Structures algébriques

PTSI B Lycée Eiffel

30 janvier 2013

Qu'est-ce qu'un Kinder surprise sans son jouet ?
Un Kinder injectif, son noyau est réduit à zéro !

Un groupe de loups, c'est une horde.
Un groupe de vaches, c'est un troupeau.
Un groupe d'hommes, c'est souvent une bande de cons.

Philippe Gelück (auteur du Chat).

Introduction

Ce premier chapître d'algèbre pur de l'année est absolument fondamental pour la compréhension de tout ce qu'on fera ensuite sur les espaces vectoriels. Ce cha)tre vous semblera certainement ardu au premier abord car les structures étudiées sont très générales, et le formalisme rebutant. Mais vous faites ici vos premiers pas vers une nouvelle façon de considérer les mathématiques, non plus comme un simple alignement de calcul utilisant de temps à autre, par commodité, des notations ou des théorèmes dont on ne saisit pas toujours la portée, mais bien comme une science visant à dégager à partir des objets mathématiques usuels des structures très générales, qu'on étudie ensuite de façon abstraite pour énoncer des théorèmes très généraux qui s'appliqueront ensuite de façon identique quelle que soit l'ensemble étudié en pratique. Ainsi, un résultat théorique sur les groupes pourra aussi bien s'appliquer sur les nombres entiers, que sur des suites ou plus tard des matrices.

Objectifs du chapitre :

- comprendre l'intérêt de dégager des structures algébriques très générales, qui s'adapteront à des ensembles et des opérations variés.
- maîtriser le formalisme des groupes et des anneaux, et être capable de faire des calculs abstraits dans ces structures.
- savoir factoriser ou effectuer une division euclidienne sur des polynômes à coefficients réels ou complexes.

1 Groupes

1.1 Lois de composition interne

Définition 1. Soit E un ensemble, une **loi de composition interne** (ou plus simplement lci) sur E est une application $\star : E \times E \to E$. On note en général l'image du couple (x, y) par cette application $x \star y$ plutôt que $\star(x, y)$.

Remarque 1. Une loi de composition est tout simplement une opération sur l'ensemble E, d'où la notation utilisée pour les images. Ainsi, la somme ou le produit sont des lci sur les ensembles $\mathbb{R}$, $\mathbb{Z}$ ou encore sur l'ensemble de toutes les suites réelles. Par contre, la soustraction est une lci sur $\mathbb{R}$ mais pas sur $\mathbb{N}$ où elle n'est plus interne (la différence de deux entiers naturels peut ne plus être un entier naturel). La division est une lci sur $\mathbb{R}^*$ (on ne peutpas diviser par 0). Le produit vectoriel est une lci sur l'ensemble des vecteurs de l'espace, mais pas le produit scalaire (le résultat n'étant plus un vecteur mais un réel). On peut évidemment multiplier les exemples puisqu'aucune condition n'est imposée pour l'instant sur notre lci.

Définition 2. Un ensemble E muni d'une lci $\star$ est appelé un **magma**. On le note $(E, \star)$.

Définition 3. Soit $(E, \star)$ un magma. La lci $\star$ est **associative** si $\forall (x, y, z) \in E^3$, $x \star (y \star z) = (x \star y) \star z$. La loi est **commutative** si $\forall (x, y) \in E^2$, $x \star y = y \star x$.

Exemples : La opération de somme ou de produit sont associatives et commutatives sur tous les ensembles sur lesquels on a pu les étudier jusqu'à présent (mais ce ne sera pas le cas du produit matriciel, par exemple). Par contre, une opération aussi élémentaire que la soustraction sur $\mathbb{R}$ n'est ni associative ni commutative. La composition de fonction est un bon exemple de lci associative mais pas commutative.

Définition 4. Soit $(E, \star)$ un magma. Un **élément neutre** pour la loi $\star$ dans E est un élément $e \in E$ tel que $\forall x \in E$, $x \star e = e \star x = x$.

Proposition 1. S'il existe un élément neutre pour une lci, alors il est unique.

Démonstration. Supposons donc qu'il y ait deux éléments neutres dans un même magma, que nous noterons e et e'. Alors, par neutralité de e, $e \star e' = e'$. Mais par neutralité de e', ce même $e \star e'$ doit être égal à e. Cela impose $e = e'$ et l'unicité du neutre. □

Exemples : L'addition sur $\mathbb{R}$ ou $\mathbb{Z}$ admet 0 pour élément neutre. L'addition sur l'ensemble des fonctions réelles admet pour élément neutre la fonction constante égale à 0, qu'on se permettra de noter 0 par abus de notation. La multiplication admet pour élément neutre 1 (ou la fonction constante égale à 1). La composition sur l'ensemble des fonctions réelles admet pour élément neutre l'application identité. La multiplication définie sur $\{n \in \mathbb{N} \mid n \geqslant 6\}$ est une lci mais n'admet pas d'élément neutre. Le produit vectoriel sur l'ensemble des vecteurs de l'espace n'admet pas d'élément neutre.

Définition 5. Soit $(E, \star)$ un magma dans lequel $\star$ admet un élément neutre e. Un élément $x \in E$ est **symétrisable** s'il existe $y \in E$ tel que $x \star y = y \star x = e$. L'élément y est appelé **symétrique** de x et noté x^{-1}

Remarque 2. On parlera plutôt d'inverse dans le cas où l'opération $\star$ est une multiplication. On parlera d'opposé lorsque l'opération est une addition, et on notera dans ce cas le symétrique $-x$ plutôt que x^{-1}.

Proposition 2. Si x est un élément symétrisable, alors x^{-1} aussi, et $(x^{-1})^{-1} = x$. Dans le cas où la lci $\star$ est associative, le symétrique d'un élément x, s'il existe, est unique. Si x et y sont deux éléments symétrisables, alors $x \star y$ l'est aussi, et $(x \star y)^{-1} = y^{-1} \star x^{-1}$.

Démonstration. La première propriété est évidente au vu de la définition de la symétrisabilité. Pour la deuxième, supposons qu'il y ait deux symétriques y et z à un même élément x, alors d'une part $y \star (x \star z) = y \star e = y$, et d'autre part $(y \star x) \star z = e \star z = z$, ce qui prouve que $y = z$. Enfin, la dernière propriété se prouve en constatant que $(y^{-1} \star x^{-1}) \star (x \star y) = y^{-1} \star (x^{-1} \star x) \star y = y^{-1} \star e \star y = y^{-1} \star y = e$, et de même pour l'opération en sens inverse. □

Remarque 3. L'élément neutre est toujours symétrisable, il est son propre symétrique. Lorsqu'un élément est symétrisable, on peut simplifier sans problème par cet élément. Par exemple $x \star y = x \star z$ implique $y = z$ si x est symétrisable. En effet, dans ce cas, on peut multiplier les deux membre de l'égalité à gauche par x^{-1}.

Exemples :

- Dans $\mathbb{R}$, tout élément est symétrisable pour l'addition, mais il faut se placer dans $\mathbb{R}^*$ pour que ce soit le cas du produit.
- Si on considère l'addition dans $\mathbb{N}$, seul l'élément neutre 0 est symétrisable.
- Dans $\mathbb{Z}$ muni de la multiplication, les seuls éléments symétrisables sont -1 et 1.
- Dans l'ensemble des fonctions muni de la composition, les éléments symétrisables sont les fonctions bijectives (et l'inverse est alors la réciproque, ce qui justifie la notation usuelle de la réciproque).
- Si on considère l'ensemble $\mathcal{P}(E)$ des sous-ensembles d'un ensemble E, l'opération d'union est une lci sur E. Elle admet pour élément neutre l'ensemble vide, mais seul le neutre est symétrisable.

1.2 Groupes et sous-groupes

Définition 6. Un ensemble G muni d'une loi de composition interne $\star$ est un **groupe** si :

- la loi $\star$ est associative.
- elle admet un élément neutre.
- tout élément de G est symétrisable.

On note alors le groupe $(G, \star)$ (comme un magma, même si les conditions sont nettement plus strictes). Dans le cas où la lci est de plus commutative (ce qui n'est pas imposé), le groupe est dit **commutatif** ou **abélien**.

Exemples :

- $(\mathbb{R}, +)$ ou $(\mathbb{Z}, +)$ sont des groupes mais pas $(\mathbb{N}, +)$.
- $(\mathbb{R}^*, \times)$ ou $(\mathbb{C}^*, \times)$ sont des groupes.
- L'ensemble des applications bijectives de $\mathbb{R}$ dans $\mathbb{R}$ muni de la composition est un groupe non commutatif.
- Si E est un ensemble quelconque, $(\mathcal{P}(E), \Delta)$ est un groupe (où Δ désigne la différence symétrique vue en exercice dans un chapitre précédent).

Définition 7. Soit $(G, \star)$ un groupe, et H un sous-ensemble de G, H est un **sous-groupe** de G si $(H, \star_{|H})$ est un groupe.

Proposition 3. Si $H \subset G$, où $(G, \star)$ est un groupe, alors est un sous-groupe de G si et seulement si $e \in H$ et $\forall (x, y) \in H^2$, $x \star y^{-1} \in H$.

Démonstration. Si H est un sous-groupe de G, il vérifie certainement les deux propriétés citées. En effet, il doit contenir un élément neutre pour la lci $\star$, qui ne peut être autre que l'élément neutre e du groupe G. De plus, si $y \in H$, y doit admettre un symétrique dans H, donc $y^{-1} \in H$, et $\star$ étant une lci dans H, $x \star y^{-1}$ appartient également à H. La réciproque est un peu plus intéressante. La lci $\star$ étant associative sur G, elle le sera nécessairement sur H. De plus, il s'agit vraiment d'une lci sur H, car en prenant $x = e$ dans la deuxième condition, on aura, pour tout élément y de H, $y^{-1} \in H$, et on peut alors remplacer y^{-1} par $(y^{-1})^{-1}$ dans cette même condition pour obtenir $x \star y \in H$. On a montré en passant que tous les éléments de H étaient symétrisables dans H, toutes les conditions sont réunies pour que H soit un groupe. □

Remarque 4. La deuxième condition est en fait un condensé de deux conditions naturelles : le sous-ensemble H doit être **stable** par la loi $\star$ (le produit de deux éléments de H reste dans H) et par passage à l'inverse. Il est nettement plus facile en pratique de prouver qu'un ensemble est un sous-groupe d'un groupe que de montrer qu'il s'agit d'un groupe, car on évite la partie habituellement la plus technique de la preuve : la démonstration de l'associativité de la loi.

Exemples : $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{R}, +)$. Plus intéressant, $(\mathbb{U}, \times)$ est un sous-groupe de $(\mathbb{C}^*, \times)$.

Proposition 4. Soient H_1 et H_2 deux sous-groupes d'un même groupe $(G, \star)$, alors $H_1 \cap H_2$ est également un sous-groupe de G.

Démonstration. C'est quasiment immédiat : si l'élément neutre appartient à H_1 et à H_2, il appartient âussi à $H_1 \cap H_2$, et de même pour $x \star y^{-1}$ si on suppose que x et y appartiennent tous les deux aux deux sous-groupes. □

Remarque 5. Attention, l'union de deux sous-groupes n'a en général aucune raison d'être un sous-groupe, la deuxième condition n'étant pas nécessairement vérifiée. Si on prend x dans H_1 et y dans H_2, $x \star y^{-1}$ ne sera en général ni dans H_1 ni dans H_2. Ainsi, $(\mathbb{R}, +)$ et $(i\mathbb{R}, +)$ sont deux sous-groupes de $(\mathbb{C}, +)$, mais leu union n'est pas du tout un sous-groupe car elle n'est pas stable par somme.

Définition 8. Le **sous-groupe engendré** par un sous-ensemble de G est le plus petit sous-groupe de G contenant ce sous-ensemble.

Remarque 6. On considère souvent le sous-groupe engendré par un nombre fini x_1, x_2, …, x_n d'éléments de G.

Théorème 1. Sous-groupes de $\mathbb{Z}$.
Tous les sous-groupes de $(\mathbb{Z}, +)$ sont de la forme $a\mathbb{Z} = \{k \in \mathbb{Z} \mid \exists b \in \mathbb{Z}, k = a \times b$, avec $a \in \mathbb{Z}$.

Démonstration. Soit G un sous-groupe de $\mathbb{Z}$, G contient nécessairement l'élément neutre 0. S'il ne contient aucun autre élément, il est donc égal à $0\mathbb{Z}$, ce n'est pas le cas le plus intéressant. Supposons donc qu'il y ait un élément non nul dans G. Comme G est stable par passage à l'opposé, on peut toujours supposer cet élément strictement positif. L'ensemble de tous les éléments strictement positifs de G étant non vide, il admet un plus petit élément que nous noterons a. On prouve facilement par récurrence que $\forall n \in \mathbb{N}$, $na \in G$: $0 \in G$ et si $na \in G$, $na + a \in G$ car G est stable par somme. L'ensemble G contient aussi les multiples négatifs de a puisqu'il est stable par passage à l'opposé. On en conclut que $a\mathbb{Z} \subset G$. Prouvons la réciproque par l'absurde, ce qui utilisera un peu d'arithmétique que nous reverrons un peu plus loin dans ce cours. Supposons donc que G contienne un élément x qui ne soit pas un multiple de a. Par division euclidienne de x par a, on peut écrire $x = aq + r$, avec $0 < r < a$ (r ne peut pas être nul car x n'est pas multiple de a). Or, $x \in G$ et $aq \in G$, donc $r = x - aq \in G$, ce qui contredit la minimalité de a comme élément strictement positif de G. C'est absurde, on a donc $G = a\mathbb{Z}$. □

Remarque 7. On peut facilement déterminer l'intersection de deux tels sous-groupes, quitte à anticiper un peu sur l'arithmétique. En effet, on constate que $a\mathbb{Z} \cap b\mathbb{Z} = c\mathbb{Z}$, où c est le pgcd des entiers a et b.

1.3 Morphismes de groupes

Définition 9. Soit $(G, \star)$ et $(H, *)$ deux groupes. Une application $f : G \to H$ est un **morphisme de groupes** si $\forall (x, y) \in G^2$, $f(x \star y) = f(x) * f(y)$. On parle d'**isomorphisme de groupes** si f est de plus bijective. Un morphisme de $(G, \star)$ vers lui-même est appelé **endomoprhisme de groupes**, et on parlera d'**automorphisme** pour un endomorphisme bijectif.

Exemples : La multiplication par 3 dans $(\mathbb{Z}, +)$ ($f : n \mapsto 3n$) est un morphisme de groupes, mais pas un aotomorphisme. Vous connaissez déjà des morphismes de groupes nettement moins évidents : le logarithme népérien est un isomorphisme de groupes de $(\mathbb{R}^{+*}, \times)$ vers $(\mathbb{R}, +)$ (et l'exponentielle en est un dans l'autre sens).

Proposition 5. Soit f un morphisme de groupes de $(G, \star)$ vers $(H, *)$, alors $f(e) = e'$, où on a noté e et e' les éléments neutres respectifs de G et H ; et $\forall x \in G$, $f(x^{-1}) = (f(x))^{-1}$.

Démonstration. En utilisant la définition d'un morphisme de groupes, on a $f(e\star e) = f(e)*f(e)$. Mais comme $e\star e = e$, on trouve $f(e) = f(e)*f(e)$, ce qui en simplifiant par $f(e)$ dans H donne $e' = f(e)$. On peut ensuite appliquer la définition d'un morphisme à x et x^{-1} : $f(x\star x^{-1}) = f(x)*f(x^{-1})$, soit $f(e) = e' = f(x)*f(x^{-1})$ (et de même $f(x^{-1})*f(x) = e'$), ce qui prouve que $f(x^{-1}) = (f(x))^{-1}$. □

Remarque 8. On retrouve ici les propriétés classique de l'exponentielle et du logarithme : $e^{-x} = \dfrac{1}{e^x}$ et $\ln\left(\dfrac{1}{x}\right) = -\ln(x)$.

Proposition 6. La composition de deux morphismes de groupes est un morphismes de groupes. Si on note $Aut(G)$ l'ensemble des automorphismes d'un groupe G, $(Aut(G), \circ)$ est lui-même un groupe.

Démonstration. La première partie de la proposition est évidente, il suffit de l'écrire. L'ensemble $Aut(G)$ est alors stable par composition (puisqu'on sait qu'une composée de deux bijections est une bijection). Il admet certainement un élément neutre : l'application identité de G dans lui-même est un automorphisme. On sait que l'opération de composition est associative. Reste à prouver l'existence d'un inverse pour tout automorphisme, à savoir ici d'une réciproque. La réciproque d'une application bijective est certainement bien définie et bijective, reste à prouver que c'est un morphisme de groupe. En effet, si f est un automorphisme de $(G, \star)$ dans lui-même, on aura $f(x\star y) = f(x)\star f(y)$ pour tout couple d'éléments (x, y) de G. Appliquons cette formule à $f^{-1}(x)$ et $f^{-1}(y)$, on trouve alors $f(f^{-1}(x)\star f^{-1}(y)) = f(f^{-1}(x))\star f(f^{-1}(y))$, soit $f(f^{-1}(x)\star f^{-1}(y)) = x\star y$. L'application f étant bijective, on peut écrire $f^{-1}(x)\star f^{-1}(y) = f^{-1}(x\star y)$, ce qui prouve que f^{-1} est bien un morphisme de groupes. □

Définition 10. Avec les notations précédentes, si f est un morphisme de groupes, on appelle **noyau de** f l'ensemble noté $\ker(f) = \{x \in G \mid f(x) = e'\}$. On appelle **image de** f, et on note $\mathrm{Im}\,(f)$, l'image de G par le morphisme f, soit $\mathrm{Im}\,(f) = \{y \in H \mid \exists x \in G, f(x) = y\}$.

Proposition 7. Si f est un morphisme de groupes de $(G, \star)$ vers $(H, *)$, son noyau est un sous-groupe de G, et son image un sous-groupe de H.

Démonstration. Le noyau contient toujours e comme on l'a vu plus haut. De plus, si x et y appartiennent au noyau, alors $f(x\star y^{-1}) = f(x)*f(y)^{-1} = e'*(e')^{-1} = e'$, donc $x\star y^{-1} \in \ker(f)$. Le noyau est bien un sous-groupe de G. Pour l'image, c'est également élémentaire : e' appartient à $\mathrm{Im}\,(f)$ puisqu'il est l'image de e, et si z et w sont les images respectives de x et de y, alors $z*w^{-1} = f(x\star y^{-1})$ d'après les propriétés des morphismes de groupes. L'image est donc également un sous-groupe (mais de H cette fois-ci). □

Proposition 8. Un morphisme de groupes f est injectif si et seulement si $\ker(f) = \{e\}$. Un morphisme de groupes est surjectif si et seulement si $\mathrm{Im}\,(f) = H$.

Démonstration. La deuxième propriété est évidente, c'est même la définition de la surjectivité. La première est plus intéressante. On sait déjà que le noyau de f contient toujours e puisque $f(e) = e'$ pour un morphisme. Si on suppose de plus f injectif, e' ne peut avoir plus d'un antécédent par f. Puisqu'il en a déjà un, il est unique et $\ker(f) = \{e\}$. Supposons désormais le contraire, à savoir que $\ker(f) = \{e\}$, et montrons que f est injectif. Pour cela, considérons deux éléments x et y tels que $f(x) = f(y)$. On a donc, en utilisant les notations habituelles, $f(x)*f(y)^{-1} = e'$, soit, puisque f est un morphisme $f(x\star y^{-1}) = e'$. Autrement dit, $x\star y^{-1} \in \ker(f)$, ce qui induit $x\star y^{-1} = e$. Mais cela ne peut se produire que si $y^{-1} = x^{-1}$, soit $x = y$. On a bien prouvé l'injectivité du morphisme f. □

Exemples : La multiplication par 3, définie de $(\mathbb{Z}, +)$ dans lui-même, est un morphisme injectif (seul 0 a une image nulle), mais pas surjectif. Plus précisément, son image est le sous-groupe $3\mathbb{Z}$. Le module est un morphisme de groupes de $(\mathbb{C}^*, \times)$ vers $(\mathbb{R}^{+*}, \times)$, dont le noyau est l'ensemble $\mathbb{U}$ des nombres complexes de module 1. Il est par ailleurs surjectif.

2 Anneaux et arithmétique dans $\mathbb{Z}$

2.1 Anneaux et corps

Définition 11. Soit E un ensemble muni de deux lois de composition internes $\star$ et $*$. La loi $\star$ est **distributive** par rapport à la loi $*$ si $\forall (x,y,z) \in E^3$, $x \star (y * z) = (x \star y) * (x \star z)$, et $(y * z) \star x = (y \star x) * (z \star x)$.

Définition 12. Un ensemble A muni de deux lci $+$ et $\times$ est un **anneau** si :
- $(A, +)$ est un groupe commutatif.
- il existe un élément neutre pour la loi $\times$.
- la loi $\times$ est associative et distributive par rapport à la loi $+$.

Un anneau est noté $(A, +, \times)$, et ses éléments neutres sont notés 0 (pour la loi $+$) et 1 (pour la loi $\times$). Si la loi $\times$ est commutative, on dit que A est un **anneau commutatif**.

Exemples : L'exemple le plus classique d'anneau est $(\mathbb{Z}, +, \times)$ (on n'impose aucune condition d'inversibilité pour la loi multiplicative), mais les ensembles de suites ou de fonctions sont aussi des anneaux pour la somme et le produit usuels. Nous verrons plus tard dans l'année un exemple d'anneau non commutatif avec les matrices.

Proposition 9. Dans un anneau $(A, +, \times)$, 0 est un élément **absorbant** : $\forall x \in A$, $0 \times x = x \times 0 = 0$.

Démonstration. En effet, $(0+0) \times x = 0 \times x + 0 \times x$ par distributivité, ce qui implique $0 \times x = 0 \times x + 0 \times x$, soit $0 \times x = 0$. L'autre sens est identique. □

Définition 13. Un anneau $(A, +, \times)$ est **intègre** si $\forall (x,y) \in A^2$, $x \times y = 0 \Rightarrow x = 0$ ou $y = 0$. Dans un anneau non intègre, les éléments x pour lesquels il existe un y non nul tel que $x \times y = 0$ sont appelés **diviseurs de zéro**.

Remarque 9. Les diviseurs de 0 sont nécessairement des éléments non inversibles de l'anneau. Difficile de donner un exemple simple d'anneau non intègre pour l'instant, encore une fois les matrices fourniront un sujet d'étude intéressant de ce point de vue.

Définition 14. Dans un anneau A, on notera nx l'élément $\underbrace{x + \cdots + x}_{n \text{ fois}}$. On utilisera également la notation Σ pour les sommes dans les anneaux. De même, si l'anneau est commutatif, on se servira des notations x^n et Π. Les puissances entières vérifient alors toutes les propriétés usuelles des puissances.

Proposition 10. Soit x un élément différent de 1 dans un anneau commutatif A, alors $\forall n \in \mathbb{N}$, $\displaystyle\sum_{k=0}^{k=n} x^k = \frac{1 - x^{n+1}}{1 - x}$.

Démonstration. La démonstration est rigoureusement la même que celle de la somme géométrique de réels. □

Théorème 2. Formule du binôme de Newton dans un anneau.
Soit $(A, +, \times)$ un anneau et $(x,y) \in A^2$ vérifiant $xy = yx$ (on dit que x et y **commutent**), alors $\forall n \in \mathbb{N}$, $(x+y)^n = \displaystyle\sum_{k=0}^{k=n} \binom{n}{k} x^k y^{n-k}$. Sous la même hypothèse de commutation, on a également
$\forall n \in \mathbb{N}$, $x^n - y^n = (x-y) \displaystyle\sum_{k=0}^{n-1} x^k y^{n-1-k} = (x-y)(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1})$.

Démonstration. Nous n'allons sûrement pas redémontrer la formule du binôme de Newton, une fois suffit. La deuxième formule ne nécessite absolument pas de récurrence, simplement la constatation du fait que $(x-y)\displaystyle\sum_{k=0}^{n-1} x^k y^{n-1-k} = \sum_{k=0}^{n-1} x^{k+1} y^{n-1-k} - \sum_{k=0}^{n-1} x^k y^{n-k} = \sum_{k=1}^{n} x^k y^{n-k} - \sum_{k=0}^{n-1} x^k y^{n-k} = x^n - y^n$ avec un petit décalage d'indice en cours de calcul, et un superbe télescopage pour finir. □

Définition 15. Si $(A, +, \times)$ est un anneau, un sous-ensemble $B \subset A$ est un **sous-anneau** de A si $(B, +_{|A}, \times_{|A})$ est un anneau.

Proposition 11. B est un sous-anneau de A si et seulement si $(B, +)$ est un sous-groupe de $(A, +)$, B est stable par la loi $\times$, et B contient l'élément 1.

Démonstration. Comme dans le cas des groupes, le sens direct est essentiellement évident. La réciproque est ici très facile également puisque B vérifiera effectivement tous les axiomes nécessaires pour être un anneau si c'est un sous-groupe, qu'il contient un neutre pour le produit et qu'il est stable par multiplication. □

Exemples : L'anneau $(\mathbb{Z}, +, \times)$ n'a aucun autre sous-anneau que $\mathbb{Z}$ lui-même. En effet, le seul sous-groupe de $(\mathbb{Z}, +)$ contenant 1 est $\mathbb{Z}$. Par contre, $\mathbb{Z}$ est un sous-anneau de $(\mathbb{R}, +, \times)$.

Définition 16. Soit $(A, +, \times)$ et $(B, \bigoplus, \bigotimes)$ deux anneaux. Une application $f : A \to B$ est un **morphisme d'anneaux** si :

- $\forall (x, y) \in A^2,\ f(x + y) = f(x) \bigoplus f(y)$
- $\forall (x, y) \in A^2,\ f(x \times y) = f(x) \bigotimes f(y)$
- $f(1) = 1$

Remarque 10. Contrairement au cas des morphismes de groupes, la condition sur l'image du neutre multiplicatif n'est pas automatiquement vérifiée pour un morphisme d'anneaux. On utilisera pas ailleurs le même vocabulaire (endomorphisme, isomorphisme, etc.) que pour les groupes.

Exemple : La conjugaison est un morphisme d'anneaux de $(\mathbb{C}, +, \times)$ vers $(\mathbb{R}, +, \times)$. C'est même un automorphisme de corps, comme on va le voir.

Définition 17. Un anneau $(K, +, \times)$ est un **corps** si $(K^*, \times)$ est un groupe. Autrement dit, tout élément non nul de K est inversible pour le produit.

Remarque 11. Un corps est toujours un anneau intègre.

Définition 18. On définit de façon totalement similaire aux anneaux les notions de sous-corops et de morphisme de corps.

Exemples : $(\mathbb{Q}, +, \times)$ est un sous-corps de $(\mathbb{R}, +, \times)$, qui est lui-même un sous-corps de $(\mathbb{C}, +, \times)$.

2.2 Arithmétique dans $\mathbb{Z}$

L'arithmétique est en général l'étude des propriétés des anneaux, mais dans ce paragraphe, nous nous contenterons de considérerer l'anneau le plus simple qui soit, celui des entiers relatifs. Nous verrons dans la dernière partie du cours consacrée aux polynômes que beaucoup des propriétés de $\mathbb{Z}$ s'étendent aux polynômes.

Définition 19. Soient n et p deux entiers relatifs, n est **divisible par** p (ou p divise n) s'il existe un troisième entier k tel que $n = kp$.

Remarque 12. La relation de divisibilité est une relation d'ordre sur $\mathbb{N}^*$ mais pas sur $\mathbb{Z}^*$, où elle n'est pas pas antisymétrique. En effet, deux entiers relatifs qui se divisent l'un l'autre sont soit égaux soit opposés.

Théorème 3. Division euclidienne.
Soit $n \in \mathbb{Z}$ et $p \in \mathbb{N}^*$, alors il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que $n = pq + r$, et $0 \leqslant r < p$. L'entier q est appelé **quotient** de la division euclidienne de n par p, et l'entier r **reste** de cette même division.

Exemple : Pour effectuer en pratique une division euclidienne, on peut revenir à ses classiques du primaire en posant la division (et en s'arrêtant avant d'obtenir un quotient décimal). Ainsi, on aura par exemple $207 = 14 \times 14 + 11$.

Démonstration. Commençons par prouver l'existence du couple (q, r), en supposant $n > 0$ (sinon, ce n'est pas beaucoup plus compliqué). Comme $\mathbb{R}$ est archimédien, il existe certainement un entier a à partir duquel $ap > n$, notons donc $q = \max\{a \in \mathbb{N} \mid ap \leqslant n\}$, et $r = n - pq$. Par définition, $pq \leqslant n$, donc $r \geqslant 0$. De plus, par maximalité de q, on doit avoir $(q+1)p > n$, soit $pq + p - n > 0$, ou encore $p > n - pq = r$. Enfin, par définition de r, $n = pq + r$, l'existence du couple est donc prouvée.
Démontrons désormais l'unicité en supposant comme d'habitude qu'il y a deux couples convenables (q, r) et (q', r'). On a alors $pq + r = pq' + r' = n$, donc $p(q - q') = r' - r$. En particulier $r' - r$ divise p, alors que $-p < r' - r < p$. Ce n'est possible que si $r' - r = 0$, soit $r' = r$, ce qui implique $p(q' - q) = 0$, donc $q = q'$. Les deux couples sont alors identiques. □

Définition 20. Soit n et p deux entiers naturels non nuls. Le **plus grand commun diviseur** (ou pgcd) de n et p est, comme son nom l'indique, le plus grand entier divisant simultanément n et p. On le note parfois $n \wedge p$. Le **plus petit commun multiple** (ou ppcm) est le plus petit entier naturel que divisent n et p.

Définition 21. Un entier naturel n est **premier** s'il n'est divisible que par 1 et par lui-même. Deux entiers n et p sont premiers entre eux si leu pgcd est égal à 1.

Remarque 13. Par convention, le nombre 1 n'est pas considéré comme un nombre premier.

Théorème 4. Théorème de Bezout.
Deux entiers n et p sont premiers entre eux si et seulement s'il existe un couple d'entiers $(a, b) \in \mathbb{Z}^2$ tels que $an + bp = 1$. Plus généralement, il existe toujours un couple d'entiers relatifs tels que $an + bp = n \wedge p$.

Démonstration. Ce théorème étant à la lisière du programme, on ne démontrera que la deuxième partie. Les deux entiers n et p engendrent dans $\mathbb{Z}$ les sous-groupes $n\mathbb{Z}$ et $p\mathbb{Z}$. Le sous-groupe G engendré par n et p est quant à lui composé de tous les entiers de la forme $an + bp$, pour a et b parcourant $\mathbb{Z}$ (en effet, un sous-groupe contenant n et p contient nécessairement tout ces éléments puisqu'il eststable par somme, et cet ensemble est bien un sous-groupe de $\mathbb{Z}$). Or, c'est un sous-groupe de $\mathbb{Z}$, donc il est de la forme $k\mathbb{Z}$. Comme $n \in G$ et $p \in G$, les deux entiers n et p sont divisibles par k, qui divise donc nécessairement le pgcd de n et p. Autrement dit, $n \wedge p \in G$, ce qui prouve l'existence de deux entiers tels que $an + bp = n \wedge p$. □

Théorème 5. Il existe une infinité de nombres premiers.

Démonstration. On va un tout petit peu anticiper sur le dernier résultat du paragraphe. Faisons un raisonnement par l'absurde : il existerait donc une liste finie p_1, p_2, …, p_k de nombres premiers. Notons alors $p = \prod_{i=1}^{k} p_i + 1$. Cet entier n'est sûrement pas divisible par p_1 (puisque l'entier qui le précède l'est et que $p_1 \geqslant 2$), ni par aucun des p_i. Soit il est lui-même premier (mais distinct des autres, ce qui est absurde), soit il est divisible par un entier premier (c'est là qu'on utilise la décomposition), qui n'est lui-même aucun des p_i. Dans tous les cas, on aboutit à une contradiction. □

Théorème 6. Décomposition en facteurs premiers.
Tout nombre entier $n \geqslant 2$ peut se décomposer de façon unique à l'ordre des facteurs près sous la forme $n = \prod_{i=1}^{i=k} p_i^{\alpha_i} = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k}$, où p_1, p_2, …, p_k sont des nombres premiers, et $(\alpha_1, \ldots, \alpha_k) \in (\mathbb{N}^*)^k$.

Démonstration. La démonstration de ce théorème n'est pas au programme, on va s'en dispenser. On peut la faire par récurrence, mais c'est un peu technique. □

3 Polynômes

Dans toute cette dernière partie, $\mathbb{K}$ désigne un corps qui peut être le corps $\mathbb{R}$ des nombres réels ou le corps $\mathbb{C}$ des nombres complexes.

3.1 L'anneau $\mathbb{K}[X]$

Définition 22. Un **polynôme à coefficients dans** $\mathbb{K}$ est un objet mathématique formel s'écrivant $P = \sum_{k=0}^{k=n} a_k X_k$, où $(a_0, a_1, \ldots, a_n) \in \mathbb{K}^{n+1}$, et X est une indéterminée destinée à être remplacée par n'importe quel objet pour lequel le calcul de P peut avoir un sens (donc en gros des éléments qu'on sait élever à une certaine puissance et multiplier par des éléments de $\mathbb{K}$).

Définition 23. On note $\mathbb{K}[X]$ l'ensemble de tous les polynômes à coefficients dans $\mathbb{K}$.

Proposition 12. Muni de la somme (si $P = \sum_{k=0}^{n} a_k X^k$ et $Q = \sum_{k=0}^{p} b_k X^k$, alors $P+Q = \sum_{k=0}^{\max(p,n)} (a_k + b_k)X^k$) et du produit ($PQ = \sum_{k=0}^{p+n} (\sum_{i=0}^{i=k} a_i b_{k-i}) X^k$) usuels sur les polynômes, l'ensemble $\mathbb{K}[X]$ est un anneau commutatif.

Démonstration. La démonstration est un peu pénible si on définit les polynômes en dehors de tout contexte, puisqu'on doit tout prouver, y compris l'associativité des opérations. Il est nettement plus commode d'identifier $\mathbb{K}[X]$ à l'ensemble des **fonctions polynômiales** de $\mathbb{K}$ dans $\mathbb{K}$, qui constitue un sous-anneau de l'ensemble de toutes les fonctions (ce qui pour le coup est facile à prouver). Notons tout de même que l'élément neutre pour l'addition est le polynôme nul, noté 0, et l'élément neutre pour le produit le polynôme constant 1. □

Définition 24. Soit $P = \sum_{k=0}^{k=n} a_k X^k$ un polynôme, avec $a_n \neq 0$. Les nombres a_k sont appelés **coefficients** du polynôme P, l'entier n **degré** de P (souvent noté $d^\circ(P)$), le coefficient correspondant a_n est le **coefficient dominant** de P. Si ce coefficient est égal à 1, on dit que P est un polynôme **unitaire**.

Remarque 14. Par convention, le polynôme nul a pour degré $-\infty$. C'est relativement cohérent avec les propriétés énoncées ci-dessous.

Proposition 13. Soient P et Q deux polynômes, alors $d^\circ(P+Q) \leqslant \max(d^\circ(P), d^\circ(Q))$, et $d^\circ(PQ) = d^\circ(P) + d^\circ(Q)$.

Démonstration. Cela découle immédiatement des définitions données des deux opérations. L'inagalité peut être stricte pour le degré de la somme, dans le cas où P et Q sont de même degré mais ont un coefficient dominant opposé. Par contre, c'est toujours une égalité pour le produit, le coefficient dominant du produit étant le produit des coefficients dominants de P et Q. □

Remarque 15. L'anneau $\mathbb{K}[X]$ est un anneau intègre. Ses seuls éléments inversibles sont les polynômes constants (non nuls). Ces deux remarques découlent de la propriété sur le degré d'un produit de polynômes.

Définition 25. Pour tout entier $n \in \mathbb{N}$, on note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré inférieur ou égal à n.

Remarque 16. Ces ensembles $K_n[X]$ sont stables par somme (contrairement à l'ensemble des polynômes de degré exactement n), ce qui est une des conditions pour en faire des sous-espaces vectoriels de $\mathbb{K}[X]$.

Définition 26. Soit $P = \sum_{k=0}^{n} a_k X^k$ et Q deux polynômes, le **polynôme composé** de P et Q est le polynôme $P \circ Q = \sum_{k=0}^{n} a_k Q^k$.

Exemple : Si $P = X^2 + 1$ et $Q = 2X + 3$, alors $P \circ Q = (2X + 3)^2 + 1 = 4X^2 + 12X + 10$, alors que $Q \circ P = 2(X^2 + 1) + 3 = 2X^2 + 5$.

Proposition 14. Si P et Q sont deux polynômes, $d^\circ(P \circ Q) = d^\circ(P) \times d^\circ(Q)$.

Démonstration. En effet, $P \circ Q = \sum_{k=0}^{n} a_k (\sum_{i=0}^{p} b_i X^i)^k$, dont le terme dominant vaut (si on développe tout brutalement à coups de formules du binôme de Newton) $a_n b_p^n X^{in}$. □

Définition 27. Un polynôme P est **divisible** par un polynôme Q s'il existe un troisième polonôme A tel que $P = AR$.

Remarque 17. Cette relation n'est pas une relation d'ordre sur $\mathbb{K}[X]$, elle est réflexive et transitive mais pas antisymétrique. Deux polynômes qui se divisent l'un l'autre sont simplement égaux à une constante multiplicative près. Dans ce cas, on dit que les deux polynômes sont **associés**.

Théorème 7. Division euclidienne dans $\mathbb{K}[X]$.
Soient $A, B \in \mathbb{K}[X]^2$, alors il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que $A = BQ + R$ et $d^\circ(R) < d^\circ(B)$. Le polynôme Q est appelé **quotient** de la division de A par B, et le polynôme R **reste** de cette même division.

Démonstration. La preuve de l'existence de la division peut se faire par récurrence sur le degré de A, le polynôme B restant fixé. L'existencce est triviale si $d^\circ(A) < d^\circ(B)$ puisqu'on peut écrire $A = 0B + A$, ce qui sert d'initialisation. Supposons désormais l'existence de la division prouvée pour tout polynôme de degré n, et choisissons A un polynôme de degré $n + 1$. Notons $a_n X^{n+1}$ son terme dominant, et $b_p X^p$ celui de B, alors $C = A - \frac{a_n}{b_p} X^{n+1-p} B$ est un polynôme de degré n (en effet, on a soustrait à A un polynôme de même degré et de même coefficient dominant. Par hypothèse de récurrence, il existe donc des polynômes Q et R tels que $C = BQ + R$, avec $d^\circ(R) < d^\circ(B)$. Mais alors $A = \left(Q + \frac{a_n}{b_p} X^{n+1-p}\right) B + R$, et comme R n'a pas changé de degré, on vient d'écrire une division euclidienne de A par B.
Pour l'unicité, on suppose évidemment qu'il y a deux couples possibles : $BQ + R = BQ' + R'$, alors $B(Q - Q') = R - R'$, avec par hypothèse et règles de calculs sur le degré d'une somme $d^\circ(R - R') < d^\circ(B)$. Or, $d^\circ(B(Q - Q')) \geqslant d^\circ(B)$, sauf si $Q - Q' = 0$, soit $Q = Q'$. On en déduit que $R - R' = 0$, donc les deux couples sont égaux. □

Exemple : Pour effectuer en pratique une division euclidienne de polynômes, on procède comme pour les entiers, par exemple pour diviser $X^4 - 3X^3 + 5X^2 + X - 3$ par $X^2 - 2X + 1$:

$$\begin{array}{rcrcrcrcr|l}
X^4 & - & 3X^3 & + & 5X^2 & + & X & - & 3 & X^2 - 2X + 1 \\
\cline{10-10}
- \ (X^4 & - & 2X^3 & + & X^2) & & & & & X^2 - X + 2 \\
 & - & X^3 & + & 4X^2 & + & X & - & 3 & \\
 & - & (-X^3 & + & 2X^2 & - & X) & & & \\
 & & & & 2X^2 & + & 2X & - & 3 & \\
 & & & - & (2X^2 & - & 4X & + & 2) & \\
 & & & & & & 6X & - & 5 &
\end{array}$$

Conclusion : $X^4 - 3X^3 + 5X^2 + X - 3 = (X^2 - X + 2)(X^2 - 2X + 1) + 6X - 5$. Cette méthode de calcul est une alternative à l'identification lorsqu'on cherche à factoriser un polynôme, par exemple après en avoir trouvé une racine évidente.

3.2 Factorisation de polynômes

Définition 28. Soit $P \in \mathbb{K}[X]$ et $x \in \mathbb{K}$. On dit que x est une **racine** du polynôme P si $P(x) = 0$.

Remarque 18. On identifie ici le polynôme et la fonction polynômiale associée, comme ce sera le cas dans tout ce dernier paragraphe.

Proposition 15. Un réel a est racine du polynôme P si et seulement si $X - a$ divise P.

Démonstration. C'est une conséquence de la division euclidienne. Si on effectue la division de P par $X-a$, on sait que le reste sera de degré strictement inférieur à celui de $X-a$, donc sera une constante. Autrement dit, $\exists k \in \mathbb{R}$, $P = Q(X - a) + k$. On a donc $P(a) = 0 \Leftrightarrow Q(a)(a - a) + k = 0 \Leftrightarrow k = 0$. Autrement dit, a est une racine de P lorsque le reste de la division de P par $X - a$ est nul, donc quand P est divisible par $X - a$. □

Exemple : on a déjà fréquemment utilisé cette propriété pour factoriser des polynômes de degré 3 possédant une récine « évidente ». Soit par exemple $P = 2X^3 - 3X^2 + 5X - 4$. On constate que 1 est racine évidente de P : $P(1) = 2 - 3 + 5 - 4 = 0$, donc P est factorisable par $X - 1$: $P = (X - 1)(aX^2 + bX + c) = aX^3 + (b - a)X^2 + (c - b)X - c$. Par identification, on obtient $a = 2$; $b - a = -3$; $c - b = 5$ et $-c = -4$, donc $a = 2$; $b = -1$ et $c = 4$, soit $P = (X - 1)(2X^2 - X + 4)$. Ce dernier facteur ayant un discriminant négatif, P n'admet pas d'autre racine réelle que 1.

Corollaire 1. Un polynôme admet a_1, a_2, …, a_k comme racines distinctes si et seulement si il est divisible par $\prod_{i=1}^{k}(X - a_i)$.

Démonstration. On peut procéder par récurrence sur le nombre de racines distinctes. L'initialisation correspond à la propriété précédente. Si on suppose qu'on polynôme P à k racines distinctes est toujours factorisable comme décrit, en ajoutant une racine a_{k+1}, on pourra commencer par écrire $P = \prod_{i=1}^{k}(X - a_i) \times Q$, et comme $P(a_{i+1}) = 0$, on a nécessairement $Q(a_{i+1}) = 0$ (en effet, les facteurs précédents $a_{i+1} - a_i$ ne peuvent s'annuler puisque les racines sont supposées distinctes). En appliquant à nouveau notre propriété, on peut donc écrire $Q = (X - a_{k+1})R$, ce qui donne la factorisation souhaitée pour P, et achève la récurrence. □

Corollaire 2. Un polynôme de degré n admet au maximum n racines distinctes.

Démonstration. En effet, s'il en avait plus, on pourrait l'écrire sous la forme $\prod_{k=1}^{n+1}(X - a_i) \times Q$, qui est de degré au moins $n + 1$. Il y a là une contradiction flagrante. □

Corollaire 3. Un polynôme admettant une infinité de racines est nécessairement le polynôme nul.

Démonstration. En effet, par contraposée, un polynôme non nul a un certain degré n, et ne peut donc pas avoir plus de n racines. □

Corollaire 4. Principe d'identification des coefficients.
Si deux polynômes P et Q correspondent à des fonctions polynômiales identiques, alors $P = Q$.

Démonstration. Dans ce cas, $P-Q$ est un polynôme admettant tous les réels (ou tous les complexes) comme racines, ce qui en fait une grosse infinité, donc $P - Q = 0$. C'est bien ce principe qu'on utilise pour identifier les coefficients de deux polynômes correspondant à des expressions polynômiales égales. □

Définition 29. Soit P un polynôme et a une racine de P. On dit que a est une racine **d'ordre de multiplicité** $k \in \mathbb{N}^*$ si $(X - a)^k$ divise P, mais $(X - a)^{k+1}$ ne divise pas P.

Définition 30. Soit $P = \sum_{k=0}^{k=n} a_k X^k \in \mathbb{K}[X]$. Le **polynôme dérivé de** P est le polynôme $P' = \sum_{k=1}^{k=n} k a_k X^{k-1}$. On notera également P'' le polynôme de dérivé de P', et $P^{(n)}$ le polynôme dérivé n fois du polynôme P.

Remarque 19. Cette dérivation, bien que définie de façon formelle, coïncide évidemment avec la dérivation usuelle sur les fonctions polynômiales, et de ce fait vérifie toutes les formules de dérivation usuelle. En particulier celle rappelée ci-dessous :

Proposition 16. Formule de Leibniz.

Soient P et Q deux polynômes, alors $\forall n \in \mathbb{N}$, $(PQ)^{(n)} = \sum_{k=0}^{k=n} \binom{n}{k} P^{(k)} Q^{(n-k)}$.

Démonstration. Ce résultat est formellement identique à la formule du binôme de Newton. Il se démontre par récurrence, exactement comme le binôme de Newton. Du coup, on ne le fera pas. □

Proposition 17. Une racine a est d'ordre de multiplicité k pour P si et seulement si $P(a) = P'(a) = \cdots = P^{(k-1)}(a) = 0$ et $P^{(k)}(a) \neq 0$.

Démonstration. Une façon de prouver ce résultat est de prouver le lemme suivant : si a est racine d'ordre k de P alors a est racine d'ordre $k-1$ de P'. En effet, si $P = (X_a)^k Q$, avec $Q(a) \neq 0$ alors $P' = k(X-a)^{k-1}Q + (X-a)^k Q' = (X-a)^{k-1}(kQ + (X-a)Q')$, avec $kQ(a) + (a-a)Q'(a) = kQ(a) \neq 0$. Par une récurrence facile, une racine d'ordre k sera donc racine de tous les polynômes dérivés jusqu'au $k-1$-ème, mais pas du k-ème. □

Remarque 20. La notation de dérivée pour un polynôme réel correspond à la dérivée de la fonction polynômiale associée. On peut en fait définir formellement le polynôme dérivé d'un polynôme sans passer par une interprétation en terme de fonctions. On notera également qu'on emploie souvent plus simplement le terme d'ordre ou celui de multiplicité à la place d'ordre de multiplicité.

Exemple : Considérons le polynôme $P = X^4 - 2X^3 - 19X^2 + 68X - 60$ et constatons ensemble que 2 est une racine double de P. En effet, on a $P(2) = 16 - 2\times 8 - 19\times 4 + 68\times 2 - 60 = 16 - 16 - 76 + 136 - 60 = 0$; de plus, $P' = 4X^3 - 6X^2 - 38X + 68$, donc $P'(2) = 4\times 8 - 6\times 4 - 38\times 2 + 68 = 32 - 24 - 76 + 68 = 0$. on peut en déduire, via la proposition précédente, que P est factorisable par $(X-2)^2$. Effectuons une petite division euclidienne pour obtenir cette factorisation :

$$\begin{array}{rcccccccc|l}
X^4 & - & 2X^3 & - & 19X^2 & + & 68X & - & 60 & \dfrac{X^2 - 4X + 4}{X^2 + 2X - 15} \\
- \ (X^4 & - & 4X^3 & + & 4X^2) & & & & & \\
 & & 2X^3 & - & 23X^2 & + & 68X & - & 60 & \\
 & - & (2X^3 & - & 8X^2 & + & 8X) & & & \\
 & & & - & 15X^2 & + & 60X & - & 60 & \\
 & & & - & (-15X^2 & + & 60X & - & 60) & \\
 & & & & & & & & 0 &
\end{array}$$

On a donc $P(X) = (X-2)^2(X^2+2X-15)$. Le deuxième facteur a pour discriminant $\Delta = 4+60 = 64$, et admet deux racines réelles $x_1 = \dfrac{-2-8}{2} = -5$ et $x_2 = \dfrac{-2+8}{2} = 3$. On peut donc factoriser P sous la forme $P(X) = (X-2)^2(X-3)(X+5)$. On ne risque pas de factoriser plus puisqu'il ne reste que des facteurs de degré 1.

Remarque 21. Un polynôme de degré n ne peut admettre plus de n racines comptées avec multiplicité. Ainsi, un polynôme de degré 5 admettant une racine triple ne peut plus admettre que deux autres racines.

Définition 31. Un polynôme P est **scindé** s'il peut s'écrire comme produit de polynômes de degré 1 (autrement s'il a un nombre de racines égal à son degré). Il est **scindé à racines simples** si de plus toutes ses racines sont distinctes.

Théorème 8. Théorème de d'Alembert-Gauss.
Tout polynôme dans $\mathbb{K}[X]$ est scindé.

Démonstration. Ce résultat fondamental a déjà été croisé dans le chapître sur les nombres complexes. Nous n'avons toujours pas les moyens de le démontrer maintenant. □

Exemple : Le polynôme $X^4 - 1$ se factorise dans $\mathbb{C}[X]$ sous la forme $X^4 - 1 = (X-1)(X+1)(X-i)(X+i)$.

Théorème 9. Tout polynôme $P \in \mathbb{R}[X]$ peut se factoriser sous la forme $P = \alpha(X - a_1)\dots(X - a_k)Q_1 \dots Q_p$, où α est le coefficient dominant de P, les a_i sont les racines réelles du polynôme P, et les polynômes Q_i sont des polynômes de degré 2 à discriminant strictement négatif.

Démonstration. Puisqu'on peut identifier $\mathbb{R}$ à un sous-corps de $\mathbb{C}$, le polynôme P peut être vu comme un élément de $\mathbb{C}[X]$ et donc s'écrire, d'après le théorème précédent, sous la forme $P = \prod_{j=1}^{d^\circ(P)} (X - \alpha_i)$, où les α_i sont les racines complexes de P. Parmi tous ces facteurs, on peut déjà isoler tous ceux qui correspondent à des racines réelles, qui donneront les premiers termes dans la factorisation annoncée. Reste à savoir quoi faire des racines complexes. Commençons par constater que, si z est racine complexe de P, alors $\overline{z}$ également. En effet, $P(\overline{z}) = \sum_{k=1}^{n} a_k \overline{z}^k = \sum_{k=1}^{n} \overline{a_k z^k} = \overline{P(z)}$, puisque les coefficients a_k sont réels et donc égaux à leur conjugué. Si $P(z) = 0$, on aura également $\overline{P(z)} = 0$, donc $P(\overline{z}) = 0$. De plus, la multiplicité de z sera toujours la même que celle de $\overline{z}$ puisque le raisonnement précédent peut s'appliquer à l'identique aux polynômes dérivés successifs de P. On peut donc regrouper tous les termes faisant intervenir des racines complexes sous la forme (quitte à répéter plusieurs fois chaque racine et chaque conjugué) $(X - z_1)(x - \overline{z_1})\dots(X - z_p)(X - \overline{z_p})$. Reste à constater que $(X - z_i)(X - \overline{z_i}) = X^2 - (z_i + \overline{z_i})X + z_i\overline{z_i} = X^2 - 2\text{Re}\ (z_i) + |z_i|^2$ est un polynôme de degré 2 à coefficients réels, et à discriminant négatif puisque ses racines sont complexes. La factorisation annoncée en découle. □

Définition 32. Un polynôme P est **irréductible** s'il ne peut pas se décomposer comme produit de deux polynômes de degré strictement inférieur au sien. Autrement dit, les seuls diviseurs d'un polynôme irréductibles sont ses polynômes associés et les polynômes constants.

Remarque 22. Par convention, on décrète que les polynômes constants ne sont pas irréductibles.

Théorème 10. Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.
Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 à discriminant strictement négatif.

Théorème 11. Tout polynôme $P \in \mathbb{K}[X]$ s'écrit comme produit de facteurs irréductibles, et ce produit est unique à l'ordre des facteurs et au remplacement de certains polynômes par des polynômes associés près.

Démonstration. Ces derniers théorèmes ne sont que des façons légèrement différentes d'énoncer la factorisation des polynômes vue un peu plus haut. L'unicité de la décomposition en produit d'irréductibles est admise. □

Proposition 18. Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{C}[X]$, et α_1, α_2, …, α_n ses racines (éventuellement répétées plusieurs fois). On a alors les relations suivantes entre les coefficients et les racines de P :

- $\sum_{k=1}^{k=n} \alpha_i = -\frac{a_{n-1}}{a_n}$
- $\sum_{1 \leqslant i < j \leqslant n} \alpha_i \alpha_j = \frac{a_{n-2}}{a_n}$
- $\dots$
- $\sum_{1 \leqslant i_1 < i_2 < \dots < i_p \leqslant n} \alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_p} = (-1)^p \frac{a_{n-p}}{a_n}$
- $\dots$
- $\prod_{k=1}^{n} \alpha_i = (-1)^n \frac{a_0}{a_n}$

Démonstration. Il suffit d'identifier la forme développée du polynôme et sa forme factorisée. On sait que $P = a_n(X - \alpha_1)(X - \alpha_2)\dots(X - \alpha_n)$. Si on développe brutalement ce produit, le terme dominant sera $a_n X^n$ (heureusement !), le terme de degré $n-1$ est obtenu dans le développement en piochant des X dans $n-1$ parenthèses et un coefficient dans la dernière, ce qui donne $a_n(-\alpha_1 X^{n-1} - \alpha_2 X^{n-1} - \dots - \alpha_n X^{n-1})$, qu'on identifie à $a_{n-1}X^{n-1}$ pour obtenir la première formule annoncée. Les autres sont obtenues de la même façon, les termes en X^{n-p} étant obtenus en prenant au choix p racines dans p parenthèses et $n-p$ X dans les autres, ce qui donne un terme en $(-1)^p \alpha_{i_1} \dots \alpha_{i_p} X^{n-p}$. Le terme constant est obtenu en prenant les racines dans toutes les parenthèses, il est égal à $a_n \times (-1)^n \prod_{k=1}^{n} \alpha_i$. □

Exemple : Pour un polynôme de degré 4 ayant pour racines a, b, c et d, les formules deviennent $a+b+c+d = -\frac{a_3}{a_4}$; $ab+ac+ad+bc+bd+cd = \frac{a_2}{a_4}$; $abc+abd+acd+bcd = -\frac{a_1}{a_4}$ et $abcd = \frac{a_0}{a_4}$.

Exemple : On cherche à factoriser le polynôme $4X^3 - 4X^2 - 15X + 18$, sachant qu'un ami nous a glissé un indice : il possède une racine double. deux méthodes sont possibles pour celà.

Première méthode : Puisqu'il y a une racine double, celle-ci est également racine de P'. Or, $P' = 12X^2 - 8X - 15 = 4\left(3X^2 - 2X - \frac{15}{4}\right)$. Ce trinôme a pour discriminant $\Delta = 4 + 3 \times 15 = 49$, et admet pour racines $X_1 = \frac{2+7}{6} = \frac{3}{2}$ et $X_2 = \frac{2-7}{6} = -\frac{5}{6}$. Vérifions si X_1 est racine de P : $4 \times \frac{27}{8} - 4 \times \frac{9}{4} - \frac{45}{2} + 18 = \frac{27}{2} - \frac{45}{2} + 9 = 0$, donc $\frac{3}{2}$ est la racine double recherchée. Inutile de vérifier si $\frac{5}{6}$ est aussi racine double, un polynôme de degré 3 ne peut pas avoir deux racines doubles. Pour déterminer la dernière racine, on peut effectuer une division euclidienne ou plus simplement utiliser le fait que le produit des trois racines sera égal à $-\frac{18}{4}$. Comme ce produit vaut, en notant α la dernière racine, $\left(\frac{3}{2}\right) \times \alpha = \frac{9}{4}\alpha$, on en déduit que $\alpha = -2$, et $P = 4\left(X - \frac{3}{2}\right)^2 (X+2)$.

Deuxième méthode : On utilise directement les relations coefficients-racines. En notant a la racine double et b la troisième racine de P, on aura le système $\begin{cases} 2a+b &= 1 \\ a^2+2ab &= -\frac{15}{4} \\ a^2 b &= -\frac{9}{2} \end{cases}$ En substituant $b = 1-2a$ dans la deuxième équation, on trouve $a^2 + 2a(1-2a) = -\frac{15}{4}$, soit $-3a^2 + 2a + \frac{15}{4} = 0$. Tiens, comme c'est curieux, c'est la même équation que plus haut. Pour déterminer si les deux solutions trouvées sont valables, on vérifie que la troisième équation du système fonctionne avec les valeurs obtenues. Si $a = -\frac{5}{6}$, on trouive $b = 1 - 2a = \frac{8}{3}$, d'où $a^2 b = \frac{25}{36} \times \frac{8}{3} = \frac{50}{27}$, ce qui assez différent de $-\frac{9}{2}$. Par contre, si $a = \frac{3}{2}$, $b = 1 - 2a = -2$, et $a^2 b = \frac{9}{4} \times (-2) = -\frac{9}{2}$, là ça marche. La conclusion est la même que ci-dessus.