Université Blaise Pascal
U.F.R. Sciences et Technologies
Département de Mathématiques et Informatique

Licence de Mathématiques

Troisième année, U.E. 35MATF2

ALGEBRE: GROUPES ET ANNEAUX 1

Polycopié du cours

2007-2008

François Dumas

Licence de Mathématiques, 3ème année
U.E. 35MATF2

Cours d'algèbre : groupes et anneaux 1

François DUMAS

Chapitre 1. – Groupes : les premières notions

Chapitre 2. – Groupes : groupes quotients

Chapitre 1

Groupes : les premières notions

1. Groupes et sous-groupes

1.1 Notion de groupe

1.1.1 Définition. Soit G un ensemble non-vide. On appelle *loi de composition interne* dans G, ou *opération interne* dans G, toute application $\star : G \times G \to G$.

Une telle loi de composition interne permet donc d'associer à tout couple (x, y) d'éléments de G un autre élément de G, noté $x \star y$, et appelé le produit de x par y pour la loi $\star$.

1.1.2 Définition. On appelle *groupe* tout ensemble non-vide G muni d'une loi de composition interne $\star$, vérifiant les 3 propriétés suivantes (appelées axiomes de la structure de groupe):

(A1) la loi $*$ est associative dans G ;
rappelons que cela signifie que $x * (y * z) = (x * y) * z$ pour tous $x, y, z \in G$.

(A2) la loi $*$ admet un élément neutre dans G ;
rappelons que cela signifie qu'il existe $e \in G$ tel que $x * e = e * x = x$ pour tout $x \in G$.

(A3) tout élément de G admet un symétrique dans G pour la loi $*$;
rappelons que cela signifie que, pour tout $x \in G$, il existe $x' \in G$ tel que $x * x' = x' * x = e$.

1.1.3 Définition. On appelle *groupe commutatif*, ou *groupe abélien*, tout groupe G dont la loi $\star$ vérifie de plus la condition supplémentaire de commutativité: $x * y = y * x$ pour tous $x, y \in G$.

1.1.4 Exemples.

(a) Pour tout ensemble X, l'ensemble $\mathcal{S}(X)$ des bijections de X sur X muni de la loi $\circ$ de composition des bijections est un groupe, appelé groupe symétrique sur X.

Le neutre en est l'identité de X, car $f \circ \mathrm{id}_X = \mathrm{id}_X \circ f = f$ pour toute $f \in \mathcal{S}(X)$. Pour toute $f \in \mathcal{S}(X)$, le symétrique de f pour la loi $\circ$ est la bijection réciproque f^{-1}, car $f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}_X$. Dès lors que X contient au moins trois éléments, le groupe $\mathcal{S}(X)$ n'est pas abélien (montrez-le).

(b) Pour tout entier $n \geq 1$, l'ensemble $\mathrm{GL_n}(\mathbb{R})$ des matrices carrées d'ordre n inversibles à coefficients réels est un groupe pour la multiplication des matrices.

Le neutre en est la matrice identité I_n, car $M \times I_n = I_n \times M = M$ pour toute $M \in \mathrm{GL_n}(\mathbb{R})$. Pour toute $M \in \mathrm{GL_n}(\mathbb{R})$, le symétrique de M pour la loi $\times$ est la matrice inverse M^{-1}, car $M \times M^{-1} = M^{-1} \times M = I_n$. Dès lors que $n \geq 2$, le groupe $\mathrm{GL_n}(\mathbb{R})$ n'est pas abélien (montrez-le).

(c) L'ensemble $\mathbb{C}$ des nombres complexes muni de l'addition est un groupe abélien.

Le neutre en est le nombre complexe nul 0, car $z + 0 = 0 + z = z$ pour tout $z \in \mathbb{C}$. Pour tout $z \in \mathbb{C}$, le symétrique de z pour l'addition est son opposé $-z$, car $z + (-z) = (-z) + z = 0$.

(d) L'ensemble $\mathbb{C}^*$ des nombres complexes non-nuls muni de la multiplication est un groupe abélien.

Le neutre en est le nombre complexe 1, car $z.1 = 1.z = z$ pour tout $z \in \mathbb{C}^*$. Pour tout $z \in \mathbb{C}^*$, le symétrique de z pour la multiplication est son inverse z^{-1}, car $z.z^{-1} = z^{-1}.z = 1$.

1.1.5 Remarques et conventions de notation. Afin d'éviter la lourdeur de la notation $*$, on convient généralement de noter la loi de composition interne d'un groupe quelconque G, soit comme une multiplication (par un point .), soit comme une addition (par un $+$). Dans le premier cas, le symétrique d'un élément est appelé son inverse, dans le second cas, son opposé. Usuellement, on réserve la notation additive au cas des groupes abéliens. C'est pourquoi, dans toute la suite de ce polycopié, on adoptera pour les groupes quelconques, conformément à l'usage courant, la notation multiplicative.

(a) Un groupe G sera donc un ensemble non-vide G muni d'une loi de composition interne .
 $\rightarrow$ associative ($x.(y.z) = (x.y).z$ pour tous $x, y, z \in G$),
 $\rightarrow$ admettant un élément neutre e ($x.e = e.x = x$ pour tout $x \in G$),
 $\rightarrow$ et telle que tout élément $x \in G$ admette un symétrique x^{-1} pour la loi . ($x.x^{-1} = x^{-1}.x = e$).

(b) De plus, l'éventuelle commutativité de G se traduira par: $x.y = y.x$ pour tous $x, y \in G$.

(c) On utilisera la notation $x^n = x.x.x \cdots x$ (n facteurs) pour tous $x \in G$ et $n \in \mathbb{N}^*$, ainsi que les conventions $x^0 = e$, et $x^{-n} = (x^n)^{-1}$.

(d) Pour tous $x, y \in G$, on a $(x.y)^{-1} = y^{-1}.x^{-1}$ (montrez-le, attention à l'ordre !)

1.1.6 *Quelques remarques techniques, mais parfois utiles, sur les axiomes de la structure de groupe.*

(a) Dans un groupe G, l'élément neutre e est nécessairement unique, et le symétrique d'un élément quelconque est nécessairement unique.

(b) Si G est un ensemble non-vide muni d'une loi de composition interne . qui est supposée associative, il suffit que G admette un élément neutre e à droite (ce qui signifie que $x.e = x$ pour tout $x \in G$) et que tout élément $x \in G$ admette un symétrique $x' \in G$ à droite (ce qui signifie que $x.x' = e$) pour conclure que G est un groupe.

1.2 Sous-groupe

1.2.1 Exemple introductif. Considérons le groupe $\mathbb{C}^*$ pour la multiplication. Dans $\mathbb{C}^*$, considérons le sous-ensemble $\mathbb{R}^*$. En restreignant à $\mathbb{R}^*$ la multiplication dans $\mathbb{C}^*$, on obtient une loi de composition interne dans $\mathbb{R}^*$ (car le produit de deux réels non-nuls est encore un réel non-nul). La question de savoir si $\mathbb{R}^*$ est lui-même un groupe pour la loi . est donc fondée.

L'associativité de . dans $\mathbb{R}^*$ est évidemment vérifiée (la relation $x.(y.z) = (x.y).z$ étant vraie pour tous $x, y, z \in \mathbb{C}^*$, elle est a fortiori vraie pour tous $x, y, z \in \mathbb{R}^*$).

Le nombre complexe 1 est un élément de $\mathbb{R}^*$, et il est neutre pour la loi . dans $\mathbb{R}^*$ (la relation $x.1 = 1.x = x$ étant vraie pour tout $x \in \mathbb{C}^*$, elle est a fortiori vraie pour tout $x \in \mathbb{R}^*$).

Pour tout $x \in \mathbb{R}^*$, l'inverse x^{-1} de x dans $\mathbb{C}^*$ appartient à $\mathbb{R}^*$ et est donc l'inverse de x dans $\mathbb{R}^*$ (les égalités $x.x^{-1} = x^{-1}.x = 1$ étant alors vraies dans $\mathbb{R}^*$ comme dans $\mathbb{C}^*$).

On conclut que le sous-ensemble $\mathbb{R}^*$ est lui-même un groupe pour la multiplication déduite de celle de $\mathbb{C}^*$ par restriction. On dit alors que $\mathbb{R}^*$ est un sous-groupe de $\mathbb{C}^*$.

Le même raisonnement s'applique si on remplace $\mathbb{R}^*$ par $\mathbb{Q}^*$, mais pas si on le remplace par l'ensemble des nombres imaginaires purs (car le produit de deux imaginaires purs n'est pas un imaginaire pur), ou par l'ensemble $\mathbb{Z}^*$ (car l'inverse d'un entier non-nul peut ne pas être un entier).

1.2.2 Définition. Soit G un groupe muni d'une loi de composition interne . et soit H un sous-ensemble non-vide de G. On dit que H est un *sous-groupe* de G lorsque les deux conditions suivantes sont vérifiées:

(1) H est stable pour la loi . (ce qui signifie $x.y \in H$ pour tous $x, y \in H$),

(2) H est stable par passage à l'inverse (ce qui signifie $x^{-1} \in H$ pour tout $x \in H$).

Dans ce cas, la restriction à H de la loi . de G définit une loi de composition interne dans H, pour laquelle H est lui-même un groupe.

1.2.3 Exemples.

(a) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ sont des sous-groupes du groupe $\mathbb{C}$ muni de l'addition, mais pas $\mathbb{N}$ (car l'opposé d'un élément de $\mathbb{N}$ n'est pas nécessairement un élément de $\mathbb{N}$).

(b) L'ensemble $\mathbb{U}$ des nombres complexes de module égal à 1 est un sous-groupe de $\mathbb{C}^*$ muni de la multiplication. Pour tout entier $n \geq 1$, l'ensemble $\mathbb{U}_n$ des racines n-ièmes de l'unité est un sous-groupe de $\mathbb{U}$.

(c) Pour tout $n \geq 2$, l'ensemble des matrices triangulaires supérieures d'ordre n à coefficients réels sans 0 sur la diagonale est un sous-groupe non-abélien de $\mathrm{GL}_n(\mathbb{R})$. L'ensemble des matrices diagonales d'ordre n à coefficients réels sans 0 sur la diagonale en est un sous-groupe abélien.

1.2.4 Remarques.

(a) Les deux conditions de la définition 1.2.2 peuvent être synthétisées en une seule: soit H un sous-ensemble non-vide d'un groupe G, alors

(H est un sous-groupe de G) si et seulement si (pour tous $x, y \in H$, on a $x.y^{-1} \in H$).

(b) Si H est un sous-groupe de G, alors l'élément neutre e de G appartient nécessairement à H (car pour tout $x \in H$, on a $x^{-1} \in H$, et $x.x^{-1} = e \in H$). A contrario, un sous-ensemble de G qui ne contient pas le neutre de G ne peut en aucun cas être un sous-groupe (ce qui est dans la pratique une façon pratique très fréquente de vérifier qu'un sous-ensemble d'un groupe connu n'est pas un sous-groupe).

(c) Tout sous-groupe d'un groupe abélien est lui-même abélien, mais un groupe non abélien peut contenir des sous-groupes abéliens aussi bien que des sous-groupes non-abéliens (voir 1.2.3.c).

(d) Dans la pratique, dans la plupart des cas, pour montrer qu'un ensemble donné est un groupe, on ne revient pas à la définition par les trois axiomes, mais on cherche à montrer qu'il est un sous-groupe d'un groupe déjà connu.

(e) Attention, pour vérifier qu'un sous-ensemble donné d'un groupe est un sous-groupe, on n'oubliera pas de vérifier au préalable qu'il est non-vide; d'après la remarque (b) ci-dessus, le plus naturel pour cela est de s'assurer qu'il contient le neutre.

(f) Tout groupe G contient toujours au moins pour sous-groupes le sous-groupe trivial $\{e\}$ formé du seul élément neutre, et le groupe G lui-même.

1.2.5 Exemples.

(a) Soit E un espace vectoriel. L'ensemble $\mathrm{GL}(E)$ des automorphismes d'espace vectoriel de E est un groupe appelé groupe linéaire de E; pour le montrer, il suffit de vérifier que c'est un sous-groupe de $\mathcal{S}(E)$. Les éléments de $\mathrm{GL}(E)$ qui ont un déterminant égal à 1 forment un sous-groupe de $\mathrm{GL}(E)$, noté $\mathrm{SL}(E)$.

(b) Supposons de plus que E est euclidien. L'ensemble $\mathrm{O}(E)$ des isométries vectorielles de E est un groupe appelé groupe orthogonal de E; pour le montrer, il suffit de vérifier que c'est un sous-groupe de $\mathrm{GL}(E)$. L'ensemble $\mathrm{SO}(E)$ des isométries vectorielles positives de E est un sous-groupe de $\mathrm{O}(E)$, et l'on a $\mathrm{SO}(E) = \mathrm{O}(E) \cap \mathrm{SL}(E)$. L'ensemble des isométries vectorielles négatives de E n'est pas un sous-groupe de $\mathrm{O}(E)$ (il ne contient pas le neutre id_E).

(c) L'ensemble des bijections continues et strictement croissantes de $\mathbb{R}$ dans $\mathbb{R}$ est un groupe pour la loi $\circ$; pour le montrer, il suffit de vérifier que c'est un sous-groupe du groupe $\mathcal{S}(\mathbb{R})$ de toutes les bijections de $\mathbb{R}$ sur $\mathbb{R}$.

1.2.6 Proposition. *L'intersection de deux sous-groupes d'un groupe G est un sous-groupe de G. Plus généralement, l'intersection d'une famille quelconque de sous-groupes d'un groupe G est un sous-groupe de G.*

Preuve. Il suffit pour le montrer de prouver le second point. Soit donc $(H_i)_{i\in I}$ une famille de sous-groupes d'un groupe G. Posons $K = \bigcap_{i\in I} H_i$ l'intersection de tous les H_i. L'ensemble K est non-vide, car il contient le neutre e puisque celui-ci appartient à chacun des sous-groupes H_i. Soient x et y deux éléments de K. Pour tout $i \in I$, on a $x.y^{-1} \in H_i$ puisque H_i est un sous-groupe. Donc $x.y^{-1} \in K$. Ce qui prouve que K est un sous-groupe de G. □

1.2.7 Remarque. Attention, la réunion de deux sous-groupes n'est en général pas un sous-groupe.

Contre-exemple. Dans le groupe $\mathbb{C}^*$ muni de la multiplication, considérons le sous-groupe $\mathbb{U}_2 = \{1, -1\}$ des racines carrées de l'unité et le sous-groupe $\mathbb{U}_3 = \{1, j, j^2\}$ des racines cubiques de l'unité. Notons $K = \mathbb{U}_2 \cup \mathbb{U}_3 = \{1, -1, j, j^2\}$. On a $j \in K$ et $-1 \in K$, mais le produit $(-1).j = -j \notin K$. Donc K n'est pas stable par la multiplication, et ce n'est donc pas un sous-groupe de $\mathbb{C}^*$. □

1.3 Cas particulier des groupes finis

1.3.1 Définitions et notation. On appelle *groupe fini* un groupe G qui, en tant qu'ensemble, n'a qu'un nombre fini d'éléments. Ce nombre d'éléments (qui n'est autre que le cardinal de l'ensemble G) est appelé l'*ordre* du groupe G, noté $o(G)$ ou $|G|$.

1.3.2 Exemples.

(a) Soit n un entier strictement positif. Soit X un ensemble fini à n éléments. Le groupe $\mathcal{S}(X)$ des bijections de X sur X est alors un groupe fini d'ordre $n!$, que l'on appelle (indépendamment de l'ensemble X) le *groupe symétrique* sur n éléments, et que l'on note S_n.

(b) Soit n un entier strictement positif. Le sous-groupe $\mathbb{U}_n$ des racines n-ièmes de l'unité dans $\mathbb{C}^*$ est fini, d'ordre n. On peut expliciter $\mathbb{U}_n = \{1, \mathrm{e}^{2i\pi/n}, \mathrm{e}^{4i\pi/n}, \mathrm{e}^{6i\pi/n}, \ldots, \mathrm{e}^{2(n-1)i\pi/n}\}$

1.3.3 Théorème (dit théorème de Lagrange) *Soit H un sous-groupe d'un groupe fini G. Alors H est fini, et l'ordre de H divise l'ordre de G.*

Preuve. Notons $|G| = n$. Il est clair que H est fini. Notons $|H| = m$. Pour tout $x \in G$, notons $xH = \{xh\,;\, h \in H\}$ (ce sous-ensemble est appelé la classe de x à gauche modulo H).

D'une part, pour tout $x \in G$, l'ensemble xH est formé de m éléments.

En effet, si l'on note $H = \{h_1, h_2, \ldots, h_m\}$, alors xH est l'ensemble des éléments de la forme xh_i pour $1 \le i \le m$, et $xh_i \ne xh_j$ lorsque $i \ne j$ (car $xh_i = xh_j$ implique $x^{-1}xh_i = x^{-1}xh_j$ donc $h_i = h_j$ donc $i = j$).

D'autre part, l'ensemble des classes xH distinctes obtenues lorsque x décrit G est une partition de G.

En effet, tout $x \in G$ s'écrit $x = xe$ avec $e \in H$, donc $x \in xH$; ceci prouve que G est inclus dans la réunion des classes xH, et donc lui est égal puisque l'inclusion réciproque est triviale. Il reste à vérifier que deux classes xH et yH distinctes sont forcément disjointes. Pour cela, supposons qu'il existe $z \in xH \cap yH$, c'est-à-dire qu'il existe $h', h'' \in H$ tels que $z = xh' = yh''$. Tout élément xh de xH (avec $h \in H$) s'écrit alors $xh = (yh''h'^{-1})h = y(h''h'^{-1}h)$ avec $(h''h'^{-1}h) \in H$, et donc $xh \in yH$. On conclut que $xH \subseteq yH$. L'inclusion réciproque s'obtient de même et l'on déduit que $xH = yH$. On a ainsi prouvé que deux classes non disjointes sont égales, d'où le résultat voulu par contraposée.

On conclut que $n = mq$, où q désigne le nombre de classes xH distinctes obtenues lorsque x décrit G.□

1.3.4 Remarques. On peut représenter un groupe fini G d'ordre n par un tableau à n lignes et n colonnes portant dans la case d'intersection de la ligne indexé par un élément x de G et de la colonne indexé par un élément y de G la valeur du produit $x.y$. Il est facile de vérifier que tout élément de G apparaît une fois et une seule dans chaque ligne et chaque colonne de la table. Il est clair enfin qu'un groupe fini est abélien si et seulement si sa table est symétrique par rapport à la diagonale principale.

1.3.5 Exemples.

(a) Les tables des groupes $\mathbb{U}_2 = \{-1, 1\}$, $\mathbb{U}_3 = \{1, j, j^2\}$, $\mathbb{U}_4 = \{1, i, -1, -i\}$ sont:

	1	-1
1	1	-1
-1	-1	1

	1	j	j^2
1	1	j	j^2
j	j	j^2	1
j^2	j^2	1	j

	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

(b) Dans $\mathrm{GL}_2(\mathbb{R})$, notons:

$e = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), a = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right), b = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right), c = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right).$

Alors $G_1 = \{e, a, b, c\}$ est un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$ dont la table est:

G_1	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

(c) Dans $\mathrm{GL}_2(\mathbb{R})$, notons:

$e = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), a = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right), b = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right), c = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right).$

Alors $G_2 = \{e, a, b, c\}$ est un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$ dont la table est:

G_2	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

(d) Le groupe symétrique S_3 est d'ordre $3! = 6$. On peut décrire explicitement ses six éléments. On convient pour cela de noter chaque élément $\sigma \in S_3$ comme une matrice à 2 lignes et 3 colonnes, où la seconde ligne indique les images respectives par σ de trois éléments arbitraires désignés par les entiers 1,2,3 sur la première ligne. On a alors $S_3 = \{e, \gamma, \gamma^2, \tau_1, \tau_2, \tau_3\}$ avec:

$$e = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix}\right), \quad \gamma = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right), \quad \gamma^2 = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix}\right), \quad \tau_1 = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right), \quad \tau_2 = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix}\right), \quad \tau_3 = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right),$$

On peut alors dresser la table du groupe symétrique S_3.
On en déduit en particulier que le groupe S_3 n'est pas abélien.
On en tire aussi que le groupe S_3 admet trois sous-groupes d'ordre 2 qui sont $\{e, \tau_1\}$, $\{e, \tau_2\}$ et $\{e, \tau_3\}$, et un sous-groupe d'ordre 3 qui est $\{e, \gamma, \gamma^2\}$.
D'après le théorème de Lagrange, ce sont, avec le sous-groupe trivial $\{e\}$ et S_3 lui-même, ses seuls sous-groupes.

	e	γ	γ^2	τ_1	τ_2	τ_3
e	e	γ	γ^2	τ_1	τ_2	τ_3
γ	γ	γ^2	e	τ_3	τ_1	τ_2
γ^2	γ^2	e	γ	τ_2	τ_3	τ_1
τ_1	τ_1	τ_2	τ_3	e	γ	γ^2
τ_2	τ_2	τ_3	τ_1	γ^2	e	γ
τ_3	τ_3	τ_1	τ_2	γ	γ^2	e

2. Groupes monogènes, groupes cycliques

2.1 Sous-groupe engendré par un élément

2.1.1 Proposition et définition. *Soient G un groupe et X un sous-ensemble non-vide de G. L'intersection de tous les sous-groupes de G qui contiennent X est un sous-groupe de G, appelé le sous-groupe de G engendré par X, noté $\langle X\rangle$, et qui est le plus petit (pour l'inclusion) sous-groupe de G contenant X.*

Preuve. Résulte sans difficultés de la proposition 1.2.6. Les détails sont laissés au lecteur. □

2.1.2 Définition et proposition. *Soit G un groupe. Soit x un élément de G. On appelle sous-groupe monogène engendré par x dans G le sous-groupe engendré par le singleton $\{x\}$. On le note $\langle x\rangle$. C'est le plus petit sous-groupe de G contenant x, et l'on a:*

$$\langle x\rangle = \{x^m \,;\, m \in \mathbb{Z}\}.$$

Preuve. Le sous-groupe $\langle x\rangle$ contient x, donc (par stabilité pour la loi de G) il contient aussi $x.x = x^2$, $x^2.x = x^3$, et par récurrence x^m pour tout entier $m \geq 1$. Il contient aussi nécessairement le symétrique x^{-1} de x, donc aussi $x^{-1}.x^{-1} = x^{-2}$, et par récurrence x^{-m} pour tout entier $m \geq 1$. Enfin il contient le neutre $e = x.x^{-1}$ que l'on note par convention x^0. Ceci montre que $\langle x\rangle \supset \{x^m \,;\, m \in \mathbb{Z}\}$. Il est clair réciproquement que $\{x^m \,;\, m \in \mathbb{Z}\}$ est un sous-groupe de G contenant x. □

2.1.3 Remarque. Attention: l'énoncé précédent est formulé pour la notation multiplicative du groupe G. Dans le cas d'une loi notée comme une addition, il faut remplacer x^n par $nx = x + x + \cdots + x$ et x^{-1} par $-x$. Par exemple, dans le groupe $\mathbb{Z}$ muni de l'addition, $\langle x \rangle = \{mx\,;\, m \in \mathbb{Z}\}$.

2.1.4 Définition. Soit G un groupe. Soit x un élément de G. On dit que x est d'ordre fini dans G lorsqu'il existe des entiers $m \geq 1$ tel que $x^m = e$. Dans ce cas, on appelle ordre de x le plus petit d'entre eux. En d'autres termes:

$$(x \text{ est d'ordre } n \text{ dans } G) \Leftrightarrow (x^n = e \text{ et } x^m \neq e \text{ si } 1 \leq m < n).$$

Remarquons qu'alors le symétrique de x est $x^{-1} = x^{n-1}$.

2.1.5 Proposition. *Soit G un groupe. Soit x un élément de G. Si x est d'ordre fini $n \geq 1$ dans G, alors le sous-groupe $\langle x \rangle$ est fini d'ordre n, et l'on a:*

$$\langle x \rangle = \{e, x, x^2, x^3, \ldots, x^{n-1}\}.$$

Preuve. Soit x^m avec $m \in \mathbb{Z}$ un élément quelconque de $\langle x \rangle$. Par division euclidienne de m par n, il existe des entiers uniques q et r tels que $m = nq + r$ avec $0 \leq r \leq n-1$. On a $x^m = x^{nq+r} = (x^n)^q.x^r = e^q.x^r = x^r$, ce qui prouve que $\langle x \rangle$ est inclus dans l'ensemble $E := \{x^r\,;\, 0 \leq r \leq n-1\}$. La réciproque étant claire, on a $\langle x \rangle = E$. Il reste à vérifier que E est formé des n éléments distincts $e, x, x^2, x^3, \ldots, x^{n-1}$. Pour cela, supposons que $x^i = x^j$ avec $0 \leq i, j \leq n-1$; alors $x^{i-j} = e$ avec $-n < i - j < n$, ce qui, par minimalité de l'ordre n de x, implique $i - j = 0$ et donc $i = j$. On a donc bien $E = \{e, x, x^2, x^3, \ldots, x^{n-1}\}$, ce qui achève la preuve. □

2.1.6 Remarques.

(a) Il résulte de la proposition précédente et du théorème de Lagrange que, si le groupe G est fini, tout élément est d'ordre fini divisant $|G|$.

(b) Si x n'est pas d'ordre fini, le sous-groupe $\langle x \rangle$ n'est pas fini, ce qui ne peut se produire que si G est lui-même infini.

(c) Mais réciproquement, un groupe G infini peut contenir des sous-groupes du type $\langle x \rangle$ finis ou infinis. Par exemple, dans le groupe $\mathbb{C}^*$ pour la multiplication, le groupe $\langle i \rangle = \{1, i, -1, -i\}$ est fini et le groupe $\langle 5 \rangle = \{5^m\,;\, m \in \mathbb{Z}\}$ est infini.

2.2 Groupes monogènes, groupes cycliques.

2.2.1 Définitions. Un groupe G est dit *monogène* lorsqu'il est engendré par un de ses éléments, c'est-à-dire lorsqu'il existe un élément $x \in G$ tel que $G = \langle x \rangle$.

Si de plus x est d'ordre fini $n \geq 1$, alors on dit que le groupe G est *cyclique* d'ordre n, et l'on a d'après ce qui précède:

$$G = \{e, x, x^2, x^3, \ldots, x^{n-1}\}.$$

Sinon, $x^i \neq x^j$ pour tous $i \neq j$ dans $\mathbb{Z}$, et $G = \{x^m\,;\, m \in \mathbb{Z}\}$ est monogène infini.
Il est clair qu'un groupe monogène (en particulier un groupe cyclique) est toujours abélien.

2.2.2 Proposition (Sous-groupe d'un groupe monogène infini). *Tout sous-groupe non-trivial d'un groupe monogène infini est monogène infini.*

Preuve. On a $G = \{x^m\,;\, m \in \mathbb{Z}\}$ avec $x \neq e$ qui n'est pas d'ordre fini. Soit H un sous-groupe de G distinct de $\{e\}$. Il existe donc dans H des éléments de la forme x^ℓ avec $\ell \in \mathbb{Z}^*$. Comme l'inverse d'un élément de H appartient à H, on peut préciser qu'il existe dans H des éléments de la forme x^ℓ avec $\ell \in \mathbb{N}^*$. Soit alors d le plus petit entier strictement positif tel que $x^d \in H$. Posons $K = \{x^{dm}\,;\, m \in \mathbb{Z}\}$. Il est clair que $K \subseteq H$ (car $x^d \in H$ et H est stable par produit et passage à l'inverse). Réciproquement, soit x^m un élément quelconque de H (avec $m \in \mathbb{Z}$). Par division euclidienne de m par d, il existe $a, r \in \mathbb{Z}$ uniques tels que $m = ad + r$ avec $0 \leq r < d$. On a $x^r = x^{m-ad} = x^m.(x^d)^{-a}$ avec $x^m \in H$ et $(x^d)^{-a} \in K \subset H$, et donc $x^r \in H$. Par minimalité de d, on a donc forcément $r = 0$; d'où $x^m = x^{ad}$ et donc $x^m \in K$. Ceci prouve que $H \subseteq K$. On conclut que $H = K = \langle x^d \rangle$. □

2.2.3 Proposition (Sous-groupe d'un groupe cyclique). *Tout sous-groupe d'un groupe cyclique est cyclique. Plus précisément, si $G = \langle x \rangle$ est un groupe cyclique d'ordre $n \geq 1$, alors il existe pour tout diviseur q de n un et un seul sous-groupe d'ordre q, et c'est le sous-groupe cyclique engendré par x^d où $n = dq$.*

Preuve. On a $G = \{e, x, x^2, x^3, \ldots, x^{n-1}\}$. Il est clair que, si q est un diviseur de n, et si l'on pose $n = pq$ avec $p \in \mathbb{N}^*$, alors $\langle x^p \rangle = \{e, x^p, x^{2p}, x^{3p}, x^{(q-1)p}\}$ est un sous-groupe de G cyclique d'ordre q. Réciproquement, soit H un sous-groupe de G. D'après le théorème de Lagrange, l'ordre q de H doit diviser l'ordre de G. On peut supposer $H \neq \{e\}$, c'est-à-dire $q \neq 1$. Comme dans la preuve de la proposition précédente, on peut considérer d le plus petit entier $1 \leq d \leq n-1$ tel que $x^d \in H$, et montrer que $H = \langle x^d \rangle$. Comme H est d'ordre q, on déduit que $dq = n$ et $H = \{e, x^d, x^{2d}, x^{3d}, \ldots, x^{(q-1)d}\}$. $\square$

2.3 Générateurs d'un groupe cyclique.

2.3.1 Exemple préliminaire.

Figure 1

Dans $\mathbb{C}^*$, considérons $x = \mathrm{e}^{i\pi/3}$, et $G = \{e, x, x^2, x^3, x^4, x^5\}$ le groupe cyclique d'ordre 6 engendré par x. Ce groupe G est le groupe $\mathbb{U}_6$ des racines sixièmes de l'unité dans $\mathbb{C}^*$. Ses éléments $e = 1$, $x = -j^2$, $x^2 = j$, $x^3 = -1$, $x^4 = j^2$, $x^5 = -j$ peuvent être représentés dans le plan complexe comme les sommets respectifs A, B, C, D, E, F d'un hexagone régulier centré en l'origine et inscrit dans le cercle unité.
Considérons dans G les sous-groupes cycliques qu'engendrent les différents éléments. On a bien sûr $\langle e \rangle = \{e\}$ et $\langle x \rangle = G$. De plus $\langle x^2 \rangle = \langle x^4 \rangle = \{e, x^2, x^4\}$ est le sous-groupe d'ordre 3 de G (cf. proposition 2.2.3), qui correspond au triangle ACE. De même $\langle x^3 \rangle = \{e, x^3\}$ est le sous-groupe d'ordre 2 de G, qui correspond au segment AD.
Considérons enfin le sous-groupe engendré par x^5. Il contient $(x^5)^2 = x^{10} = x^4$, $(x^5)^3 = x^{15} = x^3$, $(x^5)^4 = x^{20} = x^2$, $(x^5)^5 = x^{25} = x$, $(x^5)^6 = x^{30} = e$, et donc $\langle x^5 \rangle = G$. L'élément x^5 est, comme x, un générateur du groupe G.
Ce résultat est un cas particulier du théorème suivant.

2.3.2 Théorème. *Soit $G = \langle x \rangle$ un groupe cyclique d'ordre $n \geq 2$. Alors les générateurs de G sont les éléments x^k tels que les entiers k et n soient premiers entre eux.*

Preuve. On a $G = \{e, x, x^2, x^3, \ldots, x^{n-1}\}$. Soit $k \in \mathbb{Z}^*$ et $H = \langle x^k \rangle$. On a $H = G$ si et seulement si $x \in H$ (puisqu'alors H contient toutes les puissances de x et donc tous les éléments de G). Or:

$x \in H \Leftrightarrow$ il existe $u \in \mathbb{Z}$ tel que $x = x^{ku}$
$x \in H \Leftrightarrow$ il existe $u \in \mathbb{Z}$ tel que $x^{ku-1} = e$
$x \in H \Leftrightarrow$ il existe $u \in \mathbb{Z}$ tel que $ku - 1$ est multiple de l'ordre n de x
$x \in H \Leftrightarrow$ il existe $u, v \in \mathbb{Z}$ tel que $ku + nv = 1$.

Cette dernière condition équivaut, d'après le théorème de Bezout, au fait que k et n sont premiers entre eux, ce qui achève la preuve. $\square$

2.3.3 Remarque (Indicatrice d'Euler). On appelle *fonction indicatrice d'Euler* l'application $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ définie par $\varphi(1) = 1$ et, pour tout entier $n \geq 2$:

$\varphi(n)$ est le nombre d'entiers k tels que $1 \leq k \leq n-1$ et k est premier avec n.

D'après le théorème précédent, $\varphi(n)$ est le nombre de générateurs d'un groupe cyclique d'ordre n.
Par définition de φ, on peut calculer:

$$\varphi(2) = 1,\ \ \varphi(3) = 2,\ \ \varphi(4) = 2,\ \ \varphi(5) = 4,\ \ \varphi(6) = 2,\ \ \varphi(7) = 6,\ \ \varphi(8) = 4,\ \ \ldots$$

Il est clair que, pour tout nombre premier p, on a $\varphi(p) = p - 1$.
Montrer en exercice que $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ pour tout nombre premier p et tout entier $\alpha \geq 1$.
On verra plus loin une formule générale permettant de calculer $\varphi(n)$ pour tout entier $n \geq 1$.

2.3.4 Exercice. Montrer que, si $G = \langle x \rangle$ est un groupe monogène infini, alors les seuls générateurs de G sont x et x^{-1}.

2.4 Groupes finis d'ordre premier

Proposition. *Soit G un groupe fini d'ordre premier p. Alors:*

1. *G est cyclique,*
2. *les seuls sous-groupes de G sont $\{e\}$ et G,*
3. *tous les éléments de G distincts de e sont des générateurs de G.*

Preuve. Comme $p > 1$, $G \neq \{e\}$. Soit $x \in G$ quelconque distinct de e. Posons $H = \langle x \rangle$ le sous-groupe de G engendré par x. D'après le théorème de Lagrange, l'ordre q de H doit diviser p. Comme p est premier, et comme $q \neq 1$ puisque $x \neq e$, on a forcément $q = p$. Donc $H = G$, c'est-à-dire $G = \langle x \rangle = \{e, x, x^2, x^3, \ldots, x^{p-1}\}$. Ceci prouve les points 1 et 2, et le point 3 résulte alors immédiatement du théorème 2.3.2. $\square$

3. Morphismes de groupes

3.1 Notion de morphisme de groupes

3.1.1 Définition. Soient G un groupe muni d'une loi de composition interne . et G' un groupe muni d'une loi de composition interne $*$. On appelle *morphisme de groupes*, ou *homomorphisme de groupes* de G dans G' toute application $f : G \to G'$ telle que:

$$f(x.y) = f(x) * f(y) \quad \text{pour tous } x, y \in G.$$

3.1.2 Exemples.
(a) L'application dét : $\mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$ qui à toute matrice carrée d'ordre inversible associe son déterminant est un morphisme de groupes de $\mathrm{GL}_n(\mathbb{R})$ muni du produit matriciel dans $\mathbb{R}^*$ muni de la multiplication, car:

$$\text{dét}(A \times B) = \text{dét}\, A \,.\, \text{dét}\, B, \;\text{ pour toutes } A, B \in \mathrm{GL}_n(\mathbb{R}).$$

(b) L'application $\exp : \mathbb{R} \to \mathbb{R}_+^*$ qui à tout nombre réel associe son exponentielle est un morphisme de groupes de $\mathbb{R}$ muni de l'addition dans $\mathbb{R}_+^*$ muni de la multiplication, car:

$$\exp(x + y) = \exp x \,.\, \exp y, \;\text{ pour tous } x, y \in \mathbb{R}.$$

3.1.3 Convention et remarques. Comme on a convenu précédemment de noter les groupes multiplicativement, on continuera à utiliser le point de multiplication pour désigner aussi bien la loi de groupe de G que celle de G'. La condition caractérisant le fait qu'une application $f : G \to G'$ est un morphisme de groupes devient alors:

$$f(x.y) = f(x).f(y) \quad \text{pour tous } x, y \in G,$$

en prenant garde que le point désigne à gauche la loi de G et à droite celle de G'. Il est immédiat de vérifier alors que, pour un tel morphisme de groupes $f : G \to G'$, on a:

(i) $f(e) = e'$, où e désigne le neutre de G et e' celui de G',

(ii) $f(x^{-1}) = f(x)^{-1}$, pour tout $x \in G$,

(iii) $f(x^n) = f(x)^n$, pour tout $x \in G$ et tout $n \in \mathbb{Z}$.

3.1.4 Proposition. *L'image directe d'un sous-groupe et l'image réciproque d'un sous-groupe par un morphisme de groupes sont des sous-groupes. Plus précisément, si G et G' sont deux groupes et si $f : G \to G'$ est un morphisme de groupes, on a:*

(i) *pour tout sous-groupe H de G, l'image directe $f(H) = \{x' \in G' \,;\, \exists\, x \in H,\; f(x) = x'\} = \{f(x) \,;\, x \in H\}$ est un sous-groupe de G';*

(ii) *pour tout sous-groupe H' de G', l'image réciproque $f^{-1}(H') = \{x \in G \,;\, f(x) \in H'\}$ est un sous-groupe de G.*

Preuve. On montre le point (ii) en laissant au lecteur le soin de rédiger de même la preuve du (i). Considérons donc un sous-groupe H' de G', posons $H = f^{-1}(H')$, et montrons que H est un sous-groupe de G. Comme $f(e) = e'$ d'après 3.1.3.(i) et que $e' \in H'$ puisque H' est un sous-groupe de G', on a $e \in H$, et en particulier H n'est pas vide. Soient x et y deux éléments quelconques de H. On a donc $f(x) \in H'$ et $f(y) \in H'$, d'où $f(x).f(y)^{-1} \in H'$ car H' est un sous-groupe de G'. Or en utilisant 3.1.3.(ii), on a $f(x).f(y)^{-1} = f(x.y^{-1})$. On conclut que $f(x.y^{-1}) \in H'$, c'est-à-dire $x.y^{-1} \in H$, ce qui prouve le résultat voulu. $\square$

3.1.5 Proposition. *La composée de deux morphismes de groupes est encore un morphisme de groupes. Plus précisément, si G, G' et G'' sont trois groupes, et si $f : G \to G'$ et $g : G' \to G''$ sont des morphismes de groupes, alors $g \circ f : G \to G''$ est un morphisme de groupes.*

Preuve. Evidente, laissée au lecteur. □

3.2 Image et noyau

3.2.1 Proposition et définition. *Soit $f : G \to G'$ un morphisme de groupes.*

(i) *l'ensemble $f(G) = \{x' \in G' \,;\, \exists\, x \in G,\ f(x) = x'\} = \{f(x)\,;\, x \in G\}$ est un sous-groupe de G' appelé l'image de f, et noté* $\operatorname{Im} f$;

(ii) *l'ensemble $f^{-1}(\{e'\}) = \{x \in G\,;\, f(x) = e'\}$ est un sous-groupe de G, appelé le noyau de f, et noté* $\operatorname{Ker} f$.

Preuve. Il suffit d'appliquer la proposition 3.1.4 avec $H = G$ et $H' = \{e'\}$. □

3.2.2 Proposition et définition. *Soit $f : G \to G'$ un morphisme de groupes.*

(i) *f est surjective si et seulement si* $\operatorname{Im} f = G'$;

(ii) *f est injective si et seulement si* $\operatorname{Ker} f = \{e\}$.

Preuve. Le point (i) est immédiat par définition même de la surjectivité. Pour montrer le (ii), supposons d'abord que f est injective. Soit $x \in \operatorname{Ker} f$. On a $f(x) = e'$, et puisque $f(e) = e'$ comme on l'a vu en 3.1.3.(i), on déduit $f(x) = f(e)$, qui implique $x = e$ par injectivité de f. On conclut que $\operatorname{Ker} f = \{e\}$. Réciproquement, supposons que $\operatorname{Ker} f = \{e\}$ et montrons que f est injective. Pour cela , considérons $x, y \in G$ tels que $f(x) = f(y)$. On a alors $f(x).f(y)^{-1} = e'$, donc $f(x.y^{-1}) = e'$, c'est-à-dire $x.y^{-1} \in \operatorname{Ker} f$. L'hypothèse $\operatorname{Ker} f = \{e\}$ implique alors $x.y^{-1} = e$, d'où $x = y$. L'injectivité de f est ainsi montrée, ce qui achève la preuve. □

3.2.3 Exemples. Reprenons les exemples 3.1.2.

(a) Le noyau du morphisme dét : $\mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$ est $\operatorname{Ker}\text{dét} = \{A \in \mathrm{GL}_n(\mathbb{R})\,;\, \text{dét}\, A = 1\} = \mathrm{SL}_n(\mathbb{R})$ qui, dès lors que $n \geq 2$, n'est pas réduit à $\{I_n\}$; donc le morphisme dét n'est pas injectif. En revanche, il est clair que, quel que soit un réel $x \in \mathbb{R}^*$, on peut trouver une matrice $A \in \mathrm{GL}_n(\mathbb{R})$ telle que dét $A = x$, ce qui prouve l'égalité $\operatorname{Im}\text{dét} = \mathbb{R}^*$ et la surjectivité de dét.

(b) Le morphisme $\exp : \mathbb{R} \to \mathbb{R}_+^*$ est surjectif; son noyau est $\operatorname{Ker}\exp = \{x \in \mathbb{R}\,;\, \exp(x) = 1\} = \{0\}$, ce qui prouve qu'il est aussi injectif.

3.3 Isomorphismes de groupes

3.3.1 Définition. Soient G et G' deux groupes. On appelle *isomorphisme de groupe* de G sur G' tout morphisme de groupes $f : G \to G'$ qui est de plus une bijection de G sur G'.
L'exemple 3.2.3.(b) ci-dessus est un exemple d'isomorphisme de groupes.

3.3.2 Proposition. *Si f est un isomorphisme de groupes de G sur G', alors la bijection réciproque f^{-1} est un isomorphisme de groupes de G' sur G.*

Preuve. Soient x' et y' deux éléments quelconques de G'. Posons $x = f^{-1}(x')$ et $y = f^{-1}(y')$. Parce que f est un morphisme de groupes, on a $f(x.y) = f(x).f(y)$, donc $f(x.y) = x'.y'$, d'où $x.y = f^{-1}(x'.y')$, c'est-à-dire $f^{-1}(x').f^{-1}(y') = f^{-1}(x'.y')$. Ceci prouve que f^{-1} est un morphisme de groupes de G' sur G, ce qui achève la preuve. □

3.3.3 Définition. Soient G et G' deux groupes. On dit que G et G' sont *isomorphes* lorsqu'il existe un isomorphisme de groupes de G sur G'. On note $G \simeq G'$.

3.3.4 Remarques importantes.

(a) Soient G et G' deux groupes isomorphes, et f un isomorphisme de G sur G'. Tout élément de G correspond par f à un et un seul élément de G' (et réciproquement), et ceci de telle façon que toute égalité vérifiée dans G par certains éléments sera vérifiée à l'identique dans G' par les images de ces derniers par f.

Si par exemple x est d'ordre fini n dans G, alors $x^n = e$ et $x^m \neq e$ pour tout $1 \leq m < n$; l'élément $f(x)$ de G' vérifie $f(x)^n = e'$ et $f(x)^m \neq e'$ pour tout $1 \leq m < n$, et donc $f(x)$ est aussi d'ordre n.

Si par exemple deux éléments x et y commutent dans G, c'est-à-dire vérifient $x.y = y.x$, alors on a dans G' l'égalité $f(x).f(y) = f(y).f(x)$, de sorte que les éléments $f(x)$ et $f(y)$ commutent dans G'.

(b) Il en résulte que deux groupes isomorphes ont exactement les mêmes propriétés algébriques. C'est pourquoi on exprime souvent l'isomorphisme de deux groupes G et G' en disant qu'il s'agit du même groupe (en fait c'est le même groupe "à isomorphisme près"), indépendamment de la réalisation concrète que l'on rencontre.

Par exemple, le sous-groupe $G_1 = \{\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right), \left(\begin{smallmatrix}-1&0\\0&-1\end{smallmatrix}\right), \left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)\}$ de $GL_2(\mathbb{R})$ étudié en 1.3.5.b et le sous-groupe $\mathbb{U}_4 = \{1, i, -1, -i\}$ de $\mathbb{C}^*$ sont évidemment isomorphes, et sont deux réalisations concrètes du même groupe abstrait, à savoir le groupe cyclique $C_4 = \{e, x, x^2, x^3\}$ d'ordre 4 (il suffit de poser $x = i$ dans le premier cas, et $x = \left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right)$ dans le second).

En revanche, le sous-groupe $G_2 = \{\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right), \left(\begin{smallmatrix}-1&0\\0&-1\end{smallmatrix}\right), \left(\begin{smallmatrix}-1&0\\0&1\end{smallmatrix}\right)\}$ étudié en 1.3.5.c ne leur est pas isomorphe (car il contient trois éléments d'ordre 2 alors que C_4 n'en contient qu'un seul). Il s'agit donc réellement d'un autre groupe.

3.3.5 Quelques conséquences à retenir.

(a) Pour tout entier $n \geq 1$, il existe à isomorphisme près un et un seul groupe cyclique d'ordre n. On le note C_n.

De façon abstraite, on le note multiplicativement $C_n = \{e, x, x^2, x^3, \ldots, x^{n-1}\}$. Une réalisation concrète en est le groupe $\mathbb{U}_n$ des racines n-ièmes de l'unité de $\mathbb{C}^*$, que l'on peut représenter géométriquement comme un polygone régulier à n côtés. On verra plus loin dans le cours une autre réalisation du groupe C_n, notée $\mathbb{Z}/n\mathbb{Z}$, avec une loi additive.
Comme deux groupes finis isomorphes ont évidemment le même ordre, il est clair que $C_n \not\simeq C_m$ dès lors que $n \neq m$.

(b) Pour tout nombre premier p, il existe à isomorphisme près un et un seul groupe fini d'ordre p ; c'est le groupe cyclique C_p.

Celà résulte immédiatement de la proposition 2.4 et de ce qui précède.

(c) Tout groupe monogène infini est isomorphe au groupe $\mathbb{Z}$ muni de l'addition.

En effet, si G est un groupe monogène infini, il existe $x \in G$ tel que $G = \{x^m\,;\, m \in \mathbb{Z}\}$. Cet élément x n'est pas d'ordre fini dans G (sinon G ne serait pas infini). L'application:

$$\begin{array}{rccc} f: & \mathbb{Z} & \longrightarrow & G \\ & m & \longmapsto & x^m \end{array}$$

est alors un morphisme du groupe $\mathbb{Z}$ muni de l'addition dans le groupe G muni de la loi . (car $f(m+n) = x^{m+n} = x^m.x^n = f(m).f(n)$). Ce morphisme est surjectif par construction. De plus, si $m \in \operatorname{Ker} f$, alors $x^m = e$, ce qui implique $m = 0$ puisque x n'est pas d'ordre fini; ceci prouve que $\operatorname{Ker} f = \{0\}$, donc que f est injectif. On conclut que f est un isomorphisme de groupes.

(d) Il existe à isomorphisme près deux groupes d'ordre 4, et deux seulement: l'un est le groupe cyclique C_4, l'autre est noté V et appelé le groupe de Klein; ils sont tous les deux abéliens, et leurs tables respectives sont:

C_4	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

V	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

En effet, soit $G = \{e, a, b, c\}$ un groupe d'ordre 4 de neutre e. Deux cas peuvent se présenter.
Premier cas: G contient un élément d'ordre 4. Supposons par exemple que ce soit a. Alors G doit contenir a^2 et $a^3 = a^{-1}$ qui sont distincts de a. On a donc $b = a^2$ et $c = a^3$ (ou le contraire), ce qui donne la première table.

Second cas: G ne contient pas d'élément d'ordre 4. Comme e est le seul élément d'ordre 1, et que G ne peut pas contenir d'éléments d'ordre 3 d'après le théorème de Lagrange, c'est que a, b, c sont tous les trois d'ordre 2. Donc $a^2 = b^2 = c^2 = e$, et chacun des trois est son propre inverse. Considérons le produit $a.b$. Si l'on avait $a.b = a$, on aurait $b = e$, ce qui est exclu. Si l'on avait $a.b = b$, on aurait $a = e$, ce qui est exclu. Si l'on avait $a.b = e$, on aurait $b = a^{-1}$, c'est-à-dire $b = a$, ce qui est exclu. On a donc forcément $a.b = c$. On calcule de même les autres produits. On obtient la seconde table.

(e) On peut de même démontrer (un peu plus difficile, et laissé en exercice) qu'il existe à isomorphisme près deux groupes d'ordre 6, et deux seulement: l'un est le groupe cyclique C_6 (et est donc abélien), l'autre est non abélien, et est isomorphe par exemple au groupe symétrique S_3 dont on a donné la table en 1.3.5.d.

CONVENTION. – On a convenu de noter les groupes multiplicativement. Désormais, on s'autorisera aussi à ne pas écrire le point de multiplication s'il n'est pas absolument nécessaire à la compréhension; on notera donc xy pour $x.y$ le produit de deux éléments par la loi du groupe.

3.4 Automorphismes de groupes

3.4.1 Définition. Soit G un groupe. On appelle *automorphisme* de G tout morphisme de groupes de G dans G qui est une bijection de G sur G.

En d'autres termes, un automorphisme de groupe est un isomorphisme de groupes dont le groupe d'arrivée est le même que le groupe de départ.

Il est clair, d'après la proposition 3.3.2, que la bijection réciproque d'un automorphisme de G est elle-même un automorphisme de G.

3.4.2 Exemples. L'application $\gamma : \mathbb{C} \to \mathbb{C}$ définie par $z \mapsto \gamma(z) = \overline{z}$ est un automorphisme du groupe $\mathbb{C}$ muni de l'addition; il vérifie $\gamma^{-1} = \gamma$. L'application $c : \mathbb{R}_+^* \to \mathbb{R}_+^*$ définie par $x \mapsto c(x) = x^2$ est un automorphisme du groupe $\mathbb{R}_+^*$ muni de la multiplication; sa bijection réciproque est l'automorphisme $c^{-1} : \mathbb{R}_+^* \to \mathbb{R}_+^*$ défini par $x \mapsto c^{-1}(x) = \sqrt{x}$.

3.4.3 Proposition et définition. *Soit G un groupe. L'ensemble des automorphismes du groupe G est un groupe pour la loi $\circ$, dont l'élément neutre est id_G. On le note $\operatorname{Aut} G$.*

Preuve. On montre que $\operatorname{Aut} G$ est un sous-groupe du groupe $\mathcal{S}(G)$ des bijections de l'ensemble G sur lui-même. Il est clair que $\operatorname{Aut} G \subset \mathcal{S}(G)$. L'ensemble $\operatorname{Aut} G$ n'est pas vide car $\mathrm{id}_G \in \operatorname{Aut} G$. Si $f, g \in \operatorname{Aut} G$, alors $f \circ g$ est bijectif (comme composé de deux bijections) et est un morphisme de groupes (d'après 3.1.5), donc $f \circ g \in \operatorname{Aut} G$. Ainsi $\operatorname{Aut} G$ est stable pour la loi $\circ$. Enfin, si $f \in \operatorname{Aut} G$, on a $f^{-1} \in \operatorname{Aut} G$ d'après la dernière remarque de 3.4.1, ce qui achève la preuve.

3.5 Automorphismes intérieurs et centre.

3.5.1 Proposition et définition. *Soit G un groupe.*

(i) *L'ensemble des éléments de G qui commutent avec tous les éléments de G est un sous-groupe de G, appelé le centre du groupe G, et noté $Z(G)$:*

$$Z(G) = \{x \in G\,;\, gx = xg \text{ pour tout } g \in G\}.$$

(ii) *Le sous-groupe $Z(G)$ est abélien.*

(iii) *G est abélien si et seulement si $Z(G) = G$.*

Preuve. Pour tout $g \in G$, on a $eg = ge = g$, donc $e \in Z(G)$, et $Z(G)$ n'est donc pas vide. Soient $x, y \in Z(G)$; pour tout $g \in G$, on a: $(xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy)$, et donc $xy \in Z(G)$. Soit $x \in Z(G)$; pour tout $g \in G$, on multiplie les deux membres de l'égalité $xg = gx$ par x^{-1} à gauche et à droite, et l'on obtient $gx^{-1} = x^{-1}g$, ce qui prouve que $x^{-1} \in Z(G)$. Ceci prouve (i). Les points (ii) et (iii) sont alors évidents.

3.5.2 Exercice. Montrer que, pour tout $x \in G$ l'ensemble $C(x) = \{g \in G\,;\, gx = xg\}$ des éléments de G qui commutent avec x est un sous-groupe de G. On l'appelle le centralisateur de x. Montrer que $Z(G) = \bigcap_{x\in G} C(x)$.

3.5.3 Proposition et définition. *Soit G un groupe.*

(i) *Pour tout $x \in G$, l'application $\sigma_x : G \to G$ définie par:*
$$\sigma_x(g) = xgx^{-1} \quad \textit{pour tout } g \in G$$
est un automorphisme du groupe G; on l'appelle l'automorphisme intérieur déterminé par x.

(ii) *L'ensemble $\operatorname{Int} G = \{\sigma_x\,;\, x \in G\}$ de tous les automorphismes intérieurs de G est un sous-groupe du groupe $\operatorname{Aut} G$ de tous les automorphismes de G.*

(iii) *L'application $\sigma : G \to \operatorname{Aut} G$ qui, à tout élément $x \in G$, associe l'automorphisme intérieur σ_x, est un morphisme de groupe, d'image $\operatorname{Int} G$ et de noyau le centre $Z(G)$.*

Preuve. (i) Fixons $x \in G$. Pour tout $g \in G$, on a:
$$\sigma_{x^{-1}}(\sigma_x(g)) = x^{-1}(xgx^{-1})x = g = x(x^{-1}gx)x^{-1} = \sigma_x(\sigma_{x^{-1}}(g)).$$
Ceci montre que $\sigma_x \circ \sigma_{x^{-1}} = \sigma_{x^{-1}} \circ \sigma_x = \mathrm{id}_G$, ce qui prouve que σ_x est une bijection de G sur G, dont la bijection réciproque est $\sigma_{x^{-1}}$. En d'autres termes, $\sigma_x^{-1} = \sigma_{x^{-1}}$. Par ailleurs, quels que soient $g, h \in G$, on a:
$$\sigma_x(gh) = x(gh)x^{-1} = xg(x^{-1}x)hx^{-1} = (xgx^{-1})(xhx^{-1}) = \sigma_x(g)\sigma_x(h),$$
ce qui montre que σ_x est un morphisme de groupes. On conclut que $\sigma_x \in \operatorname{Aut} G$.

(ii) L'ensemble $\operatorname{Int} G$ n'est pas vide: il contient en particulier $\mathrm{id}_G = \sigma_e$. Soient $x, y \in G$. Pour tout $g \in G$, on a: $\sigma_x(\sigma_y(g)) = x(ygy^{-1})x^{-1} = (xy)g(y^{-1}x^{-1}) = (xy)g(xy)^{-1} = \sigma_{xy}(g)$. Donc $\sigma_x \circ \sigma_y = \sigma_{xy}$. Ceci prouve que $\operatorname{Int} G$ est stable pour la loi $\circ$. Par ailleurs, on a déjà observé dans la preuve du point (i) que, pour tout $x \in G$, $\sigma_x^{-1} = \sigma_{x^{-1}} \in \operatorname{Int} G$, de sorte que $\operatorname{Int} G$ est aussi stable par passage à l'inverse. Ce qui achève la preuve.

(iii) On vient de voir que $\sigma_{xy} = \sigma_x \circ \sigma_y$ pour tous $x, y \in G$, ce qui montre que σ est un morphisme de groupes. Le fait que $\operatorname{Im} \sigma = \operatorname{Int} G$ découle de la définition même de $\operatorname{Int} G$. Soit maintenant $x \in \operatorname{Ker} \sigma$. Cela équivaut à $\sigma_x = \mathrm{id}_G$, c'est-à-dire à $xgx^{-1} = g$ pour tout $g \in G$, ou encore (en multipliant à droite par x) à $xg = gx$ pour tout $g \in G$. On conclut que $\operatorname{Ker} \sigma = Z(G)$.

Le point (iii) de cette proposition sera utilisé de façon cruciale au corollaire 2.3.3 du chapitre 2.

4. Produit direct de groupes.

4.1 Produit direct (externe) de deux groupes

4.1.1 Proposition et définition. *Soient G_1 et G_2 deux groupes, de neutres respectifs e_1 et e_2.*

(i) *Le produit cartésien $G_1 \times G_2 = \{(x_1, x_2),\ x_1 \in G_1,\ x_2 \in G_2\}$ est un groupe pour la loi:*
$$(x_1, x_2).(y_1, y_2) = (x_1y_1, x_2y_2) \qquad \textit{pour tous } x_1, y_1 \in G_1,\ x_2, y_2 \in G_2.$$
Ce groupe est appelé le produit direct de G_1 par G_2. On le note $G = G_1 \times G_2$. Son neutre est (e_1, e_2).

(ii) *L'application $p_1 : G_1 \times G_2 \to G_1$ qui, à tout élément $(x_1, x_2) \in G_1 \times G_2$, associe sa première composante x_1, est un morphisme de groupes (appelé première projection).*

(iii) *L'application $p_2 : G_1 \times G_2 \to G_2$ qui, à tout élément $(x_1, x_2) \in G_1 \times G_2$, associe sa seconde composante x_2, est un morphisme de groupes (appelé seconde projection).*

Preuve. Simple vérification, laissée au lecteur. □

4.1.2 Remarques. Il est clair que:

(a) $G_1 \times G_2$ est fini si et seulement si G_1 et G_2 le sont; on a alors $|G_1 \times G_2| = |G_1| \times |G_2|$;
(b) $G_1 \times G_2$ est abélien si et seulement si G_1 et G_2 le sont;
(c) le produit direct $G_1 \times G_2$ est isomorphe au produit direct $G_2 \times G_1$;
(d) on définit de même de façon évidente le produit direct d'un nombre fini quelconque de groupes.

4.2 Produit direct de groupes cycliques, théorème chinois

4.2.1 Question. Si G_1 et G_2 sont deux groupes cycliques, le produit direct $G_1 \times G_2$ est-il cyclique? Le théorème suivant, dit théorème chinois, répond à cette question. On regarde d'abord des exemples.

4.2.2 Premier exemple introductif.

Considérons le groupe cyclique $C_2 = \{e, x\}$ avec $x^2 = e$, et formons le produit direct $C_2 \times C_2$. On établit aisément sa table.

	(e,e)	(e,x)	(x,e)	(x,x)
(e,e)	(e,e)	(e,x)	(x,e)	(x,x)
(e,x)	(e,x)	(e,e)	(x,x)	(x,e)
(x,e)	(x,e)	(x,x)	(e,e)	(e,x)
(x,x)	(x,x)	(x,e)	(e,x)	(e,e)

On reconnaît le groupe de Klein $V = \{e, a, b, c\}$ pour: $e = (e, e)$, $a = (e, x)$, $b = (x, e)$ et $c = (x, x)$.

Donc $C_2 \times C_2$ n'est pas cyclique.

4.2.3 Second exemple introductif.

Considérons les groupes cycliques $C_2 = \{e, x\}$ et $C_3 = \{\varepsilon, y, y^2\}$ et formons le produit direct $C_2 \times C_3$. On établit aisément sa table.

	(e,ε)	(x,y)	(e,y^2)	(x,ε)	(e,y)	(x,y^2)
(e,ε)	(e,ε)	(x,y)	(e,y^2)	(x,ε)	(e,y)	(x,y^2)
(x,y)	(x,y)	(e,y^2)	(x,ε)	(e,y)	(x,y^2)	(e,ε)
(e,y^2)	(e,y^2)	(x,ε)	(e,y)	(x,y^2)	(e,ε)	(x,y)
(x,ε)	(x,ε)	(e,y)	(x,y^2)	(e,ε)	(x,y)	(e,y^2)
(e,y)	(e,y)	(x,y^2)	(e,ε)	(x,y)	(e,y^2)	(x,ε)
(x,y^2)	(x,y^2)	(e,ε)	(x,y)	(e,y^2)	(x,ε)	(e,y)

En posant $z = (x, y)$, on a: $(e, y^2) = z^2$, $(x, \varepsilon) = z^3$, $(e, y) = z^4$, $(x, y^2) = z^5$ et $(e, \varepsilon) = z^6$.
On conclut que $C_2 \times C_3 \simeq C_6$ est cyclique.

4.2.4 Théorème (dit théorème chinois). *Soient G_1 et G_2 deux groupes cycliques d'ordres respectifs n et m. Alors, le produit direct $G_1 \times G_2$ est cyclique si et seulement si les entiers n et m sont premiers entre eux.*

Preuve. Supposons que n et m sont premiers entre eux. Notons $G_1 = \langle x \rangle \simeq C_n$ avec x d'ordre n, et $G_2 = \langle y \rangle \simeq C_m$ avec y d'ordre m. Soit $z = (x, y)$ dans $G_1 \times G_2$. Quel que soit $k \in \mathbb{Z}$, on a $z^k = (e_1, e_2)$ si et seulement si $x^k = e_1$ et $y^k = e_2$, ce qui équivaut à dire que k est multiple à la fois de n et de m. Or le ppcm de n et m est ici nm puisque n et m sont premiers entre eux. Donc $z^{nm} = (e_1, e_2)$ et $z^k \neq (e_1, e_2)$ pour tout $1 \leq k < nm$. On conclut que l'élément z est d'ordre nm dans $G_1 \times G_2$. Or on sait que $G_1 \times G_2$ est formé de nm éléments; on conclut que $G_1 \times G_2 = \langle z \rangle \simeq C_{nm}$. La réciproque est laissée au lecteur. □

Remarque. Avec les notations multiplicatives utilisées ici, le théorème chinois s'énonce donc sous la forme:

$$C_n \times C_m \simeq C_{nm} \iff m \text{ et } n \text{ premiers entre eux.}$$

4.3 Produit direct (interne) de deux sous-groupes

4.3.1 NOTATION ET REMARQUES. Soient G un groupe, H et K deux sous-groupes de G. On note HK le sous-ensemble de G formé des éléments qui s'écrivent comme le produit d'un élément de H par un élément de K.

$$HK = \{hk\,;\, h \in H, k \in K\}.$$

(a) Si $H \cap K = \{e\}$, tout élément de HK s'écrit *de façon unique* sous la forme hk avec $h \in H, k \in K$.

En effet, si $h_1k_1 = h_2k_2$ avec $h_1, h_2 \in H$ et $k_1, k_2 \in K$, on a $h_2^{-1}h_1 = k_2k_1^{-1}$. Le premier produit est dans H puisque H est un sous-groupe, et le second est dans K puisque K est un sous-groupe. Donc $h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K$, c'est-à-dire $h_2^{-1}h_1 = k_2k_1^{-1} = e$, et donc $h_2 = h_1$ et $k_2 = k_1$.

(b) Si $H \cap K = \{e\}$, et si H et K sont finis, alors HK est fini et $\operatorname{card} HK = |H| \times |K|$.

En effet, il résulte du point précédent que $H \times K$ est alors équipotent à HK, via la bijection $(h, k) \mapsto hk$.

(c) On a $HK = KH$ si et seulement si, quels que soient $h \in H$ et $k \in K$, il existe $h' \in H$ et $k' \in K$ tels que $hk = k'h'$. Attention, cela n'implique pas que tout élément de H commute avec tout élément de K.

4.3.2 DÉFINITION. Soient G un groupe, H et K deux sous-groupes de G. On dit que G est le produit direct (interne) de H par K lorsque les trois conditions suivantes sont vérifiées:

$$(1)\;\; G = HK, \qquad (2)\;\; H \cap K = \{e\}, \qquad (3)\;\; \forall\, h \in H,\; \forall\, k \in K,\; hk = kh.$$

Il est clair qu'alors, on a aussi $G = KH$ et que G est donc le produit direct de K par H.

(a) *Exemple.* Soient: $G = \{\left(\begin{smallmatrix} 1 & 0 & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{smallmatrix}\right)\,;\, b, c \in \mathbb{R}\}$, $\quad H = \{\left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & b \\ 0 & 0 & 1 \end{smallmatrix}\right)\,;\, b \in \mathbb{R}\}$, $\quad K = \{\left(\begin{smallmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)\,;\, c \in \mathbb{R}\}$,

Montrer que G est un sous-groupe de $\mathrm{GL}_3(\mathbb{R})$, que H et K sont des sous-groupes de G, et que G est le produit direct de H par K.

(b) *Exemple.* Soit: $G = \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & j \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & j^2 \end{smallmatrix}\right), \left(\begin{smallmatrix} j & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} j^2 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} j & 0 \\ 0 & j \end{smallmatrix}\right), \left(\begin{smallmatrix} j & 0 \\ 0 & j^2 \end{smallmatrix}\right), \left(\begin{smallmatrix} j^2 & 0 \\ 0 & j \end{smallmatrix}\right), \left(\begin{smallmatrix} j^2 & 0 \\ 0 & j^2 \end{smallmatrix}\right)\}$.

Montrer que G est un sous-groupe de $\mathrm{GL}_2(\mathbb{C})$, que $x = \left(\begin{smallmatrix} 1 & 0 \\ 0 & j \end{smallmatrix}\right)$ engendre un sous-groupe $H \simeq C_3$, que $y = \left(\begin{smallmatrix} j & 0 \\ 0 & 1 \end{smallmatrix}\right)$ engendre un sous-groupe $K \simeq C_3$, et que G est le produit direct de H par K.

4.3.3 REMARQUE. Soient G un groupe, H et K deux sous-groupes de G. Si G est le produit direct de H et K, alors tout élément de G s'écrit de façon unique comme le produit d'un élément de H par un élément de K. Cela découle des conditions (1) et (2), et de la remarque (a) de 4.3.1. Attention, la réciproque est fausse (voir plus loin en 6.2.2.(c)).

Les notions de produit direct externe de deux groupes (vue en 4.2) et de produit direct interne de deux sous-groupes d'un groupe (vue ci-dessus) sont en fait deux formulations d'une même notion, comme le montre la proposition suivante.

4.3.4 PROPOSITION. *Soient G_1 et G_2 deux groupes de neutres respectifs e_1 et e_2, et $G = G_1 \times G_2$ leur produit direct. Posons:*

$$H = G_1 \times \{e_2\} = \{(x_1, e_2)\,;\, x_1 \in G_1\} \quad \text{et} \quad K = \{e_1\} \times G_2 = \{(e_1, x_2)\,;\, x_2 \in G_2\}.$$

Alors H est un sous-groupe de G isomorphe à G_1, K est un sous-groupe de G isomorphe à G_2, et G est le produit direct interne de ses sous-groupes H et K.

Preuve. Simple vérification, laissée au lecteur. □

5.1 Notion de groupe symétrique.

5.1.1 Remarque préliminaire. Soit n un entier strictement positif. Soit X un ensemble fini à n éléments. On sait que le groupe $\mathcal{S}(X)$ des bijections de X sur X est alors un groupe fini d'ordre $n!$. Si Y est un autre ensemble de même cardinal n, il existe une bijection f de X sur Y et l'on construit de façon évidente un isomorphisme de groupes φ de $\mathcal{S}(X)$ sur $\mathcal{S}(Y)$ en posant $\varphi(\sigma) = f \circ \sigma \circ f^{-1}$ pour tout $\sigma \in \mathcal{S}(X)$. Le groupe $\mathcal{S}(X)$ est donc, à isomorphisme près, indépendant du choix de l'ensemble X, et ne dépend donc que de son cardinal.

5.1.2 Définition et remarque. Pour tout entier $n \geq 1$, on appelle *groupe symétrique sur n éléments*, ou *n-ième groupe symétrique*, le groupe des bijections d'un ensemble fini à n éléments quelconque sur lui-même. On le note S_n.

(a) S_n est un groupe fini, d'ordre $n!$.

(b) Les éléments de S_n sont appelés les permutations sur n éléments. On note une telle permutation sous la forme $\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$.

(c) Sa loi de composition interne, qui est la composition $\circ$ des bijections est notée multiplicativement, c'est-à-dire que l'on note $\sigma\tau$ au lieu de $\sigma \circ \tau$ pour toutes $\sigma, \tau \in S_n$. On note e l'élément neutre de S_n, qui est l'identité de $\{1, 2, \ldots, n\}$.

(d) Pour $n = 1$, le groupe S_1 est le groupe trivial $\{e\}$ d'ordre 1. Pour $n = 2$, le groupe S_2 est d'ordre 2, donc $S_2 = C_2 = \{e, \tau\}$ où $e = \left(\begin{smallmatrix} 1 & 2 \\ 1 & 2 \end{smallmatrix}\right)$ et $\tau = \left(\begin{smallmatrix} 1 & 2 \\ 2 & 1 \end{smallmatrix}\right)$, qui vérifie bien $\tau^2 = e$.

(e) Dès lors que $n \geq 3$, le groupe S_n n'est pas abélien.

En effet, considérons trois entiers $1 \leq i, j, k \leq n$ distincts deux à deux (ce qui est possible car $n \geq 3$). Posons $\gamma = \left(\begin{smallmatrix} i & j & k \\ j & k & i \end{smallmatrix}\right)$ et $\tau = \left(\begin{smallmatrix} i & j & k \\ i & k & j \end{smallmatrix}\right)$. On a $\gamma\tau = \left(\begin{smallmatrix} i & j & k \\ j & i & k \end{smallmatrix}\right)$ et $\tau\gamma = \left(\begin{smallmatrix} i & j & k \\ k & j & i \end{smallmatrix}\right)$. Donc $\gamma\tau \neq \tau\gamma$.

(f) Pour $n = 3$, le groupe S_3 est d'ordre 6. On a: $S_3 = \{e, \gamma, \gamma^2, \tau_1, \tau_2, \tau_3\}$ avec:

$$e = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix}\right), \quad \gamma = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right), \quad \gamma^2 = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix}\right), \quad \tau_1 = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right), \quad \tau_2 = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix}\right), \quad \tau_3 = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right).$$

	e	γ	γ^2	τ_1	τ_2	τ_3
e	e	γ	γ^2	τ_1	τ_2	τ_3
γ	γ	γ^2	e	τ_3	τ_1	τ_2
γ^2	γ^2	e	γ	τ_2	τ_3	τ_1
τ_1	τ_1	τ_2	τ_3	e	γ	γ^2
τ_2	τ_2	τ_3	τ_1	γ^2	e	γ
τ_3	τ_3	τ_1	τ_2	γ	γ^2	e

On a déjà vu en 1.3.5.(d) la table de S_3, rappelée ci-contre.

Le groupe S_3 est le plus petit groupe non abélien (car les groupes d'ordre 2, 3 ou 5 sont abéliens car cycliques d'après 3.3.5.(b), et les deux seuls groupes d'ordre 4 sont abéliens comme on l'a vu en 3.3.5.(d)).

S_3 admet trois sous-groupes d'ordre 2 qui sont $\{e, \tau_1\}$, $\{e, \tau_2\}$ et $\{e, \tau_3\}$, et un sous-groupe d'ordre 3 qui est $\{e, \gamma, \gamma^2\}$.

5.2 Décomposition d'une permutation en produit de transpositions.

5.2.1 Définition. On appelle *transposition* de S_n toute permutation τ qui échange deux éléments i et j en laissant fixes les $n - 2$ autres. On note alors $\tau = [i, j]$. On a de façon évidente $\tau^2 = e$, c'est-à-dire $\tau^{-1} = \tau$.

5.2.2 Théorème. *Toute permutation de S_n est un produit d'un nombre fini de transpositions. En d'autres termes, le groupe S_n est engendré par ses transpositions.*

Preuve. On raisonne par récurrence sur n. C'est clair si $n = 2$. Supposons (H.R.) le résultat vrai pour S_{n-1} où $n \geq 3$. Prenons $\sigma \in S_n$ quelconque. Distinguons deux cas. Si $\sigma(n) = n$, notons σ' la restriction de σ à $\{1, 2, \ldots, n-1\}$. Il est clair que $\sigma' \in S_{n-1}$. Donc par H.R., $\sigma' = \tau_1'\tau_2' \ldots \tau_m'$ où τ_k' est une transposition de $\{1, 2, \ldots, n-1\}$ pour tout $1 \leq k \leq m$. Chaque τ_k' se prolonge en une transposition τ_k de $\{1, 2, \ldots, n\}$ en posant $\tau_k(i) = \tau_k'(i)$ pour tout $1 \leq i \leq n-1$ et $\tau_k(n) = n$. Il est clair que l'on a alors $\sigma = \tau_1\tau_2 \ldots \tau_m$. Si maintenant $\sigma(n) = p \neq n$, posons $\tau = [n, p]$ et $\eta = \tau\sigma$. On a $\eta(n) = n$. En appliquant le premier cas, η se décompose en produit de transpositions. Donc $\sigma = \tau\eta$ aussi. $\square$

5.2.3 Remarque. Il n'y a pas unicité de cette décomposition.

Par exemple, dans S_4, on a $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{smallmatrix}\right) = [2,4][1,4][4,2][1,3] = [2,3][1,2]$.

5.3 Signature

5.3.1 Définitions. Soit $n \geq 2$ un entier. Pour toute permutation $\sigma \in S_n$, on appelle *nombre d'inversions* de σ l'entier:

$$I(\sigma) = \text{card } \{ \ (i,j) \in \{1,2,\dots,n\}^2 \ ; \ i < j \ \text{ et } \ \sigma(i) > \sigma(j) \ \}.$$

On appelle *signature* de σ l'entier valant $+1$ ou -1 défini par:

$$\varepsilon(\sigma) = (-1)^{I(\sigma)}.$$

5.3.2 Exemple. Si τ est une transposition de S_n, on a $\varepsilon(\tau) = -1$.

En effet, si $\tau = [i,j]$ avec $i < j$, les couples $(u,v) \in \{1,2,\dots,n\}^2$ vérifiant $u < v$ et $\sigma(u) > \sigma(v)$ sont exactement les $j-i$ couples $(i,i+1), (i,i+2), \dots, (i,j)$ et les $j-i-1$ couples $(i+1,j), (i+2,j), \dots, (j-1,j)$. Donc $I(\sigma) = j - i + j - i - 1 = 2(j-i) - 1$ est impair.

5.3.3 Proposition. *Quelles que soient deux permutations $\sigma, \gamma \in S_n$, on a: $\varepsilon(\gamma\sigma) = \varepsilon(\gamma)\varepsilon(\sigma)$. En d'autres termes, l'application:*

$$\begin{aligned} \varepsilon : \ S_n &\longrightarrow \{+1,-1\} \\ \sigma &\longmapsto \varepsilon(\sigma) \end{aligned}$$

est un morphisme de groupes.

Preuve. Pour toute permutation $\sigma \in S_n$ et toute application $f : \mathbb{Q}^n \to \mathbb{Q}$, on note $\sigma * f$ l'application $\mathbb{Q}^n \to \mathbb{Q}$ définie par: $\sigma * f(x_1, x_2, \dots, x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)})$. Il est clair que, pour toutes $\gamma\sigma \in S_n$, on a $\gamma * (\sigma * f) = (\gamma\sigma) * f$. Considérons en particulier l'application $\Delta : \mathbb{Q}^n \to \mathbb{Q}$ définie par:

$$\Delta(x_1, x_2, \dots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

Par définition du nombre d'inversions, on a $\sigma * \Delta(x_1, x_2, \dots, x_n) = (-1)^{I(\sigma)} \Delta(x_1, x_2, \dots, x_n)$ pour tous $x_1, x_2, \dots, x_n \in \mathbb{Q}^n$ et toute $\sigma \in S_n$. Donc $\sigma * \Delta = \varepsilon(\sigma)\Delta$. On déduit que, pour toutes $\sigma, \gamma \in S_n$, on a: $\varepsilon(\gamma\sigma)\Delta = (\gamma\sigma) * \Delta = \gamma * (\sigma * \Delta) = \gamma * (\varepsilon(\sigma)\Delta) = \varepsilon(\sigma)\gamma * \Delta = \varepsilon(\sigma)\varepsilon(\gamma)\Delta$. Comme l'application Δ n'est évidemment pas identiquement nulle, on conclut que $\varepsilon(\gamma\sigma) = \varepsilon(\sigma)\varepsilon(\gamma) = \varepsilon(\gamma)\varepsilon(\sigma)$. □

5.3.4 Corollaire. *Soit $\sigma \in S_n$.*

(i) *Si σ se décompose d'une part en un produit de m transpositions, d'autre part en un produit de m' transpositions, alors les entiers naturels m et m' sont de même parité.*

(ii) *On a $\epsilon(\sigma) = (-1)^m$, où m désigne le nombre de transpositions d'une décomposition quelconque de σ en produit de transpositions.*

Preuve. Résulte immédiatement de 5.2.2, 5.3.2 et 5.3.3. □

5.4 Groupe alterné.

5.4.1. Définition. Pour tout entier $n \geq 2$, le noyau de ε est appelé n-ième groupe alterné. On le note A_n.

Le sous-groupe A_n de S_n est donc l'ensemble des permutations de S_n qui sont de signature 1 (c'est-à-dire qui se décomposent en un nombre pair de transpositions).

5.4.2 Proposition. *Pour tout entier $n \geq 2$, le groupe A_n est fini d'ordre $\frac{n!}{2}$.*

Preuve. Notons X l'ensemble des permutations de S_n qui sont de signature -1. Le sous-ensemble X est non-vide (il contient par exemple les transpositions, voir 5.3.2). Si l'on fixe $\tau \in X$, il est facile de vérifier d'après 5.3.3 que l'application $\sigma \mapsto \tau\sigma$ réalise une bijection de A_n sur X. Comme $S_n = A_n \cup X$ et $A_n \cap X = \emptyset$, on conclut que $\text{card}X = |A_n| = \frac{1}{2}\,|S_n| = \frac{1}{2}\,n!$. □

5.4.3 Exemple. Pour $n = 2$, on a $A_2 = \{e\}$. Pour $n = 3$, on a $A_3 = \{e, \gamma, \gamma^2\}$ avec $\gamma = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right)$.

5.4.4 Exemple. Pour $n = 4$, le groupe alterné A_4 est d'ordre 12. Donnons quelques précisions.

Le groupe A_4 contient les trois produits de deux transpositions disjointes:

$$a = [1, 2][3, 4] = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{smallmatrix}\right), \quad b = [1, 3][2, 4] = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{smallmatrix}\right), \quad c = [1, 4][2, 3] = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{smallmatrix}\right).$$

Il contient aussi les huit permutations qui permutent circulairement trois éléments i, j, k en fixant le quatrième, et qui sont donc de la forme $[i, k][i, j]$. (De tels éléments sont appelés des 3-cycles).

$$x_1 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{smallmatrix}\right), \quad y_1 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{smallmatrix}\right) = x_1^2, \quad x_2 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{smallmatrix}\right), \quad y_2 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{smallmatrix}\right) = x_2^2,$$
$$x_3 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{smallmatrix}\right), \quad y_3 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{smallmatrix}\right) = x_3^2, \quad x_4 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{smallmatrix}\right), \quad y_4 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{smallmatrix}\right) = x_4^2.$$

	e	a	b	c	x_1	y_1	x_2	y_2	x_3	y_3	x_4	y_4
e	e	a	b	c	x_1	y_1	x_2	y_2	x_3	y_3	x_4	y_4
a	a	e	c	b	x_3	x_4	y_3	y_4	x_1	x_2	y_1	y_2
b	b	c	e	a	y_4	x_2	y_1	x_3	y_2	x_4	y_3	x_1
c	c	b	a	e	y_2	y_3	x_4	x_1	y_4	y_1	x_2	x_3
x_1	x_1	y_4	y_2	x_3	y_1	e	c	x_4	x_2	a	b	y_3
y_1	y_1	y_3	x_4	x_2	e	x_1	x_3	b	c	y_4	y_2	a
x_2	x_2	x_4	y_3	y_1	b	y_4	y_2	e	a	x_1	x_3	c
y_2	y_2	x_3	x_1	y_4	y_3	c	e	x_2	x_4	b	a	y_1
x_3	x_3	y_2	y_4	x_1	x_4	a	b	y_1	y_3	e	c	x_2
y_3	y_3	y_1	x_2	x_4	c	y_2	y_4	a	e	x_3	x_1	b
x_4	x_4	x_2	y_1	y_3	a	x_3	x_1	c	b	y_2	y_4	e
y_4	y_4	x_1	x_3	y_2	x_2	b	a	y_3	y_1	c	e	x_4

Les trois éléments a, b, c sont d'ordre 2, et le sous-groupe $V = \{e, a, b, c\}$ de A_4 est le groupe de Klein.

Les huit 3-cycles x_i, y_i pour $1 \leq i \leq 4$ sont d'ordre 3. On obtient donc quatre sous-groupes cycliques $G_i = \{e, x_i, y_i\}$, pour $1 \leq i \leq 4$.

On observe au passage que, bien que 4 et 6 soient des diviseurs de $|A_4| = 12$, le groupe A_4 ne contient pas d'élément d'ordre 4 ni 6.

5.5 Support et orbites.

5.5.1 Définition. Pour toute $\sigma \in S_n$, on appelle *support* de σ l'ensemble des éléments de $\{1, 2, \ldots, n\}$ qui ne sont pas fixés par σ:

$$\text{Supp } \sigma = \{i \in \{1, 2, \ldots, n\} \, ; \, \sigma(i) \neq i\}.$$

En particulier, Supp $\sigma = \emptyset$ si et seulement si $\sigma = e$.

5.5.2 Lemme. *Pour toute $\sigma \in S_n$ non triviale, la restriction de σ à* Supp σ *est une permutation de* Supp σ.

Preuve. Soit $i \in$ Supp σ; notons $j = \sigma(i)$. Si on avait $j \notin$ Supp σ, on aurait $\sigma(j) = j$, donc $\sigma(j) = \sigma(i)$, donc $i = j$, c'est-à-dire $i = \sigma(i)$, ce qui contredirait $i \in$ Supp σ. C'est donc que Supp σ est stable par σ. La restriction σ' de σ à Supp σ est une application de Supp σ dans lui-même, injective car σ l'est, et donc bijective. □

5.5.3 Proposition. *Deux permutations de S_n dont les supports sont disjoints commutent.*

Preuve. On peut supposer $n \geq 2$. Soient $\sigma, \eta \in S_n$ tels que Supp $\sigma \cap$ Supp $\eta = \emptyset$. Soit $i \in \mathbb{N}_n$ quelconque. Si $i \notin$ Supp $\sigma \cup$ Supp η; alors $\sigma(i) = i = \eta(i)$; donc $\sigma\eta(i) = \eta\sigma(i)$. Supposons maintenant $i \in$ Supp σ. D'une part, $i \notin$ Supp η, donc $\eta(i) = i$, donc $\sigma\eta(i) = \sigma(i)$. D'autre part, $i \in$ Supp σ implique $\sigma(i) \in$ Supp σ d'après le lemme précédent, donc $\sigma(i) \notin$ Supp η, donc $\eta\sigma(i) = \sigma(i)$. On conclut que $\sigma\eta(i) = \eta\sigma(i)$. Le dernier cas est celui où $i \in$ Supp η, que l'on traite de façon analogue en échangeant les rôles de σ et η. □

5.5.4 Définition. Pour toute $\sigma \in S_n$ et tout $i \in \{1, 2, \ldots, n\}$, on appelle σ-*orbite* de i l'ensemble des images de i par les différents éléments du groupe cyclique $\langle\sigma\rangle$; on note

$$\Omega_\sigma(i) = \{\sigma^k(i) \, ; \, k \in \mathbb{Z}\}, \quad \text{pour tout } 1 \leq i \leq n.$$

Il est clair que les différentes σ-orbites forment une partition de $\{1, 2, \ldots, n\}$, et que $\Omega_\sigma(i) = \{i\}$ si et seulement $i \notin$ Supp σ, (on dit alors que c'est une σ-orbite ponctuelle).

Exemple: soit $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 8 & 3 & 6 & 4 & 1 & 7 & 2 \end{smallmatrix}\right) \in S_8$; on a: $\Omega_\sigma(3) = \{3\}$, $\Omega_\sigma(7) = \{7\}$, $\Omega_\sigma(2) = \Omega_\sigma(8) = \{2, 8\}$, $\Omega_\sigma(1) = \{1, 5, 4, 6\} = \Omega_\sigma(5) = \Omega_\sigma(4) = \Omega_\sigma(6)$. Donc Supp $\sigma = \{1, 2, 4, 5, 6, 8\}$.

5.6 Décomposition d'une permutation en produit de cycles disjoints.

5.6.1 Définition. Une permutation $\sigma \in S_n$ est appelée un cycle lorsqu'il existe une σ-orbite et une seule qui n'est pas ponctuelle.

Exemple: soit $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 3 & 6 & 4 & 1 \end{smallmatrix}\right) \in S_6$; on a: $\Omega_2 = \{2\}$, $\Omega_3 = \{3\}$, $\Omega_1 = \{1,5,4,6\} = \Omega_5 = \Omega_4 = \Omega_6$. Donc σ est un cycle.

5.6.2 Proposition et définition. *Soit $\sigma \in S_n$ un cycle. On note p l'ordre de σ dans S_n.*

(i) *L'unique σ-orbite non ponctuelle est égale au support de σ.*

(ii) *Le cardinal du support de σ est égal à l'ordre p de σ.*

(iii) *Il existe $j_1, j_2, \ldots, j_p$ distincts dans $\{1, 2, \ldots, n\}$ tels que:*

$$\sigma(j_1) = j_2,\ \sigma(j_2) = j_3,\ \ldots,\ \sigma(j_p) = j_1 \quad \text{et} \quad \sigma(i) = i \ \text{ si } \ i \notin \{j_1, \ldots, j_p\}.$$

Preuve. Notons Ω l'unique σ-orbite non ponctuelle. Soit j_1 un représentant quelconque de Ω. Donc: $\Omega = \Omega_\sigma(j_1) = \{i \in \{1,2,\ldots,n\}\,;\, \Omega_\sigma(i) \neq \{i\}\}$ c'est-à-dire $\Omega = \operatorname{Supp} \sigma$, par définition même du support. Soit $q = |\Omega| = |\operatorname{Supp} \sigma|$. Donc:

$$\Omega = \operatorname{Supp} \sigma = \{j_1, \sigma(j_1), \sigma^2(j_1), \ldots, \sigma^{q-1}(j_1)\},$$

les éléments étant deux à deux distincts. On a alors $\sigma^q(j_1) = j_1$, et ceci étant vrai pour tout représentant j_1 dans $\Omega = \operatorname{Supp} \sigma$, on a $\sigma^q(i) = i$ pour tout $i \in \operatorname{Supp} \sigma$. Mais l'égalité $\sigma^q(i) = i$ est claire si $i \notin \operatorname{Supp} \sigma$ puisqu'alors $\sigma(i) = i$. Ainsi $\sigma^q = e$ dans S_n. Comme $\sigma^k \neq e$ pour $1 \leq k < q$, (puisque j_1 et $\sigma^k(j_1)$ sont alors deux éléments distincts de Ω), on conclut que q est exactement l'ordre de σ dans S_n. □

On dit que σ est un *p-cycle*, ou *cycle d'ordre p*. On note: $\sigma = [j_1, j_2, \ldots, j_p]$.

Remarque. On a aussi: $\sigma = [j_k, j_{k+1}, \ldots, j_p, j_1, \ldots, j_{k-1}]$ pour tout $1 < k \leq p$.

5.6.3 Exemples et premières propriétés.

1. Le seul 1-cycle est e. Les 2-cycles sont les transpositions $[i, j]$.
2. Le n-cycle $[1, 2, \ldots, n] = \left(\begin{smallmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ 2 & 3 & 4 & \ldots & n & 1 \end{smallmatrix}\right)$ s'appelle la permutation circulaire de S_n. Il existe des n-cycles qui ne sont pas la permutation circulaire, par exemple $[1, 3, 4, 2] \in S_4$.
3. L'inverse d'un p-cycle est un p-cycle: $[j_1, j_2, \ldots, j_p]^{-1} = [j_p, j_{p-1}, \ldots, j_1]$.
4. Attention: si $\gamma \in S_n$ est un r-cycle, et si $2 \leq k \leq r-2$, alors γ^k n'est pas nécessairement un cycle. Par exemple, si γ est la permutation circulaire $[1, 2, 3, 4] \in S_4$, alors $\gamma^2 = [1, 3][2, 4]$ n'est pas un cycle.
5. Le conjugué d'un p-cycle est un p-cycle. Plus précisément:

$$\text{si } \gamma = [j_1, j_2, \ldots, j_p] \ \text{ et } \ \sigma \in S_n, \ \text{ alors } \ \sigma\gamma\sigma^{-1} = [\sigma(j_1), \sigma(j_2), \ldots, \sigma(j_p)].$$

   Preuve. Soit $i \in \{1, 2, \ldots, n\}$. Si $\sigma^{-1}(i) \in \operatorname{Supp} \gamma$, il existe $1 \leq k \leq p$ tel que $i = \sigma(j_k)$. On a $\sigma\gamma\sigma^{-1}(i) = \sigma\gamma(j_k) = \sigma(j_{k+1})$ si $1 \leq k < p$, et $\sigma\gamma\sigma^{-1}(i) = \sigma\gamma(j_p) = \sigma(j_1)$ si $k = p$. Si maintenant $\sigma^{-1}(i) \notin \operatorname{Supp} \gamma$, alors $\gamma\sigma^{-1}(i) = \sigma^{-1}(i)$ et donc $\sigma\gamma\sigma^{-1}(i) = i$. Ceci prouve par définition même que $\sigma\gamma\sigma^{-1}$ est le p-cycle $[\sigma(j_1), \sigma(j_2), \ldots, \sigma(j_p)]$. □

6. Pour $n \geq 3$, le groupe alterné A_n est engendré par les 3-cycles de S_n.

   Preuve. Un produit de deux transpositions est nécessairement de l'un des deux types suivants (où i, j, k, l sont distincts deux à deux): ou bien $[i, j][i, k] = [i, k, j]$, ou bien $[i, j][k, l] = [i, l, k][i, j, k]$. Ce qui prouve le résultat voulu puisque A_n est l'ensemble des produits d'un nombre pair de transpositions. □

7. Si γ est un p-cycle, alors $\varepsilon(\gamma) = (-1)^{p-1}$.

   Preuve. Si $\gamma = [j_1, j_2, \ldots, j_p]$, alors $\gamma = [j_1, j_p][j_1, j_{p-1}] \cdots [j_1, j_2]$. □

On a vu en 5.2.3 que la décomposition d'une permutation en produit de transpositions n'est pas unique. En revanche, comme on va le voir maintenant, toute permutation se décompose en produits de cycles disjoints (et donc commutant deux à deux), et ceci de façon unique.

5.6.4 Théorème (Décomposition en produit de cycles disjoints).

(i) *Toute $\sigma \in S_n$ non triviale se décompose en un produit de cycles non triviaux à supports disjoints.*

(ii) *Les cycles dans une telle décomposition commutent deux à deux.*

(iii) *Cette décomposition est unique à l'ordre près des facteurs.*

Preuve. Soit $\sigma \in S_n$ non triviale. Il existe donc au moins une σ-orbite non ponctuelle. Désignons par $\Omega_1, \ldots, \Omega_q$ les σ-orbites non ponctuelles deux à deux distinctes (et donc deux à deux disjointes). Pour tout $1 \leq k \leq q$, définissons $\gamma_k : \{1, 2, \ldots, n\} \longrightarrow \{1, 2, \ldots, n\}$ par: $\gamma_k(i) = \sigma(i)$ si $i \in \Omega_k$ et $\gamma_k(i) = i$ sinon. Alors γ_k est un cycle dans S_n, (car si l'on note $r_k = |\Omega_k|$, on a $\Omega_k = \{j, \sigma(j), \sigma^2(j), \ldots, \sigma^{r_k-1}(j)\}$ quel que soit $j \in \Omega_k$), de support égal à Ω_k. Il en résulte que les supports des γ_i sont deux à deux disjoints, donc (d'après la proposition de 1.2), que les γ_i commutent deux à deux dans S_n. Posons $\sigma' = \gamma_1\gamma_2 \ldots \gamma_q$; on va montrer que $\sigma' = \sigma$.

En effet, soit $j \in \{1, 2, \ldots, n\}$; distinguons deux cas.

- Si $j \in \Omega_1 \cup \ldots \cup \Omega_q$, alors j appartient à une seule de ces orbites: il existe $1 \leq k \leq q$ tel que $j \in \Omega_k$ et $j \notin \Omega_i$ si $i \neq k$. Puisque les γ_i commutent deux à deux, on peut écrire $\sigma' = \gamma_k\gamma_1 \ldots \gamma_{k-1}\gamma_{k+1} \ldots \gamma_q$. Pour tout indice $i \neq k$, on $\gamma_i(j) = j$ car $j \notin \Omega_i = \text{Supp } \gamma_i$; donc $\gamma_1 \ldots \gamma_{k-1}\gamma_{k+1} \ldots \gamma_q(j) = j$, d'où $\sigma'(j) = \gamma_k(j)$. Or $\gamma_k(j) = \sigma(j)$ puisque $j \in \Omega_k$. On conclut finalement que $\sigma'(j) = \sigma(j)$.
- Si $j \notin \Omega_1 \cup \ldots \cup \Omega_q$, alors, pour tout $1 \leq k \leq q$, on a $j \notin \text{Supp } \gamma_k$ donc $\gamma_k(j) = j$, de sorte que $\sigma'(j) = j$. Mais par ailleurs, $j \notin \Omega_1 \cup \ldots \cup \Omega_q$ signifie que la σ-orbite de j est ponctuelle, c'est-à-dire que $\sigma(j) = j$. Dans ce cas aussi, on a vérifié que $\sigma'(j) = \sigma(j)$.

On a ainsi prouvé les points (i) et (ii) du théorème. Pour prouver (iii), supposons que l'on a une décomposition $\sigma = \gamma'_1\gamma'_2 \ldots \gamma'_p$ en produit de cycles non triviaux à supports deux à deux disjoints (donc commutant deux à deux). Pour tout $1 \leq i \leq p$, notons $\Omega'_i = \text{Supp } \gamma'_i$. Chaque Ω'_i est une σ-orbite non ponctuelle, plus précisément:

$$\text{pour tout } 1 \leq k \leq p \text{ et pour tout } j \in \Omega'_k, \text{ on a } \Omega'_k = \Omega_\sigma(j). \qquad (*)$$

En effet. Fixons $1 \leq k \leq p$ et $j \in \Omega'_k$. Il en résulte que $j \notin \Omega'_i$ si $1 \leq i \neq k \leq p$ (puisque les supports des γ'_i sont deux à deux disjoints). En d'autres termes, $\gamma'_i(j) = j$ pour tout $1 \leq i \neq k \leq p$. Donc en écrivant $\sigma = \gamma'_k\gamma'_1 \ldots \gamma'_{k-1}\gamma'_{k+1} \ldots \gamma'_p$, suivant la méthode déjà employée ci-dessus, on calcule $\sigma(j) = \gamma'_k(j)$. Comme $\gamma'_k(j)$ appartient à Ω'_k et n'appartient pas à Ω'_i pour $1 \leq i \neq k \leq p$, on réitère pour obtenir $\sigma^2(j) = (\gamma'_k)^2(j)$. Et finalement $\sigma^m(j) = (\gamma'_k)^m(j)$ pour tout entier $m \geq 1$. On conclut que: $\Omega'_k = \Omega_\sigma(j)$.

Réciproquement, on obtient ainsi toutes les σ-orbites non ponctuelles, plus précisément:

$$\text{pour tout } j \in \{1, 2, \ldots, n\} \text{ telle que } \Omega_\sigma(j) \neq \{j\}, \text{ il existe } 1 \leq k \leq p \text{ tel que } \Omega'_k = \Omega_\sigma(j). \qquad (**)$$

En effet. Par contraposée, si l'on suppose que quel que soit $1 \leq k \leq p$, on a $j \notin \Omega'_k$, alors $\gamma'_k(j) = j$ pour tout $1 \leq k \leq p$, de sorte que $\sigma(j) = j$, c'est-à-dire $\Omega_\sigma(j) = \{j\}$.

Il résulte de $(*)$ et $(**)$ que la décomposition $\sigma = \gamma'_1\gamma'_2 \ldots \gamma'_p$ est, à l'ordre près, celle que l'on a construite dans la preuve du point (i), c'est-à-dire que $p = q$ et $\{\gamma_1, \ldots, \gamma_p\} = \{\gamma'_1, \ldots, \gamma'_p\}$. □

5.6.5 Exemples d'applications (en exercices)

(a) *Une définition équivalente de la signature.* Montrer que, pour toute permutation $\sigma \in S_n$, la signature de σ vérifie $\varepsilon(\sigma) = (-1)^{n-t}$, où t désigne le nombre de σ-orbites distinctes dans S_n.

Indication: utiliser 5.6.4 et le point 7 de 5.6.3

(b) *Ordre d'un élément quelconque de S_n.* Montrer que l'ordre dans S_n d'un élément quelconque σ non trivial est égal au p.p.c.m. des longueurs des cycles disjoints de la décomposition canonique de σ.

Indication: utiliser 5.6.4 et le point (ii) de 5.6.2

6.1 Exemples préliminaires.

6.1.1 Premier exemple. Soit D_3 l'ensemble des isométries du plan affine euclidien conservant un triangle équilatéral (ABC). On montre aisément en géométrie que D_3 est formé de l'identité e, de la rotation r de centre l'isobarycentre O de (ABC) et d'angle $2\pi/3$, de la rotation r^2 de centre O et d'angle $4\pi/3$, et des réflexions s_1, s_2, s_3 par rapport aux trois médianes (ou hauteurs) du triangle. A noter que:

$$s_3 = rs_1, \quad s_2 = r^2 s_1.$$

On vérifie immédiatement que D_3 est un groupe (un sous-groupe du groupe des isométries du plan), d'ordre 6, non abélien, engendré par les deux éléments r et s_1, et dont la table est donnée ci-dessous.

Figure 2

D_3	e	r	r^2	s_1	s_2	s_3
e	e	r	r^2	s_1	s_2	s_3
r	r	r^2	e	s_3	s_1	s_2
r^2	r^2	e	r	s_2	s_3	s_1
s_1	s_1	s_2	s_3	e	r	r^2
s_2	s_2	s_3	s_1	r^2	e	r
s_3	s_3	s_1	s_2	r	r^2	e

Cette table est identique à celle du groupe symétrique S_3 donnée en 1.3.5.(d), donc: $D_3 \simeq S_3$.

6.1.2 Second exemple. Soit D_4 l'ensemble des isométries du plan affine euclidien conservant un carré $(ABCD)$. On montre aisément que D_4 est formé de l'identité e, de la rotation r de centre le centre O du carré $(ABCD)$ et d'angle $\pi/2$, de la symétrie centrale r^2 de centre O, de la rotation r^3 de centre O et d'angle $3\pi/2$, des réflexions s_1, s_2 par rapport aux deux médianes du carré, et des réflexions t_1, t_2 par rapport aux deux diagonales du carré. A noter que

$$t_1 = rs_1, \quad s_2 = r^2 s_1, \quad t_2 = r^3 s_1.$$

On vérifie immédiatement que D_4 est un groupe (un sous-groupe du groupe des isométries du plan), d'ordre 8, non abélien, engendré par les deux éléments r et s_1, et dont la table est donnée ci-dessous.

Figure 3

D_4	e	r	r^2	r^3	s_1	s_2	t_1	t_2
e	e	r	r^2	r^3	s_1	s_2	t_1	t_2
r	r	r^2	r^3	e	t_1	t_2	s_2	s_1
r^2	r^2	r^3	e	r	s_2	s_1	t_2	t_1
r^3	r^3	e	r	r^2	t_2	t_1	s_1	s_2
s_1	s_1	t_2	s_2	t_1	e	r^2	r^3	r
s_2	s_2	t_1	s_1	t_2	r^2	e	r	r^3
t_1	t_1	s_1	t_2	s_2	r	r^3	e	r^2
t_2	t_2	s_2	t_1	s_1	r^3	r	r^2	e

6.2 Notion de groupe diédral.

6.2.1 Définition. Pour tout entier $n \geq 2$, on appelle groupe diédral d'ordre $2n$, noté D_n, le sous-groupe des isométries affines conservant un polygone régulier à n côtés (avec la convention que pour $n = 2$, D_2 est le groupe des isométries conservant un segment).

On montre en géométrie que D_n est formé des $2n$ éléments distincts:

$$D_n = \{e, r, r^2, r^3, \ldots, r^{n-1}, s, sr, sr^2, sr^3, \ldots, sr^{n-1}\},$$

vérifiant les relations:

$$r^n = e, \qquad s^2 = e, \qquad sr^k = r^{n-k}s \quad \text{pour tout } 1 \leq k \leq n.$$

6.2.2 Remarques.

(a) Il est clair que D_2, qui est d'ordre 4, est isomorphe au groupe de Klein V. On a vu que D_3, qui est d'ordre 6, est isomorphe au groupe symétrique S_3 (en fait, comme on l'a déjà dit en 3.3.5.(e), il n'existe à isomorphisme près qu'un seul groupe non abélien d'ordre 6). Le groupe D_4 est d'ordre 8, non abélien (mais on pourra voir en exercice qu'il existe d'autres groupes non abéliens d'ordre 8 non isomorphes à D_4, comme le groupe de quaternions Q_8).

(b) Reprenons les notations de la définition 6.2.1 du groupe D_n. Les deux éléments s et r suffisent à obtenir tous les éléments de D_n, au sens où tout élément de D_n peut s'écrire comme le produit d'une puissance de r par une puissance de s, ou encore le produit d'une puissance de s par une puissance de r:

$$e = r^0 = s^0,\ r,\ \ r^2,\ \ \ldots,\ r^{n-1},\ s,\ \ rs = sr^{n-1},\ \ r^2s = sr^{n-2},\ \ r^{n-1}s = sr.$$

En d'autres termes, le groupe D_n est engendré par les deux éléments s et r. Avec les notations de 2.1.1, on a $D_n = \langle X \rangle$ pour $X = \{s, r\}$.

(c) Reprenons les notations de la définition 6.2.1. Notons $H = \langle r \rangle = \{e, r, r^2, \ldots, r^{n-1}\}$ le sous-groupe cyclique de D_n engendré par r. Notons $K = \langle s \rangle = \{e, s\}$ le sous-groupe cyclique de D_n engendré par s.

(1) Il résulte de la remarque (b) ci-dessus que $D_n = HK$.

(2) Il est clair que $H \cap K = \{e\}$.

(3) En revanche, les éléments de H ne commutent pas nécessairement avec les éléments de K. Par exemple $sr \neq rs$ lorsque $n \geq 3$.

Ainsi, D_n n'est pas le produit direct de H par K (au sens de la définition 4.3.2), car la condition (3) n'est pas vérifiée. Elle est ici remplacée par la condition plus faible $HK = KH$, ce qui est équivaut au fait que:

quels que soient $h \in H$ et $k \in K$, il existe $h' \in H$ et $k' \in K$ tels que $hk = k'h'$,

mais sans avoir nécessairement $h = h'$ et $k = k'$. On verra plus loin que cette situation correspond à une notion plus faible que le produit direct (appelée produit semi-direct), et que D_n est le produit semi-direct de H par K.

Chapitre 2

Groupes : groupes quotients

1. Sous-groupes normaux

1.1 Conjugaison.

1.1.1 DÉFINITION. Soit G un groupe. Soient g et g' deux éléments de G. On dit que g' est *conjugué* avec g lorsqu'il existe un élément $x \in G$ tel que $g' = xgx^{-1}$.

(a) Si $g' = xgx^{-1}$, alors $g = x^{-1}g'x = yg'y^{-1}$ pour $y = x^{-1}$, de sorte que g est conjugué avec g'. On dira donc simplement que g et g' sont conjugués.

(b) Tout élément $g \in G$ est conjugué à lui-même (car $g = ege^{-1}$).

(c) La notion de conjugaion n'a bien sûr d'intérêt que pour un groupe G non abélien, car si G est abélien, le seul élément conjugué à un élément quelconque g de G est g lui-même.

(d) Dire que g' est conjugué avec g se traduit par l'existence d'un automorphisme intérieur σ_x tel que $g' = \sigma_x(g)$, ou encore $g = \sigma_x^{-1}(g')$.

1.1.2 PROPOSITION. *Soit G un groupe. La relation "être conjugué" dans G est une relation d'équivalence.*

Preuve. La réflexivité et la symétrie découlent des remarques (a) et (b) ci-dessus. Pour la transitivité, supposons que g' est conjugué avec g, et que g'' est conjugué avec g'. Il existe donc x et y dans G tels que $g' = xgx^{-1}$ et $g'' = yg'y^{-1}$. On a alors $g'' = yxgx^{-1}y^{-1} = (yx)g(yx)^{-1}$, ce qui prouve que g'' est conjugué avec g. □

1.1.3 REMARQUES ET NOTATIONS. Pour tout $g \in G$, la classe d'équivalence de g pour la relation de conjugaison est appelé la classe de conjugaison de g. On la note $\mathrm{cl}(g)$. Rappelons que:

$$\mathrm{cl}(g) = \{g' \in G\,;\, g' \text{ conjugué avec } g\} = \{xgx^{-1}\,;\, x \in G\} = \{\sigma(g)\,;\, \sigma \in \operatorname{Int} G\}.$$

Comme on l'a dit en 1.1.1.(c), cette notion n'a d'intérêt que si G n'est pas abélien car, si G est abélien, on a $\mathrm{cl}(g) = \{g\}$ pour tout $g \in G$. Rappelons aussi que, comme pour toute relation d'équivalence, les classes de conjugaison forment une partition de G.

1.2 Notion de sous-groupe normal.

1.2.1 NOTATION. Soit G un groupe. Pour tout sous-groupe H de G, et pour tout $x \in G$, on note xHx^{-1} l'image de H par l'automorphisme intérieur σ_x :

$$xHx^{-1} = \{xhx^{-1}\,;\, h \in H\} = \sigma_x(H) \quad \text{pour tout } x \in G.$$

D'après la prop. 3.1.3 du chap. 1, c'est un sous-groupe de G. Cette notion n'a d'intérêt que si G n'est pas abélien car, si G est abélien, on a $xhx^{-1} = h$ pour tous $x \in G, h \in H$.

1.2.2 REMARQUES. Soient G un groupe et H un sous-groupe de G. Considérons les quatre assertions suivantes:

(1) pour tout $h \in H$, pour tout $x \in G$, on a $xhx^{-1} = h$,
(2) pour tout $h \in H$, pour tout $x \in G$, on a $xhx^{-1} \in H$,
(3) pour tout $h \in H$, pour tout $x \in G$, il existe $h' \in H$ tel que $xhx^{-1} = h'$,
(4) pour tout $x \in G$, on a $xHx^{-1} = H$.

(a) Il est clair que (1) implique (2), mais la réciproque est fausse. On peut avoir (2) sans avoir (1).

En effet, considérons par exemple, dans le groupe symétrique $S_3 = \{e, \gamma, \gamma^2, \tau_1, \tau_2, \tau_3\}$, le sous-groupe $H = \{e, \gamma, \gamma^2\}$. On a $\tau_1\gamma\tau_1^{-1} = \tau_1\gamma\tau_1 = \gamma^2$. Donc $\tau_1\gamma\tau_1^{-1} \in H$ mais $\tau_1\gamma\tau_1^{-1} \neq \gamma$. Ce qui prouve que l'on n'a pas (1). Mais on a $\tau_1\gamma\tau_1^{-1} = \tau_2\gamma\tau_2^{-1} = \tau_3\gamma\tau_3^{-1} = \gamma^2$ et $\tau_1\gamma^2\tau_1^{-1} = \tau_2\gamma^2\tau_2^{-1} = \tau_3\gamma^2\tau_3^{-1} = \gamma$, qui suffit à prouver que l'on a (2).

(b) Il est clair que, si G est abélien, alors on a (1), mais la réciproque est fausse.

En effet, il suffit de prendre G non abélien et $H = \{e\}$, ou plus généralement $H = Z(G)$ le centre de G (voir 3.5.1 du chap. 1).

(c) Il est clair que (2) est équivalent à (3).

(d) Les assertions (2) et (4) sont équivalentes.

En effet, comme (2) équivaut à $xHx^{-1} \subset H$ pour tout $x \in G$, il est clair que (4) implique (2). Réciproquement, supposons que l'on a (2). On a donc l'inclusion $xHx^{-1} \subset H$; pour l'inclusion réciproque, tout $h \in H$ s'écrit $h = x(x^{-1}hx)x^{-1}$, et comme $x^{-1}hx \in H$ d'après l'hypothèse (2), on a $h \in xHx^{-1}$, ce qui prouve que $H \subset xHx^{-1}$.

1.2.3 Définition. Soient G un groupe et H un sous-groupe de G. On dit que H est *normal dans* G, ou encore *distingué dans* G, lorsque $xHx^{-1} = H$ pour tout $x \in G$. On note alors $H \triangleleft G$.

$$(H \triangleleft G) \Leftrightarrow (xHx^{-1} = H \text{ pour tout } x \in G) \Leftrightarrow (xhx^{-1} \in H \text{ pour tous } h \in H,\, x \in G)$$

• Par exemple, les calculs effectués à la remarque 1.2.2(a) ci-dessus montrent que le sous-groupe $H = \{e, \gamma, \gamma^2\}$ de S_3 est normal dans S_3.

• Ré-insistons sur le fait que la notion de sous-groupe normal n'a d'intérêt que pour les groupes non-abéliens puisqu'il résulte des remarques 1.2.2(a) et 1.2.2(b) que:

tout sous-groupe d'un groupe abélien G est normal dans G.

• Ré-insistons sur le fait vu en 1.2.2.(a) que, si $H \triangleleft G$, on a $xHx^{-1} = H$ pour tout $x \in G$, mais pas nécessairement $xhx^{-1} = h$ pour tous $x \in G, h \in H$.

1.3 Premiers exemples.

1.3.1 Proposition. *Pour tout groupe G, les sous-groupes $\{e\}$ et G sont normaux dans G.*

Preuve. Evident □

1.3.2 Proposition. *Pour tout groupe G, le centre $Z(G)$ est un sous-groupe normal dans G.*

Preuve. Quels que soient $h \in Z(G)$ et $x \in G$, on a $xhx^{-1} = h$ par définition du fait que h est dans le centre de G, donc $xhx^{-1} \in Z(G)$. □

1.3.3 Proposition. *Pour tout morphisme f d'un groupe G dans un groupe G', le noyau* $\operatorname{Ker} f$ *est un sous-groupe normal dans G.*

Preuve. Soient $h \in \operatorname{Ker} f$ et $x \in G$ quelconques. Il s'agit de vérifier que $xhx^{-1} \in \operatorname{Ker} f$. Pour cela, calculons $f(xhx^{-1}) = f(x)f(h)f(x)^{-1}$. Mais $f(h) = e'$, donc $f(xhx^{-1}) = f(x)f(x)^{-1} = e'$, ce qui prouve le résultat voulu. □

1.3.4 Applications. Dans la pratique, reconnaître un sous-groupe donné comme le noyau d'un morphisme est un moyen immédiat et fréquent de montrer qu'il est normal. Par exemple:

(i) $A_n \triangleleft S_n$,

En effet, le groupe alterné A_n n'est autre que le noyau du morphisme signature $\varepsilon : S_n \to \{1, -1\}$.

(ii) $\mathrm{SL}_n(\mathbb{R}) \triangleleft \mathrm{GL}_n(\mathbb{R})$.

En effet, le groupe spécial linéaire $\mathrm{SL}_n(\mathbb{R})$ n'est autre que le noyau du morphisme déterminant $\mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$.

1.3.5 Proposition. *Si G est un groupe fini d'ordre pair $2n$ et si H est un sous-groupe d'ordre n de G, alors H est normal dans G.*

Preuve. Notons $H = \{h_1, h_2, h_3, \dots, h_n\}$, avec $h_1 = e$. Fixons un élément $y \in G$ tel que $y \notin H$ (il en existe car $|G| = 2n$ alors que $|H| = n$). Notons yH l'ensemble des produits par y à gauche des éléments de H. Comme $yh_i = yh_j$ si et seulement si $h_i = h_j$ (en multipliant à gauche par y^{-1}), on déduit que $yH = \{yh_1, yh_2, \dots, yh_n\}$ est formé de n éléments distincts. S'il existait un élément commun à H et yH, il s'écrirait $yh_i = h_j$, ce qui est impossible car on aurait alors $y = h_jh_i^{-1} \in H$, ce qui est contraire au choix de y. On conclut donc que $G = H \cup yH$ et $H \cap yH = \emptyset$.

Dès lors, soient h_i un élément quelconque de H et x un élément quelconque de G. Si $x \in H$, alors xh_ix^{-1} est le produit de trois éléments de H, donc appartient à H. Si $x \notin H$, alors $x \in yH$, donc il existe $h_j \in H$ tel que $x = yh_j$. Donc $xh_ix^{-1} = yh_jh_ih_j^{-1}y^{-1} = yh_\ell y^{-1}$ où l'on a posé $h_\ell = h_jh_ih_j^{-1} \in H$. Si $yh_\ell y^{-1}$ n'appartenait pas à H, il appartiendrait à yH, donc on aurait $yh_\ell y^{-1} = yh_k$ pour un certain $h_k \in H$, d'où $h_\ell y^{-1} = h_k$, donc $y = h_k^{-1}h_\ell$ appartiendrait à H. Comme ce n'est pas le cas, c'est que $yh_\ell y^{-1} \in H$, c'est-à-dire $xh_ix^{-1} \in H$. □

On verra plus loin que cette même preuve permet de montrer un résultat analogue dans un cadre un peu plus général pour G non nécessairement fini.

1.3.6 Proposition. *Si H et K sont deux sous-groupes d'un groupe G tels que $H \triangleleft G$ et $K \triangleleft G$, alors $H \cap K \triangleleft G$.*

Preuve. Immédiate; laissée au lecteur en exercice. □

1.3.7 Remarque. Attention: si H et K sont deux sous-groupes d'un groupe G tels que $K \subset H$,

$$(K \triangleleft H \text{ et } H \triangleleft G) \text{ n'implique pas } (K \triangleleft G).$$

Contre-exemple. Considérons le groupe alterné A_4, en reprenant pour ses éléments toutes les notations du paragraphe 5.4.4 du chapitre 1. Rappelons d'abord que:

pour toute permutation $\sigma \in S_4$ et toute transposition $[i, j]$, on a: $\sigma[i, j]\sigma^{-1} = [\sigma(i), \sigma(j)]$.

Considérons dans A_4 le sous-groupe $V = \{e, a, b, c\}$. Pour tout $\sigma \in A_4$, on a:

$$\sigma a\sigma^{-1} = \sigma[1, 2][3, 4]\sigma^{-1} = \sigma[1, 2]\sigma^{-1}\sigma[3, 4]\sigma^{-1} = [\sigma(1), \sigma(2)][\sigma(3), \sigma(4)] \in V.$$

On montre de même que $\sigma b\sigma^{-1} \in V$ et $\sigma c\sigma^{-1} \in V$ pour tout $\sigma \in A_4$. On conclut que $V \triangleleft A_4$.

Considérons dans A_4 le sous-groupe $K = \{e, a\}$ de V, donc de A_4. Il n'est pas normal dans A_4, car par exemple, $x_1ax_1^{-1} = x_1ay_1 = b \notin K$. Et pourtant K est normal dans V puisque V est abélien.

1.3.8 Exercice. Montrer que, pour tout groupe G, on a: $\operatorname{Int} G \triangleleft \operatorname{Aut} G$, (voir chap. 1, 3.5.3).

1.4 Classe modulo un sous-groupe, indice.

1.4.1 Définition. Soit G un groupe. Soit H un sous-groupe. Pour tout $x \in G$, on note:

$$xH = \{xh\,;\, h \in H\} \quad \text{et} \quad Hx = \{hx\,;\, h \in H\}.$$

Le sous-ensemble xH s'appelle la classe à gauche de x modulo H. Le sous-ensemble Hx s'appelle la classe à droite de x modulo H.

(a) Pour tout $x \in G$, H est en bijection avec xH via $h \mapsto xh$, et en bijection avec Hx via $h \mapsto hx$.

(b) En particulier, pour $x = e$, on a: $eH = He = H$.

(c) Pour tout $x \in G$, on a $x \in xH$ et $x \in Hx$, (car $x = xe = ex$ et $e \in H$).

1.4.2 Lemme. *Soient G un groupe et H un sous-groupe de G.*

(i) Pour tous $x, y \in G$, on a:

$$(xH = yH) \Leftrightarrow (x^{-1}y \in H) \quad \text{et} \quad (Hx = Hy) \Leftrightarrow (xy^{-1} \in H).$$

(ii) *Les classes à gauche modulo H forment une partition de G, (de même que les classes à droite).*

(iii) *L'ensemble des classes à droite modulo H est en bijection avec l'ensemble des classes à gauche modulo H, via la bijection $Hx \mapsto x^{-1}H$.*

(iv) *Pour tout sous-groupe H de G, on a:*

$$(H \triangleleft G) \Leftrightarrow (xH = Hx \text{ pour tout } x \in G).$$

Preuve. (i) Supposons que $xH = yH$. En particulier, comme $y \in yH$, on a $y \in xH$, donc il existe $h \in H$ tel que $y = xh$, d'où $x^{-1}y = h \in H$. Réciproquement, supposons que $x^{-1}y \in H$. Posons $h_0 = x^{-1}y$. Soit $z \in yH$ quelconque. Il existe $h \in H$ tel que $z = yh = xh_0h$, qui appartient à xH puisque $h_0h \in H$. D'où $yH \subseteq xH$. Soit $z' \in xH$ quelconque. Il existe $h' \in H$ tel que $z' = xh' = yh_0^{-1}h'$, qui appartient à yH puisque $h_0^{-1}h \in H$. D'où $xH \subseteq yH$, et finalement $xH = yH$. On raisonne de même pour les classes à droite.

(ii) On a vu que tout $x \in G$ vérifie $x \in xH$, donc G est égal à la réunion des classes à gauche. Il reste à montrer que deux classes distinctes sont disjointes, ou encore que deux classes non disjointes sont égales. Considérons donc xH et yH (avec $x, y \in G$) tel que $xH \cap yH$ contienne au moins un élément z. Il existe donc $h, h' \in H$ tels que $z = xh = yh'$. Dans ce cas, $x^{-1}y = h(h')^{-1} \in H$, d'où $xH = yH$ d'après le point (i). Ainsi $xH = yH$ dès lors que $xH \cap yH \neq \emptyset$. La preuve à droite est identique.

(iii) Soit φ l'application $Hx \mapsto x^{-1}H$ de l'ensemble des classes à droite dans l'ensemble des classes à gauche. Il est clair qu'elle est surjective. De plus, si $x, y \in G$ vérifient $x^{-1}H = y^{-1}H$, alors $xy^{-1} \in H$ d'après la première équivalence du (i), d'où $Hx = Hy$ d'après la seconde équivalence du (i). Ce qui prouve que φ est injective, et donc finalement bijective.

(iv) Supposons que $xH = Hx$ pour tout $x \in G$. Alors quels que soient $x \in G$ et $h \in H$, il existe $h' \in H$ tel que $xh = h'x$, d'où $xhx^{-1} \in H$. Ceci prouve que $H \lhd G$. Réciproquement, supposons que $H \lhd G$. Fixons $x \in G$ quelconque. Tout élément z de xH s'écrit $z = xh$ avec $h \in H$, donc $z = xhx^{-1}x$. Mais $xhx^{-1} \in H$ par normalité de H, de sorte que $z = (xhx^{-1})x \in Hx$. Ceci prouve que $xH \subseteq Hx$. L'inclusion réciproque se montre de même, ce qui achève la preuve. □

1.4.3 Définition. Soient G un groupe et H un sous-groupe de G. On appelle *indice de H dans G*, noté $[G : H]$, le cardinal de l'ensemble des classes modulo H (à droite ou à gauche indifféremment d'après le (iii) du lemme précédent). On dit que H est d'indice fini lorsque ce cardinal est fini.

1.4.4 Proposition. Si G est un groupe fini, alors tout sous-groupe H de G est d'indice fini dans G, et on a d'après le théorème de Lagrange l'égalité:

$$|G| = |H| \times [G : H].$$

Preuve. Notons $|G| = m$, $|H| = n$, et $[G : H] = p$. Par définition, p est le nombre de classes (à gauche par exemple) modulo H. Or, d'après la remarque (a) de 1.4.1, chacune des classes est en bijection avec H, donc admet exactement n éléments. Il résulte alors du point (ii) du lemme 1.4.2 que $m = pn$. □

A noter qu'un sous-groupe infini H d'un groupe infini G peut très bien être d'indice fini (prendre par exemple $G = \mathrm{O}_n(\mathbb{R})$ et $H = \mathrm{SO}_n(\mathbb{R})$).

1.4.5 Proposition. *Soit G un groupe (fini ou non). Tout sous-groupe H d'indice 2 dans G est normal dans G.*

Preuve. Par hypothèse, il n'y a que deux classes à gauche modulo H; l'une est $eH = H$ qui, d'après le point (i) de 1.4.2, est aussi la classe de tout élément de H, et l'autre yH (avec $y \notin H$) est donc la classe commune à tous les éléments de G qui ne sont pas dans H. De même, il n'y a que deux classes à droite modulo H; l'une est $He = H$ qui, d'après le point (i) de 1.4.2, est aussi la classe de tout élément de H, et l'autre Hz (avec $z \notin H$) est donc la classe commune à tous les éléments de G qui ne sont pas dans H. Comme les classes forment une partition de G, il en résulte que $yH = Hz$. Dès lors, quel que soit $x \in G$, on a $xH = H = Hx$ si $x \in H$, et $xH = yH = Hz = Hx$ si $x \notin H$. Dans les deux cas, on a $xH = Hx$. Ce qui prouve que $H \lhd G$. □

Dans le cas particulier où G est fini d'ordre m, si H est d'indice 2 dans G, on a (d'après la proposition 1.4.4) m pair et H d'ordre $n = m/2$, de sorte que l'on retrouve la proposition 1.3.5.

1.5 Normalisateur.

1.5.1 Proposition et définition. *Soient G un groupe et H un sous-groupe de G. L'ensemble $N_G(H) = \{x \in G\,;\, xHx^{-1} = H\}$ est un sous-groupe de G, appelé le normalisateur dans G de H.*

Preuve. Vérification immédiate, laissée au lecteur. □

1.5.2 Proposition. *Soient G un groupe et H un sous-groupe de G. On a:*

(i) $H \lhd N_G(H)$,

(ii) *$N_G(H)$ est le plus grand sous-groupe de G dans lequel H est normal;*

(iii) *en particulier $H \lhd G$ si et seulement si $N_G(H) = G$.*

Preuve. Vérification immédiate, laissée au lecteur. □

2.1 Congruence modulo un sous-groupe normal.

2.1.1 Proposition et définition. *Soient G un groupe et H un sous-groupe de G. On suppose que $H \lhd G$. La relation binaire définie sur G par:*

$$\text{pour tous } x, y \in G,\ \ x \equiv y \ \ \text{lorsque} \ \ xy^{-1} \in H$$

est une relation d'équivalence dans G, appelée la congruence modulo H, ou encore l'équivalence modulo H, dont les classes d'équivalence vérifient:

$$\text{pour tout } x \in G,\ \ \overline{x} = xH = Hx.$$

Preuve. Pour tout $x \in G$, on a $x \equiv x$ puisque $xx^{-1} = e \in H$. Donc $\equiv$ est réflexive. Si $x, y \in G$ vérifient $x \equiv y$, alors $xy^{-1} \in H$, donc par passage à l'inverse $yx^{-1} \in H$, d'où $y \equiv x$. Donc $\equiv$ est symétrique. Si $x, y, z \in G$ vérifient $x \equiv y$ et $y \equiv z$, alors $xy^{-1} \in H$ et $yz^{-1} \in H$, donc par produit $xy^{-1}yz^{-1} \in H$, c'est-à-dire $xz^{-1} \in H$, d'où $x \equiv z$. Donc $\equiv$ est transitive, ce qui achève de montrer que $\equiv$ est une relation d'équivalence.

Pour tout $x \in G$, la classe d'équivalence de x est par définition $\overline{x} = \{y \in G\,;\, y \equiv x\}$. Or $y \equiv x$ si et seulement si $yx^{-1} \in H$, ce qui équivaut à l'existence d'un élément $h \in H$ tel que $y = hx$. Ceci prouve que $\overline{x} = Hx$, et comme $H \lhd G$, il résulte de 1.4.2.(iv) que l'on a aussi $\overline{x} = xH$. □

2.1.2 Remarques. Soient G un groupe et H un sous-groupe normal de G.

(a) Pour tout $x \in G$, $\overline{x}$ est par définition l'ensemble des éléments $y \in G$ tels que $y \equiv x$. Tout élément y de $\overline{x}$ s'appelle un représentant de $\overline{x}$.

$$(\ y \in \overline{x}\ ) \Leftrightarrow (\ y \equiv x\ ) \Leftrightarrow (\ yx^{-1} \in H\ ) \Leftrightarrow (\ \exists\ h \in H,\ y = hx) \Leftrightarrow (y \in Hx\ )$$

Comme $Hx = xH$ puisque $H \lhd G$, on a aussi:

$$(\ y \in \overline{x}\ ) \Leftrightarrow (\ y \in xH\ ) \Leftrightarrow (\ \exists\ h' \in H,\ y = xh') \Leftrightarrow (\ x^{-1}y \in H\ )$$

En particulier, x lui-même est un représentant de sa classe: $x \in \overline{x}$ pour tout $x \in G$.

(b) Deux éléments de G ont la même classe si et seulement s'ils sont congrus modulo H:

$$\text{pour tous } x, y \in G,\ \ \overline{x} = \overline{y} \ \text{ si et seulement si } \ x \equiv y.$$

(c) On a en particulier: $\overline{e} = H$.

2.1.3 Notations. L'ensemble quotient de G par la relation d'équivalence $\equiv$ (qui est par définition l'ensemble des classes d'équivalence des éléments de G) est ordinairement noté $G/\equiv$. Comme ici la relation $\equiv$ est défini à partir du sous-groupe normal H, on convient de noter G/H l'ensemble quotient.

$$G/H = \{\,\overline{x}\ ;\ x \in G\,\}.$$

Rappelons que l'on appelle surjection canonique l'application $G \to G/H$ qui, à tout élément de G, associe sa classe d'équivalence.

$$\begin{aligned} p:\ G &\longrightarrow G/H \\ x &\longmapsto \overline{x} \end{aligned}$$

L'application p est surjective par construction, mais en général non injective (car $p(x) = p(y)$ dès lors que $x \equiv y$, même si $x \neq y$).

Notons enfin que, d'après 1.4.3, le cardinal (fini ou infini) de G/H n'est autre que l'indice $[G : H]$ de H dans G.

2.2 Notion de groupe quotient.

2.2.1 Commentaire préliminaire. Soient G un groupe et H un sous-groupe normal de G. Le but du théorème fondamental suivant est de munir l'ensemble quotient G/H d'une structure de groupe, déduite de celle de G. L'idée la plus naturelle pour cela est de définir la loi interne dans G/H par: $\overline{x}.\overline{y} = \overline{xy}$ pour tous $\overline{x}, \overline{y} \in G/H$. Mais il y a un point important auquel il faut faire attention ! Le produit de deux classes ainsi défini ne dépend-il pas des représentants x et y que l'on choisit pour poser $\overline{xy}$? En d'autres termes, si l'on prend d'autres représentants $x' \in \overline{x}$ et $y' \in \overline{y}$, (il n'y a aucune raison alors pour que $xy = x'y'$) est-il clair que $\overline{xy} = \overline{x'y'}$? C'est bien sûr indispensable pour que la définition de la loi dans G/H ait un sens. Et c'est effectivement le cas comme le montrent les calculs ci-dessous.

Supposons que $x' \in \overline{x}$ et $y' \in \overline{y}$. Alors $x'x^{-1} \in H$ et $y'y^{-1} \in H$. On a:

$$(x'y')(xy)^{-1} = x'y'y^{-1}x^{-1} = x'y'y^{-1}(x')^{-1}x'x^{-1} = \big[x'(y'y^{-1})(x')^{-1}\big]x'x^{-1}.$$

Or, $y'y^{-1} \in H$ par hypothèse et donc, parce que H est supposé normal dans G (c'est là qu'intervient cette hypothèse fondamentale), on a aussi $x'(y'y^{-1})(x')^{-1} \in H$. Finalement comme par ailleurs $x'x^{-1} \in H$, on conclut que $[x'(y'y^{-1})(x')^{-1}]x'x^{-1}$ appartient à H comme produit de deux éléments de H. On a ainsi vérifié que $(x'y')(xy)^{-1} \in H$, donc $\overline{xy} = \overline{x'y'}$.

2.2.2 Théorème. *Soient G un groupe et H un sous-groupe de G. On suppose $H \triangleleft G$.*

(i) *On définit une loi de composition interne dans G/H en posant, indépendamment des représentants choisis:*

$$\overline{x}.\overline{y} = \overline{xy} \quad \text{pour tous } x, y \in G.$$

(ii) *Cette loi munit l'ensemble G/H d'une structure de groupe, appelé le groupe quotient de G par H.*

(iii) *La surjection canonique $p : G \to G/H$ est alors un morphisme du groupe G dans le groupe quotient G/H.*

Preuve. Le point (i) a été montré ci-dessus en 2.2.1. Pour (ii), l'associativité de la loi définie dans G/H est évidente, car pour tous $x, y, z \in G$ on a $\overline{x}.(\overline{y}.\overline{z}) = \overline{x(yz)} = \overline{(xy)z} = (\overline{x}.\overline{y}).\overline{z}$. De même, pour tout $x \in G$, on a $\overline{x}.\overline{e} = \overline{xe} = \overline{x}$ et $\overline{x}.(\overline{x})^{-1} = \overline{xx^{-1}} = \overline{e}$, ce qui montre que G/H est un groupe. Enfin, le point (iii) est clair puisque, par définition, on a $p(xy) = \overline{xy} = \overline{x}.\overline{y} = p(x)p(y)$ pour tous $x, y \in G$. □

Retenons en particulier que l'élément neutre du groupe quotient G/H est $\overline{e} = H$ et, pour tout $x \in G$, le symétrique dans G/H de $\overline{x}$ est $\overline{x}^{-1} = \overline{x^{-1}}$.

2.2.3 Exemples.

(a) Soit G un groupe. Si l'on prend $H = \{e\}$, alors $\overline{x} = \{x\}$ pour tout $x \in G$ (car $x \equiv y$ est alors équivalent à $xy^{-1} = e$, c'est-à-dire $y = x$). Il en résulte $G/\{e\} \simeq G$, via l'isomorphisme $x \mapsto \overline{x}$.

(b) Soit G un groupe. Si l'on prend $H = G$, alors $\overline{x} = \overline{e}$ pour tout $x \in G$ (car on a trivialement $xe^{-1} \in G$ c'est-à-dire $x \equiv e$ pour tout $x \in G$). Il n'y a donc qu'une seule classe, d'où $G/G = \{\overline{e}\}$ est le groupe trivial à un élément.

(c) Prenons $G = S_3 = \{e, \gamma, \gamma^2, \tau_1, \tau_2, \tau_3\}$ et $H = A_3 = \{e, \gamma, \gamma^2\} \triangleleft S_3$. On a $\overline{e} = H = \{e, \gamma, \gamma^2\}$ et $\overline{\tau_1} = \tau_1 H = \{\tau_1 e, \tau_1\gamma, \tau_1\gamma^2\} = \{\tau_1, \tau_2, \tau_3\} = \overline{\tau}_2 = \overline{\tau}_3$. Il n'y a que deux classes distinctes, donc $S_3/A_3 = \{\overline{e}, \overline{\tau}_1\} \simeq C_2$.

(d) Prenons $G = \mathrm{O}_n(\mathbb{R})$ et $H = \mathrm{SO}_n(\mathbb{R}) \triangleleft \mathrm{O}_n(\mathbb{R})$. On a $\overline{e} = \mathrm{SO}_n(\mathbb{R})$. Soit $s \in \mathrm{O}_n(\mathbb{R})$ tel que $s \notin \mathrm{SO}_n(\mathbb{R})$ quelconque. Pour tout élément $t \in \mathrm{O}_n(\mathbb{R})$ tel que $t \notin \mathrm{SO}_n(\mathbb{R})$, on a $st^{-1} \in \mathrm{SO}_n(\mathbb{R})$ (le produit de deux isométries négatives est une isométrie positive). Il n'y a que deux classes distinctes (la classe de toutes les isométries positives qui est égale à $\mathrm{SO}_n(\mathbb{R})$ et la classe de toutes les isométries négatives), donc $\mathrm{O}_n(\mathbb{R})/\mathrm{SO}_n(\mathbb{R}) \simeq C_2$.

Les exemples ci-dessus ne sont que des cas particuliers des résultats généraux que l'on verra un peu plus loin.

2.2.4 Remarques.

(a) Il est clair que, si G est abélien, alors G/H est abélien. Mais réciproquement on peut avoir G/H abélien sans que G le soit (voir les exemples (c) et (d) ci-dessus).

(b) Si H est normal et d'indice fini dans G, alors G/H est fini et l'on a d'après la définition 1.4.3:
$$|G/H| = [G : H].$$

(c) Si G est fini et H est normal dans G, alors G/H est fini et l'on a d'après la proposition 1.4.4:
$$|G/H| = |G|/|H|.$$
Attention, on peut avoir G/H fini sans que ni G ni H le soit (voir l'exemple (d) ci-dessus).

2.3 Premier théorème d'isomorphisme.

2.3.1 Théorème. *Soit G un groupe. Pour tout groupe G' et tout morphisme de groupes $f : G \to G'$, le groupe quotient de G par le sous-groupe normal $\operatorname{Ker} f$ est isomorphe au sous-groupe $\operatorname{Im} f$ de G'. On note:*
$$\operatorname{Ker} f \lhd G \qquad \textit{et} \qquad G/\operatorname{Ker} f \simeq \operatorname{Im} f.$$

Preuve. On a déjà montré en 1.3.3 que $\operatorname{Ker} f \lhd G$. Pour tout $\overline{x} \in G/\operatorname{Ker} f$, posons $\varphi(\overline{x}) = f(x) \in \operatorname{Im} f$. Cette définition est indépendante du choix du représentant dans $\overline{x}$; en effet, si l'on choisit un autre représentant $y \in \overline{x}$, on a par définition $xy^{-1} \in \operatorname{Ker} f$, donc $f(xy^{-1}) = e$, d'où $f(x)f(y)^{-1} = e$, c'est-à-dire $f(x) = f(y)$, ou encore $\varphi(\overline{x}) = \varphi(\overline{y})$. On définit donc bien une application:
$$\begin{aligned} \varphi :\ G/\operatorname{Ker} f &\longrightarrow \operatorname{Im} f \\ \overline{x} &\longmapsto f(x) \end{aligned}$$
L'application φ est surjective par construction. Il est clair que c'est un morphisme de groupes puisque, pour tous $\overline{x}, \overline{y} \in G/\operatorname{Ker} f$, on a $\varphi(\overline{x}.\overline{y}) = \varphi(\overline{xy}) = f(xy) = f(x)f(y) = \varphi(\overline{x})\varphi(\overline{y})$. Vérifions qu'elle est injective. Pour cela, considérons $\overline{x} \in \operatorname{Ker} \varphi$. On a alors $\varphi(\overline{x}) = e'$, le neutre du groupe d'arrivée G'. D'où $f(x) = e'$, c'est-à-dire $x \in \operatorname{Ker} f$, ou encore $\overline{x} = \overline{e}$. Ceci montre que $\operatorname{Ker} \varphi = \{\overline{e}\}$, donc φ est injective. On conclut que φ est un isomorphisme de groupes de $G/\operatorname{Ker} f$ sur $\operatorname{Im} f$. □

2.3.2 Remarque et exemples. Le théorème ci-dessus peut se déduire d'une forme plus générale que l'on verra plus loin en 3.1. La forme particulière $G/\operatorname{Ker} f \simeq \operatorname{Im} f$ est cependant d'un usage tellement fréquent qu'il nous a semblé utile de la dégager immédiatement.

(a) Exemple: considérons le morphisme déterminant $\text{dét} : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$. Il est clairement surjectif (car pour tout réel non-nul λ, on peut trouver des matrices $A \in \mathrm{GL}_n(\mathbb{R})$ telles que $\text{dét}(A) = \lambda$), de sorte que $\operatorname{Im} \text{dét} = \mathbb{R}^*$. Par ailleurs, $\operatorname{Ker} \text{dét} = \mathrm{SL}_n(\mathbb{R})$ par définition. On conclut que:
$$\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \simeq \mathbb{R}^*.$$

(b) Exemple: considérons le morphisme signature $\epsilon : S_n \to C_2 = \{+1, -1\}$. Il est clairement surjectif, de sorte que $\operatorname{Im} \epsilon = C_2$. Par ailleurs, $\operatorname{Ker} \epsilon = A_n$ par définition. On conclut que:
$$S_n/A_n \simeq C_2.$$

2.3.3 Corollaire. *Pour tout groupe G, on a: $Z(G) \lhd G$ et $G/Z(G) \simeq \operatorname{Int} G$.*

Preuve. Résulte immédiatement de 1.3.2, et du point (iii) de la proposition 3.5.3 du chapitre 1. □

2.3.4 Corollaire. *Soit G un groupe. On suppose que G est le produit direct de deux sous-groupes H et K. Alors:*
$$(\ H \lhd G \ \text{ et } \ G/H \simeq K\ ) \quad \text{et} \quad (\ K \lhd G \ \text{ et } \ G/K \simeq H\ ).$$

Preuve. D'après la remarque 4.3.3 du chapitre 1, pour tout élément $x \in G$, il existe $h \in H$ et $k \in K$ uniques tels que $x = hk = kh$; posons $f_1(x) = h$ et $f_2(x) = k$. Il est facile de vérifier (écrivez les détails) que $f_1 : G \to H$ et $f_2 : G \to K$ sont des morphismes de groupes, qu'ils sont surjectifs, de noyaux respectifs $\operatorname{Ker} f_1 = K$ et $\operatorname{Ker} f_2 = H$. D'où le résultat en appliquant le théorème 2.3.1. □

2.4 Exemple: groupe dérivé et abélianisé.

2.4.1 Définitions et notations. Soit G un groupe. Pour tous $x, y \in G$, on appelle *commutateur* de x et y l'élément:

$$[x, y] := x^{-1}y^{-1}xy.$$

L'inverse d'un commutateur est un commutateur, mais le produit de deux commutateurs n'est a priori pas un commutateur. Les commutateurs ne constituent donc pas un groupe; on considère alors le sous-groupe engendré par les commutateurs (qui est ici l'ensemble de tous les produits d'un nombre fini de commutateurs).

On appelle *groupe dérivé* de G, noté $D(G)$, le sous-groupe de G engendré par les commutateurs.

Cette notion n'a d'intérêt que pour des groupes non abéliens, puisqu'il est clair que:

$$(\ G \text{ abélien }) \Leftrightarrow (\ [x, y] = e \text{ pour tous } x, y \in G\ ) \Leftrightarrow (\ D(G) = \{e\}\ )$$

2.4.2 Proposition et définition. *Soit G un groupe.*

(i) $D(G) \lhd G$

(ii) *Pour tout sous-groupe $N \lhd G$, on a: (G/N abélien) $\Leftrightarrow$ ($D(G) \subseteq N$).*

(iii) *En particulier, $G/D(G)$ est un groupe abélien, appelé l'abélianisé de G.*

Preuve. Soient $x, y \in G$ quelconques. Considérons le commutateur $c = x^{-1}y^{-1}xy$. Pour tout $z \in G$, on calcule le conjugué de c par z:

$$zcz^{-1} = zx^{-1}y^{-1}xyz^{-1} = zx^{-1}z^{-1}zy^{-1}z^{-1}zxz^{-1}zyz^{-1} = (zxz^{-1})^{-1}(zyz^{-1})^{-1}(zxz^{-1})(zyz^{-1}).$$

On déduit que zcz^{-1} est un commutateur, et ceci pour tout commutateur c et tout $z \in G$. Soit alors $d \in D(G)$ quelconque. Comme on l'a remarqué en 2.4.1, $d = c_1c_2c_3 \ldots c_p$, avec $c_1, c_2, c_3, \ldots, c_p$ des commutateurs. Pour tout $z \in G$, il vient $zdz^{-1} = zc_1c_2c_3 \ldots c_pz^{-1} = zc_1z^{-1}zc_2z^{-1}zc_3z^{-1} \ldots zc_pz^{-1}$. Donc zdz^{-1} est, d'après l'étape précédente, un produit de commutateurs. On conclut que $zdz^{-1} \in D(G)$ pour tous $d \in D(G)$ et $z \in G$. Ce qui prouve (i).

Pour (ii), fixons un sous-groupe N normal dans G. Supposons G/N abélien. Pour tous $x, y \in G$, on a $\overline{xy} = \overline{yx}$, donc $\overline{x^{-1}y^{-1}xy} = \overline{e}$, ou encore $x^{-1}y^{-1}xy \in N$. Ainsi, le sous-groupe N contient tous les commutateurs d'éléments de G. Comme $D(G)$ est par définition le plus petit sous-groupe de G qui contient les commutateurs, on conclut que $D(G) \subseteq N$. La réciproque s'obtient en remontant les mêmes calculs. Ceci prouve (ii), et (iii) s'en déduit immédiatement pour $N = D(G)$. □

2.5 Exemple: quotients $\mathbb{Z}/n\mathbb{Z}$.

2.5.1 Attention ! Ce paragraphe étant consacré aux sous-groupes de $\mathbb{Z}$ et aux quotients correspondants, on abandonne provisoirement la notation multiplicative: le groupe $\mathbb{Z}$ est muni de l'addition usuelle des entiers, on note naturellement $x + y$ ce que l'on notait xy dans le cadre général, le neutre que l'on notait e est ici 0, le symétrique de x (que l'on notait x^{-1} dans le cadre général) est ici l'opposé $-x$, et on note $nx = x + x + \cdots + x$ ce que l'on notait x^n (pour $n \in \mathbb{Z}$). On pose enfin:

$$n\mathbb{Z} = \{nx\,;\, x \in \mathbb{Z}\}, \text{ pour tout } n \in \mathbb{Z}.$$

2.5.2 Proposition. *Le groupe additif $\mathbb{Z}$ vérifie les propriétés suivantes.*

(i) *Le groupe $\mathbb{Z}$ muni de l'addition est monogène infini, les générateurs de $\mathbb{Z}$ sont 1 et -1, et tout groupe monogène infini est isomorphe à $\mathbb{Z}$.*

(ii) *Pour tout $n \in \mathbb{Z}$, l'ensemble $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$, qui est le sous-groupe engendré par n, et l'on a: $n\mathbb{Z} = n'\mathbb{Z}$ si et seulement si $n' = n$ ou $n' = -n$.*

(iii) *Réciproquement, pour tout sous-groupe H de $\mathbb{Z}$, il existe un unique $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.*

Preuve. L'isomorphisme du (i) a été vu au 3.3.5.(c) du chapitre 1. Le reste se déduit alors immédiatement des résultats analogues vus en notation multiplicative au chapitre 1, en particulier 2.3.4 et 2.2.2.
□

2.5.3 REMARQUES. Le groupe $\mathbb{Z}$ étant abélien, tous ses sous-groupes sont normaux; d'après la proposition précédente, ils sont de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$. Par définition de la congruence modulo le sous-groupe $n\mathbb{Z}$, on a pour tous $x, y \in \mathbb{Z}$:

$$(\ x \text{ et } y \text{ congrus modulo } n\mathbb{Z}\ ) \Leftrightarrow (\ x - y \in n\mathbb{Z}\ ) \Leftrightarrow (\ \text{il existe } z \in \mathbb{Z} \text{ tel que } x - y = nz\ ).$$

On retrouve donc la notion de congruence modulo n de l'arithmétique élémentaire.
Le groupe quotient est naturellement noté $\mathbb{Z}/n\mathbb{Z}$. Ses éléments sont notés $\overline{x}$, avec $x \in \mathbb{Z}$. Sa loi est l'addition déduite de celle de $\mathbb{Z}$ par passage aux classes, c'est-à-dire:

$$\overline{x+y} = \overline{x} + \overline{y} \text{ pour tous } x, y \in \mathbb{Z}.$$

En particulier, son neutre est $\overline{0} = n\mathbb{Z}$.

Convention. Puisqu'il résulte des exemples 2.2.3.(a) et 2.2.3.(b) que $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}/\{0\} \simeq \mathbb{Z}$ et que $\mathbb{Z}/1\mathbb{Z} = \mathbb{Z}/\mathbb{Z} = \{\overline{e}\}$, on ne considérera plus dans la suite les cas triviaux $n = 0$ et $n = 1$.

2.5.4 THÉORÈME. *Fixons un entier $n > 1$.*

(i) *Le groupe $\mathbb{Z}/n\mathbb{Z}$ est fini d'ordre n, et l'on a $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$.*

(ii) *Le groupe additif $\mathbb{Z}/n\mathbb{Z}$ est cyclique d'ordre n, c'est-à-dire isomorphe au groupe cyclique C_n.*

(iii) *Les générateurs du groupe $\mathbb{Z}/n\mathbb{Z}$ sont les classes $\overline{k}$ des entiers k qui sont premiers avec n.*

(iv) *Pour tout diviseur q de n, il existe un et un seul sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre q, qui est le sous-groupe cyclique engendré par $\overline{d}$, où $n = dq$.*

Preuve. D'après le 3.3.5.(a) du chapitre 1, il n'existe à isomorphisme près qu'un groupe cyclique d'ordre n, noté $C_n = \{e, x, x^2, x^3, \dots, x^{n-1}\}$ suivant la proposition 2.1.5 du chapitre 1. Définissons alors l'application:

$$\begin{aligned} f :\ \mathbb{Z} &\longrightarrow C_n \\ k &\longmapsto x^k \end{aligned}$$

On a $f(k+h) = x^{k+h} = x^k x^h = f(k)f(h)$ pour tous $h, k \in \mathbb{Z}$, ce qui prouve que f est un morphisme de groupes. Il est clair que f est surjective puisque tout élément de C_n est de la forme x^k pour un entier k. Enfin un entier k appartient à $\operatorname{Ker} f$ si et seulement si $x^k = e$, ce qui, puisque x est d'ordre n, équivaut au fait que k est multiple de n; en d'autres termes $\operatorname{Ker} f = n\mathbb{Z}$. On déduit alors du théorème 2.3.1 que $\mathbb{Z}/n\mathbb{Z} \simeq C_n$. Les points (i), (iii) et (iv) se déduisent alors immédiatement des résultats analogues démontrés en notation multiplicative au chapitre 1 (en particulier 2.2.3 et 2.3.2). □

EXEMPLES ($2 \leq n \leq 5$):

	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

2.5.5 COROLLAIRE (écriture additive du théorème chinois). *Pour tous $n > 1$ et $m > 1$, on a:*

$$(\ \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/nm\mathbb{Z}\ ) \ \Leftrightarrow\ (\ n \text{ et } m \text{ premiers entre eux}\ ).$$

EXEMPLES:

	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$
$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$
$(\overline{0},\overline{1})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{1},\overline{0})$
$(\overline{1},\overline{0})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$
$(\overline{1},\overline{1})$	$(\overline{1},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{0})$

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ n'est pas cyclique; c'est le groupe de Klein $V = \{e, a, b, c\}$ pour:
$e = (\overline{0},\overline{0})$, $a = (\overline{0},\overline{1})$, $b = (\overline{1},\overline{0})$ et $c = (\overline{1},\overline{1})$.

	$(\overline{0},\widetilde{0})$	$(\overline{1},\widetilde{1})$	$(\overline{0},\widetilde{2})$	$(\overline{1},\widetilde{0})$	$(\overline{0},\widetilde{1})$	$(\overline{1},\widetilde{2})$
$(\overline{0},\widetilde{0})$	$(\overline{0},\widetilde{0})$	$(\overline{1},\widetilde{1})$	$(\overline{0},\widetilde{2})$	$(\overline{1},\widetilde{0})$	$(\overline{0},\widetilde{1})$	$(\overline{1},\widetilde{2})$
$(\overline{1},\widetilde{1})$	$(\overline{1},\widetilde{1})$	$(\overline{0},\widetilde{2})$	$(\overline{1},\widetilde{0})$	$(\overline{0},\widetilde{1})$	$(\overline{1},\widetilde{2})$	$(\overline{0},\widetilde{0})$
$(\overline{0},\widetilde{2})$	$(\overline{0},\widetilde{2})$	$(\overline{1},\widetilde{0})$	$(\overline{0},\widetilde{1})$	$(\overline{1},\widetilde{2})$	$(\overline{0},\widetilde{0})$	$(\overline{1},\widetilde{1})$
$(\overline{1},\widetilde{0})$	$(\overline{1},\widetilde{0})$	$(\overline{0},\widetilde{1})$	$(\overline{1},\widetilde{2})$	$(\overline{0},\widetilde{0})$	$(\overline{1},\widetilde{1})$	$(\overline{0},\widetilde{2})$
$(\overline{0},\widetilde{1})$	$(\overline{0},\widetilde{1})$	$(\overline{1},\widetilde{2})$	$(\overline{0},\widetilde{0})$	$(\overline{1},\widetilde{1})$	$(\overline{0},\widetilde{2})$	$(\overline{1},\widetilde{0})$
$(\overline{1},\widetilde{2})$	$(\overline{1},\widetilde{2})$	$(\overline{0},\widetilde{0})$	$(\overline{1},\widetilde{1})$	$(\overline{0},\widetilde{2})$	$(\overline{1},\widetilde{0})$	$(\overline{0},\widetilde{1})$

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ est cyclique, engendré par $x = (\overline{1},\widetilde{1})$.

3.1 Propriété universelle du groupe quotient.

3.1.1 Théorème. *Soient G un groupe, H un sous-groupe normal dans G, et p la surjection canonique $G \to G/H$.*

(i) *Pour tout groupe G' et tout morphisme de groupes $f : G \to G'$ tel que $H \subseteq \operatorname{Ker} f$, il existe un unique morphisme de groupes $\varphi : G/H \to G'$ tel que $f = \varphi \circ p$.*

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "p"'] & G' \\ G/H \arrow[ur, "\varphi"'] & \end{tikzcd}$$

(ii) *Avec les données ci-dessus, on a de plus:*

$$(\ f \text{ surjectif } \Rightarrow\ \varphi \text{ surjectif}\ ) \quad \text{et} \quad (\ H = \operatorname{Ker} f\ \Rightarrow\ \varphi \text{ injectif}\ ).$$

Preuve. Pour tout $\overline{x} \in G/H$, posons $\varphi(\overline{x}) = f(x) \in G'$. Montrons que cette définition est indépendante du choix du représentant dans $\overline{x}$. Pour cela, considérons $y \in G$ tel que $\overline{y} = \overline{x}$; on a par définition $xy^{-1} \in H$. Puisque $H \subseteq \operatorname{Ker} f$, on déduit que $xy^{-1} \in \operatorname{Ker} f$, donc $f(xy^{-1}) = e$ d'où $f(x)f(y)^{-1} = e'$, c'est-à-dire $f(x) = f(y)$, ou encore $\varphi(\overline{x}) = \varphi(\overline{y})$. On définit donc bien une application:

$$\begin{array}{rccc} \varphi : & G/H & \longrightarrow & G' \\ & \overline{x} & \longmapsto & f(x) \end{array}$$

qui, par définition, vérifie $\varphi \circ p = f$ puisque $\varphi(p(x)) = \varphi(\overline{x}) = f(x)$ pour tout $x \in G$. Il est clair que φ est un morphisme de groupes puisque, pour tous $\overline{x}, \overline{y} \in G/H$, on a $\varphi(\overline{x}.\overline{y}) = \varphi(\overline{xy}) = f(xy) = f(x)f(y) = \varphi(\overline{x})\varphi(\overline{y})$. Il reste à montrer l'unicité de φ. Soit donc ψ un morphisme $G/H \to G'$ tel que $\psi \circ p = f$. Alors, pour tout $\overline{x} \in G/H$, on a: $\psi(\overline{x}) = \psi(p(x)) = (\psi \circ p)(x) = f(x) = \varphi(\overline{x})$. D'où $\psi = \varphi$, ce qui achève de montrer le point (i).

Pour (ii), supposons d'abord que f est surjective. Soit $x' \in G'$ quelconque. Par surjectivité de f, il existe $x \in G$ tel que $x' = f(x)$. Comme $f(x) = \varphi(\overline{x})$, on déduit qu'il existe $\overline{x} \in G/H$ tel que $x' = \varphi(\overline{x})$. Ce qui prouve que φ est surjective.

Supposons enfin que $H = \operatorname{Ker} f$. Soit $\overline{x} \in G/H$ tel que $\overline{x} \in \operatorname{Ker} \varphi$. On a $e' = \varphi(\overline{x}) = f(x)$, d'où $x \in \operatorname{Ker} f$, c'est-à-dire $x \in H$; par suite $\overline{x} = \overline{e}$. Ceci prouve que $\operatorname{Ker} \varphi = \{\overline{e}\}$, et l'injectivité de φ. □

3.1.2 Remarque. Dans le cas où l'on prend dans le théorème ci-dessus $H = \operatorname{Ker} f$ et $G' = \operatorname{Im} f$, on a φ à la fois injectif et surjectif, qui réalise donc un isomorphisme de $G/\operatorname{Ker} f$ sur $\operatorname{Im} f$, et l'on retrouve le premier théorème d'isomorphisme vu en 2.3.1.

3.1.3 Lemme (fondamental de factorisation). *Soient G un groupe, H un sous-groupe normal dans G, et p la surjection canonique $G \to G/H$. Soient G' un groupe, H' un sous-groupe normal dans G', et p' la surjection canonique $G' \to G'/H'$. Alors, pour tout morphisme de groupes $f : G \to G'$ vérifiant la condition $f(H) \subseteq H'$, il existe un unique morphisme $\varphi : G/H \to G'/H'$ tel que $\varphi \circ p = p' \circ f$.*

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "p"'] \arrow[dr, "g"'] & G' \arrow[d, "p'"] \\ G/H \arrow[r, "\varphi"'] & G'/H' \end{tikzcd}$$

Preuve. Posons $g = p' \circ f$, qui est un morphisme de groupes $G \to G'/H'$, comme composé de deux morphismes. Afin d'appliquer le théorème 3.1.1, montrons que $H \subseteq \operatorname{Ker} g$. Soit $x \in H$. On a $f(x) \in f(H)$. L'hypothèse $f(H) \subseteq H'$ implique donc $f(x) \in H'$. D'où $p'(f(x)) = \overline{e}'$. On déduit que $g(x) = \overline{e}'$, c'est-à-dire $x \in \operatorname{Ker} g$. Ainsi $g : G \to G'/H'$ est un morphisme vérifiant $H \subseteq \operatorname{Ker} g$; le théorème 3.1.1 assure l'existence d'un unique morphisme $\varphi : G/H \to G'/H'$ tel que $\varphi \circ p = g$, d'où le résultat. □

3.1.4 Remarque. Avec les données et notations ci-dessus, on a:

$$(\ p' \circ f \text{ surjectif } \Rightarrow \ \varphi \text{ surjectif }) \quad \text{et} \quad (\ H = \mathrm{Ker}(p' \circ f) \ \Leftrightarrow \ f^{-1}(H') = H \ \Rightarrow \ \varphi \text{ injectif }).$$

3.2 Deuxième théorème d'isomorphisme.

3.2.1 Théorème. *Soient G un groupe et H un sous-groupe normal dans G. Pour tout sous-groupe K de G, le sous-ensemble HK est un sous groupe de G, et l'on a:*

$$H \cap K \lhd K, \qquad H \lhd HK, \qquad \text{et} \qquad K/(H \cap K) \simeq HK/H.$$

Preuve. Rappelons que $HK = \{hk\,;\, h \in H, k \in K\}$.

Vérifions que HK est un sous-groupe de G. On a clairement $e \in HK$. Soient $x, y \in HK$. Il existe $h, h' \in K$ et $k, k' \in K$ tels que $x = hk$ et $y = h'k'$. Donc $x^{-1}y = k^{-1}h^{-1}h'k' = k^{-1}(h^{-1}h')k(k^{-1}k')$. Puisque $h^{-1}h' \in H$ et $H \lhd G$, on a $k^{-1}(h^{-1}h')k \in H$. Comme par ailleurs $k^{-1}k' \in K$, on a bien $x^{-1}y \in HK$. On conclut que HK est un sous-groupe de G.

Vérifions que $H \cap K \lhd K$. Soit $h \in H \cap K$ et $x \in K$. On a $xhx^{-1} \in H$ puisque $H \lhd G$. On a aussi $xhx^{-1} \in K$ puisque x et h appartiennent au sous-groupe K. On conclut que $xhx^{-1} \in H \cap K$. Ce qui pouve que $H \cap K \lhd K$. On peut donc considérer le groupe quotient $K/H \cap K$. Notons $p : K \to K/H \cap K$ la surjection canonique.

Vérifions que $H \lhd HK$. Soit $\ell \in H$ et $x = hk \in HK$, avec $h \in H, k \in K$. On a $x\ell x^{-1} = hk\ell k^{-1}h^{-1}$. Puisque $H \lhd G$ et $\ell \in H$, on a $k\ell k^{-1} \in H$. Donc $x\ell x^{-1} = h(k\ell k^{-1})h^{-1} \in H$ comme produit de trois éléments de H. Ce qui prouve que $H \lhd HK$. On peut donc considérer le groupe quotient HK/H. Notons $p' : HK \to HK/H$ la surjection canonique.

Notons j l'injection canonique $K \to HK$. Rappelons que j est le morphisme défini par $j(k) = ke = k$ pour tout $k \in K$. On a bien sûr $j(H \cap K) \subseteq H$, de sorte que l'application directe du lemme 3.1.3 assure l'existence d'un morphisme de groupes $\varphi : K/H \cap K \to HK/H$ tel que $\varphi \circ p = p' \circ j$:

$$\begin{tikzcd}
K \arrow[r, "j"] \arrow[d, "p"'] & HK \arrow[d, "p'"] \\
K/H \cap K \arrow[r, "\varphi"] & HK/H
\end{tikzcd}$$

Montrons que φ est surjective. Soit $\overline{hk}$ un élément quelconque de HK/H, avec $h \in H, k \in K$. On a $\overline{hk} = \overline{h}\,\overline{k} = \overline{k}$; on déduit que $HK/H = p'(K) = (p' \circ j)(K)$. On conclut avec 3.1.4 que φ est surjective.

Montrons que φ est injective. Soit $k \in K$ un élément quelconque de $\mathrm{Ker}(p' \circ j)$. On a $\overline{e} = p'(j(k)) = p'(k) = \overline{k}$, c'est-à-dire $k \in H$. Donc $k \in H \cap K$; on déduit que $\mathrm{Ker}(p' \circ j) \subseteq H \cap K$. L'inclusion réciproque étant claire, on déduit que $\mathrm{Ker}(p' \circ j) = H \cap K$. On conclut avec 3.1.4 que φ est injective. On conclut que φ réalise un isomorphisme de $K/H \cap K$ sur HK/H. □

3.2.2 Remarque. En notation additive, l'isomorphisme 3.2.1 devient $K/(H \cap K) \simeq (H + K)/H$.

3.3 Sous-groupes d'un groupe quotient et troisième théorème d'isomorphisme.

3.3.1 Proposition. *Soient G un groupe et H un sous-groupe normal dans G. L'ensemble des sous-groupes de G/H est en bijection avec l'ensemble des sous-groupes de G contenant H.*
Plus précisément, si l'on note $p : G \to G/H$ la surjection canonique, il existe pour tout sous-groupe $\overline{K}$ de G/H un unique sous-groupe K de G contenant H tel que $\overline{K} = p(K) = K/H$.

Preuve. Soit $\overline{K}$ un sous-groupe de G/H. Posons $K = p^{-1}(\overline{K}) = \{x \in G\,;\, p(x) \in \overline{K}\}$. En tant qu'image réciproque d'un sous-groupe par un morphisme de groupes, K est un sous-groupe de G. Si $h \in H$, on a $p(h) = \overline{e}$, donc $p(h) \in \overline{K}$, de sorte que $h \in p^{-1}(\overline{K})$, c'est-à-dire $h \in K$. Ceci montre que $H \subseteq K$. Par définition de K, on a $p(K) \subseteq \overline{K}$. Réciproquement, soit $\overline{x} \in \overline{K}$, avec $x \in G$; comme $p(x) = \overline{x} \in \overline{K}$, on a clairement $x \in p^{-1}(\overline{K}) = K$, et donc $\overline{x} = p(x) \in p(K)$. En résumé, $\overline{K} = p(K)$. Enfin, $H \lhd G$ implique $H \lhd K$, et il est clair alors que $K/H = p(K)$.

Montrons maintenant l'unicité. Soit donc K' un sous-groupe de G tel que $H \subseteq K'$ et $\overline{K} = p(K')$. On a donc $p(K) = p(K')$. Quel que soit $k' \in K'$, il existe alors $k \in K$ tel que $p(k') = p(k)$, donc $k'k^{-1} \in H$; on a $k' = hk$ avec $h \in H$, et l'hypothèse $H \subseteq K$ implique $h \in K$, d'où $k' \in K$ comme produit de deux éléments de K. On conclut que $K' \subseteq K$. L'inclusion réciproque s'obtient de même. □

3.3.2 Théorème. *Soient G un groupe et H un sous-groupe normal dans G. Pour tout sous-groupe K normal dans G contenant H, on a:*

$$K/H \triangleleft G/H, \qquad \text{et} \qquad (G/H)/(K/H) \simeq G/K.$$

Preuve. Notons q la surjection canonique $G \to G/K$ et p la surjection canonique $G \to G/H$. Il est clair que $K/H = p(K)$ est un sous-groupe de G/H (comme image du sous-groupe K par le morphisme de groupes p). Quels que soient $\overline{x} \in G/H$ et $\overline{k} \in K/H$, on a $\overline{x}\overline{k}\overline{x}^{-1} = p(xkx^{-1})$; or $xkx^{-1} \in K$ puisque $K \triangleleft G$, donc $\overline{x}\overline{k}\overline{x}^{-1} \in p(K)$. Ceci prouve que $K/H \triangleleft G/H$. On peut donc considérer le groupe quotient $(G/H)/(K/H)$; notons q' la surjection canonique $G/H \to (G/H)/(K/H)$. Puisque $p(K) = K/H$, on applique le lemme 3.1.3 pour conclure qu'il existe un morphisme $\varphi : G/K \to (G/H)/(G/K)$ tel que $\varphi \circ q = q' \circ p$.

$$\begin{tikzcd} G \arrow[r, "p"] \arrow[d, "q"'] & G/H \arrow[d, "q'"] \\ G/K \arrow[r, "\varphi"] & \dfrac{(G/H)}{(K/H)} \end{tikzcd}$$

Le morphisme $q' \circ p$ est surjectif comme composé de deux surjections, et il résulte donc de 3.1.4 que φ est surjectif. On a $\mathrm{Ker}(q' \circ p) = K$, d'où l'on déduit avec 3.1.4 que φ est injectif. On conclut que φ est un isomorphisme de groupes de G/K sur $(G/H)/(K/H)$. □

3.4 Produit semi-direct.

3.4.1 Rappel. On a vu au chapitre 1 qu'un groupe G est produit direct (interne) de deux de ses sous-groupes H par K lorsque les trois conditions suivantes sont vérifiées:

$$(1)\ \ G = HK, \qquad (2)\ \ H \cap K = \{e\}, \qquad (3)\ \ \forall\, h \in H,\ \forall\, k \in K,\ hk = kh.$$

Tout élément de G s'écrit de façon unique comme le produit d'un élément de H par un élément de K. On en a déduit au corollaire 2.3.4 de ce chapitre que $H \triangleleft G$ et $G/H \simeq K$.
De plus, la condition (3) implique que les deux sous-groupes H et K jouent dans un tel produit direct des rôles absolument symétriques. On a donc également $K \triangleleft G$ et $G/K \simeq H$.

3.4.2 Définition. Soient G un groupe, H et K deux sous-groupes de G. On dit que G est le produit semi-direct (interne) de H par K lorsque les trois conditions suivantes sont vérifiées:

$$(1)\ \ G = HK, \qquad (2)\ \ H \cap K = \{e\}, \qquad (3')\ \ H \triangleleft G.$$

3.4.3 Remarques. Avec les notations ci-dessus:

(a) Si G est produit semi-direct de H par K, on a aussi $G = KH$.

En effet, d'après la condition (1), tout élément x de G s'écrit $x = hk$ avec $h \in H$ et $k \in K$. Donc $g = kk^{-1}hk$, et comme $H \triangleleft G$, le produit $h' = k^{-1}hk$ est un élément de H. On a donc $g = kh'$ avec $k \in K$ et $h' \in H$. □

(b) Si G est produit semi-direct de H par K, tout élément x de G s'écrit de façon unique $x = hk$ avec $h \in H, k \in K$, et s'écrit aussi de façon unique $x = k'h'$ avec $h' \in H, k' \in K$, mais pas forcément avec $h = h'$.

Preuve. Le fait qu'un élément quelconque $x \in G$ s'écrive $x = hk = kh'$ avec $h' = k^{-1}hk$ a été vu à la remarque ci-dessus. L'unicité des décompositions découle de la seule condition (2) comme on l'a vu à la remarque 4.3.1.(a) du chapitre 1. □

(c) Si G est produit semi-direct de H par K, alors $G/H \simeq K$.

Preuve. Analogue à celle de 2.3.4. □

(d) Si G est produit direct de H par K, alors a fortiori G est produit semi-direct de H par K.

Preuve. Il s'agit de vérifier que, si les conditions (1) et (2) sont vérifiées, alors la condition (3) implique la condition (3'). Pour cela, soient $\ell \in H$ et $x \in G$ quelconques. Il existe $h \in H, k \in K$ tels que $x = hk$. D'après la condition (3), on a: $x\ell x^{-1} = hk\ell k^{-1}h^{-1} = h\ell kk^{-1}h^{-1} = h\ell h^{-1}$, qui est un élément de H comme produit de trois éléments de H. Ceci prouve que $H \lhd G$. □

(e) La réciproque de (d) est fausse.

Preuve. Prenons par exemple comme en 2.2.3.(c) le groupe symétrique $S_3 = \{e, \gamma, \gamma^2, \tau_1, \tau_2, \tau_3\}$. Le sous-groupe alterné est $A_3 = H = \{e, \gamma, \gamma^2\}$. On a $\tau_1 = e\tau_1$, $\tau_3 = \gamma\tau_1$ et $\tau_2 = \gamma^2\tau_1$. En posant $K = \{e, \tau_1\}$, on a donc $S_3 = HK$ et $H \cap K = \{e\}$. On conclut que S_3 est le produit semi-direct de H par le sous-groupe $K = \{e, \tau_1\}$. Et pourtant la condition (3) d'un produit direct n'est pas vérifiée puisque par exemple $\tau_1\gamma = \tau_2 \neq \tau_3 = \gamma\tau_1$. □

Parce que $S_3 \simeq D_3$, l'exemple de S_3 n'est qu'un cas particulier du résultat suivant.

3.4.4 EXEMPLE (groupes diédraux). En reprenant les notations du paragraphe 6.2 du chapitre 1, considérons le groupe diédral

$$\begin{aligned} D_n &= \{e, r, r^2, r^3, \ldots, r^{n-1},\ s\,,\ sr\,,\ sr^2\,,\ sr^3, \ldots,\ sr^{n-1}\} \\ &= \{e, r, r^2, r^3, \ldots, r^{n-1},\ r^{n-1}s\,,\ r^{n-2}s\,,\ \ldots,\ r^2s\,,\ rs\,,\ s\}, \end{aligned}$$

et les sous-groupes $C_n = \{e, r, r^2, r^3, \ldots, r^{n-1}\}$ et $K = \{e, s\}$. Il est clair que $D_n = C_nK$ et $C_n \cap K = \{e\}$. D'après les propositions 1.3.5 ou 1.4.5, on a de plus que $C_n \lhd D_n$. On conclut que D_n est produit semi-direct de C_n par K. En particulier, $D_n/C_n \simeq K \simeq C_2$.

Si $n > 2$, ce produit semi-direct n'est pas direct car $sr^k = r^{n-k}s \neq r^ks$, de sorte que la condition (3) n'est pas vérifiée. Dans le cas particulier où $n = 2$, D_2 (qui n'est autre que le groupe de Klein) est abélien, et produit direct de C_2 par K (qui sont tous les deux isomorphes au groupe d'ordre 2).

3.4.5 EXERCICE. Montrer que, dans $\mathrm{GL}_3(\mathbb{R})$, les matrices triangulaires supérieures dont les termes diagonaux valent 1 forment un sous-groupe, que l'on notera U. Montrer que:

$$H = \{\begin{pmatrix} 1 & 0 & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix},\ b, c \in \mathbb{R}\}, \quad K = \{\begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},\ a \in \mathbb{R}\}, \quad L = \{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix},\ b \in \mathbb{R}\}, \quad C = \{\begin{pmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},\ c \in \mathbb{R}\},$$

sont des sous-groupes de U, que U est le produit semi-direct de H par K, et que H est le produit direct de L par C.

On a vu à la proposition 4.3.4 que la notion de produit direct interne de deux sous-groupes internes était directement liée à la notion de produit direct externe construit à partir de deux groupes quelconques. C'est aussi le cas pour la notion plus générale de produit semi-direct, comme le montrent la proposition 3.4.7 suivante, et le lemme préliminaire 3.4.6.

3.4.6 LEMME. *Soient G un groupe, H un sous-groupe normal de G, et K un sous-groupe de G. On suppose que G est le produit semi-direct de H par K. Soient x, x' deux éléments quelconques de G. Si $x = hk$ et $x' = h'k'$ sont les décompositions (uniques) de x et x' (avec $h, h' \in H, k, k' \in K$), alors la décomposition du produit xx' est donnée par:*

$$xx' = h\gamma_k(h')kk', \qquad \text{avec } h\gamma_k(h') \in H \text{ et } kk' \in K$$

où γ_k désigne l'automorphisme intérieur de G défini par $y \mapsto kyk^{-1}$.

Preuve. Résulte simplement du calcul $xx' = hkh'k' = hkh'k^{-1}kk'$, et du fait que $kh'k^{-1}$ appartient à H puisque $H \lhd G$. □

3.4.7 PROPOSITION ET DÉFINITION. *Soient G_1 et G_2 deux groupes. Soit $\gamma : G_2 \to \operatorname{Aut} G_1$ un morphisme de groupes. Pour tout $x_2 \in G_2$, on note γ_{x_2} l'automorphisme de G_1 image de x_2 par γ.*

(i) *Le produit cartésien $G_1 \times G_2 = \{(x_1, x_2),\ x_1 \in G_1,\ x_2 \in G_2\}$ est un groupe pour la loi définie par:*

$$(x_1, x_2).(y_1, y_2) = (x_1\gamma_{x_2}(y_1), x_2y_2) \quad \text{pour tous } x_1, y_1 \in G_1,\ x_2, y_2 \in G_2.$$

Ce groupe est appelé le produit semi-direct de G_1 par G_2. On le note $G = G_1 \times_\gamma G_2$, ou $G = G_1 \rtimes G_2$.

(ii) *Si l'on note $H = G_1 \times \{e_2\}$ et $K = \{e_1\} \times G_2$, alors H est un sous-groupe de G normal dans G et isomorphe à G_1, K est un sous-groupe de G isomorphe à G_2, et G est le produit semi-direct interne de H par K.*

Preuve. La vérification des axiomes de groupes pour (i) et des isomorphismes pour (ii) est technique et fastidieuse, mais élémentaire. C'est un excellent exercice, à faire absolument ! $\square$

3.4.8 REMARQUES

1. Le produit direct de G_1 et G_2 est un cas particulier de produit semi-direct, correspondant au cas où γ_{x_2} est l'identité de G_1 pour tout $x_2 \in G_2$, c'est-à dire au cas où $\gamma : G_2 \to \operatorname{Aut} G_1$ est le morphisme constant $x_2 \mapsto \mathrm{id}_{G_1}$.
2. Dans le produit semi-direct $G_1 \rtimes G_2$, les groupes G_1 et G_2 ne jouent a priori pas des rôles symétriques. En particulier, même si G_1 et G_2 sont abéliens, $G_1 \rtimes G_2$ n'est en général pas abélien (et de fait il ne l'est que lorsque γ est trivial, c'est-à-dire lorsque le produit est direct). Par exemple, pour $n \geq 3$: les groupes cycliques C_n et C_2 sont abéliens, mais le groupe diédral $D_n \simeq C_n \rtimes C_2$ ne l'est pas.

Anneaux : les premières notions

1. Anneaux et sous-anneaux

1.1 Notion d'anneau

1.1.1 Définition. Un *anneau* est un ensemble non vide muni de deux lois de composition internes, l'une notée comme une addition et l'autre comme une multiplication, vérifiant les propriétés:

(1) A est un groupe abélien pour l'addition, (on note 0 son élément neutre),

(2) la multiplication est associative, c'est-à-dire:
$$x(yz) = (xy)z \text{ pour tous } x, y, z \in A.$$

(3) la multiplication est distributive sur l'addition à gauche et à droite, c'est-à-dire:
$$x(y + z) = xy + xz \text{ et } (x + y)z = xz + yz \text{ pour tous } x, y, z \in A.$$

On dit que l'anneau A est *commutatif* si de plus la multiplication est commutative, c'est-à-dire:
$$xy = yx \text{ pour tous } x, y \in A.$$
On dit que A est *unitaire* si de plus la multiplication admet un élément neutre 1.
$$x.1 = 1.x = x \text{ pour tout } x \in A.$$

1.1.2 Premiers exemples.

(a) L'ensemble $\mathbb{Z}$ des entiers est un anneau commutatif unitaire. Il en est de même de $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$.

(b) L'ensemble des matrices carrées d'ordre $n \geq 2$ à coefficients réels est un anneau non-commutatif (pour le produit matriciel) unitaire (de neutre multiplicatif la matrice identité). Il en est de même de l'anneau des endomorphismes d'un espace vectoriel (pour la loi $\circ$).

(c) L'anneau nul est l'anneau $\{0\}$ formé d'un unique élément.

(d) Pour tout intervalle I de $\mathbb{R}$, l'ensemble $\mathcal{F}(I, \mathbb{R})$ des applications de I dans $\mathbb{R}$ est un anneau commutatif (la multiplication étant le produit des fonctions défini par $(fg)(x) = f(x)g(x)$ pour tout $x \in \mathbb{R}$) unitaire (de neutre multiplicatif la fonction constante égale à 1). Il en est de même pour l'ensemble $\mathbb{R}^{\mathbb{N}}$ des suites de réels.

1.1.3 Exemple de $\mathbb{Z}/n\mathbb{Z}$. Fixons un entier $n \geq 2$.
Considérons le groupe additif $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. Rappelons que l'addition est définie par:
$$\overline{x} + \overline{y} = \overline{x + y} \quad \text{pour tous } \overline{x}, \overline{y} \in \mathbb{Z}/n\mathbb{Z}.$$
On a vu que cette définition est indépendante des représentants choisis, et que le groupe additif $\mathbb{Z}/n\mathbb{Z}$ est abélien. On définit une multiplication dans $\mathbb{Z}/n\mathbb{Z}$ à partir de celle de $\mathbb{Z}$ en posant:
$$\overline{x}\,\overline{y} = \overline{xy} \quad \text{pour tous } \overline{x}, \overline{y} \in \mathbb{Z}/n\mathbb{Z}.$$
Cette multiplication est bien définie, indépendamment des représentants choisis.

En effet, si $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$, alors $x' = x + nu$ et $y' = y + nv$ pour deux entiers $u, v \in \mathbb{Z}$, de sorte que $x'y' = xy + n(uy + vx + nuv)$, d'où $\overline{x'y'} = \overline{xy}$.

Il est immédiat de vérifier que $\mathbb{Z}/n\mathbb{Z}$ satisfait les conditions (2) et (3) de 1.1.1, que $\overline{1}$ est neutre pour la multiplication, et que la multiplication est commutative. On conclut que:

$\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif unitaire.

On verra plus loin que l'anneau $\mathbb{Z}/n\mathbb{Z}$, que nous avons souhaité introduire dès le début afin de disposer d'exemples significatifs pour les différentes notions que l'on va voir, est un exemple d'anneau quotient.

1.1.4 Exemple des anneaux de polynômes. On fixe un anneau commutatif unitaire A.

Notons (provisoirement) $B = A^{(\mathbb{N})}$ l'ensemble des suites d'éléments de A qui sont "à support fini" c'est-à-dire dont tous les termes sont nuls sauf un nombre fini d'entre eux.

On note $0_B = (0_A, 0_A, \ldots)$. Pour tout $f = (a_n)_{n\in\mathbb{N}}$ distinct de 0_B, on appelle degré de f le plus grand des entiers $n \in \mathbb{N}$ tels que $a_n \neq 0$. On définit une addition et une multiplication dans B en posant, pour tous $f = (a_n)_{n\in\mathbb{N}}$ et $g = (b_n)_{n\in\mathbb{N}}$ dans B,

$$f + g = (a_n + b_n)_{n\in\mathbb{N}} \quad \text{et} \quad fg = (c_n)_{n\in\mathbb{N}}, \text{ avec } c_n = \sum_{i=0}^{n} a_i b_{n-i}.$$

On peut montrer (vérification technique et fastidieuse, mais élémentaire) que, pour ces opérations, B est un anneau commutatif unitaire, avec $0_B = (0_A, 0_A, \ldots)$ et $1_B = (1_A, 0_A, 0_A, \ldots)$. On l'appelle l'anneau des polynômes en une indéterminée à coefficients dans A.

On définit aussi le produit externe d'un élément $\alpha \in A$ par un élément $f = (a_n)_{n\in\mathbb{N}}$ en posant $\alpha f = (\alpha a_n)_{n\in\mathbb{N}}$. A noter que le produit externe $\alpha.f$ n'est autre que le produit interne de f par $(\alpha, 0_A, 0_A, \ldots)$. C'est pourquoi on convient de noter encore α l'élément $(\alpha, 0_A, 0_A, \ldots)$ de B. En particulier $0_B = 0_A$ et $1_B = 1_A$.

En posant $e_i = (0_A, 0_A, \ldots, 0_A, 1_A, 0_A, 0_A, \ldots)$, avec le 1_A en $i+1$-ième position, pour tout $i \in \mathbb{N}$, tout élément de B s'écrit de façon unique $f = \sum_{n\in\mathbb{N}} a_n e_n$ avec les $a_n \in A$ nuls sauf un nombre fini d'entre eux (de sorte que la somme est finie). Il est clair que $e_n e_m = e_{n+m}$ pour tous $n, m \in \mathbb{N}$, et donc $e_n = e_1^n$ pour tout $n \in \mathbb{N}$. On note traditionnellement $X = e_1$ et $B = A[X]$, et l'on retrouve les notations usuellement utilisées pour désigner les polynômes.

On retiendra que:

(a) Pour tout anneau commutatif unitaire A, les polynômes en une indéterminée à coefficients dans A forment un anneau commutatif unitaire, noté $A[X]$. Son neutre pour l'addition est 0_A. Son neutre pour la multiplication est 1_A.

(b) Pour tout élément non-nul P de $A[X]$, il existe un unique entier naturel n et un unique $(n+1)$-uplet $(a_0, a_1, \ldots, a_n)$ d'éléments de A tels que:

$$P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \quad \text{et} \quad a_n \neq 0.$$

L'entier n est appelé le degré de P, noté $\deg P$. L'élément non-nul a_n de A est appelé le coefficient dominant de P, noté $\mathrm{cd}(P)$. Par convention, on pose $\deg 0 = -\infty$ et $\mathrm{cd}\, 0 = 0$.

(c) Deux polynômes $P = \sum\limits_{i=0}^{n} a_i X^i$ et $Q = \sum\limits_{i=0}^{m} b_i X^i$ sont égaux si et seulement si $n = m$ et $a_i = b_i$ pour tout $0 \leq i \leq n$. Un polynôme est nul si et seulement si tous ses coefficients sont nuls.

(d) Si $P = \sum\limits_{i=0}^{n} a_i X^i$ et $Q = \sum\limits_{i=0}^{m} b_i X^i$, on a: $P+Q = \sum\limits_{i=0}^{\max(n,m)} (a_i+b_i) X^i$ et $PQ = \sum\limits_{i=0}^{n+m} (\sum\limits_{j=0}^{i} a_j b_{i-j}) X^i$.

Sous forme développée explicite, la formule du produit est donc:

$PQ = (a_n X^n + a_{n-1} X^{n-1} + a_{n-2} X^{n-2} + \cdots + a_1 X + a_0)(b_m X^m + b_{m-1} X^{m-1} + b_{m-2} X^{m-2} + \cdots + b_1 X + b_0) = a_n b_m X^{n+m} + (a_n b_{m-1} + a_{n-1} b_m) X^{n+m-1} + (a_n b_{m-2} + a_{n-1} b_{m-1} + a_{n-2} b_m) X^{n+m-2} + \cdots + (a_1 b_0 + a_0 b_1) X + a_0 b_0.$

(e) On en déduit que, pour tous P et Q dans $A[X]$, on a:

$$\deg(P+Q) \leq \max(\deg P, \deg Q) \quad \text{et} \quad \deg(PQ) \leq \deg P + \deg Q.$$

1.2 Sous-anneau.

1.2.1 Définition. Soit A un anneau. On appelle *sous-anneau* de A toute partie non-vide B de A qui vérifie les deux conditions suivantes:

(1) B est un sous-groupe du groupe additif A.

(2) B est stable par la multiplication de A, c'est-à-dire que l'on a:

$$xy \in B \ \text{ quels que soient } x \in B \text{ et } y \in B.$$

1.2.2 Définition. Soit A un anneau unitaire. On appelle *sous-anneau unitaire* de A tout sous-anneau de A qui contient 1_A.

1.2.3 Remarques.

(a) Si B est un sous-anneau de A, alors B est lui-même un anneau (pour les lois déduites de celles de A par restriction à B). De fait, dans la pratique, pour montrer qu'un ensemble donné est un anneau, on cherche souvent à montrer que c'est un sous-anneau d'un anneau déjà connu.

(b) Si B est un sous-anneau unitaire d'un anneau unitaire A, alors B est lui-même un anneau unitaire, et l'on a $1_B = 1_A$.

(c) Si l'anneau A est commutatif, alors tout sous-anneau de A est commutatif.

(d) Dans la pratique, pour montrer qu'un sous-ensemble non-vide B d'un anneau A est un sous-anneau de A, il suffit de vérifier que:

$$\text{pour tous } x \in B \text{ et } y \in B, \text{ on a } \ x - y \in B \ \text{ et } \ xy \in B.$$

Pour montrer qu'un sous-ensemble B d'un anneau unitaire A est un sous-anneau unitaire de A, il suffit de vérifier que:

$$(\ 1_A \in B\ ) \quad \text{et} \quad (\text{ pour tous } x \in B \text{ et } y \in B, \text{ on a } \ x - y \in B \ \text{ et } \ xy \in B\ ).$$

1.2.4 Premiers exemples.

(a) Si A est un anneau, alors $\{0\}$ et A lui-même sont des sous-anneaux de A.

(b) Tout anneau unitaire A est un sous-anneau unitaire de $A[X]$.

(c) $\mathbb{Z}$ est un sous-anneau unitaire de $\mathbb{Q}$ (et de $\mathbb{R}$, et de $\mathbb{C}$). Pour tout $n \geq 2$, l'ensemble $n\mathbb{Z} = \{nx\,;\, x \in \mathbb{Z}\}$ est un sous-anneau non unitaire de $\mathbb{Z}$.

(d) Dans $\mathcal{F}(I, \mathbb{R})$ les fonctions continues forment un sous-anneau unitaire.

1.2.5 Exemple des entiers de Gauss.

On appelle entier de Gauss tout nombre complexe dont la partie réelle et la partie imaginaire sont des entiers. On note $\mathbb{Z}[i]$ leur ensemble:

$$\mathbb{Z}[i] = \{a + ib\ ;\ a, b \in \mathbb{Z}\}.$$

$\mathbb{Z}[i]$ *est un anneau commutatif unitaire, contenant* $\mathbb{Z}$ *comme sous-anneau.*

En effet, quels que soient $x = a+ib$ et $x' = c+id$ avec $a, b, c, d \in \mathbb{Z}$, les complexes $x-x' = (a-c)+i(b-d)$ et $xx' = (ac - bd) + i(ad + bc)$ ont des parties réelles et imaginaires dans $\mathbb{Z}$, donc appartiennent à $\mathbb{Z}[i]$. Ceci prouve que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$ (donc en particulier un anneau commutatif). Il est clair que $\mathbb{Z}$ est un sous-anneau de $\mathbb{Z}[i]$, d'où il résulte en particulier que $1 \in \mathbb{Z}[i]$. □

L'application $N : \mathbb{Z}[i] \to \mathbb{N}$ définie par $N(a + ib) = (a + ib)(a - ib) = a^2 + b^2$ jouera dans l'étude de l'anneau $\mathbb{Z}[i]$ un rôle important. Bornons-nous pour l'instant à observer que, puisque $N(x) = x\overline{x} = |x|^2$ pour tout $x \in \mathbb{Z}[i]$, on a clairement $N(xx') = N(x)N(x')$ pour tous $x, x' \in \mathbb{Z}[i]$.

1.2.6 Généralisation.

Soit d un entier non-nul, que l'on suppose sans facteurs carrés (c'est-à-dire que d n'est divisible par aucun carré d'entier distinct hormis 1). On désigne par ω une racine carrée dans $\mathbb{C}$ de d. On vérifie (la preuve est laissée en exercice):

$$\mathbb{Z}[\omega] = \{a + \omega b\ ;\ a, b \in \mathbb{Z}\} \textit{ est un anneau commutatif unitaire, contenant } \mathbb{Z} \textit{ comme sous-anneau,}$$

et que l'application $N : \mathbb{Z}[\omega] \to \mathbb{Z}$ définie par $N(a + \omega b) = (a + \omega b)(a - \omega b) = a^2 - db^2$ vérifie $N(xx') = N(x)N(x')$ pour tous $x, x' \in \mathbb{Z}[\omega]$.

CONVENTION. – Bien que les anneaux non-commutatifs interviennent dans de nombreuses situations variées et intéressantes en mathématiques, on se limitera dans la suite de ce cours (en fonction des applications visées par les programmes) à l'étude des anneaux commutatifs et unitaires.
C'est pourquoi, dans les pages qui suivent, même lorsqu'on ne le précisera pas dans les énoncés, tous les anneaux seront supposés commutatifs, unitaires, et de plus non triviaux (c'est-à-dire distinct de $\{0\}$).

1.3 Groupe des unités.

1.3.1 DÉFINITION. Soit A un anneau commutatif unitaire. On appelle *unité* de A, ou *élément inversible dans A*, tout élément $x \in A$ tel qu'il existe un élément $y \in A$ vérifiant $xy = 1$.

Remarques.

(a) Si $x \in A$ est inversible dans A, il est facile de vérifier (faites-le...) qu'il n'existe qu'un seul élément $y \in A$ tel que $xy = 1$. On note $y = x^{-1}$; on l'appelle l'inverse de x dans A.

(b) Les éléments 1 et -1 sont toujours inversibles dans A, avec $1^{-1} = 1$ et $(-1)^{-1} = -1$. L'élément 0 n'est jamais inversible (dès lors que l'anneau A n'est pas trivial, c'est-à-dire $1 \neq 0$) car on a (vérifiez-le) $0x = 0 \neq 1$ pour tout $x \in A$.

1.3.2 PROPOSITION ET DÉFINITION. *Soit A un anneau commutatif unitaire. L'ensemble des éléments de A inversibles dans A est un groupe pour la multiplication, appelé groupe des unités de A, et noté $U(A)$.*

Preuve. D'après la remarque (b) ci-dessus, $U(A)$ n'est pas vide, car il contient 1. Soient x et y deux éléments de $U(A)$. Il existe x' et y' dans A tels que $xx' = 1 = yy'$. Donc $(xy)(y'x') = x(yy')x' = x1x' = xx' = 1$, ce qui prouve que $xy \in U(A)$ (et que $(xy)^{-1} = y^{-1}x^{-1}$). On a ainsi vérifié que la multiplication de A se restreint en une loi de composition interne de $U(A)$. Elle est associative, et admet comme neutre 1 qui, comme on l'a observé, appartient à $U(A)$. Il reste à vérifier que tout élément $x \in U(A)$ admet un inverse dans $U(A)$, ce qui est évident puisque l'inverse $x' = x^{-1}$ d'un élément $x \in U(A)$ est lui-même dans $U(A)$, d'inverse $(x')^{-1} = x$. □

1.3.3 EXEMPLES.

(a) $U(\mathbb{Z}) = \{-1, 1\}$.

(b) $U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$.

Preuve. Reprenons les notations de 1.2.5. Soient $x = a + ib$ et $y = c + id$ avec $a, b, c, d \in \mathbb{Z}$ tels que $xy = 1$. On a alors $1 = N(xy) = N(x)N(y)$ avec $N(x), N(y) \in \mathbb{N}^*$, d'où $N(x) = N(y) = 1$ d'après l'exemple précédent. Or $N(x) = 1$ équivaut à $a^2 + b^2 = 1$ ce qui, dans $\mathbb{Z}$, se produit si et seulement si (a, b) est l'un des quatre couples $(1, 0)$, $(-1, 0)$, $(0, 1)$ ou $(0, -1)$. □

(c) Pour tout entier $n \geq 2$, $U(\mathbb{Z}/n\mathbb{Z}) = \{\ \overline{x}\ ;\ 0 \leq x \leq n-1,\ \text{et } x \text{ premier avec } n\}$.

Preuve. Soit $\overline{x}$ un élément quelconque de $\mathbb{Z}/n\mathbb{Z}$, avec $0 \leq x \leq n - 1$. On a:

$$\begin{aligned}
(\ \overline{x} \text{ inversible dans } \mathbb{Z}/n\mathbb{Z}\ ) &\Leftrightarrow (\text{ il existe } u \in \mathbb{Z} \text{ tel que } \overline{x}\,\overline{u} = \overline{1}\ )\\
&\Leftrightarrow (\text{ il existe } u \in \mathbb{Z} \text{ tel que } \overline{xu - 1} = \overline{0}\ )\\
&\Leftrightarrow (\text{ il existe } u, v \in \mathbb{Z} \text{ tels que } xu - 1 = nv\ )\\
&\Leftrightarrow (\text{ il existe } u, v \in \mathbb{Z} \text{ tels que } xu + n(-v) = 1\ )
\end{aligned}$$

d'où le résultat par le théorème de Bézout dans $\mathbb{Z}$. □

Remarquons que les éléments $\overline{x}$ qui sont inversibles dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ sont aussi, d'après le point (iii) du théorème 2.5.4 du chapitre 2, ceux qui engendrent le groupe additif $\mathbb{Z}/n\mathbb{Z}$. En particulier le groupe $U(\mathbb{Z}/n\mathbb{Z})$ est fini d'ordre $\varphi(n)$, (où φ est l'indicatrice d'Euler).

1.4 Corps.

1.4.1 DÉFINITION. On appelle *corps commutatif* (ou plus simplement corps) tout anneau commutatif unitaire dans lequel tout élément non-nul est inversible.
En notant, pour tout anneau A commutatif unitaire $A^* = A \setminus \{0\}$, on a donc:

$$(\ A \text{ corps }\ ) \Leftrightarrow (\ U(A) = A^*\ )$$

1.4.2 DÉFINITION. Soit K un corps. On appelle *sous-corps* de K tout sous-anneau unitaire F de K tel que l'inverse de tout élément non-nul de F appartienne à F.

1.4.3 EXEMPLES.

(a) $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ sont des corps; ils contiennent comme sous-anneau $\mathbb{Z}$ qui, lui, n'est pas un corps.

(b) $\mathbb{Q}(i) = \{p + qi\ ;\ p, q \in \mathbb{Q}\}$ est un sous-corps de $\mathbb{C}$; il contient $\mathbb{Z}[i]$ comme sous-anneau qui, lui, n'est pas un corps.

Preuve. On vérifie aisément que $\mathbb{Q}(i)$ est un sous-anneau de $\mathbb{C}$; pour tout $x = p+qi \in \mathbb{Q}(i)$ non-nul, son inverse x^{-1} dans $\mathbb{C}$ est égal à $\frac{p}{p^2+q^2} + \frac{-q}{p^2+q^2}i$ et appartient donc à $\mathbb{Q}(i)$. Ce qui prouve que $\mathbb{Q}(i)$ est un sous-corps de $\mathbb{C}$. Il est clair que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{Q}(i)$, et le fait que ce n'est pas un corps découle immédiatement de 1.3.3.(b). □

(c) Pour tout entier $n \geq 2$, $(\ \mathbb{Z}/n\mathbb{Z}$ est un corps $)\ \Leftrightarrow\ (\ n$ est un nombre premier $)$.

Preuve. Résulte immédiatement de 1.3.3.(c). □

1.5 Intégrité.

1.5.1 DÉFINITION. Soit A un anneau commutatif. On dit que A est *intègre*, ou encore que A est un *domaine d'intégrité*, lorsqu'il est non-nul et vérifie la propriété suivante:

$$\text{pour tous } x, y \in A,\ (\ xy = 0\ )\ \Leftrightarrow\ (\ x = 0 \ \text{ ou }\ y = 0\ ).$$

Un élément x de A est appelé un *diviseur de zéro* dans A lorsque $x \neq 0$ et lorsque qu'il existe $y \neq 0$ dans A tel que $xy = 0$. En d'autres termes, A est intègre si et seulement s'il n'admet pas de diviseurs de zéro.

1.5.2 PREMIERS EXEMPLES ET CONTRE-EXEMPLES.

(a) Tout corps est un anneau intègre.

Preuve. Soit K un corps. Soient $x, y \in K$ tels que $xy = 0$. Si $x \neq 0$, alors x est inversible dans K par définition d'un corps. Donc $x^{-1}xy = x^{-1}0$, c'est-à-dire $y = 0$. De même $y \neq 0$ implique $x = 0$. En résumé l'un au moins des deux facteurs x et y est nul. □

(b) Tout sous-anneau d'un anneau intègre est intègre. En particulier tout sous-anneau d'un corps est intègre. Par exemple, $\mathbb{Z}$ et $\mathbb{Z}[i]$ sont intègres, bien que ce ne soient pas des corps (d'après les points (a) et (b) de 1.3.3).

(c) Considérons les tables de multiplication des anneaux $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$.

	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

L'anneau $\mathbb{Z}/5\mathbb{Z}$ est un corps puisque 5 est un nombre premier. Il est donc a fortiori intègre.

	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

L'anneau $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre car, par exemple, $\overline{2}\,.\,\overline{3} = \overline{0}$ bien que $\overline{2} \neq \overline{0}$ et $\overline{3} \neq \overline{0}$.
A fortiori, ce n'est pas un corps.

Ces exemples sont des cas particuliers de la proposition suivante.

1.5.3 PROPOSITION (cas des anneaux $\mathbb{Z}/n\mathbb{Z}$). *Pour tout entier $n \geq 2$, on a:*

$$(\text{ l'anneau } \mathbb{Z}/n\mathbb{Z} \text{ est intègre }) \Leftrightarrow (\text{ } n \text{ est un nombre premier}) \Leftrightarrow (\text{ l'anneau } \mathbb{Z}/n\mathbb{Z} \text{ est un corps })$$

Preuve. D'après 1.4.3.(c) et 1.5.2.(a), le seul point à montrer est que $\mathbb{Z}/n\mathbb{Z}$ intègre implique n premier. Par contraposée, supposons que n n'est pas premier; il existe donc $k, m \in \mathbb{Z}$ tels que $n = km$ avec $1 < k < n$ et $1 < m < n$. On a alors $\overline{k}.\overline{m} = \overline{n} = \overline{0}$, bien que $\overline{k} \neq \overline{0}$ et $\overline{m} \neq \overline{0}$. □

1.5.4 PROPOSITION (cas des anneaux de polynômes). *Soit A un anneau commutatif unitaire.*

(i) *Si A est intègre, alors pour tous polynômes $P, Q \in A[X]$, on a:*

$$\deg(PQ) = \deg P + \deg Q \quad \text{ et } \quad \mathrm{cd}(PQ) = \mathrm{cd}(P)\,\mathrm{cd}(Q)$$

(ii) *$A[X]$ est intègre si et seulement si A est intègre.*

(iii) *En particulier, si K est un corps, alors l'anneau $K[X]$ est intègre.*

Preuve. Les égalités $\deg(PQ) = \deg P + \deg Q$ et $\mathrm{cd}(PQ) = \mathrm{cd}\,P\,\mathrm{cd}\,Q$ sont claires si P ou Q est nul. Supposons-les tous les deux non-nuls, et écrivons $P = a_nX^n + \cdots + a_1X + a_0$ et $Q = b_mX^m + \cdots + b_1X + b_0$, avec $\mathrm{cd}(P) = a_n \neq 0$ et $\mathrm{cd}(Q) = b_m \neq 0$. Alors:

$$PQ = a_nb_mX^{n+m} + (a_nb_{m-1} + a_{n-1}b_m)X^{n+m-1} + \cdots + (a_1b_0 + a_0b_1)X + a_0b_0.$$

L'intégrité de A implique $a_nb_m \neq 0$, donc $\mathrm{cd}(PQ) = a_nb_m$, d'où $\deg(PQ) = n + m$, ce qui prouve (i). Il résulte immédiatement de (i) que, si A est intègre, le produit de deux éléments non-nuls de $A[X]$ est non-nul, ce qui prouve que $A[X]$ est intègre. L'implication réciproque étant triviale d'après 1.5.2.(b), le point (ii) est établi. Le point (iii) en découle d'après 1.5.2.(a). □

1.5.5 COROLLAIRE (groupe des unités des anneaux de polynômes). *Soit A un anneau commutatif unitaire. Si A est intègre, alors: $U(A[X]) = U(A)$.*

Preuve. L'inclusion $U(A) \subset U(A[X])$ est claire puisque A est un sous-anneau de $A[X]$. Pour la réciproque, considérons $P \in U(A[X])$. Il existe donc $Q \in A[X]$ tel que $PQ = 1$. Ces deux polynômes sont nécessairement non-nuls, donc il résulte du point (i) de la proposition précédente que $\deg P + \deg Q = 0$. On en tire $\deg P = \deg Q = 0$, c'est-à-dire $P \in A$ et $Q \in A$, et donc l'égalité $PQ = 1$ implique $P \in U(A)$ et $Q \in U(A)$. □

Remarque. $A[X]$ n'est jamais un corps.

En effet, que A soit ou non intègre, l'élément X de $A[X]$ vérifie $\deg PX = \deg P + 1$ pour tout $P \in A[X]$, de sorte que l'on ne peut pas avoir $PX = 1$, ce qui montre que X n'est jamais inversible. □

1.6 Morphisme d'anneaux.

1.6.1 DÉFINITIONS. Soient A et B deux anneaux commutatifs unitaires. On appelle *morphisme d'anneaux unitaires* de A dans B toute application $f : A \to B$ vérifiant les trois propriétés suivantes:

$$(\ f(x+y) = f(x) + f(y) \ \text{ et } \ f(xy) = f(x)f(y) \ \text{ pour tous } x, y \in A\ ) \text{ et } (\ f(1_A) = 1_B\ ).$$

Il résulte de la première condition qu'un morphisme d'anneaux unitaires est a fortiori un morphisme de groupes additifs. Les propriétés générales des morphismes d'anneaux unitaires sont de fait analogues à celles que nous avons démontrées pour les morphismes de groupes au chapitre 1. C'est pourquoi nous synthétisons ci-dessous les plus usuelles en laissant au lecteur le soin d'adapter les démonstrations.

1.6.2 PROPRIÉTÉS.

(a) Si $f : A \to B$ est un morphisme d'anneaux unitaires, alors l'image directe par f de tout sous-anneau unitaire de A est un sous-anneau unitaire de B, et l'image réciproque par f de tout sous-anneau unitaire de B est un sous-anneau unitaire de A.

(b) Si $f : A \to B$ et $g : B \to C$ sont des morphismes d'anneaux unitaires, alors $g \circ f : A \to C$ est un morphisme d'anneaux unitaires.

(c) Si $f : A \to B$ est un morphisme d'anneaux unitaires bijectif, alors sa bijection réciproque $f^{-1} : B \to A$ est un morphisme d'anneaux unitaires; on dit dans ce cas que f est un *isomorphisme*, et que les deux anneaux A et B sont *isomorphes*.

1.7 Corps des fractions d'un anneau intègre.

1.7.1 Construction. Il existe, on l'a vu, des anneaux intègres qui ne sont pas des corps. Le but de ce qui suit est de montrer que, néanmoins, on peut construire de façon canonique pour tout anneau intègre A un corps K qui le contient, et qui est (en un sens que l'on précisera) le plus petit corps qui le contient. Evidemment, la question ne se pose pas pour des anneaux non intègres (d'après les remarques 1.5.2.(a) et 1.5.2.(b)).

Fixons A un anneau commutatif unitaire intègre. Posons $A^* = A \setminus \{0\}$. On définit dans $A \times A^*$ la relation $\sim$ par:

$$(a,b) \sim (c,d) \Leftrightarrow ad = bc.$$

Etape 1: *la relation $\sim$ est une relation d'équivalence dans $A \times A^*$.*

Preuve. La réflexivité et la symétrie sont évidentes. Pour la transitivité, considérons trois couples (a,b), (c,d) et (e,f) dans $A \times A^*$. Supposons que $(a,b) \sim (c,d)$ et $(c,d) \sim (e,f)$. On a donc: $ad = bc$ et $cf = de$. Il vient $adf = bcf = bde$, et comme $d \neq 0$, l'intégrité de A implique $af = be$, d'où $(a,b) \sim (e,f)$. □

Pour tout couple $(a,b) \in A \times A^*$, on note $\frac{a}{b}$ la classe d'équivalence de (a,b) pour la relation $\sim$:

$$\tfrac{a}{b} = \{(c,d) \in A \times A^* \,;\, (c,d) \sim (a,b)\} = \{(c,d) \in A \times A^* \,;\, ad = bc\}.$$

Une telle classe s'appelle une fraction. On note $K = (A \times A^*)/\sim$ l'ensemble quotient de $A \times A^*$ par la relation $\sim$, c'est-à-dire l'ensemble des fractions. Tout couple (c,d) appartenant à $\frac{a}{b}$ s'appelle un représentant de la fraction $\frac{a}{b}$. On a:

$$\left(\tfrac{a}{b} = \tfrac{c}{d} \text{ dans } K \right) \Leftrightarrow \left((a,b) \sim (c,d) \text{ dans } A \times A^* \right) \Leftrightarrow \left(ad = bc \text{ dans } A \right).$$

Etape 2: *L'application $\phi : A \to K$ qui, à un élément $a \in A$ associe la fraction $\phi(a) = \frac{a}{1}$, est injective, et est appelée injection canonique de A dans K.*

Preuve. Soient $a, c \in A$ tels que $\phi(a) = \phi(c)$. Alors $\frac{a}{1} = \frac{c}{1}$, d'où $a.1 = 1.c$, donc $a = c$. □

On convient d'identifier A avec le sous-ensemble $\phi(A)$ de K, qui lui est équipotent. Via cette identification, A est un sous-ensemble de K, et on pose $a = \frac{a}{1}$, pour tout $a \in A$. En d'autres termes:

$$\text{quel que soit } a \in A, \text{ on a: } \quad a = \tfrac{a}{1} = \{(c,d) \in A \times A^* \,;\, c = ad\} = \tfrac{ad}{d} \quad \text{pour tout } d \in A^*.$$

En particulier: $0 = \frac{0}{1} = \frac{0}{b}$ pour tout $b \in A^*$ et $1 = \frac{1}{1} = \frac{b}{b}$ pour tout $b \in A^*$.

Etape 3: *Les lois de composition internes dans K définies par:*

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \qquad \text{et} \qquad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$$

sont bien définies (indépendamment des représentants choisis), munissent K d'une structure d'anneau commutatif unitaire, et prolongent celles de A (ce qui signifie que l'injection canonique est un morphisme d'anneaux unitaires, ou encore que A peut être considéré, en l'identifiant avec son image par ϕ, comme un sous-anneau unitaire de K).

Preuve. Supposons que $\frac{a}{b} = \frac{a'}{b'}$ et $\frac{c}{d} = \frac{c'}{d'}$. Un calcul évident montre que $ab' = a'b$ et $cd' = c'd$ impliquent:

– d'une part: $(ad+bc)b'd' = (a'd'+b'c')bd$, et donc $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$,

– d'autre part: $(ac)(b'd') = (a'c')(bd)$, et donc $\frac{ac}{bd} = \frac{a'c'}{b'd'}$.

Ce qui prouve que les deux lois sont bien définies. Qu'elles satisfont alors tous les axiomes de la structure d'anneau commutatif unitaire (avec $0 = \frac{0}{1}$ pour neutre additif et $1 = \frac{1}{1}$ pour neutre multiplicatif) est une simple vérification, qu'on laisse au lecteur. Enfin quels que soient deux éléments $a, c \in A$, on a:

$$\phi(a+c) = \tfrac{a+c}{1} = \tfrac{a}{1} + \tfrac{c}{1} = \phi(a) + \phi(c) \quad \text{et} \quad \phi(ac) = \tfrac{ac}{1} = \tfrac{a}{1}.\tfrac{c}{1} = \phi(a).\phi(c),$$

ce qui achève la preuve. □

Etape 4: *Tout élément non-nul de K est inversible dans K. Plus précisément, tout élément $\frac{a}{b} \in K$ avec $(a,b) \in A^* \times A^*$ admet $\frac{b}{a}$ pour inverse.*

Preuve. Evident puisque $\frac{a}{b}.\frac{b}{a} = \frac{ab}{ba} = 1$. □

En particulier, tout élément non-nul $a \in A$ admet dans K l'inverse $\frac{1}{a}$.

On déduit de cette construction et des vérifications faites aux différentes étapes le théorème suivant.

1.7.2 Théorème. *Soit A un anneau commutatif unitaire intègre.*

(i) *L'ensemble $K = (A \times A^*)/\sim$ des fractions sur A, muni des lois construites ci-dessus, est un corps commutatif, qui contient A comme sous-anneau unitaire.*

(ii) *Si K' est un sous-corps tel que $A \subseteq K' \subseteq K$, alors $K' = K$.*

Preuve. Le (i) a été montré en 1.7.1. Pour le (ii), supposons que $A \subseteq K' \subseteq K$ avec K' un corps. Soit $x \in K$. Par définition, il existe $a \in A$ et $b \in A^*$ tel que $x = \frac{a}{b} = a.\frac{1}{b}$. On a $b \in A$ donc $b \in K'$, avec $b \neq 0$; comme l'inverse de b dans K est $\frac{1}{b} \in K$, et que cet inverse doit appartenir à K' puisque K' est un sous-corps, on a $\frac{1}{b} \in K'$. Par ailleurs $a \in A$ donc $a \in K'$. Le sous-corps K' est stable par produit, donc $a.\frac{1}{b} \in K'$, c'est-à-dire $\frac{a}{b} = x \in K'$. Cela prouve que $K \subseteq K'$, donc $K = K'$. $\square$

1.7.3 Exemples. Deux exemples classiques ont déjà été rencontrés lors des années précédentes:

(a) Le corps de fractions de l'anneau intègre $\mathbb{Z}$ est appelé corps des rationnels et est noté $\mathbb{Q}$.

(b) Le corps de fractions de l'anneau intègre de polynômes $\mathbb{R}[X]$ est appelé corps des fractions rationnelles à coefficients réels, et est noté $\mathbb{R}(X)$.

Plus généralement, pour tout anneau intègre A, le corps de fractions de l'anneau intègre $A[X]$ (voir 1.5.4) est appelé corps des fractions rationnelles à coefficients dans A. Ses éléments sont de la forme: $F(X) = \frac{P(X)}{Q(X)}$ avec $P, Q \in A[X]$, $Q \neq 0$.

A titre d'exercice, montrer que le corps de fractions de $\mathbb{Z}[i]$ est $\mathbb{Q}(i) = \{p + qi\,;\, p \in \mathbb{Q}, q \in \mathbb{Q}\}$.

1.8 Anneaux produits.

1.8.1 Proposition et définition. *Soient A_1 et A_2 deux anneaux commutatifs unitaires.*

(i) *Le produit cartésien $A_1 \times A_2 = \{(x_1, x_2),\ x_1 \in A_1,\ x_2 \in A_2\}$ est un anneau commutatif unitaire pour les lois définies par:*

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2) \quad \text{et} \quad (x_1, x_2).(y_1, y_2) = (x_1y_1, x_2y_2),$$

pour tous $x_1, y_1 \in A_1$, $x_2, y_2 \in A_2$, et l'on a $1_{A_1 \times A_2} = (1_{A_1}, 1_{A_2})$. Cet anneau est appelé le produit direct de A_1 par A_2. On le note $A = A_1 \times A_2$.

(ii) *L'application $p_1 : A_1 \times A_2 \to A_1$ qui, à tout élément $(x_1, x_2) \in A_1 \times A_2$, associe sa première composante x_1, est un morphisme d'anneaux unitaires (appelé première projection).*

(iii) *L'application $p_2 : A_1 \times A_2 \to A_2$ qui, à tout élément $(x_1, x_2) \in A_1 \times A_2$, associe sa seconde composante x_2, est un morphisme d'anneaux unitaires (appelé seconde projection).*

Preuve. Simple vérification, laissée au lecteur. $\square$

1.8.2 Remarques.

(a) Le produit direct $A_1 \times A_2$ est isomorphe au produit direct $A_2 \times A_1$.
(b) On définit de même de façon évidente le produit direct d'un nombre fini quelconque d'anneaux.
(c) Attention: l'anneau $A_1 \times A_2$ n'est pas intègre (même si A_1 et A_2 le sont, et même si ce sont des corps). *En effet,* les éléments $(1_{A_1}, 0_{A_2})$ et $(0_{A_1}, 1_{A_2})$ sont non-nuls, alors que leur produit l'est.

1.8.3 Proposition (théorème chinois). *Soient deux entiers $n \geq 2$ et $m \geq 2$. L'anneau produit $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est isomorphe à l'anneau $\mathbb{Z}/nm\mathbb{Z}$ si et seulement si n et m sont premiers entre eux.*

Preuve. D'après le corollaire 2.5.5 du chapitre 2 (voir aussi théorème 4.2.4 du chapitre 1), on sait que, pour n et m premiers entre eux, l'application $\overline{x} \mapsto (\widetilde{x}, \widehat{x})$ réalise un isomorphisme de groupes de $\mathbb{Z}/nm\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Il est clair, par définition même des multiplications dans ces différents anneaux, que c'est aussi un isomorphisme d'anneaux unitaires. La réciproque est évidente. $\square$

2.1 Notion d'idéal.

2.1.1 Définition. Soit A un anneau commutatif unitaire. On appelle *idéal* de A toute partie non-vide I de A qui vérifie les deux conditions suivantes:

(1) I est un sous-groupe du groupe additif A,

(2) pour tous $x \in I$ et $a \in A$, on a $xa \in I$.

Exemples.

(a) $\{0\}$ et A sont des idéaux de A.

(b) Pour tout $n \in \mathbb{Z}$, l'ensemble $n\mathbb{Z}$ des multiples de n est un idéal de l'anneau $\mathbb{Z}$.

(c) Dans l'anneau $\mathcal{F}(\mathbb{R}, \mathbb{R})$, l'ensemble des fonctions qui s'annulent en 0 est un idéal.

2.1.2 Lemme (très utile dans la pratique). *Soit A un anneau commutatif unitaire.*

(i) *si I est un idéal de A qui contient* 1, *alors $I = A$.*

(ii) *si I est un idéal de A qui contient un élément de $U(A)$, alors $I = A$.*

Preuve. Supposons $1 \in I$. Tout $a \in A$ s'écrit $a = 1.a$ donc, comme $1 \in I$, il résulte de la propriété (2) que $a \in I$. On a alors $A \subseteq I$, donc $A = I$, ce qui prouve (i). Supposons maintenant que I contienne un élément x inversible dans A. On a $1 = xx^{-1}$ avec $x \in I$ et $x^{-1} \in A$, donc $1 \in I$, et on applique (i) pour conclure que $I = A$. $\square$

2.1.3 Proposition. *Soient A et B des anneaux commutatifs unitaires. Soit $f : A \to B$ un morphisme d'anneaux unitaires. On a:*

(i) *Pour tout idéal J de B, l'image réciproque $f^{-1}(J)$ est un idéal de A.*

(ii) *En particulier,* $\operatorname{Ker} f = \{x \in A\,;\ f(x) = 0_B\}$ *est un idéal de A.*

(iii) *Pour tout idéal I de A, l'image directe $f(I)$ est un idéal de l'anneau $f(A) = \operatorname{Im} f$; (attention, ce n'est pas en général un idéal de B).*

Preuve. Sous les hypothèses de (i), on sait déjà que $f^{-1}(J)$ est un sous-groupe additif de A (voir 3.1.4 du chapitre 1). Soit $x \in f^{-1}(J)$ et $a \in A$. On a $f(xa) = f(x)f(a)$ avec $f(a) \in B$ et $f(x) \in J$, donc $f(xa) \in J$ puisque J est un idéal de B, c'est-à-dire $xa \in f^{-1}(J)$, ce qui prouve que $f^{-1}(J)$ est un idéal de A. On obtient (ii) en appliquant ce qui précède à $J = \{0_B\}$.

Pour (iii), considérons un idéal I de A. On sait que $f(I)$ est un sous-groupe additif de B. Soit $y \in f(I)$, de sorte qu'il existe $x \in I$ tel que $y = f(x)$. Pour tout élément $b \in B$ qui appartient à $\operatorname{Im} f$, il existe $a \in A$ tel que $b = f(a)$; on a alors $yb = f(a)f(x) = f(ax)$ avec $ax \in I$ puisque $x \in I$ et que I est un idéal, et donc $yb \in f(I)$. Ceci prouve que $f(I)$ est un idéal de l'anneau $\operatorname{Im} f$. $\square$

2.1.4 Proposition. *Soit A un anneau commutatif unitaire. L'intersection de deux idéaux de A est un idéal de A. Plus généralement, l'intersection d'une famille quelconque d'idéaux de A est un idéal de A.*

Preuve. Il suffit de montrer le second point. Soit donc $(I_j)_{j\in X}$ une famille d'idéaux de A. Posons $I = \bigcap_{j\in X} I_j$ l'intersection de tous les I_j. On sait déjà que I est un sous-groupe additif (proposition 1.2.6 du chapitre 1). Soient $x \in I$ et $a \in A$. On a $xa \in I_j$ pour tout $j \in X$ puisque I_j est un idéal, et donc $xa \in I$. Ce qui prouve que I est un idéal de A. $\square$

2.2 Idéal principal, idéal engendré par une partie, somme d'idéaux.

2.2.1 Proposition et définition. *Soit A un anneau commutatif unitaire. Pour tout $x \in A$:*

(i) *l'ensemble $xA = \{xy\,;\ y \in A\}$ est un idéal de A, appelé l'idéal principal engendré par x;*

(ii) *xA est le plus petit idéal de A contenant x;*

(iii) *on a:* $(\ xA = A\ ) \Leftrightarrow (\ x \in U(A)\ )$.

Preuve. Il est clair que xA est non-vide (il contient x puisque $x = x.1$). Soient $y \in xA$ et $z \in xA$ quelconques; il existe $a, b \in A$ tels que $y = xa$ et $z = xb$, donc $y - z = x(a - b) \in xA$, ce qui prouve que xA est un sous-groupe additif. Soient $y \in xA$ et $c \in A$ quelconques; il existe $a \in A$ tel que $y = xa$, donc $yc = xac = x(ac) \in xA$. On conclut que xA est un idéal de A.

Soit I un idéal de A contenant x. Comme $x \in I$, on a $xa \in I$ pour tout $a \in A$. Donc $xA \subseteq I$, d'où (ii).

Si $xA = A$, alors $1 \in xA$, de sorte qu'il existe $y \in A$ tel que $xy = 1$, ce qui prouve $x \in U(A)$. L'implication réciproque découle de 2.1.2.(ii). □

Bien que très simple, le corollaire suivant est important, et montre que la notion d'idéal n'a d'intérêt que pour des anneaux qui ne sont pas des corps.

2.2.2 Corollaire. *Soit A un anneau commutatif unitaire.*

$$(\ A \text{ est un corps }) \Leftrightarrow (\ \text{les seuls idéaux de } A \text{ sont } \{0\} \text{ et } A\ ).$$

Preuve. Supposons que A est un corps. Soit I un idéal de A. Si $I \neq \{0\}$, il existe dans I un élément non-nul, donc inversible dans A puisque A est un corps. On conclut avec 2.1.2.(ii) que $I = A$. Supposons réciproquement que A n'admette que $\{0\}$ et A comme idéaux. Soit $x \in A$ quelconque non-nul. L'idéal xA étant alors distinct de $\{0\}$, on a nécessairement $xA = A$, d'où $x \in U(A)$ d'après 2.2.1.(iii). Ainsi tout élément non-nul de A est inversible dans A: on conclut que A est un corps. □

2.2.3 Proposition et définition. *Soit A un anneau commutatif unitaire.*

(i) *Si I et J sont des idéaux de A, alors l'ensemble $I + J = \{x + y\,;\ x \in I, y \in J\}$ est un idéal de A, appelé l'idéal somme de I et J, et c'est le plus petit idéal contenant I et J;*

(ii) *En particulier, si x et y sont des éléments de A, l'ensemble $xA + yA = \{xa + yb\,;\ a, b \in A\}$ est le plus petit idéal de A contenant x et y.*

Preuve. Soient I et J deux idéaux de A. Il est clair que $I + J$ est un sous-groupe additif de A (c'est le sous-groupe engendré par $I \cup J$). Soit $z \in I + J$ et $a \in A$ quelconques; il existe $x \in I$ et $y \in J$ tels que $z = x + y$, d'où $za = xa + ya$. Or $xa \in I$ car $x \in I$ et I est un idéal; de même $ya \in J$. On conclut que $za \in I + J$, ce qui prouve que $I + J$ est un idéal de A. Il est clair que $I \subseteq I + J$, puisque tout $x \in I$ s'écrit $x = x + 0$ avec $0 \in J$; de même $J \subseteq I + J$. Pour montrer que c'est le plus petit, supposons que K est un idéal de A contenant I et J. En particulier, K est stable par addition, et donc, quels que soient $x \in I \subseteq K$ et $y \in J \subseteq K$, on a $x + y \in K$. Donc $I + J \subseteq K$. Ce qui achève de prouver (i). Le point (ii) s'en déduit avec $I = xA$ et $J = yA$. □

2.2.4 Remarques. Soit A un anneau commutatif unitaire.

(a) On définit généralement, pour toute partie non-vide X de A, l'idéal engendré par X comme l'intersection de tous les idéaux contenant X; c'est le plus petit idéal de A contenant X.

La proposition 2.2.1 correspond à $X = \{x\}$, le point (i) de 2.2.3 à $X = I \cup J$, et le point (ii) de 2.2.3 à $X = \{x, y\}$.

(b) L'intérêt de la notion d'idéal somme réside bien sûr dans le fait que la réunion de deux idéaux n'est en général pas un idéal (ce n'est pas en général un sous-groupe additif; prendre par exemple $A = \mathbb{Z}$, $I = 2\mathbb{Z}$ et $J = 3\mathbb{Z}$).

2.3 Produit d'idéaux, opérations sur les idéaux.

2.3.1 Définition et proposition. *Soit A un anneau commutatif unitaire. Si I et J sont des idéaux de A, on appelle produit des idéaux I et J, et on note IJ, l'ensemble des éléments de A qui sont somme d'un nombre fini de produits d'un élément de I par un élément de J.*

$$(\ x \in IJ\ ) \Leftrightarrow (\ \text{il existe } n \in \mathbb{N}^*,\ y_1, \ldots, y_n \in I,\ z_1, \ldots, z_n \in J, \text{ tels que } x = \sum_{i=1}^{n} y_i z_i\ ).$$

Alors IJ est un idéal de A, et c'est le plus petit idéal contenant l'ensemble $\{yz\,;\ y \in I, z \in J\}$.

Preuve. Il est clair que IJ est un sous-groupe additif de A. Soit $x = \sum_{i=1}^{n} y_i z_i$ un élément quelconque de IJ, avec $y_1, \dots, y_n \in I$ et $z_1, \dots, z_n \in J$. Pour tout $a \in A$, on a $ay_i \in I$ quel que soit $1 \leq i \leq n$, donc $ax = \sum_{i=1}^{n} (ay_i)z_i$ appartient encore à IJ. Ceci prouve que IJ est un idéal. Il est clair qu'il contient $X = \{yz\,;\, y \in I, z \in J\}$. Soit maintenant K un idéal qui contient X. Il contient aussi les sommes d'éléments de X, et donc $IJ \subseteq K$. □

2.3.2 Proposition. *Soit A un anneau commutatif unitaire. Si I, J et K sont des idéaux de A, on a:*

$$I + (J + K) = (I + J) + K, \qquad I(JK) = (IJ)K, \qquad I(J + K) = IJ + IK.$$

2.4 Caractéristique d'un anneau.

2.4.1 Remarques préliminaires.

(a) Pour tout idéal I de l'anneau $\mathbb{Z}$, il existe un unique $k \in \mathbb{N}$ tel que $I = k\mathbb{Z}$.

En effet, cela résulte immédiatement de l'exemple (b) du 2.1.1 de ce chapitre, et du 2.5.2 du chapitre 2.

(b) Soit A un anneau commutatif unitaire. Pour tout $x \in A$, on note $2x = x+x$, $3x = x+x+x$ et de même $nx = x + x + \cdots + x$ (avec n termes) pour tout entier $n \geq 2$. On pose naturellement $1x = x$ et $0x = 0$, ce qui définit la notation nx pour tout $n \in \mathbb{N}$. Si l'on considère maintenant un entier $m \leq 0$, on convient que $mx = n(-x) = -(nx)$ où $n = -m \in \mathbb{N}$. On a ainsi défini la notation nx pour tout $x \in A$ et tout $n \in \mathbb{Z}$.

(c) Soit A un anneau commutatif unitaire. On vérifie aisément que, pour tout $n \in \mathbb{Z}$, on a:

$$(\ n1_A = 0_A\ ) \Leftrightarrow (\ nx = 0_A \ \text{ pour tout } x \in A\ ).$$

2.4.2 Lemme et définition. *Soit A un anneau commutatif unitaire. Il existe un unique morphisme d'anneaux unitaires $f : \mathbb{Z} \to A$. Il est défini par $f(n) = n1_A$ pour tout $n \in \mathbb{Z}$. On l'appelle le morphisme canonique de $\mathbb{Z}$ dans A.*

Preuve. Si f est un morphisme d'anneaux unitaires $\mathbb{Z} \to A$, on doit avoir $f(1) = 1_A$, d'où par additivité $f(2) = f(1) + f(1) = 1_A + 1_A = 21_A$, et par récurrence $f(n) = n1_A$ pour tout entier $n \geq 1$. Comme f est un morphisme de groupes additifs, on a aussi $f(0) = 0_A$ et $f(m) = f(-n) = -f(n) = -(n1_A) = (-n)1_A = m1_A$ pour tout entier $m \leq 0$ et en posant $n = -m$. En résumé, on a $f(n) = n1_A$ pour tout $n \in \mathbb{Z}$. Réciproquement, il est facile de vérifier (faites-le) que f ainsi défini est bien un morphisme d'anneaux unitaires. □

2.4.3 Définition. Soit A un anneau commutatif unitaire. On appelle *caractéristique* de A, notée $\operatorname{car} A$, l'unique entier $k \in \mathbb{N}$ tel que $\operatorname{Ker} f = k\mathbb{Z}$, où f est le morphisme canonique de $\mathbb{Z}$ dans A.

Comme $f : \mathbb{Z} \to A$ est un morphisme d'anneaux unitaires d'après 2.4.2, $\operatorname{Ker} f$ est un idéal de $\mathbb{Z}$ d'après 2.1.3.(ii), et il est donc de la forme $k\mathbb{Z}$ pour un unique $k \in \mathbb{N}$ d'après 2.4.1.(a).

Grâce à la remarque 2.4.1.(c), cette définition se traduit par:

$$\operatorname{car} A = 0 \ \Leftrightarrow\ \Big[\ (nx = 0_A \text{ pour tout } \ x \in A\ ) \Leftrightarrow (n = 0)\ \Big]$$

$$\operatorname{car} A = k > 0 \ \Leftrightarrow\ \Big[\ (nx = 0_A \text{ pour tout } \ x \in A\ ) \Leftrightarrow (n \in k\mathbb{Z})\ \Big]$$

2.4.4 Exemples.

(a) L'anneau $\mathbb{Z}$ est de caractéristique nulle, ainsi que les corps $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(b) Pour tout $n \geq 2$, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est de caractéristique n. En particulier, pour tout nombre premier p, le corps $\mathbb{Z}/p\mathbb{Z}$ est de caractéristique p.

(c) Soit A un anneau commutatif unitaire. Pour tout sous-anneau unitaire B de A, on a:

$$\operatorname{car} A = \operatorname{car} B.$$

3.1 Quotient d'un anneau par un idéal.

3.1.1 Remarques préliminaires. Soit A un anneau commutatif unitaire. Soit I un idéal de A.

(a) L'idéal I est en particulier un sous-groupe du groupe additif A, et il est trivialement normal puisque A est abélien. On peut considérer le groupe additif quotient A/I. Rappelons que, si l'on note $\overline{a}$ la classe dans A/I d'un élément a de A, on a par définition:

$$\overline{a} = \{b \in A\,;\, a - b \in I\} := a + I,$$

et que l'addition dans A/I est définie par:

$$\overline{a} + \overline{b} = \overline{a+b} \quad \text{pour tous } a, b \in A,$$

d'où en particulier A/I abélien, de neutre additif $\overline{0} = I$. La surjection canonique $p : A \to A/I$, qui à tout élément a de A associe sa classe $\overline{a}$ est alors un morphisme de groupes pour l'addition.

(b) On définit dans A/I une multiplication en posant:

$$\overline{a}.\overline{b} = \overline{ab} \quad \text{pour tous } a, b \in A,$$

1. Elle est bien définie, indépendamment des représentants choisis.

   En effet. Soient $x' \in \overline{x}$ et $y' \in \overline{y}$. Alors $x' - x \in I$ et $y' - y \in I$. On a: $x'y' - xy = (x' - x + x)(y' - y + y) - xy = (x' - x)(y' - y) + (x' - x)y + x(y' - y)$. Comme $x' - x \in I$ et que I est un idéal, on a $(x' - x)(y' - y) \in I$ et $(x' - x)y \in I$; de même $x(y' - y) \in I$ puisque $y' - y \in I$. On conclut que $x'y' - xy \in I$ comme somme de trois éléments de I, et donc $\overline{x'y'} = \overline{xy}$.

2. Elle est associative, commutative, distributive sur l'addition dans A/I, et admet $\overline{1}$ comme élément neutre.

   En effet. Quels que soient $x, y, z \in A$, on a $(\overline{x}\,\overline{y})\,\overline{z} = \overline{(xy)z} = \overline{x(yz)} = \overline{x}\,(\overline{y}\,\overline{z})$, ce qui montre l'associativité. Le reste se montre de même. □

3. La surjection canonique p vérifie $p(1) = \overline{1}$ et $p(xy) = p(x)p(y)$ pour tous $x, y \in A$.

   En effet. Par définition de p d'une part, et de la multiplication dans A/I d'autre part, on a $p(xy) = \overline{xy} = \overline{x}\,\overline{y} = p(x)p(y)$. □

On a ainsi démontré:

3.1.2 Théorème. *Soit A un anneau commutatif unitaire. Pour tout idéal I de A, le quotient A/I est un anneau commutatif, et la surjection canonique $p : A \to A/I$ est un morphisme d'anneaux unitaires.*

On a pour les anneaux quotients des résultats de même nature que ceux que l'on a montré au chapitre 2 pour les groupes quotients, en particulier:

3.1.3 Théorème (dit premier théorème d'isomorphisme). *Soient A et A' deux anneaux commutatifs unitaires, et $f : A \to A'$ un morphisme d'anneaux unitaires. Alors l'anneau quotient de A par l'idéal* $\operatorname{Ker} f$ *est isomorphe au sous-anneau* $\operatorname{Im} f = f(A)$ *de A'. On note:* $\quad A/\operatorname{Ker} f \simeq \operatorname{Im} f$.

Preuve. En reprenant la preuve du théorème 2.3.1 du chapitre 2, on sait déjà que l'application:

$$\begin{array}{rrcl} \varphi : & A/\operatorname{Ker} f & \longrightarrow & \operatorname{Im} f \\ & \overline{x} & \longmapsto & f(x) \end{array}$$

est bien définie et réalise un isomorphisme de groupes additifs de $A/\operatorname{Ker} f$ sur $\operatorname{Im} f$. Par ailleurs, en utilisant le fait que f est un morphisme d'anneaux unitaires, on a clairement $\varphi(\overline{1_A}) = f(1_A) = 1_{A'}$ et $\varphi(\overline{x}\,\overline{y}) = \varphi(\overline{xy}) = f(xy) = f(x)f(y) = \varphi(\overline{x})\varphi(\overline{y})$ pour tous $x, y \in A$, ce qui achève de prouver que φ est un isomorphisme d'anneaux. □

3.1.4 Proposition (idéaux d'un anneau quotient). *Soient A un anneau commutatif et I un idéal de A. Tout idéal de A/I est de la forme J/I pour J un unique idéal de A contenant I, avec la notation naturelle $J/I = p(J)$.*

Preuve. Soit K un idéal de A/I. Posons $J = p^{-1}(K) = \{x \in A\,;\, p(x) \in K\}$. En tant qu'image réciproque d'un idéal par un morphisme d'anneaux, J est un idéal de A. Si $x \in I$, on a $p(x) = \overline{0}$, donc $p(x) \in K$, de sorte que $x \in p^{-1}(K)$, c'est-à-dire $x \in J$. Ceci montre que $I \subseteq J$. Par définition de J, on a $p(J) \subseteq K$. Réciproquement, soit $\overline{x} \in K$, avec $x \in A$; comme $p(x) = \overline{x} \in K$, on a clairement $x \in p^{-1}(K) = J$, et donc $\overline{x} = p(x) \in p(J)$. En résumé, $K = p(J)$, ce que l'on note $K = J/I$.

On renvoie pour l'unicité à la preuve de la proposition 3.3.1 du chapitre 2. □

3.1.5 Exemple. Fixons un entier $n \geq 2$. Alors $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$, et l'anneau quotient n'est autre que l'anneau commutatif unitaire $\mathbb{Z}/n\mathbb{Z}$ déjà considéré en 1.1.3. Pour tout diviseur q de n, il existe un et un seul idéal de $\mathbb{Z}/n\mathbb{Z}$ d'ordre q, qui est $d\mathbb{Z}/n\mathbb{Z}$ où $n = dq$ (voir aussi 2.5.4.(iv) du chapitre 2). Réciproquement tout idéal de $\mathbb{Z}/n\mathbb{Z}$ est de ce type.

Exemple: dans $\mathbb{Z}/12\mathbb{Z}$, les idéaux sont: $\{\overline{0}\} = 12\mathbb{Z}/12\mathbb{Z}$, $\{\overline{0},\overline{6}\} = 6\mathbb{Z}/12\mathbb{Z}$, $\{\overline{0},\overline{4},\overline{8}\} = 4\mathbb{Z}/12\mathbb{Z}$, $\{\overline{0},\overline{3},\overline{6},\overline{9}\} = 3\mathbb{Z}/12\mathbb{Z}$, $\{\overline{0},\overline{2},\overline{4},\overline{6},\overline{8},\overline{10}\} = 2\mathbb{Z}/12\mathbb{Z}$ et $\mathbb{Z}/12\mathbb{Z}$. □

Citons encore les deux résultats généraux suivants (on ne détaille pas les preuves, qui sont de simples adaptations de celles de 3.1.1 et 3.1.3 du chapitre 2), et précisons que les théorèmes 3.2.1 et 3.3.2 du chapitre 2 ont aussi leurs analogues pour les anneaux (on laisse au lecteur le soin d'en préciser l'énoncé et la preuve).

3.1.6 Théorème (propriété universelle de l'anneau quotient) *Soient A un anneau commutatif unitaire, I un idéal de A, et p la surjection canonique $A \to A/I$.*

(i) *Pour tout anneau commutatif unitaire A' et tout morphisme d'anneaux unitaires $f : A \to A'$ tel que $I \subseteq \operatorname{Ker} f$, il existe un unique morphisme d'anneaux unitaires $\varphi : A/I \to A'$ tel que $f = \varphi \circ p$.*

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "p"'] & A' \\ A/I \arrow[ur, "\varphi"'] & \end{tikzcd}$$

(ii) *De plus: (f surjectif $\Rightarrow$ φ surjectif) et ($I = \operatorname{Ker} f$ $\Rightarrow$ φ injectif).*

3.1.7 Lemme (fondamental de factorisation). *Soient A un anneau commutatif unitaire, I un idéal de A, et p la surjection canonique $A \to A/I$. Soient A' un anneau commutatif unitaire, I' un idéal de A', et p' la surjection canonique $A' \to A'/I'$. Alors, pour tout morphisme d'anneaux unitaires $f : A \to A'$ vérifiant la condition $f(I) \subseteq I'$, il existe un unique morphisme $\varphi : A/I \to A'/I'$ tel que $\varphi \circ p = p' \circ f$.*

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "p"'] \arrow[dr, "g"'] & A' \arrow[d, "p'"] \\ A/I \arrow[r, "\varphi"'] & A'/I' \end{tikzcd}$$

3.2 Idéaux premiers, idéaux maximaux.

3.2.1 Définitions. Soit A un anneau commutatif unitaire.

Un idéal P de A est dit *premier* lorsque $P \neq A$ et vérifie:

quels que soient deux éléments x et y de A, si $xy \in P$, alors $x \in P$ ou $y \in P$.

Un idéal M de A est dit *maximal* lorsque $M \neq A$ et vérifie:

quel que soit I un idéal de A, si M est strictement inclus dans I, alors $I = A$.

3.2.2 Théorème. *Soit I un idéal d'un anneau commutatif unitaire A. On a:*

$$\begin{array}{ccc} I \text{ maximal} & \Longleftrightarrow & A/I \text{ corps} \\ \Big\Downarrow & & \Big\Downarrow \\ I \text{ premier} & \Longleftrightarrow & A/I \text{ intègre} \end{array}$$

Preuve. Supposons que M est un idéal maximal de A. Comme $M \neq A$, l'anneau A/M est non-nul. Considérons un idéal quelconque K de A/M. D'après la proposition 3.1.4, il existe un idéal J de A tel que $M \subseteq J$ et $K = J/M$. Mais, par maximalité de M, l'inclusion $M \subseteq J$ implique que $J = M$ ou $J = A$, c'est-à-dire $J/M = \{\overline{0}\}$ ou $J/M = A/M$. Ceci prouve que les seuls idéaux de A/M sont $\{\overline{0}\}$ et A/M. On conclut avec 2.2.2 que A/M est un corps. L'implication réciproque découle des mêmes calculs. L'équivalence de la première ligne est donc vérifiée.

Supposons que P est un idéal premier de A. Comme $P \neq A$, l'anneau A/P est non-nul. Considérons $\overline{x}, \overline{y} \in A/P$ tels que $\overline{x}\,\overline{y} = \overline{0}$. On a $\overline{xy} = \overline{0}$, c'est-à-dire $xy \in P$. Comme P est premier, on a $x \in P$ ou $y \in P$, c'est-à-dire $\overline{x} = \overline{0}$ ou $\overline{y} = \overline{0}$. Donc A/P est intègre. L'implication réciproque découle des mêmes calculs. L'équivalence de la seconde ligne est donc vérifiée.

Il suffit de rappeler que tout corps est un anneau intègre, voir 1.5.2.(a), pour achever la preuve. □

3.2.3 Remarques.

(a) Par définition, ($\{0\}$ premier) $\Leftrightarrow$ (A intègre). Si A est un corps, l'idéal $\{0\}$ est l'unique idéal maximal de A, et si A n'est pas un corps, $\{0\}$ n'est pas maximal (résulte de 2.2.2).

(b) Dans l'anneau $\mathbb{Z}$, considérons un idéal quelconque I. D'après 2.4.1.(a), il existe $k \in \mathbb{N}$ unique tel que $I = k\mathbb{Z}$. Si $k = 1$, alors $I = \mathbb{Z}$ n'est ni premier, ni maximal. Si $k = 0$, alors $I = \{0\}$ est premier mais non maximal (voir remarque précédente). Si maintenant $k \geq 2$, il résulte de la proposition 1.5.3 et du théorème 3.2.2 que:

$$(\ k\mathbb{Z} \text{ est premier }) \ \Leftrightarrow\ (\ k \text{ est un nombre premier }) \Leftrightarrow\ (\ k\mathbb{Z} \text{ est maximal })$$

Ainsi dans l'anneau $\mathbb{Z}$, les notions d'idéal maximal et d'idéal premier non-nul coïncident. On verra plus loin que c'est le cas pour toute une vaste famille d'anneaux (les anneaux principaux) à laquelle appartient $\mathbb{Z}$.

(c) Il existe des anneaux commutatifs unitaires A possédant des idéaux premiers non-nuls qui ne sont pas maximaux.

Exemple. Prenons $A = \mathbb{Z}[X]$ et $I = XA$ l'idéal principal engendré par X. Soit $f : A \to \mathbb{Z}$ l'application qui à tout polynôme $P = a_m X^m + \cdots + a_1 X + a_0$, avec les $a_i \in \mathbb{Z}$, associe le terme constant a_0. Il est facile de vérifier que f est un morphisme d'anneaux unitaires, qu'il est surjectif, et que son noyau est $I = XA$. D'après 3.1.3, on a alors $A/I \simeq \mathbb{Z}$. Comme $\mathbb{Z}$ est intègre sans être un corps, l'idéal I est premier sans être maximal. □

(d) Le définition d'un idéal premier que l'on a donné en 3.2.1 en termes de produits d'éléments est équivalente (parce qu'on se limite à des anneaux commutatifs) à la caractérisation suivante en termes de produits d'idéaux, dont on laisse la démonstration au lecteur à titre d'exercice.

Soit A un anneau commutatif unitaire. Un idéal P de A distinct de A est premier si et seulement s'il vérifie: (I et J idéaux de A et $IJ \subseteq P$) $\Rightarrow$ ($I \subseteq P$ ou $J \subseteq P$).

3.2.4 Lemme. *Soient A et B des anneaux commutatifs unitaires.*

(i) *Si $f : A \to B$ est un morphisme d'anneaux unitaires, alors, quel que soit Q un idéal premier de B, l'image réciproque $f^{-1}(Q)$ est un idéal premier de A, qui contient* $\operatorname{Ker} f$.

(ii) *Si $f : A \to B$ est un morphisme d'anneaux unitaires* surjectif, *alors, quel que soit P un idéal premier de A contenant* $\operatorname{Ker} f$, *l'image directe $f(P)$ est un idéal premier de B.*

(iii) *Soit A un anneau commutatif unitaire et I un idéal de A, distinct de A. Les idéaux premiers de A/I sont de la forme P/I où P est un idéal premier de A contenant I.*

Preuve. On prouve (ii), en laissant au lecteur le soin de rédiger de même la preuve de (i). Comme f est supposée surjective, on sait d'après 2.1.3.(iii) que $f(P)$ est un idéal de $B = f(A)$. Montrons d'abord que $f(P) \neq B$. Par l'absurde, supposons $B = f(P)$. Quel que soit $a \in A$, il existerait alors $x \in P$ tel que $f(a) = f(x)$, d'où $a - x \in \operatorname{Ker} f$. Puisque $\operatorname{Ker} f \subseteq P$, on aurait $a - x \in P$, ce qui impliquerait $a \in P$; on obtiendrait $A = P$, ce qui contredit la primalité de P dans A. On conclut donc $f(P) \neq B$.

Soient maintenant $a, b \in B$ tels que $ab \in f(P)$. Par surjectivit de f, il existe $x, y \in A$ tels que $a = f(x)$ et $b = f(y)$. On a $f(xy) = f(x)f(y) = ab \in f(P)$, donc il existe $c \in P$ tel que $f(xy) = f(c)$, d'où $xy - c \in \operatorname{Ker} f$. Comme $\operatorname{Ker} f \subseteq P$, ceci implique $xy - c \in P$, et en rappelant que $c \in P$, il vient $xy \in P$. La primalité de P implique $x \in P$ ou $y \in P$, d'où $a \in f(P)$ ou $b \in f(P)$. Ceci prouve (ii).

D'après 3.1.4, le point (iii) se déduit immédiatement de (ii) en prenant $B = A/I$ et f la surjection canonique $A \to A/I$. □

3.2.5 Exemple d'application (cas des polynômes). Soit A un anneau commutatif unitaire. Pour tout idéal I de A, on note $I[X]$ le sous-ensemble de $A[X]$ formé des polynômes à coefficients dans I, c'est-à-dire de la forme: $\sum_{i=0}^{n} a_i X^i$, avec $n \geq 0$ et $a_0, a_1, \dots, a_n \in I$. Alors on a:

(i) $I[X]$ est un idéal de $A[X]$;

(ii) les anneaux $(A/I)[X]$ et $A[X]/I[X]$ sont isomorphes;

(iii) $I[X]$ est un idéal premier de $A[X]$ si et seulement si I est un idéal premier de A.

Preuve. Le point (i) est une simple vérification. Pour le (ii), considérons la surjection canonique $p : A \to A/I$ et définissons son extension canonique:

$$\begin{array}{rrcl} f : & A[X] & \longrightarrow & (A/I)[X] \\ & P = \sum\limits_{i=0}^{n} a_i X^i & \longmapsto & f(P) = \sum\limits_{i=0}^{n} p(a_i) X^i \end{array}$$

Il est clair que f est un morphisme d'anneaux unitaires, qu'il est surjectif, et que son noyau est $\operatorname{Ker} f = I[X]$. L'isomorphisme $A[X]/\operatorname{Ker} f \simeq \operatorname{Im} f$ devient donc $A[X]/I[X] \simeq (A/I)[X]$. Pour (iii), rappelons que I est premier si et seulement si A/I est intègre, ce qui équivaut d'après 1.5.4.(ii) à $(A/I)[X]$ intègre, c'est-à-dire $A[X]/I[X]$ intègre d'après le point (ii), ou encore $I[X]$ premier dans $A[X]$. □

3.3 Théorème de Krull.

Le théorème suivant est un résultat important et non trivial qui démontre l'existence d'idéaux maximaux dans tout anneau unitaire commutatif. Sa preuve utilise des arguments d'algèbre générale sur les structures ordonnées, dont le lemme de Zorn, et on ne donnera ci-dessous que le plan général de la preuve, sans entrer dans le détail des justifications de chaque étape.

3.3.1 Théorème (de Krull). *Tout anneau commutatif unitaire a un moins un idéal maximal.*

Grandes lignes de la preuve. Soit A un anneau commutatif unitaire. Soit E l'ensemble de tous les idéaux de A distincts de A. Il est non vide, car contient au moins $\{0\}$. L'inclusion définit une relation d'ordre dans E. Ce n'est pas un ordre total, mais seulement un ordre partiel (c'est-à-dire que, si $I, J \in E$ quelconques, on n'a pas forcément $I \subseteq J$ ou $J \subseteq I$).

Soit $F = (I_k)_{k \in X}$ une famille d'éléments de E totalement ordonnée par l'inclusion (quels que soient $k, \ell \in X$, on a $I_k \subseteq I_\ell$ ou $I_\ell \subseteq I_k$). On peut facilement vérifier qu'alors $I = \bigcup_{k \in X} I_k$ est un idéal de A. (Rappelons qu'en général une réunion d'idéaux n'est pas un idéal, mais le fait que I soit ici un idéal provient du fait que tous les I_k sont emboités puisque la famille est totalement ordonnée). L'idéal I est distinct de A (car sinon on aurait $1 \in I$, donc il existerait $k \in X$ tel que $1 \in I_k$, d'où $I_k = A$, ce qui contredirait $I_k \in E$). Donc $I \in E$, et il est clair que tout $I_k \in F$ vérifie $I_k \subseteq I$. En résumé, toute famille déléments de E totalement ordonnée admet un plus grand élément. On traduit cette propriété en disant que l'ensemble partiellement ordonné E est *inductif.*

Or un résultat d'algèbre très général (et non trivial) sur les structures ordonnées (le lemme de Zorn) affirme que tout ensemble (non vide) ordonné inductif admet (au moins) un élément maximal. Soit donc M un élément maximal de E. Cela signifie que, quel que soit un $J \in E$ tel que $M \subseteq J$, on a $J = M$. En d'autres termes, quel que soit un idéal J de A tel que $J \neq A$ et $M \subseteq J$, on a $J = M$. □

3.3.2 Corollaire. *Soit A un anneau commutatif unitaire.*

(i) *Pour tout idéal I de A, distinct de A, les idéaux maximaux de A/I sont de la forme M/I où M est un idéal maximal de A contenant I.*

(ii) *Tout idéal distinct de A est contenu dans un idéal maximal de A.*

(iii) *Tout élément de A non inversible dans A est contenu dans un idéal maximal de A.*

Preuve. Soit I un idéal de A tel que $I \neq A$. D'après 3.3.1, l'anneau A/I admet un idéal maximal N. D'après 3.1.4, il existe un unique idéal M de A contenant I tel que $N = M/I$, où M/I désigne l'image $p(M)$ de M par la surjection canonique $p : A \to A/I$. On se propose de montrer que M est un idéal maximal de A. Pour cela, soit J un idéal de A tel que $M \subseteq J$. On a donc $I \subseteq M \subseteq J \subseteq A$, ce qui implique pour les images par p que $M/I \subseteq J/I \subseteq A/I$. La maximalité de l'idéal $N = M/I$ implique $J/I = M/I$ ou $J/I = A/I$, c'est-à-dire $J = M$ ou $J = A$. On conclut que M est un idéal maximal de A, ce qui prouve à la fois (i) et (ii). Le point (iii) résulte immédiatement du (ii) et de 2.2.1.(iii). □

4. Anneaux euclidiens, anneaux principaux.

4.1 Multiples, diviseurs et idéaux principaux.

4.1.1 Définitions. Soit A un anneau commutatif unitaire. Soient x et y deux éléments de A. On dit que x est un *diviseur* de y dans A, ou encore que x *divise* y dans A, ou encore que y est un *multiple* de x dans A, lorsqu'il existe $a \in A$ tel que $y = xa$. On note alors: $x|y$.

4.1.2 Proposition. *Soit A un anneau commutatif unitaire. Pour tous $x, y \in A$, on a:*

$$(\ x|y \ ) \Leftrightarrow (\ y \in xA \ ) \Leftrightarrow (\ yA \subseteq xA \ ).$$

Preuve. Supposons que $x|y$. Il existe $a \in A$ tel que $y = xa$. Donc $y \in xA$. De plus, tout élément de yA est de la forme yb avec $b \in A$, donc de la forme xab, et donc appartient à xA, ce qui montre que $yA \subseteq xA$. La réciproque est claire. □

4.2 Notion d'anneau euclidien.

4.2.1 Proposition (exemple préliminaire de l'anneau $\mathbb{Z}$). *Quels que soient des entiers a et b, avec $b \neq 0$, il existe $q \in \mathbb{Z}$ et $r \in \mathbb{N}$ uniques tels que $a = bq + r$ et $0 \leq r < |b|$.*

Preuve. Pour montrer l'unicité, supposons l'existence de deux couples (q, r) et (q', r') dans $\mathbb{Z} \times \mathbb{N}$ satisfaisant aux conditions $a = bq + r$ avec $0 \leq r < |b|$, et $a = bq' + r'$ avec $0 \leq r' < |b|$. On a alors $b(q - q') = r' - r$ et $-|b| < r' - r < |b|$. Donc $-|b| < b(q - q') < |b|$. Comme $b \neq 0$, on en déduit que $-1 < q - q' < 1$, ce qui, puisque $q - q'$ est un entier, implique $q - q' = 0$. Ainsi $q = q'$, d'où $r = r'$.

Pour montrer l'existence, supposons d'abord $b > 0$. Posons $B = \{k \in \mathbb{Z} ; kb \leq a\}$. C'est une partie de $\mathbb{Z}$ qui est non-vide (car $0 \in B$ si $a \geq 0$ et $a \in B$ si $a < 0$) et qui est majorée (par le maximum des entiers a et 0). Donc elle admet un plus grand élément. Notons-le q. On a par définition de q la double inégalité $qb \leq a < (q + 1)b$, de sorte que l'entier $r = a - qb$ vérifie $0 \leq r < b$.

Supposons maintenant $b < 0$. D'après ce qui précède, il existe $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que $a = (-b)q + r$ et $0 \leq r < |b|$. Le couple $(-q, r) \in \mathbb{Z} \times \mathbb{N}$ vérifie alors $a = b(-q) + r$ et $0 \leq r < |b|$. □

4.2.2 Proposition (exemple préliminaire de l'anneau $K[X]$). *Soit K un corps commutatif. Quels que soient des polynômes F et G dans $K[X]$, avec $G \neq 0$, il existe $Q \in K[X]$ et $R \in K[X]$ uniques tels que $F = GQ + R$ et $\deg R < \deg G$.*

Preuve. Pour montrer l'unicité, supposons que deux couples (Q, R) et (Q', R') dans $K[X] \times K[X]$ satisfassent aux conditions $F = GQ + R = GQ' + R'$ avec $\deg R < \deg G$ et $\deg R < \deg G'$. On a alors: $G(Q - Q') = R' - R$. Comme K est un corps (en particulier intègre), on a d'après 1.5.4.(i) l'égalité $\deg G + \deg(Q - Q') = \deg(R' - R)$. Or $\deg R < \deg G$ et $\deg R' < \deg G$ implique d'après 1.1.4.(e) que $\deg(R' - R) < \deg G$. Donc $\deg G + \deg(Q - Q') < \deg G$, ce qui n'est possible que si $\deg(Q - Q') = -\infty$, c'est-à-dire $Q = Q'$. On a alors forcément aussi $R = R'$.

Pour montrer l'existence, notons $n = \deg F$ et $m = \deg G \in \mathbb{N}$. Si $n < m$, on a le résultat voulu en prenant $Q = 0$ et $R = F$. On suppose donc désormais que $n \geq m \geq 0$. Notons:

$$F = a_n X^n + \cdots + a_1 X + a_0 \quad \text{et} \quad G = b_m X^m + \cdots + b_1 X + b_0$$

avec les a_i et les b_j dans K, tels que $a_n \neq 0 \neq b_m$.

Si $n = m = 0$, alors $F = a_0 \neq 0$ et $G = b_0 \neq 0$, donc $F = (a_0 b_0^{-1})G$, ce qui prouve le résultat voulu avec $Q = a_0 b_0^{-1}$ et $R = 0$.

Par récurrence sur n, supposons la propriété voulue vraie pour G et tout polynôme F_1 de degré n_1 tel que $n > n_1 \geq m \geq 0$. Or on peut écrire $F = a_n b_m^{-1} X^{n-m} G + F_1$ avec $\deg F_1 \leq n - 1 < n$. Par hypothèse de récurrence, il existe $Q_1, R_1 \in K[X]$ tels que $F_1 = Q_1 G + R_1$ et $\deg R_1 < \deg G$. On déduit que $F = (a_n b_m^{-1} X^{n-m} + Q_1)G + R_1$, ce qui prouve le résultat voulu avec $Q = a_n b_m^{-1} X^{n-m} + Q_1$ et $R = R_1$. □

4.2.3 Définition. On appelle *anneau euclidien* un anneau commutatif unitaire qui est intègre, et pour lequel il existe une application $\delta : A^* \to \mathbb{N}$ vérifiant les deux conditions suivantes:

1. pour tous $a, b \in A^*$, $(\ a|b\ ) \Rightarrow (\ \delta(a) \leq \delta(b)\ )$;
2. pour tout $a \in A$ et $b \in A^*$, il existe $q, r \in A$ tels que:
$$(\ a = bq + r\ ) \quad \text{et} \quad (\ r = 0 \ \text{ ou } \ \delta(r) < \delta(b)\ ).$$

Une application δ vérifiant ces deux conditions s'appelle un *stathme* euclidien. Dans la condition 2, on dit que q est un *quotient* et r un *reste* dans la *division euclidienne* de a par b.

4.2.4 Exemples.

(a) L'anneau $\mathbb{Z}$ est euclidien, pour le stathme défini par $\delta(x) = |x|$ pour tout $x \in \mathbb{Z}^*$.

(b) Si K est un corps, l'anneau $K[X]$ est euclidien, pour le stathme défini par $\delta(F) = \deg F$ pour tout $F \in K[X]$ non-nul.

(c) L'anneau $\mathbb{Z}[i]$ est euclidien, pour le stathme défini par $\delta(z) = z\,\overline{z}$ pour tout $z \in \mathbb{Z}[i]$ non-nul.

Preuve. Les exemples (a) et (b) découlent directement des propositions 4.2.1 et 4.2.2 respectivement. L'exemple (c) est laissé en exercice. □

4.2.5 Remarque. La définition d'un stathme n'impose pas de conditions d'unicité de q et r dans la seconde condition.

Et effectivement, ils ne sont pas forcément uniques. Par exemple, pour $a = 19$ et $b = 3$, on a: $19 = 6 \times 3 + 1 = 7 \times 3 + (-2)$ avec $r = 1$ et $r' = -2$ qui vérifient tous les deux

$$\delta(r) = |1| = 1 < \delta(3) = 3 \ \text{ et } \ \delta(r') = |-2| = 2 < \delta(3) = 3.$$

L'unicité de q et r qui apparaît dans la proposition 4.2.1 tient au fait qu'on y a remplacé la condition ($r = 0$ ou $|r| < |b|$), qui correspond à la définition du stathme, par la condition plus forte $0 \leq r < |b|$.

4.3 Notion d'anneau principal.

4.3.1 Définition. On appelle *anneau principal* un anneau commutatif unitaire qui est intègre, et dans lequel tout idéal est principal.

En d'autres termes, quel que soit I un idéal de A, il existe $x \in A$ (non unique a priori) tel que $I = xA$.

Le théorème suivant fournit une vaste classe d'anneaux principaux.

4.3.2 Théorème. *Tout anneau euclidien est principal.*

Preuve. Soit A un anneau euclidien, de stathme δ. Il est intègre, et il s'agit donc de montrer que tout idéal I de A est principal. C'est clair si $I = \{0\}$ (alors $I = 0A$) ou si $I = A$ (alors $I = 1A$). On suppose donc $I \neq \{0\}$ et $I \neq A$. On considère $E = \{\delta(x)\,;\, x \in I, x \neq 0\}$. C'est une partie non-vide de $\mathbb{N}$, elle admet donc un plus petit élément n. Il existe $x \in I$, $x \neq 0$ tel que $n = \delta(x)$. Soit alors $a \in I$ quelconque; par division euclidienne de a par x, il existe $q, r \in A$ tels que $a = xq + r$ avec $r = 0$ ou $\delta(r) < \delta(x) = n$. Or $r = a - xq$ avec $a \in I$ et $x \in I$, donc $r \in I$ par définition d'un idéal. Par minimalité de n, on ne peut donc pas avoir $\delta(r) < n$, et donc nécessairement $r = 0$, d'où $a = xq$. Ceci prouve que tout $a \in I$ appartient à xA. On conclut que $I \subseteq xA$, et donc $I = xA$. □

4.3.3 Exemples, contre-exemples, remarques.

(a) $\mathbb{Z}$, $\mathbb{Z}[i]$, et $K[X]$ lorsque K est un corps, sont des anneaux principaux.

Preuve. Résulte immédiatement du théorème ci-dessus et des exemples 4.2.4. □

(b) L'anneau $\mathbb{Z}[X]$ n'est pas principal.

Preuve. On le montre de façon élémentaire en vérifiant que, par exemple, l'idéal $I = 2A + XA$ (qui n'est autre que l'idéal engendré par 2 et X) n'est pas un idéal principal.

Par l'absurde, supposons qu'il existe $P \in A$ tel que $I = PA$. Comme $2 \in I$, il existerait $Q \in A$ tel que $2 = PQ$, ce qui impliquerait par un raisonnement sur les degrés que $P \in \mathbb{Z}$. Comme de plus $X \in I$, il existerait $R \in A$ tel que $X = PR$, ce qui impliquerait $P = \pm 1$ (et $R = \pm X$). On aurait donc $1 = \pm P \in I$, de sorte qu'il existerait $S, T \in A$ tels que $1 = 2S + TX$, ce qui est clairement impossible dans $A = \mathbb{Z}[X]$, puisque le coefficient constant de $2S + TX$ est pair. □

On retiendra: (A euclidien $\not\Rightarrow$ $A[X]$ euclidien) et (A principal $\not\Rightarrow$ $A[X]$ principal).

(c) La réciproque du théorème 4.3.2 est fausse. Il existe des exemples d'anneaux principaux qui ne sont pas euclidiens. On pourra par exemple montrer en TD que:

l'anneau $\mathbb{Z}[\omega] = \{a + \omega b\,;\, a, b \in \mathbb{Z}\}$ pour $\omega = \frac{1+i\sqrt{19}}{2}$ est principal et non euclidien.

4.3.4 Proposition. *Dans un anneau principal, tout idéal premier non-nul est maximal (et donc, pour les idéaux non-nuls, les notions de premier et de maximal coïncident).*

Preuve. Soit I un idéal premier non-nul de A. Il existe donc $a \in A$, $a \neq 0$, tel que $I = aA$. Soit J un idéal de A tel que $I \subset J$. Il existe $b \in A$, $b \neq 0$, tel que $J = bA$. Comme $a \in I$, on a $a \in J$ donc il existe $x \in A$ tel que $a = bx$. Supposons que $I \neq J$, c'est-à-dire, d'après 4.1.2.(i), que $b \notin I$. Ainsi $a = bx \in I$ avec $b \notin I$, donc le fait que I soit premier implique que $x \in I$. Donc il existe $y \in A$ tel que $x = ay$. On déduit que $a = bx = bay$, ou encore $a(1 - by) = 0$. L'intégrité de A implique, puisque $a \neq 0$, que $1 - by = 0$, d'où $by = 1$, ce qui prouve que $b \in U(A)$. D'après 2.2.1.(iii), on conclut que $J = A$. Ainsi, pour tout idéal J de A tel que $I \subset J$ et $J \neq I$, on a $J = A$. Donc I est maximal.

Rappelons que, réciproquement, d'après 3.2.2, un idéal maximal est toujours premier. □

On a vu en 3.2.3.(c) que $\mathbb{Z}[X]$ possède des idéaux premiers non-nuls non maximaux, ce qui fournitune nouvelle preuve du fait que $\mathbb{Z}[X]$ n'est pas principal. On a en fait le résultat général suivant:

4.3.5 Théorème. *Soit A un anneau commutatif unitaire. Les trois conditions suivantes sont équivalentes.*

(i) *A est un corps.* (ii) *$A[X]$ est euclidien;* (iii) *$A[X]$ est principal.*

Preuve. On a déja vu que (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii). Supposons donc maintenant $A[X]$ principal. En particulier, $A[X]$ est intègre, et donc, d'après 1.5.4.(ii), A est intègre. Considérons l'application $f : A[X] \to A$ qui, à tout polynôme $P = \sum_{i=0}^{n} a_i X^i$, associe le coefficient a_0. Il est facile de voir que f est un morphisme d'anneaux, qui est clairement surjectif. Donc le premier théorème d'isomorphisme 3.1.3 conduit à $A[X]/\operatorname{Ker} f \simeq A$. L'intégrité de A implique que $A[X]/\operatorname{Ker} f$ est intègre, donc, d'après 3.2.2, $\operatorname{Ker} f$ est un idéal premier non-nul de $A[X]$. Mais comme $A[X]$ est supposé principal, $\operatorname{Ker} f$ est alors, d'après 4.3.4, un idéal maximal de $A[X]$, et donc, d'après 3.2.2, $A[X]/\operatorname{Ker} f$ est un corps. On conclut via l'isomorphisme $A[X]/\operatorname{Ker} f \simeq A$ que A est un corps. □

Anneaux : divisibilité, arithmétique

1. Notions générales

1.1 Multiples et diviseurs.

1.1.1 Rappel (voir 4.1.1 du chapitre précédent). Soit A un anneau commutatif unitaire. Soient x et y deux éléments de A. On dit que x est un *diviseur* de y dans A, ou encore que x *divise* y dans A, ou encore que y est un *multiple* de x dans A, lorsque il existe $a \in A$ tel que $y = xa$. On note alors: $x|y$. On a montré que: pour tous $x, y \in A$, on a:

$$(x|y) \Leftrightarrow (y \in xA) \Leftrightarrow (yA \subseteq xA).$$

1.1.2 Remarques. On déduit immédiatement que:

(i) *Pour tous* $x, y, z \in A$, $(x|y \text{ et } y|z) \Rightarrow (x|z)$.

(ii) *Pour tout* $u \in A$, $(u \in U(A)) \Leftrightarrow (uA = A) \Leftrightarrow (u|y \text{ quel que soit } y \in A)$.

(iii) *Pour tous* $x, u \in A$, $(u \in U(A) \text{ et } x|u) \Rightarrow (x \in U(A))$.

1.2 Eléments associés.

1.2.1 Définition. Soit A un anneau commutatif unitaire *intègre*. Soient x et y deux éléments de A. On dit que x et y sont *associés* lorsqu'on a à la fois $x|y$ et $y|x$. On note alors $x \sim y$.

1.2.2 Proposition. *Soit A un anneau commutatif unitaire intègre. Soient x et y deux éléments de A. On a:*

$$(x \sim y) \Leftrightarrow (x|y \text{ et } y|x) \Leftrightarrow (xA = yA) \Leftrightarrow (\text{il existe } u \in U(A) \text{ tel que } x = uy).$$

Preuve. La première équivalence est vraie par définition, la seconde découle directement de 4.1.1. Pour la dernière, supposons que $x \sim y$. Il existe $u, v \in A$ tels que $x = uy$ et $y = vx$, donc $x = uvx$. Si $x = 0$, alors $y = 0$, et on a $x = uy$ pour tout $u \in U(A)$. Si $x \neq 0$, on écrit $x(1 - uv) = 0$ et on utilise l'intégrité de A pour déduire que $uv = 1$, d'où $u \in U(A)$, ce qui montre le résultat voulu. Réciproquement, supposons $x = uy$ avec $u \in U(A)$; on a $y|x$ et, puisque $y = u^{-1}x$ avec $u^{-1} \in A$, on a aussi $x|y$. On conclut que $x \sim y$. □

1.2.3 Exemples.

(a) Dans $\mathbb{Z}$, deux entiers m et n sont associés si et seulement si $m = \pm n$; (rappelons en effet que $U(\mathbb{Z}) = \{1, -1\}$).

(b) Pour tout anneau intègre A, deux polynômes P et Q de $A[X]$ sont associés si et seulement s'il existe $c \in U(A)$ tel que $P = cQ$, (rappelons que $U(A[X]) = U(A)$), et l'on a alors $Q = c^{-1}P$.

(c) En particulier, si K est un corps, deux polynômes P et Q de $K[X]$ sont associés si et seulement s'il existe $c \in K^*$ tel que $P = cQ$.

1.2.4 Remarque. Deux éléments associés ont les mêmes multiples et les mêmes diviseurs dans A.

En effet. Supposons $x \sim y$. On a $x = uy$ avec $u \in U(A)$. On sait déjà (voir 1.2.2) que $xA = yA$. Soit z un diviseur de y; il existe $a \in A$ tel que $y = za$. Donc $x = uy = uza$, et donc z divise x. □

1.3 Eléments irréductibles, éléments premiers.

1.3.1 DÉFINITIONS. Soit A un anneau commutatif unitaire *intègre*. Soit x un élément de A.

(a) x est dit irréductible dans A lorsqu'il n'est pas inversible dans A, et vérifie la condition:

$$\text{si } x = ab \text{ avec } a, b \in A, \text{ alors } a \in U(A) \text{ ou } b \in U(A).$$

(b) x est dit premier dans A lorsqu'il est non-nul et non inversible dans A, et vérifie la condition:

$$\text{si } x \text{ divise } ab \text{ avec } a, b \in A, \text{ alors } x \text{ divise } a \text{ ou } x \text{ divise } b.$$

1.3.2 REMARQUES.

(a) 0 n'est pas irréductible dans A.

(b) Dans la définition 1.3.1.(a), le "ou" est exclusif. En d'autres termes, si x est irréductible dans A et s'écrit $x = ab$, alors un seul des deux éléments a, b appartient à $U(A)$ (car si les deux étaient dans $U(A)$, alors x appartiendrait aussi à $U(A)$, ce qui est contraire à la définition).

(c) Un élément de A peut être irréductible dans A mais ne plus l'être dans un anneau contenant A. Par exemple, 3 est irréductible dans $\mathbb{Z}$, mais ne l'est pas dans $\mathbb{Q}$ puisqu'il est inversible dans $\mathbb{Q}$.

1.3.3 PROPOSITION (caractérisation en termes d'idéaux principaux). *Soit A un anneau commutatif unitaire intègre. Pour tout $x \in A$, on a:*

(i) (*x irréductible dans A*) $\Leftrightarrow$ (*xA maximal parmi les idéaux principaux distincts de A*).

(ii) (*x premier dans A*) $\Leftrightarrow$ (*xA idéal premier non-nul de A*).

Preuve. Supposons x irréducible. L'idéal principal $M = xA$ est distinct de A puisque $x \notin U(A)$. Soit $J = aA$ un idéal principal de A distinct de A, c'est-à-dire tel que $a \notin U(A)$, et supposons que $M \subseteq J$. Alors en particulier $x \in J$, donc il existe $b \in A$ tel que $x = ab$. Puisque $a \notin U(A)$, l'irréductibilité de x implique que $b \in U(A)$. Donc $x \sim a$, d'où $M = J$. Ceci prouve que M est maximal parmi les idéaux principaux distincts de A.

Réciproquement soit $x \in A$ tel que xA soit maximal parmi les idéaux principaux distincts de A. Soient $a, b \in A$ tels que $x = ab$. Alors $x \in aA$, et donc $xA \subseteq aA$. Si $a \in U(A)$, alors $aA = A$. Sinon, $aA \neq A$ et la maximalité de xA implique alors que $xA = aA$, donc $x \sim a$, d'où l'existence de $u \in U(A)$ tel que $x = ua$. Mais $x = ua = ba$ implique par intégrité de A que $b = u$, et donc $b \in U(A)$.

Ceci prouve (i). L'équivalence (ii) est quant à elle évidente par définition même d'un idéal premier et la traduction de la divisibilité en termes d'idéaux principaux rappelée en 1.1.1. □

1.3.4 COROLLAIRE. *Soit A un anneau commutatif unitaire intègre.*

(i) *Tout élément de A associé à un élément irréductible dans A est encore irréductible dans A.*

(ii) *Tout élément de A associé à un élément premier dans A est encore premier dans A.*

Preuve. Découle de 1.3.3 puisque deux éléments associés engendrent le même idéal principal. □

1.3.5 PROPOSITION. *Soit A un anneau commutatif unitaire intègre. Tout élément premier dans A est irréductible dans A.*

Preuve. Soit $x \in A$ premier dans A. On a $x \notin U(A)$. Supposons que $x = ab$ avec $a, b \in A$. En particulier $x|ab$, donc puisque x est premier, $x|a$ ou $x|b$. Supposons que $x|a$. Il existe $y \in A$ tel que $a = xy$, d'où $x = xyb$, ou encore $x(1 - yb) = 0$. Comme x est non-nul car premier, et que A est intègre, on conclut que $yb = 1$, et donc que $b \in U(A)$. On prouve de même que $a \in U(A)$ si $x|b$. □

1.3.6 REMARQUE. La réciproque est fausse en général. Par exemple, dans l'anneau $\mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5}\,; a, b \in \mathbb{Z}\}$, l'élément 3 est irréductible, mais non premier.

En effet. Posons $A = \mathbb{Z}[i\sqrt{5}]$. C'est un anneau commutatif unitaire intègre (vérifiez-le) qui contient $\mathbb{Z}$ comme sous-anneau.

Montrons d'abord que 3 n'est pas premier dans A. Observons d'abord que 3 ne divise pas $2+i\sqrt{5}$ dans A (en effet, on aurait sinon $(2+i\sqrt{5}) = 3(a+ib\sqrt{5})$ avec $a,b \in \mathbb{Z}$, d'où $3a = 2$ et $1 = 3b$, ce qui est impossible), et que de même 3 ne divise pas $2-i\sqrt{5}$. Et pourtant 3 divise $9 = (2+i\sqrt{5})(2-i\sqrt{5})$ dans A, puisque $9 = 3.3$. On conclut que 3 n'est pas premier dans A.

Montrons maintenant que 3 est irréductible dans A. Il est clair que 3 n'est pas inversible dans A. Supposons que $3 = xy$ avec $x = a+ib\sqrt{5}$ et $y = c+id\sqrt{5}$, où $a,b,c,d \in \mathbb{Z}$. Posons $N(x) = |x|^2 = a^2+5b^2$ et $N(y) = |y|^2 = c^2+5d^2$. On a: $9 = N(xy) = N(x)N(y)$ dans $\mathbb{N}^*$, et donc trois cas seulement sont possibles: $N(x) = N(y) = 3$, ou $N(x) = 1$ et $N(y) = 9$, ou $N(x) = 9$ et $N(y) = 1$. Or le premier cas est impossible (car $a^2+5b^2 = 3$ n'a pas de solutions entières), le second implique que $x \in U(A)$ (car $a^2+5b^2 = 1$ implique $a = \pm 1$ et $b = 0$, et donc $x = \pm 1$), et le troisième implique de même que $y \in U(A)$. On conclut que 3 est irréductible dans A. □

Néanmoins, on a le résultat suivant:

1.3.7 Proposition (cas particulier des anneaux principaux). *Si A est un anneau principal, tout élément irréductible est premier, et donc les notions d'élément premier et d'élément irréductible coïncident dans ce cas.*

Preuve. Soit x un élément irréductible de A. Il est non-inversible (par définition), non-nul (voir remarque (a) de 1.3.2), et l'idéal $M = xA$ est maximal parmi les idéaux principaux de A distincts de A. Mais ici, tout idéal de A est par hypothèse principal. Donc M est tout simplement un idéal maximal de A. Donc M est un idéal premier de A (voir 3.2 du chapitre 3), et comme il est non-nul, on déduit de 1.3.3.(ii) que x est un élément premier dans A. □

1.3.8 Exemples.

(a) Dans $\mathbb{Z}$, les éléments premiers (ou irréductibles) sont les nombres premiers et leurs opposés.

(b) Pour tout corps K, les polynômes de degré un sont toujours irréductibles dans $K[X]$.

(c) Si $K = \mathbb{C}$, les éléments irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré un.

(d) Si $K = \mathbb{R}$, les éléments irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré un, et les polynômes de degré deux de discriminant strictement négatif.

1.4 Eléments premiers entre eux, plus grand commun diviseur.

1.4.1 Définition. Soit A un anneau commutatif unitaire intègre. Soient x et y deux éléments de A. On dit que x et y sont *premiers entre eux*, ou *étrangers*, lorsque les seuls éléments de A qui divisent à la fois x et y sont les éléments de $U(A)$.

Exemple. Dans $\mathbb{Z}$ l'ensemble des diviseurs de 10 est $D_{10} = \{-10,-5,-2,-1,1,2,5,10\}$ et l'ensemble des diviseurs de 9 est $D_9 = \{-9,-3,-1,1,3,9\}$. On a donc $D_{10} \cap D_9 = \{-1,1\} = U(\mathbb{Z})$, donc 10 et 9 sont premiers entre eux. □

Exercice. Montrer que, dans $\mathbb{R}[X]$, les polynômes $P = X+2$ et $Q = X-1$ sont premiers entre eux. □

Remarque: si x est premier avec y, alors x est premier avec tout élément associé à y.

1.4.2 Proposition. *Tout élément irréductible est premier avec tout élément qu'il ne divise pas.*

Preuve. Soit x irréductible dans A. Soit $y \in A$ tel que x ne divise pas y. Par l'absurde, supposons que u soit un diviseur commun de x et y non inversible dans A. On aurait alors $x = ua$ et $y = ub$ avec $a,b \in A$. Comme $x = ua$ et $u \notin U(A)$, l'irréductibilité de x impliquerait que $a \in U(A)$. On obtiendrait $u = xa^{-1}$ avec $a^{-1} \in A$, de sorte que $y = xa^{-1}b$, ce qui contredit le fait que x ne divise pas y.

1.4.3 Définition. Soit A un anneau commutatif unitaire intègre. Soient x et y deux éléments de A. On dit que x et y admettent un plus grand commun diviseur dans A lorsqu'il existe un élément $d \in A$ tel que:

$$d \text{ divise } x, \quad d \text{ divise } y, \quad \text{et tout élément qui divise à la fois } x \text{ et } y \text{ divise aussi } d.$$

On dit alors que d est un pgcd de a et b.

1.4.4 Proposition. *Soit A un anneau commutatif unitaire intègre. Soient $x, y \in A$.*

(i) *Si x et y admettent un pgcd d, alors un élément quelconque $d' \in A$ est un pgcd de x et y si et seulement si d' est associé à d.*

(ii) *x et y sont premiers entre eux si et seulement si 1 est un pgcd de x et y.*

(iii) *x et y sont premiers entre eux si et seulement si $U(A)$ est l'ensemble des pgcd de x et y.*

Preuve. Montrons (i). Si d' est un pgcd de x et y, il divise x et y, et donc puisque d est un pgcd de x et y, on a $d'|d$. De même, $d|d'$, et donc $d \sim d'$. Comme deux éléments associés ont les mêmes multiples et les mêmes diviseurs (voir 1.2.4), la réciproque est claire. Les points (ii) et (iii) se déduisent alors immédiatement de (i) et de 1.4.1. □

1.4.5 Remarques.

(a) Si $x = 0$, alors l'ensemble des diviseurs de x est A. Donc, pour tout $y \in A$, un pgcd de x et y est y. Les autres pgcd sont les éléments associés à y. En particulier, si $x = y = 0$, le seul pgcd de x et y est 0.

(b) On définit de même le pgcd d'un nombre fini quelconque d'éléments de A.

1.4.6 Proposition. *Soit A un anneau commutatif unitaire intègre. Soient $x, y \in A$ non-nuls. Si x et y admettent un pgcd d, alors les deux éléments x' et y' tels que $x = dx'$ et $y = dy'$ sont premiers entre eux dans A.*

Preuve. Soit z un diviseur commun à x' et y'. Il existe $a, b \in A$ tels que $x' = za$ et $y' = zb$. Donc $x = dza$ et $y = dzb$. Ceci prouve que dz est un diviseur commun à x et y, donc un diviseur de leur pgcd d. Il existe donc $u \in A$ tel que $d = dzu$, ou encore $d(1 - zu) = 0$. Comme A est intègre et $d \neq 0$ (car x et y sont non-nuls), on a $zu = 1$. On conclut que $z \in U(A)$. □

1.4.7 Exemples et remarque.

(a) Dans $\mathbb{Z}$, les pgcd de 12 et 30 sont 6 et -6.

(b) Dans $\mathbb{R}[X]$, les pgcd de $X^2 - 3X + 2$ et $X^2 - 1$ sont tous les polynômes $\alpha(X - 1)$ où $\alpha \in \mathbb{R}^*$.

De fait, dans les situations que l'on connaît bien de l'arithmétique dans $\mathbb{Z}$ ou $\mathbb{R}[X]$ ou $\mathbb{C}[X]$, deux éléments quelconques ont toujours des pgcd, et l'on a des résultats importants dans la pratique (Théorème de Bézout, de Gauss,...) qui leur sont liés. On va les retrouver ci-dessous dans le cadre général des anneaux principaux. On étudiera ensuite à la section 3 une classe d'anneaux encore plus générale (les anneaux factoriels), qui englobent strictement les anneaux principaux, et où, là encore, l'existence de pgcd pour tous les couples d'éléments permet de faire de l'arithmétique.

2.1 Pgcd, théorème de Bézout et applications.

2.1.1 Théorème. *Soit A un anneau principal. Deux éléments quelconques de A admettent toujours des pgcd dans A. Plus précisément, quels que soient a et b dans A, tout générateur de l'idéal principal $aA+bA$ est un pgcd de a et b.*

$$(\ d \text{ est un pgcd de } a \text{ et } b\ ) \Leftrightarrow (\ aA+bA=dA\ )$$

Preuve. Soient $a,b \in A$ fixés. Comme A est principal, l'idéal $aA+bA$ est principal. Il existe $d \in A$ tel que $aA+bA=dA$. Montrons que d est un pgcd de a et b. On a d'abord $aA \subseteq aA+bA$, donc $aA \subseteq dA$, donc $d|a$. De même, $d|b$. Soit maintenant $c \in A$ tel que $c|a$ et $c|b$. Alors $aA \subseteq cA$ et $bA \subseteq cA$, donc, puisque cA est stable par addition, $aA+bA \subseteq cA$, c'est-à-dire $dA \subseteq cA$, et donc $c|d$. Ceci prouve que d est un pgcd de a et b. Réciproquement, soit d' un pgcd de a et b. D'après 1.4.4.(i), on a $d' \sim d$, donc $dA = d'A$, c'est-à-dire $d'A = aA+bA$. □

2.1.2 Théorème de Bézout. *Soit A un anneau principal. Pour tous a et b dans A, on a:*

$$(\ a \text{ et } b \text{ premiers entre eux dans } A\ ) \Leftrightarrow (\ \text{il existe } u,v \in A \text{ tels que } au+bv=1\ )$$

Preuve. Soient $a,b \in A$ fixés. Supposons a et b sont premiers entre eux. D'après 1.4.4.(ii), 1 est un pgcd de a et b. Il résulte alors du théorème précédent que $aA+bA=A$. En particulier $1 \in aA+bA$, et donc il existe $(u,v) \in A^2$ tel que $au+bv=1$. Supposons réciproquement qu'il existe $u,v \in A$ tels que $au+bv=1$; alors 1 appartient à $aA+bA$, donc $aA+bA=A$. Or, si d est un pgcd de a et b, on a $dA=aA+bA$. On déduit que $dA=A$, donc $d \in U(A)$, c'est-à-dire a et b premiers entre eux. □

2.1.3 Corollaire (lemme de Gauss). *Soit A un anneau principal. Pour tous a,b,c dans A, on a:*

$$(\ a \text{ divise } bc, \text{ et } a \text{ premier avec } b\ ) \Rightarrow (\ a \text{ divise } c\ )$$

Preuve. Comme a et b sont premiers entre eux, il existe d'après le théorème de Bézout $u,v \in A$ tels que $au+bv=1$. Donc $c=cau+cbv$. Comme a divise bc, on a $bc \in aA$, donc $bcv \in aA$. Par ailleurs il est clair que $acu \in aA$. Par stabilité de l'idéal aA pour l'addition, on conclut que $c=acu+bcv \in aA$. □

2.1.4 Remarques.

(a) Attention, si d est un pgcd de a et b, il existe d'après le théorème 2.1.1 des éléments $u,v \in A$ tels que $d=au+bv$. Le théorème de Bézout montre que la réciproque est vraie aussi si $d=1$ (et donc plus généralement si $d \in U(A)$). Mais si $d \neq 1$, l'existence d'un couple (u,v) tel que $au+bv=d$ n'implique pas que d est le pgcd de a et b. Par exemple, dans $\mathbb{Z}$, on a $3 \times 10 + (-2) \times 14 = 2$, mais 2 n'est pas le pgcd de 3 et -2.

(b) Attention, dans le théorème de Bézout, il n'y a pas unicité du couple (u,v); le corollaire ci-dessous du théorème de Gauss détermine tous les couples (u,v) solutions.

2.1.5 Corollaire. (Une précision sur le théorème de Bézout). *Soit A un anneau principal. Soient a et b premiers entre eux dans A. Pour tout couple $(u,v) \in A^2$ tel que $au+bv=1$, l'ensemble de tous les couples $(x,y) \in A^2$ tels que $ax+by=1$ est égal à $\{(u,v)+c(-b,a)\,;\,c \in A\}$.*

Preuve. Soit $(u,v) \in A^2$ tel que $au+bv=1$. Pour tout $c \in A$, le couple $(x,y)=(u,v)+c(-b,a)=(u-cb,v+ca)$ vérifie $ax+by=a(u-cb)+b(v+ca)=au-acb+bv+bca=au+bv=1$. Réciproquement, quel que soit $(x,y) \in A^2$ tel que $ax+by=1$, on a $ax+by=au+bv$, d'où $a(u-x)=b(y-v)$. Comme a et b sont premiers entre eux, il résulte du théorème de Gauss que a divise $y-v$. Il existe donc $c \in a$ tel que $y-v=ca$. On a alors: $cab=b(y-v)=a(u-x)$. Si $a \neq 0$, on déduit par intégrité de A que $u-x=cb$; on obtient donc bien $x=u-cb$ et $y=v+ca$. Si $a=0$, la propriété est claire. □

2.1.6 Remarques. Comme on le fait dans $\mathbb{Z}$, on définit naturellement la notion de ppcm (plus petit commun multiple) dans tout anneau principal A.

(a) On appelle ppcm de deux éléments $a,b \in A$ tout élément $m \in A$ tel que $aA \cap bA = mA$.

(b) (m est un ppcm de a et b) $\Leftrightarrow$ ($a|m$, $b|m$, et tout multiple de a et b est multiple de m).

(c) Le produit de tout pgcd de a et b par tout ppcm de a et b est associé à ab.

(d) En particulier (a et b sont premiers entre eux) $\Leftrightarrow$ (ab est un ppcm de a et b).

Comme la notion de pgcd, la notion de ppcm est clairement définie à l'association près, et s'étend naturellement à un nombre fini quelconque d'éléments de A.

2.2 Cas particulier des anneaux euclidiens.

2.2.1. Remarque préliminaire. Ce que l'on vient de voir sur l'arithmétique dans les anneaux principaux, basé sur les idéaux, s'applique en particulier aux anneaux euclidiens (voir 4.3.2 du chapitre 3). Néanmoins, dans ce cas particulier, on dispose de plus d'un processus algorithmique important basé sur la division euclidienne, appelé algorithme d'Euclide, qui permet entre autres de calculer les pgcd.

Quels que soient $a, b \in A$, on convient de désigner par $\operatorname{pgcd}(a, b)$ un pgcd quelconque de a et b. En d'autres termes, un élément $d \in A$ est un pgcd de a et b si et seulement si $d \sim \operatorname{pgcd}(a, b)$.

2.2.2. Lemme (fondamental de l'algorithme d'Euclide). *Soit A un anneau euclidien. Soient $a, b \in A$ tels que $b \neq 0$. Alors, pour tout reste r d'une division euclidienne de a par b, tout pgcd de a et b est associé à tout pgcd de b et r. En d'autres termes, en notant δ le stathme de A:*

$$(\ a = bq + r, \ \ \textit{avec } r = 0 \ \ \textit{ou} \ \ \delta(r) < \delta(b) \ ) \ \Rightarrow \ (\ \operatorname{pgcd}(a, b) \sim \operatorname{pgcd}(b, r) \ ).$$

Preuve. Il résulte de l'égalité $a = bq + r$ que $a \in bA + rA$; comme $bA + rA$ est un idéal, on en déduit que $ax \in bA + rA$ pour tout $x \in A$, c'est-à-dire $aA \subset bA + rA$. Comme par ailleurs $bA \subset bA + rA$, la stabilité de $bA + rA$ pour l'addition implique alors $aA + bA \subset bA + rA$. En écrivant ensuite $r = a - bq$, on montre de même que $bA + rA \subset aA + bA$. Finalement $aA + bA = bA + rA$. Donc, en notant d un pgcd de a et b, et d' un pgcd de b et r, on a $dA = d'A$, c'est-à-dire $d \sim d'$. □

2.2.3 Théorème (algorithme d'Euclide). *Soient $a, b \in A$ non-nuls.*

(i) *il existe $k \in \mathbb{N}^*$ et des éléments $q_1, \ldots, q_k, r_0, r_1, \ldots, r_k \in A$, avec*

$$r_0 = b \neq 0, \ \ r_1 \neq 0, \ \ r_2 \neq 0, \ \ \ldots \ \ \ r_{k-2} \neq 0, \ \ r_{k-1} \neq 0, \ \ r_k = 0,$$

vérifiant la condition:

$$\delta(r_{k-1}) < \delta(r_{k-2}) < \cdots < \delta(r_2) < \delta(r_1) < \delta(r_0) = \delta(b),$$

et les égalités:

$$\begin{aligned} & a = bq_1 + r_1 = r_0q_1 + r_1, \\ & r_0 = r_1q_2 + r_2, \\ & r_1 = r_2q_3 + r_3, \\ & \ldots\ldots\ldots \\ & r_{k-3} = r_{k-2}q_{k-1} + r_{k-1}, \\ & r_{k-2} = r_{k-1}q_k + r_k = r_{k-1}q_k. \end{aligned}$$

(ii) *On a alors:* $\operatorname{pgcd}(a, b) \sim r_{k-1}$.

Preuve. On effectue la division euclidienne de a par b. Notons $a = bq_1 + r_1$ avec $r_1 = 0$ ou $\delta(r_1) < \delta(b)$.
Si $r_1 = 0$, on arrête.
Si $r_1 \neq 0$, on a $\delta(r_1) < \delta(b)$, et on effectue la division euclidienne de b par r_1.
Notons $b = r_1q_2 + r_2$ avec $r_2 = 0$ ou $\delta(r_2) < \delta(r_1)$.
Si $r_2 = 0$, on arrête.
Si $r_2 \neq 0$, on a $\delta(r_2) < \delta(r_1) < \delta(b)$, et on effectue la division euclidienne de r_1 par r_2.
Notons $r_1 = r_2q_3 + r_3$ avec $r_3 = 0$ ou $\delta(r_3) < \delta(r_2)$.
Si $r_3 = 0$, on arrête.
Si $r_3 \neq 0$, on a $\delta(r_3) < \delta(r_2) < \delta(r_1) < \delta(b)$, et on effectue la division euclidienne de r_2 par r_3.
On itère ainsi le processus. Comme il n'existe pas de suite strictement décroissante dans $\mathbb{N}$, il existe un rang $k \in \mathbb{N}^*$ tel que $r_k = 0$. En notant $r_0 = b$ pour la cohérence des notations, ceci prouve le point (i).

Pour (ii), remarquons que le lemme 2.2.2 appliqué dans la première égalité de (i) donne $\operatorname{pgcd}(a, b) \sim \operatorname{pgcd}(b, r_1) \sim \operatorname{pgcd}(r_0, r_1)$. De même dans la deuxième égalité, on obtient $\operatorname{pgcd}(r_0, r_1) \sim \operatorname{pgcd}(r_1, r_2)$. Puis $\operatorname{pgcd}(r_1, r_2) \sim \operatorname{pgcd}(r_2, r_3)$, et par une récurrence évidente, $\operatorname{pgcd}(a, b) \sim \operatorname{pgcd}(r_{k-1}, r_k)$. Or puisque r_k est nul, $\operatorname{pgcd}(r_{k-1}, r_k) \sim r_{k-1}$, ce qui achève la preuve. □

On traduit le point (ii) en disant que les pgcd de a et b sont les éléments associés au dernier reste non-nul dans la suite des divisions successives de a par b.

2.2.4 Exemple et remarque.

Dans l'anneau euclidien $\mathbb{Z}$, soient $a = 33810$ et $b = 4116$. La suite des divisions successives donne:

$$\underbrace{33810}_{a} = \underbrace{4116}_{b=r_0} \times 8 + \underbrace{882}_{r_1} \quad ; \quad \underbrace{4116}_{r_0} = \underbrace{882}_{r_1} \times 4 + \underbrace{588}_{r_2} \quad ; \quad \underbrace{882}_{r_1} = \underbrace{588}_{r_2} \times 1 + \underbrace{294}_{r_3} \quad ; \quad \underbrace{588}_{r_2} = \underbrace{294}_{r_3} \times 2 + 0$$

On conclut que $\mathrm{pgcd}(a, b) \sim r_3$ donc $\mathrm{pgcd}(33810, 4116) \sim 294$.

Remarque. L'algorithme d'Euclide permet non seulement de calculer $d = \mathrm{pgcd}(a, b)$ mais aussi, en remontant les calculs dans la suite des divisions successives, de déterminer un couple (u, v) d'éléments de A tel que $d = au + bv$, faisant ainsi apparaître effectivement d comme un élément de $aA + bA$.

Ainsi, en reprenant l'exemple ci-dessus, on a:

$d = 294 = 882 - 588 = 882 + (4 \times 882) - 4116 = 5 \times (33810 - 8 \times 4116) - 4116 = 5 \times 33810 - 41 \times 4116.$

C'est un point crucial pour une bonne compréhension du théorème de Bézout.

3. Arithmétique dans les anneaux factoriels

3.1 Notion d'anneau factoriel.

3.1.1 Définition. On appelle anneau *factoriel* un anneau commutatif unitaire qui est intègre, et dans lequel tout élément non-nul et non-inversible se décompose en un produit d'un nombre fini d'éléments irréductibles dans A, de façon unique, à l'ordre et au produit par un élément inversible près.

Explicitement, cela signifie que A est intègre et que l'on a:

(F1) tout élément $a \in A$, $a \neq 0$, $a \notin U(A)$, s'écrit $a = r_1 r_2 \dots r_n$, avec $r_1, r_2, \dots, r_n$ irréductibles dans A;

(F2) si $r_1 r_2 \dots r_n = s_1 s_2 \dots s_m$, avec $r_1, \dots, r_n, s_1, \dots, s_m$ irréductibles dans A, alors $m = n$, et il existe une permutation $\sigma \in S_n$ telle que $s_i \sim r_{\sigma(i)}$ pour tout $1 \leq i \leq n$.

On parlera de <u>*la*</u> décomposition de a en produit de facteurs irréductibles, bien que l'unicité s'entende à la relation d'association près.

Exemple. $\mathbb{Z}$ est factoriel (la décomposition ci-dessus n'étant autre que la classique décomposition en produit de facteurs premiers, d'après 1.3.8.(a)). Ce n'est qu'un cas particulier du théorème 3.1.3 ci-dessous.

3.1.2 Proposition (une définition équivalente de la factorialité). *Un anneau intègre A est factoriel si et seulement s'il vérifie la condition* (F1) *de la définition et la condition suivante:*

(F2') *tout élément irréductible dans A est premier dans A.*

Preuve. Montrons d'abord que (F1) et (F2) impliquent (F2'). Soit r un élément irréductible de A; en particulier $r \neq 0$ et $r \notin U(A)$. Supposons que r divise dans A un produit ab, avec $a, b \in A$ non-nuls. Il s'agit de montrer que r divise a ou b. Soit $x \in A$ tel que $ab = rx$. Si $a \in U(A)$, on a alors r divise b. De même $b \in U(A)$ implique que r divise a. On suppose donc maintenant que $a \notin U(A)$ et $b \notin U(A)$. D'après la condition (F1), on a des décompositions en produits d'éléments irréductibles: $a = a_1 \dots a_n$, $b = b_1 \dots b_m$ et $x = x_1 \dots x_k$. D'où $a_1 \dots a_n b_1 \dots b_m = r x_1 \dots x_k$. Comme r est irréductible, le condition (F2) implique qu'ou bien il existe $1 \leq i \leq n$ tel que $r \sim a_i$, auquel cas r divise a, ou bien il existe $1 \leq j \leq m$ tel que $r \sim b_j$, auquel cas r divise b. On a ainsi prouvé que r est premier dans A.

Montrons maintenant que (F2') implique (F2). On suppose donc que tout irréductible est premier dans A. Supposons que $r_1 r_2 \dots r_n = s_1 s_2 \dots s_m$ avec r_i et s_j irréductibles dans A pour tous $1 \leq i \leq n$ et $1 \leq j \leq m$. L'élément r_1 est premier car irréductible, et comme il divise $s_1 s_2 \dots s_m$, il existe $1 \leq j \leq m$ tel que r_1 divise s_j. On a donc $s_j = a r_1$ pour un certain $a \in A$. Comme s_j est irréductible et que $r_1 \notin U(A)$, on a $a \in U(A)$, c'est-à-dire $r_1 \sim s_j$. Par intégrité, on simplifie par r_1 pour obtenir $r_2 \dots r_n \sim s_1 \dots s_{j-1} s_{j+1} \dots s_m$. On réitère, et le résultat voulu s'en déduit par récurrence. □

3.1.3 Théorème. *Tout anneau principal est factoriel.*

Preuve. Soit A un anneau principal. En particulier, il est intègre (par définition) et il vérifie la condition (F2') comme on l'a montré en 1.3.7. D'après 3.1.2, il suffit donc de montrer que A vérifie la condition (F1). Pour cela, raisonnons par l'absurde, en supposant que A ne vérifie pas (F1). Cela signifie que l'ensemble:

$$R = \{a \in A,\ a \neq 0,\ a \notin U(A),\ a \ \text{ n'est pas produit d'éléments irréductibles}\}$$

est non-vide. Il en résulte qu'est également non-vide l'ensemble E des idéaux principaux de A engendrés par les éléments de R.

$$E = \{aA\ ;\ a \in R\} \neq \emptyset.$$

On montre que E est inductif (voir 3.3.1 du chapitre 3) pour l'inclusion. Pour cela, considérons $F = (I_k)_{k\in X}$ une famille d'éléments de E totalement ordonnée par l'inclusion. Pour tout $k \in X$, considérons un élément $a_k \in R$ tel que $I_k = a_kA$. La réunion $I = \bigcup_{k\in X} I_k$ est un idéal non-nul de A. Comme A est principal, il existe $b \in A$, $b \neq 0$, tel que $I = bA$. Puisque $b \in I$, il existe $a_k \in R$ tel que $b \in a_kA$, et donc $bA \subseteq a_kA$. Comme par ailleurs $a_kA \subseteq I = bA$, on conclut que $I = a_kA$, et donc $I \in E$. En résumé, toute famille d'éléments de E totalement ordonnée admet un plus grand élément. On conclut que E est inductif.

D'après le lemme de Zorn, E admet (au moins) un élément maximal; notons-le cA, avec $c \in R$. Parce que $c \in R$, il est non-nul, non-inversible, et non-irréductible. Donc il existe $x, y \in A$ tel que $c = xy$ avec $x \notin U(A)$ et $y \notin U(A)$. Il en résulte que $cA \subset xA$ avec $cA \neq xA$, et $cA \subset yA$ avec $cA \neq yA$. De plus, il est clair que $x \in R$ ou $y \in R$ (en effet, sinon, x et y seraient produits d'irréductibles, et donc $c = xy$ aussi), d'où $xA \in E$ ou $yA \in E$. Dans l'un ou l'autre cas, il y a contradiction avec la maximalité de cA dans E. □

3.1.4 Exemples et remarques.

(a) Il résulte de 3.1.3 qu'en particulier les anneaux $\mathbb{Z}$, $K[X]$ pour K un corps, et $\mathbb{Z}[i]$, sont factoriels, car principaux.

(b) La réciproque du théorème 3.1.3 est fausse. Il existe des anneaux factoriels qui ne sont pas principaux. En effet, on démontrera au paragraphe 4.3 un théorème fondamental établissant que, si A est factoriel, alors $A[X]$ est factoriel. On conclura alors que par exemple $\mathbb{Z}[X]$ est factoriel, alors qu'il n'est pas principal, comme on l'a vu en 4.3.3.(b) et 4.3.5 au chapitre 3.

(c) Il existe des anneaux intègres non factoriels, par exemple l'anneau $\mathbb{Z}[i\sqrt{5}]$ étudié en 1.3.6, puisqu'il possède des éléments irréductibles non premiers, et ne vérifie donc pas la condition (F2') de 3.1.2.

Commentaire. Nous allons voir que les anneaux factoriels vérifient certaines propriétés arithmétiques que nous avons déjà établies pour les anneaux principaux (existence de pgcd, lemme de Gauss). Sur le plan strictement logique, il est donc suffisant de les montrer comme en 3.2.3 et 3.2.4 ci-dessous dans le cadre général des anneaux factoriels, puisque principal implique factoriel. Il n'est néanmoins pas inutile de connaître les preuves directes que nous avons données dans le cas particulier des anneaux principaux. Ne serait-ce que pour différencier les arguments généraux de ceux spécifiques au cas principal, comme le théorème de Bezout (voir plus loin, remarque 3.2.5).

3.2 Divisibilité dans les anneaux factoriels, lemme de Gauss.

3.2.1 Remarques préliminaires sur les notations. Soit A un anneau factoriel.

(a) Dans l'ensemble des éléments irréductibles de A, l'association définit d'après 1.3.4 une relation d'équivalence. En choisissant dans chaque classe d'équivalence un représentant particulier, on définit un *système de représentants* $\mathcal{R}$ des éléments irréductibles. En d'autres termes, tout élément irréductible de A est équivalent à un unique élément irréductible de la famille $\mathcal{R}$.

quel que soit r irréductible dans A, il existe $r' \in \mathcal{R}$ et $u \in U(A)$ uniques tels que $r = ur'$.

Exemples.

1. Dans l'anneau $\mathbb{Z}$, on choisit généralement comme système de représentants des éléments irréductibles l'ensemble $\mathcal{P}$ des nombres premiers positifs. Tout élément irréductible de $\mathbb{Z}$ est de la forme εp avec $p \in \mathcal{P}$ et $\varepsilon \in U(\mathbb{Z}) = \{-1, +1\}$.
2. Dans l'anneau $\mathbb{C}[X]$, on choisit généralement comme système de représentants des éléments irréductibles l'ensemble $\mathcal{R}$ les polynômes de degré 1 unitaires (c'est-à-dire de coefficient dominant égal à 1). Tout élément irréductible est de la forme $\alpha(X-\beta)$ avec $X-\beta \in \mathcal{R}$ et $\alpha \in U(\mathbb{C}[X]) = \mathbb{C}^*$.

(b) Soit $\mathcal{R}$ un système de représentants des éléments irréductibles dans A. Soit $a \in A$ non-nul et non-inversible. Il résulte de la condition (F1) que a s'écrit de façon unique:

$$a = u\, r_1^{n_1} r_2^{n_2} \dots r_s^{n_s}, \quad \text{avec } u \in U(A),\ r_i \in \mathcal{R} \text{ et } n_i \in \mathbb{N}^* \text{ pour tout } 1 \leq i \leq s.$$

Exemples.

1. Dans $\mathbb{Z}$, tout élément a non-nul et distinct de ± 1 s'écrit de façon unique $a = \varepsilon\, p_1^{n_1} p_2^{n_2} \dots p_s^{n_s}$, avec $\varepsilon = \pm 1$, et $n_i \in \mathbb{N}^*$ et $p_i \in \mathcal{P}$ pour tout $1 \leq i \leq s$.
2. Dans $\mathbb{C}[X]$, tout polynôme $P(X)$ de degré ≥ 1 s'écrit de façon unique:
$$P(X) = \alpha(X-\beta_1)^{n_1}(X-\beta_2)^{n_2} \dots (X-\beta_s)^{n_s},$$
avec $\alpha \in \mathbb{C}^*$, et $n_i \in \mathbb{N}^*$ et $\beta_i \in \mathbb{C}$ pour tout $1 \leq i \leq s$.

(c) Soit $\mathcal{R}$ un système de représentants des éléments irréductibles dans A. Soient $a, b \in A$ non-nuls et non-inversibles. En réunissant les facteurs irréductibles intervenant dans l'écriture ci-dessus de a et dans celle de b, et en autorisant alors des exposants nuls dans l'une des décompositions, a et b s'écrivent de façon unique:

$$a = u\, r_1^{n_1} r_2^{n_2} \dots r_q^{n_q} \quad \text{et} \quad b = v\, r_1^{m_1} r_2^{m_2} \dots r_q^{m_q}, \quad \text{avec } u, v \in U(A),$$
$$r_i \in \mathcal{R},\ \ n_i \in \mathbb{N},\ \ m_i \in \mathbb{N},\ \ (n_i, m_i) \neq (0,0) \ \text{ pour tout } 1 \leq i \leq q.$$

3.2.2 Lemme (diviseurs d'un élément dans un anneau factoriel). *Soit A un anneau factoriel. Soit $a \in A$, non-nul et non-inversible. Avec la notation du* 3.2.1.(b) *ci-dessus, les diviseurs de a dans A sont tous les éléments de la forme:*

$$w r_1^{p_1} r_2^{p_2} \dots r_s^{p_s}, \quad 0 \leq p_i \leq n_i \textit{ pour tout } 1 \leq i \leq s,\ \ w \in U(A).$$

Preuve. Soit b un diviseur de a. Si $b \in U(A)$, le résultat est clair avec $b = w$ et $p_1 = p_2 = \dots = p_s = 0$. Supposons donc maintenant que $b \notin U(A)$. Soit r un des facteurs irréductibles intervenant dans la décomposition de b. Comme $b|a$, on a $r|a$, c'est-à-dire que r divise $r_1^{n_1} r_2^{n_2} \dots r_s^{n_s}$. Puisque r est premier (car irréductible dans un anneau factoriel, voir 3.1.2), on en tire que r est associé à l'un des r_i. Ceci prouve que b est de la forme $b = w\, r_1^{p_1} r_2^{p_2} \dots r_s^{p_s}$, avec $w \in U(A)$ et $p_i \geq 0$ pour tout $1 \leq i \leq s$.

Pour montrer que $p_i \leq n_i$ pour tout $1 \leq i \leq s$, raisonnons par l'absurde. Supposons par exemple (pour fixer les idées) que $p_1 > n_1$. En notant $a = xb$ avec $x \in A$, on aurait donc: $u\, r_2^{n_2} \dots r_s^{n_s} = xw\, r_1^{p_1 - n_1} r_2^{p_2} \dots r_s^{p_s}$, avec $p_1 - n_1 > 0$, ce que contredirait la condition (F2). Ce qui achève la preuve. □

3.2.3 Proposition (pgcd et ppcm dans un anneau factoriel). *Soit A un anneau factoriel.*

(i) *Deux éléments quelconques admettent toujours un pgcd, et un ppcm dans A.*

(ii) *En particulier, si a et b sont deux éléments de A non-nuls et non-inversibles donnés par les notations* 3.2.1.(c), *on a:*

$$\mathrm{pgcd}(a,b) \sim r_1^{h_1} r_2^{h_2} \dots r_q^{h_q} \quad \textit{et} \quad \mathrm{ppcm}(a,b) \sim r_1^{\ell_1} r_2^{\ell_2} \dots r_q^{\ell_q},$$

avec $h_i = \min(n_i, m_i)$ et $\ell_i = \max(n_i, m_i)$ pour tout $1 \leq i \leq q$.

Preuve. Soient $a, b \in A$. Si $a = 0$, on a $\mathrm{pgcd}(a,b) \sim b$. Si $a \in U(A)$, on a $\mathrm{pgcd}(a,b) \sim a \sim 1$. De même si $b = 0$ ou $b \in U(A)$. Sinon, a et b sont non-nuls et non-inversibles: le point (ii) résulte alors immédiatement de 3.2.2 et de la définition des pgcd et ppcm. □

3.2.4 Théorème (dit lemme de Gauss). *Soit A un anneau factoriel. Soient a, b, c trois éléments de A. Si a divise bc et si a est premier avec b, alors a divise c. En d'autres termes:*

$$(\ a|bc \quad et \quad \mathrm{pgcd}(a,b) \sim 1\ ) \quad \Rightarrow \quad (\ a|c\ )$$

Preuve. On peut sans restriction supposer que a, b, c sont non-nuls et non inversibles. Conformément à 3.2.1.(c), on pose:

$$a = u\, r_1^{n_1} r_2^{n_2} \dots r_q^{n_q}, \quad b = v\, r_1^{m_1} r_2^{m_2} \dots r_q^{m_q}, \quad c = w\, r_1^{p_1} r_2^{p_2} \dots r_q^{p_q}, \quad \text{avec } u, v, w \in U(A).$$

On suppose $a|bc$, donc $n_i \leq m_i + p_i$ pour tout $1 \leq i \leq q$. Par contraposée, supposons que a ne divise pas c, c'est-à-dire qu'il existe au moins un indice j tel que $n_j > p_j$. Alors $m_j \geq n_j - p_j > 0$. Ainsi $n_j > 0$ et $m_j > 0$, donc r_j divise à la fois a et b, ce qui contredit $\mathrm{pgcd}(a,b) \sim 1$. □

3.2.5 Remarque. L'existence de pgcd et le lemme de Gauss, que nous avions démontrés pour les anneaux principaux, sont donc vrais dans le cadre plus général des anneaux factoriels. En revanche, la propriété de Bézout n'est plus forcément vraie dans un anneau qui n'est pas principal (même s'il est factoriel).

Par exemple, dans $\mathbb{Z}[X]$, les éléments 2 et X sont clairement premiers entre eux, mais pourtant il n'existe pas de polynômes $S, T \in \mathbb{Z}[X]$ tels que $2S + XT = 1$, comme on l'a montré au 4.3.3.(b) du chapitre 3. Néanmoins, comme on l'a déjà noté en 3.1.4.(b), et comme on le montrera un peu plus loin, $\mathbb{Z}[X]$ est factoriel. □

4. Factorialité des anneaux de polynômes

4.1 Irréductibilité des polynômes à coefficients dans un anneau factoriel

4.1.1 Définition. Soit A un anneau factoriel. Soit P un élément de $A[X]$ tel que $P \notin A$. On appelle *contenu* de P, noté $c(P)$, un pgcd dans A des coefficients de P.

Remarque. La notion de contenu n'est définie qu'à l'association dans $A[X]$ près, c'est-à-dire au produit par un inversible de A près. Lorsque l'on écrit $c(P) = a$, on a aussi $c(P) = ua$ pour tout $u \in U(A)$. On peut aussi écrire $c(P) \sim a$.

4.1.2 Définition. Soit A un anneau factoriel. Un polynôme P dans $A[X]$ est dit *primitif* lorsque $\deg P \geq 1$ et lorsque ses coefficients sont premiers entre eux.

$$(\ P \text{ primitif}\ ) \ \Leftrightarrow\ (\ \deg P \geq 1 \ \text{ et } \ c(P) = 1\ ) \ \Leftrightarrow\ (\ \deg P \geq 1 \ \text{ et } \ c(P) \in U(A)\ ).$$

Rappelons que l'on appelle polynôme *unitaire* tout polynôme de coefficient dominant égal à 1.

Remarques.

(1) Tout polynôme unitaire est primitif.

(2) Tout polynôme $P \in A[X]$ tel que $P \notin A$ s'écrit $P = c(P)P_1$ avec P_1 primitif.

4.1.3 Lemme. *Soit A un anneau factoriel. Soient P_1 et P_2 primitifs dans $A[X]$. Soient a_1 et a_2 non-nuls dans A. Si $a_1P_1 = a_2P_2$, alors a_1 et a_2 sont associés dans A, et P_1 et P_2 sont associés dans $A[X]$.*

Preuve. Comme P_1 est primitif, on a $c(a_1P_1) = a_1$. De même $c(a_2P_2) = a_2$. Donc a_1 et a_2 sont deux pgcd des coefficients du polynôme $a_1P_1 = a_2P_2$. Ils sont donc associés dans A: il existe $u \in U(A)$ tel que $a_2 = ua_1$. On a alors $a_1P_1 = ua_1P_2$, ce qui par intégrité de $A[X]$ (puisque A est intègre, voir 1.5.4.(ii) du chapitre 3) implique que $P_1 = uP_2$. Comme u est un élément inversible de $A[X]$, on conclut que P_1 et P_2 sont associés. □

4.1.4 Lemme (Gauss). *Soit A un anneau factoriel. Soient P et Q deux éléments de $A[X]$. D'une part P et Q sont primitifs si et seulement si PQ est primitif. D'autre part $c(PQ) = c(P)c(Q)$.*

Preuve. Supposons que P et Q soient primitifs et que PQ ne le soit pas. Comme $c(PQ)$ n'est pas inversible dans l'anneau factoriel A, il est divisible par au moins un élément p irréductible et donc premier. Considérons l'anneau intègre $B = A/pA$. La surjection canonique $\pi : A \to B$ se prolonge canoniquement en un morphisme d'anneaux $\hat{\pi} : A[X] \to B[X]$ défini par $\hat{\pi}(\sum a_i X^i) = \sum \pi(a_i) X^i$. Comme $c(P) = 1$, l'élément p ne divise pas tous les coefficients de P, donc $\hat{\pi}(P) \neq 0$. De même, $\hat{\pi}(Q) \neq 0$. L'intégrité de B impliquant celle de $B[X]$, on en déduit que $\hat{\pi}(P)\hat{\pi}(Q) \neq 0$, c'est-à-dire $\hat{\pi}(PQ) \neq 0$. Or, p divise $c(PQ)$, donc tous les coefficients de PQ, donc $\hat{\pi}(PQ) = 0$. D'où une contradiction. On a ainsi montré que P et Q primitifs implique PQ primitif.

Réciproquement, supposons PQ primitif. On peut toujours écrire P et Q sous la forme $P = c(P)P_1$ et $Q = c(Q)Q_1$ avec P_1 et Q_1 primitifs. Alors P_1Q_1 est primitif d'après ce qui précède, et l'égalité $PQ = c(P)c(Q)P_1Q_1$ implique avec le lemme 4.1.3 que $c(P)c(Q)$ est associé à 1 dans A, c'est-à-dire inversible dans A. D'où $c(P) \in U(A)$ et $c(Q) \in U(A)$, de sorte que P et Q sont primitifs.

Enfin, plus généralement, en notant $P = c(P)P_1$, $Q = c(Q)Q_1$ et $PQ = c(PQ)S_1$ avec P_1, Q_1, S_1 primitifs, l'égalité $c(PQ)S_1 = c(P)c(Q)P_1Q_1$ implique, puisque P_1Q_1 est primitif d'après le début de la preuve, que $c(PQ)$ est associé à $c(P)c(Q)$ dans A, ce que l'on a convenu d'écrire aux éléments inversibles près $c(PQ) = c(P)c(Q)$. □

4.1.5 Lemme. *Soient A un anneau factoriel et K son corps de fractions. Tout polynôme $P \in K[X]$ tel que $P \notin K$ peut s'écrire $P = qP_1$, avec $q \in K^*$ et $P_1 \in A[X]$ primitif dans $A[X]$.*

Preuve. Notons $P = \sum_{i=0}^{n} \frac{a_i}{s_i} X^i$ avec $n \geq 1$, $a_i \in A$, s_i non-nuls dans A, et $a_n \neq 0$. Quitte à multiplier le numérateur et le dénominateur de chaque fraction $\frac{a_i}{s_i}$ par un même élément non-nul de A, on peut écrire toutes les fractions $\frac{a_i}{s_i}$ avec un même dénominateur s (par exemple un ppcm des s_i puisque cette notion existe dans l'anneau factoriel A, ou encore simplement le produit de s_i), sous la forme $\frac{a_i}{s_i} = \frac{a_i'}{s}$, avec $a_i' \in A$. Donc $P = \frac{1}{s} \sum_{i=0}^{n} a_i' X^i$. En désignant par d un pgcd des a_i', et en écrivant $a_i' = db_i$, les b_i sont premiers entre eux dans A, de sorte que $P = \frac{d}{s} P_1$ avec $P_1 = \sum_{i=0}^{n} b_i X^i$ primitif. □

4.1.6 Théorème. *Soient A un anneau factoriel et K son corps de fractions. Soit R un élément non-nul de $A[X]$.*

(i) *Ou $R \in A$; alors R est irréductible dans $A[X]$ si et seulement si R est irréductible dans A.*

(ii) *Ou $R \notin A$; alors R est irréductible dans $A[X]$ si et seulement si R est primitif dans $A[X]$ et irréductible dans $K[X]$.*

Preuve. Rappelons que $U(A[X]) = U(A)$ puisque A est intègre (voir 1.5.5 du chapitre 3).

(i) Supposons $R \in A$. Notons alors $R = r$. Supposons d'abord r irréductible dans A. En particulier $r \notin U(A)$ donc $r \notin U(A[X])$. Si P et Q dans $A[X]$ sont tels que $r = PQ$, on a $0 = \deg r = \deg P + \deg Q$ donc $P \in A$ et $Q \in A$, de sorte que l'irréductibilité de r dans A implique $P \in U(A)$ ou $Q \in U(A)$, c'est-à-dire $P \in U(A[X])$ ou $Q \in U(A[X])$, ce qui prouve que r est irréductible en tant qu'élément de $A[X]$. Supposons maintenant que r est irréductible dans $A[X]$. En particulier $r \notin U(A[X])$ donc $r \notin U(A)$. Si $a, b \in A$ sont tels que $r = ab$, alors cette égalité dans $A[X]$ implique $a \in U(A[X])$ ou $b \in U(A[X])$, c'est-à-dire $a \in U(A)$ ou $b \in U(A)$, ce qui prouve que r est irréductible en tant qu'élément de A.

(ii) Supposons R de degré non-nul dans $A[X]$, primitif dans $A[X]$, et irréductible dans $K[X]$. Si P et Q dans $A[X]$ sont tels que $R = PQ$, comme R est irréductible dans $K[X]$, on a P ou Q dans $U(K[X]) = K^*$. Mais P et Q étant à coefficients dans A, cela signifie que P ou Q appartient à A^*. Considérons le cas où $P \in A$, $P \neq 0$. Dans $A[X]$, on peut toujours écrire $Q = c(Q)Q_1$ avec Q_1 primitif. On a l'égalité $R = Pc(Q)Q_1$ avec $Pc(Q) \in A$, Q_1 primitif dans

$A[X]$ et R primitif dans $A[X]$. On en déduit avec le lemme 4.1.3 que $Pc(Q) \in U(A)$. D'où a fortiori $P \in U(A)$, ou encore $P \in U(A[X])$. De même $Q \in A$, $Q \neq 0$, implique $Q \in U(A[X])$. On a ainsi montré que R est irréductible dans $A[X]$.

Récipoquement, supposons R de degré non-nul irréductible dans $A[X]$. Ecrivons-le sous la forme $R = c(R)R_1$ avec R_1 primitif dans $A[X]$, de même degré que R; l'irréductibilité de R implique alors R_1 ou $c(R)$ inversible dans $A[X]$. Comme $\deg R_1 = \deg R \geq 1$, le premier cas est exclu, donc $c(R) \in U(A[X])$, c'est-à-dire $c(R) \in U(A)$, et donc R est primitif dans $A[X]$. Pour montrer maintenant que R est irréductible dans $K[X]$, considérons P et Q dans $K[X]$ tels que $R = PQ$. Raisonnons par l'absurde en supposant que P et Q ne sont pas dans K; ils sont d'après le lemme 4.1.5 de la forme $P = \frac{a}{b}P_1$ et $Q = \frac{c}{d}Q_1$ avec a, b, c, d non-nuls dans A, et P_1, Q_1 primitifs dans $A[X]$, de mêmes degrés strictement positifs que P et Q respectivement. L'égalité $R = PQ$ devient $bdR = acP_1Q_1$. Or R est primitif dans $A[X]$ comme on vient de le voir, et P_1Q_1 l'est aussi d'après le lemme 4.1.4. En appliquant le lemme 4.1.3, on déduit que R est associé à P_1Q_1 dans $A[X]$. Il existe donc $u \in U(A[X]) = U(A)$ tel que $R = uP_1Q_1$. Comme R est supposé irréductible dans $A[X]$, il en résulte que P_1 ou Q_1 appartient à $U(A[X]) = U(A)$, ce qui contredit l'hypothèse faite selon laquelle P et Q sont de degrés strictement positifs. C'est donc que P ou Q appartient à $U(K[X]) = K^*$, ce qui achève de prouver que R est irréductible dans $K[X]$. $\square$

4.2 Première application: critère d'irréductibilité d'Eisenstein

4.2.1 THÉORÈME. *Soit A un anneau factoriel. Soit $P = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ un élément de $A[X]$ de degré $n \geq 1$. On suppose qu'il existe dans A un élément p, premier dans A, et satisfaisant les trois conditions suivantes:*

$$p \text{ divise } a_0, a_1, \ldots, a_{n-1}, \qquad p \text{ ne divise pas } a_n, \qquad p^2 \text{ ne divise pas } a_0.$$

(i) *Alors P est irréductible dans $K[X]$, où K désigne le corps de fractions de A.*

(ii) *Si de plus P est primitif dans $A[X]$ (en particulier s'il est unitaire dans $A[X]$), alors P est irréductible dans $A[X]$.*

Preuve. On montre d'abord le point (ii). Supposons donc P primitif. Par l'absurde, supposons P non irréductible dans $A[X]$: il existe donc $Q, R \in A[X]$ tels que $P = QR$, avec $0 < \deg Q < \deg P$ et $0 < \deg R < \deg P$. Comme P est primitif, le lemme 4.1.4 implique que Q et R le sont. Posons $Q = \sum_{i=0}^{q} b_iX^i$ et $R = \sum_{i=0}^{r} c_iX^i$, avec $b_i, c_i \in A$, et $0 < q < n$ et $0 < r < n$. On a $a_n = b_qc_r \neq 0$, et l'hypothèse p ne divise pas a_n implique que p ne divise pas b_q et ne divise pas c_r. On a aussi $a_0 = b_0c_0$, et donc par hypothèse p divise b_0c_0 mais p^2 ne divise pas b_0c_0, ce qui implique que p ne divise pas b_0 ou p ne divise pas c_0. Si l'on est dans le cas où p ne divise pas b_0, alors p divise c_0 en utilisant le fait que p est premier dans A. On a vu que p ne divise pas c_r, et on peut donc considérer le plus petit entier $k \in \{1, \ldots, r\}$ tel que p ne divise pas c_k. Par construction, p ne divise pas b_0c_k, et p divise b_ic_{k-i} pour tout $i \in \{1, \ldots, k\}$. Il en résulte que p ne divise pas $a_k = b_0c_k + b_1c_{k-1} + \cdots + b_kc_0$. Comme $1 \leq k \leq r < n$, ceci est contraire aux hypothèses faites au départ sur P. C'est donc que P est irréductible dans $A[X]$.

On ne suppose plus maintenant que P est primitif. Notons $P = c(P)P_1$ avec P_1 primitif. Comme $c(P)$ est un pgcd des a_i (pour $0 \leq i \leq n$), il existe $a'_0, a'_1, \ldots, a'_n$ premiers entre eux dans leur ensemble tels que $a_i = c(P)a'_i$ pour tout $0 \leq i \leq n$. Donc $P_1 = a'_nX^n + \cdots + a'_1X + a'_0$. On a clairement p qui ne divise pas a'_n (sinon il diviserait $a_n = c(P)a'_n$) et p^2 qui ne divise pas a'_0 (par le même argument). Pour $0 \leq i \leq n-1$, p divise $a_i = c(P)a'_i$ avec p qui ne divise pas $c(P)$ (car sinon p diviserait en particulier a_n, ce qui est exclu), et donc p divise a'_i. Les coefficients a'_i du polynôme primitif P_1 vérifiant donc les conditions du critère, on peut appliquer à P_1 la première étape, et conclure que P_1 est irréductible dans $A[X]$. D'après le point (ii) du théorème 4.1.6, il s'ensuit que P_1 est irréductible dans $K[X]$. En multipliant par $c(P) \in K^* = U(K[X])$, il en est de même de $c(P)P_1 = P$. $\square$

4.2.2 EXEMPLE: $P = X^5 + 4X^3 + 12X + 2$ est unitaire donc primitif dans $\mathbb{Z}[X]$, et il est irréductible dans $\mathbb{Z}[X]$ par application du critère d'Eisenstein.

4.3 Seconde application: factorialité de l'anneau des polynômes sur un anneau factoriel

4.3.1 THÉORÈME. *Si A est un anneau factoriel, alors l'anneau $A[X]$ est factoriel.*

Preuve. Montrons que $A[X]$ vérifie (F1). Soit $P \in A[X]$, non-nul et non inversible. Si $\deg P = 0$, alors $P \in A$. Comme A est factoriel, P s'écrit comme un produit d'éléments de A irréductibles dans A, donc irréductibles dans $A[X]$ d'après le point (i) du théorème 4.1.6. On supposera dans la suite que $n = \deg P$ est strictement positif. On peut sans restriction supposer que P est primitif (car sinon $P = c(P)P_1$ avec P_1 primitif, et $c(P)$ se décomposant d'après ce qui précède en produit d'éléments irréductibles dans A donc dans $A[X]$, il suffit de trouver une décomposition en produit d'éléments irréductibles de P_1 pour en déduire une décomposition de P). On raisonne par récurrence sur n. Si $n = 1$, on écrit $P = aX + b$ avec $a, b \in A$ premiers entre eux. Il est clair que P est irréductible dans $A[X]$. Prenons maintenant $n > 1$ et supposons (H.R.) la condition (F1) vérifiée par tout polynôme primitif de degré $< n$. Si P est irréductible, c'est fini. Sinon, il s'écrit $P = QR$ avec $0 < \deg Q < \deg P$ et $0 < \deg R < \deg P$. D'après le lemme 4.1.4, Q et R sont primitifs, donc par application de l'hypothèse de récurrence, ils se décomposent en produits d'éléments irréductibles de $A[X]$, d'où $P = QR$ aussi.

Montrons que $A[X]$ vérifie (F2'). Soit R un élément irréductible de $A[X]$; montrons qu'il est premier. Si $\deg R = 0$, alors R est irréductible dans A (point (i) du théorème 4.1.6), donc premier dans A puisque A est factoriel (voir 3.1.2). Il s'agit de montrer que l'élément R de A est premier dans $A[X]$. Pour cela, supposons que R divise PQ dans $A[X]$. Alors R divise $c(PQ) = c(P)c(Q)$, donc divise $c(P)$ ou $c(Q)$ dans A puisque R est premier dans A, donc a fortiori divise $c(P)$ ou $c(Q)$ dans $A[X]$, et finalement R divise P ou Q dans $A[X]$.

Considérons maintenant le cas non trivial où $\deg R > 0$. D'après le point (ii) du théorème 4.1.6, R est primitif dans $A[X]$ et irréductible dans $K[X]$, où K est le corps de fractions de A. Mais comme K est un corps, $K[X]$ est principal donc factoriel, de sorte que d'après 3.1.2, l'irréductibilité de R dans $K[X]$ implique que R est premier dans $K[X]$. Il s'agit de montrer que R est premier dans $A[X]$. Pour cela, supposons que R divise PQ dans $A[X]$. On a a fortiori que R divise PQ dans $K[X]$, et comme R est premier dans $K[X]$, on déduit que R divise P ou Q dans $K[X]$. Supposons pour fixer les idées que R divise P dans $K[X]$. Il existe $S \in K[X]$ tel que $P = RS$.

Supposons d'abord $S \notin K$. D'une part $P = c(P)P_1$ avec P_1 primitif dans $A[X]$. D'autre part, d'après le lemme 4.1.5, on a $S = \frac{d}{s}S_1$ avec $d, s \in A$ non-nuls et S_1 primitif dans $A[X]$. D'où $sc(P)P_1 = dRS_1$ dans $A[X]$, avec P_1 primitif et et RS_1 primitif (comme produit de deux polynômes primitifs, voir lemme 4.1.4). On en déduit avec le lemme 4.1.3 que d et $sc(P)$ sont associés dans A. Il existe $u \in U(A)$ tel que $d = usc(P)$, donc s divise d dans A, donc $\frac{d}{s} \in A$, et finalement $S \in A[X]$. On conclut que R divise P dans $A[X]$. Si maintenant $S \in K$, on raisonne comme ci-dessus, mais en prenant $S_1 = 1$.

Ceci achève de prouver que R est premier dans $A[X]$. On a ainsi montré que $A[X]$ vérifie les conditions (F1) et (F2'); on conclut avec 3.1.2 que $A[X]$ est factoriel. □

4.3.2 EXEMPLES.

(a) $\mathbb{Z}[X]$ est factoriel (rappelons une fois encore qu'il n'est pas principal).

(b) Pour tout anneau A, on définit l'anneau des polynômes en deux indéterminées $A[X, Y]$ à coefficients dans A, qui n'est autre à isomorphisme près que $A[X][Y]$. Si A est factoriel, $A[X]$ est factoriel d'après 4.3.1, et en réappliquant 4.3.1, on déduit que $A[X][Y]$ est factoriel. En résumé:

$$(\ A \text{ factoriel }) \Rightarrow (\ A[X, Y] \text{ factoriel }).$$

(c) Plus généralement, en définissant par récurrence $A[X_1, X_2, \ldots, X_n] = A[X_1, \ldots, X_{n-1}][X_n]$, l'application itérée n fois du théorème 4.3.1 montre que:

$$(\ A \text{ factoriel }) \Rightarrow (\ A[X_1, X_2, \ldots, X_n] \text{ factoriel }).$$

Les anneaux de polynômes en n indéterminées seront étudiés en détail dans l'UE "Groupes et anneaux 2" du second semestre. Le théorème de transfert de la factorialité ci-dessus est le premier résultat important sur ce sujet.