre sur un corps

3.1.9 Algèbre sur un anneau

	Structure de base	**Module**	**Algèbre**
Sur un anneau	Anneau A Lois additive et multiplicative, distributivité	A-module M Loi de groupe et loi externe sous l'action de A	A-algèbre sur un anneau Anneau et module Compatibilité des lois multiplicative et externe
Sur un corps	Corps (donc anneau) K Anneau et inversibilité	K-ev E Même chose	K-algèbre sur un corps Même chose

FIGURE 3.1.1 : *Comparaison des différentes structures relatives à la notion d'anneau.* —

Exemples. ***(Algèbres sur un anneau)***

1. Pour tout anneau A, A est une A-algèbre.
2. Si A est un sous-anneau de B, B est une A-algèbre pour l'injection canonique, dans ce cas injective.
3. Les quotients de A sont des A-algèbres.
4. $A = \mathbb{K}$ un corps, $B = \mathbb{K}[X]$.
5. A un anneau, $B = A[X]$ pour $\eta : a \longrightarrow a \cdot X^0$.
6. $\mathfrak{M}_n(A)$ est une A-algèbre, par $\eta : a \longrightarrow aI_n$. Remarquer que $\eta(A) = Z(\mathfrak{M}_n(A))$.

3.1.9.1 Définition ouverte de la notion d'algèbre (Lang, Bourbaki)

Définition. ***(Algèbre sur un anneau)***

Soit A un anneau. Soit B un autre anneau. On dit que B est une A-algèbre s'il existe un morphisme $\eta : A \longrightarrow B$ tel que $\forall x \in A \ \forall y \in B \quad \eta(x)y = y\eta(x)$.

Le morphisme η, dit *morphisme de définition de l'algèbre* ou *homomorphisme de définition*, qui est canonique, n'est pas forcément injectif ! Par exemple : $\mathbb{Z}/2\mathbb{Z}$ est une $\mathbb{Z}$-algèbre.

Remarque. Si A est un corps, le morphisme de définition de l'algèbre (et donc de l'espace vectoriel) est nécessairement injectif, car tout morphisme partant d'un corps est injectif.

Cette idée centrale en théorie des modules donne que le phénomène de torsion n'existe pas dans les espaces vectoriels, ne qui leur permet d'avoir une base. Dans les anneaux, le défaut de régularité empêche de démontrer le théorème d'échange !

Théorème. ***(Les $\mathbb{Z}$-algèbres sont les anneaux)***

La catégorie des $\mathbb{Z}$-algèbres est équivalente à la catégorie des anneaux.

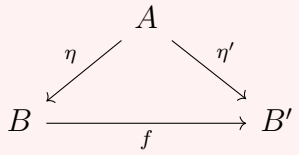
▷ On sait qu'il existe un unique homomorphisme de $\mathbb{Z}$ dans un anneau donné A. On a bien alors $\eta(k)x = x\eta(k)$, d'où le résultat. ■

Remarque. Remarquer le parallèle entre cette équivalence et celle liant les $\mathbb{Z}$-modules avec les groupes abéliens.

3.1.9.2 Morphisme d'algèbres

Définition. ***(Morphisme d'algèbre)***

Soit A un anneau. Soient B,B' deux A-algèbres et $f : B \longrightarrow B'$ un morphisme d'anneaux. Alors f est dit *morphisme de A-algèbres* si le diagramme



commute, autrement dit, si $f \circ \eta = \eta'$.

3.1.9.3 Génération d'une algèbre

La notion de génération d'une algèbre se formalise légèrement différemment que sur les structures habituelles. Voyons plutôt.

Définition. ***(Génération d'une algèbre)***

Soit X une partie de B. On dit que X *engendre* B comme A-algèbre, si le sous-anneau de B engendré par $\eta(A) \cup X$ est B lui-même.

3.1.10 Produit d'anneaux

Définition. ***(Produit d'anneaux)***

Soit $(A_i)_{i\in I}$ une famille d'anneaux. On note $\prod_{i\in I} A_i$ l'ensemble des suites indexées par I à valeurs dans $\bigcup_{i\in I} A_i$ tel que la i-ième soit dans A_i.

Proposition. ***(Propriété universelle du produit d'anneaux)***

Soit $(A_i)_{i\in I}$ une famille d'anneaux et pour tout $j \in I$, $p_j : \prod_{i\in I} A_i \twoheadrightarrow A_j$ un morphisme d'anneaux. Alors pour tout anneau B, pour toute famille $f_i : B \longrightarrow A_i$, il existe un unique morphisme d'anneaux $f : B \longrightarrow \prod_i A_i$ tel que $p_j \circ f = f_j$ pour tout j.

Exemple

Soit E un espace vectoriel et F un sous-espace vectoriel de E. Il existe bien sûr une injection canonique $F \hookrightarrow E$. Ainsi, il existe une surjection $E \twoheadrightarrow F$: on le sait, c'est la projection sur F parallèlement à un supplémentaire.

Définition. ***(Exponentiation d'anneau)***

Soit $(A_i)_{i\in I}$ une famille d'anneaux telle que pour tout $i \in I$, $A_i = A$ un anneau ! Alors on note $A^I = \prod_{i=1} A_i$ muni des lois précédemment définies. C'est l'ensemble des *suites indexées par I à valeurs dans A.*

Définition. ***(Coproduit d'anneaux)***

Soit $(A_i)_{i\in I}$ une famille d'anneaux. On appelle *co-produit* de $\prod_{i\in I} A_i$ le sous-ensemble des éléments à support fini.

Ce n'est pas un anneau !

Définition. ***(Suites presque nulles d'un anneau)***

Soit $(A_i)_{i\in I}$ une famille d'anneaux telle que pour tout $i \in I$, $A_i = A$ un anneau ! Alors on note $A^{(I)}$ le co-produit de A^I, c'est-à-dire le sous-ensemble des éléments dont les composantes sont presque toutes nulles au sens ensembliste.

On ne suppose pas I au plus dénombrable.

Théorème

Si I est fini, $A^{(I)} = A^I$.

Ensemblistement, $\mathbb{R}[X] = \mathbb{R}^{(\mathbb{N})}$, mais ça ne va pas plus lois : les lois ne sont manifestement pas les mêmes, car les lois induites sur le co-produit sont terme à terme, mais certainement pas dans un espace de polynômes.

Proposition. ***(Structure du co-produit dans le produit)***

Soit $(A_i)_{i\in I}$ une famille d'anneaux. Alors le co-produit de $\prod_{i\in I} A_i$ est un idéal bilatère de $\prod_{i\in I} A_i$.

Heuristique

En dimension infinie non dénombrable, l'algèbre tient encore dans la structure de produit mais il ne se passe rien d'intéressant : en particulier, il faut l'axiome du choix pour construire (au sens non constructif...) une base. Donc, on munit l'espace d'une norme, on parle de topologie et de convergence, et pour cela, on renvoie au cours d'analyse fonctionnelle.

3.1.11 Idéal d'un anneau

3.1.11.1 Notion d'idéal

Définition. ***(Idéal à gauche)***

Soit A un anneau et I une partie de A. On dit que I est un *idéal à gauche* de A si $(I,+)$ est un sous-groupe de $(A,+)$ et Definition tous $a \in A$, $x \in I$, on a $ax \in I$.

Astuce !

Pour retenir le sens : un idéal à gauche agit *à gauche* sur l'anneau :

$$\forall x \in I \ \forall y \in A \quad y \cdot x \in I.$$

Définition. ***(Idéal à droite)***

Soit A un anneau et I une partie de A. On dit que I est un *idéal à droite* de A si $(I,+)$ est un sous-groupe de $(A,+)$ et pour tous $a \in A$, $x \in I$, on a $xa \in I$.

Définition. ***(Idéal bilatère)***

Soit A un anneau et I une partie de A. On dit que I est un *idéal bilatère* de A si I est un idéal à droite et un idéal à gauche.

VOC Certains auteurs parlent plutôt d'*absorbeur*. Ce terme rare a l'avantage de parler visuellement.

Proposition. ***(Idéal dans un anneau commutatif)***

Dans un anneau commutatif, les notions d'idéal à droite, d'idéal à gauche et d'idéal bilatère sont confondues.

Remarque. Ceci démarre un parallèle très important entre sous-groupe distingué et idéal bilatère, qui trouvera son point culminant dans la théorie des quotients d'anneaux.

Contre-exemple. ***(Idéaux non bilatères)***

Si $n \geqslant 2$, $\mathfrak{M}_n(\mathbb{R})$ n'a pas d'autre idéal bilatère que les deux idéaux triviaux. En revanche, il possède des idéaux à gauche et à droite non triviaux.
Pour tout F sev de E $\mathbb{R}$-espace de dimension n, l'ensemble des endomorphismes de noyau contenant F est un idéal à gauche de $\mathrm{End}(E) \simeq \mathfrak{M}_n(\mathbb{R})$.
Pour tout F sev de E $\mathbb{R}$-espace de dimension n, l'ensemble des endomorphismes d'image contenue dans F est un idéal à droite de $\mathrm{End}(E) \simeq \mathfrak{M}_n(\mathbb{R})$. □

3.1.11.2 Idéaux triviaux

Définition. ***(Idéaux triviaux)***

Soit A un anneau. On appelle :

- *idéal trivial*, tout idéal égal à $\{0\}$ ou A ;
- *idéal nul*, l'idéal $\{0\}$;
- *idéal grossier*, l'idéal A ;
- *idéal propre*, tout idéal qui n'est pas A.

Propriétés. ***(Caractérisation de l'idéal grossier)***

Soit A un anneau et I un idéal de A. Les propriétés suivantes sont équivalentes :

(i) $I = A$;
(ii) $1 \in I$;
(iii) $I \cap A^\times \neq \emptyset$.

▷ La preuve est laissé en bon exercice. ■

3.1.11.3 Opérations sur les idéaux

3.1.11.3.1 Intersection d'idéaux

Propriété. ***(Intersection d'idéaux)***

Toute intersection d'idéaux à gauche (resp. à droite, bilatères) est un idéal à gauche (resp. à droite, bilatère). C'est le plus grand idéal contenu dans tous ceux-là.

VOC Une *somme quelconque d'idéaux* est par définition l'idéal engendré par ses termes, c'est-à-dire l'ensemble des combinaisons linéaires, ou sommes finies, d'éléments de la partie.

3.1.11.3.2 Somme finie d'idéaux

Propriété. ***(Somme d'idéaux)***

Toute somme finie d'idéaux à gauche (resp. à droite, bilatères) est un idéal à gauche (resp. à droite, bilatère). C'est le plus petit idéal contenant tous ceux-là.

3.1.11.3.3 Produit d'idéaux

Définition. ***(Produit de deux idéaux)***

Soient I,J deux idéaux d'un anneau A. On note IJ l'idéal engendré par $I \times J$, c'est-à-dire, l'ensemble des sommes finies de produits d'un élément de I par un élément de J.

Propriété. ***(Cardinal du produit)***

Soient I,J deux idéaux d'un anneau A. Alors $IJ \subseteq I$.

Corollaire

Soit I un idéal de A. Alors $(I^n)_{n\in\mathbb{N}}$ est une suite décroissante d'idéaux de A.

Propriété. ***((Associativité du produit d'idéaux)***

Le produit des idéaux est associatif.

$IJ \subseteq I \cap J$ mais il n'y a pas égalité en général ! (Prendre deux entiers non étrangers dans $\mathbb{Z}$.

3.1.11.3.4 Image et image réciproque d'idéaux

Propriété. ***(Image réciproque d'un idéal par un morphisme)***

Soient A,B deux anneaux. Soit $f : A \longrightarrow B$ un **morphisme d'anneaux**. Soit J un idéal de B. Alors $f^{-1}(J)$ est un idéal de A.

▷ Facile. ■

Proposition. ***(Propriété de l'image d'un idéal par un morphisme)***

Soient A,B deux anneaux. Soit $f : A \longrightarrow B$ un morphisme d'anneaux. Alors f est surjectif si et seulement si pour tout idéal I de A, $f(I)$ est un idéal de B.

▷ Facile. ■

Corollaire. ***(Image d'un idéal par un morphisme surjectif)***

Soient A,B deux anneaux. Soit $f : A \longrightarrow B$ un morphisme d'anneaux **surjectif**. Soit I un idéal de A. Alors $f(I)$ est un idéal de B.

Corollaire. ***(Image d'un idéal par un morphisme)***

Soient A,B deux anneaux. Soit $f : A \longrightarrow B$ un morphisme d'anneaux. Soit I un idéal de A. Alors $f(I)$ est un idéal de $f(A)$.

Remarque. Encore une fois, on observe le parallèle avec la notion de sous-groupe distingué.

3.1.11.3.5 Anneau produit et idéaux

Propriété. ***(Quotient d'un produit par un idéal)***

Soient A,B deux anneaux et I,J deux idéaux bilatères respectivement de A et de B, ce qui revient à la donnée d'un idéal de $A \times B$. Alors :

$$(A \times B)/(I \times J) \simeq A/I \times B/J.$$

▷ Application directe du premier théorème d'isomorphisme. ■

3.1.11.4 Notion de principalité

Soit A un anneau.

Définition-propriété. ***(Idéal principal à droite engendré par un élément)***

Soit $a \in A$. Alors aA est un idéal à droite de A, appelé *idéal principal à droite de A engendré par a*. On dit aussi que a est UN *générateur* de aA. On note $aA = (a)_d$.

Définition-propriété. ***(Idéal principal à gauche engendré par un élément)***

Soit $a \in A$. Alors Aa est un idéal à gauche de A, appelé *idéal principal à gauche de A engendré par a*. On dit aussi que a est UN *générateur* de Aa. On note $Aa = (a)_g$.

Définition-propriété. ***(Idéal principal bilatère engendré par un élément)***

Soit $a \in A$. Alors AaA est un idéal bilatère de A, appelé *idéal principal bilatère de A engendré par a*. On dit aussi que a est UN *générateur* de AaA. On note $AaA = (a)$.

Définition-propriété. ***(Idéal principal engendré par un élément)***

Soit $a \in A$. Si A est commutatif, alors $aA = Aa = AaA$ est un idéal de A, appelé *idéal principal de A engendré par a*. On dit aussi que a est UN *générateur* de aA. On note $aA = (a)$.

▷ Simple vérification. ■

Voilà maintenant un chapelet de lemmes élémentaires, mais fort utiles.

Propriété. ***(Caractérisation de l'idéal grossier parmi les idéaux principaux)***

Soit A un anneau et a un élément de A. Les propriétés suivantes sont équivalentes :

(i) $(a) = A$;
(ii) $a \in A^\times$;
(iii) $1 \in (a)$;
(iv) $(a) \cap A^\times \neq \emptyset$.

▷ Montrons *(i)* implique *(ii)*. Puisque $1 \in A$, $1 \in (a)$. Il existe donc b,b' tels que $ab = 1$ et $b'a = 1$. Ainsi a est inversible. Si maintenant a est inversible, alors il existe b tel que $ba = 1$, donc $1 \in (a)$. Si maintenant $1 \in (a)$, puisque $1 \in A^\times$, un anneau étant toujours unitaire, on a *(iv)*. Enfin, si l'on suppose qu'il existe $x \in A^\times$ dans (a), soit b un inverse de x. Alors $bx = 1 \in (a)$ puisque (a) est un idéal à gauche. Soit $c \in A$ quelconque. Alors $c = c1 = c(bx) = (cb)x \in (a)$ de même, donc $A \subseteq (a)$. L'autre inclusion étant claire, on a *(i)*, ce qui termine la chaîne d'implications et toutes les propriétés sont équivalentes. ■

Exercice 73

Quels sont les idéaux d'un corps ?

▷ **Éléments de réponse.**

Montrer qu'un idéal non nul contient nécessairement 1.

On énonce dans cette partie la propriété suivante, qui caractérise les corps par leurs idéaux (les plus concentrés remarqueront que c'est une réciproque à la propriété énoncée sur les idéaux d'un corps). Ce fait, quoique élémentaire, sera d'une grande utilité dans certains raisonnements qui suivront.

Corollaire

Soit A un anneau. Alors A est un corps (non nécessairement commutatif) si et seulement s'il possède exactement deux idéaux à gauche, à savoir $\{0_A\}$ et A.

▷ Soit A un corps, non nécessairement commutatif. $0_A \neq I_A$, car un corps, par axiome, n'est jamais trivial, donc $\{0_A\}$ et A sont deux idéaux à gauche de A distincts. Soit I un idéal à gauche de A.

S'il est non nul, il contient un élément non nul, donc inversible puisque A est un corps, et donc égal à A par le lemme précédent. Réciproquement, supposons que $\{0_A\}$ et A soient les deux seuls idéaux à gauche de A. Puisqu'ils sont distincts, $0_A \neq 1_A$ donc A n'est pas trivial. Soit $a \in A \setminus \{0_A\}$. Alors $(a)_g$ est un idéal à gauche de A non nul, car il contient a, car A est unitaire, et comme $1_A \in A$, il existe $b \in A$ tel que $ba = 1_A$. Remarquons que b est non nul, car 0_A est absorbant et l'on aurait encore $0_A = 1_A$. Par le même raisonnement, il existe $c \in A$ tel que $cb = 1_A$. On a lors $a = 1_A a = (cb)a = c(ba) = c1_A = c$, donc $ab = 1_A$ par substitution. Ainsi a est inversible. Donc, A est un corps. ■

Exercice 74

Soit un anneau non commutatif ayant exactement deux idéaux bilatères. Est-ce un corps gauche ?

▷ **Éléments de réponse.**

Non. On appelle ce type d'anneau un *anneau simple*. Leur étude sera un sujet plus loin dans notre article.

On en déduit la propriété suivante, qui se révèle très utile dans le travail sur les idéaux maximaux. On anticipe sur la notion d'idéal maximal : c'est tout simplement un idéal qui soit un élément maximal pour l'inclusion dans l'ensemble des idéaux propres de l'anneau.

Corollaire

Tout non-inversible d'un anneau est inclus dans un idéal maximal propre. Réciproquement, tout élément d'un anneau inclus dans un idéal maximal propre est non-inversible.

▷ Soit $a \in A$ non inversible, A un anneau. Alors (a) est un idéal propre, car il ne contient pas 1, autrement a serait inversible. D'après le lemme de Zorn, il est donc inclus dans un idéal maximal propre, car l'ensemble des idéaux maximaux propres de A est inductif. Réciproquement, si $x \in I$ idéal maximal propre, si x est inversible, $I = A$, absurde. Ainsi x est non inversible. ■

Reformulation pratique

Un élément d'un anneau est non inversible, si et seulement si, il est inclus dans un idéal maximal.

Voilà, en guise de récréation, une propriété dont la démonstration a été requise lors des oraux de l'École normale supérieure.

Propriété

Soient a,b dans un anneau commutatif A. Si l'idéal $(a) + (b)$ est principal, il en est de même de l'idéal $(a) \cap (b)$.

▷ On utilise l'intuition donnée par $\mathbb{Z}$ pour nous guider. Soit d un générateur de $(a) + (b)$ (ce qui correspond au pgcd), on pose $a = d\alpha$, $b = d\beta$ et enfin $m = d\alpha\beta$ (ce qui correspond au

ppcm). Montrons par double inclusion que $(a) \cap (b) = (m)$. Soit $x \in (m)$. Il existe $\lambda \in A$ tel que $x = \lambda m = \lambda d\alpha\beta = \lambda a\beta = \lambda\beta a$ et d'autre part $x = \lambda m = \lambda d\alpha\beta = \lambda\alpha d\beta = \lambda\alpha b$, de sorte que $x \in (a) \cap (b)$. Réciproquement, soit $x \in (a) \cap (b)$. On écrit $x = ua = vb$. On sait par ailleurs qu'il existe $\lambda, \mu \in A$ tels que $d = \lambda a + \mu b$. On a alors :

$$x = ua = u\alpha d = u\alpha(\lambda a + \mu b) = \alpha\lambda x + u\mu m = \alpha\lambda vb + u\mu m = m(\lambda\nu + \mu u),$$

d'où la seconde inclusion. ■

3.1.11.5 Anneaux quotients ; quotient d'un anneau par un idéal

On rappelle quelque chose de dit plus haut dans notre composition.

Propriété. ***(Anneau quotient)***

Si $(\mathbb{A}, +, \times)$ est un groupe, $\mathcal{R}$ une relation d'équivalence sur $\mathbb{A}$ compatible avec $+$ et avec $\times$, alors $\mathbb{A}/\mathcal{R}$ muni des deux lois quotients est un anneau d'éléments neutres $\overline{0}$ et $\overline{1}$.

Avant de préparer la suite, on conseille de revoir les choses suivantes du cours de mathématiques : définition d'un idéal, ce que l'on dit d'un idéal contenant 1 ou un inversible, noyaux de morphismes d'anneaux, condition nécessaire et suffisante pour qu'un anneau soit un corps avec les idéaux, idéaux classiques, intersection et somme d'idéaux.

Exercice 75

Pourquoi les corps quotients ne vont-ils pas nous intéresser ?

Nous remarquons qu'un anneau, un sous-anneau et un idéal étant en particulier des sous-groupes additifs, les quotients intéressants vont devoir, comme on l'a montré précédemment, vérifier au moins les propriétés analogues à celles des sous-groupes distingués (ce doivent être donc des congruences modulo un sous-groupe). Nous voyons qu'il faut et qu'il suffit que ce soient des congruences modulo un idéal bilatère.

Soit $(\mathbb{A}, +, \times)$ un anneau unitaire, non nécessairement commutatif. On aurait pu considérer seulement les pseudo-anneaux. On rappelle qu'un idéal est dit *bilatère*, s'il est idéal à gauche et idéal à droite.

Propriété. ***(Congruences compatibles avec la structure d'anneau)***

Si I est un idéal bilatère de $\mathbb{A}$, alors la congruence modulo le sous-groupe I est compatible avec les lois de $\mathbb{A}$, et réciproquement, toute relation d'équivalence compatible avec les deux lois de $\mathbb{A}$ est la congruence modulo un idéal bilatère (à savoir la classe de 0).

▷ Soit $\sim$ la congruence modulo l'idéal bilatère I, définie par $a \sim b \iff a - b \in I$. Comme le groupe additif d'un anneau est commutatif par axiome, I est un sous-groupe distingué du groupe additif de $\mathbb{A}$. Il ne reste qu'à montrer la compatibilité multiplicative. Elle provient tout simplement

de la définition de stabilité globale de l'idéal : si $a \sim b$ et c est quelconque, alors $c(a-b) \in I$, donc $ca - cb \in I$, donc $ca \sim cb$. La loi est compatible à gauche. On montre de même la compatibilité à la droite, d'où la compatibilité avec la multiplication. Réciproquement, si $\sim$ est une relation d'équivalence compatible avec l'addition et la multiplication, alors on sait déjà, d'après la partie sur les groupes, que $\overline{0} = I$ est un sous-groupe de $\mathbb{A}$ et que $\sim$ est la congruence modulo I. Il reste seulement à montrer que I est un idéal bilatère. Cela vient tout simplement du caractère absorbant (à gauche et à droite, car il y a distributivité à gauche et à droite) de 0. Cela termine la preuve. ■

⟶ **Convention.** Dans le contexte des anneaux quotients par des idéaux, on parle de *réduction modulo I de a*, pour parler de la classe de a modulo I. On dit aussi que a est *pris modulo I*.

Remarque. À l'instar des groupes, on pouvait montrer un résultat plus précis (se référer à la preuve) : une relation est compatible à gauche avec la loi multiplicative si et seulement si c'est celle associée à un idéal à gauche, puisque la loi additive n'a aucun intérêt, on l'a vu, pour les quotients d'anneaux.

Le lecteur aura soin de revoir la partie sur les quotients de magma pour se convaincre que les idéaux bilatère, à l'instar des sous-groupes distingués, sont le cadre le plus général pour quotienter des anneaux. Remarquons qu'alors, l'anneau quotient est bien un anneau (ouf !) et que la projection canonique, que l'on appellera donc quelquefois *réduction*, est un morphisme d'anneaux. (Pour vérifier cela, il suffit de considérer le magma $(\mathbb{A}, \times)$.)

Propriété. ***(Anneau commutatif quotient)***

Soient A un anneau et I un idéal bilatère de A. Si A est commutatif, alors A/I est commutatif.

▷ C'est déjà vu avec les magmas. ■

Exercice 76

Si A est principal, décrire tous ses quotients.

Exemple fondamental. ***(Anneaux modulaires)***

Pour $A = \mathbb{Z}$, les idéaux $n\mathbb{Z}$ sont bilatères, car l'anneau A est commutatif. Ainsi les anneaux modulaires... sont bien des anneaux (commutatifs).

Voilà le schéma général pour les quotients d'anneaux (par des idéaux).

$$\begin{array}{ccc} I & \xhookrightarrow{\iota} & A \\ & & \downarrow{\scriptstyle \pi} \\ & & A/I \end{array}$$

Exercice 77

1. *Symétrisation de monoïde* Expliquer comment on construit un groupe à partir d'un monoïde M grâce à la relation d'équivalence sur $M \times M$: $(a,b) \sim (a',b') \iff \exists k \quad a+b'+k = a'+b+k$. Que représente (a,b) ?
2. *Corps des fractions* Expliquer comment on construit un corps à partir d'un anneau intègre A grâce à la relation d'équivalence sur $A \times A$: $(a,b) \sim (a',b') \iff ab' = a'b$. Que représente (a,b) ?

Maintenant, on peut énoncer les théorèmes de factorisation et d'isomorphisme pour les anneaux. Ils sont très semblables à ceux pour les groupes ; pour la plupart, ce n'en est que reformulation et vérification que les propriétés multiplicatives sont encore vérifiées, ce qui est le cas systématiquement, sachant que maintenant, le cadre général a été réduit aux idéaux, et non plus seulement aux sous-groupes distingués (les idéaux sont bien sûr des sous-groupes distingués additifs par commutativité).

Théorème. ***(Théorème de factorisation pour les anneaux)***

Soit f un morphisme d'anneaux de A dans A'. I est dans $\mathrm{Ker}(f)$ si et seulement s'il existe un unique morphisme $\tilde{f}$ tel que $f = \tilde{f} \circ \pi$ (se qui se réécrit $f(x) = \tilde{f}(\overline{x})$ pour tout $x \in A$).

▷ C'est une adaptation du théorème de factorisation pour les groupes. Il ne reste qu'à vérifier que $\tilde{f}$ est un morphisme pour la multiplication, et que l'image de $\overline{1_A}$ est $1_{A'}$. ■

Méthode. ***(Recette pour passer au quotient dans les morphismes d'anneaux)***

1. Je vérifie que je dispose de deux anneaux A, A', d'un morphisme f entre les deux, et d'une partie I de A.
2. **Je vérifie que I est un idéal bilatère de A.** J'en déduis cette affirmation, que le quotient existe dans toute sa splendeur d'ensemble quotient univoquement défini par une relation de congruence et a la structure d'anneau.
3. **Je vérifie maintenant que I est inclus dans** $\mathrm{Ker}(f)$**.** Si je veux, pour crâner, je précise que c'est une condition nécessaire et suffisante à la compatibilité de f avec la congruence, car je connais même la preuve de mon théorème de factorisation sur les groupes.
4. Je peux maintenant définir un morphisme $= \tilde{f} : A/I \longrightarrow A'$ sans trouble, telle que pour tout $\overline{x} \in A/I$, $\tilde{f}(\overline{x}) = f(x)$, et j'insiste bien sur ce que cette construction n'est possible que grâce aux deux hypothèses vérifiées précédemment.

Si je veux une propriété d'injectivité, de surjectivité, voire de bijectivité pour mon application, je me réfère aux résultats de l'exercice précédent.

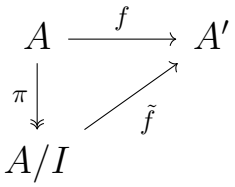
De la même façon que dans la section sur les groupes quotients, il est tout à fait inutile d'énoncer un théorème de factorisation carré (il aurait exactement le même énoncé que le théorème de factorisation simple !). Toutefois, on dispose d'un corollaire intéressant.

Exercice 78

Dans le théorème précédent, montrer que :

1. $\tilde{f}$ est injective si et seulement si $I = \mathrm{Ker}(f)$;
2. $\tilde{f}$ est surjective si et seulement si f est surjective ;
3. $\tilde{f}$ est un isomorphisme si et seulement si f est surjective et $I = \mathrm{Ker}(f)$.

Une illustration du théorème de factorisation. Le lecteur ayant l'habitude, on ne précise plus les lois des anneaux.



On note l'existence de deux corollaires d'un grand intérêt formel dont on ne regrette que l'apparition dans cette section un peu marginale.

Corollaire

Soit f un morphisme d'anneaux de A dans B et J un idéal de B. Alors $f^{-1}(J)$ est un idéal de A et l'on a un morphisme injectif $A/f^{-1}(J) \longrightarrow B/J$.

▷ On compose le morphisme $A \longrightarrow B \longrightarrow B/J$ en $\pi \circ f$, morphisme d'anneaux. Son noyau est $f^{-1}(J)$, c'est donc un idéal. Le reste est corollaire du théorème et de l'exercice précédents. ■

Corollaire

Si $A \subseteq B$, J un idéal de B, alors $A \cap J$ est une idéal de A et l'on a un morphisme injectif : $A/(A \cap J) \longrightarrow B/J$.

▷ C'est un cas particulier du corollaire précédent. ■

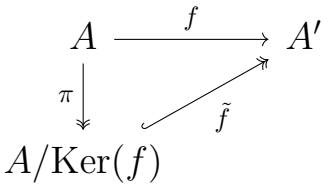
Maintenant, nous énonçons les théorèmes d'isomorphisme pour les anneaux, tout à fait semblables à leurs cousins pour les groupes.

Théorème. ***(Premier théorème d'isomorphisme pour les anneaux)***

On considère l'anneau A. Soit A' un autre anneau, et $f : A \longmapsto A'$ un morphisme d'anneaux. Alors les anneaux $A/\mathrm{Ker}(f)$ et $\mathrm{Im}(f)$ sont isomorphes par le morphisme $\tilde{f}$.

▷ On invoque le théorème d'isomorphisme pour les groupes ; il ne reste qu'à vérifier que $\tilde{f}$ est bien un morphisme pour la multiplication, ce qui est facile. ■

Nous pouvons, encore une fois, l'illustrer par un diagramme :



Le théorème de correspondance est prolongé dans les anneaux de façon immédiate.

Théorème. ***(Théorème de correspondance pour les anneaux)***

Soit I un idéal bilatère de A. Alors $J \longmapsto J/I$ définit une bijection de l'ensemble des idéaux de A contenant I sur l'ensemble des sous-groupes de A/I ; c'est un isomorphisme d'ensembles ordonnés.

▷ Il n'y a rien à faire. ■

Il est complété par les faits suivants qui l'adaptent à la structure d'idéal et d'anneau.

Propositions

Soient A,B deux anneaux commutatifs. Soit $f : A \longrightarrow B$ un morphisme. Soient I et J respectivement un idéal de A et un idéal de B. Alors si f est surjectif, alors f^{-1} induit une bijection des idéaux de B sur les idéaux de A contenant $\mathrm{Ker}(f)$; ainsi, l'ensemble des idéaux de A/I est en bijection avec l'ensemble des idéaux de A contenant I.

On peut encore énoncer les autres théorèmes d'isomorphismes. Il suffit alors de vérifier que les constructions correspondantes pour les sous-groupes distingués sont bien compatibles avec la multiplication, ce qui est facile, et laissé au lecteur déterminé.

Théorème. ***(Deuxième théorème d'isomorphisme pour les anneaux)***

Si J est un idéal de A contenant I, I est un idéal de J, J/I est un idéal de A/I, alors $\frac{A/I}{J/I} \simeq \frac{A}{J}$.

▷ On doit seulement dire pourquoi si J est un idéal de A contenant I, I est un idéal de J. ■

Remarquons simplement qu'il n'y a pas de traduction du deuxième théorème d'isomorphisme (le lecteur attentif aura remarqué que c'était la traduction du troisième théorème d'isomorphisme). Le deuxième théorème pour les groupes fait intervenir la notion de produit direct HK, qui est bien un groupe si H est normal, mais le produit de deux idéaux n'est ni un sous-anneau, ni un idéal.

Exercice 79

On appelle idéal produit de I et J, l'idéal engendré par IJ. Le deuxième théorème d'isomorphisme pour les groupes se généralise-t-il aux anneaux en remplaçant les produits directs de groupes par cette définition sur les idéaux ?

Exercice 80

Quels sont les idéaux de $\mathbb{Z}/n\mathbb{Z}$ et les quotients correspondants ?

3.1.11.6 Primalité, maximalité d'idéaux

Dans cette section, on ne considère que des anneaux commutatifs. Soit donc A un anneau commutatif unitaire.

Définition. ***(Idéal propre)***

Un idéal I de A est *propre* si $I \neq A$.

Définition. ***(Idéal maximal)***

Un idéal I de A est dit *maximal* s'il est élément maximal[a] pour l'inclusion parmi les idéaux propres de A.

[a] Un élément a d'un espace ordonnée $(E, \leq)$ est dit *maximal* si pour tout $x \in E$, $a \leq x \implies x = a$.

Remarque. *D'après la définition*, l'idéal qui est l'anneau entier n'est jamais maximal.

Exercice 81

Soit A un anneau quelconque et I l'ensemble des éléments non inversibles de A. On suppose que la somme de deux non inversibles est encore non inversible. Montrer que I est un idéal (bilatère) maximal de A (parmi tous les idéaux de A, bilatères ou non).

▷ **Éléments de réponse.**

Vérifier d'abord que c'est un idéal. Soit J un idéal tel que $I \subseteq J$. Montrer que $J = I$ ou $J = A$, autrement, si J est propre, alors $J = I$, ce qui colle bien à la définition.

Propriété. ***(Caractérisation calculatoire des idéaux maximaux)***

L'idéal I est maximal si et seulement si I est propre et pour tout $x \in A \setminus I$, $I + Ax = A$.

▷ Attendre la preuve suivante qui montre tout d'une pierre deux coups. ■

Propriété. ***(Caractérisation fondamentale des idéaux maximaux)***

L'idéal I est maximal si et seulement si A/I est un corps (commutatif).

▷ Si I est maximal, pour tout $x \in A \setminus I$, $I + Ax$ est un idéal contenant strictement I, donc par maximalité, il égale A. Soit maintenant $\overline{x}$ un élément non nul de l'anneau quotient A/I. Cela signifie que $x \notin I$, et, par hypothèse, il existe $a \in A$ et $i \in I$ tel que $i + ax = 1$, ce qui entraîne $\overline{ax} = 1$ dans A/I, donc tout élément non nul de A/I est inversible. Puisque I est propre, A/I est non trivial ; A/I est donc un corps non nécessairement commutatif. Si l'on suppose cela, enfin, ses seuls idéaux sont triviaux. Or le théorème de correspondance (donnant les sous-groupes distingués d'un groupe quotient) énonce que l'existence d'une bijection entre les idéaux de A contenant I et les idéaux de A/I : le seul idéal propre de A contenant I est donc lui-même, ce qui signifie que I est maximal parmi les idéaux propres de A. Toutes ses propositions sont donc équivalentes. ■

En se rappelant l'exercice précédent, on peut établir le cas limite suivant :

Corollaire. ***(Maximalité de l'idéal nul)***

L'idéal nul de A est maximal si et seulement si A est un corps.

▷ Si A est nul, l'idéal nul n'est pas propre, donc il n'est pas maximal : ça tombe bien, A n'est pas un corps. Autrement, $A/\{0\} \simeq A$ donc d'après la caractérisation précédente, 0 est maximal si et seulement si A est un corps. Remarquer qu'il ne servait à rien de distinguer le premier cas. ■

La manipulation des idéaux maximaux est facilitée (comme on l'a déjà éprouvée précédemment, d'ailleurs) par le théorème suivant qui permet d'inclure tout idéal propre dans un idéal maximal. Sans surprise, c'est le lemme de Zorn, et donc l'axiome du choix, qui permet d'énoncer ce théorème, fondamental en algèbre constructiviste.

Théorème. ***(Krull, 1929)***

Tout idéal propre d'un anneau A est inclus dans un idéal maximal de A.

▷ C'est une conséquence directe du lemme de Zorn appliqué à l'ensemble des idéaux propres de A contenant I, qui est clairement inductif. En effet, si $(I_t)_{t\in T}$ est une famille non vide d'idéaux, alors sa réunion est un idéal non vide. La totalité du sous-ordre intervient pour montrer que cette réunion est un sous-groupe, et non la stabilité par multiplication par tout élément de l'anneau ! ■

VOC Pour ne pas se tromper, prononcer « krül ».

Remarque. Contrairement au théorème d'existence d'une base des espaces vectoriels, qui ne sert pas énormément, le théorème de Krull, qui utilise aussi l'axiome du choix, qui extraordinairement utile.

On peut également montrer le théorème de Krull par des moyens plus sobres, mais également plus généraux. Nous nous y employons dès maintenant.

Lemme

Soit A un anneau commutatif. Soit I un idéal de A. Alors l'ensemble des idéaux de A/I est en bijection avec l'ensemble des idéaux de A contenant I.

▷ Nous avons déjà vu ce résultat. ■

Lemme

Soit A un anneau commutatif. Soit $(I_t)_{t\in\mathcal{T}}$ une famille d'idéaux de A totalement ordonnée pour l'inclusion. Alors $\bigcup_{t\in\mathcal{T}} I_t$ est un idéal de A.

▷ Soient $x \in I_{t_1}$ et $y \in I_{t_2}$. Alors sans perte de généralité $I_{t_1} \subseteq I_{t_2}$ donc $x + y \in I_{t_2}$. On conclut facilement que c'est un sous-groupe, et le fait que c'est un idéal est clair. ■

Lemme

Soit A un anneau commutatif et S une partie de A contenant 1 et stable par multiplication. Soit I un idéal de A ne rencontrant pas S. Soit $\mathcal{T}$ l'ensemble des idéaux de A contenant I et ne rencontrant pas S. Alors :

1. $\mathcal{T}$ admet un idéal maximal pour l'inclusion ;
2. tout élément maximal de $\mathcal{T}$ est un idéal premier de A.

▷ Soit T une sous partie de $\mathcal{T}$ totalement ordonnée pour l'inclusion. On veut vérifier que T admet une borne supérieure. Si T est vide, I est une borne supérieure. Sinon on pose $J = \bigcup_{I \in T} I$ idéal de A. De plus, pour tout $I \in T$, $I \subseteq J$, donc J est un majorant pour T. D'autre part $J \cap S = \emptyset$. Il reste à voir que $J \in \mathcal{T}$ dès que $I \subseteq J$. ■

On peut donc conclure :

Proposition. ***(Théorème de Krull)***

Soit A un anneau et I un idéal de A propre. Alors il existe un idéal maximal de A contenant I.

▷ On applique le dernier lemme avec $S = \{1\}$. ■

Exercice 82

Démontrer le théorème de Krull dans un anneau noethérien.

▷ **Éléments de réponse.**

Soit A un anneau noethérien. Soit I un idéal propre de A. S'il n'est pas maximal, c'est par définition qu'il existe I_1 un idéal propre de A tel que $I \subseteq I_1$. Si I_1 n'est pas maximal, c'est qu'il existe I_2 un idéal propre de A tel que $I_1 \subseteq I_2$, et ainsi de suite, on obtient une suite croissante d'idéaux propres de A. Par construction elle est stricte. Absurde, puisque A est noethérien ! Donc l'un des I_n est maximal, et bel et bien propre. Il contient I.

On peut énoncer le théorème de Krull dans sa version légèrement plus faible :

Théorème. ***(Krull faible)***

Tout anneau non nul admet un idéal maximal.

Un monde sans Krull

Pour les mathématiciens constructivistes, qui ne croivent pas en l'axiome du choix, il n'y a pas de théorème de Krull. En effet, on peut démontrer que ce dernier est en fait équivalent au

lemme de Zorn, lui-même équivalent à l'axiome du choix. C'est le cas du très éminent Henri Lombardi, qui a écrit à ce sujet.

Pour un constructiviste, il existe donc un anneau n'ayant aucun idéal maximal. De là à le construire...

On termine cette moitié de partie sur les idéaux maximaux, par deux propriétés sur leur réunion et leur intersection qui trouveront par ailleurs leur égal pour les idéaux premiers.

Corollaire. ***(Réunion de tous les idéaux maximaux)***

L'ensemble des éléments non inversibles de A est $\bigcup_{I \text{ idéal maximal de } A} I$.

▷ Il suffit de reprendre dans le bon ordre les considérations précédentes. ■

Quant à l'intersection de tous les idéaux maximaux de A, on peut montrer que c'est $\{x \in A \mid \forall y \in A \quad 1 + xy \in A^\times\}$. Il s'agit du *radical de Jacobson* d'un anneau, mais nous l'étudierons indépendamment dans les compléments.

Remarque. Pour un constructiviste, l'étude du radical de Jacobson est inenvisageable. Preuve que ce sont vraiment des fous.

On passe maintenant à la notion d'idéal premier.

Définition. ***(Idéal premier)***

On appelle *idéal premier* de A tout idéal I tel que l'anneau quotient A/I est intègre.

Remarque. Puisqu'un anneau intègre, par définition, est non nul, un idéal premier est nécessairement propre.

Propriété. ***(Caractérisation calculatoire des idéaux premiers)***

Un idéal I est premier si et seulement si pour tous x,$y \in A$, si $xy \in I$, alors $x \in I$ ou $y \in I$.

▷ Notons $\overline{x}$ la classe de $x \in A$ dans A/I. Alors $\overline{x} = 0 \iff x \in I$ et tous les éléments de A/I sont de la forme $\overline{x}$, $x \in A$. L'implication de la définition se réécrit donc $\forall \overline{x}, \overline{y} \in A/I \quad \overline{xy} \implies (\overline{x} = 0 \text{ ou } \overline{y} = 0)$, ce qui caractérise l'intégrité de A/I. ■

Remarque. Par récurrence, on montre que pour tous éléments a_1,...,$a_n \in A$, $n \in \mathbb{N}$, si I est un idéal premier, $a_1...a_n \in I \implies \exists i \quad a_i \in A$.

On peut penser qu'il y a une dissymétrie dans les définitions entre idéaux maximaux et idéaux premiers : en effet, pour les deux notions, on a une caractérisation calculatoire. Pourtant la caractérisation fondamentale de la maximalité est dans le cas de la primalité la définition. Il n'en est rien : on aurait pu définir la notion d'idéal premier de la manière suivante (mais en pratique, c'est très marginal).

Propriété. ***(Caractérisation fondamentale des idéaux premiers)***

Un idéal I est premier si et seulement s'il est propre et pour tous idéaux J,K de A, si $JK \subseteq I$, alors I contient J ou K.

C'est un choix pédagogique pratique que d'avoir introduit les deux notions sur cette dissymétrie. On l'effacera rapidement en pratique.

On a les propriétés suivantes, à retenir absolument.

Corollaire

Tout idéal maximal est premier.

▷ Tout corps est intègre. ■

Corollaire

Tout anneau non nul admet des idéaux premiers.

▷ Conséquence directe de la définition précédente et du théorème de Krull. ■

Propriété. ***(Primalité de l'idéal nul)***

L'idéal nul d'un anneau est premier si et seulement s'il est intègre.

On termine par les propriétés sur la réunion et l'intersection d'idéaux premiers, comme promis.

Propriété. ***(Réunion de tous les idéaux premiers)***

$\bigcup_{I \text{ premier}} I$ est l'ensemble des non-inversibles de A.

▷ Puisque tout maximal est premier et que l'on connaît déjà la réunion de tous les idéaux maximaux. ■

La deuxième propriété est bien plus importante. La preuve nécessite pourtant la notion de localisation, que nous verrons un peu plus tard dans notre exposé.

Propriété. ***(Intersection de tous les idéaux premiers)***

On a $\bigcap_{I \text{ premier}} I = \mathrm{Nil}(A)$.

▷ Soit a un élément nilpotent de A et I un idéal premier de A. C'est en particulier un sous-groupe, donc il contient 0. Comme il existe $n \in \mathbb{N}$ tel que $a^n = 0$, on a $a^n \in I$. Puisque I est premier, $a \in I$. Ceci vaut pour tout I premier, donc $a \in \bigcap_{I \text{ premier}} I$.

Réciproquement, soit $a \notin \mathrm{Nil}(A)$. Alors $S = \{1,a,a^2,...\}$ est une partie multiplicative de A ne contenant pas 0. On peut donc localiser A par S. De plus, par un corollaire du théorème de Krull, l'anneau $S^{-1}A$ admet au moins un idéal premier ; or on sait d'après la théorie de la localisation que les idéaux premiers de $S^{-1}A$ sont en correspondance bijective avec les idéaux premiers de A ne rencontrant pas S. Il existe donc un idéal premier I de A ne rencontrant pas S, en particulier, $a \notin I$. Ainsi $a \notin \bigcap_{I \text{ premier}} I$. ■

On notera avant de partir qu'un idéal premier n'a aucune raison d'être maximal, y compris dans un anneau factoriel. En revanche, dans un anneau principal, tout idéal premier non nul est maximal.

Lemme. ***(Propriété de primalité sur l'idéal produit)***

Soit A un anneau et $\mathfrak{p}$ un idéal premier. Soient $I_1,...,I_n$ des idéaux de A tels que $I_1,...,I_n \subseteq \mathfrak{p}$. Alors il existe k tel que $I_k \subseteq \mathfrak{p}$.

▷ Si pour tout k, $I_k \not\subseteq \mathfrak{p}$, alors il existe $x_k \in I_k$ tel que $x_k \notin \mathfrak{p}$ pour tout k. Mais alors $x_1...x_k \in I_1...I_n \subseteq \mathfrak{p}$ donc il existe $x_i \in \mathfrak{p}$ pour un i, contradiction. ■

3.1.11.7 Anneau local

Définition. ***(Anneau local)***

On appelle *anneau local* un anneau commutatif ayant un unique idéal maximal.

Propriété. ***(Caractérisation des anneaux locaux)***

Un anneau commutatif non nul A est local si et seulement si $\forall a,b \in A \setminus A^* \quad a+b \in A \setminus A^*$.

Définition. ***(Idéal très maximal)***

Soit A un anneau local et I son unique idéal maximal. On dit que I est son idéal *très maximal*.

Propriété. ***(Description des idéaux très maximaux)***

Soit A un anneau local et I son idéal très maximal. Alors $A = A \setminus A^*$.

3.1.11.8 Morphismes et idéaux premiers, maximaux

Lemme. ***(Trace d'un idéal premier)***

Si A est un anneau, A' un sous-anneau de A, alors p est un idéal premier de A. Alors $p \cap A'$ est un idéal premier de A'.

▷ Voir la propriété suivante. ■

Propriété. ***(Image réciproque d'un idéal premier)***

Soit $f : A \longrightarrow B$ et I un idéal premier de B. Alors $f^{-1}(I)$ est un idéal premier de A.

▷ Par hypothèse, au sens de la catégorie des anneaux,

$$A \xrightarrow{f} B \xrightarrow{\pi} B/I$$

où $\mathrm{Ker}(\pi \circ f) = f{-}1(I)$. Ainsi par factorisation, $A/f^{-1}(I) \xhookrightarrow{\overline{\pi \circ f}} B/I$. Or B/I est intègre et d'après le diagramme précédent $A/f^{-1}(I)$ s'identifie à un sous-anneau de B/I, donc $A/f^{-1}(I)$ est intègre et $f^{-1}(I)$ est premier. ■

Propriété. ***(Quotient par une somme, double quotient)***

Soit A un anneau et I,J deux idéaux de A. On note $\overline{J}$ l'image de l'idéal J dans A/I. Alors $A/(I+J)$ est isomorphe à $(A/I)/\overline{J}$.

▷ On note $p : A \xrightarrow{\pi} A/I \xrightarrow{\pi'} (A/I)/\overline{J}$. Par théorème d'isomorphisme, on a $A/\mathrm{Ker}(p) \simeq (A/I)/\overline{J}$. Or x est dans $\mathrm{Ker}(p)$ si et seulement si $\pi(x) \in \overline{J}$, si et seulement s'il existe $z \in J$ tel que $\pi(x) = \pi(z)$, c'est-à-dire s'il existe $z \in J$ tel que $x - z \in I$ soit $x \in I + J$. ■

Corollaire

Soit A un anneau et I un idéal de A, J un idéal de A contenant I. Alors $(A/I)/\overline{J} \simeq A/J$.

Remarque. C'est beaucoup plus simple dans les anneaux principaux.

Propriété. ***(Polynômes à coefficients dans un quotient)***

Soit A un anneau et I un idéal de A. Alors $(A/I)[X] \simeq A[X]/I \cdot A[X]$.

▷ On introduit la réduction des coefficients modulo I : $\phi : A[X] \longrightarrow (A/I)[X]$. On vérifie que c'est un morphisme d'anneaux, de plus surjectif. Or $\mathrm{Ker}(\Phi) = I[X] = I \cdot A[X]$. ■

⟶ **Notation.** On notera $I[X] = I \cdot A[X]$

Exemple. ***(Idéaux premiers de $\mathbb{Z}[X]$ engendrés par un entier)***

Ainsi, pour p premier, $(\mathbb{Z}/p\mathbb{Z})[X] \simeq \mathbb{Z}[X]/p\mathbb{Z}[X]$. En particulier, $p\mathbb{Z}[X]$ est un idéal premier des polynômes à coefficients dans $\mathbb{Z}$.
La question de la détermination des idéaux premiers de $\mathbb{Z}[X]$ est plus subtile.

3.1.12 Localisation, corps des fractions d'un anneau intègre

Soit pour l'instant un anneau A simplement supposé commutatif.

3.1.12.1 Anneau des fractions d'un anneau commutatif ou localisé

Définition. ***(Partie multiplicative d'un anneau)***

Une partie non vide S d'un anneau A est dite *multiplicative*, ou un *système multiplicatif*, si pour tous $(x,y) \in S^2$, $xy \in S$ et si S ne contient pas zéro.

Remarque. Si S est une partie multiplicative, alors $S \cup \{1\}$ est encore multiplicative, car ajouter 1 ne change rien : en multipliant n'importe quel élément par 1, on reste sur cet élément. Le lecteur pourra vérifier dans quelques instants que si $S' = S \cup \{1\}$, alors $S^{-1}A = S'^{-1}A$, ce qui rend l'appartenance ou non de 1 à S tout à fait caduque. On donnera ensuite une autre considération au même sujet.

Soit $S \subseteq A$ une partie multiplicative. On va construire une A-algèbre notée $S^{-1}A$ ou AS^{-1}, que l'on appellera *localisée* de A par S. Heuristiquement, le but est de définir un sur-anneau de A tels que les éléments de S soient inversibles. (On comprend alors l'hypothèse de multiplicativité, car il est illusion de supposer que le produit de deux inversibles ne le soient pas.) Pour ce faire, on munit le produit $S \times A$ de la relation R définie par

$$(s,x)R(s',x') \text{ ssi } \exists \sigma \in S \quad \sigma s'x = \sigma sx'.$$

Lemme

R est d'équivalence.

▷ C'est clair par hypothèse de multiplicativité sur S. ■

Remarque. Si l'anneau A est intègre, la relation R s'écrit : $(s,x)R(s',x')$ si $s'x = sx'$.

⟶ **Notation.** On note $\frac{x}{S} \in S^{-1}A$ la classe de x et on appelle un tel élément une *fraction*, « à dénominateur dans S ». Notons également le fait suivant qui vaut pour tous $x,x' \in A$, $s,s' \in S$.

Lemme

Les quantités $\frac{xx'}{SS'}$ et $\frac{xs'+x's}{SS'}$ ne dépendent que $\frac{x}{s}$ et de $\frac{x'}{s'}$.

On peut donc dire :

Proposition. ***(Anneau de fractions sur un anneau)***

Les opérations $+$ et $\times$ sur $S^{-1}A$ définissent une structure d'anneau sur $S^{-1}A$.

Remarque. La terminologie *anneaux de(s) fractions* est mauvaise, car elle oublie que le localisé dépend de la partie multiplicative choisie. Toutefois elle remédie à l'homonymie éventuelle avec la notion de *localisé* absolu par rapport à un idéal premier.

Exercice 83

(Plongement de A dans son localisé) Montrer que pour tout $a \in A$, pour tout $s \in S$, $s' \in S$, $\frac{as}{s} = \frac{as'}{s'}$, et que de plus, si S contient 1, $\frac{as}{s} = \frac{a}{1}$.

Puisque $(S^{-1}A, +, \cdot\ )$ est un anneau, l'application η de A dans S^1A qui à a fait correspondre $\frac{a}{1} = \frac{as}{s}$ pour n'importe quel $s \in S$ est un morphisme d'anneaux, bien défini, car S est non vide. Autrement dit :

Proposition. ***(Localisation)***

$(S^{-1}A, +, \times)$ est une A-algèbre.

Notons que η n'est pas injective, dès que S possède des diviseurs de 0.
Ceci donne un exemple simple de construction de A-algèbre dans laquelle le morphisme canonique η n'est pas injectif.

Remarque. Pour certains auteurs, une partie multiplicative peut contenir zéro. Dans ce cas, il n'y a qu'une seule classe d'équivalence modulo R, donc le localisé est l'anneau nul.

Proposition

Soit A un anneau et S une partie multiplicative. Pour toute A-algèbre B définie par η, si $\eta(S) \subseteq B^\times$, il existe un unique A-algèbre-morphisme de $S^{-1}A$ dans B.

Ainsi on a la propriété universelle suivante énoncée dans le cas, le seul intéressant, où S n'a pas de diviseurs de zéro.

Proposition. ***(Minimalité du localisé)***

Soit A un anneau et S une partie multiplicative ne contenant pas de diviseurs de zéro. Alors $S^{-1}A$ se plonge dans tout anneau ayant A pour sous-anneau tel que tout élément de S soit inversible.

▷ Conséquence de la proposition précédente et de l'injectivité de η lorsque S est intègre. ■

Exercice 84

Localiser $\mathbb{Z}^2$ muni des lois produits par $\mathbb{Z}^* \times \{0\}$.

Reprenons le cas général.

Remarque. Grâce à la définition usuelle d'opérations entre fraction, on dispose des identités usuelles du premier cycle entre fractions. Il faut simplement prendre garde à ce genre de choses :

$$\frac{a}{s} = 1 \text{ donc } \frac{s}{a} = 1,$$

car $a \notin S$ a priori !

On dispose du fait suivant qui relie la localisation et la divisibilité.

Propriété. ***(Divisibilité et localisation)***

Soit $s \in S$ divisant $a \in A$ par le diviseur associé $k \in A$. Alors $\frac{a}{s} = k$.

▷ Il faut comprendre $k = \frac{k}{1}$. Autrement, c'est une simple réécriture de l'égalité $sk = a$. ■

Enfin, dans le localisé par S, on a la propriété suivante, qui reflète l'intérêt de la construction :

Propriété. ***(Quelques inversibles du localisé)***

Les inversibles de $S^{-1}A$ contiennent au moins $A^\times$, S, $\frac{A^\times}{S}$ et $\frac{S}{S}$.

Exercice 85

Y en a-t-il d'autres ?

Plus généralement :

Propriété. ***(Inversibles du localisé)***

Les inversibles de $S^{-1}A$ sont les fractions à numérateur dans les A-diviseurs d'éléments de S.

▷ Soit $a \in A$. Si a est inversible dans $S^{-1}A$, il existe $a' \in A$, $s \in A$ tel que $\frac{a}{1} = \frac{a'}{s}$. Ainsi il existe $\sigma \in S$ tel que $\sigma a a' = \sigma s$, soit $a(\sigma a') = \sigma s \in S$, donc a divise un élément de S. On vérifie facilement que cette condition est suffisante. On en déduit, puisque $\frac{a}{s} \in (S^{-1}A)^\times$ si et seulement si $a \in (S^{-1}A)^\times$, que $\frac{a}{s} \in (S^{-1}A)^\times$ si et seulement s'il existe $b \in A$ tel que $ab \in S$. ■

Cette dernière propriété est riche d'une conséquence très pratique pour la manipulation plus avancée des localisés. Nous aurons besoins des considérations suivantes.

Lemme

Soient S,T deux parties multiplicatives de A telles que $S \subseteq T$. Alors $S^{-1}A \hookrightarrow T^{-1}A$.

▷ Puisque tout élément $s \in S$ est un élément de T, toute fraction $\frac{a}{s}$ peut être vue comme une fraction de $T^{-1}A$. ■

Définissons maintenant une notion propre aux parties multiplicatives.

Définition. ***(Saturé d'une partie multiplicative)***

Soit S une partie multiplicative de A. Le *saturé* S' de S est l'ensemble des diviseurs d'éléments de S. On note souvent $S' = S_{\text{sat}}$.

Exercice 86

Vérifier que le saturé d'une partie multiplicative est encore une partie multiplicative.

On a clairement $S \subseteq S_{\text{sat}}$, puisque tout point se divise lui-même dans un anneau unitaire.

Définition. ***(Saturation d'une partie multiplicative)***

Soit S une partie multiplicative de A. On dit que S est *saturée* si elle contient son saturé.

On a le résultat fondamental suivant.

Propriété. ***(La saturation est une opération bénigne)***

Soit S une partie multiplicative de A. Alors $S^{-1}A = S_{\text{sat}}^{-1}A$.

▷ Il suffit donc de montrer que $S_{\text{sat}}^{-1}A \subseteq S^{-1}A$ (au sens de l'injection morphique bien sûr). Soit $s \in S_{\text{sat}}$. Alors il existe $b \in A$ tel que $sb = s' \in S$. On remarque que b ne peut être nul car $0 \notin S$. Soit $a \in A$. Il s'agit de montrer que $\frac{a}{s}$ s'écrit comme une fraction de $S^{-1}A$. Or dans cet anneau, $\frac{ab}{s'} = \frac{ab}{sb} = \frac{a}{s}$, ce qui fournit trivialement le plongement cherché. ■

On peut donc formuler la propriété sur les inversibles du localisé de la manière suivante : les inversibles de $S^{-1}A$ sont $\frac{S_{\text{sat}}}{S_{\text{sat}}}$.

On termine en mentionnant la propriété universelle des localisés, inutile, mais essentielle.

Propriété. ***(Propriété universelle de la localisation)***

Soit A un anneau, B un autre. Soit S une partie multiplicative de A. Pour tout morphisme d'anneaux $f : A \longrightarrow B$, il existe un unique morphisme d'anneaux $\tilde{f} : S^{-1}A \longrightarrow B$ tel que $f = \tilde{f} \circ \eta_A$.

$$\begin{array}{ccc} A & \xrightarrow{\ f\ } & B \\ {\scriptstyle \eta_A}\downarrow & \nearrow_{\tilde{f}} & \\ S^{-1}A & & \end{array}$$

▷ L'écrire. ■

3.1.12.2 Corps des fractions proprement dit

On s'intéresse maintenant au cas particulier où A est intègre et $S = A \setminus \{0\}$.

Définition-propriété. ***(Corps des fractions)***

L'anneau $Frac(A) = (A \setminus \{0\})^{-1}A$ est un corps, appelé *corps des fractions* de A.

Propriété. ***(Structure du corps des fractions)***

Le corps des fractions de A est une A-algèbre par $\eta : a \longmapsto \frac{a}{1}$.

Fait

Si S est une partie multiplicative de A qui ne contient pas 0, $S^{-1}A$ s'identifie aux éléments de $Frac(A)$ de la forme $\frac{a}{s}$, $s \in S$.

Propriété. ***(Minimalité du corps des fractions)***

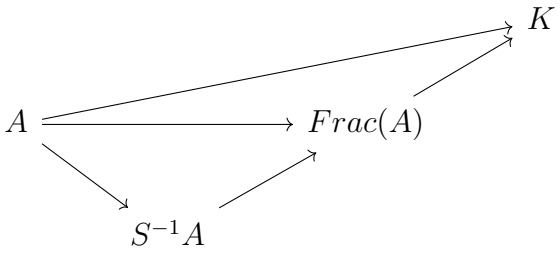
Le corps des fractions de A est une A-algèbre par $\eta : a \longmapsto \frac{a}{1}$.

On peut énoncer cette propriété de la manière universelle suivante. Pour clore cette section constructive, on propose une démonstration de la construction de $Frac(A)$ moins formalisante que le procédé de localisation.

Propriété. ***(Corps des fractions)***

Pour tout corps K et toute morphisme injectif $j : A \hookrightarrow K$, il existe un unique morphisme de corps $\overline{j} : Frac(A) \longrightarrow K$ prolongeant j.

▷ L'ensemble $E = A \times A \setminus \{0\}$ est muni d'une structure algébrique en posant $(a,b) + (c,d) = (ad + cb,bd)$ et la multiplication terme à terme (on constate alors l'existence d'un élément neutre additif (0,1) et d'un élément neutre multiplicatif (1,1)). Ces deux pseudo-lois sont aussi associatives et commutatives en conséquence de ces propriétés des lois de A. On définit une relation sur E par $(a,b) \simeq (c,d)$ si et seulement si $ad = bc$. C'est une relation d'équivalence. Elle est compatible avec l'addition et la multiplication sur E ; par le théorème de factorisation, on peut définir la structure $K(A) = E/\simeq$. Dans $K(A)$, le couple $(-a,b)$ est un symétrique du couple (a,b), car $(-a,b) + (a,b) = (-ab + ab,b^2)$, $\times$ étant commutative et l'on remarque que $(0,b^2) \simeq (0,1)$. Donc $K(A)$ muni de la pseudo-addition induite est un groupe. Il reste seulement à montrer la distributivité de la pseudo-multiplication induite sur la pseudo-addition induite. ■



Exercice 87

(Cardinal du corps des fractions) Soit A un anneau intègre.

1. Si A est fini, quel est le cardinal de $Frac(A)$?
2. On suppose A infini. Discuter du cardinal de $Frac(A)$.

▷ **Éléments de réponse.**

Si A est fini et intègre, que peut-on en déduire ? Pour le cas infini, se référer à la construction théorique du corps des fractions.

3.1.12.3 Localisation d'un anneau (par rapport à un idéal premier)

Définition-propriété. ***(Localisation en un idéal premier)***

Soit A un anneau et I un idéal premier. Alors l'anneau des fractions de A sur la partie $S = A \setminus I$, noté $A_{(I)}$, est appelé *localisé* en I.

▷ Il est clair que S est multiplicative. ■

Propriété. ***(Localité du localisé)***

Tout localisé (en un idéal premier) est un anneau local.

Exemples

1. Si A est intègre et $I = \{0\}$, on retombe sur le corps des fractions.
2. $A = \mathbb{Z}$ et $I = p\mathbb{Z}$ avec p un nombre premier.

3.1.13 Idempotence dans un anneau

Dans un anneau, l'idempotence se ramène naturellement à celle de son monoïde multiplicatif.

3.1.14 Nilpotence

Propriété. *(Nilpotence du nul)*

L'élément nul d'un anneau est nilpotent. Son ordre de nilpotence est 1 si A est non nul, 0 sinon.

Remarque. *(Nilpotence d'ordre nul)* Soit A un anneau. Il admet des nilpotents d'ordre nul si et seulement s'il est nul, auquel cas tous les éléments sont nilpotents d'ordre nul. Autrement dit, dans un anneau non nul, aucun élément n'est nilpotent d'ordre nul.

Propriété. *(Grands ordres de nilpotence)*

Soit A un anneau non nul et $x \in \mathrm{Nil}(A)$. Alors $\mathrm{ord}(x) \geqslant 2 \iff x \neq 0$.

Propriété. *(Nilpotence de l'opposé)*

Soit A un anneau. Si x est nilpotent, $-x$ également.

Propriété. *(Non-nilpotence des inversibles)*

Soit A un anneau non nul. Si x est inversible, x n'est pas nilpotent.

Propriété. *(Lien nilpotent-inversible)*

Soit A un anneau. Si $x \in \mathrm{Nil}(A)$, alors $1 - x \in A^\times$.

Exercice 88

Si x est inversible, $1 - x$ est-il nilpotent ?

▷ **Éléments de réponse.**

Clairement pas... Il suffit de se placer dans $\mathbb{R}$ et prendre $x = 2$.

Propriété. *(Structure des nilpotents)*

Soit A un anneau **commutatif**. Alors $\mathrm{Nilp}(A)$ est un idéal de A.

Exercice 89

Montrer que si A n'est pas commutatif, alors $\mathrm{Nil}(A)$ n'est pas un idéal de A.

3.2 Compléments à l'étude élémentaire des anneaux

3.2.1 Anneaux des entiers de Gauss

Proposition

$\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2+1)$.

▷ C'est le premier théorème d'isomorphisme sur le polynôme minimal ■

3.2.2 Radical d'un idéal

Très vite, tous les anneaux dans cette section sont supposés commutatifs. La commutativité intervient dès la preuve de ce que le radical d'un idéal est lui-même un idéal. On verra dès lors un contre-exemple dans le cas non commutatif.

Définition. ***(Radical d'un idéal)***

Soit A un anneau et I un idéal de A. On appelle *radical* de I, l'ensemble :

$$\sqrt{I} = \{a \in A \mid \exists n \in \mathbb{N} \quad a^n \in I\}.$$

Proposition

Soit A un anneau **commutatif**. Le radical d'un idéal de A est un idéal.

▷ On le vérifie point par point.

⋆ Vérifions d'abord que I est un sous-groupe additif de A. Il contient évidemment 0, car $0^1 = 0 \in I$ lui-même sous-groupe additif de A.

⋆ Ensuite, ce n'est pas dur.

Ceci termine la preuve. ■

Exercice 90

Donner un exemple d'anneau dans lequel le radical d'un certain idéal bilatère n'est pas un idéal.

▷ **Éléments de réponse.**

Prenons l'idéal nul dans $\mathfrak{M}_2(\mathbb{R})$. Le radical de cet idéal est, par définition, l'ensemble des matrices nilpotentes de cet espace. Ce n'est pas un idéal (ni à droite, ni à gauche...).

Fait. ***(Lien entre nilpotents et radical d'un idéal)***

Pour tout anneau A (non nécessairement commutatif), $\mathrm{Nil}(A) = \sqrt{\{0\}}$.

▷ Simple réécriture de la définition. ■

En fait, on peut énoncer le fait suivant qui, bien qu'il ne soit pas utile pour démontrer les propriétés élémentaires du radical, accessibles en première année de Licence, décrit de façon bien plus claire le radical d'un idéal.

Propriété. ***(Lien entre radical d'un idéal et nilpotence)***

Soit A un anneau et I un idéal de A. Alors :

$$\sqrt{I} = \mathrm{Nil}(A/I).$$

On remarque les deux propriétés suivantes, très utiles pour la suite, et qui ne découlent que de la définition ensembliste d'idéal radical.

Propriété. ***(Supériorité du radical)***

Soit A un anneau et I un idéal de A. Alors $I \subseteq \sqrt{I}$.

Propriété. ***(Croissance du radical)***

Soit A un anneau et I,J deux idéaux de A tels que $I \subseteq J$. Alors $\sqrt{I} \subseteq \sqrt{J}$.

On peut maintenant énoncer des propriétés pratiques de calcul du radical.

Propriété. ***(Idempotence du radical)***

Soit A un anneau **commutatif** et I un idéal de A. Alors $\sqrt{\sqrt{I}} = \sqrt{I}$.

Propriété. ***(Radical d'une intersection)***

Soit A un anneau **commutatif** et I, J deux idéaux de A. Alors $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

Exercice 91

Calculer $\sqrt{6\mathbb{Z}}$ dans $\mathbb{Z}$, puis $\sqrt{24\mathbb{Z}}$.

Propriété. ***(Radical d'une somme)***

Soit A un anneau **commutatif** et I,J deux idéaux de A. Alors $\sqrt{I+J} \subseteq \sqrt{I} + \sqrt{J}$.

Exercice 92

Donner un exemple dans lequel l'inclusion réciproque n'est pas vérifiée.

Pour terminer, on énonce cette propriété très générale qui relie la notion de radical et celle d'idéal premier.

Propriété. ***(Description spectrale du radical)***

Soit A un anneau et I un idéal propre de A. Le radical de I est l'intersection des idéaux premiers le contenant.

En particulier, dans le cas de l'idéal nul, on retrouve que $\mathrm{Nil}(A) = \bigcap_{I \text{ premier}} I$ dans le cas d'un anneau non nul.

3.2.3 Radical de Jacobson d'un anneau

3.2.4 Caractéristique d'un anneau, morphisme de Frobenius

Définition. ***(Caractéristique d'un anneau)***

Soit A un anneau. On note $\mathrm{car} : \mathbb{Z} \longrightarrow A$ l'unique homomorphisme (qui à 1 fait correspondre 1_A). On a $\mathrm{Ker}(\mathrm{car}) = n\mathbb{Z}$, n générateur minimal naturel. On appelle n, la *caractéristique* de l'anneau A.

Exercice 93

Commenter : si la caractéristique est première et que l'on suppose l'anneau commutatif, alors l'anneau est intègre.

▷ **Éléments de réponse.**

Que dire de $(\mathbb{Z}/3\mathbb{Z})^2$?

On a le résultat plus général suivant :

Curiosité. ***(Anneaux infinis de caractéristique finie)***

Pour tout entier naturel $n \geqslant 2$, il existe des anneaux infinis de caractéristique n.

▷ On sait que $\mathbb{Z}/n\mathbb{Z}$ est de caractéristique n. En posant $A = \mathbb{Z}/n\mathbb{Z}^{\mathbb{N}}$, on obtient un anneau infini dont on vérifie très vite qu'il est de caractéristique n. ■

Propriété. ***(Morphisme de Frobenius)***

Soit A un anneau commutatif. Supposons $\mathrm{car}(A) = p$ premier. Alors :

$$\begin{array}{rccc} \mathrm{Frob} : & A & \longrightarrow & A \\ & x & \longmapsto & x^p \end{array}$$

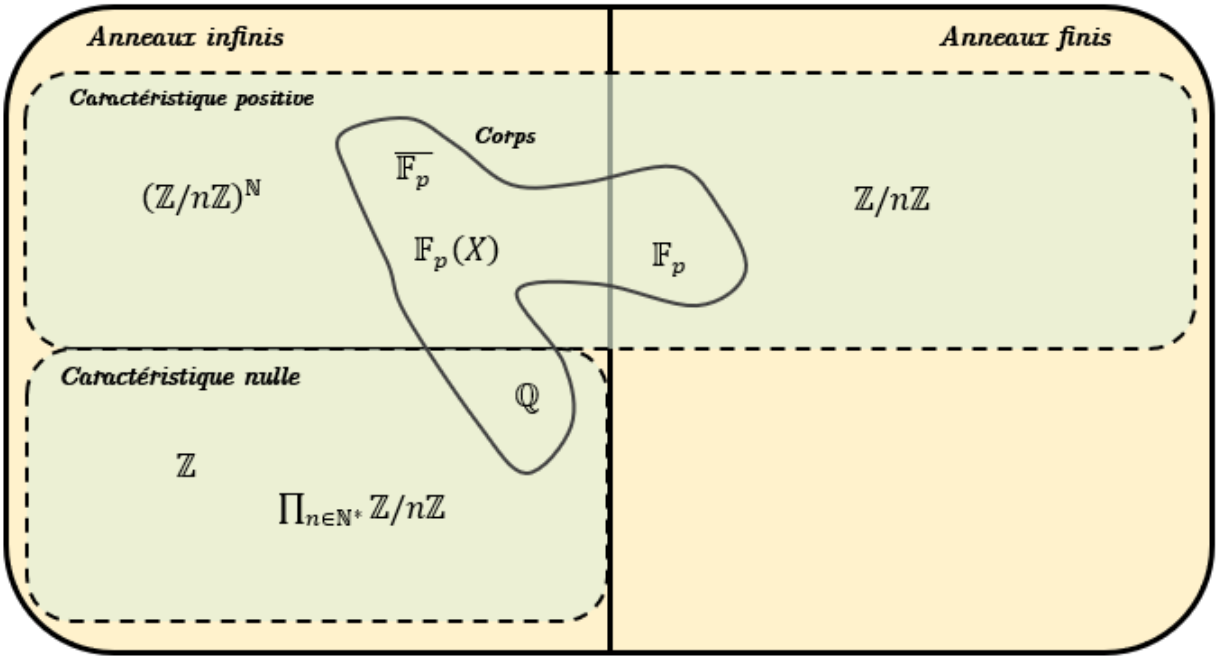


FIGURE 3.2.1 : *Lien entre le cardinal des anneaux et leur caractéristique finie ou finie. Par théorème de Lagrange, un anneau fini est forcément de caractéristique finie.* —

est un morphisme d'anneaux.

Il faut être en milieu commutatif et bien sûr ne pas oublier l'hypothèse de caractéristique indécomposable !

Proposition

Soient $a_1,...,a_r$ éléments d'un anneau de caractéristique p. Alors

$$(a_1 + ... + a_r)^p = a_1^p + ... + a_r^p.$$

Remarques.

1. Si K est intègre, en particulier s'il est intègre, F_K = Frob dans K est clairement injectif. Il est donc surjectif si K est fini.
2. En particulier, si A est intègre, la seule racine p-ième de l'unité est 1. On l'aurait vu par $X^p - 1 = (X - 1)^p$.

Définition. ***(Corps parfait)***

Un corps K est dit *parfait* s'il est de caractéristique nulle ou s'il est de caractéristique positive et son morphisme de Frobenius $\in \mathrm{Aut}(K)$ (*i.e.* , il est surjectif).

Remarques.

1. D'après les remarques précédentes, tout corps fini est parfait.
2. Tout corps admettant $\mathbb{Q}$ comme sous-corps premier est parfait. Il faut donc s'intéresser essentiellement aux extensions de cardinal infini des corps finis.
3. $\overline{\mathbb{F}_q}$ est parfait... (clairement)
4. Par contre, $K = \mathbb{F}_p(X)$ n'est pas parfait. En effet, $F_K(K) = \mathbb{F}_p(X^p) \subsetneq K$. D'abord, pour tout $a \in \mathbb{F}_p$, $a^p = a$. Ainsi, $f(X) = \frac{a_0+a_1X+\ldots+a_nX^n}{b_0+b_1X+\ldots+b_nX^n}$ d'où $f(X)^p = f(X^p)$. Par suite, $K^p \subsetneq K$.
5. Concrètement, sur un corps parfait, tous les polynômes irréductibles sont à racines simples. Avec l'exemple précédent, pour $K' = K^p$, $T^p - X^p \in K'[T] = (\mathbb{F}_p(X^p))[T] = (T - X)^p$ est tout de même irréductible. Ceci n'arrive pas dans un corps parfait, en particulier les corps finis ou de caractéristique nulle[1].

Reformulation pratique. ***(Reformulation de la perfection)***

K est parfait si et seulement si $\mathrm{car}(K) = 0$ ou $\mathrm{card}(K) = p$ et $K^p = K$.

3.2.5 Hypothèses de l'algèbre commutative

Soit A un anneau commutatif. Alors :

Proposition

Un élément $a \in A$ est inversible si et seulement s'il existe $b \in A$ tel que $ab = 1$.

Proposition

Un élément $a \in A$ est inversible si et seulement s'il existe $b \in A$ tel que $ba = 1$.

Proposition

Le binôme de Newton.

Proposition

$\mathrm{Nil}(A)$ est un idéal de A.

[1] Cet exemple n'est pas tordu, et c'est essentiellement le seul exemple.

Proposition

Pour tout idéal I de A, A/I existe.

Soit maintenant A un anneau intègre. Alors :

Proposition

A est commutatif (on a donc toutes les propositions précédentes).

Proposition

A est non nul.

Proposition. *(Primalité du nul)*

L'idéal (0) est premier dans A.

Proposition

L'ensemble $A \setminus \{0\}$ est une partie multiplicative de A. En particulier, $Frac(A)$ est bien défini. En particulier, A se plonge dans un corps commutatif.

3.3 Arithmétique des anneaux

Théorème. *(Propriétés fondamentales de $\mathbb{Z}$)*

1. Il existe une division euclidienne sur $\mathbb{Z}$ (*(euclianité)*).
2. Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, $n \in \mathbb{Z}$ (*(principalité)*).
3. $\mathbb{Z}^* = \{\pm 1\}$.
4. Les irréductibles de $\mathbb{Z}$ sont les $\pm p$, où p est un nombre premier (*(lemme d'Euclide)*).
5. Il y a existence et unicité de la décomposition en nombres premiers à signe près (*(factorialité)*).
6. On dispose du théorème de Bézout (qui découle de la principalité) et du lemme de Gauss (qui découle de la factorialité ou du théorème de Bézout).
7. On a également le théorème chinois.

Voir d'abord le chapitre Généralités sur les anneaux pour aborder cette section. Nous nous intéressons plus généralement à la généralisation de l'arithmétique de $\mathbb{Z}$, très naturelle, dans les anneaux commutatifs, à l'aide d'un formalisme épuré grâce à la notion d'idéal. On s'aperçoit que l'arithmétique des anneaux s'assimile d'autant plus à celle des entiers lorsque que l'on renforce les hypothèses sur l'anneau considéré : intégrité en premier lieu, puis factorialité, principalité, et enfin présence d'une division euclidienne. Dans cette construction, les anneaux principaux ont un rôle crucial : s'ils généralisent les anneaux euclidiens, on montre que les

anneaux principaux sont tous factoriels, c'est-à-dire qu'ils admettent un théorème fondamental de l'arithmétique ; c'est ainsi dans la structure d'anneau factoriel ou plus encore d'anneau principal que l'arithmétique devient significativement plus manipulable. Nous verrons enfin l'application de cette arithmétique dans la résolution d'équations diophantiennes cas particuliers de la grande équation de Fermat.

Nous ne nous intéressons qu'aux anneaux unitaires, de même que, très vite, nous ne nous intéressons qu'aux anneaux commutatifs. En effet, dans un pseudo-anneau, nous ne disposons pas du lemme de la deuxième partie, ni de la caractérisation de l'association dans la troisième partie.

3.3.1 Divisibilité dans un anneau : théorie générale de l'arithmétique

3.3.1.1 Division et association

Définition. ***(Divisibilité)***

Soient a,$b \in A$. On dit que a *divise* b, ou que a est un *diviseur* de b, ou que b est un *multiple* de a, si b appartient à l'idéal principal à gauche ou à droite engendré par a, c'est-à-dire, s'il existe $c \in A$ tel que $b = ac$ ou $b = ca$. On note : $a \mid b$.

Remarque. Cela correspond bien à la définition de la divisibilité dans $\mathbb{Z}$ apprise dans les petites classes. Cependant remarquons : dans un anneau quelconque, l'élément 0 est absorbant. On en déduit que tout élément divise 0, mais aussi que 0 ne divise que lui-même. Comme on s'y attend *(voir la notion d'intégrité)*, 0 peut diviser au sens de la divisibilité des éléments non nuls ; nous nous attarderons là-dessus plus tard. Notons :

Fait

Un élément $a \in A$ est un diviseur de zéro au sens algébrique si et seulement s'il est non nul et que 0_A le divise au sens arithmétique.

Remarque importante. On prendra garde au fait suivant : la notion de divisibilité est intrinsèque à l'anneau ambiant. Ainsi 2 divise 3 dans $\mathbb{Q}$, car $3 = 2.\frac{3}{2}$, mais 2 ne divise pas 3 dans $\mathbb{Z}$.

Propriété. ***(Définition équivalente de la divisibilité)***

Soient a,$b \in A$. L'élément a divise b, si et seulement si, $bA \subseteq aA$.

▷ Supposons que $bA \subseteq aA$. L'élément b est inclus dans bA, car $b = b1_A$, A étant unitaire. Donc $b \in aA$, autrement dit, b est dans l'idéal principal engendré par a, ce qui signifie exactement que a divise b. Réciproquement, si a divise b, il existe $c \in A$ tel que $b = ac$. Soit $x \in bA$: $x = bu$

pour un certain $u \in A$. Alors $x = acu$, car $b = ac$. En posant $y = cu$, $x = ay$ pour $y \in A$ stable par multiplication. Donc $x \in aA$, donc $bA \subseteq aA$. ■

Attention à ne pas inverser le sens de l'inclusion dans $bA \subseteq aA$!

On commence à remarquer que la divisibilité est une notion d'anneau, très inintéressante dans le cas des corps où l'arithmétique est toujours triviale. Nous commençons l'étude systématique de ce cas limite par la remarque fondamentale suivante :

Propriété. ***(Division dans un corps)***

Supposons $A = K$ un corps quelconque gauche. Soient a,$b \in K$. Alors a divise b dès que a est non nul.

▷ En effet, si a est non nul, a est inversible, et $a(a^{-1}b) = b$. ■

Étudions la relation de divisibilité un instant.

Propriété. ***(Préordre de divisibilité)***

La relation de divisibilité dans un anneau est réflexive et transitive.

▷ Ces deux propriétés sont héritées de l'ordre $\subseteq$ et de la propriété précédente. ■

Définition. ***(Éléments associés)***

Deux éléments a,$b \in A$ sont dits *associés* si $a \mid b$ et $b \mid a$ (autrement dit, si $aA = bA$).

Remarques.

1. Deux éléments associés ne sont pas nécessairement égaux (voir l'exemple ci-dessous).
2. Si cette propriété est vérifiée, alors la divisibilité est un ordre sur A, comme le remarque le fait ci-dessous. Ce n'est pas le cas dans $\mathbb{Z}$: deux éléments associés sont a priori seulement opposés. Si l'on se restreint à $\mathbb{N}$ (qui n'est pas un anneau !), la relation de divisibilité est donc un ordre.
3. Dans $\mathbb{K}[X]$, pour un corps $\mathbb{K}$, les éléments associés à un polynôme P sont les λP pour $\lambda \in \mathbb{K} \setminus \{0\}$. En particulier, tout polynôme non nul est associé à un unique polynôme unitaire de même degré.

On se place dès à présent dans des anneaux **commutatifs**.

Propriété. ***(Caractérisation de l'association dans les anneaux intègres)***

Deux éléments d'un anneau **intègre** sont associés s'il existe une unité $c \in A^*$ telle que $b = ac$, cette relation étant bien sûr symétrique.

▷ Soient $a,b \in A$. On a successivement :

$$\begin{aligned} aA = bA &\iff \begin{cases} aA \subseteq bA \\ bA \subseteq aA \end{cases} \\ &\iff \begin{cases} a = bc, c \in A \\ b = ac', c' \in A \end{cases} \\ &\iff \begin{cases} a = bc, c \in A \\ b = bcc', c' \in A \end{cases} \\ &\iff \begin{cases} a = bc, c \in A \\ cc' = 1, c' \in A \end{cases} \\ &\iff a = bc, c \in A^*, \end{aligned}$$

l'avant-dernière équivalence n'ayant lieu que par ce que b est régulier dans A, car A est intègre. ■

Remarque. Dans un anneau commutatif quelconque, deux éléments égaux à un inversible près sont clairement associés. En revanche, si l'anneau A n'est pas intègre, deux éléments peuvent être associés sans être égaux à un inversible près, mais il est très délicat d'exhiber un contre-exemple (il s'agit d'étudier les inversibles de l'anneau $\mathbb{Z}[X,Y,Z]/(X(1-YZ))$).

Proposition

L'association $\mathcal{A}$ est une relation d'équivalence.

Fait

Pour tout anneau unitaire A, la divisibilité est un ordre sur $A/\mathcal{A}$.

Propriété. ***(Combinaison linéaire)***

Si a divise b et c, alors pour tous m,n, a divise $bm+cn$.

▷ Par hypothèse, $ak = b$ et $aq = c$. Ainsi $akm = bm$ et $aqn = cn$, d'où $akm + aqn = a(km+qn) = bm+cn$ par distributivité, donc, comme $km+qn \in A$, a divise $bm+cn$. ■

3.3.1.2 Primalité relative et étrangeté

Définition. ***(Primalité relative)***

On dit que $a,b \in A$ sont *premiers entre eux*, ou que a est *premier à* b, si pour tout $d \in A$, on a $d \mid a$ et $d \mid b) \implies d \in A^*$.

Définition. ***(Étrangeté)***

On dit que $a,b \in A$ sont *étrangers*, s'il existe $u,v \in A$ tels que $au + bv = 1$.

Note générale

Plus généralement, on peut définir dans un anneau A les trois concepts suivants :

- deux éléments $a,b \in A$ sont *premiers entre eux* si $(a) + (b)$ n'est inclus dans aucun idéal principal propre (ou, ce qui revient au même, si $1 \in \text{pgcd}(a,b)$) ;
- deux éléments sont *indissolubles* si b est simplifiable dans $A/(a)$ (ou, ce qui revient au même, si $ab \in \text{ppcm}(a,b)$) ;
- deux éléments sont *étrangers* lorsque $(a) + (b) = A$ (ou, ce qui revient au même, si les idéaux (a) et (b) sont étrangers).

On a les implications strictes : étrangers $\implies$ indissolubles entre eux $\implies$ premiers entre eux. (Les réciproques peuvent être fausses même dans un anneau intègre.)

Propriété

Deux éléments étrangers sont premiers entre eux.

▷ Soient a,b étrangers. Il existe donc $u,v \in A$ tels que $ua + vb = 1$. Soit $d \in A$ tel que d divise a et b. Alors d divise la combinaison linéaire $ua + vb$, c'est-à-dire d divise 1. Ceci signifie exactement, dans un anneau commutatif, que d est inversible. ■

3.3.1.3 Pgcd et ppcm

Définition. ***(Plus grand commun diviseur)***

Soient $a,b \in A$. On dit que $d \in A$ est UN *plus grand diviseur commun*, ou *pgcd*, de a et b, si d divise a et b et pour tout $c \in A$, si c divise a et b, c divise d.

Définition. ***(Plus petit commun multiple)***

Soient $a,b \in A$. On dit que $m \in A$ est UN *plus grand multiple commun*, ou *ppcm*, de a et b, si a et b divisent m et pour tout $c \in A$, si a et b divisent c, m divise c.

Remarques.

1. Pgcd et ppcm n'existent pas toujours. Par exemple, si $A = \mathbb{Z}[i\sqrt{5}]$, on peut montrer que 9 et $3(2 + i\sqrt{5})$ n'ont pas de pgcd et que 3 et $2 + i\sqrt{5}$ n'ont pas de ppcm.
2. Le pgcd et le pcpm ne sont pas forcément unique : voir par exemple dans $\mathbb{R}[X]$, mais la proposition suivante permet d'y voir nettement plus clair.

3. Si $a = 0$, b est un pgcd de a et b. En particulier, $pgcd(0,0) = 0$. Si $(a,b) \neq (0,0)$, un pgcd de a et b est non nul.
4. Si $a = 0$ ou $b = 0$, 0 est un ppcm de a et b. De plus, c'est le seul. Si a et b sont non nuls, un ppcm m de a et b est non nul dès que A est intègre, puisque m divise ab, qui est non nul.

Lemme. ***(Unicités essentielles du pgcd et du ppcm)***

Deux pgcd (resp. ppcm) de deux éléments d'un anneau A, lorsqu'ils existent, sont uniques à association près.

▷ On le montre pour le pgcd, le cas du ppcm étant similaire. Supposons que d et d' soient deux pgcd de a et b. Alors, puisque d' est un pgcd de a et b et que d est un diviseur commun à a et b, on a $d \mid d'$. Symétriquement, $d \mid d'$; autrement dit, d et d' sont associés. ■

3.3.1.4 Irréductibilité, primalité

Définition. ***(Irréductible)***

Un élément $\pi \in A$ est dit *irréductible* s'il est non nul, non inversible, et si pour tous $a,b \in A$, on a $\pi = ab \implies a \in A^*$ ou $b \in A^*$.

Remarques.

1. Cela revient à dire que π est non nul, non inversible, et que ses seuls diviseurs sont les éléments $u \in A^*$ et $v\pi$, $v \in A^*$. Ceux-ci sont toujours diviseurs, puisque l'on peut écrire $a = u(u^{-1}A) = (va)v^{-1}$.
2. Si a et b sont deux éléments de A associés, alors a est irréductible dans A si et seulement si b l'est. Dans ce cas, on a nécessairement $b = ua$ avec $u \in A^*$. En effet, supposons a et b associés, soit $(a) = (b)$. Supposons également que a soit irréductible. Comme a est non nul et non inversible, (a) est non nul et distinct de A. Il en est donc de même de (b), et b est alors non nul et non inversible. Puisque $a \in (a) = (b)$, il existe $c \in A$ tel que $a = bc$. Puisque b est non inversible et a est irréductible, on a $c \in A^*$. Enfin, si π est irréductible et $u \in A^*$, alors $u\pi$ est irréductible. En effet, si $u\pi = ab$, alors $\pi = (u^{-1}A)b$. Ainsi, b est inversible ou $u^{-1}A$ est inversible, mais cette dernière condition est équivalente à ce que a soit inversible, car si $u^{-1}A = v$ inversible, $a = uv$ est inversible et si a est inversible, $u^{-1}A$ l'est comme produit d'inversibles.
   Dans $\mathbb{Z}[i\sqrt{3}]$, les éléments $1 \pm i\sqrt{3}$ sont irréductibles mais non associés (voir la suite).
3. Un anneau ne possède pas nécessairement d'éléments irréductibles. C'est le cas des corps, ou par exemple de $\mathbb{Z}/6\mathbb{Z}$. En effet, il suffit d'écrire $4 = 2 \times 2$, $2 = 2 \times 4$, et $3 = 3 \times 3$.

4. Les irréductibles de $\mathbb{Z}$ sont les $\pm p$ où p est un nombre premier. Les irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

Exemple fondamental

On considère l'anneau $A = \mathbb{Z}[i\sqrt{3}]$ des polynômes en $i\sqrt{3}$ à coefficients dans $\mathbb{Z}$. Montrons que les éléments 2 et $1 \pm i\sqrt{3}$ sont irréductibles non associés deux à deux.
Remarquons tout d'abord que si $z \in A$, il est inversible, si et seulement si $z \in \mathbb{U}$.
En effet, si $|z| = 1$, alors $|z^2| = z\overline{z} = 1$, et comme $\overline{z} \in A$, z est inversible.
Inversement, si z est inversible, il existe $z' \in A$ tel que $zz' = 1$, et donc $|z|^2|z'|^2 = 1$. Comme ces deux quantités sont des entiers positifs, on en déduit en particulier que $|z|^2 = 1$, donc $|z| = 1$.
Déterminons A^*. Par ce qui précède, $z = a + ib\sqrt{3}$ est inversible, si et seulement si, $a^2 + 3b^2 = 1$. Nécessairement, on a $b = 0$, ce qui implique $a = \pm 1$. Réciproquement 1 et -1 sont inversibles. Par conséquent, $A^* = \{\pm 1\}$.
Supposons enfin que z soit égal à 2, $1 + i\sqrt{3}$ ou $1 - i\sqrt{3}$.
Alors on a dans les trois cas $|z|^2 = 4$, donc z est non nul et non inversible par le point précédent. De plus, si $z = z_1z_2$, z_1,$z_2 \in A$, alors $|z_1|$ divise 4. On a donc $|z_1| = 1, 2$ ou 4. Dans le premier cas, $z_1 \in A^*$ et dans le dernier, $z_2 \in A^*$.
Supposons que $|z_1| = 2$. C'est impossible : si $z_1 = a + bi\sqrt{3}$, $a^2 + 3b^2 = 2$ d'où $b = 0$ puis $a^2 = 2$. Ainsi, ces trois éléments sont irréductibles.
Il est immédiat qu'ils sont associés puisque les inversibles de A sont ± 1.

Propriété

Deux irréductibles non associés sont premiers entre eux.

▷ Soient π, π' deux éléments irréductibles de A. Soient $d \in A$ tel que $d \mid \pi$ et $d \mid \pi'$. Il existe donc des éléments b,b' tels que $db = \pi$ et $db' = \pi'$. Puisque π est irréductible, d est inversible ou b est inversible. Supposons que b soit inversible. Alors $d = b^{-1}\pi$ et $\pi' = (b^{-1}b)'\pi$. Comme π est irréductible, π est non inversible par définition. Mais, π' étant un élément irréductible, on en déduit que l'on a $u = b^{-1}b' \in A^*$. En particulier, π et π' sont associés, ce qui est contredit l'hypothèse. Ainsi, $d \in A^*$, ce que l'on voulait vérifier. ■

Remarque. D'après l'exemple fondamental, cette propriété ne suffit pas à garantir l'unicité de la décomposition.

On dispose du lemme suivant donnant une condition suffisante pour qu'un élément d'un anneau intègre soit irréductible.

Lemme

Soient A un anneau, $\pi \in A$.

1. L'idéal (π) est premier non nul si et seulement si π est non nul, non inversible et vérifie le lemme d'Euclide : pour tous a,$b \in A$, π divise ab si et seulement si π divise a ou π divise b.
2. Si A est intègre, et si π vérifie l'une des deux conditions équivalentes précédentes, alors π est irréductible.

▷ Successivement :

1. Supposons que $(\pi) = \pi A = A\pi$ soit premier non nul. Alors π est non nul, car πA ne l'est pas, et non inversible, car sinon, $\pi A = A$ et $A/(\pi)$ est non trivial, car il est intègre, car (π) est premier. Soient a,$b \in A$ tels que π divise ab. Par définition, $ab \in (\pi)$. Puisque (π) est un idéal premier, on a $a \in (\pi)$ ou $b \in (pi)$ ce qui signifie que π divise a ou π divise b. Inversement, si π est non nul, non inversible et vérifie le lemme d'Euclide, on a en particulier $(\pi) \neq \{0\}$ et $(\pi) \neq A$ pour les mêmes arguments que précédemment. Si maintenant a,$b \in A$ vérifient $ab \in (\pi)$, alors π divise ab, donc π divise a ou π divise b, soit $a \in (\pi)$ ou $b \in (\pi)$. Ainsi (π) est premier non nul.
2. On suppose de plus A intègre. Supposons par exemple que π vérifie la deuxième condition. Montrons qu'il est irréductible. Par hypothèse, il est non nul et non inversible. Soient a,$b \in A$ tels que $\pi = ab$. En particulier, π divise ab et donc π divise a ou π divise b. Supposons par exemple que π divise a. Alors il existe $u \in A$ tel que $a = u\pi$, et donc $\pi = u\pi b$. Comme A est intègre et $\pi \neq 0$, on obtient $1 = ub$. Par conséquent, $b \in A^*$, donc π est irréductible. ■

Définition. ***(Élément premier)***

Un élément $\pi \in A$ est dit *premier* si l'idéal (π) est premier non nul.

Remarques.

1. Tout nombre premier p est un élément premier de $\mathbb{Z}$.
2. De manière évidente, si a et b sont associés, alors a est premier si et seulement si b l'est.
3. En particulier, si π est premier et $u \in A^*$, alors $u\pi$ est premier.
4. *(Remarque)* Si A est intègre, tout élément premier est irréductible d'après ce qui précède. Ce n'est plus vrai si A n'est pas intègre. De plus, un élément irréductible n'est pas nécessairement premier : c'est le cas de 2 dans $\mathbb{Z}[i\sqrt{3}]$.

On donne deux propriétés intéressantes par anticipation. Celles-ci sont immédiatement données par le théorème de Krull et le fait que dans un anneau intègre, tout élément premier est maximal.

Corollaire

Tout anneau principal non nul et qui n'est pas un corps admet des éléments premiers.

Corollaire corollaire

Tout anneau principal non nul et qui n'est pas un corps admet des éléments irréductibles.

On aurait pu le déduire de la proposition suivante, mais ç'aurait été tricher.

Corollaire

Tout anneau factoriel (en fait, *atomique* suffit) non nul et qui n'est pas un corps admet des éléments premiers.

Corollaire corollaire

Tout anneau factoriel (en fait, atomique suffit) non nul et qui n'est pas un corps admet des éléments irréductibles.

3.3.1.5 Factorisation dans un anneau

On peut se poser la question suivante : tout élément non nul d'un anneau peut-il se décomposer en produit d'un élément inversible et d'éléments irréductibles ? Si oui, la décomposition est-elle unique à permutation et association près des facteurs ?

On a déjà les réponses négatives suivantes :

- En toute généralité, l'existence d'une telle décomposition est infirmée. On peut exhiber des exemples d'anneaux pour lesquels certains éléments n'ont pas de décomposition.
- Pire, il existe des anneaux qui ne sont pas des corps et qui ne possèdent aucun élément irréductible. C'est le cas de $\mathbb{Z}/6\mathbb{Z}$, ce coquin. Si l'on veut un anneau intègre, il faut travailler un peu plus : l'ensemble des entiers algébriques $\overline{Z}$ convient.
- Dans un anneau où l'existence de la décomposition est assurée, l'unicité ne l'est pas forcément. Il suffit de reprendre l'exemple fondamental de $\mathbb{Z}[i\sqrt{3}]$ développé précédemment et d'observer que $4 = 2^2 = (1 + i\sqrt{3})(1 - i\sqrt{3})$.

Les choses se passent déjà mieux en termes d'unicité lorsqu'on se place dans un anneau intègre et si les éléments intervenant dans la décomposition sont premiers.

Lemme

Soient A un anneau simplifiable. On suppose que l'on a un égalité $up_1...p_r = u'\pi_1...\pi_s$ où r,s sont deux entiers naturels, u,u' inversibles, p_1,...,p_r premiers et π_1,...,π_s irréductibles. Alors $r = s$ et il existe une permutation $\sigma \in \mathfrak{S}_r$ telle que $p_i = \pi_{\sigma(i)}$ soient associés pour tout $i \in [\![1,r]\!]$. Puisque associés à des éléments premiers, les π_1,...,π_s sont en fait premiers.

▷ On raisonne par récurrence sur r. Traitons d'abord le cas $r = 0$. On a donc $u = u'\pi_1...\pi_s$, soit $u^{-1}u'\pi_1...\pi_s = 1$. Si $s \geqslant 1$, π_1 est inversible ce qui est absurde, car il est irréductible. Ainsi $s = 0$ et la propriété d'association est trivialement vérifiée. Supposons maintenant que ce fait soit vrai pour un entier $r \geqslant 0$ quelconque, et montrons qu'il l'est également au rang $r + 1$. Considérons une égalité du type $up_1...p_{r+1} = u'\pi_1...\pi_s$. Puisque p_1 est premier et que p_1 divise $u'\pi_1...\pi_s$, p_1 divise u' ou p_1 divise l'un des π_j. Mais le premier cas ne peut se produire, car p_1 est premier, donc non inversible, donc il ne peut diviser u', auquel cas il diviserait 1 et serait donc inversible. Ainsi, quitte à changer la numérotation, on peut supposer que p_1 divise π_1. On a donc $\pi_1 = vp_1$ où $v \in A$. Puisque π_1 est irréductible, $p_1 \in A^*$ ou $v \in A^*$. Mais p_1 étant premier, il est non inversible donc $v \in A^*$. ■

Pour parler de factorisation plus généralement, on introduit les définitions suivantes :

Définition. ***(Décomposition en facteurs irréductibles)***

Soit A un anneau. Un élément a est dit *décomposable (en facteurs irréductibles)* si $a = u\pi_1...\pi_r$, où $\pi_1,...,\pi_r$ sont irréductibles dans A et $u \in A^*$.

Définition. ***(Unicité de la décomposition)***

La décomposition précédente est dite *essentiellement unique* ou *unique à association et permutation près des facteurs* si si $(m,n) \in \mathbb{N}^2$, $p_1,...p_m,q_1,...,q_n$ des éléments irréductibles, si $\prod_{i=1}^{m} p_i \sim \prod_{j=1}^{n} q_j$ (pour la relation d'association) alors $n = m$ et quitte à réindexer $p_i \sim q_i$, c'est-à-dire s'il existe $s \in \mathfrak{S}_n$ tel que $p_i = q_{s(i)}$ pour tout $i \in [\![1,n]\!]$.

De même :

Définition. ***(Décomposition en facteurs premiers)***

Soit A un anneau. Un élément a est dit *décomposable en facteurs premiers* si $a = u\pi_1...\pi_r$, où $\pi_1,...,\pi_r$ sont premiers dans A et $u \in A^*$.

Remarque. On n'a aucun mal à définir de même l'unicité de la décomposition en facteurs premiers.

On a évidemment :

Propriété. ***(Décomposable en premiers donc en irréductibles)***

Soit A un anneau intègre. Si $x \in A$ est décomposable en produit de facteurs premiers, il est décomposable en produit de facteurs irréductibles.

VOC Soit $\mathrm{Irr} = P$ un ensemble de représentants irréductibles de A, c'est-à-dire pour la relation $\sim$. Si $x \in A$ est décomposable, alors :

$$x \sim \prod_{p \in \mathrm{Irr}} p^{n_p}$$

où la famille $(n_p) \in \mathbb{N}^{\mathrm{Irr}}$ est presque nulle. On appellera plus tard $n_p = \nu_p(x)$ la *p-valuation* de x.

Exercice 94

Donner un exemple d'anneau avec une infinité indénombrable d'éléments irréductibles.

▷ **Éléments de réponse.**

Considérer $\mathbb{Z}^{\mathbb{R}}$ muni de la loi produit. Pour un anneau intègre, il faut travailler un peu plus.

On a les propriétés premières suivantes :

Proposition. ***(Non-décomposabilité de*** 0***)***

On suppose A intègre. L'élément nul de A n'est jamais décomposable.

Heuristique

Et il n'est pas non plus décomposable ! Autrement dit, pour faire sérieusement de l'arithmétique, il ne faut pas prendre zéro en compte.

▷ Un irréductible n'est jamais diviseur de zéro... dans un anneau intègre. ■

Si l'on ne suppose pas l'anneau intègre, le début de l'exercice précédent donne un contre-exemple plutôt intéressant.

Proposition. ***(Décomposabilité des inversibles)***

Tous les éléments de $A^\times$ sont décomposables.

▷ Il suffit de prendre aucun irréductible dans le produit et pour inversible d'association, l'inversible considéré. ■

Pour conclure, on peut définir le concept suivant permettant de formaliser autrement la réelle unicité de la décomposition.

Définition. ***(Système complet de représentants irréductibles)***

Soit A un anneau. Un *système complet de représentants irréductibles* est un sous-ensemble P de A composé d'irréductibles tel que tout irréductible de A soit associé à exactement un élément de P.

Proposition

Tout anneau ayant au moins un irréductible possède au moins un système complet de représentants irréductibles non vide.

▷ Il suffit de prendre le sous-système d'éléments irréductibles d'un système de représentant de la relation d'équivalence d'association, qui existe toujours d'après l'axiome du choix. ■

Il faut faire très, très attention au vocabulaire qui en arithmétique se chevauche ici très vite. On dit souvent qu'un élément a de l'anneau A est décomposable s'il n'est pas irréductible : c'est le terme contraire. Ceci ne doit pas être confondu avec la notion de *décomposable en produit de facteurs irréductibles* : un irréductible est toujours décomposable en ce sens, ayant un seul facteur : lui-même. On peut même envisager, réciproquement, un élément décomposable non décomposable en produit de facteurs irréductibles (le construire).

On encourage le lecteur à donner un coup d'œil sur la section Anneaux factoriels, qui se rapporte directement à cette section et définit une propriété très attendue sur les anneaux, la factorisation étant le nec plus ultra sur un ensemble où l'on a toujours défini la somme de la bonne façon (un anneau est un groupe additif abélien) et le problème se rapporte toujours aux produits.

3.3.2 Anneau euclidien

Définition. ***(Anneau euclidien)***

Un anneau A est dit *euclidien* s'il est intègre et s'il existe une application appelée *stathme euclidien* $\delta : A \setminus \{0\} \longrightarrow \mathbb{N}$ telle que pour tout $a \in A$ et pour tout $b \in A \setminus \{0\}$, il existe $q,r \in A$ tels que $a = bq + r$, et $r = 0$ ou $\delta(r) < \delta(b)$.

Remarque. On ne demande pas l'unicité de q ni de r.

3.3.3 Anneau principal

Les développements précédents ont montré que les propriétés arithmétiques de $\mathbb{Z}$ ne sont plus vraies en général dans un anneau quelconque, même intègre. Nous allons maintenant vérifier que dans les anneaux principaux en général, tout se passe pour le mieux, excepté la division euclidienne.

3.3.3.1 Définition

Définition. ***(Anneau principal)***

Un anneau est dit *principal* s'il est intègre et si tout idéal de A est principal.

Théorème

L'anneau $\mathbb{Z}$ est principal.

▷ Tout l'intérêt de la preuve réside dans ce que les sous-groupes additifs de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$ pour un certain $n \in \mathbb{Z}$. Rappelons pourquoi. Soit H un sous-groupe de $\mathbb{Z}$. S'il est trivial, c'est terminé : il est engendré par 0. Sinon, H contient n non nul. Si n est négatif, $-n \in H$ est positif ; quitte à permuter l'un en l'autre, on prend $n \in \mathbb{N}^*$. Ainsi $H \cap \mathbb{N}^*$ est non vide. C'est une partie de $\mathbb{N}$, par propriété fondamentale, elle admet un plus petit élément que nous notons encore n. Montrons que $H = n\mathbb{Z}$. La stabilité additive de H donne que, puisque $n \in H$, $n\mathbb{Z}$ les itérés de n sont aussi dans H. Réciproquement, si $a \in H$, on effectue la division euclidienne de a par n : $a = nq + r$ où $0 \leqslant r < n$. Or si r est non nul, $r = a - nq \in H$ par stabilité additive et $r < n$ ce qui contredit la minimalité de n, donc $r = 0$. Ainsi $a = nq$, donc $a \in n\mathbb{Z}$. Enfin, il est immédiat que les $n\mathbb{Z}$ sont tous des idéaux de $\mathbb{Z}$, et l'on sait aussi que $\mathbb{Z}$ est intègre. ■

Remarque importante. On montre de même, en faisant intervenir le degré, que pour tout corps $\mathbb{K}$, l'anneau des polynômes $\mathbb{K}[X]$ est principal. En effet, si $\mathbb{K}$ est un corps, c'est un anneau intègre donc $\mathbb{K}[X]$ est intègre. Il est pertinent de souligner le rôle de la division euclidienne dans les deux démonstrations précédentes : plus généralement, on verra que tout anneau euclidien est en particulier principal.

3.3.3.2 Arithmétique dans les anneaux principaux

La principalité est riche de conséquences arithmétiques.

3.3.3.2.1 Conséquences sur la divisibilité

Propriété. ***(Pgcd, ppcm dans un anneau principal)***

Soit A un anneau principal. Soient a,$b \in A$ et $d \in A$ tels que $(a) + (b) = (d)$. Alors d est un pgcd de a et b. Soit $m \in A$ tel que $(a) \cap (b) = (m)$. Alors m est un ppcm de a et b.

▷ D'une part, $a \in (a) + (b)$ donc $a \in (d)$, soit $a = ud$, $u \in A$, donc d divise a. De même d divise b. D'autre part, $d \in (d)$, car A est unitaire. Ainsi $d = au + bv$. Ainsi, si u divise a et b, u divise $au + bv = d$, ce qui montre que d est un *pgcd* de (a,b). La preuve est similaire pour le ppcm. ■

Corollaire. ***(Existences du pgcd et du ppcm)***

Dans un anneau principal, tout couple d'élément admet un pgcd et un ppcm.

▷ Les parties $(a)+(b), (a)\cap(b)$ sont des idéaux de A, ils sont donc principaux. Il suffit donc, d'après la proposition précédente, de considérer au moins un générateur. ■

Dans un anneau principal, on dispose du grand théorème de Bézout.

Théorème. ***(Théorème de Bézout)***

Soit A un anneau principal. Deux éléments sont étrangers si et seulement s'ils sont premiers entre eux.

▷ On sait que deux éléments étrangers sont premiers entre eux. Réciproquement, si 1 est un pgcd de a et b, alors $(a)+(b)=1A=A$ donc a et b sont étrangers. ■

Il faut remarquer que dans les anneaux que nous allons étudier en premier lieu (euclidiens, principaux, factoriels, noethériens), les anneaux principaux sont les plus larges dans lequel le théorème de Bézout a lieu.

Le théorème de Bézout entraîne de façon très simple le lemme de Gauss. Il faut cependant dès maintenant dire que, dans des anneaux plus larges que les anneaux principaux, il est encore vérifié.

Théorème. ***(Lemme de Gauss)***

Soient a,$b\in A$ deux éléments premiers entre eux d'un anneau principal. Alors pour tout $c\in A$, si a divise bc, alors a divise c.

▷ Soient a,$b\in A$ principal, premiers entre eux, donc étrangers : $au+bv=1$. Soit $c\in A$. Alors $acu+bcv=c$. Or a divise bc, donc a divise bcv. De plus a divise acu, donc a divise $acu+bcv=c$, ce qu'il fallait montrer. ■

Théorème. ***(Théorème chinois)***

Soient a_1,...,$a_n\in A$ principal deux à deux premiers entre eux. Alors les anneaux $A/(a_1...a_n)$ et $A/(a_1)\times...\times A/(a_n)$ sont isomorphes.

▷ Il suffit d'observer que le morphisme

$$\begin{array}{rccc} f: & A & \longrightarrow & A/(a_1)\times...\times A/(a_n) \\ & x & \longmapsto & ([x]_1,...,[x]_n) \end{array}$$

est surjectif, de noyau $(a_1...a_n)$. ■

3.3.3.2.2 Conséquences sur l'irréductibilité

Nous allons maintenant nous intéresser de plus près aux éléments irréductibles. Les deux lemmes suivants sont fondamentaux.

Lemme

Soit A un anneau commutatif unitaire et π un élément irréductible. Alors (π) est maximal parmi les idéaux propres principaux de A.

▷ Soit $\pi \in A$ un élément irréductible. Soit $a \in A \setminus A^*$, ce qui revient à prendre le générateur d'un idéal propre de A. On suppose que $(\pi) \subseteq (a)$. Il existe donc b tel que $\pi = ab$ d'après la définition de la divisibilité. Puisque π est irréductible, comme a n'est pas inversible, $b \in A^*$. Mais alors $(\pi) = (a)$, ce qui démontre la maximalité de (π). ■

Lemme. *(Lemme fondamental de l'arithmétique principale)*

Soit A un anneau principal. Tout irréductible de A engendre un idéal maximal.

▷ Soit $\pi \in A$ un élément irréductible, en supposant A principal. Comme π est non inversible, (π) est propre. En particulier, il existe un idéal maximal $\mathfrak{m}$ contenant (π) d'après le théorème de Krull. Soit $a \in A$ un générateur de $\mathfrak{m}$, qui existe par principalité de A. On a donc $(\pi) \subseteq (a)$, d'où $(\pi) = (a)$ par le point précédent, soit encore $(\pi) = \mathfrak{m}$. Ainsi, $\mathfrak{m}$ est maximal. ■

On en déduit les propriétés suivantes :

Propriété. *(Lemme d'Euclide)*

Dans un anneau principal, un élément est irréductible si et seulement s'il est premier.

▷ L'anneau principal A est intègre, donc tout élément premier est irréductible. Réciproquement, si π est irréductible, (π) est maximal, donc premier, et non nul, car π est non nul. Par définition, π est donc premier. ■

Corollaire

Dans un anneau principal, tout idéal premier non nul est maximal.

▷ Soit $\mathfrak{p}$ un idéal premier non nul. Soit π un générateur de $\mathfrak{p}$. Alors π est irréductible en particulier. D'après le premier lemme, $\mathfrak{p} = (\pi)$ est maximal. ■

Corollaire

Dans un anneau principal, un idéal non nul est premier si et seulement s'il est maximal.

Corollaire

Soit A un anneau principal et π un élément non nul. Les propositions suivantes sont équivalentes :

(i) $A/(\pi)$ est un corps ;
(ii) $A/(\pi)$ est un anneau intègre ;
(iii) π est irréductible ;
(iv) π est premier.

3.3.3.2.3 Conséquences sur la factorisation

Lemme

Soit A un anneau principal. Alors tout élément non nul et non inversible possède un diviseur irréductible.

▷ Soit $a \in A$ un élément non nul et non inversible. Puisque a est non inversible, $(a) \neq A$. L'idéal (a), propre, est donc contenu dans un idéal maximal $\mathfrak{m}$ par le théorème de Krull. En particulier, $\mathfrak{m}$ est un idéal premier, non nul (sinon a serait nul). Posons $\mathfrak{m} = (\pi)$. L'élément π est premier, donc irréductible puisqu'un anneau principal est intègre. Mais alors comme $(a) \subseteq (\pi)$, on obtient π qui divise a, et π est un diviseur irréductible de A. ■

On anticipe sur la section suivante pour énoncer le théorème fondamental. On a :

Théorème. *(Principal implique factoriel)*

Tout anneau principal est factoriel.

▷ Soit A un anneau principal et $a \in A$, $a \neq 0$. Commençons par montrer l'existence d'une décomposition de la forme voulue. Si $a \in A^*$, c'est clair. On suppose donc que A n'est pas un corps, et que a est non nul et non inversible. D'après le lemme précédent, a possède donc au moins un diviseur irréductible $\pi_1 \in A$. On écrit $a = \pi_1 a_1$. Si a_1 est inversible, c'est terminé. Sinon, a_1 divise a, donc $(a) \subseteq (a_1)$ et de plus, si $(a) = (a_1)$, on aurait $a = ua_1$ avec $u \in A^*$, car A est intègre. Mais alors $a = \pi_1 a_1 = ua_1$. Comme $a_1 \neq 0$, car $a \neq 0$, on a, par intégrité, $\pi = u \in A^*$, ce qui est absurde. Ainsi $(a) \subsetneq (a_1)$.

Puisque a_1 est non nul et non inversible, par le lemme, il possède un diviseur irréductible π_2. On écrit $a_1 = \pi_2 a_2$; si a_2 est inversible, on s'arrête. Sinon, comme précédemment, $(a_1) \subsetneq (a_2)$. Supposons que l'élément a_n construit à l'étape n ne soit jamais inversible. Par récurrence, on a alors construit une chaîne infinie d'idéaux $(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \ldots \subsetneq (a_n) \subsetneq \ldots$, où $a_n \in A \setminus A^*$ pour tout $n \geqslant 1$.

Posons $a_0 = a$ et soit $\mathfrak{a} = \bigcup_{n \in \mathbb{N}} (a_n)$. On vérifie aisément que $\mathfrak{a}$ est, dans ce cas, un idéal de A. Puisque A est principal, $\mathfrak{a} = (x)$. En particulier, il existe un certain entier naturel j tel que $x \in (a_j)$. On a alors $(x) \subseteq (a_j) \subseteq \mathfrak{a} = (x)$, d'où $(x) = (a_j)$. Mais ceci est contradictoire, car $(x) = (a_j) \subsetneq (a_{j+1}) \subseteq x$, et donc $(x) \subsetneq (x)$.

Ainsi, il existe $n \geqslant 1$ tel que $a_{n+1} \in A^*$. En posant $u = a_{n+1}$, on obtient $a = u\pi_1...\pi_n$, ce qui est la décomposition cherchée.

L'unicité de la décomposition découle du lemme correspondant sur les anneaux simplifiables, puisqu'en vertu du lemme de la section précédente, tout élément irréductible est ici premier. ■

3.3.3.3 Principalité des anneaux euclidiens

On termine cet exposé de la notion d'anneau principal sur un théorème permettant de vérifier aisément qu'un anneau est principal. En effet, dans les cas complexes, il est souvent plus facile d'exhiber une division euclidienne sur un anneau que de vérifier que tous les idéaux de l'anneau sont engendrés chacun par un seul élément.

Théorème. ***(Euclidien implique principal)***

Tout anneau euclidien est principal.

▷ Supposons (A, δ) euclidien. Alors A est intègre par définition. Soit I un idéal de A. Si I est nul, il n'y a rien à faire. On peut donc supposer qu'il ne l'est pas. On considère l'ensemble $E = \{\delta(a), a \in I \setminus \{0\}\}$. L'ensemble E est une partie non vide de $\mathbb{N}$, par propriété fondamentale, elle admet donc un plus petit élément que nous notons $a_0 \in I \setminus \{0\}$. On va donc montrer que $I = (a_0)$. Puisque I est un idéal de A contenant a_0, on a $(a_0) \subseteq I$. Réciproquement, soit $a \in I$. On écrit $a = qa_0 + r$ avec $r = 0$ ou $\delta(r) < \delta(a_0)$. Puisque a et a_0 sont des éléments de I, $r = a - qa_0 \in I$ puisqu'un idéal est en particulier un sous-groupe. Si r était non ul, on aurait alors $r \in I \setminus \{0\}$ et $\delta(r) < \delta(a_0)$, ce qui contredirait le choix de a_0. Par conséquent, $r = 0$ et $a = qa_0 \in I$. Par double inclusion, $I = (a_0)$, ce qui conclut la preuve. ■

3.3.4 Anneau factoriel

Définition. ***(Anneau factoriel)***

Un anneau A est dit *factoriel* s'il est intègre et tout élément non nul est décomposable.

Autre définition. ***(Anneau factoriel)***

Un anneau A est dit *factoriel* s'il est intègre et s'il vérifie les deux conditions suivantes :

F1. tout élément non nul est associé à un produit fini d'irréductibles (on dira *décomposable*) ;

F2. si $(m,n) \in \mathbb{N}^2$, $p_1,...p_m,q_1,...,q_n$ des éléments irréductibles, si $\prod_{i=1}^{m} p_i \sim \prod_{j=1}^{n} q_j$ (pour la relation d'association) alors $n = m$ et quitte à réindexer $p_i \sim q_i$.

Reformulation pratique

Soit A un anneau principal, P un système complet de représentants irréductibles. La propriété précédente dit que tout élément non nul de A s'écrit sous la forme $a = u \prod_{\pi \in P} \pi^{n_\pi}$ où u est inversible et les (n_π) sont des entiers naturels presque tous nuls. Cette décomposition est unique au sens des π et (n_π).

En théorie, on utilisera également la caractérisation suivante de la factorialité des anneaux :

Théorème. ***(Caractérisation quasi-noethérienne des anneaux factoriels)***

Un anneau A est dit *factoriel* s'il est intègre et s'il vérifie les deux conditions suivantes :

F1. toute suite croissante d'idéaux principaux est stationnaire ;

F2. pour tout irréductible f, l'idéal (f) est premier.

▷ On montre que les axiomes notés $'$ impliquent ceux de la première formulation. Montrons que **F'1** implique**F1**. Soit $f \in A \setminus \{0\}$. Montrons que l'existence d'un non-décomposable contredirait F'1. Si f n'est pas décomposable, alors f peut s'écrire sous la forme $f = gh$ avec g non décomposable et h non inversible. En effet, f n'est ni irréductible, ni inversible ; il est donc le produit de deux éléments (car il admet au moins un diviseur) tous deux non inversibles, qui ne peuvent être tous deux décomposables sinon f le serait.) Ainsi $(f) \subsetneq (g)$ et l'on construit ainsi grâce à l'axiome du choix dépendant une chaîne d'idéaux principaux non stationnaire.

Montrons maintenant que **F'2** implique **F2**. ■

Corollaire

Si un anneau noethérien intègre est tel que tout irréductible engendre un idéal premier, alors A est factoriel.

▷ L'unicité de la décomposition est claire. Pour l'existence, si a_1 n'est pas irréductible ni inversible, $a_1 = a_2 b_1$ où a_2 est non inversible, non irréductible. Ainsi a_2 se décompose de même, etc., d'où une suite (a_i) croissante d'idéaux qui contredit la noethérianité. ■

3.3.4.1 Valuations π-adique dans un anneau factoriel

On notera que la notion de valuation est définissable dans tout anneau mais qu'alors c'est une fonction multivaluée, ce qui n'est digne d'aucun intérêt.

Théorème. ***(Nombre de diviseurs dans un anneau factoriel)***

Soit A un anneau factoriel et Irr une famille de représentants irréductibles. Soit x un élément non nul de A. Alors le nombre de diviseurs de x est $\prod_{p \in \mathrm{Irr}} (\nu_p(x) + 1)$.

En particulier, tout élément d'un anneau factoriel n'admet qu'un nombre fini de diviseurs à association près.

Exercice 95

Produire un contre-exemple dans le cas général d'un anneau intègre qui n'est pas un corps.

▷ **Éléments de réponse.**

On considère à nouveau l'ensemble des entiers algébriques sur $\mathbb{Q}$. On sait que $2 \in \overline{\mathbb{Z}}$, puisque $X - 2$ admet 2 comme racine. De plus, si a est un entier algébrique, sa racine carré l'est également. Puisque la suite $a_0 = 2$ et $a_{n+1} = \sqrt{a_n}$ est injective, 2 a une infinité de diviseurs deux à deux non associés, car tous positifs.

On peut étendre la valuation p-adique au corps des fractions d'un anneau factoriel.

3.3.5 Anneau noethérien

Définition. ***(Anneau noethérien)***

Soit A un anneau commutatif. On dit que A est *noethérien* s'il est intègre et si toute suite croissante d'idéaux de A est stationnaire.

Reformulation pratique. ***(Anneaux noethériens)***

Un anneau intègre est noethérien si et seulement si l'ensemble de ses idéaux est bien ordonné pour l'inclusion.

Théorème. ***(Caractérisation des anneaux noethériens)***

Un anneau intègre est noethérien si et seulement si il est typé-principal, c'est-à-dire, si tout idéal est de type fini (*i.e.* engendré par un nombre fini d'éléments).

▷ Soit I un idéal qui n'est pas de type fini. On a donc une suite $(x_n)_{n\in\mathbb{N}}$ d'éléments de I tels que $x_{n+1} \notin (x_1,...,x_n)$ en vertu de l'axiome du choix dépendant. On pose pour tout entier naturel n : $I_n = (x_1,...,x_n)$. Alors (I_n) est une suite croissante d'idéaux non stationnaire par construction. Réciproquement, si I_n est une suite croissante d'idéaux, alors la réunion de cette famille est un idéal par un lemme déjà rencontré. ■

Remarque. On aurait pu changer le théorème et la définition sans conséquence, mais, en pratique, aucune des deux définitions n'est meilleure que l'autre. À la limite, on préférera en pratique la condition de typage fini, mais pour nier la noethérianité, par exemple, il sera bien plus facile de manipuler la première définition.

Fait. ***(Principal implique factoriel)***

Tout anneau principal est factoriel.

▷ Un idéal monogène, c'est-à-dire engendré par un élément est engendré par un nombre fini d'éléments ! ■

La réciproque est fausse. De plus, il est facile de trouver un anneau non noethérien.

Contre-exemple. ***(Anneau non noethérien)***

L'anneau $\mathbb{Q}[X_i, i \in \mathbb{N}]$ n'est pas noethérien. Il suffit de considérer $(X_i)_{i\in I}$. □

Contre-exemple. ***(Anneau noethérien non principal)***

L'anneau $\mathbb{Q}[X,Y]$ est noethérien mais non principal. □

Contre-exemple. ***(Anneau noethérien non factoriel)***

L'anneau $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel, car comme on l'a éprouvé, il n'y a pas unicité de la décomposition. Il est noethérien comme quotient d'un anneau noethérien. □

Exercice 96

Donner un exemple d'anneau noethérien à gauche mais pas à droite.

▷ **Éléments de réponse.**
On prend $\begin{pmatrix} \mathbb{Z} & 0 \\ \mathbb{Q} & \mathbb{Q} \end{pmatrix}$.

L'étude des anneaux noethériens se prolonge bien plus naturellement dans le cadre de la théorie des modules, et l'on renvoie à cette section.

Lemme. ***(Idéaux contenant des produits de premiers)***

Soit A un anneau quasi-noethérien. Alors tout idéal de A contient un produit d'idéaux premiers. Si de plus A est intègre, alors tout idéal non nul de A contient un produit d'idéaux premiers non nuls.

▷ On prouve la première proposition, la deuxième étant semblable. On raisonne par l'absurde. Soit Φ l'ensemble des idéaux non nuls de A qui ne contiennent aucun produit d'idéaux non nuls. Comme A est noethérien, soit I maximal dans Φ. Par hypothèse, I n'est pas premier. Soient $x,y \in A \setminus I$ tels que $xy \in I$. Alors $I \subsetneq I + (x) \notin \Phi$, donc il existe des idéaux p_i premiers tels que $p_1...p_r \subseteq I + (x)$. De même, $q_1...q_m \subseteq I + (y)$. Alors $p_1...p_r q_1...q_m \subseteq (I + (x))(I + (y)) \subseteq I + (xy) \subseteq I$, donc $I \notin \Phi$ (respectivement, et si I est intègre, $p_1...q_m$ est non nul), contradiction. ■

3.3.6 Résumé des notions arithmétiques sur les anneaux

Un dessin vaut mieux qu'un long discours :

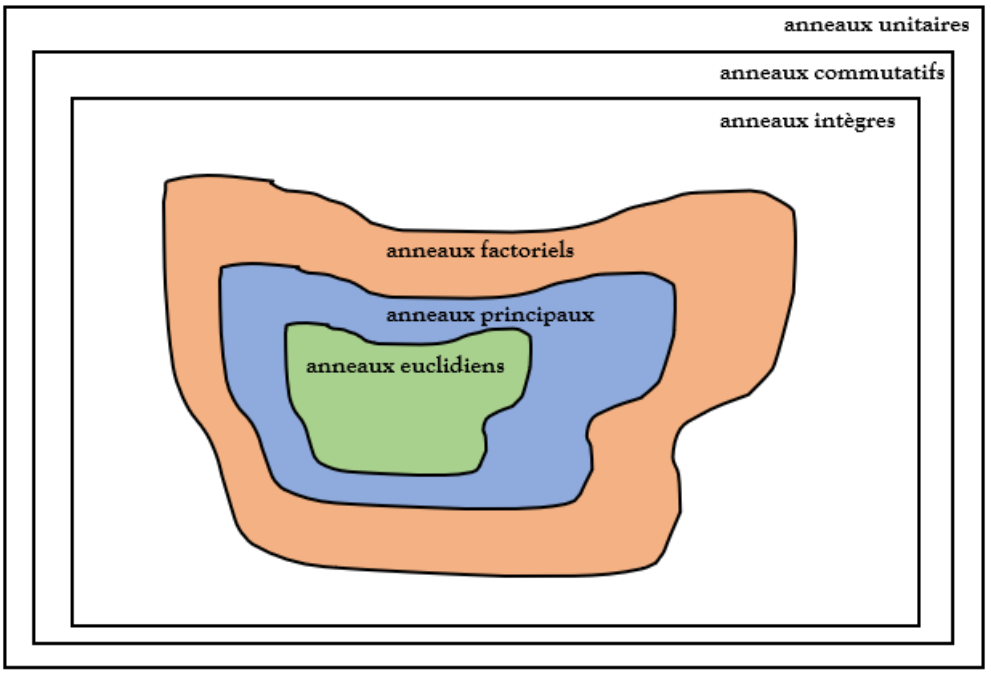


FIGURE 3.3.1 : *Structures particulières d'anneaux.* —
Les anneaux euclidiens forment la classe d'anneaux la plus restrictive que nous avons étudiée dans ce document. Parmi tous, les anneaux intègres constituent la classe ne possédant aucune propriété intéressante du point de vue de l'arithmétique. Travail personnel.

Toutes les implications rencontrées jusqu'alors peuvent être résumées de la façon suivante. Soit A un anneau intègre.

Formule. ***(Implications relatives entre anneaux arithmétiques, v. 1)***

$$A \text{ euclidien} \implies \text{principal} \implies \text{factoriel.}$$

Formule. ***(Implications relatives entre anneaux arithmétiques, v. 2)***

$$A \text{ euclidien} \implies \text{principal} \implies \text{noethérien.}$$

3.3.7 Utilisation de la factorialité de $\mathbb{Z}$ pour la résolution d'équations diophantiennes

La première propriété énonce de façon complète les solutions de l'équation des triplets pythagoriciens.

Proposition

Si $x^2+y^2=z^2$, x,y,z des entiers supérieurs à 1, il existe un entier d et des entiers premiers entre eux u,v tels qu'à permutation près de x et y, on ait $x=d(u^2-v^2)$ et $y=2duv$.

Réciproquement, en posant $z = d(u^2 + v^2)$, ces entiers donnent des solutions de l'équation de Pythagore.

En utilisant ce résultat, on obtient le lemme suivant :

Lemme

L'équation $x^4 + y^4 = z^2$ n'a pas de solutions dans $\mathbb{N}^{*3}$.

d'où l'on déduit immédiatement le cas particulier du théorème de Fermat dans le cas $n = 4$:

Théorème

L'équation $x^4 + y^4 = z^4$ n'a pas de solutions dans $\mathbb{N}^{*3}$.

Chapitre 4

Théorie des corps

Résumé

Principalement, la théorie de la correspondance de Galois (dans le cas fini), après quelques mots à mon sens très importants sur les extensions de corps (la remarque fondamentale étant que toute extension de corps est un espace vectoriel, et les degrés = dimensions des tours d'extension finies = de dimension finie se calculent multiplicativement (théorème de la base télescopique).

4.1 Théorie des corps

4.1.1 Corps engendré par

4.1.2 Sous-corps premier

Curiosité

Le corps $\mathbb{C}(X)$ contient une infinité de copies de $\mathbb{C}$.

4.1.3 Construction des corps finis, corps de Galois

Cette théorie est tout à fait constructive.

Exercice 97

On sait par la théorie des corps qu'il existe un unique corps $\mathbb{F}_{p^2}$ à p^2 élément pour tout premier p. A-t-on $\mathbb{F}_{p^2} \simeq \mathbb{Z}/p^2\mathbb{Z}$?

▷ **Éléments de réponse.**

Ce dernier n'est pas intègre...

Proposition

Soit P un polynôme irréductible de degré d dans un corps de caractéristique p. Alors $P \mid X^{p^d} - X$.

▷ Théorème de Lagrange dans le groupe multiplicatif de $K/(P)$. ■

Note. Sans le dire, construire les corps finis revient à faire de la théorie de Galois sur les corps finis.

Remarque. Soit K un corps de caractéristique $p \geqslant 2$ et m un entier naturel. Alors $(-1)^{p^m} = -1$.

Théorème. ***(Cardinal d'un corps fini)***

Soit K un corps fini. Alors $\mathrm{card}(K) = p^k$ où p est un nombre premier et $k \in \mathbb{N}$.

Un corollaire immédiat par le théorème de Lagrange :

Proposition. ***(Séparabilité de $X^{p^m} - X$)***

Soit K un corps fini de cardinal p^m avec les notations évidentes. Alors

$$X^{p^m} - X = \prod_{a \in K} (X - a).$$

Par conséquence, K est le corps de décomposition de $X^{p^m} - X$ sur $\mathbb{F}_p$ (**cette description est fondamentale et sans cesse utilisée**). Inversement, si l'on pose K le corps de décomposition du polynôme $X^{p^m} - X$ sur $\mathbb{F}_p$, alors montrons que $|K| = p^m$.

▷ Soit $K_0 = \{a \in K, a^{p^m} - a = 0\}$. Alors $K_0 \subseteq K$, et comme les racines sont simples, $|K_0| = p^m$, car $(X^{p^m} - X)' = -1$. Enfin, K_0 est un sous-corps de K : en effet, pour $a,b \in K_0$, $(ab)^{p^m} = a^{p^m} b^{p^m}$ et $(a+b)^{p^m} = a^{p^m} + b^{p^m}$. ■

On a tous les éléments pour énoncer le théorème suivant :

Théorème. ***(Existence et unicité des corps finis)***

Pour tout nombre premier p et entier $m \geqslant 1$, il existe un corps K de cardinal p^m, unique à isomorphisme près. On le note $K = \mathbb{F}_{p^m}$ (celui de la construction suivante).
En fait, K est un corps de décomposition de $X^{p^m} - X \in \mathbb{F}_p[X]$.

Par exemple, $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$. De même, $\mathbb{F}_8 = \mathbb{F}_2[X]/(X^3 + X + 1) \simeq \mathbb{F}_2[X](X^3 + X^2 + 1)$. Il est rare que la non-canonicité de cette construction pose problème.

Théorème. ***(Sous-corps d'un corps fini)***

Soit K un corps fini de cardinal $q = p^n$. Alors ses sous-corps sont exactement les corps de la forme K' de cardinal $q' = p^d$ où d divise n.

▷ En effet, K est un K'-ev, donc $q = (q')^k = p^{dk} = p^n$, d'où $d \mid n$. Réciproquement, on peut considérer $F(d) = \{x \in K, x^{q'} - x = 0\}$. ■

Exercice 98

(Type d'étude de corps finis) Soit $P = X^3 + X + 1$ le polynôme à coefficients dans $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. On note $F = \mathbb{F}_2[X]/(P)$. On note α la classe de X dans cet anneau quotient.

1. Montrer que P est irréductible dans $\mathbb{F}_2[X]$. Qu'en déduit-on pour F ? Montrer qu'il est de cardinal 8.
2. Quel est le cardinal de $F^\times$? En déduire les ordres possibles pour les éléments de $F^\times$.
3. Montrer que α engendre $F^\times$, c'est-à-dire qu'il est exactement d'ordre $\mathrm{card}(F) - 1$.
4. Donner la liste des générateurs de $F^\times$ sous forme de puissances de α.
5. Exprimer $\alpha^3, \alpha^4, \alpha^6$ et α^8 en fonction de la base $(1, \alpha, \alpha^2)$ de F vu comme $\mathbb{F}_2$-espace vectoriel, en détaillant les calculs.
6. α est-il une racine primitive de α ? Que dire de $\beta = \alpha - 1$?

4.1.3.1 Puissances dans un corps fini

Soit p un nombre premier ; $\mathbb{F}_p$ est un corps.

⟶ **Notation.** On prend $\mathbb{F}_p^{\times n} = \{x^n, x \in \mathbb{F}_p^\times\}$ et $G_n = \{x \in \mathbb{F}_p^\times, x^n = 1\}$. Alors en notant $\phi : x \longmapsto x^n$ de $\mathbb{F}_p^\times$ dans lui-même, on a $\mathrm{Ker}(\phi) = G_n$ et $\mathrm{Im}(\phi) = \mathbb{F}_p^{\times n}$.

Proposition

On a :

1. $\mathrm{card}(\{x \in \mathbb{F}_p^\times\}) = (p-1) \wedge n$.
2. $\mathrm{card}(\{x^n, x \in \mathbb{F}_p^\times\}) = \frac{p-1}{(p-1)\wedge n}$.
3. Si $n \mid p-1$, $\mathbb{F}_p^{\times n} = \{x \in \mathbb{F}_p^\times \mid x^{\frac{p-1}{n}} = 1\}$.

▷ Il s'agit donc de montrer que $\mathrm{card}(G_n) = \mathrm{pgcd}(p-1, n)$. Le reste vient de la formule de Cauchy et d'un simple calcul. Il s'agit alors simplement de remarquer que $\{x \in \mathbb{F}_p^\times, x^n = 1\} = \{x \in \mathbb{F}_p^\times, x^d = 1$ où $d = \mathrm{pgcd}(n, p-1)$ qui est de cardinal d, car $\mathbb{F}_p^\times$ est cyclique. En effet, $x^{p-1} = 1$ et par le théorème de Bézout, $x^d = (x^n)^u (x^{p-1})^v = 1$, et réciproquement $d \mid n$ d'où l'égalité. ■

4.1.3.2 Automorphismes de corps finis

On rappelle que le groupe multiplicatif d'un corps fini est cyclique et que le groupe des automorphismes d'un groupe cyclique est isomorphe à son groupe multiplicatif. Ainsi, pour tout p premier,

$$\mathrm{Aut}(\mathbb{F}_p) \simeq \mathbb{F}_p^\times \simeq \mathbb{Z}/p-1\mathbb{Z}.$$

En reprenant les preuves de ces résultats, on obtient la description plus générale suivante. Soit $q = p^m$. En notant $\mathbb{F}_p \subseteq K \simeq \mathbb{F}_{p^m}$, $\phi(x) = x^p$ est un homomorphisme de corps (c'est le morphisme de Frobenius en caractéristique p). Remarque : toute puissance du morphisme de Frobenius, c'est-à-dire toute fonction $x \mapsto x^{p^s}$, est encore un automorphisme. De plus, $\phi_{|\mathbb{F}_p} = id_{\mathbb{F}_p}$, d'où $\phi : K \simeq K$, soit $\phi \in \mathrm{Aut}(K) := \mathrm{Aut}(K/\mathbb{F}_p)$. De plus, ϕ engendre un groupe cyclique d'ordre m.

▷ En effet, $\phi^m(x) = x^{p^m} = x$ pour tout $x \in K$, donc $\phi^m = id$. Si $d \mid m$ avec $d \neq m$, alors $\phi^d \neq id$, car $\#\{x \in K, \phi^d(x) = x\} \leqslant p^d < |K| \iff x$ est racine de $X^{p^d} - X$. Donc il existe $x \in K$, $\phi^d(x) \neq x$. ■

On voit *(paragraphe suivant)* que $\langle\phi\rangle = \mathrm{Aut}(K) = \mathrm{Aut}(K/\mathbb{F}_p)$. Observons que $\#\langle\phi\rangle = [K : \mathbb{F}_p]$.

Précisons donc ce point grâce au lemme d'Artin. Dans notre exemple, $K = \mathbb{F}_p$ et $L = F = \mathbb{F}_{p^m}$. On a ici $\mathrm{Hom}(L,L) = \mathrm{Aut}(L,L)$ et $\mathrm{Hom}_K(L,L) = \mathrm{Aut}(L/K)$. On a vu que $\langle\phi\rangle \simeq \mathbb{Z}/m\mathbb{Z}$ est contenu dans $\mathrm{Aut}(L/K)$ donc $\langle\phi\rangle = \mathrm{Aut}(L/K)$.

Ceci étant dit, on peut en conclure :

Théorème. ***(Automorphismes d'un corps fini)***

Soit K un corps fini de cardinal $q = p^n$. Alors $\mathrm{Aut}(K)$ est un groupe cyclique d'ordre n engendré par l'automorphisme de Frobenius qui à x associe x^p.

4.1.4 Extensions de corps : généralités

Lemme. ***(Lemme fondamental des extensions de corps)***

Si L est un sur-corps de K, alors L est un K-espace vectoriel.

Proposition. ***(Formule du produit)***

Soient $K \subseteq L \subseteq F$ des corps sous-corps les uns des autres. Alors :

$$[F : K] = [F : L][L : K]$$

avec la convention : si deux des termes sont finis, le troisième également et $\infty = \infty$.

▷ Si $(e_i)_{i=1\grave{a}m}$ est une base de L sur K et $(f_j)_{j=1\grave{a}n}$ une base de F sur L. Alors la base tensorielle $(e_i f_j)_{i,j}$ convient. ■

Remarque. Ceci est une conséquence de la formule de composition des dimensions pour les espaces vectoriels.

Proposition. ***(Égalité des degrés d'extension)***

Soient $K \subseteq L \subseteq F$ des corps. Alors $L = F \iff [F : K] = [L : K]$.

▷ En exercice. ■

Théorème. ***(Extension de corps polynomiale)***

Soient K un corps et P un polynôme à coefficients dans K. Alors (la K-algèbre) $K[X]/(P)$ est un K-espace vectoriel de dimension $\deg P$; c'est un corps, soit une extension de K, si et seulement si, P est irréductible dans $K[X]$.

▷ Si $n = \deg P$, on vérifie que les classes de $1,\ldots,X^{n-1}$ forment une base de A. Elle est génératrice par division euclidienne et libre, car un polynôme de degré $\leqslant n-1$ n'est divisible par P que s'il est nul, dans un anneau intègre. De plus, $K[X]$ étant principal, ce quotient est un corps si et seulement si (P) est maximal, si et seulement si P est irréductible. ■

Définition. ***(Extension simple)***

Une extension L/K est dite *simple* s'il existe $\alpha \in L$ tel que $L = K(\alpha)$.

Définition. ***(Extension de type fini)***

Une extension L/K est dite *de type fini* si elle est engendrée par un nombre fini d'éléments.

Définition. ***(Extension finie)***

Une extension L/K est dite *finie* si $[L : K]$ est finie.

Il existe des extensions simples qui ne sont pas finies ! Ils existe des extensions finies qui ne sont pas simples ! Observer : $\mathbb{Q}(\pi)$ et $\mathbb{Q}(\sqrt{2},\sqrt{3})$.

Définition. ***(Lien fini-type fini)***

Toute extension finie est de type fini.

▷ Soit L/K une extension finie et $e_1,...,e_r$ une base de L sur K. Alors immédiatement $L = K(e_1,...,e_n)$. ■

4.1.5 Construction d'extensions

4.1.5.1 Compositum de deux sous-corps

Remarque. Si $K \subseteq F_1 \subseteq L$ et $K \subseteq F_2 \subseteq L$, alors on peut définir un sous-corps $F_1 \cap F_2$. Cette notion ne suffit pas à priori.

Définition. ***(Compositum)***

On appelle *composé* ou *compositum* des deux sous-corps F_1 et F_2 d'un même corps contenant tous deux un corps, et l'on note F_1F_2, le plus petit sous-corps de L contenant F_1 et F_2, c'est-à-dire, $F_1(F_2) = F_2(F_1)$.
On ne définit le compositum qu'en se plongeant dans un même corps.

Sans plonger les deux corps dans un même corps, on ne peut pas définir de manière raisonnable le compositum. En effet, trouvons $\mathbb{Q} \subseteq F_1 = \mathbb{Q}(\sqrt[3]{2})$ et $\mathbb{Q} \subseteq F_2 \simeq F_1$. Prenons $F_2 = F_1 \subseteq \mathbb{C}$ comme choix 1 et $F_2 = \mathbb{Q}(j\sqrt[3]{2}) \subseteq \mathbb{C}$ comme choix 2. Dans le premier choix, $F_1 \cap F_2 = F_1$ et $F_1F_2 = F_1$. Dans le deuxième choix, $F_1 \cap F_2 = \mathbb{Q}$. De plus, $F_1F_2 = \mathbb{Q}(\sqrt[3]{2}, j)$ de degré 6 : les résultats ne sont pas isomorphes.

Mentionnons le lemme suivant, utile pour la démonstration du théorème de Galois :

Lemme

Supposons L_1,L_2 finies et séparables. Alors $[L_1L_2 : K] \leqslant \frac{[L_1:K][L_2:K]}{[L_1\cap L_2:K]}$.

▷ Posons $L_1 = K(\alpha)$ et $L_2 = K(\beta)$. Alors $L_1L_2 = L_2(\alpha)$ et $[L_1L_2 : L_2]$ est le degré du polynôme minimal de α sur L_2, inférieur au degré du polynôme minimal de α sur $K = [L_1 : K]$. Donc $[L_1L_2 : K] = [L_1L_2 : L_2][L_2 : K] \leqslant [L_1 : K][L_2 : K]$, si $K' = L_1 \cap L_2$. Ainsi $[L_1L_2 : K]/[K' : K] = [L_1L_2 : K'] \leqslant [L_1 : K'][L_2 : K'] = [L_1 : K]/[K' : K].[L_2 : K]/[K' : K]$, sachant bien que $[L_i : K]/[K' : K] = [L_i : K']$. La preuve est terminée. ■

4.1.5.2 Homomorphismes entre corps, morphismes d'extension

Définition. *(K-homomorphisme, morphisme d'extension)*

Soient L/K et F/K des extensions de corps. Un *K-homomorphisme* est un homomorphisme de corps $L \xrightarrow{f} F$ tel que $f_{|K} = id_K$.
On note $\mathrm{Hom}_K(L,F)$ l'ensemble de ces K-homomorphismes.

Exemples

1. *(Corps premier-homomorphismes)* Si $L/\mathbb{Q}$, $F/\mathbb{Q}$, alors $\mathrm{Hom}_{\mathbb{Q}}(L,F) = \mathrm{Hom}(L,F)$. De même, avec $\mathbb{F}_p$ à la place de $\mathbb{Q}$.

   ▷ En effet, si $m \in \mathbb{Z}$, $f(m.1_L) = mf(1_L) = 1_F$. De plus, si $n \in \mathbb{Z}$, on vérifie que $f(\frac{m}{n}) = \frac{m}{n}1_F = \frac{m}{n}$. ■

2. $L = \mathbb{Q}(\sqrt{d})$ avec $\sqrt{d}$ non contenu dans $\mathbb{Q}^\times$. Alors $\mathrm{Hom}(L,L) = \mathrm{Hom}_{\mathbb{Q}}(L,L) = \{id_L, \sigma\}$ où $\sigma(\sqrt{d}) = -\sqrt{d}$.

   ▷ En effet, soit $f : L \longrightarrow L$. Il est, d'après ce qui précède, déterminée par $f(\sqrt{d})$. Mais, $\sqrt{d}$ est racine de $X^2 - d \in \mathbb{Q}[X]$. Donc $f(\sqrt{d})^2 - d = 0$. Donc $f(\sqrt{d}) \in \{\sqrt{d}, -\sqrt{d}\}$. À vérifier que $\sigma(a + b\sqrt{d}) = a - b\sqrt{d}$ donne un isomorphisme de corps $\mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d})$ et l'on a le résultat. ■

   D'ailleurs, $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(-\sqrt{d}) \simeq \mathbb{Q}[X]/(X^2 - d)$.

3. Un exemple plus étonnant. Soit $L = \mathbb{Q}(\sqrt[3]{2}) = F$. Alors $\mathrm{Hom}(L,L) = \mathrm{Hom}_{\mathbb{Q}}(L,L) = \{id_L\}$.

   ▷ En effet, si $\alpha = \sqrt[3]{2}$, alors α est racine de $X^3 - 2 \in \mathbb{Q}[X]$. Si $f : L \longrightarrow L$, alors $f(\alpha)$ est aussi racine de $X^3 - 2$ par les mêmes arguments que précédemment, mais les racines de $X^3 - 2$ dans $\mathbb{Q}$, ou $\mathbb{C}$, sont $\alpha, j\alpha$ et $j^2\alpha$ où $j = e^{\frac{2i\pi}{3}}$ et ces deux dernières racines $\notin L$. Donc $f(\alpha) = \alpha$ et $f = id_L$. Mais $\#(\mathrm{Hom}(L,\mathbb{C})) = 3$. ■

4. Les morphismes d'extension sont utiles dans notre cours dans le cas où L/K est algébrique. Alors F/K n'est pas forcément algébrique, mais ce n'est pas intéressant si ce n'est pas le cas.

Lemme. *(Lemme d'Artin)*

Soient $\sigma_1,...,\sigma_n \in \mathrm{Hom}(L,F)$ deux à deux distincts. Alors ils sont linéairement indépendants sur F.

▷ Par récurrence sur n. Le résultat pour $n = 1$ est trivial par intégrité dans un corps, en prenant par exemple l'évaluation en 1_L. Soient $a_1,...,a_n \in F$. On suppose que pour tout x, $a_1\sigma_1(x) + ... + a_n\sigma_n(x) = 0 \qquad (\star_1)$. Faisons l'hypothèse de récurrence et montrons que $a_1 = ... = a_n = 0$. Pour tous $x,y \in L$, $xy \in L$, donc en appliquant l'hypothèse à xy, on a :

$$a_1\sigma_1(y)\sigma_1(x) + ...a_n\sigma_n(y)\sigma_n(x) = 0 \quad (\star_2).$$

En opérant pour $(\star_1)$ sur les lignes $\sigma_n(y)(\star_1) - (\star_2)$, on obtient

$$a_1(\sigma_n(y) - \sigma_1(y))\sigma_1(x) + ... + a_n(\sigma_n(y) - \sigma_{n-1}(y))\sigma_{n-1}(x) = 0$$

pour tous x,$y \in L$. Or par hypothèse de récurrence, σ_1,...,σ_{n-1} sont linéairement indépendants. Ainsi pour tout $i \in [\![1,n-1]\!]$, $a_i(\sigma_n(y) - \sigma_i)(y)$ pour tout y. Puisque $\sigma_n \neq \sigma_i$, il existe un $y(i)$ tel que $\sigma_n(y) \neq \sigma_i(y)$ ce qui donne $a_i = 0$ pour tout $i < n$, puis le cas $n = 1$ donne $a_n = 0$, et le lemme est montré. ■

Ce résultat qui tient sans hypothèse aucune sur l'extension, est particulièrement intéressant dans le cas de l'extension finie.

Application. ***(Construction du groupe de Galois)***

Prenons L/K et F/K avec $[L : k] = m$. Alors σ_1,...,$\sigma_n \in \mathrm{Hom}_K(L,F)$ sont F-li-indépendants. Si on choisit e_1,...,e_m une base de L sur k, σ est déterminée par $(\sigma(e_1),...,\sigma(e_m)) \in F^m$. Conclusion, $n \leqslant m$. D'où :

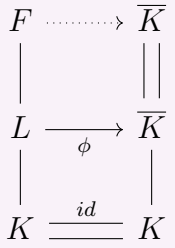
$$|\#\mathrm{Hom}_K(L,F) \leqslant [L : K]|.$$

En effet, $\mathrm{Hom}_K(L,F) \xrightarrow{\psi} F^m$ qui à $\sigma \longmapsto (\sigma(e_1),...,\sigma(e_m))$. Alors $\psi(e_1),...,\psi(e_m)$ sont F-linéairement indépendants.
Le lemme d'Artin nous dit qu'il n'y a pas beaucoup d'extensions algébriques de degré fini.

On fournit un autre lemme utile :

Lemme. ***(Lemme de prolongement, lemme de Stein)***

Si L/K est finie, si $\phi \in \mathrm{Hom}_K(L,\overline{K})$ et si $L \subseteq F \subseteq \overline{K}$, où F/L est finie, alors il existe $\tilde{\phi} \in \mathrm{Hom}_K(F,\overline{K})$ tel que $\tilde{\phi}_{|L} = \phi$. On a donc :



▷ Il suffit de traiter le cas où $F = L(\alpha)$. Alors on prend pour $\overline{K}$, $L' = \phi(L)$. Soit $P_\alpha \in L[X]$ le polynôme minimal de α. Alors $(\mathrm{ev}_\alpha)^{-1}$ induit un isomorphisme $F = L(\alpha) \simeq L[X]/(P_\alpha)$. Posons $P'_\alpha = \phi(P_\alpha) \in L'[X]$, irréductible dans $L'[X]$. On choisit $\beta \in \overline{K}$ racine de P'_α. Alors $\tilde{\phi} : L(\alpha) \simeq L[X]/p_\alpha \simeq L'[X]/(P'_\alpha) \simeq L'(\beta)$ par ev_β, sous corps de $\overline{K}$. Remarquons au passage qu'on a un contrôle sur le nombre d'extensions ; il est inférieur au nombre de racines de P_α.

On en déduit en effet le cas général par récurrence forte sur $n = [F : L]$. Pour $n = 1$, c'est trivial.

Après, pour $\alpha \notin L$, $L \subsetneq L(\alpha) \subseteq F$. Alors $[F : L(\alpha)] < [F : L] = n$. Ainsi $\tilde{\phi}_{|L(\alpha)} = \tilde{\phi}_1$ et $\tilde{\phi}_{1|L} = \phi$, où $\tilde{\phi}_2 : F \longrightarrow \overline{K}$ est donnée par l'hypothèse de récurrence et $\tilde{\phi}_1 : L(\alpha) \longrightarrow \tilde{\phi}_1(L(\alpha)) \subseteq \overline{K}$. ■

Remarque. Toutes les extensions finies (resp. algébriques) d'un corps se plongent dans sa clôture algébrique.

On peut généraliser :

Lemme. ***(Prolongement des morphismes aux extensions algébriques)***

Soit L/K une extension algébrique et $\Omega = \overline{K}$. Soit σ un morphisme de K dans Ω. Alors on peut trouver un morphisme σ' de L dans Ω prolongeant σ.

▷ Soit $\mathcal{E}$ l'ensemble des couples (M, θ) où M est un sous-corps de L contenant K et θ un morphisme de M dans Ω prolongeant σ, autrement dit l'ensemble des prolongements de σ. Il est naturellement ordonné par : M est un sous-corps de M' et θ' prolonge θ. Cet ordre est inductif, car si $(M_i, \theta_i)_{i\in I}$ est totalement ordonnée dans $\mathcal{E}$, alors $\bigcup_{i\in I} M_i$ est bien un corps, contenant évidemment, tous les M_i, et θ défini sur cette réunion pour tout $i \in I$ par θ_i est également bien défini et prolonge tous les θ_i, de sorte que $(M_i, \theta_i$ est majorée. Par le lemme de Zorn, soit (M, θ) un élément maximal. Il suffit maintenant de vérifier que M est L, et alors θ convient. Si ce n'est pas le cas, soit x dans L et non dans M. Alors d'après le lemme précédent, on peut exhiber un prolongement défini sur le sur-corps strict de M, $M(x)$, car $x \in L$ est algébrique donc $M(x)/M$ l'est. Ceci contredirait la maximalité de M. D'où le résultat. ■

4.1.6 Corps de rupture

Exercice 99

Montrer que $\mathbb{R}[X]/((X^2 - 1)) \simeq \mathbb{R}^2$.

▷ **Éléments de réponse.**

Théorème chinois. Cet espace est donc isomorphe au plan...

Définition. ***(Corps de rupture)***

Soit K un corps et $P \in K[X]$. On appelle *corps de rupture* de P tout extension *minimale* de K dans laquelle P possède une racine.

Certains ne supposent pas la minimalité. Avec cette convention, tout corps de décomposition par exemple est de rupture : nous ne prenons pas cette convention. Notons également que la minimalité de la définition coïncide avec la minimalité du degré.

Fait. ***(Définition de la rupture)***

Un corps de rupture d'un polynôme $P \in k[X]$ est une extension simple de k sur lequel k a une racine, engendrée par une racine de P dans k.

Corollaire

Tout corps de rupture est une extension finie, en particulier algébrique.

Remarquons le fait suivant :

Proposition. ***(Plongement d'un corps dans ses quotients)***

Soit P un polynôme sur K. Alors K se plonge dans $K[X]/(P)$.

▷ En effet, un morphisme d'anneaux partant d'un corps est injectif ! Il suffit de prendre $i : K \longrightarrow K[X] \longrightarrow K[X]/PK[X]$. ■

Remarque. Dans le cas où P a déjà une racine dans K, cette construction reste cohérente. En effet, pour $P = X - x_0$, $K[X]/(P) = K[x_0] \simeq K$. Cela n'a aucun intérêt.

Proposition. ***(Règles de calcul dans $\mathbb{K}[X]/(P)$)***

On a :

1. $T(x) = S(x) \iff P \mid T - S$.
2. $\pi(T) \in (K[X]/(P))^*$.

▷ Bref. ■

Théorème. ***(Existence du corps de rupture)***

Soient K un corps et P un polynôme à coefficients dans K. Alors :

1. Il existe $L \supseteq K$ et $\alpha \in L$ tel que $P(\alpha) = 0$.
2. Si de plus P est irréductible et si $L = K(\alpha)$, alors L est unique à isomorphisme près.

▷ En fait, on peut supposer P irréductible dès le départ : sinon, choisir un facteur irréductible de P. On pose $L = K[X]/PK[X]$: c'est donc un corps. K se plonge naturellement dedans, donc L est une extension de $i(K) \simeq K$. Montrons que $\alpha = X \bmod PK[X]$ est une racine de $i(P)$. On pose $P = X^d + a_{d-1}X^{d-1} + ...a_0$. Ainsi $i(P)(\alpha) = i(P)(X \bmod PK[X]) = i(P(X)) \bmod PK[X] = 0$ dans $K[X]/PK[X]$, car $P \longmapsto P \bmod PK[X]$ est un homomorphisme d'anneaux. On en conclut que $L :=$ est un corps de rupture, $\alpha = X \bmod PK[X]$ étant une racine. Et $L = K(\alpha)$, car $K[X]$ étant engendré par X, L est engendré par α l'image de X.

Soit $\alpha \in L \supseteq K$ tels que $P(\alpha) = 0$ et $L = K(\alpha)$. Observons que P est le polynôme minimal de α sur K, puisque P_α divise P qui est irréductible. On a vu que $\mathrm{ev}_\alpha : K[X] \longrightarrow K[\alpha] = K(\alpha)$ induit $K[X]/PK[X] \simeq K(\alpha)$, et c'est terminé. ■

Corollaire. *(Type du corps de rupture)*

Tout corps de rupture est de type fini.

4.1.7 Corps de décomposition, corps des racines

Définition. *(Corps de décomposition)*

Soit K un corps et $P \in K[X]$. On appelle *corps de décomposition* ou *corps des racines* ou encore *corps de déploiement* de P toute extension de K dans laquelle P est scindé (= admet autant de racines que son degré, comptées avec leur multiplicité), et qui est une sous-extension de toute extension dans laquelle P est scindé.

Théorème. *(Existence du corps de décomposition)*

Soient K un corps et P un polynôme à coefficients dans K. Alors si $\deg(P) = d \geqslant 1$,

1. Il existe $L \supseteq K$, $\alpha_1,...,\alpha_d \in L$ tels que $P = a_d(X - \alpha_1)...(X - \alpha_d)$, soit P scindé.
2. De plus, si $L = K(\alpha_1,...,\alpha_d)$, alors L est unique à isomorphisme près.

Remarque. En fait, d'après la définition, les racines de P engendrent automatiquement L le corps de décomposition.

Preuve.

▷ C'est facile par récurrence sur d. Pour $d = 1$, c'est trivial. Par le théorème précédent, il existe $L_1 \ni \alpha_1$ avec $P(\alpha_1) = 0$, on factorise $P = (X-\alpha_1)P_1(X)$ avec $P_1 \in L_1[X]$, $\deg(P_1) = d-1$. En utilisant l'hypothèse de récurrence, il existe $L_1 \subseteq L$ tel que $\alpha_1,...,\alpha_d \in L$, tels que $P_1 = (X - \alpha_2)...(X - \alpha_d)$ donc P est scindé sur L.

Pour bien faire fonctionner la récurrence, on admet l'énoncé plus général suivant. Il permet de conclure. ■

Sous-lemme

Soit $K \simeq K'$ par un morphisme i. Soit $P \in K[X]$. Soit $L = K(\alpha_1,...,\alpha_d)$ avec $P = (X - \alpha_1)...(X - \alpha_d)$. On prend $L' = K(\beta_1,...,\beta_d)$ avec $i(P) = (X - \beta_1)...(X - \beta_d)$. Alors $\exists \phi : L \longrightarrow L'$ tel que $\Phi_{|K} = i$.

▷ Pour $d = 1$, c'est trivial. Sinon, $\exists L_1 K(\alpha_1)$ avec $P(\alpha_1) = 0$, donc si α_1 est racine du polynôme $P_1|P$ irréductible, choisissons β_1 racine de $i(P_1)$ dans une extension $L'_1 = K'(\beta_1)$. On en déduit que

$$\begin{array}{ccc} L_1 & \xrightarrow{\phi_1} & L'_1 \\ | & & | \\ K & \xrightarrow{i} & K' \end{array}$$

où $L_1 \ni \alpha_1, L_1' \ni \beta_1$, avec $L_1 \neq K[X]/P_1K[X]$ et $L_1' = K'[X]/i(P_1)K[X]$. On en déduit

$$\begin{array}{ccc} K[X] & \xrightarrow{\quad i \quad} & K'[X] \\ \Big| & & \Big| \\ K[X]/P_1K[X] & \xrightarrow{\sim} & K'[X]/i(P_1)K'[X] \end{array}$$

sans problème. Dans $L_1[X]$, $P = (X - \alpha_1)Q$ avec $\deg(Q) = d - 1$. Donc $i(P) = (X - \beta_1)\phi_1(Q)$ avec $\deg(Q) = d - 1$. D'après l'hypothèse de récurrence, $L = L_1(\alpha_1,...,\alpha_d) \simeq L' = L_1'(\beta_2,...,\beta_d)$. Or,

$$\begin{array}{ccc} L & \xhookrightarrow{\phi} & L' \\ \downarrow & & \downarrow \\ L_1 & \xrightarrow[\phi_1]{} & L_1' \\ \downarrow & & \downarrow \\ K & \xhookrightarrow{i} & K' \end{array}$$

ce qui termine la preuve. ■

Par exemple, si $K = \mathbb{Q}$ et $P = X^3 - 2$, $L = \mathbb{Q}(\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, j)$.

Remarque. Un corps de rupture d'un polynôme irréductible n'a aucune raison d'être un corps de décomposition, mais c'est possible, même si son degré est > 2. En revanche, on rappelle que dans un corps fini, un corps de rupture d'un polynôme irréductible est toujours un corps de décomposition du même.

Corollaire

Tout corps de décomposition est une extension finie, en particulier algébrique.

Corollaire. ***(Type du corps de décomposition)***

Tout corps de décomposition est de type fini.

Heuristique

Car un polynôme non nul n'a qu'un nombre fini de racines.

Un corps de rupture concerne les polynômes irréductibles ; un corps de décomposition concerne n'importe quel polynôme.

4.1.8 Clôture algébrique

Cette construction n'est absolument pas constructive.

Définition. ***(Clôture algébrique)***

Soit F un corps. Alors F est dit *algébriquement clos* si pour tout unitaire $P \in F[X] \setminus F$, $\exists \alpha_1,...,\alpha_d \in F$, $P = (X-\alpha_1)...(X-\alpha_d)$.
De façon équivalente, tout polynôme non constant admet une racine.

Définition. ***(Clôture algébrique)***

Soit F un corps. Une clôture algébrique de F est un corps, extension *algébrique* de F, algébriquement clos.

Propriété

Si deux corps K_1 et K_2 sont isomorphes, et si l'un est algébriquement clos, alors l'autre est aussi algébriquement clos.

▷ Ce n'est pas tout à fait trivial, nous nous donnons la peine de l'écrire. Supposons, par symétrie, que K_1 est algébriquement clos. Soit $P = a_0 + a_1X + ... + a_nX^n$ un polynôme à coefficients dans K_2. Par surjectivité de l'isomorphisme de corps $\varphi : K_1 \longrightarrow K_2$ que nous pouvons invoquer, il existe des éléments de K_2, notés $b_0,...,b_1$ dont les images par φ sont respectivement les $a_1,...,a_n$, de sorte que l'on puisse écrire $P = \varphi(a_0) + \varphi(a_1)X + ... + \varphi(a_n)X^n$. D'autre part, le polynôme $b_0 + b_1X + ... + b_nX^n$ est à coefficients dans K_1. Comme ce corps est algébriquement clos, il admet une racine α, soit $b_0 + b_1\alpha + ... + b_n\alpha^n = 0_{K_1}$. Composons par φ : $\varphi(b_0 + b_1\alpha + ... + b_n\alpha^n) = \varphi(0_{K_1}) = 0_{K_2}$. Or φ est un morphisme de corps, ce qui permet, en utilisant les trois axiomes de morphisme d'anneaux, d'écrire exactement $\varphi(b_0+b_1\alpha+...+b_n\alpha^n) = \varphi(b_0)+\varphi(b_1)\varphi(\alpha)+...+\varphi(b_n)\varphi(\alpha)^n = a_0+a_1\varphi(\alpha)+...+a_n\varphi(\alpha)^n = P(\varphi(\alpha))$, soit $P(\varphi(\alpha)) = 0_{K_2}$. En notant $\beta = \varphi(\alpha) \in K_2$, $P(\beta) = 0$, donc P a une racine dans K_2. ■

Il nous faudra surtout utiliser le théorème suivant, dont la démonstration, remarquons-le, nécessite (encore) l'axiome du choix au moyen du lemme de Zorn démontré en début de composition.

Théorème. ***(Steinitz)***

Tout corps commutatif admet une clôture algébrique, c'est-à-dire une extension algébrique de corps (aussi appelée parfois *sur-corps*) algébriquement close. De plus, cette clôture algébrique est unique à isomorphisme près.

▷ Soit K un corps (commutatif, non trivial). On choisit un ensemble Ω de cardinal $\max(2^{\aleph_0}, 2^{\mathrm{card}(K)})$. C'est possible ; il suffit de considérer l'ensemble des réels ou bien l'ensemble des parties de K. On considère l'ensemble des triplets $(L, +, \times)$ avec L un sous-ensemble de Ω contenant K, et des lois prolongeant celles de K faisant de L une extension algébrique, c'est-à-dire telle que tous les éléments de L sont algébriques sur K, c'est-à-dire racines d'un polynôme à coefficients dans K. On définit une relation d'ordre sur l'ensemble de ces triplets par $(L, +, \times) \leqslant (L', +, \times)$ si $L \subseteq L'$ et si L est un sous-corps de L' (on entend, pour ces lois). On vérifie aisément que l'ensemble des triplets considéré

est alors un ensemble inductif. Il est non vide, car il contient K. Par le lemme de Zorn, on en déduit qu'il admet un élément maximal, que nous notons F. Montrons que F est une clôture algébrique de K.

Soit E une extension algébrique de F. F étant algébrique sur K par construction, il est de même cardinal que K ou, lorsque K est fini, est au plus dénombrable. Justifions le : $F = \bigcup_{n\in\mathbb{N}} \bigcup_{P\in K_n[X],P\neq 0} \mathcal{Z}(P)$, d'après la définition d'algébricité, où l'on note $\mathcal{Z}(P)$ l'ensemble des racines de P. Or cet ensemble est fini puisque P est non nul, $K_n[X]$ est un K-espace de dimension $n+1$, donc isomorphe à K^{n+1}. Si K est infini, cet ensemble est équipotent à K, car tout ensemble infini est équipotent à son carré cartésien, et comme il est encore infini, en passant à une réunion dénombrable, F est de cardinal K. Si K est fini, cet ensemble est encore fini, puis en passant à la réunion dénombrable, il est au plus dénombrable. E étant une extension algébrique de F, il est, de même cardinal que F, donc de même cardinal que K. Par suite, le complémentaire de F dans E est de cardinal inférieur à celui de $\complement_\Omega F$, qui a le même cardinal que Ω. Ainsi, il existe une application injective de E dans Ω qui soit l'identité sur F. Si l'on munit son image de la structure de corps induite par celle de E, on obtient une extension algébrique de F. Par maximalité de F, cette image est égale à F. Donc $E = F$, et F est algébriquement clos, ce qui termine la preuve.

Cette clôture algébrique est unique à isomorphisme près. En effet, si F_1, F_2 sont deux clôtures algébriques de K, on considère les couples (L, ρ) où L est une sous-K-extension de F_1 et où $\rho : L \longrightarrow F_2$ est un morphisme de corps. L'ensemble de ces couples est non vide et est naturellement ordonné. On vérifie également qu'il est inductif. Soit (L, ρ) un élément maximal donné par le lemme de Zorn. Si a est un élément de F_1, on considère son polynôme minimal $P(x) \in L[x]$ sur L, qui existe. Le polynôme $\rho(P(x)) \in \rho(L)[x]$ admet une racine b dans F_2. Il existe alors un morphisme de corps $L[a] \longrightarrow F_2$ qui vaut ρ sur L, envoyant a sur b. Par maximalité de (L, ρ), on a $L[a] = L$, donc $L = F_1$. Comme $\rho(F_1) \subseteq F_2$ est algébriquement clos, on a $\rho(F_1) = F_2$, puis ρ est un isomorphisme de F_1 sur F_2. ■

Remarques.

1. Sans rien supposer de plus que la définition, on a l'unicité à isomorphisme près de la clôture algébrique (supposée algébrique). Ainsi, on peut la voir comme une extension algébriquement close minimale, mais également comme une extension algébrique maximale.
2. La clôture algébrique n'est pas nécessairement finie, ni de type fini.

(Erreur courante) La clôture algébrique de $\mathbb{Q}$ n'est pas $\mathbb{C}$! (Elle n'est pas non plus incluse dans $\mathbb{R}$).)

4.1.9 Nombres algébriques, nombres transcendants

4.1.9.1 Théorie élémentaire

On conseille au lecteur de relire la construction du morphisme évaluation, même s'il ne présente qu'un intérêt formel. En particulier, il n'est un morphisme que si l'arrivée est commutative.

Définitions. ***(Algébrique, transcendant)***

Soient L/K deux corps et $\alpha \in L$. Soit ev_α le morphisme évaluation de $K[X]$ dans L.

1. Si $\mathrm{Ker}(\mathrm{ev}_\alpha) = \{0\}$, on dit que α est *transcendant* sur K.
2. Si $\mathrm{Ker}(\mathrm{ev}_\alpha) = P_\alpha K[X]$ avec P_α non nul, on dit que α est *algébrique* sur K. On peut alors toujours prendre P_α unitaire et irréductible par intégrité dans L.

On note $K[\alpha]$ l'image de ev_α, et $K(a)$ le plus petit sous-corps de L contenant K et α, qui existe, car l'intersection de corps est corps.

En particulier, on peut utiliser à loisir la caractérisation suivante : **le polynôme annulateur est le seul polynôme annulateur de α irréductible dans K.**

Proposition. ***(Description de l'extension engendrée)***

Avec les notations précédentes :

1. Si α est transcendant, $K[a] \simeq K[X]$ et $K(\alpha) = K(X)$. On remarque $\dim_\pi K[\alpha] = \infty$.
2. Si α est algébrique, $K[a] = K(\alpha) = K[X]/P_\alpha K[X]$ d'où $[K(\alpha) : K] = \deg(P)$.

▷ Dans le cas transcendant, le premier isomorphisme découle de ce que l'évaluation est un morphisme injectif. La description du sous-corps engendré vient de la définition du corps des fractions. Le cas algébrique vient de la théorie des extensions de corps finies. ■

Corollaire. ***(Caractérisation des nombres algébriques)***

Soient L/K deux corps et $\alpha \in L$. Les propositions suivantes sont équivalentes :

1. α est algébrique sur K,
2. $K[\alpha] = K(\alpha)$,
3. $\dim_K K(\alpha) < \infty$ (dans le cas contraire, elle est infinie dénombrable).

On verra par quelles opérations les nombres algébriques sont stables, mais il faut avant cela introduire la notion d'extension algébrique.

4.1.9.2 Extension algébrique

Définition. ***(Extension algébrique)***

Soient L/K deux corps. On dit que L est *algébrique* sur K si tous les éléments de L sont algébriques sur K.

On a la proposition immédiate suivante, qui nous vient de la formule du produit :

Proposition. ***(Degré du polynôme minimal en extension finie)***

Si L/K est une extension finie (donc algébrique), si $\alpha \in L$, alors le degré du polynôme minimal de α divise $[L : K]$.

Propositions. ***(Degré d'une extension algébrique)***

1. Si $[L : K] < \infty$, alors K est algébrique sur L et la réciproque est fausse.
2. Si L est de type fini, alors $L = K(\alpha_1,...,\alpha_m)$ avec α_i algébrique, alors $[L : K] < \infty$.

▷ Successivement :

1. Si $\alpha \in L$, où $K \subseteq K(\alpha) \subseteq L$, alors $[L : K(\alpha)][K(\alpha : K] = [L : K]$ finie, donc $[K(\alpha) : K] < \infty$, donc α est algébrique sur K.
2. On fait une preuve par récurrence sur m. Pour $m = 1$, c'est déjà vu. Autrement, si $K \subseteq K(\alpha_1,...,\alpha_{m-1}) \subseteq K(\alpha_1,...,\alpha_m)$, par hypothèse de récurrence, $[K(\alpha_1,...,\alpha_{m-1}) : K] < \infty$. Mais $K(\alpha_1,...,\alpha_m) = K(\alpha_1,...,\alpha_{m-1})(\alpha_m)$. Puisque α_m est algébrique sur K, α_m est algébrique sur $K(\alpha_1,...,\alpha_{m-1})$ par le même polynôme annulateur, éventuellement non irréductible mais peu importe, donc $[K(\alpha_1,...,\alpha_m),K(\alpha_1,...,\alpha_{m-1})] < \infty$. Finalement, par produit et formule des indices, $[K(\alpha_1,...,\alpha_m) : K]$. ■

Remarque. En observant la preuve, on a mieux :

$$[K(\alpha_1,...,\alpha_m) : K] \leqslant [K(\alpha_1) : K]...[K(\alpha_m) : K].$$

▷ Par majoration du degré du polynôme minimal. ■

Proposition. ***(Extension algébrique simple)***

Une extension simple est finie si et seulement si elle est algébrique.

Propriété. ***(Tour d'extensions algébriques)***

Soient $F/L/K$ une tour d'extensions de corps. Si F est algébrique sur L et L est algébrique sur K, alors F est algébrique sur K.

▷ Soit $\alpha \in F$. Il existe $P_L \in L[X] \setminus \{0\}$, $P_L(\alpha) = 0$. On note $P_L(X) = X^d + a_{d-1}X^{d-1} + ... + a_0$. Ainsi $a_i \in L$ est algébrique sur K. Appelons $L_0 = K(a_0,...,a_{d-1})$. On a $[L_0 : K] < \infty$ et évidemment $P_L \in L_0[X]$. Par formule des degrés sur les deux premiers termes de $K \subseteq L_0 \subseteq L_0(\alpha) \subseteq F$, $[L_0(\alpha) : K] < \infty$. En particulier, $[K(\alpha) : K] < \infty$. Donc α est algébrique sur K. ■

Corollaire. ***(Opérations sur les nombres algébriques)***

Soient $K \subseteq L$ corps. Si α et β sont algébriques, alors $-\alpha, \alpha + \beta, \alpha\beta, \frac{1}{\alpha}$ sont algébriques.

▷ En effet, $[K(\alpha,\beta):K]<\infty$ donc tous les éléments de $K(\alpha,\beta)$ sont algébriques sur K. ■

Exemple. ***(Corps des nombres algébriques)***

Soit $\overline{\mathbb{Q}}=\{z\in\mathbb{C}, z \text{ algébrique sur } \mathbb{Q}\}$. Alors par définition, $\overline{\mathbb{Q}}$ est une extension algébrique sur $\mathbb{Q}$.
On peut montrer que $\overline{\mathbb{Q}}$ est algébriquement clos. Soit $P=X^d+a_{d-1}X^{d-1}+...+a_0\in\overline{\mathbb{Q}}[X]$. Il existe $\beta\in\mathbb{C}$, $P(\beta)=0$. Montrons qu'en fait, $\beta\in\overline{\mathbb{Q}}$. Posons $L_0=\mathbb{Q}(\alpha_0,...,\alpha_{d-1})$. Alors $[L_0:\mathbb{Q}]<\infty$. De plus, $P\in L_0[X]$, donc β est algébrique sur L_0, donc $[L_0(\beta):\mathbb{Q}]=[L_0(\beta):L_0][L_0:\mathbb{Q}]<\infty$. Donc $[\mathbb{Q}(\beta):\mathbb{Q}]<\infty$, d'où le résultat. *Cette technique est classique : bien qu'on ait affaire à un corps beaucoup trop gros, on considère le corps engendré par les coefficients du polynôme, en nombre fini, et l'on peut commencer à travailler.*
D'autre part, $[\overline{\mathbb{Q}}:\mathbb{Q}]=\infty$. En effet, pour tout $n\in\mathbb{N}$, X^n-2 est irréductible dans $\mathbb{Q}[X]$. Or $[\mathbb{Q}(\sqrt[n]{2}),\mathbb{Q}]=n$, d'où le résultat. *En effet, pour montrer qu'une extension est infinie, il suffit d'exhiber des sous-extensions de degré arbitrairement grand. Trouver une suite de polynômes irréductibles de degré strictement croissant convient.*

4.1.9.3 Théorie géométrique

On peut démontrer de manière très élémentaire suivant qui, contrairement au paradoxe de Banach-Tarski, auquel il ressemble, n'utilise pas l'axiome du choix. On le laisse en exercice.

Exercice 100

(Paradoxe de Sierpinski-Mazurkiewicz) On souhaite montrer qu'il existe une partie E du plan telle que E est la réunion disjointe de deux ensembles A et B tels que A et B sont toutes les deux isométriques à E. On identifie le plan à $\mathbb{C}$. On fixe un nombre complexe transcendant de module 1.

1. Justifier de l'existence d'un tel u.
2. On pose $E=\{P(u), P\in\mathbb{N}[X]\}$. Soient t la translation de vecteur d'affixe 1 et r la rotation par u. On pose $A=t(E)$ et $B=r(E)$. Montrer que (A,B) partitionne E. Pour la disjonction, utiliser la transcendance de u.
3. Conclure.

▷ **Éléments de réponse.**

Tout est dit...

4.1.9.4 Application du lemme d'Artin

On conseille de relire de lemme d'Artin à ce sujet.

Théorème

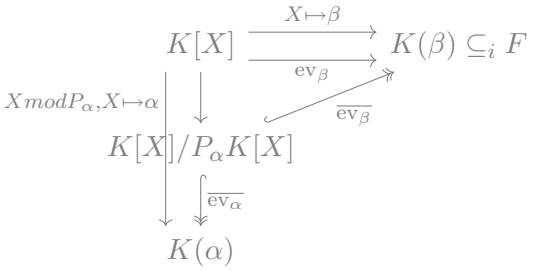
Soient L/K deux corps et l'on suppose $L = K(\alpha)$ avec α algébrique sur K, de polynôme minimal P_α. Alors on a la bijection suivante

$$\begin{array}{rcl} \mathrm{Hom}_K(L,F) & \longrightarrow & \{\beta \in F | P_\alpha(\beta) = 0\} = S \ . \\ f & \longmapsto & f(\alpha) \end{array}$$

▷ Si $f \in \mathrm{Hom}_K(L,F)$, alors $f(\alpha) \in S$. En effet, $P_\alpha(\alpha) = 0$ donc puisque f est un homomorphisme de K-algèbres, $P_\alpha(f(\alpha)) = f(P_\alpha(\alpha)) = 0$.

L'application est injective, car $f(\alpha)$ est détermine f.

La surjectivité, pour bien prendre un homomorphisme de corps, n'a rien de triviale. Soit $\beta \in S$. Comme P_α est irréductible, on peut écrire :



Considérons $f = i \circ \overline{\mathrm{ev}_{beta}} \circ \overline{\mathrm{ev}_\alpha}^{-1} \in \mathrm{Hom}(K(\alpha),F)$. Alors on a bien $f(\alpha) = \beta$ et $f_{|K} = id_K$. Ceci termine la preuve. ■

Exemple

$\mathrm{Hom}(\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})) = \emptyset$. Il suffit de trouver les racines d'un polynôme minimal !

En particulier, $\#\mathrm{Hom}_K(L,F) \leqslant \deg P_\alpha = [L : K]$ et on a l'égalité $\#\mathrm{Hom}_K(L,F) = [L : K]$ si et seulement si :

1. P_α est scindé sur F, *i.e.* toutes les racines sont dans F (ce deuxième énoncé étant un peu imprécis),
2. P_α n'a pas de racines multiples.

Nous démontrons ce résultat dans la section suivante, qui étudie l'influence de ces deux obstacles à la théorie des corps.

4.1.10 Extension séparable, extension normale

Définition. ***(Élément séparable)***

Soient L/K deux corps, on suppose que L/K est algébrique. Soit $a \in L$. On dit que a est *séparable sur* K si son polynôme minimal (qui existe, puisque L est algébrique sur K) est séparable, c'est-à-dire n'a pas de racines multiples, soit que des racines simples. Autrement dit, il est premier avec son polynôme dérivé.

D'après le critère différentiel de multiplicité des racines à l'ordre 1, en toute généralité, P est séparable ssi $P \wedge P' = 1$.

Définition. ***(Extension séparable)***

Soient L/K deux corps, on suppose que L/K est algébrique.
On dit que L/K est *séparable* si pour tout $\alpha \in L$, le polynôme $P_\alpha \in K[X]$ n'a pas de racines multiples, autrement dit, si tous ses éléments sont séparables sur K.

Définition. ***(Élément normal)***

Soient L/K deux corps, on suppose que L/K est algébrique. Soit $a \in L$. On dit que a est *normal sur* K si son polynôme minimal (qui existe, puisque L est algébrique sur K) est normal = scindé, c'est-à-dire admet autant de racines que son degré, comptées avec leur multiplicité.

Définition. ***(Extension normale)***

Soient L/K deux corps, on suppose que L/K est algébrique.
On dit que L/K est *normale* si pour tout $\alpha \in L$, le polynôme $P_\alpha \in K[X]$ est scindé dans $L[X]$. Cela revient à dire que tout polynôme P irréductible de $K[X]$ ayant au moins une racine dans L est scindé sur L.

Exemple

Prenons $L = K(\alpha)$. $\#\mathrm{Hom}_K(K(\alpha), K(\alpha)) = [K(\alpha) : K]$ si et seulement si $K(\alpha)/K$ est normale et séparable.

Intuitivement, « il y a le bon nombre de morphismes d'extension de L dans lui-même ».

On rappelle qu'il est possible, dans certains cas bizarres, qu'un polynôme irréductible tel que le polynôme minimal, admette des racines multiples. On mentionne donc un lien fondamental avec la notion de corps parfait.

Proposition. ***(Lien entre séparabilité et perfection)***

Un corps K est parfait, si et seulement si, toutes ses extensions algébriques sont séparables.

▷ On rappelle qu'en toute caractéristique, $(X-\alpha)^2|Q$ si et seulement si $Q(\alpha)=Q'(\alpha)=0$ (le redémontrer).

Si Q est irréductible (dans $K[X]$), et a une racine double $\alpha \in L$ extension de K, $Q'(\alpha)=0$ donc $Q \mid Q'$ et $\deg(Q') < \deg(Q)$, donc $Q'=0$. Si on écrit $Q(X)=\sum_{m=0}^{d} a_m X^m$, $Q'(X)=\sum_{m=1}^{d} m a_m X^{m-1}$, donc $ma_m=0$ pour $1 \leqslant m \leqslant d$. En caractéristique zéro, on obtient $a_1=...=a_m=0$. Contradiction. Si maintenant $\mathrm{car}(K)=p$, si p ne divise pas m, $a_m=0$, donc $Q(X)=\sum_{m\geqslant 0} a_{mp}X^{mp}$. Si K est parfait, c'est qu'il existe $b_m \in K$ tel que $a_{mp}=(b_m)^p$. Alors $Q(X)=\sum_{m\geqslant 0} b_m^p X^{mp}=(\sum_{m\geqslant 0} b_m X^m)^p$, contradiction.

Réciproquement, si K est non parfait, il existe $t \in K$ avec $t \notin K^p$. Construisons un polynôme irréductible non séparable. Posons simplement $Q=X^p-t$. Il est irréductible dans $K[X]$. De plus, si α est racine de W, $Q=(X-\alpha)^p=X^p-\alpha^p$, puisque $\alpha^p=t$. Vérifions que Q est irréductible. Si $Q=Q_1Q_2$ avec $Q_i \in K[X]$ et $\deg(Q_i) \geqslant 1$ dans $K(\alpha)[X]$ et $Q=(X-\alpha)^p$, alors $Q_1=(X-\alpha)^j$ et $Q_2=(X-\alpha)^{p-j}$. Ainsi $Q_1=X^j-j\alpha X^{j-1}+...$, donc $\alpha \notin K$, et comme $1 \leqslant j \leqslant p-1$ donc $j\alpha \in K$; contradiction. ■

Heuristique

Ainsi, un corps est parfait si et seulement si tout polynôme irréductible à coefficient dans lui est séparable, *i.e.* , un polynôme irréductible (c'est-à-dire, minimal d'un élément algébrique sur une extension) est sans racines multiples.

Tout prend sens !

Exemples. ***(Extensions séparables)***

1. Tout extension algébrique d'un corps fini est séparable. Toute extension algébrique de $\mathbb{Q}$ est séparable. (En effet, un corps fini ou de caractéristique nulle est parfait ; on conclut par le théorème de sous-corps premiers.) Par contre, rien ne dit qu'une extension algébrique d'un corps infini de caractéristique positive soit séparable, mais enfin, il faut déjà se lever de bonne heure.
2. L'extension $L=\mathbb{F}_p(X^{1/p})$ n'est pas séparable sur $\mathbb{K}=\mathbb{F}_p(X)$. Il n'y a même aucune sous-extension séparable.
3. Tout corps de décomposition d'un polynôme séparable est une extension séparable finie du corps de base. (Et donc, le TEP s'applique : l'extension est donc simple.)
4. Voici un exemple très pathologique. Soit p un nombre premier et $K=\mathbb{F}_p(X,Y)$. On pose α, β deux racines hors de K de polynômes de $K[X]$ vérifiant $\alpha^p=X$ et $\beta^p=Y$. ON prend $L=K(\alpha,\beta)$. Alors il se passe des choses horribles :
   - $[L:K]=p^2$,

- si $\gamma \in L \setminus K$, alors $[K(\gamma) : K] = p^2$,
- il n'existe pas de $\gamma \in L$ tel que $L = K(\gamma)$,
- il existe une infinité de F avec $K \subseteq F \subseteq L$,
- L/K n'est pas séparable mais est normale,
- $L \simeq K$ en tant que corps, et on peut identifier $L = \mathbb{F}_p(\alpha, \beta)$.

Montrons ces résultats. Pour commencer, on voit que $K \subseteq K(\alpha) \subseteq K(\alpha, \beta)$. On montre que ces extensions sont consécutivement de degré p, ce qui suffirait. Il suffit de montrer que, α étant racine de $T^p - X \in K[T]$, le polynôme $T^p - X$ est irréductible dans $K[T]$ (car alors $[K(\alpha) : K] = p$). On a $T^p - X = (T - \alpha)^p$ bien sûr, mais $\alpha \notin K$, attention à ne pas écrire n'importe quoi ! Donc si $T^p - X = Q_1(T)Q_2()$ pour Q_1,Q_2 à coefficients dans K cette fois, on a $Q_1 = (T - a)j = T^j - j\alpha T^{j-1} + ...$ et $Q_2 = (T - \alpha)^{p-j} = T^{p-j} - (p - j)\alpha T^{p-j-1} + ...$ pour $1 \leqslant j \leqslant p - 1$, mais $j\alpha \notin K$, car $j \neq 0$, absurde. D'autre part β est racine de $T^p - Y \in K[T] \subseteq K(\alpha)[T]$ avec $\beta \notin K(\alpha)$ car les indéterminées ne se mélangent pas.

Soit $\gamma \in L, \gamma \notin K$. Il existe une fraction rationnelle en deux indéterminées telle que $\gamma = \frac{P(\alpha,\beta)}{Q(\alpha,\beta)}$ avec P,Q à coefficients dans $\mathbb{F}_p$. Alors $\gamma^p = \frac{P(\alpha,\beta)^p}{Q(\alpha,\beta)^p} = \frac{P(\alpha^p,\beta^p)}{Q(\alpha^p,\beta^p)} = P(X,Y)/Q(X,Y) \in K[X]$ grâce au petit théorème de Fermat. Donc $1 < [K(\gamma) : K] \leqslant p$ et divise p^2 ; donc $[K(\gamma) : K] = p$ et $T^p - \gamma_i^p nK[T]$ est irréductible.

Si $f \in K = \mathbb{F}_p(X,Y)$, $f = f(X,Y)$. Alors $f^{1/p} = f(\alpha, \beta)$ par Fermat-caractéristique p d'où $f_i \in \mathbb{F}_p[X,Y]$ est irréductible et multiplicativement indépendant. On a $K(f^{1/p}) = K(g^{1/p})$ si $f = h^p g$. Ainsi la famille infinie des $f_i \in \mathbb{F}_p[X,Y]$ forme une infinité d'extensions sous-extensions différentes.

Exemples. ***(Extensions normales)***

1. K est normal sur lui-même.
2. La clôture algébrique $\overline{K}$ de K est une extension normale de K.
3. Le polynôme $P = X^3 - 2$ est irréductible sur $K = \mathbb{Q}$. Prenons $L = \mathbb{Q}(\sqrt[3]{2}$. Alors P a une racine dans L mais clairement pas toutes ses racines dans L. Ainsi, L n'est pas une extension normale de K.
4. Toute extension *quadratique*, *i.e.* de degré 2 est normale. Supposons $[L : K] = 2$. Soit $\alpha \in L, \alpha \notin K$. Alors $\deg(P_\alpha) = 2$. Ainsi $P_\alpha = X^2 + aX + b$. En caractéristique différente de 2, $P_\alpha = (X + \frac{a}{2})^2 + b - \frac{a^2}{4}$ dont les racines sont $-\frac{a}{2} \pm \sqrt{d}$ avec $d = b - \frac{a^2}{4}$. Donc $L = K(\sqrt{d})$ et $-\sqrt{d} \in L$. Si maintenant K est de caractéristique 2, $P_\alpha = X^2 + aX + b = (X - \alpha)(X - \beta)$. Ainsi, $\alpha + \beta = -a$ et $\alpha\beta = b$, donc $\beta = -a - \alpha \in K(\alpha)$. Dans tous les cas, L/K est normale.
5. Sous quelle condition une extension simple algébrique est normale ? En déduire quand elle est galoisienne.
6. Tout corps de décomposition est une extension normale (du corps de "base"). En effet,

soient r_1,...,r_n les racines de P dans Ω clôture algébrique de P. Alors $L = K(r_1,...,r_n)$. Tout morphisme de L dans Ω permute les racines, donc laisse L stable. Plus précisément, si P est irréductible sur K, alors $P = \prod(X - \alpha_i)$ et $L = K(\alpha_1,..., \alpha_n)$. Soit $f : L \longrightarrow \overline{K}$ avec $f_{|K} = id$. Ainsi $f(\alpha_i)$ est une racine de P_α donc $f : \{\alpha_i, ..., \alpha_n\} \longrightarrow \{\alpha_i, ..., \alpha_n\}$. Donc $f(\alpha_i) \in L$, donc $f(L) \subseteq L$. Donc $\mathrm{Hom}_K(L,L) \hookrightarrow \mathrm{Hom}_K(L,\overline{K})$ est une bijection, donc L/K est normale. Dans le cas général, c'est la même preuve.

En fait, *tout extension normale fine d'un corps est un certain corps de décomposition d'un polynôme*. En effet, si L/K est normale, alors du lemme $L = K(\alpha_1,..., \alpha_m)$, donc en notant P_1 le polynôme minimal de α_1,..., P_m celui de α_m sur K, alors $P = P_1...P_m \in K[X]$. Toutes les racines de P_i sont dans L, donc par normalité, toutes les racines de P et L est engendré par ces racines.

Heuristique

Une extension non séparable est vraiment dégueulasse. Une extension non normale, c'est plus courant. Mais c'est assez faisable d'avoir les deux.

Dans le cas $L = K(\alpha)$, $\#\mathrm{Hom}_K(L,\overline{K}) = \#\{\text{racines de } P_\alpha \in K[X]\}$. Alors si $K(\alpha)/K$ est séparable, $\#\mathrm{Hom}_K(L,\overline{K}) = \deg P_\alpha = [L : K]$ et si elle est normale, $\mathrm{Hom}_K(L,L) = \mathrm{Hom}_K(L,\overline{K})$. On peut étendre ces observations au cas fini. On rappelle que quelles que soient les extensions, $\mathrm{Hom}_K(L,L) \overset{i}{\hookrightarrow} \mathrm{Hom}_K(L,\overline{K})$. Il est équivalent de dire que i est une bijection que dire dire que $\#\mathrm{Hom}_K(L,L) = \#\mathrm{Hom}_K(L,\overline{K})$.

Proposition. ***(Caractérisation en termes de*** $\mathrm{Hom}_K(L,\overline{K})$***)***

Si L/K est une extension finie, avec $K \subseteq L \subseteq \overline{K}$. Alors :

$$L/K \text{ est séparable } \iff \#\mathrm{Hom}_K(L,\overline{K}) = [L : K]$$

et

$$L/K \text{ est normale } \iff \#\mathrm{Hom}_K(L,L) = \#\mathrm{Hom}_K(L,\overline{K}) \text{ soit } \mathrm{Hom}_K(L,L) = \mathrm{Hom}_K(L,\overline{K})$$

(par une légère identification).

▷ Successivement :

1. Le cas direct est donné par l'observation précédente. Réciproquement, soit $\alpha \in L$. Alors $K \subseteq K(\alpha) \subseteq L$, et notons P_α le polynôme minimal. On sait par définition que P_α est séparable si et seulement si $\#(\text{racines de } P_\alpha) = [K(\alpha) : K]$, si et seulement si $\mathrm{Hom}_K(K(\alpha)\overline{K}) = [K(\alpha), K]$. Il est donc non séparable si et seulement si $<$. On a $\#\mathrm{Hom}_{K(\alpha)}(L,\overline{K}) \leqslant [L : K(\alpha)]$ et $\#\mathrm{Hom}_K(K(\alpha),\overline{K}) \leqslant [K(\alpha) : K]$. On a la surjection $\mathrm{Hom}_K(L,\overline{K}) \twoheadrightarrow \mathrm{Hom}_K(K(\alpha),\overline{K})$, qui à $f \mapsto f_{|K(\alpha)}$. De plus, en observant la preuve du lemme de prolongement, le nombre de prolongements de $f' \in \mathrm{Hom}_K(K(\alpha),\overline{K})$ en

$f \in \mathrm{Hom}_K(L,\overline{K})$ est $\leqslant [L : K(\alpha)]$. Pour le cas général, on raisonne par induction sur $[L : K]$.

2. Supposons L/K normale. On veut montrer que si $f : L \longrightarrow \overline{K}$ est un K-homomorphisme, c'est-à-dire que $f_{|K} = id_K$, alors $f(L) \subseteq L$. Si $\alpha \in L$, alors $f(\alpha)$ est une racine du polynôme minimal de α sur K donc $f(\alpha) \in L$, donc $f(L) \subseteq L$. Réciproquement, soit $\alpha \in L$, notons P_α son polynôme minimal dans $K[X]$, si $P_\alpha(\beta) = 0$, on a vu qu'il existait $f : L \longrightarrow \overline{K}$ passant par K avec $f(\alpha) = \beta$, donc $\beta \in f(L) \subseteq L$, donc L/K est normale. ■

4.1.10.1 Propriétés calculatoires

Pour les extensions séparables, tout se passe bien.

Propriété. ***(Sous-extension d'une extension séparable)***

Toute sous-extension d'une extension de corps séparable est séparable.

Propriété. ***(Séparabilité d'une extension simple par un élément séparable)***

Soient L/K corps $\alpha \in L$ séparable sur K, alors $K(\alpha)/K$ est séparable.

Plus généralement :

Propriété. ***(Séparabilité par un système de générateurs séparables)***

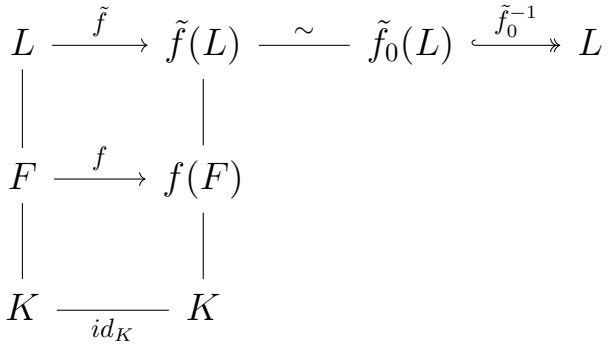
Soient L/K corps avec $L = K(\alpha_1,...,\alpha_m)$ avec les $\alpha_i \in L$ séparables sur K, alors L/K est séparable.

Propriété. ***(Tour d'extensions séparables)***

Soient $L/F/K$ une tour d'extensions de corps. Alors L/K est séparable si et seulement si L/F et F/K sont séparables.

▷ On a la surjection $\mathrm{Hom}_K(L,\overline{K}) \underset{r_F}{\twoheadrightarrow} \mathrm{Hom}_K(F,\overline{K})$, $F = K(\alpha)$ et $K \longrightarrow F \longrightarrow L \subseteq \overline{K}$, avec $r_F^{-1}(id_F) = \mathrm{Hom}_F(L,\overline{K})$ avec $id_F : F \longrightarrow \overline{K}, x \mapsto x$. Pour $f \in \mathrm{Hom}_K(F,\overline{K})$, $\#(r_F^{-1}(f) = \#\mathrm{Hom}_F(L,\overline{K})$. On a toujours $[L : K] \geqslant \#\mathrm{Hom}_K(L,\overline{K}) = \#\mathrm{Hom}_K(F,\overline{K})\#\mathrm{Hom}_F(L,\overline{K})$ où ce premier terme $\leqslant [F : K]$ et le second $\leqslant [L : F]$. Puisque $[L : K] = [F : K][L : F]$, si L/K est séparable, alors $[L : K] = \#\mathrm{Hom}_K(L,\overline{K})$ donc $\#\mathrm{Hom}_K(F,\overline{K}) = [F : K] \iff F/K$ séparable et $\#\mathrm{Hom}_F(L,\overline{K}) = [L : F] \iff L/F$ séparable. Si maintenant F/K et L/F sont séparable, alors $[L : K] = \#\mathrm{Hom}_K(L,\overline{K})$ donc L/K sont séparables. ■

On a déjà vu l'égalité clef de cette preuve : rappelons pourquoi. Choisissons $\tilde{f}_0 \in S_f$. Alors on a le schéma suivant :



donc $\tilde{f}_0{}^{-1} \circ \tilde{f}_{|F} = id_F$. On peut donc définir $S_f \longrightarrow S_{id_K}$ qui à $\tilde{f}$ donne $\tilde{f}_0^{-1} \circ \tilde{f}$.

Propriété. ***(Séparabilité du composé)***

Si $K \subseteq L_1 \subseteq F$ et $K \subseteq L_2 \subseteq F$, alors si L_1/K et L_2/K sont séparables, L_1L_2/K l'est. De même, si L_1/K est séparable, alors L_1L_2/L_2 est séparable.

▷ On a $L_1L_2 = L_1(\beta_1,...,\beta_n)$ avec $\beta_j \in L_1$ et β_j séparable sur K par hypothèse, donc $P_{\beta_j} \in K[X]$ a des racines simples, donc $Q_{\beta_j} \in L_2[X]$ son polynôme minimal sur L_2, qui divise P_{β_j} a donc de racines simples, car tout diviseur d'un polynôme séparable est séparable. ■

Pour les extensions normales, c'est un peu plus compliqué, mais il y a quand même des propriétés énonçables.

Contre-exemple. ***(Sous-extension non normale d'une normale)***

Prenons $L = \mathbb{Q}(\sqrt[3]{2},j)$, $F = \mathbb{Q}(\sqrt[3]{2})$. Alors $L/\mathbb{Q}$ est normale, L/F est normale, mais $F/\mathbb{Q}$ est non normale. □

Propriété. ***(Normalité par intercalation)***

Si $K \subseteq F \subseteq L$, alors si L/K est normale, L/F est normale.

▷ Soit $\alpha \in L$ et $Q_\alpha \in F[X]$ le polynôme minimal de α sur F. Soit β une racine de Q_α, alors β est aussi racine de $P_\alpha \in K[X]$, donc $\beta \in L$ (car L/K est normale). ■

Contre-exemple. ***(Normalité par intercalation)***

Même exemple que précédemment. □

Contre-exemple. ***(Tour d'extensions et normalité)***

Pour $L = \mathbb{Q}(\sqrt[4]{2})$, $F = \mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}$, on a L/F et $F/\mathbb{Q}$ normales, pourtant, $L/\mathbb{Q}$ n'est pas normale car $i\sqrt[4]{2} \notin \mathbb{Q}(\sqrt[4]{2})$. □

Propriété. ***(Normalité du composé)***

On reprend les notations du compositum. Si L_1/K est normale, alors L_1L_2/L_2 est normale. Si de plus L_2/K est normale, alors L_1L_2/K est normale.

▷ Si L_1/K est normale, alors L_1 est le corps de décomposition d'un certain $P = \prod(X - \alpha_i) \in K[X]$ (on l'a déjà vu !), soit $L_1 = K(\alpha_1,...,\alpha_d)$. Ainsi $L_1L_2 = L_2(\alpha_1,...,\alpha_d)$ est le corps de décomposition de P sur L_2 donc L_1L_2/L_2 est normale. Si de plus L_2/K est normale, L_2 est le corps de décomposition d'un $Q = \prod(X - \beta_j)$ et $L_2 = K(\beta_1,...,\beta_c)$. Ainsi $L_1L_2 = K(\alpha_1,...,\alpha_d, \beta_1,...,\beta_c)$ grâce à $PQ = \prod(X - \alpha_i)\prod(X - \beta_j) \in K[X]$. Voilà. ■

Heuristique

Quitte à rajouter des éléments, on peut toujours rendre une extension normale. Par contre, c'est impossible pour une extension qui n'est pas séparable, car le polynôme minimal divise celui de la sur-extension, dans si un morceau est inséparable, c'est râpé.

4.1.10.2 Théorème de l'élément primitif

On vérifie que sous certaine condition toute extension se ramène à une *extension simple*.

Proposition. ***(Théorème de l'élément primitif, cas des corps finis)***

Soit K un corps fini de caractéristique p. Alors il existe $\alpha \in K$ tel que $K = \mathbb{F}_p(\alpha)$.

▷ En effet, le groupe multiplicatif d'un corps est cyclique. Soit α l'un de ses générateurs du groupe multiplicatif de K (soit un élément *primitif*, d'où la terminologie). Alors clairement $K = \mathbb{F}_p(\alpha)$, d'où le résultat. ■

On montre maintenant un théorème plus général.

Théorème. ***(Caractérisation des extension simples)***

Une extension finie est simple si et seulement si elle n'a qu'un nombre fini de sous-extensions.

▷ Démontré dans le partiel. (La technique est classique : on introduit deux extensions dont l'une est inclus dans l'autre, et on montre qu'elles ont le même degré.) ■

Remarque. En écrivant $L = K(\alpha_1,...,\alpha_n)$, il existe même une combinaison des α_i qui avec K engendre L.

Théorème. ***(Théorème de l'élément primitif)***

Soit L/K une extension finie de corps, de degré n. Alors Si L/K est séparable, il existe $\alpha \in L$, tel que $L = K(\alpha)$. On dit aussi de L/K est *simple* et que α est un élément *primitif*.

▷ Montrons simplement qu'une extension finie séparable n'admet qu'un nombre fini de sous-extensions. Si L/K est séparable, il existe $\sigma_1, ..., \sigma_n : L \longrightarrow \overline{K}$ avec $\sigma_i \in \mathrm{Hom}_K(L, \overline{K})$ distincts, donc linéairement indépendants par le lemme d'Artin. Choisissons $\alpha \in L$ tel que $\forall i \neq j$, $\sigma_i(\alpha) \neq \sigma_j(\alpha)$, si cela est possible. Montrons que $L = K(\alpha)$. Soit P_α le polynôme minimal de α sur K. Alors chaque $\sigma(\alpha)$ est racine de P_α où $\sigma \in \mathrm{Hom}_K(L, \overline{K})$, donc $\deg(P_\alpha) \geqslant n$, donc $[K(\alpha) : K] = \deg(P_\alpha) \geqslant n$. Mais $[K(\alpha) : K] \leqslant [L : K] = n$, donc l'égalité vient partout, et $K(\alpha) = L$. Autrement, on voit que si V est un K-espace vectoriel de dimension finie, avec K infini. Alors si les V_i sont des sous-espaces vectoriels propres, $\bigcup_{i=1}^{n} V_i \subsetneq V$. Prenons ici $V = L$, et $V_{i,j} = \{x \in L, \sigma_i(x) = \sigma_j(x)\}$. C'est un K-sev de V. On choisit $\alpha \notin \bigcup_{i \neq j} V_{i,j}$ et tout est fait. ■

Méthode. ***(Trouver l'élément primitif d'une extension finie séparable)***

Soit L/K une telle extension. Si l'on sait trouver une base de L sur K, on peut trouver α_1,...,α_n telles que $L = K(\alpha_1,...,\alpha_n)$.

1. Si K est fini, et donc L/K, il s'agit de trouver un générateur du groupe multiplicatif d'un corps. Pour cela, on suit la preuve (constructive) donnée dans ce document : on construit à partir de deux éléments un autre d'ordre le ppcm de leurs ordres (que l'on peut toujours déterminer à la main si l'on sait calculer dans ce cas), puis de proche en proche, un élément d'ordre l'exposant du groupe.
2. Sinon, K est infini, et $K(\alpha_1, \alpha_2)$ est une sous-extension de L/K, donc n'a qu'un nombre fini de sous-extensions. Il existe donc pour λ parcourant K des extensions $K(\alpha_1 + \lambda\alpha_2) = K(\alpha_1 + \lambda'\alpha_2)$ (non constructivement, il faut creuser...). Mais puisque :

$$\beta = \frac{(\alpha_1 + \lambda\alpha_2) - (\alpha_1 + \lambda'\alpha_2)}{\lambda - \lambda'} \text{ et } \alpha_1 = \frac{\lambda(\alpha_1 + \lambda'\alpha_2) - \lambda(\alpha_1 + \lambda\alpha_2)}{\lambda - \lambda'},$$

$K(\alpha_1, \alpha_2) = K(\alpha_1 + \lambda\alpha_2)$. De proche en proche, on construit l'élément primitif

$$\alpha_1 + \lambda_1^{(\alpha_1,\alpha_2)}\alpha_2 + \lambda_1^{(\alpha_1 + \lambda_1^{(\alpha_1,\alpha_2)}\alpha_2, \alpha_3)}\alpha_3 + ... + \lambda_1^{(\alpha_1 + \lambda_1^{(\alpha_1,\alpha_2)}\alpha_2 + \lambda_1^{(\alpha_1 + \lambda_1^{(\alpha_1,\alpha_2)}\alpha_2, \alpha_3)}\alpha_3 + ... \cdot \alpha_{n-1}, \alpha_n)}\alpha_n.$$

Contre-exemple. ***(Extension finie séparable non primitive)***

On a longuement développé, dans les exemples d'extensions non séparables, une étude de cas. Remarquons que cette extension est très inséparable.
De plus, le théorème précédent assure que l'on ne peut trouver de contre-exemple qu'en caractéristique positive. □

4.1.11 Extension galoisienne

Définition. ***(Extension galoisienne)***

Soient L/K deux corps, on dit que L/K est *galoisienne* si elle est finie et si elle est normale et séparable, autrement dit (ça devrait être clair maintenant !), si $\#\mathrm{Hom}_K(L,L) = [L : K]$.

Remarque. Si L/K est finie, un morphisme valant l'identité sur K est une application K-linéaire. Comme elle est toujours injective comme morphisme de corps, elle est toujours un automorphisme si c'est un endomorphisme.

Exercice 101

Donner un endomorphisme de corps non bijectif.

▷ **Éléments de réponse.**

Soit $\mathbb{C}(X) \longrightarrow \mathbb{C}(X)$, $F \mapsto F(X^2)$. Remarque : comment montrer que $F \mapsto F(X^2)$ de $\mathbb{C}[X] \to \mathbb{C}[X]$ est injective ?

Avec les considérations précédentes, on peut sans problème énoncer la caractérisation suivante :

Propriété. ***(Caractérisation de la galoisiennité en dimension finie)***

Supposons L/K finie. Alors L/K est galoisienne si et seulement si $|\mathrm{Aut}(L/K)| = [L : K]$.

▷ En effet, $\mathrm{Aut}(L/K) = \mathrm{Hom}_K(L,L) \hookrightarrow \mathrm{Hom}_K(L,\overline{K})$, avec égalité si et seulement si L/K est normale, et $\#\mathrm{Hom}_K(L,\overline{K}) \leqslant [L : K]$ avec égalité si et seulement si L/K est séparable. ■

4.2 Théorie de Galois

4.2.1 Contexte historique : résolution d'équations par radicaux. Équations de petit degré

Étant donné un polynôme P de degré n, on sait qu'il admet n racines complexes. Les exprimer en fonctions des paramètres du polynôme, c'est-à-dire ses coefficients, n'est pas chose simple.

4.2.1.1 Trinôme du second degré

On considère une équation de la forme $X^2 + aX + b = 0$. On peut factoriser $(X + \frac{a}{2})^2 = -b + \frac{a^2}{4} = \frac{a^2-4b}{4}$ d'où deux racines $\alpha_1 = \frac{-a+\sqrt{a^2-4b}}{2}$ et $\alpha_2 = \frac{-a-\sqrt{a^2-4b}}{2}$. On remarque qu'il faut se placer sur un corps de caractéristique différente de 2.

4.2.1.2 Équations de degré 3

On considère maintenant $X^3 + aX^2 + bX + c = 0$. Intuitivement, on va devoir maintenant utiliser des racines triples. En fait, on peut se ramener à $X^3 + pX + q = 0$ (exercice) ; soient α_1,α_2, α_3 les racines de ce dernier quadrinôme. Les relations de Viète donnent :

$$\begin{cases} \alpha_1 + \alpha_2 + \alpha_3 = 0 \\ \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = p \\ \alpha_1\alpha_2\alpha_3 = -q. \end{cases}$$

On pose $j = \frac{-1+\sqrt{-3}}{2}$ de sorte que $1 + j + j^2 = 0$. On introduit :

$$A_1 = (\alpha_1 + j\alpha_2 + j^2\alpha_3)^3 A_2 = (\alpha_1 + j^2\alpha_2 + j\alpha_3)^3.$$

En posant $\tau = (2,3)$ et $\sigma = (1,2,3)$, on voit que clairement $\tau(A_1) = A_2$ et $\sigma(A_1) = A_1$, puisque $j^6 = 1$. Ainsi, le théorème des polynômes symétriques donne que $A_1 + A_2 = \text{pol}(p,q) = -27q$ et $A_1A_2 = \text{pol}(p,q) = -27p^3$[1].

[1] Explicitons ce calcul, c'est intéressant ; c'est le plus simple des deux. On a :

$$\begin{aligned} &(\alpha_1 + j\alpha_2 + j^2\alpha_3)(\alpha_1 + j^2\alpha_2 + j\alpha_3) \\ =&\alpha_1^2 + j^2\alpha_1\alpha_2 + j\alpha_1\alpha_3 \\ &\alpha_2^2 + j\alpha_1\alpha_2 \quad + j^2\alpha_2\alpha_3 \\ &\alpha_3^2 \quad + j^2\alpha_1\alpha_3 + j\alpha_2\alpha_3 \\ =&(\alpha_1 + \alpha_2 + \alpha_3)^2 - 2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) - (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) \\ =&-3p. \end{aligned}$$

On considère $(Y-A_1)(Y-A_2) = Y^2 + 27qY - 27p^3$. En posant $\pm D = (27q)^2 - 4(-27p^3) = 27(4p^3 + 27q^2)$ le discriminant de ce trinôme du second degré, on obtient $A_1 = \frac{-27q+\sqrt{D}}{2}$ et $A_2 = \frac{-27q-\sqrt{D}}{2}$. En posant $\beta_1 = \alpha_1 + j\alpha_2 + j^2\alpha_3 = \sqrt[3]{A_1}$ et $\beta_2 = \alpha_1 + j^2\alpha_2 + j\alpha_3 = \sqrt[3]{A_2}$, avec donc $\beta_1\beta_2 = -3p$ et $\alpha_1 + \alpha_2 + \alpha_3 = 0$, d'où

$$\begin{cases} \alpha_1 = \frac{1}{3}(\sqrt[3]{A_1} + \sqrt[3]{A_2}) \\ \alpha_2 = \frac{1}{3}(j^2\sqrt[3]{A_1} + j\sqrt[3]{A_2}) \\ \alpha_3 = \frac{1}{3}(j\sqrt[3]{A_1} + j^2\sqrt[3]{A_2}) \end{cases}$$

par symétrie. On remarque que ces formules ne valent plus sur un corps de caractéristique 3.

Remarquons que si $D < 0$, alors toutes les racines sont réelles. C'est un peu curieux d'introduire un complexe pour la résoudre dans ce cas, mais en fait, non.

4.2.1.3 Méthode de Descartes pour les équations du quatrième degré

Un siècle après les Italiens ayant, aux XV$^{\text{e}}$, XVI$^{\text{e}}$ siècles, obtenu les formules précédentes, on a pu les obtenir au degré 4. De la même manière que précédemment, on peut se ramener toujours à une équation de la forme $P = X^4 + pX^2 + qX + r = 0$. On veut exprimer ses racines α_1,α_2,α_3,α_4 avec $\sqrt{}$ et $\sqrt[3]{}$ (puisque la racine quatrième est la composée de deux racines carrées).

On factorise $P = (X^2 + aX + b)(X^2 - aX + c) = X^4 + X^2(c - a^2 + b) + X(ac - ab) + bc$ où

$$\begin{cases} b + c - a^2 = p \\ a(c - b) = q \\ bc = r. \end{cases}$$

Si $q = 0$, on résout avec la racine carrée. Sinon, $b + c = p + q^2$ et $c - b = q/a$ si tant est que $a \neq 0$. Dans ce cas, $c = \frac{1}{2}(p + a^2 + q/a)$ et $b = \frac{1}{2}(p + a^2 - q/a)$. Mais alors $\frac{1}{4}((p + a^2)^2 - \frac{q^2}{a^2}) = r$ et $\frac{1}{4}(p^2a^2 + 2pa^4 + a^6 - q^2 - ra^2) = 0$. Autrement dit, $Q(a^2) = 0$ où Q est un polynôme de degré 3. On exprime 3 solutions a^2 à l'aide de p,q,r grâce à la méthode précédente en racines carrées et cubiques. On trouve a grâce à une simple racine carrée, puis b et c. Reste à résoudre $X^2 + aX + b = 0$ et $X^2 - aX + c = 0$, ce que l'on sait faire.

4.2.1.4 Et après ?

Naturellement, la prochaine étape est de résoudre l'équation de degré 5. En fait, les mathématiciens ont planché là-dessus pendant deux siècles avant qu'un jeune roquet démontre que c'était impossible. Formalisons cette idée.

On définit l'assertion *résoudre par radicaux* $\sqrt{}, \sqrt[3]{}, \sqrt[5]{}$. Soient

$$\mathbb{Q} \subseteq K_1 \subseteq ... \subseteq K_r, K_i \text{ corps et } K_{i+1} = K_i(\sqrt[n_i]{a_i}), n_i \in \mathbb{N}^*, a_i \in K_i.$$

On dit que $P \in \mathbb{Q}[X]$ est résoluble par radicaux s'il existe une telle suite de K_i avec α_1,...,α_n racine de P dans K_2.

Galois a démontré le théorème suivant : pour $P \in \mathbb{Q}[X]$, $P = (X - \alpha_1)...(X - \alpha_n)$, $L = \mathbb{Q}(\alpha_1,...,\alpha_n)$, $G = \{f \in \text{Aut}(L) \mid f_{|\mathbb{Q}} = id_{\mathbb{Q}}$. Alors P est résoluble par radicaux, si et seulement si, G est résoluble.

Or en général[1], si $\deg(P) = n$, on a $G \simeq S_n$. Or $n \leqslant 4$, S_n est résoluble ; si $n \geqslant 5$, S_n est non résoluble.

4.2.2 Prérequis

Lemme. ***(Lemme de l'extension)***

Soit $f : K \longrightarrow L$ un homomorphisme de corps. Alors L est une extension de K, en effet, K s'identifie à un sous-corps de L.

Exemple

On a $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{C}, \mathbb{Q}(j\sqrt[3]{2}) \subseteq \mathbb{C}$ et $\mathbb{Q}(\sqrt[3]{2}) \simeq \mathbb{Q}(j\sqrt[3]{2})$. Il serait pourtant dangereux d'identifier tout à fait ces deux objets !

Lemme. ***(Lemme de la caractéristique)***

Il n'existe aucun homomorphisme entre des corps de caractéristiques distinctes, autrement dit, l'extension de corps préserve la caractéristique.

Lemme. ***(Théorème de Cayley)***

Tout groupe est isomorphe à un sous-groupe d'un groupe de permutations.

Ceci explique l'intérêt que l'on porte aux groupes de permutations. Tout groupe s'écrit sous cette forme (même si ce n'est pas toujours la meilleure façon de le voir !).

[1] Bien sûr, $X^{124} - a$ est résoluble par radicaux, mais c'est une équation très particulière.

4.2.3 Corps de Galois

Définition. ***(Groupe de Galois)***

Soient L/K deux corps ; on suppose L/K galoisien. Alors on note $\mathrm{Gal}(L/K) = \mathrm{Aut}(L/K)$ le *groupe de Galois* de L/K, avec $\mathrm{Hom}_K(L,L) := \mathrm{Aut}(L/K) = \{f : L \longrightarrow L, f_{|K} = id\}$.

En regardant la preuve de la caractérisation de la galoisiennité, on observe que dans le cas d'une extension normale, tout morphisme vérifie $f(L) = L$. Puisqu'un morphisme de corps est toujours injectif, on en déduit que $\mathrm{Hom}_K(L,L) = \mathrm{Aut}_K(L)$.

Introduisons la notion suivante.

Propriété. ***(Sous-groupe des automorphismes)***

Soit L/K une extension de corps. Soit $H \subseteq \mathrm{Aut}(L)$. On pose $L^H = \{x \in L \mid \forall \sigma \in H, \sigma(x) = x\} = \bigcap_{\sigma \in H} \mathrm{Ker}(\sigma - id_L)$; c'est un sous-corps de L.

▷ En effet, $0_L, 1_L \in L^H$, et si $x \neq 0, y \in L^H$, alors $x \pm y, xy, x^{-1} \in L^H$, car $\sigma(x \pm y) = \sigma(x) + \sigma(y) = x + y$, de même pour le reste. ■

Propriété

Si $H_1 \subseteq H_2 \subseteq \mathrm{Aut}(L)$, $L^{H_2} \subseteq L^{H_1}$.

De façon opératoire, on arrive à obtenir le résultat suivant :

Propriété. ***(Intercalation d'extensions galoisiennes)***

Soient $L/F/K$ des extensions de corps. Si L/K est galoisienne, alors L/F est galoisienne (mais F/K n'est pas toujours normale !).
De plus, on a $\mathrm{Gal}(L/F) = \{\sigma : L \longrightarrow L, \forall x \in F, \sigma(x) = x\} \subseteq \mathrm{Gal}(L/K) = \{\sigma : L \longrightarrow L, \forall x \in K, \sigma(x) = x\}$ avec l'identification canonique : $\mathrm{Gal}(L/F) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma_{|F} = id_F\}$. Ainsi, $\mathrm{Gal}(L/F)$ est un sous-groupe de $\mathrm{Gal}(L/K)$ (là aussi, l'ordre est renversé).

4.2.4 Correspondance de Galois

Voilà une très jolie correspondance qui constitue le cœur de la théorie.

On ne s'intéresse pour l'instant qu'aux extensions finies !

Théorème. ***(Théorème fondamental de la théorie de Galois)***

Soit L/K une extension de corps finie et galoisienne, soit $G = \mathrm{Gal}(L/K)$. Alors

$$\begin{aligned} \{\text{sous-groupes de } G\} &\longleftrightarrow \{\text{sous-extensions de } L/K\} \\ H &\longmapsto L^H \\ \mathrm{Gal}(L/F) &\longleftarrow\!\shortmid F \text{ avec } K \subseteq F \subseteq L) \end{aligned}$$

sont des bijections réciproques.

De plus, cette correspondance vérifie les énoncés suivants :

1. Si $K \subseteq F \subseteq L$ et $\sigma \in G$, $\mathrm{Gal}(L/\sigma(F)) = \sigma\mathrm{Gal}(L/K)\sigma^{-1}$. De plus, F/K est normale si et seulement si $\mathrm{Gal}(L/F) \triangleleft \mathrm{Gal}(L/K)$. Si c'est le cas, $\begin{aligned} \mathrm{Gal}(L/K) &\longrightarrow \mathrm{Gal}(F/K) \\ \rho &\longmapsto \rho_{|F} \end{aligned}$ induit $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/F) \xrightarrow{\sim} \mathrm{Gal}(F/K)$.
2. Il y a décroissance et décroissante réciproque pour ces ordres : $H_1 \subseteq H_2 \iff L^{H_2} \subseteq L^{H_1}$, en inversant, attention.
3. Cette correspondance est un isomorphisme de treillis, car si $F_1 = L^{H_1}$ et $F_2 = L^{H_2}$, alors $F_1 \cap F_2 = L^{\langle H_1, H_2\rangle}$ et $F_1F_2 = L^{H_1 \cap H_2}$.
4. *(Second théorème d'isomorphisme)* Si L_1/K est galoisien, L_2/K quelconque, toutes deux sous-extensions de $\overline{K}$, alors L_1L_2/L_2 est galoisienne et $\mathrm{Gal}(L_1L_2/L_2) \simeq \mathrm{Gal}(L_1/(L_1 \cap L_2) \subseteq \mathrm{Gal}(L_1/K)$.
5. Elle respecte le compositum. En effet, si L_1/K et L_2/K sont galoisiennes (dans $\overline{K}$) alors L_1L_2/K est galoisienne et $\mathrm{Gal}(L_1L_2/K)$ est un sous-groupe de $G_1 \times G_2$, avec $\mathrm{Gal}(L_1L_2/K) \simeq G_1 \times G_2$ si et seulement si $L_1 \cap L_2 = K$.

▷ Il faut montrer : H donne L^H donne $\mathrm{Gal}(L/L^H) = H$, et F donne $\mathrm{Gal}(L/F)$ donne $L^{\mathrm{Gal}(L/F)} = F$.

Remarquons que, par le théorème de l'élément primitif, si L/K est finie galoisien, donc séparable, il existe $\alpha \in L$, tel que $L = K(\alpha)$.

Montrons la première compatibilité. Soit $\mathrm{Gal}(L/L^H) = \{\sigma \in G \mid \forall x \in L^H \quad \sigma(x) = x\}$. En effet, par définition, $\forall x \in L^H \ \forall \sigma \in H \quad \sigma(x) = x$. Introduisons $Q = \prod_{\sigma \in H} (X - \sigma(\alpha))$. A priori, $Q \in L[X]$, mais en fait, $Q \in L^H[X]$, en effet $\forall \sigma \in H$, $\sigma Q = Q$. En effet $\sigma Q = \sigma(\prod_{\tau \in H} (X - \tau(\alpha))) = \prod_{\tau \in H} (X - \sigma\tau(\alpha)) = \prod_{t' \in H} (X - \tau'(\alpha)) = Q$. Soit P le polynôme minimal de α sur le corps L^H. Or $L = K(\alpha)$ donc $L^H(\alpha) = L$ donc $[L : L^H] = [L^H(\alpha) : L^H] = \deg(P)$. Or P divise Q. Donc $\deg(P) \leqslant \deg(Q) = |H|$, donc $|\mathrm{Gal}(L/L^H)| = [L : L^H] \leqslant |H|$. Comme $H \subseteq \mathrm{Gal}(L/L^H)$, on a $H = \mathrm{Gal}(L/L^H)$.

Montrons maintenant la deuxième partie. On a $F \subseteq L^{\mathrm{Gal}(L/F)}$, en effet, $\mathrm{Gal}(L/F) = \{\sigma \in G \mid \forall x \in F \quad \sigma(x) = x\}$ donc si $x \in F$, $\sigma \in \mathrm{Gal}(L/F)$, $\sigma(x) = x$. On a aussi $|\mathrm{Gal}(L/F)| = [L : F] = [L : L^{\mathrm{Gal}(L/F)}] = |\mathrm{Gal}(L/F)$, car les extensions L/F et $L/L^{\mathrm{Gal}(L/F)}$, d'où l'égalité $F = L^{\mathrm{Gal}(L/F)}$. Ainsi la correspondance est démontrée.

Soient $K \subseteq F \subseteq L$, $G = \mathrm{Gal}(L/K) \ni \sigma$. Alors $\tau \in \mathrm{Gal}(L/\sigma(F)) \iff \tau \in G$ et $\forall x' \in$

$\sigma(F) \quad \tau(x') = x' \iff \forall x \in F \quad \tau(\sigma(x)) = \sigma(x) \iff \forall x \in F \quad (\sigma^{-1}\tau\sigma)(x) = x \iff \sigma^{-1}\tau\sigma \in \mathrm{Gal}(F/K) \iff \tau \in \sigma\mathrm{Gal}(L/F)\sigma^{-1}$. En conclusion, on a l'identité de conjugaison proposée. Comme corollaire, on trouve que F/K est normale ssi $\mathrm{Gal}(L/F)$ est distinguée dans G. En effet, si F est normale, alors $\forall\sigma \in G \quad \sigma(F) = F$ et donc $\mathrm{Gal}(L/\sigma(F)) = \mathrm{Gal}(L/F) = \sigma\mathrm{Gal}(L/F)\sigma^{-1}$, donc il est distingué. Réciproquement, si $\mathrm{Gal}(L/F) \triangleleft G$, $\mathrm{Gal}(L/\sigma(F)) = \mathrm{Gal}(L/F)$, donc $\sigma(F) = F$, donc F est normale sur K donc galoisienne sur K. Supposons maintenant F/K normale, galoisienne. Alors

$$\begin{array}{ccc} G = \mathrm{Gal}(L/K) & \xrightarrow{r} & \mathrm{Gal}(F/K) \\ \sigma & \longmapsto & res_F(\sigma) \end{array}$$

est un homomorphisme de groupes, car $res_F(\sigma \circ \tau) = res_F(\sigma) \circ res_F(\tau)$ si elles sont bien définies. Or $\mathrm{Ker}(r) = \{\sigma \in G \mid \sigma_{|F} = id_F\} = \mathrm{Gal}(L/F)$, d'où une injection $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/F) \hookrightarrow \mathrm{Gal}(F/K)$. Il suffit de montrer la surjectivité. Il y a au moins deux méthodes : soit l'on remarque que $|\mathrm{Gal}(L/K)/\mathrm{Gal}(L/F)| = \frac{[L:K]}{[L:F]} = [F : K]$, d'où $|\mathrm{Gal}(F/K)| = [F : K]$. Sinon, on utilise le lemme de prolongement :

$$\begin{array}{ccc} L & \xrightarrow{\tilde{\sigma}} & \overline{K} \\ | & & | \\ F & \xrightarrow{\sigma} & F \\ | & & | \\ K & = & K \end{array}$$

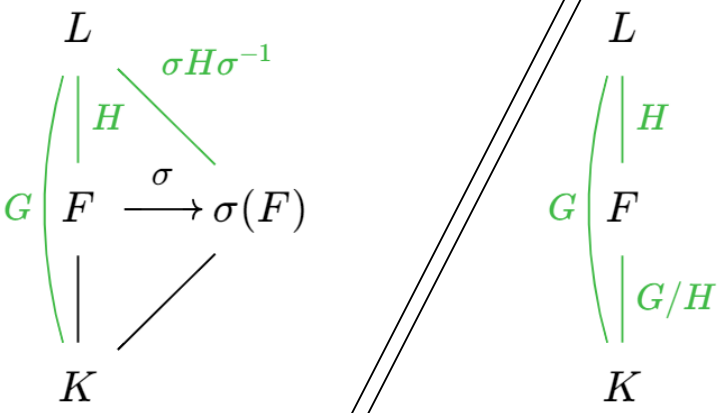
et comme L/K est normale, $\tilde{\sigma}(L) = L$.

Par définition, si $H_1 \subseteq H_2$, si $x \in L^{H_2}$, $\forall\sigma \in H_2 \quad \sigma(x) = x$, donc $\forall\sigma \in H_1 \quad \sigma(x) = x$, soit $x \in L^{H_1}$. Réciproquement, si $L^{H_2} \subseteq L^{H_1}$, alors $\mathrm{Gal}(L/L^{H_1}) = H_1 \subseteq \mathrm{Gal}(L/L^{H_2}) = H_2$: nommément, si $\forall x \in L^{H_1} \quad \sigma(x) = x$, alors $\forall x \in L^{H_2} \quad \sigma(x) = x$, donc si σ appartient au premier, il appartient au second.

Montrons la compatibilité des treillis. Si $\sigma \in H_1 \cap H_2$, σ fixe tous les éléments de F_1 et $F82$, donc les éléments de F_1F_2. Or $H_1 \cap H_2 \subseteq \mathrm{Gal}(L/F_1F_2)$ donc $F_1F_2 \subseteq L^{H_1 \cap H_2}$. Si maintenant σ fixe les éléments de F_1F_2, c'est-à-dire $\sigma \in \mathrm{Gal}(L/F_1F_2)$, alors σ fixe les éléments de F_1, soit $\sigma \in H_1$, et les éléments de F_2, soit $\sigma \in H_2$, donc $\mathrm{Gal}(L/F_1F_2) \subseteq H_1 \cap H_2$, donc $L^{H_1 \cap H_2} \subseteq L^{\mathrm{Gal}(L/F_1F_2)} = F_1F_2$ donc $x \in F_1$ et F_2 ; alors il est fixé par tout élément de H_1 et H_2, donc par tout élément de $\langle H_1, H_2\rangle$. Donc $F_1 \cap F_2 \subseteq L^{\langle H_1,H_2\rangle}$. Or $H_1 \subseteq \langle H_1,H_2\rangle \subseteq L^{H_1} = F_1$, idem dans F_2, donc $L^{\langle H_1,H_2\rangle} \subseteq F_1 \cap F_2$, d'où l'égalité.

On définit un homomorphisme de groupes $r : \mathrm{Gal}(L_1L_2/L_2) \simeq \mathrm{Gal}(L_1/L_2 \cap L_1) \subseteq \mathrm{Gal}(L_1/K)$, par $\sigma \longmapsto \sigma_{|L_1}$. Il est injectif : soit $\sigma \in \mathrm{Gal}(L_1L_2/L_2)$, tel que $\sigma_{|L_2} = id_{L_2}$. Si $\sigma \in \mathrm{Ker}(r)$, alors $\sigma_{|L_1} = id_{L_1}$, d'où $\sigma = id_{L_1L_2}$. Pour montrer la surjectivité de la première injection, c'est le lemme de prolongement des morphismes. Plus explicitement, σ est déterminé par ses valeurs sur L_2 et L_1, c'est automatique. Observons que si $\sigma \in \mathrm{Gal}(L_1L_2/L_2)$, alors $\sigma_{|L_1 \cap L_2} = id_{L_1 \cap L_2}$ donc l'image de r est incluse dans $\mathrm{Gal}(L_1/L_1 \cap L_2)$.

Pour le dernier point, la fonction $r = (r_{L_1}, r_{L_2}) : \sigma \longmapsto (res_{L_1}\sigma, res_{L_2}\sigma)$ est bien définie. C'est un homomorphisme : $res_{L_1}(\sigma \circ \tau) = res_{L_1}(\sigma) \circ res_{L_1}(\tau)$, car $\sigma(L_1) \subseteq L_1$, $\tau(L_1) \subseteq L_1$. Il est injectif, car de même que précédemment, σ est déterminé par ses valeurs sur L_1 et L_2. On rappelle le lemme : $[L_1L_2 : K] \leqslant \frac{[L_1:K][L_2:K]}{[L_1 \cap L_2:K]}$. Si $L_1 \cap L_2 \neq K$, alors $|\mathrm{Gal}(L_1L_2/K)| = [L_1L_2 : K] < [L_1 : K][L_2 : K] = |\mathrm{Gal}(L_1/K)| \times |\mathrm{Gal}(L_2/K)|$. Si maintenant $L_1 \cap L_2 = K$, alors $\mathrm{Gal}(L_1L_2/K) \xrightarrow{r} \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$ se réécrit $\mathrm{Gal}(L_1L_2/L_2) \longrightarrow \mathrm{Gal}(L_1/K) \times \{id_{L_2}\}$. Par le quatrième point,



son image est $\mathrm{Gal}(L_1/L_1 \cap L_2) = \mathrm{Gal}(L_1/K)$. On obtient donc que $\mathrm{Gal}(L_1/K) \times \{id_{L_2}\}$ est contenu dans l'image de r. Par un raisonnement symétrique, $\{id_{L_1}\} \times \mathrm{Gal}(L_2/K)$ est aussi contenu dans l'image de r, qui est donc égale au produit des deux groupes. ■

Remarques.

1. En reformulant la première phrase de l'énoncé, on obtient les identités utiles : $\mathrm{Gal}(L/L^H) = H$ et $L^{\mathrm{Gal}(L/F)} = F$. En particulier, pour $|G| = [L : K]$ et $[L : L^H] = |H|$, on a $[L : L^H] = \frac{[L:K]}{[L:L^H]} = \frac{|G|}{|H|} = (G : H)$.
2. On en déduit que l'ensemble des sous-extensions de L/K est fini, ce qui est non trivial.
3. On obtient, d'après la première propriété, la simplification du diagramme suivant en le second diagramme dans le cas normal :
4. *(Groupe de Galois d'un polynôme séparable)* Voici une des grandes applications de la théorie de Galois, celle donnée par Galois dans son mémoire. Soit $P = \prod_{i=1}^{n}(X - \alpha_i) \in K[X]$ séparable. Soit $L = K(\alpha_1,...,\alpha)/K$ le corps de décomposition de P sur K, alors L/K est galoisienne (dire pourquoi). Dans ce cas, $\mathrm{Gal}(L/K)$ s'appelle le *groupe de Galois du polynôme* P sur K.
   Hâtivement, on peut exprimer les racines avec $\sqrt{\cdot}$, $\sqrt[3]{\cdot}$, et $K \subseteq K_1 \subseteq ... \subseteq K_n$ avec $L \subseteq K_n$, $K_{i+1} = K_i(\sqrt[n_i]{\alpha_i})$, ce qui équivaut à G_P résoluble.
   Alors G agit sur $\{\alpha_1,...,\alpha_n\}$ l'ensemble des racines de P. En effet, $G \times R \longrightarrow R$ définie par $(\sigma, \alpha) \mapsto \sigma(\alpha)$ correspond au morphisme structurel $G \hookrightarrow \mathrm{Bij}(\mathbb{R}) \simeq S_n$.

4.2.5 Illustration de la correspondance galoisienne

4.2.5.1 Groupe de Galois d'un polynôme

Propriété. ***(Action du groupe de galois sur l'ensemble des racines)***

Le groupe de Galois d'un polynôme agit fidèlement sur l'ensemble de ses racines.
En particulier, le groupe de Galois d'un polynôme s'identifie à un sous-groupe du groupe des permutations des racines de ce polynôme.

▷ Déjà vu, dans la section précédente. Pour la fidélité, c'est très simple : l'intersection des stabilisateurs est réduite au nul puisque si σ stabilise toutes les racines de P, alors elle stabilise tous les éléments de $K(\alpha_1,...,\alpha_n)$, donc c'est l'identité ! ■

Propriété. ***(Transitivité de l'action du groupe de Galois)***

Le groupe de Galois d'un polynôme séparable agit transitivement sur l'ensemble de ses racines, si et seulement si, ce polynôme est irréductible. De plus, si un polynôme est seulement irréductible, son groupe de Galois agit transitivement.
En outre, le nombre d'orbites de l'action du groupe de Galois d'un polynôme séparable est le nombre de ses facteurs irréductibles.

▷ Supposons P irréductible ; on peut le supposer unitaire. Soient α, β deux racines de P. Puisque P est irréductible unitaire, on a $\mu_{\alpha,K} = P$. D'après le théorème de prolongement, il existe un plongement $\sigma_\beta : K(\alpha) \longrightarrow \overline{K}$ tel que $\sigma_\beta(\alpha) = \beta$. Ce plongement se prolonge alors en un plongement de $L \longrightarrow \overline{K}$. Comme L/K est normale, $\sigma \in \mathrm{Gal}_K(P)$. Par construction, $\sigma(\alpha) = \beta$, et l'action est bien transitive.

Supposons maintenant que P soit séparable. Si P n'est pas irréductible, il possède au moins deux facteurs irréductibles unitaires distincts Q,R. Soit X l'ensemble des racines de Q dans L et X' de R dans L. Par hypothèse sur P, ces deux sous-ensembles sont disjoints. Par le fait précédent, tout élément du groupe de Galois stabilise X et X'. On en déduit que l'orbite de toute racine de Q,R est continue dans X, respectivement X'. En particulier, les orbites d'une racine de Q et d'une racine de R sont distinctes, et l'action du groupe de Galois ne peut être transitive. On en déduit le résultat. ■

Remarque. L'action du groupe de Galois d'un polynôme séparable est libre si et seulement si $|G| = [L/K] = n$ (action transitive simplement transitive d'un groupe fini). Cela peut arriver (quand ?)

On souhaite donc étudier la structure de groupe de $\mathrm{Gal}(L/K)$ dans ce cas précis. Puisque c'est un sous-groupe de $\mathfrak{S}_n$, on peut se demander s'il est inclus dans des sous-groupes de $\mathfrak{S}_n$. Foncièrement, il faut s'intéresser à $\mathfrak{A}_n$.

Propriété. ***(Caracatérisation des discriminants carrés)***

Avec les hypothèses précédentes, il existe un polynôme en les coefficients de P, le *discriminant* Δ de P, tel que :

$$G \subseteq \mathfrak{A}_n \iff \Delta \text{ est un carré dans } K^\times.$$

De plus, Δ est un polynôme symétrique en les α_i.

▷ On rappelle que $P = \prod_{i=1}^{n} X - \alpha_i)$ est séparable. Posons $\delta = \prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j)$, puis $\Delta = \delta^2$. Si l'on identifie $G = \mathrm{Gal}(K(\alpha_1,...,\alpha_n)/K)$ a un sous-groupe de $\mathfrak{S}_n$, c'est-à-dire, $\sigma(\alpha_i) = \alpha_{\sigma(i)}$, alors par morphisme $\sigma(\delta) = \varepsilon(\sigma)\delta$, par définition de la signature. Donc pour tout $\sigma \in G$, $\sigma(\Delta) = \Delta$. Donc $\Delta \in K$. Il est également clair que Δ est symétrique en les α_i. Par le théorème fondamental, Δ est engendré par des polynômes symétriques élémentaires en les racines de P. Or ces polynômes élémentaires se retrouvent dans les coefficients de P. Donc Δ est un polynôme en les coefficients de P. Enfin, on a bien $G \subseteq \mathfrak{A}_n \implies \forall \sigma \in G, \varepsilon(\sigma) = 1 \implies \delta \in L^G = K \implies \Delta$ est carré dans K. ■

Remarque. Soit $G = \mathrm{Gal}(L/K) \subseteq \mathfrak{A}_n$, soit G est non inclus dans le groupe alterné d'ordre n. Alors $G_1 = G \cap \mathfrak{A}_n$ est un sous-groupe d'indice 2. Alors :

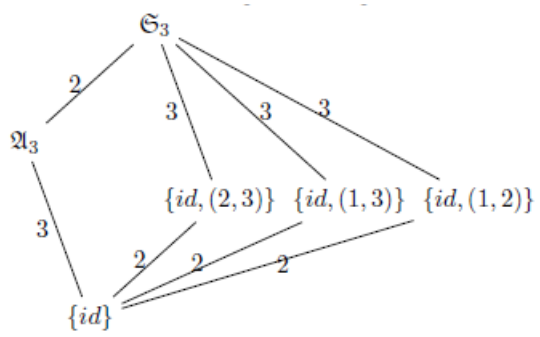
$$\begin{array}{ccc} G & & L^{\{e\}} \\ \subseteq\uparrow & & | \\ G_1 & & L^{G_1} = K(\sqrt{\Delta}) \\ | & & | \\ \{e\} & & L^G \end{array}$$

En effet, on sait que $[L^{G_1} : K] = (G : G_1) = 2$; comme Δ est non carré, $[K(\sqrt{\Delta}) : K] = 2$; $\forall \sigma \in G_1 \quad \sigma(\delta) = \delta$ donc $K(\sqrt{\Delta}) \subseteq L^{G_1}$.

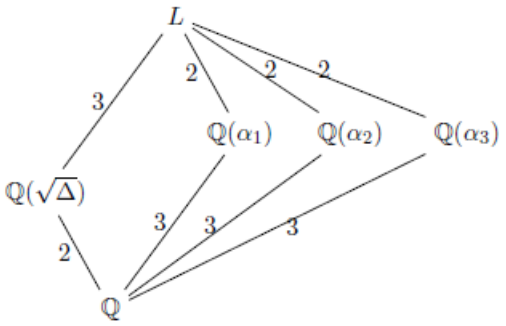
Remarque. Si P est irréductible, alors $n = [K(\alpha) : K]$ divise $[L : K] = |G|$.

Exemple

Prenons $P = X^3 + pX + q$, avec après calcul : $\Delta = -(4p3 + 27q^2)$. Supposons P irréductible, soit $L = K(\alpha_1,...,\alpha_3)$ et $G = \mathrm{Gal}(L/K) \hookrightarrow S_3$, puis $3||6|$. Donc $G = \mathfrak{A}_3 = \mathbb{Z}/3\mathbb{Z}$ ou $\mathfrak{S}_3$, selon que $\Delta =$ ■ ou non. Nous étudions le cas $G = \mathfrak{S}_3$.
Faisons la liste des sous-groupes $H \subseteq \mathfrak{S}_3$. Il y a trois sous-groupes de cardinal 2, engendrés par des transpositions. Au cardinal 3, il n'y a que $\mathfrak{A}_3$ par un théorème célèbre.
On a déjà calculé quelle était l'extension quadratique donnée. Pour les autres, ce sont les $K(\alpha_i)$: en effet, $K(\alpha_i) \subseteq L^{H_i}$ puisque $[K(\alpha_i) : K] = 3$ et $[L^{H_i} : K] = 3$ d'où l'égalité. Avec la théorie de Galois, cette description des sous-extensions n'a rien d'évident. On aurait



(a) *Treillis des sous-groupes de* $\mathfrak{S}_3$ —



(b) *Treillis des sous-extensions de* L/K. —

FIGURE 4.2.1 : Situation précédente

les $K(\alpha_i)$. On aurait même pu montrer qu'elles étaient distinctes. Mais on aurait pas pu savoir que la dernière existait ; il se trouve que, grâce au calcul précédent en remarque, on peut même la décrire.

Exemple

Prenons $K = \mathbb{Q}$, $P = X^4 + 8X + 12$ ou, plus généralement, $P = X^4 + pX^2 + qX + 2$ irréductible. Soit $L = K(\alpha_1,...,\alpha_4)$. Alors supposons comme dans l'exemple concret que $\mathrm{Gal}(L/K) = \mathfrak{A}_4$.

Pour appliquer le théorème de Galois, trouvons tous les sous-groupes de $\mathfrak{A}_4$ qui est de cardinal $12 = 2^2 \times 3$. A priori, un tel sous-groupe H est tel que $|H| = 2,3,4$ ou 6. Or :

- il n'y a pas de sous-groupe de cardinal 6. En effet, il serait d'indice 2 donc distingué, or on a déjà vu que seul le groupe de Klein, de cardinal 4, est distingué dans $\mathfrak{A}_4$.
- Celui-ci, noté $\mathcal{K}$, est le seul sous-groupe d'ordre 4. En effet, c'est un 2-Sylow distingué.
- Pour $|H| = 3$, on peut vérifier que, dans $\mathfrak{A}_4$, un tel groupe est $H = \{id, \sigma, \sigma^2\}$ avec σ un 3-cycle, soit $H_i = \{\sigma \in \mathfrak{A}_4,\ \sigma(i) = i\}$ avec $i = 1$ à 4.

- Enfin, pour $|H| = 2$, il n'y a que les éléments d'ordre 2 qui sont les doubles transpositions du groupe de Klein $\{id, t_1,...,t_3\}$, soit $J_1 = \{id, t_1\},...,$ $J_3 = \{id, t_3\}$.

Dans le diagramme ci-dessous, obtenu grâce aux considérations précédentes, on va identifier $K(\beta_i) = L^{J_i}$, $K(\beta_1^2)$ est $L^{\mathcal{K}}$ où l'on pose $\beta_1 = \alpha_1 + \alpha_2, \beta_2 = \alpha_1 + \alpha_3, \beta_3 = \alpha_1 + \alpha_4$, et l'on a $K(\alpha_i) = L^{H_i}$.

Si $\Sigma \in H_i$, $\sigma(\alpha_i) = \alpha_i$, donc $K(\alpha_i) \subseteq L^{H_i}$. Mais $[K(\alpha_i) : K] = 4$ et $[L^{H_i} : K] = 4$, donc $L^{H_i} = K(\alpha_i)$.

Prenons $J_i = \{id, t_1 = (1,2)(3,4)\}$, soit $t_1(\alpha_1) = \alpha_2$ et $t_1(\alpha_2) = \alpha_1$. Par suite, $t_1(\beta_1) = \beta_1$, donc $K(\beta_1) \subseteq L^{J_1}$. Par ailleurs $[L^{J_1} : K] = 6$. Or, puisque $\binom{4}{2} = 6$, sous l'action de

$G = \mathfrak{A}_4$, $\alpha_1 + \alpha_2$ donne $\alpha_i + \alpha_j$, soit 6 conjugués. Donc $[K(\beta_1) \cdot K] = 6$. Conclusion, $K(\beta_1) = L^{J_1}$. Pour L^{J_2} et L^{J_3}, même conclusion.
Il reste à décrire $L^{\mathcal{K}}$. On a $\mathcal{K} = \langle J_1, J_2 \rangle$, donc $L^{\mathcal{K}} = L^{J_1} \cap L^{J_2} = L^{J_1} \cap L^{J_2} \cap L^{J_3}$. Or $t_1(\beta_1) = \beta_1$, et $t_2(\beta_1) = t_2(\alpha_1) + t_2(\alpha_2) = \alpha_3 + \alpha_4 = -(\alpha_1 + \alpha_2)$, car la somme des racines est supposé nulle (voir la forme supposé de P ; remarquons que ce n'est pas très coûteux). Donc $\beta_1^2 \in L^{\mathcal{K}}$. Donc $K(\beta_1^2) \subseteq L^{\mathcal{K}}$, mais $[L^{\mathcal{K}} : K] = 3$. Or par extension égale ou quadratique, $[K(\beta_1) \cdot K(\beta_1^2)] = 1$ ou 2, d'où $[K(\beta_1^2 : K] = 3$ d'où l'égalité.

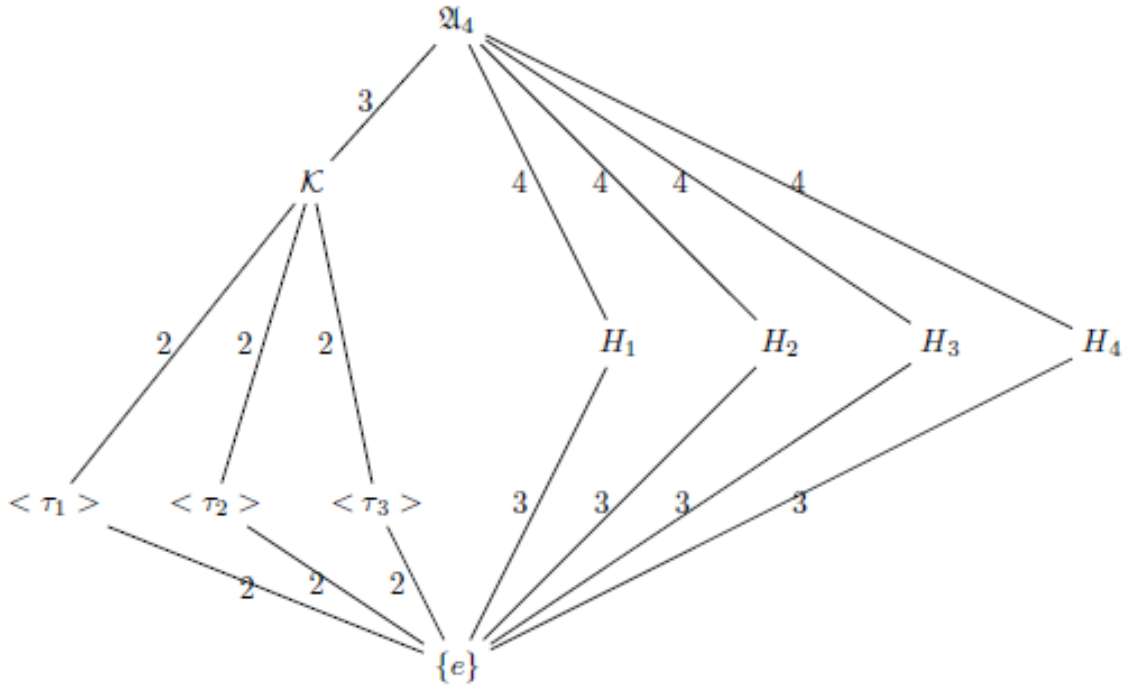


FIGURE 4.2.2 : *Treillis des sous-groupes de* $\mathfrak{A}_4$. —

Exemple

Un autre exemple. Prenons $P = X^5 - 2 \in \mathbb{Q}[X]$, et L son corps de décomposition. Posons $\alpha = \sqrt[5]{2}$ une racine de P et $\zeta = e^{\frac{2\pi i}{5}}$. Alors les racines de P sont les $\zeta^j \alpha$ où $0 \leqslant j \leqslant 4$. Posons $L = \mathbb{Q}(\zeta, \alpha)$. Alors $P_\zeta = X^4 + X^3 + X^2 + X + 1 = \frac{X^5 - 1}{X - 1}$, et $[L : \mathbb{Q}] = 20 = |G|$. On sait que si $\sigma \in G = \mathrm{Gal}(L/\mathbb{Q})$, $\sigma(\alpha) = \zeta^{j(\sigma)}\alpha$ où $j(\sigma) \in \{0,1,2,3,4\}$, et $\sigma(\zeta) = \zeta^{i(\sigma)}$ avec $i(\sigma) \in (\mathbb{Z}/5\mathbb{Z})^\times = \{1,2,3,4\}$. Pour conclure, $\sigma \longmapsto (j(\sigma), i(\sigma))$ est une bijection : c'est la description de G par générateurs. Pour un σ tel que $\sigma(\alpha) = \zeta\alpha$ et $\sigma(\zeta) = \zeta$, et un $\tau(\alpha) = \alpha, \tau(\zeta) = \zeta^2$, on a $G = \{\sigma^i \tau^j, 0 \leqslant i \leqslant 4, 0 \leqslant j \leqslant 3\}$.
Or G est résoluble, car $H = \mathrm{Gal}(L/\mathbb{Q}(\zeta)) \triangleleft G$, car $\mathbb{Q}(\zeta)/\mathbb{Q}$ est normale, et $G/H = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = (ZnZ5)^\times$.
Trouvons pour rire les sous-extensions de $\mathbb{Q}(\zeta)/\mathbb{Q}$. Son groupe de Galois est $G_1 =$

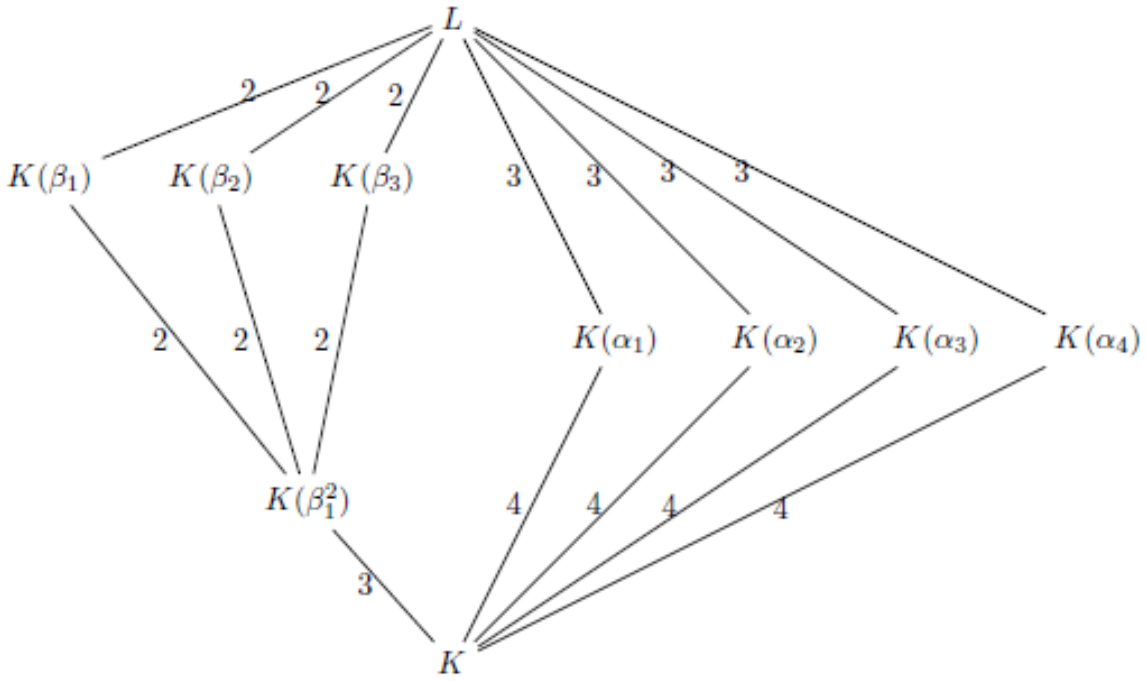


FIGURE 4.2.3 : *Treillis des sous-extensions de L/K.* —

$(ZnZ5)^{)}\times \simeq ZnZ4$. Il en existe un sous-groupe non trivial ; il est de cardinal 2, soit $\{1\} \subseteq H_1 \subseteq G_1$. On a donc une unique sous-extension, $\mathbb{Q}(\zeta)^{H_1} = \mathbb{Q}(\sqrt{d})$ avec un d à déterminer. Or $H_1 = \{\pm 1\} = \{id, c\}$ avec $c(\zeta) = \zeta^{-1}$, d'où $c(\zeta + \zeta^{-1}) = \zeta + \zeta^{-1}$, donc $\mathbb{Q}(\zeta + \zeta^{-1}) \subseteq \mathbb{Q}(\zeta)^{H_1}$, où $\zeta + \zeta^{-1} = 2\cos(\frac{2\pi}{5})$. Or des techniques de bébé permettent de montrer que ce corps est $\mathbb{Q}(\sqrt{5}$ en calculant cette ligne trigonométrique.

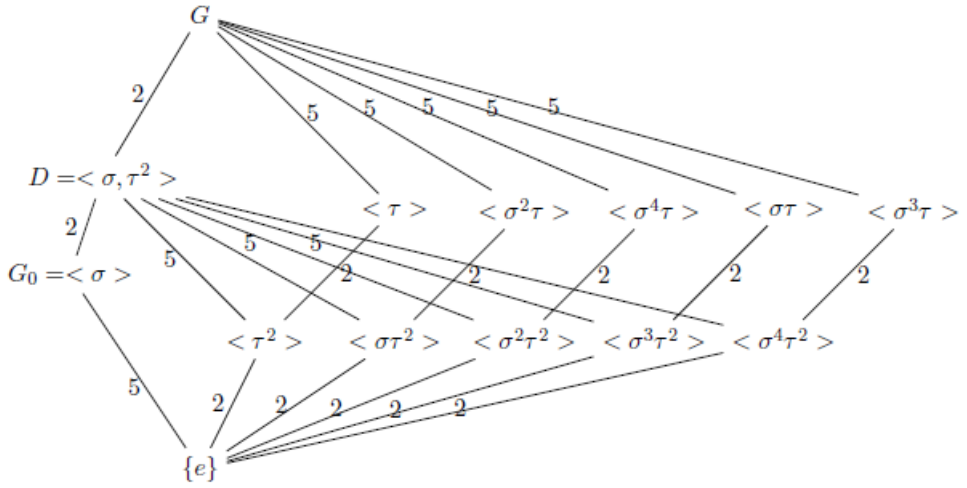


FIGURE 4.2.4 : *Treillis des sous-groupes de G.* —

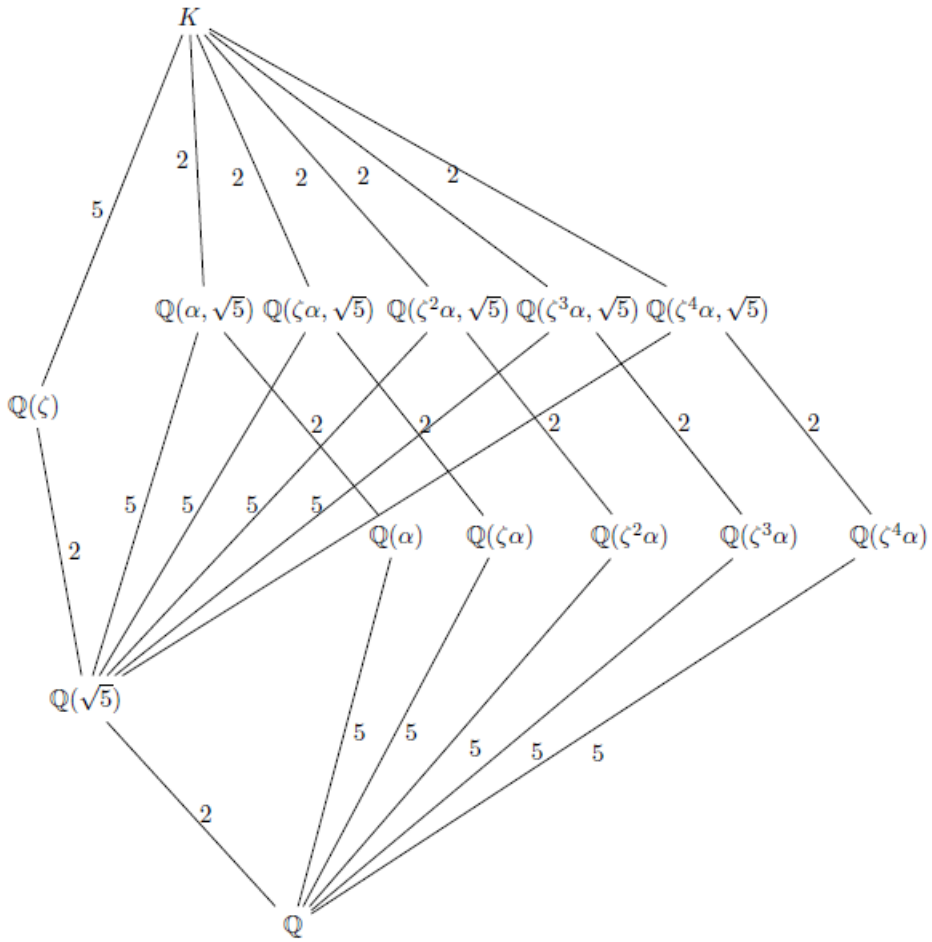


FIGURE 4.2.5 : *Treillis des sous-extensions de L/K.* —

4.2.6 Extension abélienne

Définition. ***(Extension abélienne)***

Une extension L/K est dite *abélienne* si elle est galoisienne et que son groupe de Galois est abélien.

La théorie de Galois des corps finis est assez simple. Le groupe de Galois est non seulement abélien, mais en plus, cyclique.

Théorème. ***(Abel)***

Soit K un corps fini de cardinal $q = p^m$, $m \in \mathbb{N}, p \in \mathcal{P}$. Soit $K = \mathbb{F}_q$. On suppose L/K une extension finie de degré $n = [L : K]$, soit $L = \mathbb{F}_{q^n}$.
Alors L/K est galoisienne et $\mathrm{Gal}(L/K) = \mathbb{Z}/n\mathbb{Z}$ avec pour générateur (canonique) $\phi = \mathrm{Frob} \in \mathrm{Gal}(L/K)$ donné par $\phi : x \mapsto x^q$.

▷ Si α est un générateur de $L^\times$, qui existe, alors $L = K(\alpha)$ et l'extension est normale sur K, et séparable sur K par perfection des corps finis. Soit :

$$\begin{array}{ccc} L & \xrightarrow{\sigma} & \overline{K} \\ | & & | \\ K & \xrightarrow{id} & K \end{array}$$

et puisque $\alpha^{q^n} - \alpha =, \sigma(\alpha)^{q^n} - \sigma(\alpha) = 0$, donc $\sigma(\alpha) \in L$. Donc L/K est galoisienne.

De plus, $G = \mathrm{Gal}(L/K)$ est de cardinal $[L : K] = n$. D'une part, pour tout $x \in K = \mathbb{F}_q$, $\phi(x) = x$ donc $\phi \in \mathrm{Aut}(L/K) = G$. D'autre part, l'ordre de ϕ dans G est n (exercice). D'où le résultat. ■

4.2.6.1 Extension cyclotomique

On étudie maintenant les cas des polynômes cyclotomiques, cas particulier crucial d'extensions abéliennes.

Soit K un corps, soit ζ une racine n-ème primitive dans $\overline{K}$.

Remarque. Si $\mathrm{car}(K) = p$ et $p \mid n$, il n'existe pas de racine primitive n-ème, car $\{x \in \overline{K} \mid x^p = 1\} = \{1\}$. Inversement, si p ne divise pas n, il existe une racine primitive n-ème car $X^n - 1$ est séparable : en effet, $(X^n - 1)' = nX^{n-1}$ a pour seul zéro $X = 0$.

Théorème. ***(Extension cyclotomique)***

Soit ζ une racine $n$ème primitive de l'unité dans $\overline{K}$. Alors :

1. L'extension $K(\zeta)/K$ est galoisienne.
2. $\mathrm{Gal}(K(\zeta)/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$.
3. Si $K = \mathbb{Q}$, $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$.

En particulier, elle est abélienne.

▷ Soit $\sigma : K(\zeta) \longrightarrow \overline{K}$. Alors comme déjà vu $\sigma(\zeta)$ est une racine n-ième de l'unité, primitive, car si $\zeta^m \neq 1, \sigma(\zeta^m) \neq 1$. Donc $\sigma(\zeta) = \zeta^j$ pour un certain j pris modulo n. En fait, $j \in (ZnZn)^\times$. Donc $K(\zeta)/K$ est normale et séparable. (On peut aussi dire : c'est le corps de décomposition d'un polynôme cyclotomique.)

On définit $\mathrm{Gal}(K(\zeta)/K) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$, $\sigma \mapsto i(\sigma)$ où $\sigma(\zeta) = \zeta^{i(\sigma)}$. Il est injectif car σ est déterminé par ses valeurs sur K et ζ. Il faut vérifier que c'est un homomorphisme de groupes. Or $\sigma\tau(\zeta) = \zeta^{i(\sigma\tau)} = \zeta^{i(\sigma)i(\tau)} = (\sigma(\zeta))^{i(\tau)} = \sigma(\zeta^{i(\tau)})$.

Prenons Φ_n le polynôme cyclotomique. Or $\Phi_n(X)$ est irréductible dans $\mathbb{Q}[X]$ (il est à coefficients entiers), donc puisqu'il annule les racines primitives de l'unité, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg(\Phi_n) = \varphi(n) = \mathrm{card}(\mathbb{Z}/n\mathbb{Z})^\times$. ■

Voici un autre exemple important. On suppose $\mathrm{card}(K) = 0$, ou $p = \mathrm{car}(K)$ ne divise pas l'entier n.

Théorème. ***(Extension cyclotomique, cas général)***

On suppose que K contienne une racine primitive n-ième de l'unité. Soit $a \in K$ et α une racine de $X^n - a$ dans $\overline{K}$. Alors l'extension $K(\alpha)/K$ est galoisienne et $\mathrm{Gal}(K(\alpha)/K)$ s'identifie à un sous-groupe du groupe cyclique d'ordre n.
En particulier, elle est abélienne.

▷ $X^n - a$ est séparable si $a \neq 0$ (cas trivial), car $(X^n - a) = nX^{n-1}$ non nul. Les racines de $X^n - a$ sont $\{\zeta\alpha, \zeta \in \mu_n\}$ la copie canonique du groupe cyclique d'ordre n dans notre extension. Elles sont donc dans $K(\alpha)$. Donc l'extension est normale. Définissons l'application de $G = \mathrm{Gal}(K(\alpha)/K) \longrightarrow \mu_n$, par $\sigma \longmapsto \frac{\sigma(\alpha)}{\alpha}$ par normalisation. Elle est injective, car σ est déterminée par ses valeurs sur K et par $\sigma(\alpha)$. C'est un homomorphisme de groupes. En effet, $\sigma\tau(\alpha) = \zeta(\sigma\tau)\alpha$, avec $\frac{\sigma\tau(\alpha)}{\alpha} = \frac{\sigma\tau(\alpha)}{\tau(\alpha)}\frac{\tau(\alpha)}{\alpha} = \frac{\sigma(\alpha)}{\alpha}\frac{\tau(\alpha)}{\alpha}$, et $\frac{\sigma\tau(\alpha)}{\tau(\alpha)} = \frac{\sigma(\zeta(\tau)\alpha)}{\zeta(\tau)\alpha} = \frac{\sigma(\zeta(\tau))}{\zeta(\tau)} = \frac{\sigma(\alpha)}{\alpha}$ où ce premier facteur $= 1$, car $\zeta(\tau) \in K$. ■

On énonce le lemme suivant :

Lemme. ***(Lemme de Kummer)***

Soit $n \geqslant 2$, et ζ une racine n-ième primitive dans K. Supposons L/K galoisienne avec $\mathrm{Gal}(L/K) = \langle\sigma\rangle \simeq \mathbb{Z}/n\mathbb{Z}$. Alors il existe $\alpha \in L$ telle que $L = K(\alpha)$ et $\alpha^n = a \in K$, c'est-à-dire, par définition, $L = K(\sqrt[n]{\alpha})$.

La preuve est astucieuse ; elle nécessite le sous-lemme suivant :

Sous-lemme. ***(Théorème de Hilbert 90)***

Si $x \in L/K$ une extension cyclique (galoisienne de groupe de Galois cyclique) de générateur σ, alors $N_{L/K}(x) := x\sigma(x)...\sigma^{n-1}(x) = 1 \iff \exists y \in L \quad x = \frac{y}{\sigma(y)}$.
Remarquons (même si ce n'est pas un problème dans notre preuve) que la définition de la norme ne dépend pas du générateur choisi.

▷ Le sens réciproque est facile : $N(x) = \prod_{i=0}^{n-1} \sigma^i(\frac{y}{\sigma(y)}) = \frac{\prod_{i=0}^{n-1}\sigma^i(y)}{\prod_{i=0}^{n-1}\sigma^{i+1}(y)} = 1$, car $\sigma^n = id$.

Le sens direct est moins aisé, car il faut construire ce fameux y. On a $y = y(z) = \sum_{i=0}^{n-1} x\sigma(x)\sigma^i(x)\sigma^i(z) = xz + x\sigma(x)\sigma(z) + \underline{...} + x\sigma(x)...\sigma^{n-1}(x)\sigma^{n-1}(z)$. Calculons : $x\sigma(y) = x\sigma(x)\sigma(z) + x\sigma(x)\sigma^2(x)\sigma^2(z) + x\sigma(x)... + \underline{\sigma^{n-1}(x)\sigma^{n-1}(z)} + \underbrace{x\sigma(x)...\sigma^{n-1}(x)}_{=N(x)}\underbrace{\sigma^n(x)\sigma^n(z)}_{=xz}$. Si $N(x) = 1$, on obtient bien $x\sigma(y) = y$. Si $\sigma(y) \neq 0$, on obtient bien $x = \frac{y}{\sigma(y)}$. Or pour x fixé non nul, $y(z)$ est de la forme $a_0 id + a_i\sigma + ... + a_{n-1}\sigma^{n-1}$ avec $\sigma^i \in \mathrm{Hom}_K(L,L)$, $a_i \neq 0$. Par le lemme d'Artin, il existe $z \in L$ tel que $y(z) \neq 0$. ■

On peut reprendre le lemme de Kummer.

Preuve.

▷ Il suffit de remarquer que $N(\zeta) = \zeta\sigma(\zeta)...\sigma^{n-1}(\zeta) = \zeta^n = 1$, donc il existe $\alpha \in L^\times$, $\zeta^{-1} = \frac{\alpha}{\sigma(\alpha)}$ ou encore $\sigma(\alpha) = \zeta\alpha$. Les conjugués de α sur K sont $\sigma^i(\alpha) = \zeta^i(\alpha)$. Il y en a n. Donc $[K(\alpha) : K] = n$, donc $L = K(\alpha)$. Ensuite, $\sigma(\alpha^n) = (\zeta\alpha)^n = \alpha^n$, donc $\alpha^n = a \in L^{\langle\sigma\rangle} = K$ d'où la fin de la preuve. ■

Pour faire cette théorie en caractéristique positive, le problème est la donnée d'extensions inséparables. Si l'on se pose en caractéristique avec n qui ne divise pas p, les énoncés précédents tiennent (et l'on peut donc appliquer la théorie de la résolution par radicaux qui suit).

4.2.7 Application à la résolution par radicaux des équations

Exemple

On donne un exemple d'extension dont le groupe de Galois est exactement le groupe symétrique S_5. Prenons celui du polynôme $P = X^5 - 10X + 2$. Alors $L = \mathbb{Q}(\alpha_1,...,\alpha_5)$ et $G = \mathrm{Gal}(L/\mathbb{Q}) = S_5$. Vérifions-le. P est irréductible car il est d'Eisenstein par rapport à 2. De plus, 5 divise le cardinal de G donc il existe un 5-cycle donc $G \subseteq S_5$. Le polynôme P a trois racines réelles, et une paire de racines complexes. D'autre part, soit $c \in G$ la conjugaison complexe. C'est une transposition. Donc $G = S_5$. Ainsi $\mathbb{Q} \xrightarrow{5} \mathbb{Q}(\alpha) \longrightarrow L$.

Définition. ***(Extension par radicaux)***

On reformule proprement cette définition énoncée en préambule. Une extension de corps L/K est *obtenue par radicaux* s'ils existe $K_0 = K \subseteq K_1 \subseteq ... \subseteq K_r$ avec $L \subseteq K_r$ et $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ avec $a_i \in K_i$.

Définition. ***(Extension résoluble)***

Une extension de corps L/K est dite *résoluble* s'il existe une sur-extension $\tilde{L}/K$, soit $L \subseteq \tilde{L}$, où $\mathrm{Gal}(\tilde{L}/K)$ est un groupe résoluble.

Théorème. ***(Théorème d'Abel)***

En caractéristique nulle, une extension de corps est par radicaux si et seulement si elle est résoluble.

▷ Soit L/K une extension résoluble par radicaux, avec $\mathrm{car}(K) = 0$. On utilise les notations de la définition. Prenons $\tilde{L}$ sa clôture galoisienne qui, si L/K est séparable, n'est autre que sa clôture normale (qui existe, car la clôture algébrique est normale). C'est en particulier une extension galoisienne qui est le compositum des $\sigma(K_r)$ pour $\sigma \in \mathrm{Hom}_K(K_r,\overline{K})$, donc s'obtient par adjonction successive de radicaux. En remplaçant K_i par $\tilde{K}_i$ galoisienne sur K, on peut supposer K_r/K galoisienne ($\tilde{K}_r$ est obtenue par radicaux au-dessus de K). Si $K_{i+1} = K_i(\sqrt[n]{a_i})$, $\sigma K_{i+1} = \sigma K(\sqrt[n]{a_i})$, et donc $\tilde{K}_r$ contient les racines primitives de l'unité correspondant à $m_1,...,m_r$. On se ramène donc au cas

$K_0 = K \subseteq K_1 = K(\zeta) \subseteq K_2 \subseteq ... \subseteq K_r$ (car $K_1 \rightsquigarrow K(\zeta), K_i \rightsquigarrow K_{i+1}(\zeta)$. Or chaque $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ avec $m \mid \text{ord}(\zeta) = N$. Alors $\text{Gal}(K_1/K)$ est abélien, car il se plonge dans $(\mathbb{Z}/N\mathbb{Z})^\times$, et plus généralement $\text{Gal}(K_{i+1}/K)$ est abélien d'après le théorème des extensions cyclotomiques, car il se plonge dans μ_{m_i}. Ce sont donc des extensions abéliennes. Appliquons à chaque étape la correspondance de Galois. Si $K_{i+1} = L^{H_{i+1}}$ et $K_i = L^{H_i}$.. K_{i+1}/K_i est normale si et seulement si $H_{i+1} \triangleleft H_i$ et dans ce cas $\text{Gal}(K_{i+1}/K_i) = H_i/H_{i+1}$. La suite $K_0 \subseteq K_1 ... \subseteq K_r$ correspond à $G = G_0 \supseteq H_1 \supseteq ... \supseteq H_2 = \{e\}$ où $K_i = K_2^{H_i}$. Or K_{i+1}/K_i est Galois avec un groupe abélien. Comme G est résoluble, on a bien $H_{i+1} \triangleleft H_i$ et H_i/H_{i+1} abélien.

Pour la réciproque, on utilise le lemme de Kummer. Supposons que $\text{Gal}(L/K)$ soit résoluble. On a une suite $G = G_0 \supseteq H_1 \supseteq ... \supseteq H_r = \{e\}$ qui, quitte à la minimaliser, vérifie H_i/H_{i+1} cyclique pour tout i. Notons N le cardinal de G. Supposons d'abord que ζ soit une racine N-ième primitive dans K. Posons $K_i = L^{H_i}$; on a donc K_{i+1}/K_i galoisien de groupe $\mathbb{Z}/m_i\mathbb{Z}$, avec $m_i \mid N$; par conséquence, $K_{i+1} = K_i(\sqrt[m_i]{a_i})$. Dans le cas général, on remplace K par $K' = K(\zeta)$ et L par $L' = L(\zeta)$. Alors $\text{Gal}(L'/K) = \text{Gal}(LK(\zeta)/K) \hookrightarrow \text{Gal}(L/K) \times \text{Gal}(K(\zeta)/K)$ produit d'un groupe résoluble (par hypothèse) et d'un groupe abélien, donc il est résoluble et $\text{Gal}(L'/K')$ aussi. Donc L' est obtenue par radicaux à partir de K'. On a donc $K \subseteq K' = K(\sqrt[N]{1}) \subseteq K'_1 \subseteq ... \subseteq K'_r$. ■

Corollaire. ***(Théorème de Galois)***

Les équations de degré $\geqslant 5$ ne sont pas, en général, résolubles par radicaux.

▷ D'après l'exemple précédent. ■

On renvoie à la remarque de la fin de la section précédente pour la caractéristique positive.

4.2.8 Calcul pratique du groupe de Galois en caractéristique nulle

Soit $P \in \mathbb{Q}[X]$ un polynôme irréductible de degré n. Il est donc séparable. On pose $L = \mathbb{Q}(\alpha_1,...,\alpha_n)$ un corps de décomposition de P et $G = \text{Gal}(L/\mathbb{Q}) \hookrightarrow S_n$. Alors on rappelle que :

- L'action sur les racines est transitive. En particulier, n divise $|G|$,
- $G \subseteq \mathfrak{A}_n$ si et seulement si Δ_p est carré,
- par conjugaison complexe, pour s paires de racines, il existe $\sigma = (i_1, j_1), ...(i_s, j_s)$ dans ce groupe.

On énonce le lemme de Dedekind pour lequel on aura besoin des propriétés énoncés ensuite.

Lemme. ***(Lemme de Dedekind)***

Soit $P \in \mathbb{Z}[X]$ unitaire, p premier. On suppose que P modulo p soit séparable et se factorise en $P_1...P_s$ dans $\mathbb{F}_p[X]$ avec P_i irréductible de degré m_i. Alors G contient une permutation de type $(m_1,...,m_s)$.

▷ Introduisons $A = \mathbb{Z}[\alpha_1,..., \alpha_n]$ et $L = \mathbb{Q}(\alpha_1,..., \alpha_n)$. Posons $R = \{\alpha_1,..., \alpha_n\}$ et $\tilde{R} = \{\beta_1,..., \beta_n\}$ les racines de $\tilde{P} = P$ modulo p dans $\overline{\mathbb{F}_p}$. On pose aussi $\tilde{L} = \mathbb{F}_p(\beta_1,..., \beta_n)$. On admet

les propriétés suivantes. Introduisons $\phi : \tilde{L} \longrightarrow \tilde{L}$ avec $\phi(x) = x^p$, $\phi \in \mathrm{Gal}(\tilde{L}/\mathbb{F}_p)$ qui en est un générateur. De plus, ϕ agit sur $\tilde{R}$, et les orbites sont les facteurs irréductibles de $\tilde{P} = P_1...P_s$, ϕ permute circulairement les racines de P_i. Comme permutation de $\tilde{R}$, c'est une permutation de type $(m_1,...,m_s)$, comme produit de cycles de longueur m_i à supports disjoints.

$$\begin{array}{ccc} A & -f\to & \tilde{L} \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \phi} \\ A & -f\to & \tilde{L} \end{array}$$

Soit $f \in \mathrm{Hom}(A,\tilde{L})$, alors $f : R \longrightarrow \tilde{R}, \alpha_i \longmapsto f(\alpha_i) := \beta_i$ est bijective. Par la seconde propriété, $\phi \circ f = f \circ \Sigma$ pour un certain $\sigma \in G$. Si on restreint f, σ, ϕ, ce sont tous des bijections, donc $\sigma = f^{-1} \circ \phi \circ f$, donc σ est du même type que ϕ vu comme permutation de S_n. ■

Propriétés.

Sous les hypothèses précédentes, l'ensemble $\mathrm{Hom}(A,\tilde{L})$ des homomorphismes d'anneaux est non vide et si $f_1, f_2 \in \mathrm{Hom}(A,\tilde{L})$, il existe $\sigma \in G$ tel que $f_2 = f_1 \circ \sigma$; autrement dit, si $f \in \mathrm{Hom}(A,\tilde{L})$, $\mathrm{Hom}(A,\tilde{L}) = \{f \circ \sigma, \sigma \in G\}$. Chaque f induit une bijection $R \longrightarrow \tilde{R}$.

▷ On montre les points 1, 3 puis 2. Par le lemme de Zorn (ou, ici, par noethérianité), il exite un idéal maximal tel que $pA \subseteq \mathfrak{M} \subseteq A$. On induit $f : A \longrightarrow A/\mathfrak{A}$. Or $A/\mathfrak{M}$ est une extension de $\mathbb{F}_p$, car $p \in \mathfrak{M}$, et l'image de A par f est $\mathbb{F}_p(f(\alpha_1),...,f(\alpha_n))$. Puisque $f : A[X] \longrightarrow A/\mathfrak{M}[X]$, elle induit une application sur $\mathbb{Z}[X] \longrightarrow \mathbb{F}_p[X]$. Or $f(P) = \tilde{P}$ donc $f(\alpha_i) \in \tilde{R}$, et $P(\alpha_i) = 0 \implies \tilde{P}(f(\alpha_i)) = 0$, donc $A/\mathfrak{M} \subseteq \tilde{L}$.

On a vu que $f(R) \subseteq \tilde{R}$. Par hypothèse, $\mathrm{card}(R) = \mathrm{card}(\tilde{R}) = n$. Montrons que $f_{|R}$ est injective. Si $f(\alpha_i) = f(\alpha_j)$ avec $i \neq j$, c'est-à-dire $\alpha_i - \alpha_j \in \mathfrak{M}$. Prenons $P(X) = \prod_{i=n} (X - \alpha_i)$. Alors $\tilde{P} = f(P) = \prod_{i=1}^{n} (X - f(\alpha_i)) \in \tilde{L}[X]$.

Soit $f \in \mathrm{Hom}(A,\tilde{L})$, qui existe, par le premier point. Pour tout $\sigma \in G$, on a $f \circ \sigma \in \mathrm{Hom}(A,\tilde{L})$ car σ permute les α_i donc $\sigma : A \longrightarrow A$ se prolonge sur L. Ainsi $\{f \circ \sigma | \sigma \in G\} \subseteq \mathrm{Hom}(A,\tilde{L})$. Puisque $|G| = [L : \mathbb{Q}]$, en effet, si $f \circ \sigma_1 = f \circ \sigma_2$ on a en particulier $f \circ \sigma_1(\alpha_i) = f \circ \sigma_2(\alpha_i)$, et par le deuxième point, on obtient $\sigma_1(\alpha_i) = \sigma_2(\alpha_i)$ donc $\sigma - 1 = \sigma_2$. Si α est racine de $X^n + a_{n-1}X^{n-1} + ... + a_0 \in \mathbb{Z}[X]$ irréductible, $B = \mathbb{Z}[\alpha] = B_0 = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus ... \oplus \mathbb{Z}a^{n-1} \subseteq \mathbb{Q}(\alpha) = \mathbb{Q} \oplus \mathbb{Q}\alpha \oplus ... \oplus \mathbb{Q}a^{n-1}$; en effet, $\alpha^n = -a_0 - a_1\alpha - ... - \alpha_{n-1}\alpha^{n-1}$ et $\alpha^{n+1} \in B_0$, d'où $B = B_0$. Ainsi $1, \alpha, ...\alpha^{n-1}$ est une base de $\mathbb{Q}(\alpha)$ sur $\mathbb{Q}$ et donc de $\mathbb{Z}[\alpha]$ sur $\mathbb{Z}$. Ainsi $\bigoplus_{i\in I} \mathbb{Q}\alpha_1^{i_1}...\alpha_n^{i_n} = L$ où $\mathrm{card}(I) = [L : \mathbb{Q}] = |G|$. Aussi $\bigoplus_{i\in I} \mathbb{Z}\alpha_1^{i_1}...\alpha_n^{i_n} = A$, puisque $\mathbb{Q} \subseteq_{n_1} \mathbb{Q}(\alpha_1) \subseteq_{n_2} \subseteq \mathbb{Q}(\alpha_1,\alpha_2) \subseteq ... \subseteq L$. Comme $\mathbb{Z}$-module, $A \simeq \mathbb{Z}^{|G|} = \mathbb{Z}^{[L:\mathbb{Q}]}$. D'après le lemme d'Artin, les éléments de $\mathrm{Hom}(A,\tilde{L})$ sont linéairement indépendants. Donc $\mathrm{card}(\mathrm{Hom}(A,\tilde{L})) \leqslant |G|$ ■

Remarques.

1. Il existe toujours beaucoup de nombres premiers qui permettent d'appliquer le lemme ; les seuls qui posent problème, sont ceux qui divisent le discriminant. Or il n'a qu'un

nombre fini de diviseurs.

2. On peut toujours se ramener au cas unitaire, au sens suivant : si $\alpha \in \overline{\mathbb{Q}}$ est racine de P avec les notations évidentes, en posant xa_0^{n-1}, alors $P_1(a_0\alpha) = 0$ en calculant.

Exemple

Prenons $P = X^4 + 8X + 12$. Son discriminant est un carré, donc $G \subseteq \mathfrak{A}_4$. Or $4 \mid |G|$ donc G est transitif. Il y a aussi deux paires de racines complexes donc $\tau = (i,j)(k,l) \in G$ un élément du groupe de Klein. De plus $P(-1) = 5$. Aussi, modulo 5, $P(X) = (X+1)(X^3+...)$ où l'on peut vérifier par calcul que ce deuxième facteur est irréductible. Par le lemme de Dedekind, G contient un 3-cycle. Ainsi, $G = \mathfrak{A}_4$.
En général, on applique cette méthode pour plusieurs nombres premiers ce qui permet d'obtenir beaucoup de renseignements sur le groupe de Galois.

4.2.9 Extension de la théorie de Galois aux extensions algébriques infinies

Supposons L/K galoisienne, c'est-à-dire algébrique, séparable et normale, éventuellement infinie (la théorie infinie ne rajoute rien à la théorie finie avec laquelle elle est compatible).

On définit toujours $\mathrm{Gal}(L/K) = \mathrm{Aut}(L/K) = \{\sigma : L \longrightarrow L \mid \sigma \in \mathrm{Aut}(L), \sigma_{|K} = id_K\}$.

On remarque que si $K \subseteq F \subseteq L$ où F/K est finie, alors F/K est séparable mais pas forcément normale ; cependant, $K \subseteq F \subseteq \tilde{F}$ avec $\tilde{F}/K$ normale, $[\tilde{F} : K] < \infty$: par exemple, $F = K(\alpha)$ et $\tilde{F} = K(\alpha_1,...,\alpha_n)$.

On note $\mathcal{F} = \{F_i, i \in I\}$ l'ensemble des sous-extensions $K \subseteq F_i \subseteq L$ avec $[F_i : K] < \infty$ et $G_i = \mathrm{Gal}(F_i/K)$. On fait les remarques suivantes, déjà entrevues pour certaines :

Remarques.

1. Les groupes de Galois G_i sont finis.
2. $L = \bigcup_{i \in I} F_i$.
3. On note pour $i,j \in I$, $i < j$ si et seulement si $F_i \subseteq F_j$. C'est bien défini.
4. Si $\sigma \in \mathrm{Gal}(L/K) = G$ pour chaque F_i. On a $\sigma_{|F_i} \in G_i = \mathrm{Gal}(F_i/K)$ et évidemment, si $i < j$, $(\sigma_{|F_j})_{F_i} = \sigma_{|F_i}$. On obtient $\phi : G \longrightarrow \prod_{i \in I} G_i = \{(\sigma_i)_{i \in I} \mid \sigma_i \in G_i\}$. Posons $G_1 = \{(\sigma_i)_{i \in I} \in \prod_{i \in I} G_i \mid \forall i < j \quad \sigma_{j|F_i} = \sigma_i\}$.

Lemme

$G \longrightarrow G_1$ est un isomorphisme de groupes.

▷ C'est un morphisme. Il est injectif, car $L = \cup F_i$. Montrons qu'il est surjectif. Si $(\sigma_i)_{i\in I} \in \prod G_i$ vérifie $\forall i < j \quad \sigma_{j_{|F_i}} = \sigma_i$, alors $\exists \sigma \in G \ \forall i \quad \sigma_{|F_i} = \sigma_i$. Construisons σ. $x \in L$, alors $\exists i, x \in F_i$. Posons $\sigma(x) = \sigma_i(x)$. Remarque : cela ne dépend pas de i choisi tel que $x \in F_i$. ON obtient $\sigma : L \longrightarrow L$, $\sigma_{|K} = id_K$. Pour $x,y \in L$, $\exists i, x,y \in F_i \quad \sigma(x+y) = \sigma_i(x+y) = \sigma_i(x) + \sigma_i(y) = \sigma(x) + \sigma(y)$. Enfin, σ est surjectif, car $\sigma(F_i) = F_i$. ■

On munit le produit $G_0 = \prod_{i\in I} G_i$ de la topologie produit où chaque groupe est muni de la topologie discrète. Alors d'après le théorème de Tychonov, G_0 est compact. De plus, G_1 est fermé dans G_0 et on munit G_1 de la topologie induite.

En effet, la condition $\sigma_{j_{|F_i}} = \sigma_i$ est une condition fermée. L'ensemble $G_{ij} = \{(\sigma_k) \in \prod G_k \mid \sigma_{j_{|F_i}} = \sigma_i\}$ est un fermé de $\prod_i G_i$ (aussi ouvert), puisqu'il s'écrit $P_{ij} = \prod G_k \longrightarrow G_i \times G_k$, $P_{ij}^{-1}\{X\}$ est fini et $G_1 = \bigcap_{i<j} G_{ij}$.

De plus, G est totalement discontinu grâce à la remarque précédente.

Par conséquence, $\mathrm{Gal}(L/K)$ est un groupe topologique, compact et totalement discontinu : il suffit de le vérifier sur les G_i sur lesquels c'est trivial et l'on conclut par les propriétés de G.

Soit G un sous-groupe ouvert de $\mathrm{Gal}(L/K) = G$. Alors, il est aussi fermé. En effet, G est le produit des gH pour $g \in G/H$. Puisque les gH sont ouverts, H est le complémentaire d'une réunion d'ouverts, donc ouverte.

Un sous-groupe fermé n'est pas forcément ouvert ! (Mais si l'extension est finie, oui.)

Théorème. *(Correspondance de Galois pour L/K infinie)*

Soit L/K une extension galoisienne. L'ensemble des sous-extensions $K \subseteq F \subseteq L$ est en bijection avec l'ensemble des sous-groupes fermés de $G = \mathrm{Gal}(L/K)$ par l'application de $F \longmapsto \mathrm{Gal}(L/F)$ de réciproque $L^H \longleftarrow\!\shortmid H$. De plus, elle a les mêmes propriétés que pour les extensions finies : il faut simplement prendre $F_1 \cap F_2 = L^{\overline{\langle H_1, H_2\rangle}}$ où $F_1 = L^{H_1}$ et $F82 = L^{H_2}$.

La raison profonde est que le sous-corps associé à un groupe est le même que celui associé à son adhérence : $L^H = L^{\overline{H}}$. (On rappelle que l'adhérence d'un sous-groupe d'un groupe topologique est encore un sous-groupe.) On peut aussi le voir en remarquant que l'image d'une sous-extension par la correspondance de Galois donne forcément un groupe fermé.

Pour compléter la remarque précédente, les sous-groupes ouverts des sous-groupes d'indice fini correspondent aux F/K finies.

Chapitre 5

Polynômes

Résumé

Quelques notions pêle-mêle sur les polynômes : construction des polynômes à plusieurs variables, critères d'irréductibilité, annulation des polynômes, fonctions polynomiales, dérivation des polynômes, homogénéité, polynômes symétriques.

5.1 Étude de l'anneau des polynômes sur un anneau

Soit A un anneau commutatif. Le produit polynomial est ainsi défini de façon univoque et l'anneau des polynômes à coefficients dans A est lui-même commutatif.

5.1.1 Généralités

5.1.1.1 Construction

On définit $A[X]$ grâce à $A^{(\mathbb{N})}$. Puisque $\mathbb{N}$ est muni d'une somme, mais pas forcément I, le morphisme de groupes $X^i \mapsto (\delta_i^j)_{j\in\mathbb{N}}$ permet de munir $A[X]$ d'une structure d'anneaux.

Théorème

$\forall a \in A\ \forall d \in \mathbb{N} \quad a.X^d = aX^d$.

Propriété. ***(Propriété universelle des polynômes, version générale)***

Soient A,B deux anneaux commutatifs et $f : A \longrightarrow B$ un morphisme d'anneaux. Soit $b \in B$. Alors il existe un unique morphisme $\phi_{f,b} : A[X] \longrightarrow B$ tel que $\phi_{f,b}(a) = f(a)$ pour tout $a \in A$ et $\phi_{f,b}(X) = b$, où a est identifié à aX^0.

▷ Soit $T = \sum_{k=0}^{d} a_k X^k$. Alors $\phi_{f,b}(T) = \phi_{f,b}(\sum a_k X^k) = \sum_{k=0}^{d} \phi_{f,b}(a_k X^k) = \sum_{k=0}^{d} \phi_{f,b}(a_k)\phi_{f,b}(X)^k = \sum_{k=0}^{d} f(a_k)b^k$. Il est clair que cette expression définit bien un morphisme, car f est un morphisme. ■

Remarque. On a toujours, $\varphi : A[X] \longrightarrow B$ étant un morphisme, $\varphi = \phi_{\varphi_{|A},\varphi(X)}$.

Autre remarque. En particulier, soient A,B deux anneaux. Si $\varphi : A \longrightarrow B$ est un morphisme d'anneaux, on en déduit un morphisme $\varphi : A[X] \longrightarrow B[X]$ d'anneaux, avec $\varphi : \sum a_i X^i \longmapsto \sum \varphi(a_i) X^i$.

Cette propriété permet de caractériser un morphisme de $A[X] \longrightarrow B$ par sa valeur sur les coefficients et en l'indéterminée.

Propriété. ***(Propriété universelle des anneaux de polynômes pour une algèbre)***

Soit A un anneau commutatif, B une A-algèbre et $x \in B$. Alors il existe un unique morphisme d'algèbre de $f : A[X] \longrightarrow B$ tel que $f(X) = x$.

▷ On raisonne par analyse synthèse : $f(P) = \sum_{n\in\mathbb{N}} f(a_n X^n) = \sum_{n\in\mathbb{N}}^{\eta} (a_n) f(X)^n$, car f étant un morphisme d'algèbres, il commute avec η. ■

Remarque. Cette version de la propriété universelle n'est autre que la propriété universelle adaptée au morphisme η, souvent, l'inclusion canonique.

Corollaire. ***(Morphisme d'évaluation)***

Soient A un anneau **commutatif** et $a \in A$. Alors il existe un unique morphisme

$$\begin{array}{rccc} \mathrm{ev}_A : & A[X] & \longrightarrow & A \\ & X & \longmapsto & a \end{array}.$$

Remarque. L'utilisation de la propriété universelle des polynômes pour montrer l'existence du morphisme d'évaluation est quelque peu surfaite. Il est très possible de définir le morphisme d'évaluation sans cette propriété abstraite.

Corollaire. ***(Réduction modulo un idéal)***

Soient A un anneau commutatif et I un idéal bilatère. Alors A/I est un anneau commutatif et l'on peut définir un morphisme de $A[X] \longrightarrow A/I[X]$ par $\sum a_k X^k \mapsto \sum \pi(a_k) X^k$.

▷ C'est $\phi_{\pi,Y}$. ■

5.1.1.2 Notion de degré

Propriété. ***(Degré d'un produit)***

Soit A un anneau. Alors $\deg(PQ) \leqslant \deg(P) + \deg(Q)$. De plus, il y a égalité pour tout couple de polynôme si et seulement si A est sans diviseur de zéro.

Propriété. ***(Degré d'une somme)***

Soit A un anneau. Alors $\deg(P+Q) \leqslant \max(\deg(P), \deg(Q))$. Même si A est un corps, il n'y a pas égalité en général ; il y a égalité si et seulement si $\deg(P) \neq \deg(Q)$ ou $\mathrm{dom}(P) \neq -\mathrm{dom}(Q)$.

5.1.1.3 Hérédité d'une propriété sur la catégorie des anneaux

On travaille du point de vue catégorique.

Définition. ***(Propriété héréditaire)***

Soit A un anneau commutatif. Soit P un prédicat de A. On dit que P est *héréditaire*, si $P(A)$ implique $P(A[X])$.

Exemple

L'intégrité, la factorialité (théorème de Gauss), la noethérianité (théorème de Hilbert), le caractère à PGCD sont héréditaires sur la catégorie des anneaux commutatifs. Par contre, l'euclidianité, la principalité, le Bézoutisme ne le sont pas.

Remarque. En itérant par récurrence, si P est une propriété héréditaire, alors pour tout $n \in \mathbb{N}$, si $P(A)$ est vraie, alors $P(A[X_1,...,X_n])$ également. En effet, on peut écrire $A[X_1,...,X_n] \simeq A[X_1,...,X_{n-1}][X_n]$ et la propriété se transmet *sous couvert qu'elle est bien catégorique*, c'est-à-dire qu'elle est stable par isomorphisme.

Remarque. Si P est héréditaire et $P(A)$ est vraie, alors $P[(X_i)_{i\in I}]$ n'est pas nécessairement vraie. En effet, prenons la noethérianité. Elle est héréditaire par transfert de Hilbert, mais l'anneau $\mathbb{R}[(X_n)_{n\in\mathbb{N}}]$ n'est pas noethérien.

5.1.2 Arithmétique élémentaire de $A[X]$

Lemme

Soit $P \in A[X]$. Si tous les coefficients d'un polynôme sont inversibles, il ne divise pas zéro.

Lemme

Soit $P \in A[X]$. Si le coefficient dominant de ce polynôme est inversible, il ne divise pas zéro.

Lemme

Soit $P \in A[X]$. Si le coefficient dominant de P ne divise pas zéro, le polynôme P ne divise pas zéro.

Lemme

Un monôme ne divise jamais zéro.

5.1.3 Irréductibles de $A[X]$

Soit A un anneau commutatif. On rappelle :

Définition. ***(Irréductibilité d'un polynôme)***

Un polynôme $P \in A[X]$ est dit irréductible s'il n'existe pas de polynômes $Q,R \in A[X]$ non nuls, non inversibles tels que $P = QR$.

VOC Un polynôme non irréductible est dit *réductible*, *composé*, *décomposable* ou plus rarement *factorisable*.

Le cas limites : inversibles, vont nous intéresser particulièrement, en nous posant problème.

5.1.3.1 Généralités

On peut d'abord énoncer ce résultat fondamental sur l'irréductibilité dans les polynômes à coefficients dans un corps.

Propriété. ***(Irréductibilité des polynômes unitaires de degré 1)***

Soit A un anneau commutatif **intègre**. Soit $a \in A$. Alors $X - a$ est irréductible dans l'anneau $A[X]$.

▷ En effet, on a $A[X]/(X-a) \simeq A$. Si A est intègre, $X - a$ est donc premier dans $A[X]$, mais puisque $A[X]$ est intègre, il est donc irréductible. ■

Remarque. C'est rapidement faux si l'on ne suppose pas l'anneau intègre. En effet, dans $\mathbb{Z}/6\mathbb{Z}$, $3X - 2$ et $4X + 3$ ne sont pas inversibles ; néanmoins, $X = (3X - 2)(4X + 3)$, donc X n'est pas irréductible.

Voilà un fait important. Si un polynôme s'écrit, par exemple, sous la forme :

$$P = (X-1)^2 \text{ ou } \prod_{d|n} \phi_d$$

alors P n'est pas irréductible !

C'est à peine drôle. La première façon de voir qu'un polynôme n'est pas irréductible est qu'il soit défini comme un produit de facteurs non triviaux.

Exercice 102

Soit A un anneau intègre et $P \in A[X]$ divisible par un polynôme non nul, non inversible. P peut-il être irréductible ?

Propriété. ***(Irréductibles sur un corps algébriquement clos)***

Soit K un corps algébriquement clos. Alors les irréductibles de $K[X]$ sont les $aX - b$, $a \in K \setminus \{0\}$.

▷ On sait déjà qu'ils sont irréductibles par la propriété précédente, puisque associés aux $X - \frac{b}{a}$. Soit maintenant P irréductible de degré $\geqslant 2$. Alors puisque K est algébriquement clos, P admet au moins une racine x. Dans ce cas, $X - x$ divise P d'où $(X-x)Q = P$ où P est de degré $\geqslant 1$ par degré de P. Il est donc non nul non inversible, et P est réductible. ■

On peut s'intéresser aux polynômes de petit degré où la question de l'irréductibilité se ramène à celles des racines. Notons d'abord le fait suivant :

Propriété. ***(Lien racine-irréductibilité)***

Soit A un anneau intègre et $P \in A[X]$ de degré $\geqslant 2$. Si P est irréductible, alors il n'a aucune racine.

▷ En effet, s'il avait une racine x, on aurait $X - x$ divisant P, d'où $P = (X-x)Q$ et par degré dans un anneau intègre Q est de degré $\geqslant 1$, il est donc non nul non inversible puisque $A[X]^* = A^*$. Ainsi P ne serait pas irréductible. ■

Exercice 103

Est-ce vrai si on ne suppose plus A intègre ?

▷ **Éléments de réponse.**

Non : regarder ce qui se passe dans $\mathbb{Z}/3\mathbb{Z}$.

La réciproque n'est pas vraie (!). Elle l'est pourtant pour des polynômes de degré 2 ou 3.

Propriété. ***(Irréductibilité des polynômes de degré 2)***

Soit K un anneau intègre et $P \in K[X]$ de degré 2. Alors P est irréductible si et seulement s'il n'a aucune racine.

Propriété. ***(Irréductibilité des polynômes de degré 3)***

Soit K un anneau intègre et $P \in K[X]$ de degré 3. Alors P est irréductible si et seulement s'il n'a aucune racine.

▷ Dans les deux cas, il s'agit d'examiner les degrés des diviseurs et d'observer que l'un deux doit être de degré 1. Dans un corps, cela revient à ce qu'un $X - x$ divise P pour un certain x ; le polynôme à donc une racine. La réciproque est donnée par la proposition précédente. ■

C'est faux dès $\deg(P) \geqslant 4$, même dans des anneaux très gentils !

Contre-exemple. ***(Polynôme de degré 4 irréductible sans racine)***

Prenons $X^4 + 1$. Il n'a aucune racine réelle. Pourtant, il est de degré > 2, donc décomposable. □

Il y a une certaine facilité à « descendre » d'un anneau de polynômes vers un autre, tant que les coefficients vivent encore dans un sous-corps.

Propriété. ***(Irréductibles sur un sous-corps)***

Soient K,L deux corps, L un extension de K. Si $P \in K[X]$ est irréductible dans $L[X]$, alors P est irréductible dans $K[X]$.

▷ Montrons la réciproque, car il est toujours plus simple de montrer la réductibilité que l'irréductibilité. Si $P = QR$ dans $K[X]$, les Q,R sont non nuls non inversibles dans $K[X]$. Ils sont donc non nuls dans $L[X]$. De plus, $K[X]^* = K^*$ et $L[X] = L^*$. S'ils étaient inversibles dans $L[X]$, ils seraient dans $L*$, mais comme dans K, dans K^*, puisque K est un corps, donc clos pour l'inversion, donc dans $K[X]$, par contraposée, ils sont non inversibles dans $L[X]$. On a donc une réduction licite dans $L[X]$ et c'est terminé. ■

Remarque. C'est cohérent avec ce qui se passe pour $\mathbb{R}$ et $\mathbb{C}$, par exemple : les irréductibles de $\mathbb{C}[X]$, qui sont les polynômes de degré 1, sont en particulier irréductible dans $\mathbb{R}[X]$. Le théorème précédent assure sans calcul que les polynômes de la forme $aX^2 + bX + c$ avec a,$bc \in \mathbb{Q}$ et $b^2 < 4ac$ sont irréductibles dans $\mathbb{Q}[X]$.

Ainsi, on peut « descendre » à partir de la clôture algébrique jusqu'à un sous-corps. En descendant jusqu'au sous-corps premier, on peut voir, si c'est $\mathbb{Q}$, passer à l'anneau dont c'est le corps des fractions et l'on commence à s'intéresser aux propriétés arithmétiques de l'anneau en question, ici donc $\mathbb{Z}$. C'est l'objet de la section suivante.

5.1.3.2 Passage de l'anneau au corps des fractions, contenu, théorème de Gauss, critères d'irréductibilité

Pour travailler correctement pour la question générale de l'irréductibilité dans $A[X]$, il faut supposer A intègre. Rappelons que A est intègre si et seulement si $A[X]$ l'est. Nous faisons cette hypothèse dès maintenant. Rappelons également que sous cette condition, $(A[X])^* = A^*$.

On en déduit immédiatement le résultat suivant :

Propriété. ***(Irréductibles constants de*** $A[X]$***)***

Les irréductibles de degré 0 de $A[X]$ sont donc les irréductibles de A (plongés dans $A[X]$).

▷ Soit P un polynôme réductible constant. Alors il existe Q,R deux polynômes non nuls non inversibles tels que $P = QR$. Par degré, Q,R sont constants. Ainsi l'égalité a lieu dans A et Q,R sont des éléments non nuls et non inversibles par la remarque précédente. Donc P est une constante de A réductible dans A. Réciproquement, si P est une constante réductible dans A, alors $P = qr$ où q,$r \in A$ sont non nuls non inversibles et donc des polynômes non nuls non inversibles toujours d'après la remarque précédente, ce qui conclut la preuve. ■

Corollaire. ***(Irréductibles constant d'un corps)***

Si A est un corps, l'anneau $A[X]$ n'a aucun irréductible constant.

Puisque A est supposé intègre, $A[X]$ se plonge $\longrightarrow (Frac(A))[X]$ mais la question d'irréductibilité dans cette A-algèbre est non seulement peut-être mauvaise *(voir la suite)*, mais n'est pas directement reliée à celle de l'irréductibilité dans $A[X]$.

Exemple fondamental

$A = \mathbb{Z}$, $P = 2X - 2 = 2(X - 1)$ n'est pas un irréductible ! On va voir qu'en fait, sur un anneau factoriel A, c'est essentiellement le seul défaut d'irréductibilité qui se produise.

Cet exemple est fondamental car il montre combien le problème vient de ce que l'on peut factoriser les coefficients du polynôme irréductible dans le corps par un non-inversible dans l'anneau et donc, en vertu de la proposition précédente, obtenir une décomposition licite (*i.e.* sans inversible.

Définition. ***(Polynôme primitif)***

Soit A un anneau intègre et $P \in A[X]$. Le polynôme P est dit *primitif* si les coefficients de P sont premiers entre eux dans leur ensemble. Concrètement : $P = \sum_{i=1}^{N} a_i X^i$ et $(a_0,...,a_N) = A$.

Conséquence. ***(Primitivité des polynômes unitaires)***

Les polynômes unitaires sont primitifs.

Propriété. ***(Lien entre irréductibilité et primitivité)***

Soit A intègre, $P \in A[X]$ tel que $\deg(P) \geqslant 1$. Alors si P est irréductible, il est primitif.

▷ Si P n'est pas primitif, il existe un élément $a \in A$ non nul et non inversible qui divise les coefficients de P. Ainsi $P = aQ$ où ni a, ni Q n'est inversible ou nul. Ainsi P est réductible. On conclut par contraposition. ■

Attention, la réciproque est grossièrement fausse (ce serait trop simple). En effet, le polynôme $X^2 - 1$ est primitif dans $\mathbb{Z}[X]$ mais certainement pas irréductible.
Profitons pour remarquer que, si A est un corps, cette notion est caduque : tous les polynômes sont primitifs, puisque tout PGCD est associé à 1.

La réciproque exprime un lien entre les irréductibles de $Frac(A)[X]$ et ceux de $A[X]$ dans le cas primitif.

Propriété. ***(Irréductibles primitifs de $A[X]$)***

Soit A intègre, $P \in A[X]$ tel que $\deg(P) \geqslant 1$. Si P est primitif et s'il est irréductible dans $Frac(A)[X]$, alors il est irréductible dans $A[X]$.

▷ Supposons que P soit réductible dans $A[X]$. Ainsi $P = QR$ où $(Q,R) \in (A[X])^2$. Supposons que P est primitif et montrons qu'il est réductible dans $Frac(A)[X]$. On a $\deg(Q), \deg(R) > 1$, autrement on aurait un diviseur non unitaire de tous les coefficients de P donné par Q ou R constante de A, donc Q,R ne sont pas inversibles dans $Frac(A)[X]$ et bien sûr non nuls donc P est réductible dans $Frac(A)[X]$. ■

Cela ne signifie pas que l'irréductibilité dans $Frac(A)[X]$ soit chose aisée toutefois. On donne un exemple édifiant.

Curiosité. ***(Pathologie de l'irréductibilité dans $\mathbb{Q}[X]$)***

Dans $\mathbb{Q}[X]$, il existe des polynômes irréductibles de tout ordre.

▷ On peut prendre, en utilisant le critère d'Eisenstein ou la réduction modulo 2 que l'on verra ensuite, le polynôme $X^n + 2X^{n-1} + 2X^{n-2} + ... + 2X + 2$. Ce polynôme est irréductible sur $\mathbb{Q}$ pour tout n ce qui donne des irréductibles dans $\mathbb{Q}[X]$ de tout degré. ■

On dispose dès maintenant du lemme suivant, qui peut se révéler très utile en pratique. De loin, la réduction modulo un idéal est un des arguments les plus efficaces pour prouver l'irréductibilité (meilleur que le critère d'Eisenstein qui en découle mais ne s'applique qu'aux polynômes à coefficients dans un anneau factoriel).

Lemme. ***(Critère de réduction modulo un idéal premier)***

Soit A un anneau intègre et I un idéal premier de A. Soit P un polynôme primitif à coefficients dans A non constant. On suppose que le coefficient dominant de $P \notin I$. Alors si la réduction de P modulo I est irréductible dans $(A/I)[X]$, alors P est irréductible dans $A[X]$.

▷ Par contraposée, supposons P, que l'on peut supposer non nul, réductible dans $A[X]$. Alors $P = QR$ où Q,R sont non nuls et non inversibles et P est primitif donc Q,R ne sont pas constants. De plus les coefficients dominants de Q et de R ne sont pas dans I. On réduit : $\overline{P} = \overline{QR}$. Alors $\overline{Q}, \overline{R}$ ne sont pas constants, car aucun de leurs deux coefficients dominants ne sont pas dans I, autrement leur produit $a_n = a_{\mathrm{dom}(P)}$ le serait, et l'on constate donc que $\overline{Q}, \overline{R} \notin ((A/I)[X])^* = (A/I)^*$, qui sont tous des polynômes de degré 1, étant donné que A/I est intègre, car I est premier, et puisque $(A/I)[X] \simeq A[X]/IA[X]$. Ils sont bien sûr non nuls car sinon $\overline{P}$ le serait mais c'est impossible pour le même argument. Ainsi $\overline{P}$ est réductible dans $(A/I)[X]$. ■

Remarque. On peut supprimer l'hypothèse P primitif, quitte à remplacer $P = ct(P)P_0$; mais alors on n'obtient l'irréductibilité que dans $FracA[X]$.

On remarque également la proposition suivante avant de passer à la suite.

Propriété. ***(Caractérisation de la primitivité par la réduction modulo les irréductibles)***

Un polynôme $P \in A[X]$ est primitif si et seulement si, pour tout irréductible $f \in A$, la réduction de P modulo (f) est non nulle.

▷ Le faire. ■

On suppose maintenant, et dans toute la suite, **que A est factoriel.** Remarquons que dans ce cas, $P \in A[X]$ est primitif si et seulement si le PGCD de ses coefficients est 1.

Propriété. ***(Lemme de Gauss pour les polynômes primitifs)***

Si A est factoriel, le produit de deux polynômes primitifs de $A[X]$ est primitif.

▷ Si P,Q sont primitifs, alors pour tout élément irréductible f de A, alors $\overline{P}, \overline{Q} \in A/(f)[X] \setminus \{0\}$. Mais $\overline{PQ} \neq 0$, car $A/(f)$ est intègre ; en effet, $A/(f)[X] \simeq A[X]/fA[X]$ l'est, car f es premier, car A est factoriel. On a montré que pour tout irréductible, la réduction modulo cet irréductible de PQ est non nulle, car $\overline{PQ} = \overline{P} \cdot \overline{Q}$. Donc PQ est primitif. ■

On peut aisément fournir une preuve arithmétique de ce fait (elle utilise le lemme de Gauss dans un anneau factoriel, et justifie ainsi l'appellation) :

▷ Raisonnons par l'absurde, en supposant qu'il existe deux polynômes primitifs $P = \sum a_i X^i$ et $Q = \sum b_j X^j \in A[X]$ dont le produit PQ est divisible par un élément non inversible de A. Choisissons

alors un couple (i,j) de somme maximum parmi les couples d'indices tels qu'un certain diviseur non inversible d de PQ divise aussi $a_0,...,a_{i-1},b_0,...,b_{j-1}$. Par maximalité, d est premier avec a_i et b_j, donc par le lemme de Gauss dans un anneau factoriel, avec a_ib_j, en particulier, il ne divise pas a_ib_j. C'est impossible, puisqu'il divise tous les autres termes de la somme $\sum_{i'+j'=i+j} a_{i'}b_{j'}$ et qu'il divise cette somme. ■

On peut le reformuler sous la forme suivante :

Propriété. ***(Lemme de Gauss, version historique)***

Soient P,Q deux polynômes unitaires à coefficients rationnels. Si $PQ \in \mathbb{Z}[X]$, alors P et $Q \in \mathbb{Z}[X]$.

Ce résultat peut monter en généralité en définissant la notion de contenu d'un polynôme, qui fait écho à l'exemple fondamental précédent.

Définition-propriété. ***(Contenu d'un polynôme)***

Soit A un anneau factoriel et K son corps des fractions. Soit P un polynôme non nul à coefficients dans K. Alors il existe un élément non nul de K, unique à association près dans A, noté c, tel qu'il existe un polynôme primitif Q de $A[X]$ avec $P = cQ$.

▷ Si $P \in A[X] \subseteq K[X]$ où $K = Frac(A)$, c le PGCD des coefficients, $P = cQ$ où Q est primitif. Si $P \in K[X]$, il existe $d \in A \setminus \{0\}$ tel que $dP \in A[X]$. Donc par le premier argument il existe $\gamma \in A$ tel que $dP = \gamma Q$ avec $Q \in A[X]$ primitif. Alors $c = \frac{\gamma}{d}$ convient ; ainsi $P = \frac{\gamma}{d}Q$ avec $Q \in A[X]$ primitif. Il y a donc existence du contenu. De plus, si $P = c_1Q_1 = c_2Q_2$ où $c_1,c_2 \in K \setminus \{0\}$ et $Q_1,Q_2 \in A[X]$, quitte à multiplier par un élément de A non nul, on peut supposer que c_1,c_2 appartiennent à A et sont non nuls. Posons $c_1' = cc_1$ et $c_2' = cc_2$. On a $c_1'Q_1 = c_2'Q_2 \in A[X]$, $c \neq 0$. Ainsi c_1' est le PGCD des coefficients de $c_1'Q_1$ mais également de $c_2'Q_2$, donc $c_1' \sim c_2'$ d'où $c_1 = c_2$. ■

Le contenu d'un polynôme est défini pour des polynômes à coefficients dans **un corps de fractions**. Attention, en toute généralité, le contenu dans le corps c'est pas le pgcd des coefficients, ce qui est vrai si le polynôme est à coefficient dans l'anneau dessous ; c'est par contre le pgcd des numérateurs des fractions en coefficient divisé par le ppcm des dénominateurs de ces mêmes fractions.

Cette expression est bien à valeurs dans A, puisque le PGCD d'une famille divise trivialement son PPCM. On peut la reformuler, la preuve étant laissé au lecteur.

Propriété. ***(Calcul du contenu)***

Si A est factoriel, on note K son corps des fractions. Soit $P \in K[X], P = \sum \frac{n_i}{d_i}X^i$ où $n_i, d_i \in A$. Alors $c(P) \sim \frac{\text{pgcd}(n_i)}{\text{ppcm}(d_i)}$.

Pour s'éclaircir les idées.

Propriété. ***(Contenus triviaux : contenu dans A)***

Si A est factoriel, on note K son corps des fractions. Alors pour tout $P \in K[X]$ non nul, $P \in A[X]$ si et seulement si $c(P) \in A \setminus \{0\}$.

▷ On rappelle qu'un contenu est de toute manière non nul. L'expression de la propriété précédente donne un contenu de P. Or, si l'on écrit les coefficients de P comme fractions, leurs dénominateurs sont tous 1, donc leur ppcm est 1, d'où un contenu égal à un pgcd d'élément de A, donc le contenu est dans A. Réciproquement, si $c \in A$, puisque $Q \in A[X]$, $P = cQ$ est dans $A[X]$. ■

Propriété. ***(Contenus triviaux : contenu dans A^*)***

Si A est factoriel, on note K son corps des fractions. Alors pour tout $P \in K[X]$ non nul, $P \in A[X]$ est primitif dans $A[X]$ si et seulement si $c(P) \in A^*$, c'est-à-dire $c(P) \sim 1$.

▷ En reprenant le raisonnement précédent, on a un contenu égal au pgcd des coefficients de P. S'il est primitif, c'est un pgcd associé à 1. Réciproquement, si $c = 1$, alors $P = Q$ est primitif. ■

Ainsi, pour résumer : pour tout $P \in Frac(A)[X]$, il existe un unique $c \in Frac(A)$ tel que :

$$\boxed{P = cP^\star}$$

avec $P^\star \in A[X]$ primitif.

Le résultat le plus important sur cette notion est sans aucun doute le suivant :

Propriété. ***(Lemme de Gauss pour les polynômes)***

Si A est factoriel, on note K son corps des fractions. Soient $P_1, P_2 \in K[X]$. Alors $c(P_1P_2) = c(P_1)c(P_2)$ (à un inversible près).

▷ On a $P_1 = c(P_1)Q_1$ et $P_2 = c(P_2)Q_2$ où $Q_1, Q_2 \in A[X]$ sont primitifs. Ainsi $P_1P_1 = c(P_1)c(P_2)Q_1Q_2$. Puisque, d'après la première version du lemme de Gauss, $Q_1Q_2 \in A[X]$ est primitif, par unicité du contenu, on a $c(P_1P_2) \sim c(P_1)c(P_2)$. ■

Il n'y a aucune hypothèse de primalité relative sur P, Q ! Le contenu est une forme complètement multiplicative de $A[X]$.

Propriété. ***(Lemme de Gauss, version historique)***

Soient deux polynômes unitaires P, Q. Si leurs coefficients à eux deux sont tous rationnels, sans être tous entiers, alors leur produit PQ a au moins un coefficient qui n'est pas entier.

▷ Avec le formalisme moderne, si A est un anneau intègre et K son corps des fractions, il s'agit de montrer que si P,$Q \in K[X]$ et $PQ \in A[X]$, alors P et $Q \in A[X]$. Supposons $PQ \in A[X]$. Alors $c(PQ) = c(P)c(Q) \in A$. On a $c(P) = \frac{1}{a}$ et $c(Q) = \frac{1}{b}$ puisque P,Q sont unitaires et a est le ppcm des dénominateurs des coefficients de P, idem pour b et Q. Ainsi, $\frac{1}{ab} = c(PQ) \in A$, donc $1 = abk$ pour $k \in A$. Donc $a(bk) = 1$ et $b(ak) = 1$, donc a,b sont inversibles dans A, donc leurs inverses également, donc P,$Q \in A[X]$. ■

Avec ces outils, on peut en déduire l'hérédité de la factorialité.

Théorème. ***(Théorème de Gauss)***

Soit A un anneau factoriel. Alors $A[X]$ est factoriel.

▷ On utilise la deuxième caractérisation de la factorialité. Soit $((P_n))_{n\in\mathbb{N}}$ une suite croissante d'idéaux principaux. Or on peut supposer sans problème les P_i non nuls. Pour tout $n \geqslant 0$, $(P_n) \subseteq (P_{n+1})$ donc P_{n+1} divise P_n dans $A[X]$. La suite $(\deg(P_n))_{n\in\mathbb{N}}$ est donc une suite décroissante à valeurs dans $\mathbb{N}$ donc stationnaire par axiome du bon ordre. Soit $N \in \mathbb{N}$ un rang à partir duquel la suite est constante. On note, pour tout n, c_n le coefficient directeur de P_n. Ainsi dès que $n \geqslant N$, $P_{n+1} \mid P_n$ dans $A[X]$ et $\deg P_{n+1} = \deg P_n$. On en déduit que c_{n+1} divise c_n dans A. La suite $((c_n))_{n\in\mathbb{N}}$ est une suite croissante d'idéaux principaux de A qui est factoriel, donc elle est stationnaire. Ainsi il existe un rang M à partir duquel pour tout n $(c_n) = (c_{n+1})$ *i.e.* il existe $d_n \in A^*$ tel que $d_n c_{n+1} = c_n$. Pour tout $n \geqslant M$, on a donc $d_n P_{n+1} = P_n$. Puisque $A^* = (A[X])^*$, on a pour tout $n \geqslant M$, $(P_n) = (P_M)$, car deux polynômes de même degré et de même contenu dont l'un divise l'autre, sont associés.

Soit maintenant P un polynôme irréductible de $A[X]$. Montrons que l'idéal qu'il engendre est premier. Si P est de degré 0, il est irréductible dans A. Donc l'idéal qu'il engendre dans A est premier, car A est factoriel donc $A/(P)$ est intègre, donc $A/(P)[X]$ est intègre. Mais $A/(P)[X] \simeq A[X]/(P)$ donc $A[X]/(P)$ est intègre, donc $A[X]$ est premier. Soit P irréductible de $A[X]$ non constant. Montrons que $(P) = P \cdot A[X]$ est premier. Soient Q,$R \in A[X]$ tels que $P \mid QR$. Il est évident que si P divise QR dans $A[X]$, il le divise aussi dans $K[X]$ où K est le corps des fractions de A. Or $K[X]$ est factoriel (car il est euclidien !). De plus, P est irréductible dans $A[X]$ donc a fortiori dans $K[X]$. Ainsi P est premier, car $K[X]$ vérifie la deuxième propriété. Donc P divise Q ou R dans $K[X]$. Par symétrie, on peut supposer que P divise Q dans $K[X]$. On écrit $Q = PT$ où $T \in K[X]$. Par lemme de Gauss, $cont(Q) = cont(P)cont(T)$. Or $cont(Q) \in A \setminus \{0\}$ et $cont(P) \in A^*$. On en déduit que $cont(T) \in A \setminus \{0\}$ et donc $T \in A[X]$. ■

Remarque. Il est remarquable que $(F1')$ dans A implique $(F1')$ dans $A[X]$ et $(F2')$ dans A implique $(F2')$ dans $A[X]$. (Les preuves « ne se croisent pas ».)

Théorème. ***(Irréductibles des polynômes à coefficients dans un factoriel)***

Soit A un anneau factoriel. Les éléments irréductibles de $A[X]$ non constants sont les polynômes primitifs et irréductibles dans $Frac(A)[X]$.

▷ On sait déjà que si $P \in A[X]$ est irréductible dans $A[X]$, alors P est primitif. Il reste à montrer que P est irréductible dans $K[X]$. Par l'absurde, supposons que P est réductible dans $K[X]$. Par l'absurde, supposons le contraire : $P = P_1P_2$. Sauf cas limite, on suppose $\deg P_1, \deg P_2 \geqslant 1$. On a $P_1 = c(P_1)Q_1$ et $P_2 = c(P_2)Q_2$ où $Q_1, Q_2 \in A[X]$ sont primitifs. Ainsi $A[X] \ni P = c(P_1)c(P_2)Q_1Q_2$. Or $c(P_1)c(P_2) = c(P) \in A \setminus \{0\}$. Ainsi on a $Q_1' = c(P_1)c(P_2)Q_1 \in A[X]$ et $P = Q_1'Q_2$ ce qui contredit l'hypothèse. ■

Ainsi, dans le cas d'un anneau factoriel, l'irréductibilité dans $A[X]$ se ramène à celle dans le corps des fractions, à une multiplication et calcul de PGCD près, celui des contenus, dans A.

Remarque. Les critères d'irréductibilité ne s'appliquent qu'à des polynômes de coefficient constant non nul, et c'est pas grave (pourquoi ?) !

Théorème. ***(Critère d'Eisenstein)***

Soit A factoriel et P un polynôme de coefficients notés a_i, de degré n. Soit f un irréductible. Supposons que f divise tous les a_i, $i < N$ mais ne divise pas a_N, supposons également que f^2 ne divise pas a_0. Alors P est irréductible dans $Frac(A)[X]$. (S'il est primitif, il est donc aussi irréductible dans A[X].)

▷ Supposons dans un premier temps P primitif. Si P était réductible dans $A[X]$, il s'écrirait $P = QR$ deux polynômes de degré au moins 1. Les coefficients dominants de Q et de R n'appartiennent pas à (f). On réduit P modulo (f) ce qui donne $\overline{P} = \overline{QR} = \overline{a_n}X^n \in A/(f)[X]$. Or $A/(f)$ est intègre puisque f est irréductible ? Donc $\overline{Q}$ et $\overline{R}$ sont des monômes de degré 1 car dans un anneau intègre les diviseurs des monômes sont les monômes. Les termes constants de Q et R sont tous les deux dans (f). Ceci impliquerait que $a_0 \in (f^2)$, contradiction. On a montré que si P est primitif, il est irréductible dans $A[X]$. Si P n'est pas primitif, $P = c(P)Q$ où Q est primitif et $c(P) \in A \setminus \{0\}$. Montrons que Q est irréductible dans $A[X]$. Pour cela vérifions les hypothèses de la proposition. On a $c(P) \mid a_n$ donc $c(P)$ est premier à f. Si Q est un polynôme de coefficients notés b_k, de degré inférieur à n. En fait, Q est de degré n par construction. On a f qui ne divise pas b_n et f qui divise b_k pour tout $k < n$. Puisque f^2 ne divise pas b_0, $a_k = c(P)b_k$. Donc Q satisfait les hypothèses et c'est fini. ■

Corollaire. ***(Eisenstein faible)***

Soit A factoriel, p un élément irréductible. Si $P = X^d + a_{d-1}X^{d-1} + ... + a_0 \in A[X]$. Si $p \mid a_i$ (tous) mais p^2 pas a_0, alors P est irréductible dans $A[X]$ et dans $Frac(A)[X]$.

Exemple fondamental. ***(Polynômes cyclotomiques d'ordre premier)***

On sait que les polynômes cyclotomiques sont irréductibles sur Q. Puisqu'ils sont unitaires, donc primitifs, ils sont irréductibles sur $\mathbb{Z}$. On peut le redémontrer avec le critère d'Eiseinstein pour les polynômes cyclotomiques ϕ_p, p premier.
On montre que $P = X^{p-1} + ... + X + 1$ est irréductible, sur $\mathbb{Z}$ ou sur $\mathbb{Q}$, c'est la même

chose. On fait le changement de variables $X = Y+1$, ce qui revient à montrer que $P(Y+1)$ est irréductible. On applique le critère d'Eisenstein à ce polynôme en se rappelant que p divise C_p^k pour tout k entre 1 et $p-1$.

Méthode. ***(Adapter un polynôme au critère d'Eisenstein)***

Soit P un polynôme dont 1 n'est pas racine. Alors si $P(Y+1)$ est irréductible, P est irréductible. En effet, une écriture $P = QR$ implique $P(Y+1) = Q(Y+1)R(Y+1)$. Il est clair que ces deux facteurs ne sont pas inversibles si Q,R ne le sont pas eux-mêmes. On observe que $Q(Y+1) = 0$ ne peut être nul que si $Q = Y-1$, ce qui est exclu par hypothèse.

5.1.4 Fonctions polynomiales

5.1.4.1 Définition

5.1.4.2 Fonctions polynomiales sur un corps fini

Propriété. ***(Fonctions polynomiales sur un corps fini)***

Soit K un corps fini. Alors tout fonction de K dans K est polynomiale.

▷ Soient $x_1,...,x_n$ les éléments de K pour $n = \text{card}(K)$. Soit $f : K \longrightarrow K$. Pour tout i, on pose $y_i = f(x_i)$. On pose le polynôme interpolateur de Lagrange : $P = \sum_{i=1}^{n} y_i \prod_{j=1, j\neq i}^{n} \frac{X - x_j}{x_i - x_j} \in K[X]$. Il est clair que pour tout $x_i \in K$, $P(x_i) = f(x_i)$, donc $\tilde{P} = f$. Ainsi f est polynomiale. ■

Attention ! La fonction polynomiale n'est pas associée à un unique polynôme, comme le laisse entendre légèrement la preuve précédente. On s'intéressera plus tard au noyau de l'application $P \longmapsto \tilde{P}$.

Corollaire

Soit K un corps. Alors toute fonction de K dans K est polynomiale si et seulement si K est fini.

▷ Le sens indirect est donné par la propriété précédente. Réciproquement, s'il existe une surjection $K[X] \longrightarrow K^K$, problème : $K[X]$ est de cardinal K tandis que K^K est de cardinal $\mathcal{P}(K)$. Impossible par théorème de Cantor. ■

On a le même résultat que dans K dans le cas à plusieurs variables (on peut même vérifier sans encombres que le corollaire est encore vrai).

Propriété. ***(Fonctions polynomiales de plusieurs variables sur un corps fini)***

Soit K un corps fini et p un entier naturel. Alors toute fonction de K^p dans K est polynomiale.

▷ On adapte la preuve précédente. Soient $x_1,...,x_n$ les éléments de K pour $n = \text{card}(K)$. Soit $f : K^p \longrightarrow K$. Pour tout $(x_{i_1},...,x_{i_p}) \in K^p$, on pose $y_{i_1,...,i_p} = f(x_{i_1},...,x_{i_p})$. On pose le polynôme interpolateur : $P = \sum_{(i_1,...,i_p)\in[\![1,n]\!]^p} y_{i_1,...,i_p} \prod_{j=1,j\neq i_1}^{n} \frac{X_1 - x_j}{x_{i_1} - x_j} ... \prod_{j=1,j\neq i_p}^{n} \frac{X_p - x_j}{x_{i_p} - x_j} \in K[X_1,...,X_p]$. Il est clair que pour tout $(x_{i_1},...,x_{i_p}) \in K^p$, $P(x_{i_1},...,x_{i_p}) = f(x_{i_1},...,x_{i_p})$, donc $\tilde{P} = f$. Ainsi f est polynomiale. ■

Corollaire

Soit K un corps. Alors toute fonction de K^p dans K est polynomiale si et seulement si K est fini.

▷ Le sens indirect est donné par la propriété précédente. Réciproquement, s'il existe une surjection $K[X_1,...,X_p] \longrightarrow K^{K^p}$, problème : $K[X_1,...,X_p]$ isomorphe à $K[X]$ est de cardinal K tandis que $K^{K^p} \simeq K^K$ est de cardinal $\mathcal{P}(K)$. Impossible encore par théorème de Cantor. ■

5.1.5 Dérivation en une variable

Soit A un anneau.

Proposition. ***(Caractérisation de la dérivation polynomiale)***

La dérivation dans $A[X]$ est l'unique application D linéaire sur A vérifiant la règle de Leibniz et $D(X) = 1$.

▷ Il manque seulement la valeur de $D(1)$ qui est donnée par la formule de Leibniz. ■

Remarque importante. Deux conséquences : $DQ^n = nD(Q)Q^{n-1}$ et $\deg(DP) < \deg(P)$.

Remarque. Même si A n'est pas un corps, donc $A[X]$ n'est pas euclidien, on peut faire la division euclidienne de P par $X - x$ car il est unitaire donc son coefficient dominant est inversible. On montre ainsi que x est racine n-ième de P si et seulement si $(X - x)^n$ divise P si et seulement si $P(x) = 0$, $DP(x) = 0$, $DD(P)(x) = 0$, mais $D \circ ... \circ DP(x) \neq 0$.

Théorème. ***(Noyau de la dérivation en caractéristique finie première)***

Soit A un anneau intègre. Si $\text{car}(A)$ est un nombre premier p, alors $DP = 0$ si et seulement si $P \in A[X^p]$.

Proposition. ***(Dérivation trop grande en caractéristique nulle)***

Soit A un anneau de caractéristique n. Alors pour tout $k \geqslant n$, pour tout $P \in A[X]$, $D^k(P) = 0$.

Théorème. ***(Noyau de la dérivation en caractéristique infinie)***

Soit A un anneau intègre. Si $\mathrm{car}(A)$ est nulle, alors $DP = 0$ si et seulement si $P \in A$.

Théorème. ***(Formule de Taylor)***

Soit A un anneau intègre **de caractéristique nulle**. Alors pour tout $n \in \mathbb{N}$, $n!$ divise $D^n P$ et :

$$P = \sum_{n \in \mathbb{N}} \frac{D^n P(x)}{n!} (X - x)^n.$$

Remarque. Cette somme est licite, car finie, car le degré décroit strictement et l'ordre de $\mathbb{N}$ est bon.

▷ On utilisera la caractérisation de la nullité de la dérivée d'un polynôme explicitement dérivé au niveau des coefficients. En caractéristique nulle, d'après ce qui précède, c'est facile. Ensuite, on s'intéresse à $D^n(X^m) = n! C_k^n X^{m-n}$ en caractéristique quelconque. On montre la formule de Taylor par récurrence forte sur le degré de P. On ne peut toutefois "primitiver" DP donc on pose Q ce qu'on veut, on calcule DQ. Puis $D(Q - P) = 0$. En caractéristique nulle, c'est une constante et il suffit d'évaluer en x pour conclure. ■

Corollaire. ***(Noyau de la dérivation itérée)***

Soit A intègre et de caractéristique nulle. Alors $P \in ((X - x)^n)$ si et seulement si pour tout $i = 0,...,n-1$, $D^i P(x) = 0$.

Remarque. Si l'on se pose des questions de multiplicité des racines d'un polynôme aux coefficients dans un corps fini, ou en caractéristique positive, on ne dispose pas de la formule de Taylor et l'on ne s'en sert pas avec les dérivées. En effet, la réciproque ci-haut est fausse, et c'est le sens qui sert. En caractéristique p, on a $P = X^p$ tel que $D^n P = 0$ pour tout $n > 0$. En particulier $D^n P(0) = 0$ pour tout n mais $P \notin (X^{p+1})$.

Même chose pour déterminer l'ordre exact d'une racine, ça ne marche pas : $P \notin (X - x)^{n+1}$ mais $D^{n+1}(x) \neq 0$.

La caractérisation $X - a \mid P$ si et seulement si $P(a) =$ marche toujours dans un anneau non nul. Mais à l'ordre k, elle marche seulement si $\mathrm{car}(A) > k - 1$. Ainsi, dans un corps, le critère différentiel pour les racines doubles est toujours valable. Par contre, à l'ordre 3, cela ne marche plus dans un corps de caractéristique 2 par exemple !

5.1.5.1 Dérivées partielles

Dans cette partie, on se pose A un anneau commutatif et I un ensemble de sorte qu'on construise $A[(X_i)_{i\in I}]$ l'anneau des polynômes à $\mathrm{card}(I)$ indéterminées. On rappelle que pour tout $i \in I$, il existe un isomorphisme canonique $\phi_i : A[(X_i)_{i\in I}] \simeq A[(X_i)_{i\in I\setminus\{i\}}][X_i]$. De plus, lorsque I est fini, on identifie l'anneau des polynômes correspondant à $A[X_1,...,X_n]$ et on a les mêmes isomorphismes.

Définition. ***(Dérivée partielle)***

Soit $i \in I$. La dérivée selon la variable i $D_iP = \frac{\partial}{\partial X_i}P$ est la dérivée du polynôme $\phi_i(P)$.

Propriété

$D_i(X_j) = \delta_{i,j}$.

Propriété. ***(Lemme de Schwartz)***

Sans hypothèse, $D_i \circ D_j = D_j \circ D_i$.

Remarque. L'absence d'hypothèse n'étonne pas puisque les polynômes sont tous C^2...

On suppose maintenant I fini.

Théorème. ***(Formule de Taylor en dimension n)***

Soit A un anneau intègre de caractéristique nulle. Soit $P \in A[X_1,...,X_n]$, $x = (x_1,...,x_n) \in A^n$.

$$P = \sum_{\underline{m}=(m_1,...,m_n)\in\mathbb{N}^n} \frac{1}{m_1!...m_n!} \underbrace{\left(\frac{\partial^{m_1}}{\partial x_1^{m_1}}...\frac{\partial^{m_n}}{\partial x_n^{m_n}}P\right)}_{\frac{\partial^{\underline{m}}}{\partial x_{\underline{m}}}P}(x) \prod_{i=1}^{n}(X_i - x_i)^{m_1}.$$

▷ Récurrence simple immédiate sur le nombre de variables. ■

Théorème. ***(Formule d'Euler)***

Soit $P \in A[X_1,...,X_n]$ homogène de degré d. Alors

$$\sum_{i=1}^{n} X_i \frac{\partial}{\partial x_i}P = dP.$$

▷ Sur les monômes et l'on conclut par linéarité. ■

5.2 Polynômes en plusieurs variables

5.2.1 Construction de l'anneau des polynômes en plusieurs variables

5.2.1.1 Construction directe abstraite

On rappelle la notation suivante : si I est un ensemble, alors $\mathbb{N}^{(I)}$ est l'ensemble des suites d'entiers naturels presque nulle (c'est-à-dire, nulle sur le complémentaire d'une partie finie de I) indexées par I. Dans toute la suite, on note $M = \mathbb{N}^{(I)}$.

Définition. ***(Multi-indices)***

On appelle *multi-indice*, tout élément de M.

Soit A un anneau unitaire. On définit sur $A^{(M)}$ deux opérations : si $P = (a_n)_{n\in M}$ et $Q = (b_n)_{n\in M}$, on définit :

$$P + Q = (a_n + b_n)_{n\in\mathbb{N}}$$

et :

$$PQ = (c_n = \sum_{\substack{(l,k)\in M^2 \\ l+k=n}} a_l b_k)_{n\in\mathbb{N}}.$$

Remarque. Le cardinal de I donne le nombre de variables.

Théorème. ***(Polynômes en un nombre quelconque de variables)***

$(A^{(M)}, +, \cdot\ )$ est un anneau.

⟶ **Notation.** On notera de façon assez standard : $P \sum_{m\in M} X^m$.

On a les propriétés (attendues) suivantes :

Propriété. ***(Multimonômes)***

$$X^m = \prod_{i\in I} X_i^{m_i}.$$

En fait, X^m est une suite d'éléments de A presque nulle, avec $X^m = (a_n)_{n\in M}$ avec $a_n = 0$ si $n \neq m$ et 1 si $n = m$.

Propriété. ***(Produit de monômes)***

Pour a,$b \in A$, $(aX^m) \cdot (bX^n) = abX^{n+m}$.

Fait. ***(Algèbre des polynômes en un nombre quelconque de variables)***

$A^{(M)}$ est une A-algèbre.

▷ Il suffit de considérer le morphisme d'anneaux $\eta : a \longrightarrow aX^0$ $(0 \in \mathbb{N}^{(I)})$). ■

Remarquons que $1_{A^{(M)}} = X^0 = \eta(1_A)$.

⟶ **Notation.** On notera : $A^{(M)} = A[(X_i)_{i\in I}]$, lorsque muni de ces lois.

⟶ **Notation.** On notera : X_i la *i-ième indéterminée.*

Exercice 104

Construire le corps des séries formelles de Laurent en un nombre quelconque de variables.

De même que pour les polynômes en une variable, les polynômes formel en I variables ne coïncident pas en général avec les fonctions polynomiales associées.

Propriété. ***(Propriété universelle des polynômes en plusieurs variables)***

Soit A un anneau, soit I un ensemble. Soit B une A-algèbre commutative. Soit $(x_i)_{i\in I}$ une famille d'éléments de B. Il existe un unique morphisme de A-algèbre :

$$\begin{aligned} e : \quad A[(X_i)_{i\in I}] &\longrightarrow B \\ X_i &\longmapsto e(X_i) = x_i. \end{aligned}$$

On a l'identité de construction suivante :

Théorème. ***(Théorème fondamental de construction des polynômes en un nombre quelconque de variables)***

Soit A un anneau, et soient I et J deux ensembles. Alors I et J sont équipotents, si et seulement si, $A[(X_i)_{i\in I}]$ et $A[(X_j)_{j\in J}]$ sont isomorphes en tant qu'anneaux (ou en tant A-algèbres).

5.2.2 Cas particulier des polynômes en un nombre fini de variables

Ceci correspond au cas I fini. On peut prendre, par isomorphisme, $I = \{1,...,n\}$.

⟶ **Notation.** Dans ce cas on note : $A[(X_i)_{i\in[\![1,n]\!]}] = A[X_1,...,X_n]$

Propriété. ***(Théorème de regroupement par paquets)***

Soient n,p,q trois entiers non nuls tels que $n = p+q$. Soient i injectant $[\![1,p]\!]$ dans $[\![1,n]\!]$ et j injectant $[\![1,q]\!]$ dans $[\![1,n]\!]$ tels que $[\![1,n]\!] = i([\![1,p]\!]) \cup j([\![1,q]\!])$. Alors il existe un unique isomorphisme de A-algèbre

$$\phi : A[Y_1,...,Y_p][Z_1,...,Z_q] \longrightarrow A[X_1,...,X_n]$$

vérifiant $\phi(Y_k) = X_{i(k)}$ pour tout $k \in [\![1,p]\!]$ et $\phi(Z_k) = X_{j(k)}$ pour tout $k \in [\![1,q]\!]$. En particulier, $A[Y_1,...,Y_p][Z_1,...,Z_q] \simeq A[X_1,...,X_n]$.

▷ Par propriété universelle de $A[Y_1,...,Y_p]$, il existe un unique morphisme de A-algèbre, en particulier morphisme d'anneaux, $\phi_0 : A[Y_1,...Y_p] \longrightarrow A[X_1,...,X_n]$ qui à Y_k fait correspondre $X_{i(k)}$. Ainsi ϕ_0 munit $A[X_1,...,X_n]$ d'une structure de $A[Y_1,...,Y_p]$-algèbre. Par propriété universelle de $A[Y_1,...,Y_p][Z_1,...,Z_q]$ maintenant, il existe un unique morphisme de $A[Y_1,...,Y_p]$-algèbre de $A[Y_1,...,Y_p][Z_1,...,Z_q] \longrightarrow A[X_1,...,X_n]$ qui à Z_l fait correspondre $X_{j(l)}$. En particulier, ϕ est un morphisme de A-algèbres. Par propriété universelle de $A[X_1,...X_n]$, il existe un unique morphisme de A-algèbre : $\psi : A[X_1,...,X_n] \longrightarrow A[Y_1,...,Y_p][Z_1,...,Z_n]$ tel que $\psi(X_m) = Y_k$ si $i(k) = m$ et Z_k si $j(k) = m$. On peut vérifier que ϕ et ψ sont inverses l'une de l'autre. ■

On n'utilise pas la finitude de I. Ceci donne :

Propriété. ***(Théorème de regroupement par paquets)***

Soient J,K tels que $J \cap K = \emptyset$ et $J \cup K = I$. Alors $A[(X_i)_{i\in I}] \simeq A[(Y_j)_{j\in J}][(Z_k)_{k\in K}]$, et si j et k sont les projections respectives de J et K dans I, alors il existe un unique isomorphisme de A-algèbre

$$\phi : A[(Y_j)_{j\in J}][(Z_k)_{k\in K}] \longrightarrow A[(X_i)_{i\in I}]$$

vérifiant $\phi(Y_x) = X_{j(x)}$ pour tout $x \in J$ et $\phi(Z_t) = X_{k(t)}$ pour tout $t \in K$.

En particulier (conséquence du premier théorème) :

Propriété. ***(Théorème de regroupement par paquets)***

Pour tout anneau A, $A[X,Y] \simeq A[X][Y] \simeq A[Y][X]$.

On peut donc donner des propriétés héréditaires pour le cas d'un nombre fini de variables.

Corollaire. ***(Propagation de l'intégrité)***

Soit n un entier naturel. Si A est intègre, $A[X_1,...,X_n]$ est intègre.

Corollaire. ***(Propagation de la factorialité)***

Soit n un entier naturel. Si A est factoriel, $A[X_1,...,X_n]$ est factoriel.

Corollaire. ***(Propagation de la noethérianité)***

Soit n un entier naturel. Si A est noethérien, $A[X_1,...,X_n]$ est noethérien.

Dans le cas principal et euclidien, tout va mal, comme on sait.

Propriété. ***(Non-propagation de la principalité)***

Soit n un entier naturel. Alors $A[X_1,...,X_n]$ est principal si et seulement si $n = 1$ et A est un corps.

Propriété. ***(Non-propagation de l'euclidianité)***

Soit n un entier naturel. Alors $A[X_1,...,X_n]$ est euclidien si et seulement si $n = 1$ et A est un corps.

5.2.2.1 Fonctions polynomiales et morphisme d'évaluation

Dans toute la suite, on utilise la notation générique : $P \in A[X_1,...,X_n]$ et $P = \sum_{\underline{m} \in \mathbb{N}^n} a_{\underline{m}} \prod_{i=1}^{n} X_i^{m_i}$, où $\underline{m} = (m_1,...,m_n)$.

Définition. ***(Morphisme évaluation)***

Soit $\underline{x} = (x_1,...,x_n) \in A^n$. On définit l'*évaluation* en $\underline{x}$ par :

$$\begin{aligned} \mathrm{ev}_{\underline{x}} : \quad A[X_1,...X_n] &\longrightarrow A \\ P &\longmapsto P(x_1,...,x_n) = \sum_{\underline{m} \in \mathbb{N}^n} a_{\underline{m}} \left(\prod_{i=1}^{n} x_i^{m_i} \right). \end{aligned}$$

Définition. ***(Fonction polynomiale)***

On définit la *fonction polynomiale* associée à $P \in A[X_1,...,X_n]$, la fonction :

$$\begin{aligned} f = \tilde{P} : \quad A^n &\longrightarrow A \\ \underline{x} &\longmapsto \mathrm{ev}_{\underline{x}}(P). \end{aligned}$$

Heureusement :

Propriété. ***(Identification partielle polynômes/fonctions polynomiales)***

La fonction ϕ de $A[X_1,...,X_n]$ dans A^{A^n} qui à P fait correspondre $\tilde{P}$ est un morphisme de A-algèbre.

Le problème est que, comme on le sait sûrement déjà, une fonction polynomiale peut ne pas caractériser la fonction polynomiale dont elle est issue.

Exemple fondamental. ***(ϕ n'est pas injective)***

Dans $\mathbb{Z}/2\mathbb{Z}$ dans lui-même, le polynôme $P = X^2 - X$ est nul en 0 et en 1, donc la fonction polynomiale associée est identiquement nulle. Cependant, ce n'est pas le polynôme nul

(bien évidemment : $P = (0,1,1,0,0,...) \neq 0_{\mathbb{Z}/2\mathbb{Z}[X]} = (0,0,0,0,0,...)$) !

Afin de régler le problème, il est intéressant de connaître le noyau de l'application qui à un polynôme associe la fonction polynomiale de mêmes coefficients. La question est déjà fort intéressante si les coefficients vivent dans un corps ; on s'y réduit pour l'instant.

Propriété. ***(Identification polynômes/fonctions polynomiales sur un corps)***

Si $A = \mathbb{K}$ est un corps, alors ϕ est injective si et seulement si $\mathbb{K}$ est de cardinal infini.

On reprend I un ensemble quelconque, et ϕ est donc définie sur $A[(X_i)_{i\in I}]$.

Propriété. ***(Noyau de ϕ dans le cas fini)***

Si $A = \mathbb{K}$ est un corps fini de cardinal q, alors $\mathrm{Ker}(\phi) = ((X_i^q - X_i)_{i\in I})$.

▷ On suppose dans un premier temps I fini de cardinal n et l'on note ϕ_n la restriction à $K[(X_k)_{k\leqslant n}]$ de ϕ corestreinte à K^{K^n} qui se plonge dans K^{K^I}. Pour tout $k \leqslant n$, on pose $P_k = X_k^q - X_k$ et I l'idéal engendré par les P_k, $k \leqslant n$. On a déjà vu que $P_k \in \mathrm{Ker}(\phi_n)$. D'autre part, par théorème d'isomorphisme, on sait que $K[(X_k)_{k\leqslant n}]/\mathrm{Ker}(\phi_n) \simeq K^{K^n}$, car ϕ_n est surjective, car toute application de K^{K^n} est polynomiale. En particulier, $|K[(X_k)_{k\leqslant n}]/\mathrm{Ker}(\phi_n)| = \left|K^{K^n}\right| = q^{q^n}$. On va montrer que $K[(X_k)_{k\leqslant n}]/I = q^{q^n}$. Ainsi, puisque $I \subseteq \mathrm{Ker}(\phi_n)$, la projection canonique passe au quotient, et si l'on note $\tilde{p}$ une bijection entre les deux ensembles considérés, π_I la projection du quotient par I, $\mathrm{Ker}(\pi_n) = \mathrm{Ker}(\tilde{p}\circ\pi_I) = \mathrm{Ker}(\pi_I) = I$. Reste à montrer le lemme. Dans un anneau quelconque A, pour tous idéaux A, $A/(I+J) \simeq (A/I)/J$ et $A[X]/(I) \simeq (A/I)[X]$. Puisque $K[(X_k)_{k\leqslant n}] \simeq K[X_1]...[X_n]$, on a :

$$\frac{K[(X_k)_{k\leqslant n}]}{I} \simeq \frac{\frac{\frac{K[X_1]}{(P_1)}[X_2]}{(P_2)}[X_n]}{\ddots}[X_n]}{(\tilde{P}_n)}.$$

On aimerait utiliser n fois que $\frac{K[X]}{(P)}$ est un $\mathbb{K}$-espace vectoriel de dimension $\deg(P)$. Seulement, dès la deuxième étape, $\mathbb{K}[X]/(P_1)$ n'est plus un corps. On peut toutefois utiliser le lemme suivant : si A est un anneau fini et $P \in A[X]$ de coefficient dominant inversible, alors $|A[X]/(P)| = |A|^{\deg(P)}$. En effet, si $P' \in A[X]$, P a son coefficient dominant égal à 1, donc on peut effectuer une division euclidienne $P' = PQ + R$, d'où $|A[X]/(P)| \leqslant |A_{n-1}[X]|$. De plus, $\overline{R} = \overline{R'}$ si et seulement si P de degré n divise $R' - R$ de degré $\leqslant n-1$, donc si et seulement si $R = R'$. Ainsi $|A[X]/(P)| = |A_{n-1}[X]| = |A|^n = q^n$ et le lemme est prouvé. Puisque tous les P_k sont unitaires de degré q, on a :

$$\left|\frac{\frac{\frac{K[X_1]}{(P_1)}[X_2]}{(P_2)}[X_n]}{\ddots}[X_n]}{(\tilde{P}_n)}\right| = \underbrace{\left(((q^q)^q)^{\cdot^{\cdot^{\cdot}}}\right)^q}_{q \text{ fois}} = q^{q^n}.$$

Pour le cas infini, si $P \in \mathrm{Ker}(\phi)$, P n'a qu'un nombre fini d'indéterminées apparaissant dans son écriture algébrique, en considérant ϕ' comme précédemment pour n indéterminées, on a donc $P \in \mathrm{Ker}(\phi_n) = ((X_k^q - X_k)_{k\leqslant n}) \subseteq ((X_i^q - X_i)_{i\in I})$. On a donc bien $\mathrm{Ker}(\phi) \subseteq ((X_i^q - X_i)_{i\in I})$ ce qui permet de conclure. ■

Définition. ***(Morphisme de substitution)***

Soit A un anneau, n,p deux entiers naturels. Soient Q_1,...,Q_n n éléments de $A[Y_1,...,Y_p]$. Il existe un unique morphisme de A-algèbre $\psi : A[X_1,...,X_n] \longrightarrow A[Y_1,...,Y_p]$ qui à X_i fait correspondre α_i. On note $\psi(P) = P(Q_1,...,Q_n) \in A[Y_1,...,Y_p]$.

Exercice 105

Quels opérations sur les Q_i peut-on autoriser pour le morphisme de substitution soit bijectif ?

Pour obtenir des propriétés arithmétiques élémentaires utiles, on utilisera à profit le lemme suivant :

Proposition. ***(Idéaux des polynômes divisibles par les indéterminées)***

On a $P \in (X_i)$ si et seulement si $P(X_1,...,X_{i-1},0,X_{i+1},...,X_n) = 0$.

⟶ **Notation.** $A[X_1,...,X_{i-1},X_{i+1},...,X_n] := A[X_1,...,X_{i-1},\hat{X}_i,X_{i+1},...,X_n]$.

$A[X_1,...,X_n]/(X_i) \simeq A[X_1,...,X_{i-1},\hat{X}_i,X_{i+1},...,X_n]$. De plus, X_i n'est pas un diviseur de 0 dans $A[X_1,...,X_n]$.

Conséquence. ***(Irréductibilité des indéterminées)***

Si A est intègre, X_i est premier.

▷ D'après ce qui précède, si A est intègre, (X_i) est premier, donc X_i est premier et même irréductible. ■

Conjecture ?

Si A est une $\mathbb{C}$-algèbre, supposons qu'il existe n tel que $A[X] \simeq \mathbb{C}[X_1,...,X_n]$. On se demande si $A \simeq \mathbb{C}[X_1,...,X_{n-1}]$. C'est un problème encore ouvert à ce jour.

5.2.2.2 Degré

Dans cette sous-section, on prend A un anneau et $n \in \mathbb{N}^*$ avec $X^{\underline{m}} = X_1^{m_1}...X_n^{m_n}$.

Définition. ***(Degré total d'un monôme)***

Le degré du monôme $X^{\underline{m}}$ est l'entier naturel $\sum_{i=1}^{n} m_i$.

Définition. ***(Degré total (général))***

Le degré d'un polynôme P non nul est le plus grand degré de ses monômes. S'il est nul, on pose $-\infty$.

Définition. ***(Degré partiel)***

Le degré partiel en la variable X_i d'un polynôme de $A[(X_i)_{i\in I}]$ est le degré de ce polynôme vu dans $A[(X_i)_{i\in I\setminus\{i\}}][X_i]$.

Ces considérations nous autorisent à parler de dimension si bien sûr $A = K$ est un corps, ce qui munit $K[(X_i)_{i\in I}]$ de la structure de K-espace vectoriel.

Propriété. ***(Dimension de $K[X_1,...,X_n]$)***

L'espace $K[X_1,...,X_n]$ est de dimension dénombrable, de base $\{X_1^{m_1}...X_n^{m_n}, m_1,...,m_n \in \mathbb{N}^n\}$.

Propriété. ***(Dimension de $K[(X_i)_{i\in I}]$ où I est infini)***

L'espace $K[(X_i)_{i\in I}]$ est de dimension I, de base $\{X_{i_1}^{m_1}...X_{i_n}^{m_n}, m_1,...,m_n \in \mathbb{N}^n, i_1,...,i_n \in I, n \in \mathbb{N}\}$.

▷ La famille donnée étant clairement une base, il suffit de calculer son cardinal. Elle est en bijection avec $\bigcup_{F\in\mathcal{P}_f(I)} \mathbb{N}^F$. Or $\mathcal{P}_f(I) \simeq I$, en effet, l'ensemble des parties finies de cardinal n de I s'injecte dans $I^n \simeq I$ dès que I est infini. Puisqu'il est clair qu'il est de cardinal au moins I, par théorème de Cantor-Bernstein, il est de cardinal exactement I. Or $\mathcal{P}_f(I) \simeq I$ est l'union dénombrable pour $n \in \mathbb{N}$ de ces ensembles, tous de cardinal I, donc $\mathcal{P}_f(I) \simeq I$. De plus, on sait que $\mathbb{N}^F\mathbb{N}$ dès F est fini. Or, une réunion disjointe indexée par I d'ensembles dénombrables est de cardinal I, ce qui termine la preuve. ■

Pour étudier la dimension des espaces de polynômes à degré total majoré, on aura intérêt à introduire la notion suivante :

5.2.2.3 Homogénéité

Définition. ***(Polynôme homogène)***

On dit qu'un polynôme P est homogène de degré d si tous ses monômes ont degré d.
On note $\text{Homog}_d[X_1,...,X_n]$ l'ensemble des polynômes à n variables de degré d.

Exemple

On se place dans le cas à $n = 2$ variables.

- Les polynômes homogènes de degré 0 sont les polynômes constants ;
- les polynômes homogènes de degré 1 sont les combinaisons linéaires de X et Y, avec éventuellement X ou Y n'apparaissant pas ;
- les polynômes homogènes de degré 2 sont les combinaisons linéaires de X, Y et XY ;
- les polynômes homogènes de degré 3 sont les combinaisons linéaire de X^3,X^2Y,XY^2,Y^3,
- etc.

⟶ **Convention.** Le polynôme nul est homogène de tout degré.

Remarque. Les polynômes homogènes de degré nul sont les constantes.

Proposition. ***(Stabilité des homogènes)***

Toute combinaison de polynômes homogènes de degré d est homogène de degré d.

Proposition. ***(Produit d'homogènes)***

Si A est intègre, si P est homogène de degré d, Q est homogène de degré d',alors PQ est homogène de degré $d + d'$.

On peut décomposer un polynôme en somme de polynômes homogènes de degrés distincts.

Proposition. ***(Décomposition homogène)***

Tout polynôme en n variables s'écrit de façon unique comme une somme de polynômes homogènes de degré d pour $d \in \mathbb{N}$. On appelle chaque terme de cette décomposition la *composante homogène* de degré d.

On retrouve les mêmes propriétés sur le degré que pour les anneaux normaux.

Proposition. ***(Scission homogène)***

Soit P un polynôme homogène non nul. Alors tout diviseur de P est homogène.

▷ Soit P un polynôme homogène non nul et $P = QR$. On considère le morphisme : $\begin{array}{ccc} A[X_1,...X_n] & \longrightarrow & A[X_1,...X_n,T] \\ X_i & \longmapsto & X_iT \\ P & \longmapsto & \tilde{P} \end{array}$. On note $\hat{P} = P(X_1T,...,X_nT \in A[X_1,...,X_n,T]$. Si $P = \sum_{d\in\mathbb{N}} P_d$, alors $\hat{P} = \sum_{d\in\mathbb{N}} P_dT^d$. Alors ψ est injective. De plus, P est homogène si et seulement si $\hat{P}$ est un monôme dans $A[X_1,...,X_n][T]$, *i.e.* $P = P'T^l$ avec P à n variables. Ainsi par hypothèses, $\hat{P} = \hat{Q}\hat{R}$ est un monôme dans $A[X_1,...,X_n][T]$ intègre donc $\hat{Q}$ et $\hat{R}$ aussi. Donc Q et R sont homogènes. ■

Maintenant, à la lumière de cette notion, on peut approfondir notre étude de la dimension des espaces de polynômes en plusieurs variables.

Propriété. ***(Dimension de*** $\mathrm{Homog}_d[X_1,...,X_n]$***)***

Le sous-espace de $K[X_1,...,X_n]$ des polynômes homogènes de degré d est de dimension finie qui est le nombre de d-combinaisons avec répétition d'un ensemble à n éléments $\Gamma_n^d = \binom{n+d-1}{d}$, de base $\{X_1^{\alpha_1}...X_n^{\alpha_n}, \alpha_1,...,\alpha_n \in \mathbb{N}^n \text{ avec } \alpha_1 + ... + \alpha_n = d\}$.

▷ Il est clair que la famille proposée est une base de $\mathrm{Homog}_d[X_1,...,X_n]$. Dénombrons-là. Il est clair que c'est le nombre de façons de ranger d chaussettes dans n tiroirs indiscernables, autrement dit, le nombre de partage d'un ensemble à d éléments en n sous-ensembles distincts. C'est par un argument combinatoire $\binom{n+d-1}{d}$. ■

Propriété. ***(Dimension de*** $K_d[X_1,...,X_n]$***)***

Le sous-espace $K_d[X_1,...,X_n]$ des polynômes de degré total inférieur ou égal à d est de dimension finie $\sum_{k=0}^{d} \binom{d+k-1}{k}$, de base $\{X_1^{\alpha_1}...X_n^{\alpha_n}, \alpha_1,...,\alpha_n \in \mathbb{N}^n \text{ avec } \alpha_1+...+\alpha_n \leqslant d\}$.

▷ On remarque que $\dim K_d[X_1,...,X_n] = \dim \mathrm{Homog}_d[X_1,...,X_n,X_{n+1}] = \binom{n+d}{d}$, car $K_d[X_1,...,X_n]$ et $\mathrm{Homog}_d[X_1,...,X_n,X_{n+1}]$ sont isomorphes par l'isomorphisme d'homogénéisation en degré d : pour un polynôme $P \in K[X_1,...,X_n]$, on pose $P \mapsto X_{n+1}^d P(\frac{X_1}{X_{n+1}},...,\frac{X_n}{X_{n+1}}$. ■

Corollaire. ***(Identité des chaussettes et des tiroirs)***

Pour tous entiers naturels n,d, le nombre de façons de ranger d chaussettes indistinguables dans $n+1$ tiroirs vaut $\binom{n+d}{d} = \sum_{k=1}^{d} \binom{n+k-1}{k}$.

Corollaire. ***(Identité des chaussettes et des tiroirs, deuxième version)***

Pour tous entiers naturels n,d, le nombre de façons de ranger d chaussettes indistinguables dans n tiroirs vaut $\binom{n+d-1}{d} = \sum_{k=1}^{d} \binom{n+k-2}{k}$.

Enfin :

Propriété. ***(Dimension de*** $\mathrm{Homog}_d[(X_i)_{i\in I}]$***)***

Le sous-espace de $\mathrm{Homog}_d[(X_i)_{i\in I}]$ de $A[(X_i)_{i\in I}]$ est de dimension I.

Propriété. ***(Dimension de*** $K_d[(X_i)_{i\in I}]$***)***

Le sous-espace de $K_d[(X_i)_{i\in I}]$ de $A[(X_i)_{i\in I}]$ est de dimension I.

Un petit fait pour l'étude des tangentes en géométrie projective :

Propriété. ***(Dérivée d'un polynôme homogène)***

La dérivée d'un polynôme homogène est homogène.

Propriété. ***(Facteur irréductible d'un polynôme homogène)***

Tout facteur irréductible d'un polynôme homogène est homogène.

5.2.3 Annulation

Bien sûr, un polynôme en plusieurs variables peut s'annuler sur autre chose qu'un ensemble fini, point, par exemple une droite. Prenons $P = X - Y$ et $Q = (X - Y)^2$, $A = \mathbb{R}$. Alors P s'annule si et seulement si l'on est sur la bissectrice. De même pour Q ! Ainsi P a une infinité de racines mais n'est pas nul, et P,Q coïncident sur une partie infinie mais ne sont pas égaux.

5.2.4 Polynômes symétriques

5.2.4.1 Définition

Soit $n \in \mathbb{N}$ et $\sigma \in \mathfrak{S}_n$. Alors clairement l'application :

$$\begin{array}{rccc} \rho_\sigma : & A[X_1,...,X_n] & \longrightarrow & A[X_1,...,X_n] \\ & X_i & \longmapsto & X_{\sigma(i)}. \end{array}$$

est un isomorphisme de A-algèbres.

⟶ **Notation.** On note $\rho_\sigma \longrightarrow P^\sigma$.

Formellement :

Lemme

Cette application définit une action à gauche fidèle de S_n sur $A[X_1,...,X_n]$.

▷ L'action du neutre est triviale. Pour la compatibilité, il suffit de voir que, permuter les indéterminées déjà permutées, c'est les permuter par la composée des deux permutations en jeu. ■

On peut maintenant définir :

Définition. ***(Polynôme symétrique)***

On dit que $P \in A[X_1,...,X_n]$ est symétrique si $P = P^\sigma$ pour toute $\sigma \in \mathfrak{S}_n$, c'est-à-dire s'il est invariant sous l'action de $\mathfrak{S}_n$.

⟶ **Notation.** On note $A[X_1,...,X_n]^{\mathfrak{S}_n}$ ou plutôt$A[X_1,...,X_n]^{\curvearrowleft \mathfrak{S}_n}$ l'ensemble des *polynômes symétriques* de degré n.

On a en particulier avec ce nouveau formalisme, pour $s \in \mathfrak{S}_n$, $\sigma \cdot P(X_1,...,X_n) = P(X_{\sigma(1)},...,X_{\sigma(n)}) = P^\sigma$.

Fait. ***(Polynômes symétriques à une variable)***

Un polynôme à une variable est toujours symétrique.

Propriété. ***(Structure de l'ensemble des polynômes symétriques)***

L'ensemble des polynômes symétriques à n indéterminées est une sous-A-algèbre de l'algèbre des polynômes à n indéterminées.

Si $n = 2$ par exemple, il n'y a que deux polynômes symétriques : $X + Y$ et XY. Quelques exemples généraux :

Exemples. ***(Polynômes symétriques de base)***

1. Soit $n \in \mathbb{N}$. $X_1 + ... + X_n$ est symétrique.
2. $X_1...X_n$ est symétrique.
3. On peut toujours élever à des puissances sans changer la symétrisation (c'est le produit externe et la somme qui coïncent, en fait). Ainsi $X_1^q + ... + X_n^q$, $(X_1...X_n)^q$ sont symétriques pour tout entier $q \geqslant 1$.
4. *(Exemple fondamental)* $e_k = \sum_{1 \leqslant i_1 < i_2 < ... < i_k \leqslant n} X_{i_1}...X_{i_k}$ est symétrique : c'est le k-ième *polynôme symétrique élémentaire*, pour $k \in [\![1,n]\!]$.
   Attention ! On se servira rapidement des polynômes symétriques dans le théorème de la partie suivante. Il ne faudra alors pas confondre le degré, ou la hauteur, du

polynômes à décomposer, et le nombre de variables. En effet, à n variables, il existe exactement n polynômes symétriques élémentaires, et $e_{n+1} = \sigma_{n+1} = \Sigma_{n+1}$ (selon les auteurs) n'a tout simplement aucune signification ! De plus, le degré total de e_k, qui est le degré total de n'importe lequel de ses monômes par symétrie, et k. Ils forment donc une famille échelonnée pour le degré total, donc libre.

5. Le polynôme $\prod_{i=1}^{n}(X + X_i) = \sum_{i=0}^{n} e_{n-i}X^i$ est clairement dans $A[X_1,...,X_n]^{\mathfrak{S}_n}[X]$. On fait naturellement apparaître les e dans l'expression précédente en remarquant que ce polynôme est invariant en changeant X pour l'un des X_j.

Principe. ***(Exhaustivité des variables d'un polynôme symétrique)***

Dans un polynôme symétrique, toutes les variables apparaissent (ou aucune).

▷ Si une variable i au moins apparaît dans le polynôme P, c'est-à-dire si le polynôme n'est pas nul, supposons qu'une variable $j \neq i$ n'apparaisse pas. Alors la transposition $(i,j) \in \mathfrak{S}_n$ ne laisse pas P invariant, donc il n'est pas symétrique. ■

On a la formule, utile dans la preuve de la section suivante :

Formule. ***(Récurrence entre les polynômes élémentaires selon*** n***)***

$$e_k^{(n)} = X_n e_{k-1}^{(n-1)} + e_k^{(n-1)}.$$

5.2.4.2 Théorème fondamental des polynômes symétriques

On se place dans l'anneau de polynômes en n variables : $A[S_1,...,S_n]$. **Il est important de comprendre que cet anneau est tout à fait isomorphe à l'anneau des polynômes à une indéterminées** (qui, par propriété universelle, est unique)**. Nous sommes amenés dans nos considérations à faire la distinction entre égalité et isomorphie.**

Définition. ***(Poids d'un monôme)***

Soit $P = \prod_{i=1}^{n} S_i^{m_1}$. On appelle *poids* de P l'entier $\sum_{i=1}^{n} im_i$.

Ainsi le poids dépend de l'*ordre* des variables, puisque toutes sont pondérées, en ordre croissant.

Définition. ***(Poids d'un polyôme)***

Soit $P \in A[S_1,...,S_n]$. On appelle *poids* de P, et l'on note $\omega(P)$, le plus grands des poids des monômes constituant P.

⟶ **Convention.** Si $P = 0$, on pose $\omega(P) = -\infty$

Définition. ***(Polynôme isobare)***

Soit $P \in A[S_1,...,S_n]$. On dit que P est *isobare* de poids d, s'il est constitué seulement de monômes de poids d.

Théorème. ***(Théorème fondamental des polynômes symétriques)***

$A[X_1,...,X_n]^{\mathfrak{S}_n} = A[e_1,...,e_n]$. Plus précisément, pour tout polynôme symétrique $P \in A[X_1,...,X_n]$, il existe un **unique** polynôme $Q \in A[X_1,...,X_n]$ tel que substitué $P = Q(e_1,...,e_n)$.

▷ On va montrer que l'application $\mathfrak{s}_n : \begin{array}{ccc} A[S_1,...,S_n] & \longrightarrow & A[X_1,...,X_n] \\ Q & \longmapsto & Q(e_1,e_2,...,e_n) \end{array}$, qui est clairement un morphisme de A-algèbres, est injective, d'image $A[X_1,...,X_n]^{\mathfrak{S}_n}$. Dans ce cas, on a un isomorphisme entre $A[S_1,...,S_n]$ et $A[X_1,...,X_n]^{\mathfrak{S}_n}$. De plus, si Q est de poids d, alors $\mathfrak{s}_n(Q)$ est de degré d ; si Q est isobare de poids d, alors $\mathfrak{s}_n(Q)$ est homogène de degré d.

Soit le monôme $Q = \prod_{i=1}^{n} S_i^{m_i}$ de poids $m_1 + 2m_2 + ... + nm_n$. Alors $\mathfrak{s}_n(Q) = \prod_{i=1}^{n} e_i^{m_i}$ où $\deg(e_i) = 1$. Ainsi, $\deg(\mathfrak{s}_n(Q)) = \sum_{i=1}^{n} (\deg e_i) m_i = \omega(Q)$. Il en résulte, par combinaison linéaire, que $\deg \mathfrak{s}_n(Q) \leqslant \omega(Q)$ pour tout $Q \in A[S_1,...,S_n]$. Remarquons dès maintenant que si $\mathfrak{s}_n$ est injective, alors $\deg \mathfrak{s}_n(Q) = \omega(Q)$ et si Q est isobare de degré d, alors $\mathfrak{s}_n(Q)$ est homogène de degré d.

Prouvons l'injectivité par récurrence sur n. On rappelle la notation $e_k^{(n)}$ pour $0 \leqslant k \leqslant n$. L'initialisation est immédiate, car en une variable, tout polynôme est symétrique, donc $\mathfrak{s}_0$ est injectif. Montrons maintenant l'hérédité. Soit $P \in A[X_1,...,X_n]$. On note toujours $\tilde{P}$ le polynôme $P(X_1,...,X_{n-1},0) \in A[X_1,...,X_{n-1}]$ essentiellement. On a $\deg \tilde{P} \leqslant \deg P$. De plus, si P est symétrique, alors $\tilde{P}$ est aussi symétrique. Enfin, $e_k\tilde{(n)} = e_k^{(n-1)}$ pour $0 \leqslant k \leqslant n-1$. On a aussi $e_n^{\tilde{(n)}} = 0$. Rappelons encore la formule $e_k^{(n)} = X_n e_{k-1}^{(n-1)} + e_k^{(n-1)}$. Supposons par l'absurde que $\mathfrak{s}_n$ n'est pas injective. Soit Q un élément du noyau de degré minimal et non nul. Par définition, $A[X_1,...,X_n] \ni Q(e_1^{(n)},...,e_n^{(n)}) = 0$. On annule X_n à 0 :

$$(Q(\tilde{e_1^{(n)}},...,e_n^{(n)})) = Q(e_1^{\tilde{(n)}},...,e_n^{\tilde{(n)}}) = Q(e_1^{(n-1)},...,e_{n_1}^{(n-1)},0) = \mathfrak{s}_{n-1}(Q(S_1,...,S_{n-2},0)) = 0$$

et $0 \in A[X_1,...,X_{n-1}]$ mais par hypothèse de récurrence $\mathfrak{s}_{n-1}$ est injective. Ainsi $Q(S_1,...,S_{n-1},0) = 0$. Ainsi, on sait qu'il existe $Q' \in A[S_1,...,S_n]$ tel que $Q = S_n Q'$. Ainsi $\deg(Q') + 1 = \deg(Q)$ et S_n n'est pas un diviseur de 0. On a :

$$0 = \mathfrak{s}_n(Q) = e_n \mathfrak{s}_n(Q') = \prod_{i=1}^{n} X_i \mathfrak{s}_n(Q').$$

Les X_i ne sont pas des diviseurs de 0 dans $A[X_1,...,X_n]$. Donc $\mathfrak{s}_n(Q') = 0$. Contradiction, car $\deg(Q') < \deg(Q)$ et $\mathfrak{s}_n(Q') = 0$.

On a que $\mathfrak{s}_n(A[S_1,...,S_n]) \subseteq A[X_1,...,X_n]^{\mathfrak{S}_n}$. On veut l'égalité. On démontre donc la surjectivité par récurrence sur n. L'initialisation est immédiate car on déjà un isomorphisme dans ce cas. On montre l'hérédité par l'absurde. Supposons $\mathrm{Im}(\mathfrak{s}_n) \subsetneq A[X_1,...,X_n]^{\mathfrak{S}_n}$. Soit P non nul dans $A[X_1,...,X_n]^{\mathfrak{S}_n} \setminus$

$im(\mathfrak{s}_n)$ de degré minimal, construction possible, par bon ordre sur $\mathbb{N}$. Le polynôme $\tilde{P}$ est symétrique d'où $\tilde{P} \in A[X_1,...,X_{n-1}]^{\mathfrak{S}_{n-1}}$ donc par hypothèse de récurrence, $\tilde{P} = \mathfrak{s}_{n-1}(Q)$ où $Q \in A[S_1,...,S_{n-1}] \subseteq A[S_1,...,S_n]$. On a $\omega(Q) = \deg(\tilde{P}) \leqslant \deg(P)$. Posons $P_0 = \mathfrak{s}_n(Q)$. On a $\deg(P_0) = \omega(Q) \leqslant \deg(P)$. Posons $P_1 = P - P_0 \in A[X_1,...,X_n]^{\mathfrak{S}_n}$. On a $\deg(P_1) \leqslant \deg(P)$. De plus $\tilde{P}_1 = \tilde{P} - \tilde{P}_0 = 0$. Sa spécialisation en la variable X_n en 0 est nulle, donc il est divisible par X_n : $P_1 \in (X_n)$. Tous les monômes de P_1 contiennent donc X_n, avec un degré au moins 1. Il en va de même pour toutes les variables, car P_1 est symétrique ! D'où $P_1 = \prod_{i1}^{n} X_i P_1'$. Les X_i n'étant pas diviseurs de 0, on en déduit que P_1' est symétrique et de plus $\deg(P_1') < \deg(P_1) \leqslant \deg(P)$. Par minimalité du degré de P, nécessairement $P_1' \in \mathrm{Im}(\mathfrak{s}_n)$, donc P_1 aussi. Or $P = P_1 + P_0 \in$
$im(\mathfrak{s}_n)$, contradiction, car $\mathfrak{s}_n$ est un morphisme et chacun de ces deux termes est dans son image. ■

Cette preuve constructive du théorème fondamental fournir un **algorithme de décomposition effectif** des polynômes symétriques, appelé *méthode de Waring*.

Méthode. ***(Décomposition des polynômes symétriques en polynômes symétriques élémentaires : méthode d'évaluation)***

Prenons $P = \sum_{1 \leqslant i \neq j \leqslant n} X_i^2 X_j = Q(e_1,...,e_n)$. **Si le polynôme n'est pas homogène, on le fait sur chaque polynôme de la décomposition homogène.** On a donc un polynôme de degré 3 et l'on cherche les possibilités pour $\deg(P) = 3 = \omega(Q)$. On peut écrire :

$$3 = 1 \times 3$$
$$3 = 1 \times 1 + 2 \times 1$$
$$3 = 3 \times 1.$$

Ainsi $Q = ae_1^3 + be_1e_2 + ce_3$. Il suffit ensuite d'évaluer en (1,0,...,0), puis en (1,1,0,...,0), etc.

Cette première méthode est à privilégier dans des cas très simples et lorsque l'expression du polynôme symétrique à réduire est en produit de facteurs. Autrement, on copie la preuve du théorème fondamental comme annoncé :

Méthode. ***(Décomposition des polynômes symétriques en polynômes symétriques élémentaires : méthode de Waring)***

On considère l'ordre lexicographique sur l'ensemble des monômes de P. Dans l'exemple précédent, le plus grand monôme est alors $X_1^2X_2$. Supposons en général que le monôme le plus grand pour l'ordre lexicographique dans l'ensemble des monômes de P homogène symétrique soit $a_{\underline{m}}X_1^{m_1}...X_n^{m_n}$, avec donc $m_1 \geqslant m_2 \geqslant ... \geqslant m_n$. On regarde $P - a_{\underline{m}}e_1^{m_1-m_2}e_2^{m_2-m_3}...e_{n-1}^{m_{n-1}-m_n}e_n^{m_n}$. Celui-ci est, selon l'ordre lexicographique, strictement plus petit. Voilà voilà. Sur l'exemple précédent, $P - e_1e_2 = \sum_{i\neq j} X_i^2X_j - \left(\sum_{i=1}^n X_i\right)\left(\sum_{i=1}^n X_j\right) = -3e_3$.

Heuristique

Il n'est pas du tout évident que l'anneau des polynômes symétriques soit isomorphe à un anneau de polynômes ! (Tous les anneaux n'ont pas la structure des anneaux de polynômes, bien sûr, ni tous les sous-anneaux d'un anneau de polynôme !).

Voilà un exemple édifiant pour ce fait. Si l'on fait agir $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ sur $\mathbb{C}[X,Y]$ avec $(1,0).X = -X$ et $(1,0).Y = Y$, et $(0,1).X = X$, $(0,1).Y = -Y$, ce qui suffit bien à définir l'action partout, dans ce cas on peut vérifier que les polynômes invariants sous cette action sont exactement les polynômes en X^2,Y^2 et la conclusion du théorème fondamental est vérifiée également.

Ce n'est pas général : maintenant, on fait agir $\mathbb{Z}/2\mathbb{Z}$ sur ce même ensemble avec $1.X = -X$ et $1Y = -Y$. Les polynômes $P = X^2, Q = Y^2, R = XY$ sont invariants sous cette action, et l'on peut montrer avec un peu de courage que les polynômes globalement invariants par cette action sont exactement les polynômes en P,Q,R. En particulier, $PQ = R^2$, donc l'ensemble des polynômes symétriques pour cette action n'est pas isomorphe à $\mathbb{C}[X,Y,Z]$ mais à son quotient par $PQ - R^2$, qui n'est pas un anneau de polynômes, car il ne satisfait pas la propriété universelle !

On se rend compte que le théorème fondamental est fondé sur la liberté de l'action considérée sur $A[X_1,...,X_n]$.

Exercice 106

Peut-on avoir $A_d[X_1,...,X_n]^{\mathfrak{S}_n} \simeq A_d[e_1,...,e_n]$ pour $d \in \mathbb{N}$?

▷ **Éléments de réponse.**

N'y aurait-il pas un problème de dimension ?

5.2.4.3 Identités de Newton

On se place dans l'algèbre $\mathbb{A} = K[X_1,...,X_n]$, $n \in \mathbb{N}$, K un corps. On va définir un nouveau type de polynômes symétriques remarquables et les lier au polynôme symétrique élémentaire. On note ces derniers $e_1 = X^1 + ...X^n,..,e_n = X_1...X_n$. On note encore $e_0 = 1$ par convention, ou définition, selon l'humeur.

Définition. ***(Somme de Newton)***

Soit $k \in \mathbb{N}$. La k-ième somme de Newton dans $\mathbb{A}$, est la quantité :

$$p_k = X_1^k + ...X_n^k.$$

Ainsi, une somme de Newton a toujours le même nombre de termes, ce sont seuls les degrés qui changent.

Théorème. ***(Formules de Newton)***

Soit $k \in \mathbb{N}$. On a les relations suivantes.

1. Si $k \geqslant n$, $p_k - e_1p_{k-1} + ... + (-1)^{n-1}e_{n-1}p_{k-n} + (-1)^n e_n p_{k-n} = 0$.
2. Si $1 \leqslant k \leqslant n$, $p_k - e_1p_{k-1} + ... + (-1)^{k-1}e_{k-1}p_1 + (-1)^k k e_k = 0$.

▷ Dans le premier cas, on note maintenant $x_1,...,x_n$ les indéterminées que l'on considère comme des réels quelconques et on note X une autre indéterminée. Cette façon de voir les choses est plus commode que de considérer l'anneau $\mathbb{A}[T]$, certes. On considère donc le polynôme $P = \prod_{i=1}^{n}(X - x_i) = X^n + \sum_{i=1}^{n}(-1)^i e_i X^{n-i}$. Puisque chaque x_i en est racine, on a pour tout $i \in [\![1,n]\!]$, $x_i^n - e_1 x_i^{n-1} + ... + (-1)^n e_n = 0$. En multipliant par x_i^{k-n}, puisque $k \geqslant n$, on a :

$$x_i^p - e_1 x_i^{k-1} + ... + (-1)^n e_n x_i^{k-n} = 0,$$

en additionnant pour tout i de 1 à n, on obtient la première identité.

Le second cas est nettement plus difficile, mais c'est celui qui nous intéresse le plus. Soit k un entier tel que $1 \leqslant k \leqslant n-1$. On compare p_k et $e_1 s_{k-1}$. On a $p_k = e_1 p_{k-1} - \sum_{1\leqslant i_1\neq i_2\leqslant n} x_{i_1}x_{i_2}^{k-1}$. On compare maintenant cette dernière somme et $e_2 p_{k-2}$. On a $e_2 p_{k-2} = \sum_{1\leqslant i_1\neq i_2\leqslant n} x_{i_1}x_{i_2}^{k-1} + \sum_{\substack{1\leqslant i_1<i_2\leqslant n \\ i_2\neq i_1,i_2}} x_{i_1}x_{i_2}x_{i_3}^{k-2}$. Plus généralement, on pose, pour $0 \leqslant j \leqslant j-1$, $A_j = \sum_{\substack{1\leqslant i_1<i_2<...<i_j\leqslant n \\ i_{j+1}\neq i_1,...,i_j}} x_{i_1}...x_{i_j}x_{i_{j+1}}^{k-j}$. En particulier, $A_0 = e_k$ et $A_{k-1} = k e_k$. On obtient alors, pour $1 \leqslant j \leqslant k-1$,

$$e_j p_{k-j} = A_{j-1} + A_j.$$

En multipliant cette première relation par -1, la seconde par 1, ..., la $(k-1)$-ième par $(-1)^{k-1}$, on

trouve $\sum_{j=1}^{k-1}(-1)^j e_k p_{k-j} = -p_k + (-1)^{k-1} k e_k$. En faisant tout passer à gauche, on obtient le résultat recherché. ■

On en déduit le résultat suivant, valable pour tout k.

Théorème. ***(Identités de Newton)***

Soit $k \in \mathbb{N}$. Alors $k e_k = \sum_{i=1}^{k}(-1)^{i-1} e_{k-i} p_i$.

Ces relations permettent, en connaissant les e_i (qui, on le rappelle, se lisent sur les coefficients du polynôme), d'en déduire de proche en proche les sommes p_k. En effet, d'après les formules précédentes :

$$\begin{aligned} e_1 &= p_1 \\ 2e_2 &= e_1 p_1 - p_2 \\ 3e_3 &= e_2 p_1 - e_1 p_2 + p_3 \\ 4e_4 &= e_3 p_1 - e_2 p_2 + e_1 p_3 - p_4, \end{aligned}$$

et ainsi de suite.

Ceci permet donc d'inverser les relations de Newton, selon le principe suivant :

Proposition. ***(Expression des sommes de Newton)***

On obtient :

$$\begin{aligned} p_1 &= e_1 \\ p_2 &= e_1 p_1 - 2e_2 \\ p_3 &= -e_2 p_1 + e_1 p_2 - 3e_3 \\ p_4 &= e_3 p_1 - e_2 p_2 + e_1 p_3 - 4e_4 \end{aligned}$$

etc.

On peut même essayer de les inverser complètement à l'aide d'une matrice.

Une preuve combinatoire de cette horreur

Antoine Chambert-Loir a récemment proposé une preuve combinatoire des identités de Newton.

Chapitre 6

Exercices

Difficulté des exercices :

- ● ○ ○ ○ ○ Question de cours, application directe, exercice purement calculatoire sans réelle difficulté technique
- ● ● ○ ○ ○ Exercice faisable, soit intuitivement, soit en employant des moyens rudimentaires ou des techniques déjà vues
- ● ● ● ○ ○ Exercice relativement difficile et dont la résolution appelle à une réflexion plus importante à cause d'obstacles techniques ou conceptuels, qui cependant devraient être à la portée de la plupart des étudiants bien entraînés
- ● ● ● ● ○ Exercice très exigeant, destiné aux élèves prétendant aux concours les plus difficiles, exercice « classique ».
- ● ● ● ● ● La résolution de l'exercice requiert un raisonnement et des connaissances extrêmement avancés, dépassant les attentes du prérequis. Il est presque impossible de le mener à terme sans indication. Bien qu'exigibles à très peu d'endroits, ces exercices sont très intéressants et présentent souvent des résultats forts.

Appendice

Table des matières

1 Structures algébriques **3**

1.1 Magmas . . . 3

1.2 Monoïdes . . . 5

1.3 Structures algébriques quotients élémentaires . . . 5

2 Théorie élémentaire des groupes **13**

2.1 Définition . . . 13

2.1.1 Inversion dans un groupe . . . 13

2.2 Groupes abéliens . . . 14

2.2.0.1 Théorème 5/8 . . . 14

2.3 Sous-groupe . . . 14

2.3.0.1 Sous-groupes triviaux . . . 14

2.4 Morphisme de groupes . . . 15

2.4.1 Noyau d'un morphisme . . . 15

2.4.2 Groupe des automorphismes . . . 15

2.5 Ordre d'un élément dans un groupe, génération . . . 15

2.5.1 Définition et caractérisation . . . 15

2.5.2 Notion de génération . . . 15

2.5.2.1 Système de générateurs . . . 15

2.5.2.2 Sous-groupe engendré . . . 16

2.5.3 Théorème de Lagrange et conséquences . . . 16

2.5.3.1 Groupes de cardinaux pairs, impairs . . . 16

2.5.4 Théorème de Cauchy . . . 17

2.5.5 Ordre dans un produit . . . 18

2.5.6 Propriétés opératoires de l'ordre . . . 18

2.5.6.1 IMPORTANT : ordre d'une puissance . . . 18

2.5.6.2 Ordre d'un produit . . . 18

2.5.6.3 Ordre d'une somme . . . 19

2.5.7 Exposant d'un groupe . . . 19

2.6 Groupes monogènes et groupes cycliques . . . 21

2.6.1 Définition . . . 21

2.6.2 Théorème de classification . . . 21
2.6.3 Groupes finis d'ordres premiers . . . 21
2.6.4 Structure des groupes cycliques . . . 22
2.6.4.1 Sous-groupes d'un groupe cyclique . . . 22
2.6.5 Élément primitif d'un groupe cyclique . . . 24
2.6.6 Morphismes entre groupes cycliques . . . 25
2.6.7 Automorphismes d'un groupe cyclique . . . 25
2.6.8 Classification des groupes d'ordre pq . . . 27
2.7 Groupes de symétrie . . . 28
2.7.1 Groupes symétriques . . . 28
2.7.1.1 Éléments remarquables du groupe symétrique . . . 28
2.7.1.2 Signature . . . 28
2.7.1.3 Présentations du groupe symétrique . . . 29
2.7.1.4 Sous-groupe alterné . . . 30
2.7.1.5 Propriétés calculatoires des cycles . . . 31
2.7.1.6 Propriétés combinatoires des cycles . . . 32
2.7.1.7 Propriétés matricielles des permutations . . . 32
2.7.1.8 Sous-groupes transitifs du groupe symétrique . . . 33
2.7.2 Groupes diédraux . . . 33
2.7.2.1 Définition . . . 34
2.7.3 Groupes de symétrie de l'espace . . . 38
2.8 Quotients de groupe . . . 38
2.8.1 Distinction de sous-groupes . . . 38
2.8.1.1 Notion de distinction ou normalité . . . 38
2.8.1.2 Sous-groupes distingués classiques et théorèmes opératoires . . . 43
2.8.1.3 Sous-groupe d'indice 2 . . . 50
2.8.2 Groupes quotients . . . 51
2.8.2.1 Application : le cas des anneaux modulaires . . . 62
2.8.2.2 Retour post-traumatique sur la distinction . . . 63
2.8.3 Exercices complémentaires à ce sujet . . . 65
2.9 Actions de groupes . . . 66
2.9.1 Opération d'un groupe sur un ensemble : définition . . . 67
2.9.2 Exemples fondamentaux d'actions de groupe . . . 68
2.9.3 Orbites, stabilisateurs, points fixes, etc. . . . 72
2.9.3.1 Orbites . . . 72
2.9.3.2 Stabilisateurs, centralisateurs, normalisateurs . . . 73
2.9.3.3 Stabilisateur d'une partie . . . 73
2.9.3.4 Fixateurs . . . 73
2.9.4 Équation aux classes, formule de Burnside . . . 74
2.9.5 Propriétés des actions de groupe . . . 76

2.9.6 Actions d'un groupe sur lui-même . . . 79
2.9.6.1 Actions par conjugaison et équation aux classes de conjugaison 79
2.9.6.2 Le théorème de Cayley . . . 82
2.10 Théorèmes de Sylow . . . 83
2.10.1 Notion de p-groupe . . . 83
2.10.2 Les trois théorèmes de Sylow . . . 86
2.11 Théorème de structure des groupes abéliens finis . . . 89
2.11.1 Exposé du théorème de classification . . . 89
2.11.2 Démonstration de l'existence du théorème de classification . . . 89
2.12 Groupes résolubles . . . 92
2.12.1 Un mot sur les groupes simples . . . 92
2.12.2 Commutateurs, groupe dérivée, abélianisé . . . 92
2.12.2.1 Propriétés opératoires de la dérivation de groupes . . . 93
2.12.2.2 Dérivation d'ordre supérieur . . . 93
2.12.2.3 Compléments . . . 93
2.12.3 Résolubilité . . . 94
2.12.4 Propriétés opératoires de la résolubilité . . . 96
2.12.5 Résolution des petits groupes . . . 98
2.12.6 Simplicité du groupe alterné . . . 99
2.12.6.1 Cas des plus petits ordres : $\mathfrak{S}_n$ pour $n = 1,2,3,4$ . . . 101
2.13 Groupes libres, présentation par générateurs et relations . . . 102
2.13.1 Groupe libre . . . 102
2.13.2 Présentation d'un groupe par générateurs et relations . . . 103

3 Généralités sur les anneaux 105
3.1 Notions générales sur les anneaux . . . 106
3.1.1 Définitions élémentaires . . . 106
3.1.2 Commutativité . . . 108
3.1.3 Sous-anneau . . . 108
3.1.4 Morphisme d'anneaux . . . 108
3.1.5 Inversibles d'un anneau . . . 108
3.1.5.1 Inverses latéraux dans un anneau . . . 109
3.1.6 Intégrité, division du zéro . . . 110
3.1.7 Corps . . . 111
3.1.8 Algèbre sur un corps . . . 111
3.1.9 Algèbre sur un anneau . . . 111
3.1.9.1 Définition ouverte de la notion d'algèbre (Lang, Bourbaki) . . . 112
3.1.9.2 Morphisme d'algèbres . . . 113
3.1.9.3 Génération d'une algèbre . . . 113
3.1.10 Produit d'anneaux . . . 113

3.1.11 Idéal d'un anneau . . . 115
3.1.11.1 Notion d'idéal . . . 115
3.1.11.2 Idéaux triviaux . . . 116
3.1.11.3 Opérations sur les idéaux . . . 116
3.1.11.3.1 Intersection d'idéaux . . . 116
3.1.11.3.2 Somme finie d'idéaux . . . 116
3.1.11.3.3 Produit d'idéaux . . . 117
3.1.11.3.4 Image et image réciproque d'idéaux . . . 117
3.1.11.3.5 Anneau produit et idéaux . . . 118
3.1.11.4 Notion de principalité . . . 118
3.1.11.5 Anneaux quotients ; quotient d'un anneau par un idéal . . . 121
3.1.11.6 Primalité, maximalité d'idéaux . . . 126
3.1.11.7 Anneau local . . . 132
3.1.11.8 Morphismes et idéaux premiers, maximaux . . . 133
3.1.12 Localisation, corps des fractions d'un anneau intègre . . . 134
3.1.12.1 Anneau des fractions d'un anneau commutatif ou localisé . . . 134
3.1.12.2 Corps des fractions proprement dit . . . 138
3.1.12.3 Localisation d'un anneau (par rapport à un idéal premier) . . . 139
3.1.13 Idempotence dans un anneau . . . 139
3.1.14 Nilpotence . . . 140
3.2 Compléments à l'étude élémentaire des anneaux . . . 141
3.2.1 Anneaux des entiers de Gauss . . . 141
3.2.2 Radical d'un idéal . . . 141
3.2.3 Radical de Jacobson d'un anneau . . . 143
3.2.4 Caractéristique d'un anneau, morphisme de Frobenius . . . 143
3.2.5 Hypothèses de l'algèbre commutative . . . 145
3.3 Arithmétique des anneaux . . . 146
3.3.1 Divisibilité dans un anneau : théorie générale de l'arithmétique . . . 147
3.3.1.1 Division et association . . . 147
3.3.1.2 Primalité relative et étrangeté . . . 149
3.3.1.3 Pgcd et ppcm . . . 150
3.3.1.4 Irréductibilité, primalité . . . 151
3.3.1.5 Factorisation dans un anneau . . . 154
3.3.2 Anneau euclidien . . . 157
3.3.3 Anneau principal . . . 157
3.3.3.1 Définition . . . 158
3.3.3.2 Arithmétique dans les anneaux principaux . . . 158
3.3.3.2.1 Conséquences sur la divisibilité . . . 158
3.3.3.2.2 Conséquences sur l'irréductibilité . . . 160
3.3.3.2.3 Conséquences sur la factorisation . . . 161

3.3.3.3 Principalité des anneaux euclidiens . . . 162
3.3.4 Anneau factoriel . . . 162
3.3.4.1 Valuations π-adique dans un anneau factoriel . . . 163
3.3.5 Anneau noethérien . . . 164
3.3.6 Résumé des notions arithmétiques sur les anneaux . . . 165
3.3.7 Utilisation de la factorialité de $\mathbb{Z}$ pour la résolution d'équations diophantiennes . . . 166

4 Théorie des corps 169
4.1 Théorie des corps . . . 169
4.1.1 Corps engendré par . . . 169
4.1.2 Sous-corps premier . . . 169
4.1.3 Construction des corps finis, corps de Galois . . . 169
4.1.3.1 Puissances dans un corps fini . . . 171
4.1.3.2 Automorphismes de corps finis . . . 172
4.1.4 Extensions de corps : généralités . . . 172
4.1.5 Construction d'extensions . . . 174
4.1.5.1 Compositum de deux sous-corps . . . 174
4.1.5.2 Homomorphismes entre corps, morphismes d'extension . . . 175
4.1.6 Corps de rupture . . . 177
4.1.7 Corps de décomposition, corps des racines . . . 179
4.1.8 Clôture algébrique . . . 180
4.1.9 Nombres algébriques, nombres transcendants . . . 182
4.1.9.1 Théorie élémentaire . . . 182
4.1.9.2 Extension algébrique . . . 183
4.1.9.3 Théorie géométrique . . . 185
4.1.9.4 Application du lemme d'Artin . . . 185
4.1.10 Extension séparable, extension normale . . . 187
4.1.10.1 Propriétés calculatoires . . . 191
4.1.10.2 Théorème de l'élément primitif . . . 193
4.1.11 Extension galoisienne . . . 195
4.2 Théorie de Galois . . . 196
4.2.1 Contexte historique : résolution d'équations par radicaux. Équations de petit degré . . . 196
4.2.1.1 Trinôme du second degré . . . 196
4.2.1.2 Équations de degré 3 . . . 196
4.2.1.3 Méthode de Descartes pour les équations du quatrième degré . . . 197
4.2.1.4 Et après ? . . . 197
4.2.2 Prérequis . . . 198
4.2.3 Corps de Galois . . . 199

4.2.4 Correspondance de Galois . . . 199
4.2.5 Illustration de la correspondance galoisienne . . . 203
4.2.5.1 Groupe de Galois d'un polynôme . . . 203
4.2.6 Extension abélienne . . . 208
4.2.6.1 Extension cyclotomique . . . 209
4.2.7 Application à la résolution par radicaux des équations . . . 211
4.2.8 Calcul pratique du groupe de Galois en caractéristique nulle . . . 212
4.2.9 Extension de la théorie de Galois aux extensions algébriques infinies . . . 214

5 Polynômes **217**
5.1 Étude de l'anneau des polynômes sur un anneau . . . 217
5.1.1 Généralités . . . 217
5.1.1.1 Construction . . . 217
5.1.1.2 Notion de degré . . . 219
5.1.1.3 Hérédité d'une propriété sur la catégorie des anneaux . . . 219
5.1.2 Arithmétique élémentaire de $A[X]$ . . . 219
5.1.3 Irréductibles de $A[X]$ . . . 220
5.1.3.1 Généralités . . . 220
5.1.3.2 Passage de l'anneau au corps des fractions, contenu, théorème de Gauss, critères d'irréductibilité . . . 223
5.1.4 Fonctions polynomiales . . . 230
5.1.4.1 Définition . . . 230
5.1.4.2 Fonctions polynomiales sur un corps fini . . . 230
5.1.5 Dérivation en une variable . . . 231
5.1.5.1 Dérivées partielles . . . 233
5.2 Polynômes en plusieurs variables . . . 234
5.2.1 Construction de l'anneau des polynômes en plusieurs variables . . . 234
5.2.1.1 Construction directe abstraite . . . 234
5.2.2 Cas particulier des polynômes en un nombre fini de variables . . . 235
5.2.2.1 Fonctions polynomiales et morphisme d'évaluation . . . 237
5.2.2.2 Degré . . . 239
5.2.2.3 Homogénéité . . . 241
5.2.3 Annulation . . . 243
5.2.4 Polynômes symétriques . . . 243
5.2.4.1 Définition . . . 243
5.2.4.2 Théorème fondamental des polynômes symétriques . . . 245
5.2.4.3 Identités de Newton . . . 249

6 Exercices **251**

Bibliographie

[1] *Titre du livre*, Auteur du livre, date, maison d'édition

Table des figures

2.7.1 *Les premiers ensembles sur lesquels les groupes diédraux agissent de façon stabilisatrice* — 36
2.9.1 *Quelques caractéristiques sur les actions d'un groupe sur lui-même* — 80

3.1.1 *Comparaison des différentes structures relatives à la notion d'anneau.* — 112
3.2.1 *Lien entre le cardinal des anneaux et leur caractéristique finie ou finie. Par théorème de Lagrange, un anneau fini est forcément de caractéristique finie.* — . 144
3.3.1 *Structures particulières d'anneaux.* — 166

4.2.1 Situation précédente 205
4.2.2 *Treillis des sous-groupes de* $\mathfrak{A}_4$*.* — 206
4.2.3 *Treillis des sous-extensions de* L/K*.* — 207
4.2.4 *Treillis des sous-groupes de* G*.* — 207
4.2.5 *Treillis des sous-extensions de* L/K*.* — 208

Liste des tableaux