1 Arithmétique

1.1 Nombres premiers et décomposition

1.1.1 Division euclidienne

Rappelons que l'ensemble des entiers relatifs muni de l'addition et de la multiplication vérifie les propriétés suivantes :

Si on prend deux entiers a et b avec b non nul, il existe deux entiers q et r, avec $|r| < |b|$ tels que $a = qb + r$.

Remarquons que la division euclidienne est unique dans $\mathbb{N}$ mais pas dans $\mathbb{Z}$, par exemple si on divise 19 par 7, on a dans $\mathbb{N}$, $19 = (2 \times 7) + 5$ et dans $\mathbb{Z}$, en outre, on a aussi $19 = (3 \times 7) + (-2)$.

1.1.2 Nombres premiers

Soient a et b deux entiers relatifs. On dit que a *divise* ou est un *diviseur* de b, ou encore que b est *multiple* de a s'il existe un entier n tel que $na = b$. On le note $a|b$.

On dit qu'un entier ≥ 2 est un nombre premier si les seuls nombres positifs qui le divisent sont 1 et lui-même. On dit que $n \in \mathbb{Z}$ est premier si $|n|$ est un nombre premier. Il y a une infinité de nombres premiers.

THÉORÈME **1.1** *Tout nombre entier non n nul s'écrit de manière unique sous forme* $n = \epsilon \prod_{i=1}^{k} p_i^{\alpha_i}$ *où* $\epsilon = \pm 1$*, les* p_i *sont des nombres premiers positifs rangés en ordre croissant (i.e.* $p_i < p_j$ *si* $i < j$*), et les* α_i *des entiers strictement positifs.*

EXEMPLE **1.1.1** *On a* $440 = 2^3 \times 5 \times 11$ *et* 2*,* 5 *et* 11 *sont des nombres premiers.*

1.2 pgcd et ppcm

Soient p et q deux nombres entiers strictement positifs. Il existe alors un entier strictement positif r qui est diviseur à la fois de p et de q et qui est multiple de tous les diviseurs communs à p et q. Ce nombre r est unique et s'appelle de *pgcd* (plus grand commun diviseur) de p et de q.

Une façon de calculer le pgcd de deux entiers naturels est d'effectuer l'algorithme d'Euclide.

EXEMPLE **1.2.1** *Soit à calculer* $pgcd(42, 234)$. *On a* $234 = 42 \times 5 + 24$, *d'où* $pgcd(42, 234) = pgcd(24, 42)$, *puis* $42 = 24 + 18$, *d'où* $pgcd(24, 42) = pgcd(18, 24)$, *puis* $24 = 18 + 6$, *d'où* $pgcd(18, 24) = pgcd(6, 18)$ *et comme* $18 = 6 \times 3$, $pgcd(6, 18) = 6$. *Ainsi,* $pgcd(42, 234) = 6$.

Une autre façon de calculer le pgcd de deux entiers naturels est d'effectuer leur décomposition en facteurs premiers. Si $p = \prod_{i=1}^{k} p_i^{\alpha_i}$ et $q = \prod_{i=1}^{k} p_i^{\beta_i}$, alors $pgcd(p, q) = \prod_{i=1}^{k} p_i^{\min(\alpha_i, \beta_i)}$.

N.B. : Dans la formule précédente, pour avoir la même liste de facteurs pour p et pour q, on s'autorise à ce que certains p_i soient à la puissance 0 dans une décomposition ou l'autre, ce qui fait que ce ne sont pas tout à fait leur décomposition.

EXEMPLE **1.2.2** *On a* $440 = 2^3 \times 5(\times 7^0) \times 11$ *et* $140 = 2^2 \times 5 \times 7(\times 11^0)$. *Alors,* $pgcd(440, 140) = 2^2 \times 5 = 20$.

Si maintenant p et q sont deux entiers relatifs non nuls, on définit leur pgcd comme le pgcd de $|p|$ et $|q|$.

Enfin, par convention, le pgcd d'un entier relatif n quelconque et de 0 est $|n|$.

On dit que deux entiers sont *premiers entre eux* si leur pgcd vaut 1.

Le pgcd de deux entiers p et q est parfois noté $p \wedge q$.

On peut étendre la notion de pgcd à une famille finie quelconque d'entiers par $pgcd(q_1, ..., q_k) = pgcd(pgcd(q_1, ..., q_{k-1})q_k)$, qui ne dépend pas de l'ordre dans lequel on considère les q_i.

Soient p et q deux nombres entiers strictement positifs. Il existe alors un entier strictement positif r qui est multiple à la fois de p et de q et qui divise tous les multiples communs à p et q. Ce nombre r est unique et s'appelle de *ppcm* (plus petit commun multiple) de p et de q.

Ici, aussi, on peut obtenir le ppcm de deux entiers par leur factorisaton : Si $p = \prod_{i=1}^{k} p_i^{\alpha_i}$ et $q = \prod_{i=1}^{k} p_i^{\beta_i}$, alors $pgcd(p, q) = \prod_{i=1}^{k} p_i^{\max(\alpha_i, \beta_i)}$.

EXEMPLE **1.2.3** *Reprenons les mêmes nombres, soit* $440 = 2^3 \times 5(\times 7^0) \times 11$ *et* $140 = 2^2 \times 5 \times 7(\times 11^0)$. *Alors,* $ppcm(440, 140) = 2^3 \times 5 \times 7 \times 11 = 3080$.

Si on prend deux entiers relatifs non nuls p et q, on définit leur ppcm comme étant le ppcm de $|p|$ et de $|q|$, et le ppcm d'un entier quelconque et de 0 est par convention égal à 0.

Le ppcm de deux entiers p et q est parfois noté $p \vee q$.

On peut voir que pour tous entiers relatifs p et q, on a

$$pgcd(p, q) \times ppcm(p, q) = |pq|$$

Ceci peut permettre de calculer le ppcm de deux entiers sans les factoriser, en calculant leur pgcd par l'algorithme d'Euclide.

On peut aussi, comme dans le cas du pgcd, étendre la notion de ppcm à un nombre fini quelconque de nombres.

La proposition suivante porte le nom de *lemme de Gauß* :

PROPOSITION **1.2** *Soient a et b trois entiers. On suppose que a divise bc et que a et b sont premiers entre eux. Alors a divise c.*

En particulier, si un nombre premier p divise un produit ab, il divise soit a, soit b.

1.3 Bezout et équations diophantiennes

Prenons deux nombres p et q et soit d leur pgcd. Alors, il existe deux entiers a et b tels que $ap + bq = d$ (remarquons que d divise toute expression de cette forme). Ceci s'appelle l'identité de Bezout. En particulier, si p et q sont premiers entre eux, il existe a et b tels que $ap + bq = 1$.

Deux tels entiers peuvent être trouvés grâce à l'algorithme d'Euclide.

Supposons maintenant que l'on se donne trois entiers $p \neq 0$, $q \neq 0$ et n et qu'on cherche à résoudre l'équation $px + qy = n$, où x et y sont des inconnues entières.

Appelons d le pgcd de p et de q, et posons $p' = \frac{p}{d}$, $q' = \frac{q}{d}$.

Si n n'est pas multiple de d, alors l'équation étudiée n'a pas de solution.

Si n est multiple de d, disons $n = kd$, alors on peut trouver une solution particulière de l'équation sous la forme $x_0 = ka, y_0 = kb$ où a et b sont tels que $ap + bq = d$.

L'équation étudiée se réecrit alors $p(x - x_0) + q(y - y_0) = 0$, ce qui amène à la résolution de l'équation $pX + qY = 0$. En divisant par d les deux membres de cette égalité, on trouve qu'elle équivaut à $p'X + q'Y = 0$.

Or, si un couple (X, Y) vérifie cette équation, on doit avoir $p'(-X) = q'Y$, et donc p' divise $q'Y$, et par suite Y d'après le lemme de Gauß. De même, q' doit diviser X et on écrit alors $(X, Y) = (k_1 q', k_2 p')$. Finalement, il est clair qu'un tel couple vérifie l'équation voulue si et seulement si $k_1 = -k_2$. Les solutions sont donc de la forme $(X, Y) = (kq', -kp')$ ce qui donne $(x, y) = (x_0 + kq', y_0 - kp')$.

1.4 Congruences

Considérons un entier n strictement positif. On dit que deux entiers a et b sont *congrus* modulo n si n divise $a - b$. On le note $a \equiv b\,[n]$.

La relation de congruence modulo n est une relation d'équivalence, qui possède n classes d'équivalence. L'ensemble de ces classes d'équivalence (dites classes de congruence modulo n) se note $\mathbb{Z}/n\mathbb{Z}$. La classe d'un entier a se note $\bar{a}$.

On peut mettre sur $\mathbb{Z}/n\mathbb{Z}$ une addition et une multiplication naturelles. En effet, si on se donne deux couples d'entiers a et a' congrus modulo n ainsi que b et b' congrus modulo n, alors $a+b$ et $a'+b'$ sont congrus modulo n ce qui permet de définir $\bar{a}+\bar{b}$ par $\overline{a+b}$ et $a \times b$ et $a' \times b'$ sont congrus modulo n, ce qui permet de définir $\bar{a}.\bar{b}$ par $\overline{a.b}$. Nous verrons plus tard que ces opérations munissent $\mathbb{Z}/n\mathbb{Z}$ d'une structure d'anneau, qui est un corps lorsque n est un nombre premier.

EXEMPLE **1.4.1** *Prenons $\mathbb{Z}/10\mathbb{Z}$. Considérér la classe d'un entier n revient, quand n est positif, à ne considérer que son dernier chiffre. Or, on sait que le dernier chiffre d'une somme ou d'un produit de deux nombres ne dépend que de leur dernier chiffre.*

Dans ce contexte, l'identité de Bezout se traduit de la façon suivante : Supposons qu'on se place dans $\mathbb{Z}/n\mathbb{Z}$ et prenons un entier m, et soit $d = pgcd(m,n)$. Alors, il existe deux entiers u et v tels que $um+vn=d$. Si on regarde au niveau des classes, cela donne $\bar{u}\bar{m} = \bar{d}$ car $\bar{n} = \bar{0}$. En particulier, si m et n sont premiers entre eux, il existe $\bar{u}$ dans $\mathbb{Z}/n\mathbb{Z}$ dont le produit avec $\bar{m}$ fait $\bar{1}$. On dit alors que $\bar{m}$ est *inversible* dans $\mathbb{Z}/n\mathbb{Z}$.

Le théorème suivant porte le nom de théorème des restes chinois (ou simplement théorème chinois) :

THÉORÈME **1.3** *Soient $n_1, ..., n_k$ des nombres entiers strictement positifs et deux à deux premiers entre eux. Donnons nous des entiers $m_1, ..., m_k$. Alors, il existe un entier q tel que pour $i = 1, ..., k$, q est congru à m_i modulo n_i. De plus, si q' vérifie aussi toutes ces congruences, alors q et q' sont congrus modulo $n_1 \times n_2 \times ... \times n_k$.*

2 Lois de composition et groupes

2.1 Lois de composition

DÉFINITION **2.1** *Soit E un ensemble. On appelle loi de composition interne de E une application de $E \times E$ dans E. Si $*$ est une loi de composition interne de E et a, b deux éléments de E, on notera généralement $a*b$ l'élément $*(a,b)$ et on l'appellera le composé de a par b pour la loi $*$.*

On dit qu'une loi de composition interne est *commutative* si, pour tous a et b de E, on a $a * b = b * a$.

On dit qu'une loi de composition interne est *associative* si, pour tous a, b et c de E, on a $a * (b * c) = (a * b) * c$. Pour une telle loi, on peut éviter de mettre des parenthèses dans une expression comprenant plusieurs compositions.

Prenons deux lois de composition internes $*$ et ∇ d'un ensemble E. On dit que $*$ est *distributive* à gauche (resp. à droite) par rapport à ∇ si, pour tous a, b et c de E, on a $a*(b\nabla c) = (a\nabla b)*(a\nabla c)$ (resp. $(a\nabla b)*c = (a\nabla c)*(b\nabla c)$). On dit qu'une loi est distributive par rapport à une autre si elle l'est des deux côtés.

Soit $*$ une loi de composition interne sur un ensemble E. Un élément x de E est dit *neutre* à gauche (resp. à droite) pour $*$ si, pour tout y dans E, on a $x * y = y$ (resp. $y * x = y$). On dit que x est neutre pour $*$ s'il l'est des deux côtés. Si une loi possède un élément neutre, il est unique.

Supposons que la loi de composition interne $*$ de E possède un élément neutre e, et soit x un élément de E. On dit que l'élément y de E est un *symétrique* à gauche (resp. à droite) de x pour $*$ si on a $y * x = e$ (resp. $x * y = e$). On dit que y est symétrique de x pour $*$ s'il l'est des deux côtés.

Soit $*$ une loi de composition interne sur un ensemble E. Un élément x de E est dit *absorbant* à gauche (resp. à droite) pour $*$ si, pour tout y dans E, on a $x * y = x$ (resp. $y * x = x$). On dit que x est absorbant s'il l'est des deux côtés. Si une loi possède un élément absorbant, il est unique.

Soit $*$ une loi de composition interne sur un ensemble E. Un élément x de E est dit *régulier* ou parfois *simplifiable* à gauche (resp. à droite) pour $*$

si, pour tous y et y' dans E, l'égalité $x * y = x * y'$ implique $y = y'$ (resp. $y * x = y' * x$ implique $y = y'$). On dit que x est régulier s'il l'est des deux côtés.

Soit $*$ une loi de composition interne sur un ensemble E. Une partie F de E est dite *stable* par $*$ si, pour tous x et y dans F, on a $x * y \in F$. Toute intersection de parties stables pour $*$ est encore stable ; ainsi, si on se donne une partie quelconque X de E, l'intersection des parties stables de E contenant X s'appelle la partie stable de E engendrée par X.

2.2 Groupes

DÉFINITION **2.2** *On appelle groupe un ensemble E muni d'une loi de composition interne $*$ vérifiant :*
i) La loi $*$ est associative ;
ii) la loi $*$ est possède un élément neutre ;
iii) tout élément de E possède un symétrique pour $*$.

Soit $(E, *)$ un groupe. Si la loi $*$ est commutative, on dit que le groupe est *commutatif* ou *abélien.*

Un groupe sera souvent noté G et sa loi . ou $+$, cette dernière notation étant réservée aux groupes commutatifs. L'élément neutre sera habituellement noté e si la loi s'écrit . ou 0 si la loi s'écrit $+$.

Dans un groupe, tout élément x est régulier et ne possède qu'un seul symétrique, qui sera noté x^{-1} si la loi est notée . ou $-x$ si elle est notée $+$. Si x et y sont deux éléments de G, on a $(xy)^{-1} = y^{-1}x^{-1}$.

Exemples :

Munis de l'addition, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des groupes

Munis de la multiplication, $\mathbb{R}_+^*$, $\mathbb{C}^*$ ou l'ensemble S^1 des nombres complexes de module 1 sont des groupes.

L'ensemble des bijections d'un enemble quelconque dans lui-même, muni de la composition, est un groupe.

L'ensemble des applications affines et bijectives d'un plan affine dans lui-même, muni de la composition, est un groupe. Si on se fixe une partie E de ce plan, l'ensemble des applications de la forme précédente qui, de plus, réalisent une bijection de E dans E est un groupe (toujours avec la composition). Ceci est d'ailleurs vrai en toute dimension.

DÉFINITION **2.3** *Une partie H d'un groupe $(G, .)$ s'appelle un sous-groupe si elle est stable par . et que $(H, .)$ est un groupe.*

Cela revient à demander que H contienne l'élément neutre de G, la composée de deux quelconques de ses éléments et l'inverse de chacun de ses éléments.

Cela équivaut aussi à :
i) H n'est pas vide ;
ii Pour tous x et y dans H, $x.y^{-1}$ est aussi dans H.

Un sous-groupe d'un groupe H de G a le même élément neutre que G et tout élément de H a le même inverse dans H ou dans G.

Toute intersection de sous-groupes d'un groupe G est encore un sous-groupe de G. Ainsi, si E est une partie quelconque de G, l'intersection des sous-groupes de G qui contiennent E s'appelle le sous-groupe *engendré* par E. On le note $\langle E \rangle$.

Plus précisément, le sous-groupe engendré par E est l'ensemble des éléments de G qui peuvent se mettre sous la forme $x_1^{\epsilon_1}.x_2^{\epsilon_k}...x_k^{\epsilon_k}$ où k est un entier naturel, les x_i sont des éléments de E et les ϵ_i valent ± 1.

Un groupe est dit *monogène* s'il existe une partie à un élément qui l'engendre. Un groupe monogène G engendré par un élément x est donc $\{x^k, k \in \mathbb{Z}\}$. L'application $k \to x^k$ est alors un morphisme surjectif de $\mathbb{Z}$ dans G. S'il n'existe aucun $n \in \mathbb{N}$ tel que $x^n = e$, alors cette application est un isomorphisme entre $\mathbb{Z}$ et G. Si n est le plus petit entier strictement positif tel que $x^n = e$, alors ce morphisme induit un isomorphisme entre $\mathbb{Z}/n\mathbb{Z}$ et G. Un tel groupe est alors appelé *cyclique*.

Si G est un groupe, on appelle *centre* de G, noté $Z(G)$ l'ensemble des éléments x tels que pour tout $g \in G$, on a $g.x = x.g$. C'est un sous-groupe de G, et remarquons qu'il est abélien.

Soient $(G, *)$ et (G', ∇) deux groupes. On appelle *morphisme* de groupes de $(G, *)$ dans (G', ∇) une application ϕ de G' dans G' telle que pour tous x et y de G, on a $\phi(x * y) = \phi(x)\nabla\phi(y)$. La composée de deux morphismes de groupes est encore un morphisme de groupes. Un morphisme de groupes bijectif s'appelle un *isomorphisme* (de groupes).

Soit ϕ un morphisme d'un groupe $(G, .)$ dans un groupe $(G', .)$. Alors $\phi(e_G) = e_{G'}$, pour tout x de G, $\phi(x^{-1}) = \phi(x)^{-1}$, si H est un sous-groupe de G, alors $\phi(H)$ est un sous-groupe de G', et si H' est un sous-groupe de G', alors $\phi^{-1}(H)$ est un sous-groupe de G.

DÉFINITION **2.4** *On appelle noyau d'un morphisme ϕ de groupes de G dans G' l'image réciproque par ϕ de l'élément neutre de G'. On le note* $\ker \phi$.

Un morphisme de groupes est injectif si et seulement si son noyau est réduit à lélément neutre.

Le noyau d'un morphisme de G dans G' est, nous l'avons dit, un sous-groupe de G. Ce n'est d'ailleurs pas n'importe quel sous-groupe. On remarque que si $x \in \ker \phi$ et $g \in G$ quelconque, on a $\phi(g^{-1}xg) = (\phi(g))^{-1}\phi(x)\phi(g) = \phi(g)^{-1}e_{G'}\phi(g) = \phi(g)^{-1}\phi(g) = e_{G'}$. Ainsi, $g^{-1}xg$ est lui aussi forcément un élément de $\ker \phi$.

Nous allons étudier plus précisément ce type de sous-groupes.

2.3 Conjugaison. Sous-groupes distingués. Groupes quotients

2.3.1 Conjugaison

Sioit G un groupe, x et g deux éléments de G. On appelle *conjugué* de x par g l'élément $g^{-1}.x.g$.

La relation de conjuguaison, $x\mathcal{R}y$ s'il existe g tel que y soit le conjugué de x par g est une relation d'équivalence, dont les classes d'équivalence s'appellent les *classes de conjuguaison*.

Pour tout g de G, l'application $\rho_g : x \to g^{-1}xg$ est un isomorphisme de G dans lui-même (ce qu'on appelle un *automorphisme*). Un tel automorphisme de G s'appellera un automorphisme *intérieur* de G.

De plus, on peut remarquer que les automorphismes de G forment un groupe pour la composition et que l'application $g \to \rho_g$ est un morphisme de groupes, de noyau $Z(G)$.

2.3.2 Congruences. Sous-groupes distingués

Soit G un groupe et H un sous-groupe de G. On définit alors deux relations d'équivalence appelées *congruences* modulo H, à gauche et à droite de la façon suivante :

$$\text{Congruence à gauche : } x\mathcal{R}_g y \text{ si } x^{-1}.y \in H$$
$$\text{Congruence à droite : } x\mathcal{R}_d y \text{ si } x.y^{-1} \in H$$

Les classes d'équivalence de ces deux relations s'appellent respectivement les classes à gauche modulo H et les classes à droite modulo H. La classe à gauche contenant l'élément x sera notée xH, et c'est $\{x.h, h \in H\}$. De même, la classe à droite contenant l'élément x sera notée Hx. L'ensemble des classes à gauche sera noté G/H et l'ensemble des classes à droite sera noté $H\backslash G$.

PROPOSITION **2.1** *Les conditions suivantes sont équivalentes :*
i) Les deux relations $\mathcal{R}_g$ et $\mathcal{R}_d$ sont les mêmes ;
ii) On a $xH = Hx$ pour tout $x \in G$;
iii) On a $x.h.x^{-1} \in H$ quel que soit h dans H et x dans G (i.e. H est laissé stable par les automorphismes intérieurs).

DÉFINITION **2.5** *Le sous-groupe H de G est dit distingué ou normal (parfois même invariant s'il vérifie les conditions de la proposition précédente.*

THÉORÈME **2.2** *Soit H un sous-groupe distingué d'un groupe G. Alors on peut mettre une structure naturelle de groupe sur le quotient $G/H(= H\backslash G)$*

de la facon suivante : $xH.yH = (xy)H$. Le groupe obtenu, appelé groupe quotient de G par H sera aussi noté G/H. L'application $\pi : x \to xH$ de G dans G/H est un morphisme surjectif de groupes et son noyau est H.

Décomposition canonique d'un morphisme de groupes :

Soient ϕ un morphisme d'un groupe G dans un groupe G'. Nous avons montré que le noyau de ϕ était un sous-groupe distingué de G. En fait, on dit que le morphisme ϕ "passe au quotient" par $\ker\phi$ en un morphisme $\tilde{\phi}$ de $G/\ker\phi$ dans G' donné par $\tilde{\phi}[x] = \phi(x)$ ($[x]$ désignant la classe de x modulo $\ker\phi$), c'est-à-dire que l'image d'une classe ne dépend pas du représentant choisi. Ensuite, l'application de $G/\ker\phi$ dans $Im\phi$ donnée par $\tilde{\phi}$ est un isomorphisme. On obtient alors :

$$G \xrightarrow{\pi} G/H \xrightarrow{\tilde{\phi}} Im\phi \xhookrightarrow{i} G'$$

et $\phi = i \circ \tilde{\phi} \circ \pi$, ce qu'on appelle la décomposition canonique de ϕ.

PROPOSITION **2.3** *Soient G un groupe, K un sous-groupe distingué de G, et H sous-groupe de G contenant K. Alors :*
a) K est un sous-groupe distingué de H.
b) Le groupe H/K est isomorphe à l'image de H par la projection canonique de G sur G/K (on les identifie alors).
c) Si H aussi est distingué dans G, on a G/K isomorphe à $(G/H)/(H/K)$

PROPOSITION **2.4** *Soit H un sous-groupe distingué d'un groupe G et K un sous-groupe quelconque. Alors :*
a) L'ensemble $HK = \{h.k, h \in H, k \in K\} = KH$ est un sous-groupe de G.
b) Les groupes HK/H (nous savons déjà que H est distigué dans HK) et $K/K \cap H$ ($K \cap H$ est distigué dans K) sont isomorphes.

Un groupe non trivial (i.e. non non réduit à un élément) est dit *simple* si ses seuls sous-groupes distigués sont lui-même et son sous-groupe trivial (i.e. réduit à son élément neutre). Si ϕ est un morphisme d'un groupe simple G dans un groupe quelconque G', alors soit ϕ est injectif, soit ϕ est trivial. Les seuls groupes simples commutatifs sont (à isomorphisme près), les $\mathbb{Z}/p\mathbb{Z}$, pour p premier.

2.4 Ordre des groupes finis

Soit G un groupe fini. Son cardinal est traditionnellement appelé son *ordre* et noté $|G|$.

Si on prend un sous-groupe H de G, alors toutes les classes à droite comme à gauche modulo H ont pour cardinal $|H|$, et ainsi les ensembles quotients G/H et $H\backslash G$ ont pour cardinal $|G|/|H|$, qu'on appelle *indice* de G dans H et qu'on note $[G : H]$. En particulier, si H est distigué, $|G/H| = [G : H]$.

Insistons sur le fait (théorme de Lagrange) que l'ordre d'un sous-groupe divise toujours l'ordre du groupe (si ce dernier est fini).

La réciproque de ce résultat est fausse, c'est-à-dire que si on se donne un diviseur de l'ordre d'un groupe fini G, il n'y a pas forcément de sous-groupe de G ayant l'ordre choisi. Toutefois, il est bon de connaître les résultats suivants, sans doute hors programme, mais très utiles dans l'étude concrète d'un groupe donné.

On se fixe un groupe fini G, n son ordre et p un nombre premier qui divise n. Soit k l'entier naturel tel que n soit multiple de p^k mais pas de p^{k+1}. Alors pour $k' \leq k$, il existe un sous-groupe de G d'ordre $p^{k'}$. Les sous-groupes d'ordre p^k de G s'appellent les p-(sous-groupes de)Sylow de G. Leur nombre est congru à 1 modulo p et divise $\dfrac{n}{p^k}$; de plus, ils sont tous conjugués.

3 Anneaux

DÉFINITION **3.1** *On appelle anneau unitaire ou simplement anneau un ensemble A muni de deux lois de composition internes $+$ (addition) et $\times$ (produit ou multiplication) vérifiant :*
i)$(A,+)$ est un groupe commutatif ;
ii) la multiplication est associative ;
iii) la multiplication est distributive à droite et a gauche par rapport à l'addition ;
iv) la multiplication possède un élément neutre.

On appellera élément nul de A l'élément neutre de A pour l'addition, qu'on notera 0 ou 0_A et élément unité de A l'élément neutre pour la multiplication, qu'on notera 1 ou 1_A. Ils sont différents sauf si l'anneau A est reduit à un seul élément (anneau nul).

On dit qu'un anneau est *commutatif* si la multiplication est commutative.

On peut voir qu'on a pour tout élément x d'un anneau A, $x.0 = 0.x = 0$.

On dit qu'un anneau A est *intègre* si pour tous x et y non nuls de A, on a $xy \neq 0$ (l'anneau nul étant parfois considéré comme intègre, parfois non suivant les auteurs).

Un élément a est dit *diviseur de zéro* à gauche (resp. à droite) s'il existe b non nul tel que $ab = 0$ (resp. $ba = 0$). Un élément qui ne l'est pas est simplifiable (à gauche ou à droite). Un anneau intègre est ainsi un anneau sans autre diviseur de zéro que son élément nul.

Un élément a est dit *inversible* à gauche (resp. à droite) s'il existe b tel que $ab = 1$ (resp. $ba = 1$). Il est dit *inversible* s'il l'est des deux côtés et, dans ce cas, ses inverses à droite et à gauche sont uniques et coïncident.

Un anneau autre que l'anneau nul dont tous les éléments nul nuls sont inversibles s'appelle un *corps*. Un corps est un anneau intègre car un élément inversible ne peut pas être diviseur de zéro.

Pour tout anneau A, l'ensemble des éléments inversibles muni de la multiplication forme un groupe, qu'on appelle le groupe des unités de A, noté $A^\times$, dont lélément neutre est 1_A. Par exemple, $\mathbb{Z}^\times = \{-1; 1\}$.

On appelle sous-anneau de A un sous-ensemble de A qui est un sous-groupe de A pour l'addition, qui est stable par multiplication et qui contient l'élément unité de A. Si B est un sous-anneau de A, alors $(B, +, \times)$ est un anneau et a les mêmes éléments nul et unité que A. Si B est un sous-anneau de A et que A et B sont des corps, alors B s'appelle un sous-corps de A.

Exemple : $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$, qui lui-même est un sous-corps de $\mathbb{R}$.

3.1 Idéaux et morphismes

Soient A et B deux anneaux. On appelle *(homo)morphisme d'anneaux* de A dans B une application ϕ telle que pour tous x et y de A, on ait :

$$\begin{cases} \phi(x+y) = \phi(x) + \phi(y) \\ \phi(x \times y) = \phi(x) \times \phi(y) \\ \phi(1_A) = 1_B \end{cases}$$

Un morphisme d'anneaux bijectif s'appelle un *isomorphisme* d'anneaux.

Soit A un anneau. On appelle *idéal* à gauche (resp. à droite) de A une partie I de A qui est un sous-groupe pour l'addition et telle que pour tous a dans A et i dans I, on a $a.i \in I$ (resp. $i.a \in I$). On appelle idéal bilatère, ou simplement idéal une partie de A qui est à la fois un idéal à droite et un idéal à gauche.

Soit $\phi : A \mapsto B$ un morphisme d'anneaux, I un idéal de B (à droite, à gauche, bilatère). Alors, $\phi^{-1}(B)$ est un idéal de A. L'image $Im\phi$ de A par ϕ est un sous-anneau de B et, sous l'hypothèse que ϕ est surjectif, l'image par ϕ d'un idéal (à droite, à gauche, bilatère) de A est un idéal (à droite, à gauche, bilatère) de B.

PROPOSITION **3.1** *Soient A et B deux anneaux, ϕ un morphisme de A dans B. Alors le noyau de ϕ est un idéal bilatère de A. Réciproquement, si A est un anneau et I un idéal bilatère de A, alors le groupe quotient A/I est naturellement muni d'une structure d'anneau et la projection canonique de A sur A/I est un morphisme d'anneaux de noyau I.*

PROPOSITION **3.2** *Soit $\phi : A \mapsto B$ un morphisme d'anneaux. On a alors la décomposition suivante, dite décomposition canonique de ϕ, analogue à celle des morphismes de groupes (c'est d'ailleurs la même que la decomposition canonique de ϕ en tant que morphismes de groupes de A dans B) :*

$$A \mapsto A/Ker\phi \mapsto Im\phi \hookrightarrow B$$

On peut remarquer que l'intersection d'une famille d'idéaux (à droite, à gauche ou bilatères) d'un anneau A est encore un idéal de A (de même type). Ainsi, si on se donne une partie X de A, l'intersection des idéaux (à droite, à gauche ou bilatères) de A contenant X s'appelle l'idéal (à droite, à gauche ou bilatère) de A engendré par X.

Dans toute la suite, nous ne considérerons plus que des anneaux commutatifs.

Donnons-nous deux idéaux I et J d'un anneau A. Leur *somme* $I + J = \{i + j, i \in I, j \in J\}$ est un idéal de A, et c'est l'idéal engendré par leur réunion. D'autre part, on appelle *produit* de I par J, noté IJ, l'idéal de A engendré par les produits ij où i est dans I et j dans J. En fait, c'est aussi le sous-groupe engendré par cette même partie et c'est aussi l'ensemble des éléments de A qui s'écrivent comme somme finie $i_1j_1 + i_2j_2 + ... + i_kj_k$ où les i_n sont dans I et les j_n sont dans J. On remarque que le produit de deux idéaux est nécessairement contenu dans leur intersection.

On dit que deux idéaux I et J d'un anneau A sont *étrangers* ou *comaximaux* si leur somme est égale à tout l'anneau. Dans ce cas, on peut voir que le produit IJ est égal à $I \cap J$ et on a :

THÉORÈME **3.3 Théorème chinois** *: Soient I et J deux idéaux étrangers d'un anneau A. Alors, A/IJ est isomorphe à $A/I \times A/J$.*

Réciproquement, si on prend un anneau A et que le morphisme canonique de A/IJ dans $A/I \times A/J$ est un isomorphisme, alors I et J sont étrangers.

3.2 L'anneau $\mathbb{Z}$. Caractéristique d'un anneau

On sait que $(\mathbb{Z}, +, \times)$ est un anneau commutatif. Ses idéaux sont des sous-groupes, donc de la forme $n\mathbb{Z}$. Réciproquement, l'ensemble des multiples

d'un entier n est un idéal de $\mathbb{Z}$.

L'anneau quotient de $\mathbb{Z}$ par son sous-groupe $n\mathbb{Z}$ est l'anneau $\mathbb{Z}/n\mathbb{Z}$, muni de la somme et du produit que nous avons déja vus.

Une classe $\bar{m}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si m et n sont premiers entre eux, ce qui entraîne que $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier.

Si on se donne un anneau A quelconque, il y a un unique morphisme de $\mathbb{Z}$ dans A et il est donné par $m \to m.1_A$. Le noyau de ce morphisme est un idéal de $\mathbb{Z}$, donc de la forme $n\mathbb{Z}$ pour un certain entier positif n ($n = 0$ si ce morphisme est injectif). On dit que n est la *caractéristique* de l'anneau A. On a $n.a = 0_A$ pour tout a dans A.

Par exemple, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est de caractéristique n.

Tout anneau intègre, et en particulier tout corps, a pour caractéristique 0 ou un nombre premier.

3.3 Anneaux factoriels, principaux, euclidiens

Un idéal I d'un anneau A distinct de A est dit *premier* si pour tous x et y de A pour lesquels $xy \in I$ on a alors forcément soit x soit y dans I (ou par contraposée si le produit de deux éléments hors de I n'y est pas non plus). Cela équivaut à demander que le quotient A/I soit un anneau intègre.

Un idéal I d'un anneau A distinct de A est dit *maximal* s'il n'est inclus dans aucun idéal de A autre que A et lui-même. Cela équivaut à demander que le quotient A/I soit un corps.

On a le théorème suivant :

THÉORÈME **3.4** *Tout idéal d'un anneau A distinct de A est inclus dans un idéal maximal de A.*

On suppose désormais que l'anneau A est intègre (et toujours commutatif).

On dit qu'un élément x de A est *irréductible* s'il n'est pas inversible mais que quels que soient les éléments u et v de A tels que $uv = x$, alors soit u soit v est inversible.

3.3.1 Anneaux factoriels

DÉFINITION **3.2** *On dit qu'un anneau A est factoriel s'il vérifie les deux conditions suivantes :*
i) Tout élément non nul x de A s'écrit sous la forme

$$x = \epsilon p_1 p_2 ... p_k$$

où ϵ est inversible et chaque p_i irréductible ;
ii) si un élément x s'écrit sous la forme ci-dessus de deux manières

$$x = \epsilon p_1 p_2 ... p_k = \epsilon' q_1 ... q_{k'}$$

alors $k' = k$ et on a une bijection f de $\{1; ...k\}$ dans lui-même pour laquelle on a pour chaque i, $p_i = \epsilon_i q_{f(i)}$, ϵ_i étant inversible (cette dernière condition étant d'ailleurs automatique).

Ainsi, dans un anneau factoriel, tout élément non nul se décompose de manière "essentiellement unique" en produit de facteurs irréductibles.

Prenons deux éléments x et y d'un anneau factoriel A. On dit qu'un élément z est un *pgcd* de x et y s'il divise x et y et que tout élément z' de A qui divise x et y divise aussi z. On peut voir qu'un pgcd de x et y est défini "à un inversible près", c'est-à-dire que si z est un pgcd de x et y, alors tout élément de la forme ϵz, avec ϵ inversible l'est aussi et que réciproquement, tout pgcd de x et y s'écrit sous la forme ci-dessus.

PROPOSITION **3.5** *Deux éléments quelconques d'un anneau factoriel possèdent un pgcd.*

Reprenons deux éléments x et y d'un anneau factoriel A. On dit qu'un élément z est un *ppcm* de x et y si x et y le divisent et que tout élément z' de A qui est à la fois multiple de x et de y est aussi multiple de z. On peut voir que, tout comme un pgcd, un ppcm de x et y est défini "à un inversible près".

PROPOSITION **3.6** *Deux éléments quelconques d'un anneau factoriel possèdent un ppcm.*

Il est clair qu'un pgcd de 0 avec un élément x quelconque est x ; aussi, un ppcm de 0 avec un élément x quelconque est 0. Pour les autres, on peut procéder comme suit : pour chaque classe α d'éléments irréducitibles modulo multiplication par un inversible, on prend un représentant x_α. Alors, chaque élément non nul x de A s'écrit de manière unique sous la forme

$$x = \epsilon \prod_\alpha x_\alpha^{n_\alpha}$$

où ϵ est un inversible et les n_α sont des entiers naturels pour lesquels seul un nombre fini n'est pas nul (ces derniers correspondant aux irréductibles qui divisent effectivement x, les autres n'apparaissant pas réellement dans le produit).

EXEMPLE **3.3.1** *Si on se place dans $\mathbb{Z}$, on peut prendre pour x_α les nombres premiers positifs. Tout entier relatif non nul s'écrit alors sous la forme $\pm p_1^{n_1}...p_k^{n_k}$.*

Si on prend deux éléments non nuls x et y de A, avec $x = \epsilon \prod_\alpha x_\alpha^{n_\alpha}$ et $y = \epsilon' \prod_\alpha x_\alpha^{n'_\alpha}$, alors comme pgcd de x et y, on peut prendre $\prod_\alpha x_\alpha^{\min(n'_\alpha, n'_\alpha)}$, qu'on peut alors appeler "le" pgcd de x et y (bien que ce soit relativement au système choisi). De même, comme ppcm de x et y, on peut prendre $\prod_\alpha x_\alpha^{\max(n'_\alpha, n'_\alpha)}$, qu'on appelle aussi "le" ppcm de x et y.

Par exemple dans $\mathbb{Z}$, avec le système ci-dessus, le pgcd et le ppcm de deux entiers sont toujours positifs ; par exemple le pgcd de -12 et 8 est 4, bien que -4 en soit aussi un pgcd.

Lorsque deux éléments x et y de A ont 1 pour pgcd, on dit qu'ils sont *premiers entre eux*. Si on se donne deux éléments non nuls x et y de A, alors $\frac{x}{pgcd(x,y)}$ et $\frac{y}{pgcd(x,y)}$ sont deux éléments premiers entre eux.

On a le lemme de Gauß :

PROPOSITION **3.7** *Soient x, y et z trois éléments d'un anneau factoriel tels que x divise yz et que x et y soient premiers entre eux. Alors x divise z.*

3.3.2 Anneaux principaux

Un idéal I d'un anneau A est dit *principal* s'il est engendré par un seul élément. Dans ce cas, si u est un tel générateur, on a $I = \{ux, x \in A\}$.

DÉFINITION **3.3** *Un anneau (commutatif et intègre) A est dit principal si tous ses idéaux sont principaux.*

Nous avons l'important théorème suivant :

THÉORÈME **3.8** *Tout anneau principal est un anneau factoriel.*

Pour un élément non nul x d'un anneau principal, il y a équivalence entre :
i) L'élément x est irréductible ;
ii) l'idéal xA est premier ;
iii)l'idéal xA est maximal.

On en déduit l'importante identité de Bezout : Soient x et y deux éléments d'un anneau principal, d leur pgcd. Alors il existe deux éléments u et v de A tels que $ux + vy = d$. En particulier, si x et y sont premiers entre eux, il existe u et v tels que $ux + vy = 1$.

3.3.3 Anneaux euclidiens

DÉFINITION **3.4** *Un anneau (commutatif et intègre) A est dit euclidien s'il existe une application (non unique) de $A\backslash\{0\}$ dans $\mathbb{N}$ telle que :*
i) Si b divise a non nul, alors $N(b) \leq N(a)$.
ii) Pour tout $b \neq 0$ et tout a, il existe q et r dans A tels que $a = qb + r$ et soit $r = 0$, soit $N(r) < N(b)$.

Une application N satisfaisant les propriétés de la définition ci-dessus est appelée *norme* ou *stathme* ou même *algorithme* de l'anneau euclidien A.

EXEMPLE **3.3.2** *L'anneau $\mathbb{Z}$ est un anneau euclidien lorsqu'on le munit de $N(n) = |n|$ pour $n \neq 0$.*

Si $\mathbb{K}$ est un corps, l'anneau $\mathbb{K}[X]$ des polynômes à une indéterminée sur $\mathbb{K}$ est un anneau euclidien, où on peut prendre pour norme la fonction degré.

THÉORÈME **3.9** *Tout anneau euclidien est un anneau principal (et a fortiori factoriel).*

De plus, dans un anneau euclidien, on peut appliquer l'algorithme d'Euclide (comme dans $\mathbb{Z}$) pour le calcul du pgcd et des coefficients d'une relation de Bezout entre deux éléments.

3.4 Corps des fractions d'un anneau intègre

Nous allons plonger canoniquement un anneau intègre dans un corps. Cette construction est calquée sur la construction des rationnels à partir des entiers.

Partons d'un anneau intègre A et considérerons l'ensemble $A \times (A \backslash \{0\})$, que nous noterons $\mathcal{F}$ et dont un élément (a, b) sera noté $\frac{a}{b}$ et appelé fraction. Sur $\mathcal{F}$, on pose la relation suivante :

$$\frac{a}{b} \mathcal{R} \frac{a'}{b'} \text{ si } (ab' = a'b)$$

Il s'agit d'une relation d'équivalence, et on note K l'ensemble des classes d'équivalence de cette relation.

Sur K, on définit une addition et une multiplication comme suit : Si un élément q_1 de K est représenté par la fraction $\frac{a_1}{b_1}$ et un élément q_2 par la fraction $\frac{a_2}{b_2}$, alors on pose $q_1 + q_2$ la classe de la fraction $\frac{a_1 b_2 + a_2 b_1}{b_1 b_2}$ et $q_1 q_2$ la classe de la fraction $\frac{a_1 a_2}{b_1 b_2}$. On vérifie que ces opérations sont bien définies, c'est-à-dire que $q_1 + q_2$ et $q_1 q_2$ ne dépendent pas des représentants choisis.

PROPOSITION **3.10** *Muni de ces deux opérations, l'ensemble K est un corps commutatif.*

L'élément nul de K est la classe de la fraction $\frac{0}{1}$ et l'élément unité est la classe de la fraction $\frac{1}{1}$. De plus, l'application i de A dans K qui à un élément

a associe (la classe de) $\frac{a}{1}$ est un morphisme injectif, ce qui permet d'identifier l'anneau A et l'image de i. Ainsi, A est un sous-anneau de K.

Enfin, si on prend a non nul, l'inverse de (la classe de) la fraction $\frac{a}{b}$ est (la classe de) la fraction $\frac{b}{a}$ et, si on prend (la classe de) la fraction $\frac{a}{b}$, c'est, dans K le quotient de a par b. Ainsi, tout élément de K peut être obtenu en divisant un élément de A par un autre.

EXEMPLE **3.4.1** *Si on part de l'anneau $A = \mathbb{Z}$, on obtient pour K le corps $\mathbb{Q}$ des nombres rationnels.*

Si on prend pour A l'anneau $\mathbb{K}[X]$ des polynômes à une indéterminée sur un corps $\mathbb{K}$, on obtient pour K le corps $\mathbb{K}(X)$ des fractions rationnelle à une indéterminée sur $\mathbb{K}$.

On suppose finalement que A est un anneau factoriel. Alors, tout élément de K peut être représenté par une fraction irréductible, i.e. une fraction où le numérateur et le dénominateur sont premiers entre eux. En effet, si $x \neq 0$ est représenté par la fraction $\frac{a}{b}$ -pour $x = 0$ la fraction $\frac{0}{1}$ convient-, alors si d est un pgcd de a et b, en posant $a' = a/d \in A$ et $b' = b/d \in A$, la fraction $\frac{a'}{b'}$ représente aussi x et est irréductible.

4 Polynômes

4.1 Définition

Soit A un anneau commutatif. Nous allons construire un anneau qui contient A.

On considère l'ensemble des suites $(a_0, a_1, ..., a_k, ...)$ d'éléments de A qui n'ont qu'un nombre fini de composantes non nulles (c'est-à-dire qu'il existe $k_0$tel que pour tout $k \geq k_0$ on a $a_k = 0$. Un élément $(a_0, a_1, ..., a_k, ...)$ sera noté $a_0 + a_1X + a_2X^2 + ... + a_kX^k + ...$ ou $\sum_{i\in\mathbb{N}} a_iX^i$.

REMARQUE **4.1** *Le polynôme* $(0, 1, 0, 0, ..., 0, ...)$ *est noté* X *et s'appelle l'indéterminée.*

Cet ensemble sera noté $A[X]$, et ses éléments seront appellés *polynômes* (à une indéterminée et à coefficients dans A). Si le polynôme P est $\sum_{i\in\mathbb{N}} a_iX^i$, alors a_k s'appellera le *coefficients de degré* k de P. Un polynôme ayant un seul coefficient non nul s'appellera un monôme.

Nous définissons une addition et une multiplication sur $A[X]$ comme suit :

Prenons $P = \sum_{i\in\mathbb{N}} a_iX^i$ et $Q = \sum_{i\in\mathbb{N}} b_iX^i$. Alors $P + Q$ sera $\sum_{i\in\mathbb{N}}(a_i + b_i)X^i$ (ce qui n'est autre que l'addition habituelles sur les suites d'éléments de A).

Pour le produit, prenons un entier naturel k. Alors le coefficient de degré k de PQ sera $a_0b_k + a_1b_{k-1} + ... + a_kb_0 = \sum_{i=0}^{k} a_ib_{k-i}$. En fait, on peut écrire le produit PQ comme si on développait formellement un produit :

$$\left(\sum_{i\in\mathbb{N}} a_iX^i\right)\left(\sum_{j\in\mathbb{N}} b_jX^j\right) = \sum_{i,j\in\mathbb{N}} a_ib_jX^{i+j}$$

Ceci justifie la notation employée pour les polynômes.

Muni de ces deux lois, $A[X]$ est un anneau commutatif. De plus, l'application $a \to (a, 0, ..., 0, ...)$ de A dans $A[X]$ est un morphisme d'anneau injectif, ce qui permet d'identifier A à son image dans $A[X]$ par ce morphisme, et ceci

justifie aussi la notation employée. Un polynôme qui est dans A sera dit *constant*.

REMARQUE **4.2** *Si $a \in A$ est un polynôme constant, alors chaque coefficient de aP est le produit par a du coefficient de même degré de P.*

4.1.1 Degré et valuation

Soit $P = \sum_{i \in \mathbb{N}} a_i X^i$ un polynôme non nul. Alors, le plus grand entier d pour lequel a_d n'est pas nul s'appelle le degré de P. On remarque qu'un polynôme non nul est constant si et seulement si son degré est nul.

Suivant les conventions, le polynôme nul n'a pas de degré ou a pour degré $-\infty$.

Si A est un anneau intègre, l'anneau $A[X]$ est aussi intègre et, si on prend deux polynômes non nuls, P de degré d et Q de degré d', alors PQ a pour degré $d + d'$. Si A n'est pas intègre et $PQ \neq 0$, on a l'inégalité $deg(PQ) \leq d + d'$. Ceci a pour conséquence que si A est intègre, les seuls polynômes inversibles de $A[X]$ sont les polynômes constants, inversibles dans A.

De plus, si P et Q sont non nuls et non opposés, on a $deg(P + Q) \leq \max(deg(P), \deg(Q))$.

Soit $P = \sum_{i \in \mathbb{N}} a_i X^i$ un polynôme non nul. Alors, le plus petit entier d pour lequel a_d n'est pas nul s'appelle la valuation de P. Suivant les conventions, le polynôme nul n'a pas de valuation ou a $+\infty$ pour valuation.

Si A est intègre et P, Q non nuls, P de valuation v_P et Q de valuation v_Q, alors PQ a pour valuation $v_P + v_Q$. Si A n'est pas intègre et $PQ \neq 0$, on a l'inégalité $val(PQ) \geq v_P + v_Q$.

De plus, si P et Q sont non nuls et non opposés, on a $val(P + Q) \geq \min(deg(P), \deg(Q))$.

DÉFINITION **4.1** *Soit $P = \sum_{i=0}^{d} a_i X^i$ un polynôme de degré d. On appelle*

terme dominant de P le monôme a_dX^d, coefficient dominant le coefficient a_d, terme constant le coefficient a_0.

Un polynôme est dit unitaire si son coefficient dominant vaut 1.

4.1.2 Fonctions polynomiales. Composition

Soit $P = \sum_{i\in\mathbb{N}} a_iX^i$ un polynôme à coefficients dans un anneau A. Alors pour tout élément b de A, on peut considérer l'élément $P(b) = \sum_{i\in\mathbb{N}} a_ib^i$ qui est aussi un élément de A. La fonction $b \to P(b)$ de A dans lui-même s'appelle la fonction polynomiale associée au polynôme P de $A[X]$.

REMARQUE **4.3** *Deux éléments distincts de $A[X]$ peuvent donner la même fonction polynomiale ; par exemple, si A est fini et non nul, il y a une infinité de polynômes à coefficients dans A est un nombre fini de fonctions de A dans A. Il est alors forcé que certains polynômes différents donnent la même fonction. Toutefois, si l'anneau A est intègre et infini, alors la fonction polynomiale caractérise le polynôme.*

On peut faire la même chose que ci-dessus avec un anneau B qui contient A. Dans ce cas, en reprenant le même polynôme P, on peut le considérer à coefficients dans B et définir naturellement $P(b)$.

En particulier, si $B = A[X]$ et qu'on prend un polynôme Q, le polynôme $P(Q)$ sera souvent noté $P\circ Q$ et appelé le composé de Q par P. En particulier, cette dénomination est cohérente avec celle des fonctions, c'est-à-dire que la fonction polynomiale associée à $P \circ Q$ est la composée de la fonction polynomiale associée à Q par celle associée à P.

4.1.3 Dérivation

Soit $P = \sum_i a_iX^i$. On appelle polynôme *dérivé* de P, noté P' le polynôme $\sum_{i\geq 1} ia_iX^{i-1}$. On remarque que si $A = \mathbb{R}$, la dérivée de la fonction polynômiale associée à P est celle associée à P'.

Par dérivations successives, on définit P'', P''', ..., P^k, ... On a, pour P non nul, $P' = 0$ ou $deg(P') < deg(P)$. En particulier, si $k > deg(P)$, $P^{(k)} = 0$.

D'autre part, si A est intègre et de caractéristique nulle, alors pour tout P non constant, on a $deg(P') = deg(P) - 1$.

4.2 Propriétés arithmétiques des polynômes à coefficients dans un corps

Nous nous plaçons ici dans $\mathbb{K}[X]$ où $\mathbb{K}$ est un corps. Nous avons alors une division euclidienne dans $\mathbb{K}[X]$:

PROPOSITION **4.4** *Soient A et B deux polynômes de $\mathbb{K}[X]$, $B \neq 0$. Alors, il existe deux polynômes Q et R, uniques, tels que $A = QB + R$ et soit $R = 0$, soit $deg(R) < deg(B)$.*

REMARQUE **4.5** *Si A est un anneau commutatif quelconque, alors le même résultat est vrai lorsque B est un polynôme unitaire.*

Ce résultat implique immédiatement que l'application degré est un stathme euclidien pour l'anneau $\mathbb{K}[X]$. On en déduit donc que l'anneau $\mathbb{K}[X]$ est principal et donc factoriel.

De plus, l'algorithme d'Euclide est valide pour chercher le pgcd de deux polynômes et une identité de Bezout.

4.3 Polynôme à plusieurs indéterminées

Pour A anneau commutatif et $n \geq 2$ entier naturel, on définit l'anneau $A[X_1, ..., X_n]$ des polynômes à n indéterminées à coefficients dans A comme $A[X_1, ..., X_{n-1}][X_n]$. Tout tel polynôme sécrit sous forme :

$$P = \sum_{i_1,...,i_n=0}^{\infty} a_{i_1,...,i_n} X_1^{i_1} ... X_n^{i_n}$$

où seul un nombre fini de coefficients $a_{i_1,...,i_n}$ n'est pas nul.

En fait, l'ordre des indéterminées n'a pas d'importance et pour tout i, le polynôme P peut être vu comme polynôme en X_i à coefficients dans $A[X_1, ..., X_{i-1}, X_{i+1}, ..., X_n]$.

On appelle monôme un polynôme non nul de la forme $a_{i_1,...,i_n} X_1^{i_1} ... X_n^{i_n}$. Pour chaque k, le degré en X_k de ce monôme est i_k, tandis que son degré (total) est $i_1 + ... + i_k$.

Le degré en X_i (resp. total) d'un polynôme est le plus grand des degrés en X_i (resp. totaux) des monômes qui le constituent. On remarque que le degré total d'un polynôme est majoré par, mais pas forcément égal à, la somme de ses degrés en les différentes indéterminées.

On dit qu'un polynôme est homogène de degré d si tous les monômes qui le constituent ont un degré (total) égal à d.

4.3.1 Polynômes symétriques

Un polynôme $P \in \mathbb{K}[X_1, ..., X_n]$ est dit *symétrique* si pour toute permutation σ de $\{1, ..., n\}$, le polynôme $P(X_{\sigma(1)}, ..., X_{\sigma(n)})$ est égal à P.

On appelle polynômes symétriques élémentaires les polynômes donnés, pour $1 \leq k \leq n$ par

$$\Sigma_k = \sum_{1 \leq i_1 < i_2 < ... < i_k \leq n} X_{i_1} ... X_{i_k}$$

Ce sont bien des polynômes symétriques.

EXEMPLE **4.3.1** *Le polynôme Σ_1 est la somme des X_i, le polynôme Σ_n est leur produit. Pour $n = 3, k = 2$:*

$$\Sigma_2(X_1, X_2, X_3) = X_1X_2 + X_1X_3 + X_2X_3$$

THÉORÈME **4.6** *Tout polynôme symétrique est, de manière unique, un polynôme en les polynômes symétriques élémentaires.*