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

Licence de Mathématiques

Troisième année, U.E. 36MATS1

ALGEBRE: GROUPES ET ANNEAUX 2

Polycopié du cours

2004-2005

François Dumas

Licence de Mathématiques, 3ème année
U.E. 36MATS1

Cours d'algèbre : groupes et anneaux 2

François DUMAS

Chapitre 1

Groupes finis: rappels, compléments, exemples

1. Exemples de groupes finis.

1.1 Ordre d'un sous-groupe

Définitions. Un groupe G est dit *fini* s'il n'a qu'un nombre fini d'éléments. Dans ce cas, le nombre d'éléments de G est appelé l'*ordre* de G. On le note $o(G)$, ou encore $|G|$. C'est un entier naturel non-nul.

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 $xH = \{xy\,;\, y \in H\}$ la classe de x à gauche modulo H. Il est facile de vérifier (faites-le !) que l'ensemble des classes xH lorsque x décrit G est une partition de G. Comme chaque classe xH est d'ordre m (justifiez en détail pourquoi), on conclut que n est égal au produit de m par le nombre de classes distinctes. □

Proposition et définition. *Soit G un groupe fini. Pour tout $x \in G$ distinct du neutre e, il existe un entier $n \geq 2$ unique tel que:*

$$x^n = e \quad \text{et} \quad x^k \neq e \text{ pour tout } 1 \leq k < n.$$

Le sous-groupe de G engendré par x est alors:

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

L'entier n est l'ordre du sous-groupe $\langle x \rangle$ et est appelé l'ordre de l'élément x de G. On le note $|x|$. C'est un diviseur de l'ordre de G. Dans le cas où $x = e$, on a $\langle e \rangle = \{e\}$, et $|e| = 1$.

Preuve. Evidente, laissée au lecteur. □

1.2 Groupes isomorphes.

Définition. Deux groupes G_1 et G_2 sont dits *isomorphes* lorsqu'il existe un isomorphisme de groupes de l'un sur l'autre.

Remarques.

1. Rappelons qu'un morphisme de groupes de G_1 dans G_2 est une application $f : G_1 \to G_2$ telle que $f(x.y) = f(x).f(y)$ pour tous $x, y \in G_1$, et qu'un isomorphisme de groupes est un morphisme de groupes bijectif. La bijection réciproque est alors aussi un isomorphisme de groupes.
2. Supposons que G_1 et G_2 sont deux groupes isomorphes. Si l'un est abélien (commutatif), alors l'autre l'est aussi. Si l'un est fini, l'autre l'est aussi et ils sont de même ordre. Ils ont le même nombre de sous-groupes d'ordre donné. Leurs centres, leurs groupes dérivés, leurs groupes d'automorphismes,... sont isomorphes.
3. Deux groupes finis de même ordre sont isomorphes si et seulement si leur tables sont identiques, à une permutation près des éléments.

Exemples. Soit G_1 le groupe des racines quatrièmes de l'unité dans $\mathbb{C}$. On a: $G_1 = \{1, i, -1, -i\}$. La loi de groupe est ici la multiplication des complexes.

Soit G_2 le groupe des rotations affines du plan euclidien conservant un carré. Il est facile de montrer que G_2 est constitué de la rotation r de centre le centre O du carré et d'angle $\frac{\pi}{2}$, de la symétrie centrale s de centre O, de la rotation r' de centre O et d'angle $-\frac{\pi}{2}$, et de l'identité id. On a: $G_2 = \{\mathrm{id}, r, s, r'\}$. La loi de groupe est ici la loi $\circ$ de composition des applications.

Soit G_3 le groupe $\mathbb{Z}/4\mathbb{Z}$ des classes de congruences modulo 4. Rappelons que deux entiers a et b sont congrus modulo 4 lorsque $a-b$ est un multiple de 4 dans $\mathbb{Z}$. On a: $G_3 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$. La loi de groupe est ici l'addition des classes de congruence.

Les tables de ces trois groupes sont:

G_1	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

G_2	id	r	s	r'
id	id	r	s	r'
r	r	s	r'	id
s	s	r'	id	r
r'	r'	id	r	s

G_3	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

Il est clair qu'ils sont isomorphes, via les isomorphismes:

$$1 \mapsto \mathrm{id} \mapsto \overline{0}, \qquad i \mapsto r \mapsto \overline{1}, \qquad -1 \mapsto s \mapsto \overline{2}, \qquad -i \mapsto r' \mapsto \overline{3}.$$

EXEMPLE. On se propose de déterminer tous les groupes d'ordre 4 à isomorphisme près. Notons $G = \{e, a, b, c\}$ 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). La table de G est donc:

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

Le groupe C_4

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 donc 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 maintenant le produit ab. Si l'on avait $ab = a$, on aurait $b = e$, ce qui est exclu. Si l'on avait $ab = b$, on aurait $a = e$, ce qui est exclu. Si l'on avait $ab = e$, on aurait $b = a^{-1}$, c'est-à-dire $b = a$, ce qui est exclu. On a donc forcément $ab = c$. On calcule de même les autres produits. On obtient la table:

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

Le groupe de Klein V

On a démontré, et on retiendra, que:

> *il n'existe à isomorphisme près que deux groupes d'ordre 4, l'un est appelé groupe cyclique d'ordre 4 et est noté C_4, l'autre est appelé groupe de Klein et est noté V. Les deux sont abéliens.*

Le groupe C_4 contient: le neutre d'ordre 1, deux éléments d'ordre 4, et un élément d'ordre 2.
Le groupe V contient: le neutre d'ordre 1 et trois éléments d'ordre 2.

> EXERCICE. Montrer que $\Gamma_1 = \{\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right), \left(\begin{smallmatrix}-1&0\\0&-1\end{smallmatrix}\right), \left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)\}$ et $\Gamma_2 = \{\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right), \left(\begin{smallmatrix}-1&0\\0&-1\end{smallmatrix}\right), \left(\begin{smallmatrix}-1&0\\0&1\end{smallmatrix}\right)\}$. sont des sous-groupes de $GL_2(\mathbb{R})$. Sont-ils isomorphes à C_4 ? à V ?

> EXERCICE. Montrer que, dans l'ensemble $\mathbb{Z}/5\mathbb{Z}$, le sous-ensemble $\{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ est un groupe pour la multiplication. Est-il isomorphe à C_4 ou à V ? Même question pour le sous-ensemble $\{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ de $\mathbb{Z}/8\mathbb{Z}$.

1.3 Groupes cycliques.

DÉFINITION. Un groupe fini est dit *cyclique* s'il est engendré par un élément.

REMARQUES.

1. Soit G un groupe fini d'ordre n. Dire que G est cyclique signifie qu'il existe dans G un élément a qui est d'ordre n, de sorte que $G = \langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$.
2. Un groupe cyclique est nécessairement abélien.
3. Pour tout entier $n \geq 1$, il existe à isomorphisme près un et un seul groupe cyclique d'ordre n, noté C_n.
4. Pour tout entier $n \geq 1$, le groupe C_n est isomorphe par exemple au groupe multiplicatif des racines n-ièmes de l'unité dans $\mathbb{C}$, ou encore au groupe $\mathbb{Z}/n\mathbb{Z}$ muni de l'addition des classes de congruences modulo n, ou encore à beaucoup d'autres groupes que l'on rencontre dans divers domaines des mathématiques.
5. Pour certaines valeurs de n, il existe des groupes abéliens non cycliques. On a vu par exemple ci-dessus que pour $n = 4$, le groupe V n'est pas cyclique puisqu'il ne contient pas d'éléments d'ordre 4. Le théorème suivant montre au contraire que, pour certaines valeurs de n, le groupe C_n est à isomorphisme près le seul groupe d'ordre n.

THÉORÈME. *Tout groupe fini d'ordre premier est cyclique.*

> *Preuve.* Soient p un nombre premier et G un groupe d'ordre p. Soit a un élément de G distinct du neutre e. Considérons dans G le sous-groupe $\langle a \rangle$ engendré par a. D'après le théorème de Lagrange, son ordre $|a|$ divise p. Comme p est premier, on ne peut avoir que deux cas: ou bien $|a| = 1$, mais alors $a = e$, ce qui est exclu; ou bien $|a| = p$, mais alors $\langle a \rangle$ est inclus dans G et de même ordre que G, donc il est égal à G. On conclut que $G = \langle a \rangle$ est cyclique. □

COROLLAIRE. *Pour tout nombre premier p, il existe à isomorphisme près un et un seul groupe d'ordre p, qui est le groupe cyclique (donc abélien) C_p.*

QUESTIONS. Soit $C_n = \{e, a, a^2, \ldots, a^{n-1}\}$ le groupe cyclique d'ordre n. Peut-on déterminer parmi ses éléments ceux qui engendrent C_n (à part a bien entendu) ? Peut-on déterminer tous ses sous-groupes ?

Prenons par exemple $n = 6$. Dans $C_6 = \{e, a, a^2, a^3, a^4, a^5\}$, les différents éléments engendrent les sous-groupes suivants: $\langle e\rangle = \{e\}$ d'ordre 1, $\langle a^3\rangle = \{e, a^3\}$ d'ordre 2, $\langle a^2\rangle = \langle a^4\rangle = \{e, a^2, a^4\}$ d'ordre 3, et $\langle a\rangle = \langle a^5\rangle = \{e, a, a^2, a^3, a^4, a^5\}$ d'ordre 6. La dernière égalité provient du fait que $(a^5)^2 = a^4$, $(a^5)^3 = a^3$, $(a^5)^4 = a^2$, et $(a^5)^6 = e$.

Le résultat général est le suivant:

PROPOSITION. *Soit n un entier naturel non-nul. Soit $C_n = \{e, a, a^2, \ldots, a^{n-1}\}$ le groupe cyclique d'ordre n.*

(i) *Pour tout diviseur d de n, il existe un et un seul sous-groupe d'ordre d de C_n; il est cyclique, engendré par a^k pour $k = \frac{n}{d}$.*

(ii) *Les générateurs de C_n sont tous les éléments a^k tels que k et n soient premiers entre eux.*

Preuve. Repose sur des considérations simples d'arithmétique élémentaire, en particulier le théorème de Bezout pour le point (ii). Laissée au lecteur. Rédigez-la ! □

1.4 Groupes symétriques, groupes alternés.

PROPOSITION ET DÉFINITION. *Pour tout entier $n \geq 1$, l'ensemble des bijections d'un ensemble fini à n éléments sur lui-même est un groupe fini d'ordre $n!$ pour loi $\circ$. On l'appelle le n-ième groupe symétrique et on le note S_n. Les éléments de S_n sont appelés les permutations sur n éléments.*

Preuve. Bien connue. A réviser... □

On note les éléments de S_n sous la forme: $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{smallmatrix}\right)$.

EXEMPLE. 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 $\tau^2 = e$.

EXEMPLE. 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

Le groupe S_3 n'est pas abélien. C'est le plus petit groupe non abélien (car les groupes d'ordre 2, 3 ou 5 sont abéliens car cycliques d'après le théorème de 1.3, et les deux seuls groupes d'ordre 4 sont abéliens comme on l'a vu en 1.2).

Il 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 $\{e, \gamma, \gamma^2\}$.

DÉFINITION. On appelle *transposition* de S_n toute permutation τ qui échange deux éléments i et j en laissant fixe les $n - 2$ autres. On note alors $\tau = [i, j]$. On a de façon évidente $\tau^2 = e$.

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

Preuve. Vue au semestre précédent. A réviser... On pourra procéder par récurrence sur n. □

REMARQUE. Il n'y a pas unicité de la décomposition d'une permutation en produit de transpositions.

Par exemple, dans S_4, on a $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = [2, 4][1, 4][4, 2][1, 3] = [2, 3][1, 2]$.

Néanmoins, on a le lemme suivant:

LEMME ET DÉFINITION.

(i) *Si une même permutation σ de S_n 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. On appelle signature de σ le nombre $(-1)^m$, où m désigne le nombre de transpositions d'une décomposition quelconque de σ en produit de transpositions. On la note $\varepsilon(\sigma)$.*

(ii) *L'application signature $\varepsilon : S_n \to \{-1, 1\}$ est un morphisme de groupes.*

Preuve. Vue au semestre précédent. A réviser... □

THÉORÈME ET DÉFINITION. *L'ensemble des permutations de signature 1 (c'est-à-dire des permutations qui se décomposent en un nombre pair de transpositions) est un sous-groupe du groupe S_n appelé groupe alterné, noté A_n, d'ordre $\frac{n!}{2}$.*

Preuve. Résulte directement du fait que A_n est le noyau du morphisme ε. □

REMARQUE: on verra plus loin en 2.2 que A_n est normal dans S_n.

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

EXEMPLE. Pour $n = 4$, le groupe alterné A_4 est d'ordre 12. Donnons quelques précisions sur ses éléments.

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).

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

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

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, puisqu'il est formé de huit éléments d'ordre 3, trois éléments d'ordre 2, et du neutre e d'ordre 1.

	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

On montrera plus loin que, non seulement A_4 n'admet pas d'élément d'ordre 6, mais qu'il n'admet en fait pas de sous-groupe d'ordre 6; en revanche, il admet V comme sous-groupe d'ordre 4 bien qu'il n'admette pas d'élément d'ordre 4.

1.5 Groupes diédraux.

EXEMPLE. Soit D_3 le sous-groupe des isométries du plan affine euclidien conservant un triangle équilatéral (ABC). On montre aisément 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.

Il est clair que D_3 est isomorphe au groupe symétrique S_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

Figure 1

Figure 2

EXEMPLE. Soit D_4 le sous-groupe 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: $t_1 = rs_1$, $s_2 = r^2 s_1$, $t_2 = r^3 s_1$,
Donc D_4 est engendré par les deux éléments r et s_1.

	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

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:

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

REMARQUE. 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. On peut en fait démontrer (voir plus loin) qu'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 il existe d'autres groupes non abéliens d'ordre 8 non isomorphes à D_4, comme le montre l'exercice suivant.

EXERCICE. Montrer que le sous-ensemble Q_8 de $GL_2(\mathbb{C})$ formé des huit matrices:

$$e = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \quad -e = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right), \quad j = \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right),$$
$$-j = \left(\begin{smallmatrix} -i & 0 \\ 0 & i \end{smallmatrix}\right), \quad k = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right), \quad -k = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right),$$
$$\ell = \left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right), \quad -\ell = \left(\begin{smallmatrix} 0 & -i \\ -i & 0 \end{smallmatrix}\right).$$

est un groupe, d'ordre 8, non abélien, et non isomorphe à D_4. On l'appelle groupe des quaternions. (*Indication:* vérifier que Q_8 ne contient qu'un élément d'ordre 2, alors que D_4 en contient cinq).

	e	$-e$	j	$-j$	k	$-k$	ℓ	$-\ell$
e	e	$-e$	j	$-j$	k	$-k$	ℓ	$-\ell$
$-e$	$-e$	e	$-j$	j	$-k$	k	$-\ell$	ℓ
j	j	$-j$	$-e$	e	ℓ	$-\ell$	$-k$	k
$-j$	$-j$	j	e	$-e$	$-\ell$	ℓ	k	$-k$
k	k	$-k$	$-\ell$	ℓ	$-e$	e	j	$-j$
$-k$	$-k$	k	ℓ	$-\ell$	e	$-e$	$-j$	j
ℓ	ℓ	$-\ell$	k	$-k$	$-j$	j	$-e$	e
$-\ell$	$-\ell$	ℓ	$-k$	k	j	$-j$	e	$-e$

2. GROUPES QUOTIENTS.

2.1 Classes modulo un sous-groupe, indice d'un sous-groupe.

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

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

1. 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. Pour tout $x \in G$, H est équipotent à xH via la bijection $h \mapsto xh$ de H sur xH, et à Hx via la bijection $h \mapsto hx$ de H sur Hx.

2. En particulier, pour $x = e$, on a: $eH = He = H$.

3. On vérifie (rappeler la démonstration) que les classes à gauche forment une partition de G, de même que les classes à droite.

4. On démontre ensuite (faites-le) que l'ensemble des classes à droite modulo H est équipotent à l'ensemble des classes à gauche modulo H via la bijection $Hx \mapsto x^{-1}H$.

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). On dit que H est d'indice fini lorsque ce cardinal est fini.

REMARQUE. 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:

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

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

2.2 Sous-groupe normal.

DÉFINITION. Soient G un groupe et H un sous-groupe de G. On dit que H est *normal dans* G lorsque, pour tout $x \in G$, on a: $xH = Hx$. On note alors $H \lhd G$.

REMARQUES.

1. L'égalité $xH = Hx$ ne signifie par que $xh = hx$ pour tout $h \in H$, mais que, pour tout $h \in H$, il existe $h' \in H$ tel que $xh = h'x$ et $h'' \in H$ tel que $hx = xh''$. On en déduit donc la caractérisation pratique suivante:
$$H \lhd G \quad \Leftrightarrow \quad \forall\, x \in G,\ \forall\, h \in H,\ xhx^{-1} \in H.$$
2. Pour tout $x \in G$, notons $xHx^{-1} = \{xhx^{-1}\,;\, h \in H\}$. Si $xHx^{-1} \subset H$ pour tout $x \in G$, alors $H \subset yHy^{-1}$ pour tout $y \in G$, puisque tout $h \in H$ peut s'écrire $h = y(y^{-1}hy)y^{-1}$. On en déduit donc la caractérisation suivante:
$$H \lhd G \quad \Leftrightarrow \quad \forall\, x \in G,\ xHx^{-1} = H.$$
3. Quel que soit le groupe G, les sous-groupes $\{e\}$ et G sont toujours des sous-groupes normaux de G.
4. Si G est abélien, tout sous-groupe de G est normal dans G.
5. Tout sous-groupe d'indice 2 dans un groupe G est normal dans G. (Rappeler la preuve en exercice).
6. Pour tout morphisme $f : G \to G'$ d'un groupe G dans un groupe G', le noyau $\operatorname{Ker} f$ est normal dans G. (Rappeler la preuve en exercice).
7. Si $H \lhd G$ et $K \lhd G$, alors $H \cap K \lhd G$.

EXEMPLE. Pour tout $n \geq 2$, le groupe alterné A_n est normal dans le groupe symétrique S_n. Cela résulte du point 6 ci-dessus puisque A_n est le noyau du morphisme signature, ou encore du point 5 puisque $[S_n : A_n] = 2$.

EXEMPLE. Considérons, avec les notations de 1.4, le groupe symétrique $S_3 = \{e, \gamma, \gamma^2, \tau_1, \tau_2, \tau_3\}$. Le sous-groupe $A_3 = \{e, \gamma, \gamma^2\}$ est normal dans S_3 comme on vient de le voir. Les trois sous-groupes $H_i = \{e, \tau_i\}$ pour $i = 1, 2, 3$ ne sont pas normaux dans S_3 car, par exemple pour $i = 1$, on a $\gamma\tau_1\gamma^{-1} = \gamma\tau_1\gamma^2 = \gamma\tau_3 = \tau_2 \notin H_1$.

EXEMPLE. Considérons le groupe diédral $D_n = \{e, r, r^2, r^3, \ldots, r^{n-1}, s, sr, sr^2, sr^3, \ldots, sr^{n-1}\}$, avec les notations de 1.5. Le sous-groupe cyclique $C_n = \{e, r, r^2, r^3, \ldots, r^{n-1}\}$ est normal dans D_n car d'indice 2. Dès lors que $n > 2$, le sous-groupe $K = \{e, s\}$ n'est pas normal dans D_n car $r^{-1}sr = r^{-1}r^{n-1}s = r^{n-2}s \notin K$. A noter que pour $n = 2$, le sous-groupe K est normal puisque D_2 est le groupe de Klein donc abélien.

EXERCICE. Montrer que le groupe des quaternions Q_8 admet un sous-groupe d'ordre 2 et trois sous-groupes d'ordre 4, et que tous ses sous-groupes sont normaux dans Q_8.

ATTENTION. Soient G un groupe, H et K deux sous-groupes de G tels que K soit un sous-groupe de H. Donc $K \subset H \subset G$. On peut avoir K normal dans H et H normal dans G sans avoir K normal dans G.

Exemple: plaçons-nous dans le groupe alterné A_4, en reprenant toutes les notations de 1.4. Observons d'abord (écrivez les détails !) 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 $V \lhd A_4$.

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 évidemment normal dans V puisque V est abélien.

2.3 Groupe quotient.

THÉORÈME ET DÉFINITION. *Soient G un groupe et H un sous-groupe normal dans G.*

(i) *La relation $\sim_H$ définie sur G par:*

$$\text{pour tous } x, y \in G, \quad x \sim_H y \quad \Leftrightarrow \quad xy^{-1} \in H,$$

est une relation d'équivalence.

(ii) *Pour tout $x \in G$, la classe déquivalence $\overline{x}$ de x pour la relation $\sim_H$ est:*

$$\overline{x} = xH = Hx.$$

En particulier, la classe du neutre e est $\overline{e} = H$.

(iii) *La loi de composition interne définie sur l'ensemble quotient $G/\sim_H = \{\overline{x}\,;\, x \in G\}$ par:*

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

est bien définie (indépendamment des représentants choisis) et munit $G/\sim_H$ d'une structure de groupe. On l'appelle le groupe quotient de G par le sous-groupe normal H. On le note G/H.

(iv) *L'application $\pi : G \to G/H$ qui, à tout élément $x \in G$ associe sa classe $\overline{x}$ est un morphisme de groupes surjectif, appelé surjection canonique.*

(v) *Si H est d'indice fini, alors G/H est d'ordre fini, et $|G/H| = [G : H]$.*

En particulier, si G est fini, alors G/H est d'ordre fini, et $|G/H| = \frac{|G|}{|H|}$.

Preuve. Le point (v) résulte directement du 2.1 ci-dessus. Les points (i) à (iv) ont été démontrés dans le précédent cours d'algèbre. Reprenez-en la preuve dans le détail. □

EXEMPLE. Considérons le groupe diédral $D_n = \{e, r, r^2, r^3, \ldots, r^{n-1}, s, sr, sr^2, sr^3, \ldots, sr^{n-1}\}$, et son sous-groupe normal $C_n = \{e, r, r^2, r^3, \ldots, r^{n-1}\}$. Les deux classes modulo C_n sont:

$$\overline{e} = C_n = \{e, r, r^2, r^3, \ldots, r^{n-1}\} \quad \text{et} \quad \overline{s} = sC_n = \{s, sr, sr^2, sr^3, \ldots, sr^{n-1}\},$$

car il est clair que deux éléments quelconques de la forme sr^k et sr^ℓ sont équivalents modulo C_n puisque $sr^k(sr^\ell)^{-1} = sr^k r^{-\ell} s^{-1} = sr^{k-\ell}s = ssr^{n-(k-\ell)} = r^{n-k+\ell} \in C_n$. Le groupe quotient $D_n/C_n = \{\overline{e}, \overline{s}\}$ est donc le groupe à deux éléments. On écrit: $D_n/C_n \simeq C_2$.

EXEMPLE. Considérons le groupe des quaternions $Q_8 = \{e, -e, j, -j, k, -k, \ell, -\ell\}$. On a vu en exercice en 2.2 que le sous-groupe $H = \{e, -e\}$ est normal. Les classes modulo H sont:

$$\overline{e} = H = \{e, -e\}, \quad \overline{j} = jH = \{j, -j\}, \quad \overline{k} = kH = \{k, -k\}, \quad \overline{\ell} = \ell H = \{\ell, -\ell\}.$$

Le groupe quotient $Q_8/H = \{\overline{e}, \overline{j}, \overline{k}, \overline{\ell}\}$ est d'ordre 4. Comme $(\overline{j})^2 = (\overline{k})^2 = (\overline{\ell})^2 = \overline{-e} = \overline{e}$, on conclut que Q_8/H est isomorphe au groupe de Klein. On écrit $Q_8/H \simeq V$.

EXERCICE. Montrer que le sous-groupe $V = \{e, a, b, c\}$ de A_4 est normal dans S_4, et que le groupe quotient S_4/V est isomorphe à S_3; (voir fin de 1.4 et fin de 2.2).

THÉORÈME (dit premier théorème d'isomorphisme). *Soient G et G' deux groupes, et $f : G \to G'$ un morphisme de groupes. Alors le groupe quotient de G par le sous-groupe normal* $\operatorname{Ker} f$ *est isomorphe au sous-groupe* $\operatorname{Im} f = f(G)$ *de G'. On note:*

$$G/\operatorname{Ker} f \simeq \operatorname{Im} f.$$

Preuve. (A connaître absolument !). Posons $H = \operatorname{Ker} f$. Le principe est de construire une application $\overline{f} : G/H \to \operatorname{Im} f$ en posant $\overline{f}(\overline{x}) = f(x)$ pour tout $\overline{x} \in G/H$.

On commence par montrer que $\overline{f}$ est bien définie, indépendamment des représentants choisis. Pour cela, prenons deux éléments x et x' représentants de la même classe dans G/H, c'est-à-dire tels que $\overline{x} = \overline{x'}$. On a alors $x' \sim_H x$, ou encore $x'x^{-1} \in H = \operatorname{Ker} f$, d'où $f(x'x^{-1}) = e_{G'}$, donc $f(x')f(x)^{-1} = e_{G'}$, et finalement $f(x') = f(x)$ dans $\operatorname{Im} f$. Ce qui permet bien de poser $\overline{f}(\overline{x}) = f(x) = f(x') = \overline{f}(\overline{x'})$.

$\overline{f}$ est un morphisme de groupe car, pour tous $x, y \in G$, on a: $\overline{f}(\overline{x}.\overline{y}) = \overline{f}(\overline{xy}) = f(xy) = f(x)f(y) = \overline{f}(\overline{x})\overline{f}(\overline{y})$.

Par construction, $\overline{f}$ est surjective car tout élément y de $\operatorname{Im} f$ est de la forme $y = f(x)$ pour au moins un élément $x \in G$, et il existe donc $\overline{x} \in G/H$ tel que $y = \overline{f}(\overline{x})$.

Pour l'injectivité, montrons que $\operatorname{Ker} \overline{f} = \{\overline{e}\}$. Soit donc $\overline{x} \in G/H$ tel que $\overline{f}(\overline{x}) = e_{G'}$. Cela signifie que $f(x) = e_{G'}$, c'est-à-dire $x \in \operatorname{Ker} f$. Mais $x \in H$ est équivalent à $\overline{x} = H = \overline{e}$, ce qui achève la preuve. □

EXEMPLE. Soit $\varepsilon : S_n \to \{-1, 1\}$ le morphisme signature. On a $A_n = \operatorname{Ker} \varepsilon \lhd S_n$. Comme ε est clairement surjectif (il existe dans S_n des permutations de signature -1 et des permutations de signature 1), on a $\operatorname{Im} \varepsilon = \{-1, 1\}$. On conclut que $S_n/A_n \simeq \{-1, 1\}$. On écrit: $S_n/A_n \simeq C_2$.

EXEMPLE. Soit $\mathbb{U}$ le groupe multiplicatif des nombres complexes de module 1. L'application $t \mapsto \exp it$ définit un morphisme de groupes surjectif $f : \mathbb{R} \to \mathbb{U}$, dont le noyau est $\operatorname{Ker} f = 2\pi\mathbb{Z}$. On a donc: $\mathbb{R}/2\pi\mathbb{Z} \simeq \mathbb{U}$. Fixons un entier $n \geq 2$. L'application $k \mapsto \exp \frac{2ik\pi}{n}$ définit un morphisme de groupes $g : \mathbb{Z} \to \mathbb{U}$, de noyau $\operatorname{Ker} g = n\mathbb{Z}$, dont l'image est le groupe $\mathbb{U}_n$ des racines n-ièmes de l'unité, de sorte que $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{U}_n$.

EXERCICE. En utilisant le morphisme déterminant, montrer que:

$$\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \simeq \mathbb{R}^* \quad \text{et} \quad \mathrm{O}_n(\mathbb{R})/\mathrm{SO}_n(\mathbb{R}) \simeq C_2.$$

2.4 Quelques résultats complémentaires.

On regroupe ici quelques résultats généraux relatifs aux groupes quotients, utiles comme arguments dans les preuves de plusieurs résultats à venir. On ne reprend pas ici les preuves, qui ont été détaillées lors du cours de premier semestre, et qui pourront faire l'objet de révisions personnelles ou en travaux dirigés.

1. *Centre.* Soit G un groupe.
   a. On appelle centre de G, noté $Z(G)$, l'ensemble des éléments de G qui commutent avec tous les éléments de G:
   $$Z(G) = \{g \in G \,;\, \forall\, x \in G,\ xg = gx\}.$$
   Le centre $Z(G)$ est un sous-groupe de G, abélien, et normal dans G.
   b. Si le groupe $G/Z(G)$ est monogène, alors le groupe G est abélien.

2. *Automorphismes intérieurs.* Soit G un groupe.
   a. On note $\operatorname{Aut} G$ le groupe des automorphismes du groupe G, pour la loi $\circ$. Pour tout $g \in G$, l'application $\gamma_g : G \to G$ définie par:
   $$\forall\, x \in G,\ \gamma_g(x) = gxg^{-1},$$
   est un élément de $\operatorname{Aut} G$. On l'appelle l'automorphisme intérieur déterminé par g. On note $\operatorname{Int} G$ l'ensemble des automorphismes intérieurs de G:
   $$\operatorname{Int} G = \{\gamma_g \,;\, g \in G\}.$$
   $\operatorname{Int} G$ est un sous-groupe de $\operatorname{Aut} G$, normal dans $\operatorname{Aut} G$.
   b. On a: $G/Z(G) \simeq \operatorname{Int} G$.

3. *Groupe dérivé et abélianisé.* Soit G un groupe.
   a. On appelle groupe dérivé de G, noté $D(G)$, le sous-groupe de G engendré par les commutateurs d'éléments de G, c'est-à-dire par tous les éléments de la forme $xyx^{-1}y^{-1}$, avec $x, y \in G$. On a: $D(G)$ est normal dans G, et $G/D(G)$ est abélien.
   b. Plus généralement, pour tout sous-groupe H normal dans G, le groupe quotient G/H est abélien si et seulement si $D(G) \subseteq H$.

4. *Second théorème d'isomorphisme.* Soient G un groupe, H et K deux sous-groupes de G tels que $H \lhd G$. On note $HK = \{hk \,;\, h \in H, k \in K\}$ (voir 3.1 ci-dessous pour plus de détails). Alors:
   (i) $H \cap K \lhd K$, (ii) HK sous-groupe de G et $H \lhd HK$, (iii) $K/(H \cap K) \simeq HK/H$.

5. *Sous-groupes d'un groupe quotient et troisième théorème d'isomorphisme.*
   a. Soient G un groupe et $H \lhd G$. Tout sous-groupe de G/H est de la forme K/H pour K un sous-groupe de G contenant H. De plus $K/H \lhd G/H$ si et seulement si $K \lhd G$.
   b Soient G un groupe, H et K deux sous-groupes de G tels que $H \subseteq K$, $H \lhd G$ et $K \lhd G$. Alors: $G/K \simeq (G/H)/(K/H)$.

6. *Formule des indices.* Soient G un groupe, H un sous-groupe d'indice fini dans G, et K un sous-groupe de G contenant H. Alors: $[G : H] = [G : K][K : H]$.

3. Groupes produits.

3.1 Observations préliminaires.

Notation. 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.

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

Remarques.

1. 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 $k_2 = k_1$.

2. 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 HK est alors équipotent à $H \times K$.

3. 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, ça n'implique pas que tout élément de H commute avec tout élément de K.

Exemple d'application. Le groupe alterné A_4 ne contient pas de sous-groupe d'ordre 6.

En effet, on a vu à la fin de 1.4 que A_4 contient 3 éléments a, b, c d'ordre 2, huit éléments d'ordre 3, et le neutre e d'ordre 1. On a vu à la fin de 2.2 que les trois sous-groupes $\{e, a\}$, $\{e, b\}$ et $\{e, c\}$ ne sont pas normaux, mais que le sous-groupe $V = \{e, a, b, c\}$ est normal dans A_4.

Supposons par l'absurde qu'il existe dans A_4 un sous-groupe F d'ordre 6. Il serait d'indice 2, donc normal dans A_4. Donc $F \cap V$ serait normal dans A_4 comme intersection de deux sous-groupes normaux.

De plus, $F \cap V$ étant un sous-groupe à la fois de F d'ordre 6 et de V d'ordre 4, le théorème de Lagrange impliquerait que $|F \cap V| = 1$ ou 2. Si $|F \cap V| = 1$, alors d'après la remarque 2 ci-dessus, la partie FV de A_4 compterait 24 éléments, ce qui est absurde puisque $|A_4| = 12$. C'est donc que $F \cap V$ est d'ordre 2. Donc $F \cap V$ est l'un des trois sous-groupes $\{e, a\}$, $\{e, b\}$ et $\{e, c\}$. Or ceux-ci ne sont pas normaux dans A_4. D'où une contradiction.

3.2 Produit direct (interne) et semi-direct (interne) de deux sous-groupes d'un groupe.

Définitions. 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:

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

On dit que G est le produit direct (interne) de H par K lorsque les trois conditions suivantes sont vérifiées:

$$(1)\ \ G = HK, \qquad (2)\ \ H \cap K = \{e\}, \qquad (4)\ \ \forall\, h \in H,\ \forall\, k \in K,\ hk = kh.$$

Proposition. *Avec les notations ci-dessus, supposons que G est le produit direct de H par K; alors:*

(i) *G est produit semi-direct de H par K,*

(ii) *G est produit direct de K par H,*

(iii) *H et K sont normaux dans G.*

Preuve. On suppose que les trois conditions (1), (2) et (4) sont vérifiées. D'après la remarque 1 ci-dessus, il résulte des hypothèses (1) et (2) que tout élément $g \in G$ s'écrit de façon unique sous la forme $g = hk$ avec $h \in H$ et $k \in K$. Donc pour tout $\ell \in H$, on a: $g\ell g^{-1} = hk\ell k^{-1}h^{-1} = h\ell kk^{-1}h^{-1} = h\ell h^{-1}$ en utilisant l'hypothèse (4). Ce dernier produit étant un élément du sous-groupe H, on a montré que $g\ell g^{-1} \in H$ pour tout $g \in G$ et tout $\ell \in H$. Donc $H \lhd G$ et la condition (3) est vérifiée, ce qui prouve (i). Le point (ii) est clair, et le point (iii) en découle alors par symétrie du rôle joué par H et K. □

Remarques:

4. Attention: la réciproque du point (i) est fausse; un groupe peut être produit semi-direct de deux sous-groupes sans que ce produit soit direct (voir exemples ci-dessous).

5. Si G est produit semi-direct de H par K, on a: $G = KH = HK$.

   En effet, on sait déjà que tout élément g de G s'écrit alors $g = hk$ avec $h \in H$ et $k \in K$. Donc $g = kk^{-1}hk$, et comme $H \lhd G$, le produit $h' = k^{-1}hk$ est un élément de H. On a donc $g = kh'$ avec $k \in K$ et $h' \in H$.

EXEMPLE. Considérons le groupe diédral $D_n = \{e, r, r^2, r^3, \ldots, r^{n-1}, s, sr, sr^2, sr^3, \ldots, sr^{n-1}\}$, et les sous-groupes $C_n = \{e, r, r^2, r^3, \ldots, r^{n-1}\}$ et $K = \{e, s\}$. Il est clair que $D_n = C_n K$ et $C_n \cap K = \{e\}$. On a vu en 2.2 que $C_n \lhd D_n$. On conclut que D_n est produit semi-direct de C_n par K.

Si $n > 2$, ce produit semi-direct n'est pas direct car $sr^k = r^{n-k}s \neq r^k s$, de sorte que la condition (3) n'est pas vérifiée, et K n'est pas normal dans D_n.

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).

EXERCICE. Montrer que le groupe des quaternions Q_8 n'est pas produit semi-direct de deux de ses sous-groupes (on rappelle que Q_8 n'est pas abélien, et que tous ses sous-groupes sont normaux, d'ordre 1,2,4,8).

THÉORÈME. *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. Alors:*

(i) *Soient g, g' deux éléments quelconques de G. Si $g = hk$ et $g' = h'k'$ sont les décompositions (uniques) de g et g' (avec $h, h' \in H, k, k' \in K$), alors la décomposition du produit gg' est donnée par:*

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

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

(ii) *On a: $G/H \simeq K$.*

Preuve. Le premier point résulte simplement du calcul $gg' = hkh'k' = hkh'k^{-1}kk'$, et du fait que $kh'k^{-1}$ appartient à H puisque $H \lhd G$. Pour le second, on considère l'application $f : G \to K$ qui, à tout $g \in G$ décomposé de façon unique en $g = hk$ avec $h \in H$ et $k \in K$, associe $f(g) = k$. D'après le point (i) précédent, f est un morphisme de groupes. Il est clair qu'il est surjectif et que son noyau est H. D'où l'isomorphisme voulu d'après le premier théorème d'isomorphisme (voir 2.3). □

EXERCICE. Soit $\mathbb{K}$ un corps. Montrer que, dans $GL_3(\mathbb{K})$, les matrices triangulaires supérieures dont les termes diagonaux valent 1 forment un sous-groupe, que l'on notera U. Montrer que:

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

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. Si $k = \mathbb{C}$, déterminer tous les éléments de U qui sont d'ordre fini. Si $k = \mathbb{F}_2$, montrer que U est isomorphe au groupe diédral D_4. Si $k = \mathbb{F}_3$, déterminer tous les sous-groupes de U.

3.3 Produit direct (externe) de deux groupes.

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 définie par:*

$$(x_1, x_2).(y_1, y_2) = (x_1y_1, x_2y_2) \quad \text{pour tous } x_1, y_1 \in G_1,\ x_2, y_2 \in G_2.$$

Ce groupe est appelé le produit direct de G_1 par G_2. On le note $G = G_1 \times G_2$. Son neutre est (e_1, e_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 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. □

REMARQUES

1. Il est clair que le produit direct $G_1 \times G_2$ est fini si et seulement si G_1 et G_2 le sont; on a alors $|G_1 \times G_2| = |G_1| \times |G_2|$.
2. Il est clair que le produit direct $G_1 \times G_2$ est abélien si et seulement si G_1 et G_2 le sont.
3. Il est clair que le produit direct $G_1 \times G_2$ est isomorphe au produit direct $G_2 \times G_1$.
4. On définit de même de façon évidente le produit direct d'un nombre fini quelconque de groupes.

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.

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 $G_1 = \langle a \rangle \simeq C_n$ avec a d'ordre n, et $G_2 = \langle b \rangle \simeq C_m$ avec b d'ordre m. Soit $x = (a, b)$ dans $G_1 \times G_2$. Quel que soit $k \in \mathbb{Z}$, on a $x^k = (e_1, e_2)$ si et seulement si $a^k = e_1$ et $b^k = e_2$, 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 $x^{nm} = (e_1, e_2)$ et $x^k \neq (e_1, e_2)$ pour tout $1 \leq k < nm$. On conclut que l'élément x 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 $G_1 \times G_2 = \langle x \rangle \simeq C_{nm}$. La réciproque est laissée au lecteur. □

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

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

Avec les notations additives usuelles en arithmétique, le théorème chinois s'énonce sous la forme:

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

EXEMPLES (en notation additive).

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

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 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 $x = (\overline{1},\widetilde{1})$.

3.4 Application aux groupes abéliens finis

On démontrera en TD que tout groupe abélien fini est isomorphe à un produit direct de groupes cycliques. Plus précisément, on a:

THÉORÈME ET DÉFINITION. *Soit G un groupe fini d'ordre $n \geq 2$. Il existe un entier $k \geq 1$ et des entiers $q_1, \ldots, q_k$ supérieurs ou égaux à 2 uniques, dont le produit vaut n, qui vérifient:*

(1) *q_2 est multiple de q_1, q_3 est multiple de q_2, $\ldots$, q_k est multiple de q_{k-1},*

(2) *G est isomorphe au produit direct de groupes cycliques $C_{q_1} \times C_{q_2} \times \cdots \times C_{q_k}$.*

On dit que ces entiers, qui caractérisent G à isomorphisme près, forment la suite des invariants de G.

Preuve: en TD □

EXEMPLE: en utilisant le théorème ci-dessus et le théorème chinois, on déduit qu'il existe à isomorphisme près quatre groupes abéliens d'ordre 36, qui sont:

$$C_{36} \simeq C_9 \times C_4, \qquad C_3 \times C_{12} \simeq C_3 \times C_3 \times C_4,$$
$$C_2 \times C_{18} \simeq C_2 \times C_2 \times C_9, \qquad C_6 \times C_6 \simeq C_3 \times C_3 \times C_2 \times C_2 \simeq C_6 \times C_3 \times C_2.$$

EXERCICE: montrer que tous les groupes abéliens d'ordre ≤ 12 sont, à isomorphisme près, donnés par:

$n = 1$	C_1		
$n = 2$	C_2		
$n = 3$	C_3		
$n = 4$	C_4	$C_2 \times C_2$	
$n = 5$	C_5		
$n = 6$	$C_6 \simeq C_2 \times C_3$		

$n = 7$	C_7		
$n = 8$	C_8	$C_4 \times C_2$	$C_2 \times C_2 \times C_2$
$n = 9$	C_9	$C_3 \times C_3$	
$n = 10$	$C_{10} \simeq C_2 \times C_5$		
$n = 11$	C_{11}		
$n = 12$	$C_{12} \simeq C_3 \times C_4$	$C_2 \times C_6 \simeq C_2 \times C_2 \times C_3$	

3.5 Produit semi-direct (externe) de deux groupes.

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 ! □

REMARQUES

1. Il est clair que le produit semi-direct $G_1 \rtimes G_2$ est fini si et seulement si G_1 et G_2 le sont; on a alors $|G_1 \rtimes G_2| = |G_1| \times |G_2|$.
2. Il est clair que 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 $x_2 \mapsto \mathrm{id}_{G_1}$.
3. Il est clair que, 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.

EXEMPLE. Soit $n \geq 3$: 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.

Chapitre 2

Groupes finis: groupe opérant sur un ensemble et applications

1. Groupe opérant sur un ensemble, exemples.

1.1 Rappel de quelques notions générales

Définition. Soient G un groupe et E un ensemble non vide. On dit que G *opère* (à gauche) sur E s'il existe une loi externe:

$$\begin{array}{ccc} G \times E & \longrightarrow & E \\ (g,x) & \longmapsto & g.x \end{array}$$

qui satisfait les deux conditions:

$$(1) \quad \forall\, g,g' \in G,\ \forall\, x \in E,\ g.(g'.x) = (gg').x; \qquad (2) \quad \forall\, x \in E,\ e.x = x.$$

On dit aussi que E est un *G-ensemble*, ou que l'on a une *action* de G sur E.

Théorème. La donnée d'une action d'un groupe G sur un ensemble non-vide E équivaut à la donnée d'un morphisme de groupes de G dans le groupe symétrique $S(E)$.

Preuve. Supposons donné un morphisme de groupes $\gamma : G \longrightarrow S(E)$; notons: $g \longmapsto \gamma_g$. On définit une loi externe $G \times E \longrightarrow E$ en posant $g.x = \gamma_g(x)$ pour tous $g \in G, x \in E$. En utilisant le fait que $\gamma_g \circ \gamma_{g'} = \gamma_{gg'}$ et $\gamma_e = \mathrm{id}_E$, on vérifie sans problème que les deux conditions (1) et (2) d'une action sont vérifiées.

Réciproquement, supposons que G opère sur E par $(g,x) \longmapsto g.x$. Définissons pour tout $g \in G$ une application $\gamma_g : E \longrightarrow E$ par $\gamma_g(x) = g.x$ quel que soit $x \in E$. On a alors:

$$\forall\ x \in E,\ \forall\ g,h \in G, \quad \gamma_g\gamma_h(x) = g.(h.x) = (gh).x = \gamma_{gh}(x) \quad \text{et} \quad \gamma_e(x) = e.x = x,$$

ce qui prouve que $\gamma_g\gamma_h = \gamma_{gh}$ et $\gamma_e = \mathrm{id}_E$. On en déduit que γ_g est bijective pour tout $g \in G$ (en prenant $h = g^{-1}$), puis que l'application $\gamma : G \to S(E)$ est un morphisme de groupes. □

Définition et proposition. *Soit G un groupe opérant sur un ensemble non-vide E. Pour tout $x \in E$, on appelle stabilisateur de x l'ensemble:*

$$\boxed{G_x = \{g \in G\,;\, g.x = x\}}.$$

C'est un sous-groupe de G, appelé aussi sous-groupe d'isotropie de x. On le note parfois $\mathrm{Stab}_G(x)$.

Preuve. On a $e.x = x$ donc $e \in G_x$. De plus, quels que soient $g,h \in G_x$, on calcule: $(gh^{-1}).x = (gh^{-1}).(h.x) = (gh^{-1}h).x = g.x = x$. D'où $gh^{-1} \in G_x$. □

Proposition et définition. *Soit G un groupe opérant sur un ensemble non-vide E. Pour tout $x \in E$, on appelle orbite de x l'ensemble:*

$$\boxed{\Omega_x = \{y \in E\,;\, \exists\, g \in G,\ y = g.x\} = \{g.x\,;\, g \in G\}}.$$

Les orbites des éléments de E sous l'action de G forment une partition de E.

Preuve. On vérifie aisément que la relation $\mathcal{R}$ définie sur E par: $(\forall\, x,y \in E,\ x\ \mathcal{R}\ y \ \Leftrightarrow\ \exists\, g \in G,\ y = g.x)$ est une relation d'équivalence. La classe d'équivalence pour $\mathcal{R}$ d'un élément $x \in E$ n'est autre par définition que l'orbite Ω_x. D'où le résultat puisque les classes d'équivalence forment une partition de E. □

Définitions. Soit G un groupe opérant sur un ensemble non-vide E.

1. Le noyau du morphisme $\gamma : G \longrightarrow S(E)$ canoniquement associé à l'action de G sur E est appelé le noyau de l'action. Il est clair que c'est l'intersection des stabilisateurs:

$$\boxed{\mathrm{Ker}\,\gamma = \{g \in G\,;\, \forall\ x \in E,\ g.x = x\} = \bigcap_{x \in E} G_x}.$$

   On dit que l'action est *fidèle* (ou que G opère fidèlement sur E) lorsque γ est injectif, c'est-à-dire lorsque le noyau de l'action est $\{e\}$. Si G opère fidèlement sur E, alors G est isomorphe à un sous-groupe de $S(E)$, à savoir $\mathrm{Im}\,\gamma$.

2. Un élément $x \in E$ est appelé un *point fixe* de l'action de G lorsque $g.x = x$ pour tout $g \in G$,
   On note E^G ou $\mathrm{Fix}_G(E)$ l'ensemble des points fixes de l'action de G sur E. Pour tout $x \in E$, on a:
   $$\boxed{(x \in E^G) \;\Leftrightarrow\; (G_x = G) \;\Leftrightarrow (\Omega_x = \{x\})}, \quad \text{(orbite ponctuelle)}.$$
   On dit que l'action est *sans point fixe* lorsque $E^G = \emptyset$.

3. On dit que G opère *transitivement* sur E, ou encore que l'action de G sur E est *transitive*, ou encore que E est un G-ensemble *homogène*, lorsqu'il n'y a qu'une seule orbite:
   $$\boxed{(\text{action transitive}) \;\Leftrightarrow\; (\forall\, x \in E,\ \Omega_x = E) \;\Leftrightarrow\; (\forall\, x, y \in E,\ \exists\, g \in G,\ y = g.x)}.$$

1.2 Premier exemple: action d'un groupe sur lui-même par translation.

Tout groupe G opère sur lui-même par translation à gauche:
$$\left|\begin{array}{ccc} G \times G & \longrightarrow & G \\ (g,x) & \longmapsto & g.x = gx \end{array}\right.$$

1. Pour tout $x \in G$, $G_x = \{g \in G\,;\, gx = x\} = \{e\}$.
   On en déduit que $\mathrm{Ker}\,\gamma = \bigcap_{x\in G} G_x = \{e\}$, donc l'action est fidèle.

2. Pour tout $x \in G$, $\Omega_x = \{gx\,;\, g \in G\} = G$ (car tout $y \in G$ s'écrit $y = (yx^{-1})x$).
   On en déduit qu'il n'y a qu'une seule orbite, donc l'action est transitive.
   De plus, dès lors que $G \neq \{e\}$, on a $\Omega_x = G$ non ponctuelle pour tout $x \in G$, donc l'action est sans point fixe.

1.3 Deuxième exemple: action d'un groupe sur lui-même par conjugaison.

Tout groupe G opère sur lui même par conjugaison:
$$\left|\begin{array}{ccc} G \times G & \longrightarrow & G \\ (g,x) & \longmapsto & g.x = gxg^{-1} \end{array}\right.$$

1. Pour tout $x \in G$, $G_x = \{g \in G\,;\, gx = xg\}$ est le *centralisateur* de x, usuellement noté $C_G(x)$.
   Donc $\mathrm{Ker}\,\gamma = \bigcap_{x\in G} G_x = \{g \in G\,;\, \forall\, x \in G,\ gx = xg\}$ est le *centre* de G, usuellement noté $Z(G)$.
   En particulier l'action est fidèle si et seulement si G est de centre trivial, c'est-à-dire $Z(G) = \{e\}$.

2. Pour tout $x \in G$, l'orbite $\Omega_x = \{gxg^{-1}\,;\, g \in G\}$ est la *classe de conjugaison* de x.
   On en déduit que Ω_x est ponctuelle si et seulement si x est central, donc l'ensemble des points fixes E^G est non-vide et égal au centre $Z(G)$.
   De plus $\Omega_e = \{e\}$, donc $\Omega_e \neq G$ dès lors que $G \neq \{e\}$, et l'action n'est alors pas transitive.

1.4 Troisième exemple: action d'un groupe sur l'ensemble de ses parties par conjugaison.

Tout groupe G opère sur $\mathcal{P}(G)$ par conjugaison:
$$\left|\begin{array}{ccc} G \times \mathcal{P}(G) & \longrightarrow & \mathcal{P}(G) \\ (g,X) & \longmapsto & g.X = gXg^{-1} \end{array}\right.$$

1. Pour tout $X \in \mathcal{P}(G)$, $G_X = \{g \in G\,;\, gXg^{-1} = X\}$ est le normalisateur de X, noté $N_G(X)$.

   > Rappel. Dans le cas où $X = H$ est un sous-groupe de G, on montre que H est un sous-groupe de $N_G(H)$, que $H \lhd N_G(H)$, et que $N_G(H)$ est le plus grand sous-groupe de G dans lequel H est normal; en particulier $H \lhd G$ si et seulement si $N_G(H) = G$.

2. On en déduit que $X \in \mathcal{P}(G)^G$ si et seulement si $N_G(X) = G$.

   > Dans le cas où $X = H$ est un sous-groupe de G, cela signifie que $H \lhd G$.

3. On en déduit aussi que $\mathrm{Ker}\,\gamma = Z(G)$.

   > *En effet,* $\mathrm{Ker}\,\gamma = \bigcap_{X\subseteq G} G_X = \bigcap_{X\subseteq G} N_G(X)$. En considérant parmi les $X \subseteq G$ celles qui sont des singletons, il vient: $\mathrm{Ker}\,\gamma \subseteq \bigcap_{x\in G} N_G(\{x\}) = \bigcap_{x\in G} C_G(x) = Z(G)$. L'inclusion réciproque est claire.

4. Pour $X \in \mathcal{P}(G)$, $\Omega_X = \{gXg^{-1}\,;\, g \in G\}$ est la classe de conjugaison de X dans $\mathcal{P}(G)$.
   En particulier l'action n'est pas transitive (car $\Omega_\emptyset = \{\emptyset\} \neq \mathcal{P}(G)$).

2. Equation aux classes, applications aux p-groupes.

2.1 Indice des stabilisateurs.

Proposition. *Soit G un groupe opérant sur un ensemble E. Si deux éléments x et y de E appartiennent à une même orbite, alors leurs stabilisateurs G_x et G_y sont conjugués dans G.*

Preuve. Soient $x \in E$ et $y \in \Omega_x$; il existe donc $g \in G$ tel que $y = g.x$. Montrons: $G_y = gG_xg^{-1}$.

Soit $h \in G_y$. On a $y = h.y$, c'est-à-dire $g.x = h.(g.x) = hg.x$. On en tire: $x = e.x = g^{-1}g.x = g^{-1}.(g.x) = g^{-1}.(hg.x) = (g^{-1}hg).x$, donc $g^{-1}hg \in G_x$, ou encore $h \in gG_xg^{-1}$.

Réciproquement, soit $k \in gG_xg^{-1}$. On a $g^{-1}kg \in G_x$, donc $(g^{-1}kg).x = x$, d'où $kg.x = g.x$, c'est-à-dire $k.y = y$, ou encore $k \in G_y$. □

Théorème. *Soit G un groupe opérant sur un ensemble E.*

(i) *Pour tout $x \in E$, le cardinal de l'orbite Ω_x est égal à l'indice du stabilisateur G_x. On note:*

$$\boxed{|\Omega_x| = [G : G_x]}.$$

(ii) *En particulier, si G est fini, $|\Omega_x|$ divise $|G|$.*

Preuve. On fixe $x \in E$. On note Q_{G_x} l'ensemble des classes à gauche modulo le sous-groupe G_x. On montre que Ω_x et Q_{G_x} sont équipotents en construisant une bijection λ de Ω_x sur Q_{G_x}.

• Un élément de Ω_x est de la forme $g.x$, où $g \in G$; on pose $\lambda(g.x) = gG_x$. Montrons que l'on définit bien ainsi une application $\lambda : \Omega_x \longrightarrow Q_{G_x}$, indépendamment de l'élément g choisi.

Pour cela, considérons $h, g \in G$ tels que $g.x = h.x$; alors $h^{-1}.(g.x) = h^{-1}.(h.x)$, donc $(h^{-1}g).x = (h^{-1}.h).x = e.x = x$; on conclut que $h^{-1}g \in G_x$, d'où $gG_x = hG_x$.

• L'application λ est surjective par construction: tout élément de Q_{G_x} est de la forme gG_x pour un $g \in G$, et donc $\lambda(g.x) = gG_x$.

• L'application λ est injective: en effet, si $g, h \in G$ vérifient $\lambda(g.x) = \lambda(h.x)$, alors $gG_x = hG_x$, donc $h^{-1}g \in G_x$, c'est-à-dire $(h^{-1}g).x = x$, d'où $h.x = h.((h^{-1}g).x) = (hh^{-1}g).x = g.x$. □

Corollaire. *Soit G un groupe opérant sur un ensemble fini E. Soit $\{x_i\}_{1 \leq i \leq r}$ une famille de représentants des orbites distinctes. On a:*

$$\boxed{|E| = \sum_{i=1}^{r} [G : G_{x_i}]}.$$

Preuve. L'ensemble E étant fini, il y a un nombre fini r d'orbites distinctes. Choisissons un représentant x_i dans chacune de ces r orbites. Les Ω_{x_i} pour $1 \leq i \leq r$ forment une partition de E, donc $|E| = \sum_{i=1}^{r} |\Omega_{x_i}|$, d'où le résultat en appliquant le théorème précédent. □

Exemples d'application.

(i) *Si G est un groupe fini d'ordre 33 opérant sur un ensemble E fini de cardinal 19, alors l'action admet forcément des points fixes.*

En effet, toute orbite est d'ordre 1, 3, 11 ou 33. Comme $33 > |E|$, seuls 1, 3 et 11 restent possibles. Si E^G était vide, il n'y aurait pas d'orbite ponctuelle, et on aurait donc en tout et pour tout n orbites à 3 éléments et m orbites à 11 éléments, d'où $3n + 11m = 19$. Cette équation n'ayant pas de solutions dans $\mathbb{N}$, on conclut que $E^G \neq \emptyset$.

(ii) *Soit G un groupe fini d'ordre 15 opérant sans point fixe sur un ensemble E fini de cardinal 17; donner le nombre d'orbites et le cardinal de chacune d'elles.*

Toute orbite est de cardinal 3, 5 ou 15, puisqu'il n'y a pas de points fixes, donc pas d'orbites ponctuelles. S'il y avait une orbite à 15 éléments (il ne peut de toute façon pas y en avoir plus...), les deux éléments restants de E ne pourraient pas former une orbite. C'est donc qu'il n'y a pas d'orbites à 15 éléments. On a donc en tout et pour tout n orbites à 3 éléments et m orbites à 5 éléments, d'où $3n + 5m = 17$. La seule solution dans $\mathbb{N}$ est $n = 4$ et $m = 1$.

2.2 Equation aux classes pour un groupe fini.

THÉORÈME. *Soit G un groupe fini. Pour tout $x \in G$, on note $C_G(x)$ le centralisateur de x dans G. On note $Z(G)$ le centre de G.*

(i) *Le cardinal de la classe de conjugaison de tout élément de G divise $|G|$.*

(ii) *Soit $\{x_i\}_{1\leq i\leq r}$ une famille de représentants des classes de conjugaison distinctes dans G. Alors:*

$$\boxed{|G| = \sum_{i=1}^{r} [G : C_G(x_i)]}.$$

(iii) *Soit $\{x_i\}_{1\leq i\leq k}$ une famille de représentants des classes de conjugaison distinctes* non ponctuelles *dans G. Alors:*

$$\boxed{|G| = |Z(G)| + \sum_{i=1}^{k} [G : C_G(x_i)]}.$$

Preuve. Pour l'action de G sur lui-même par conjugaison (voir 1.3), l'orbite d'un élément $x \in G$ est sa classe de conjugaison Ω_x, et son stabilisateur est son centralisateur $C_G(x)$. Les points (i) et (ii) sont donc des conséquences immédiates du théorème et du corollaire du 2.1 ci-dessus.

Pour montrer (iii), rappelons d'abord (voir 1.3) que l'orbite d'un élément $x \in G$ est ponctuelle si et seulement si $x \in Z(G)$. Notons alors $x_1, \ldots, x_k$ des représentants des orbites non ponctuelles (il peut ne pas y en avoir, auquel cas $k = 0$ et G est abélien), et $x_{k+1}, \ldots, x_r$ des représentants des orbites ponctuelles (il y en a toujours au moins une, celle de e, donc $k < r$). Pour $k+1 \leq i \leq r$, on a $x_i \in Z(G)$ et $|\Omega_{x_i}| = 1$. Pour $1 \leq i \leq k$, on a $x_i \notin Z(G)$ et $|\Omega_{x_i}| = [G : C_G(x_i)] \neq 1$. Donc: $|G| = \sum_{i=1}^{k} |\Omega_{x_i}| + \sum_{i=k+1}^{r} |\Omega_{x_i}| = \sum_{i=1}^{k} [G : C_G(x_i)] + |Z(G)|$. □

2.3 Applications aux p-groupes.

DÉFINITION. Soit p un nombre premier. Un groupe fini est un p-groupe si son ordre est une puissance de p.

Le lemme suivant est à la base de l'étude des p-groupes, et en particulier des théorèmes de Sylow qui seront vus plus tard.

LEMME. *Si G est un p-groupe non trivial opérant sur un ensemble fini non-vide E, alors: $|E^G| \equiv |E| \bmod p$.*

Preuve. On sait (voir 1.1) que $|E^G|$ est le nombre d'orbites ponctuelles. Si toutes les orbites sont ponctuelles, alors $|E| = |E^G|$ et le résultat est clair. Sinon, on note $\Omega_{x_1}, \ldots, \Omega_{x_k}$ les orbites non ponctuelles. Donc: $|E| = |E^G| + \sum_{i=1}^{k} |\Omega_{x_i}|$. Pour tout $1 \leq i \leq k$, on a $|\Omega_{x_i}|$ divise $|G|$ d'après 2.1. Puisque $|G|$ est de la forme p^n avec $n \in \mathbb{N}^*$, on déduit que $|\Omega_{x_i}| = p^{m_i}$ avec $m_i \leq n$. Mais de plus $m_i \geq 1$ puisque $|\Omega_{x_i}| \neq 1$. On conclut que $|E| - |E^G| = \sum_{i=1}^{k} p^{m_i}$ est divisible par p. □

PROPOSITION. *Le centre d'un p-groupe non trivial est non trivial.*

Preuve. On applique ce qui précède à l'action de G sur lui-même par conjugaison (voir 1.3): $E = G$ et $E^G = Z(G)$. Le lemme implique donc que $|G| - |Z(G)|$ est divisible par p. Comme $|G|$ est divisible par p, on conclut que $|Z(G)|$ est divisible par p. Donc $|Z(G)| \neq 1$. □

COROLLAIRE. *Si p est un nombre premier, tout groupe d'ordre p^2 est abélien.*

Preuve. Soit G un groupe d'ordre p^2. D'après le théorème de Lagrange, $|Z(G)|$ divise p^2. Comme $|Z(G)| \neq 1$ d'après la proposition précédente, on a donc $|Z(G)| = p$ ou $|Z(G)| = p^2$. Si $|Z(G)| = p^2$, alors $G = Z(G)$, donc G est abélien. Si $|Z(G)| = p$, alors $|G/Z(G)| = p$ (voir 2.3 du chapitre 1), donc le groupe $G/Z(G)$ est cyclique (voir 1.3 du chapitre 1). Or on a vu (voir 2.4.1.b du chapitre 1) que $G/Z(G)$ monogène implique G abélien. □

EXERCICE. Montrer que: *Si G est un groupe non-abélien d'ordre p^3 avec p premier, alors, quels que soient $x \in G$ et $y \in G$ tels que $xy \neq yx$, le groupe G est engendré par x et y.*

Solution. Soit $H = \langle x, y \rangle$ le sous-groupe engendré par x et y dans G. Son ordre divise p^3. En appliquant le corollaire précédent, $|H| \neq p^2$ car H non abélien puisque $xy \neq yx$. De plus $|H| \neq p$ car sinon H serait cyclique donc abélien. Enfin $|H| \neq 1$ car H contient au moins x et y. On conclut que $|H| = p^3$, donc $H = G$.

□

3. Actions transitives, applications à la non simplicité.

3.1 Exemple fondamental.

Soient G un groupe et H un sous-groupe propre de G. On note Q_H l'ensemble des classes à gauche relativement à H. Donc $Q_H = \{xH\,;\, x \in G\}$.

- Le groupe G opère sur l'ensemble Q_H par translation à gauche: $\left|\begin{array}{ccc} G \times Q_H & \longrightarrow & Q_H \\ (g, xH) & \longmapsto & g.xH = gxH \end{array}\right.$

  En effet. Les deux conditions définissant une action sont clairement vérifiées. Le seul problème est de vérifier d'abord que l'application ci-dessus est bien définie, indépendamment du représentant de classe à gauche choisi. Pour cela, soit y un autre représentant de xH. On a donc $xH = yH$, ou encore $y^{-1}x \in H$. Pour tout $g \in G$, on a: $(gy)^{-1}(gx) = y^{-1}g^{-1}gx = y^{-1}x$; d'où $(gy)^{-1}(gx) \in H$, c'est-à dire $gyH = gxH$. □

- Cette action est transitive et sans point fixe.

  En effet. L'orbite de $eH = H$ est $\Omega_{eH} = \{geH\,;\, g \in G\} = \{gH\,;\, g \in G\} = Q_H$. Donc l'action est transitive. De plus, comme $H \neq G$, il existe $x \in G$ tel que $x \notin H$, donc $xH \neq H$, de sorte que Q_H n'est pas un singleton. Donc l'unique orbite ci-dessus n'est pas ponctuelle: l'action est sans point fixe. □

- Le stabilisateur d'un élément $xH \in Q_H$ est $G_{xH} = xHx^{-1}$.

  En effet. On a: $g \in G_{xH} \Leftrightarrow gxH = xH \Leftrightarrow gx \in xH \Leftrightarrow g \in xHx^{-1}$. □

- Le noyau du morphisme $\gamma : G \to S(Q_H)$ canoniquement associé à l'action est égal à $\bigcap_{x\in G} xHx^{-1}$, qui est le plus grand sous-groupe normal de G contenu dans H.

  En effet. On sait que $\operatorname{Ker}\gamma = \bigcap_{xH\in Q_H} G_{xH}$ donc ici $\operatorname{Ker}\gamma = \bigcap_{x\in G} xHx^{-1}$. Il est clair qu'il est normal dans G (c'est un noyau!) et que $\operatorname{Ker}\gamma \subset H$ (car $g \in \operatorname{Ker}\gamma$ implique qu'en particulier pour $x = e$, on a $g \in eHe^{-1} = H$). Enfin, soit N un sous-groupe normal de G contenu dans H. Pour tout $x \in G$, on a: $xNx^{-1} = N$ et $xNx^{-1} \subset xHx^{-1}$, donc $N \subset xHx^{-1}$. Ceci étant vrai pour tout $x \in G$, on obtient $N \subset \bigcap_{x\in G} xHx^{-1}$. Donc $\operatorname{Ker}\gamma$ est le plus grand sous-groupe normal de G contenu dans H. □

Remarque. On peut montrer que cet exemple est en fait plus qu'un exemple, dans la mesure où toute action transitive d'un groupe G sur un ensemble E se ramène, "à isomorphisme de G-ensembles près", à l'action de G par translation sur Q_H.

3.2 Applications.

Définition. Un groupe G est dit *simple* si $G \neq \{e\}$ et si G n'admet pas de sous-groupes normaux autres que $\{e\}$ et G.

Lemme. *Si G est un groupe simple, et si H est un sous-groupe de G distinct de G, alors l'action de G sur Q_H par translation à gauche est fidèle.*

Preuve. On a vu que $\operatorname{Ker}\gamma$ est un sous-groupe normal de G contenu dans H. La simplicité de G implique donc que $\operatorname{Ker}\gamma = \{e\}$ ou $\operatorname{Ker}\gamma = G$. Si on avait $\operatorname{Ker}\gamma = G$, comme $\operatorname{Ker}\gamma \subset H$, on aurait $G = H$, ce qui est exclu. Donc $\operatorname{Ker}\gamma = \{e\}$. □

Corollaire. *Soit G un groupe fini. Soit H un sous-groupe de G d'indice $k \geq 2$. Si $|G|$ ne divise pas $k!$, alors G n'est pas simple.*

Preuve. Comme $[G : H] \geq 2$, le sous-groupe H est distinct de G. Si G était simple, il résulterait du lemme précédent que le noyau $\operatorname{Ker}\gamma$ de l'action de G sur Q_H par translation serait réduit à $\{e\}$. On aurait donc $G \simeq G/\operatorname{Ker}\gamma \simeq \operatorname{Im}\gamma$. Ainsi, G serait isomorphe à un sous-groupe de $S(Q_H)$, et donc $|G|$ diviserait $|S(Q_H)|$. Mais par définition de l'indice, on a $k = [G : H] = |Q_H|$, et donc $|S(Q_H)| = k!$ □

Remarque. Soient G un groupe et H un sous-groupe propre de G. On peut considérer la restriction à H de l'action considérée en 3.1, c'est-à-dire faire opérer H sur Q_H par translation à gauche:

$$\left|\begin{array}{ccc} H \times Q_H & \longrightarrow & Q_H \\ (h, xH) & \longmapsto & h.xH = hxH \end{array}\right.$$

Cette action n'est plus transitive.

En effet. Pour tout $xH \in Q_H$, c'est-à-dire pour tout $x \in G$, l'orbite de xH est $\Omega_{xH} = \{hxH\,;\, h \in H\}$. En particulier $\Omega_{eH} = \Omega_H = \{hH\,;\, h \in H\} = \{H\}$. Si l'action ci-dessus était transitive, on aurait pour tout $x \in G$: $\Omega_{xH} = \Omega_{eH}$, donc $xH = H$, donc $x \in H$. Ce qui contredirait l'hypothèse $H \neq G$.

THÉORÈME (dit de Frobenius). *Soient G un groupe fini, et H un sous-groupe de G dont l'indice $p = [G : H]$ est le plus petit diviseur premier de $|G|$. Alors H est normal dans G.*

Preuve. Considérons l'action de H sur Q_H par translation à gauche. Comme on vient de le voir, elle n'est pas transitive. Il existe donc un nombre $r \geq 2$ d'orbites distinctes $\Omega_{x_1 H}, \ldots, \Omega_{x_r H}$. Notons $q_i = |\Omega_{x_i H}|$ pour tout $1 \leq i \leq r$. D'une part les orbites forment une partition de Q_H, donc $p = [G : H] = |Q_H| = q_1 + \cdots + q_r$. D'autre part chaque q_i divise $|G|$. Si l'un des q_i n'est pas 1, il est forcément $\geq p$ (car p est le plus petit diviseur > 1 de $|G|$) et, comme $r \geq 2$, cela contredit l'égalité $p = q_1 + \cdots + q_r$. C'est donc que chaque q_i vaut 1 et que $r = p$. En d'autres termes, pour tout $1 \leq i \leq p$, le stabilisateur $H_{x_i H}$ est égal à H.

Soit $x \in G$. Il existe un unique $1 \leq i \leq p$ tel que $\Omega_{xH} = \Omega_{x_i H}$, ce qui, comme on l'a vu en 2.1, implique que les stabilisateurs H_{xH} et $H_{x_i H}$ sont conjugués dans H (le groupe qui opère est ici H). Il existe donc $h \in H$ tel que $H_{xH} = hH_{x_i H}h^{-1}$. Or on a vu ci-dessus que $H_{x_i H} = H$. Donc $H_{xH} = hHh^{-1} = H$. Ainsi tout $h \in H$ vérifie $h.xH = xH$, c'est-à-dire $x^{-1}hx \in H$, ou encore $h \in xHx^{-1}$. Ceci prouve que $H \subset xHx^{-1}$.

On en déduit que, pour tout $x \in G$, on a: $x^{-1}Hx \subseteq x^{-1}(xHx^{-1})x = H$. On conclut: $H \lhd G$. □

REMARQUE. Pour $p = 2$, on retrouve le fait que tout sous-groupe d'indice 2 est normal.

Chapitre 3

Groupes finis: théorèmes de Sylow

1. Les théorèmes de Sylow.

1.1 Premier théorème de Sylow.

Remarque préliminaire. Il n'y a pas de réciproque naïve au théorème de Lagrange, au sens que, pour un diviseur m de l'ordre n d'un groupe fini G, il n'existe pas forcément de sous-groupe d'ordre m dans G. Par exemple, on a vu que le groupe alterné A_4, qui est d'ordre 12, ne contient pas de sous-groupe d'ordre 6. Le premier théorème de Sylow montre que c'est cependant le cas si m est puissance d'un nombre premier.

Lemme technique. *Soit p un nombre premier. Soient r, s, n trois entiers naturels non-nuls tels que $r \leq n$ et p ne divise pas s. Alors le coefficient binomial $\binom{sp^n}{p^r}$ est de la forme kp^{n-r} pour un entier $k \geq 1$ non divisible par p.*

Preuve. On calcule: $\displaystyle\binom{sp^n}{p^r} = \frac{(sp^n)!}{p^r!(sp^n-p^r)!} = \frac{sp^n(sp^n-1)(sp^n-2)\dots(sp^n-p^r+1)}{p^r(p^r-1)\times\dots\times 2\times 1}$

$$= \frac{sp^n}{p^r}\times\frac{sp^n-1}{1}\times\frac{sp^n-2}{2}\times\dots\frac{sp^n-(p^r-1)}{p^r-1} = p^{n-r}\times \underbrace{s\times\prod_{j=1}^{p^r-1}\frac{sp^n-j}{j}}_{\text{soit } k}$$

Considérons un entier $1 \leq j \leq p^r-1$. Ecrivons-le sous la forme $j = b_j p^{t_j}$ avec $t_j \in \mathbb{N}$ et b_j non divisible par p. Comme $j < p^r$, on a nécessairement $t_j < r$, et donc $n - t_j \geq r - t_j \geq 1$. On écrit:

$$\frac{sp^n-j}{j} = \frac{sp^n-b_jp^{t_j}}{b_jp^{t_j}} = \frac{sp^{n-t_j}-b_j}{b_j} := \frac{a_j}{b_j}, \quad \text{en posant } a_j := sp^{n-t_j}-b_j.$$

Comme p ne divise pas b_j, il ne divise pas non plus a_j. Parce que p est premier, cela implique que p ne divise pas les entiers $a := a_1\times\dots\times a_{p^r-1}$ et $b := b_1\times\dots\times b_{p^r-1}$. En résumé, $k = \frac{sa}{b}$, où p ne divise ni s, ni a, ni b.

On a l'égalité: $sap^{n-r} = b\binom{sp^n}{p^r}$. Donc p^{n-r} divise $b\binom{sp^n}{p^r}$. Mais p^{n-r} est premier avec b puisque p est premier ne divisant pas b. On déduit avec le lemme de Gauss que p^{n-r} divise $\binom{sp^n}{p^r}$, donc $k = \frac{1}{p^{n-r}}\binom{sp^n}{p^r}$ est entier. Enfin, puisque p ne divise pas sa, il résulte de l'égalité $sa = kb$ et du lemme de Gauss que p ne divise pas k. □

Théorème (dit premier théorème de Sylow). *Soit G un groupe fini. Soit p un nombre premier divisant $|G|$. Notons $|G| = sp^n$ avec $n \in \mathbb{N}^*$ et $s \in \mathbb{N}^*$ non divisible par p. Alors, pour tout entier $1 \leq r \leq n$, il existe un sous-groupe de G d'ordre p^r.*

Preuve. Fixons $1 \leq r \leq n$ et notons E l'ensemble des parties de G à p^r éléments, de sorte que $|E| = \binom{|G|}{p^r} = \binom{sp^n}{p^r}$. D'après le lemme, il existe $k \in \mathbb{N}^*$ non-divisible par p tel que $|E| = kp^{n-r}$.

Pour tout $A \in E$ et tout $g \in G$, on a $|gA| = |A| = p^r$, donc G opère sur E par translation:

$$\begin{array}{ccc} G\times E & \longrightarrow & E \\ (g,A) & \longmapsto & gA. \end{array}$$

Soit $\{A_i\}_{1\leq i\leq m}$ une famille de représentants des orbites distinctes pour cette action. On sait (voir chapitre 2, 2.1) que $\sum_{i=1}^m [G : G_{A_i}] = |E| = kp^{n-r}$, où G_{A_i} est le stabilisateur de A_i. Si p^{n-r+1} divisait tous les $[G : G_{A_i}]$, il diviserait kp^{n-r}, donc p diviserait k, ce qui n'est pas le cas.

On a ainsi montré qu'il existe un entier $1 \leq h \leq m$ tel que p^{n-r+1} ne divise pas $[G : G_{A_h}]$. Pour cet entier h, notons H le stabilisateur G_{A_h}. On se propose de montrer que H est un des sous-groupes d'ordre p^r cherché.

On a: $[G : H]\times|H| = |G| = sp^n$. Si l'on note $[G : H] = s'p^\alpha$ et $|H| = s''p^\beta$, avec $\alpha, \beta \in \mathbb{N}$, et $s', s'' \in \mathbb{N}^*$ non divisibles par p, on a donc: $s's'' = s$ et $\alpha+\beta = n$. La condition $[G : H]$ non

divisible par p^{n-r+1} se traduit en outre par l'inégalité $\alpha \leq n-r$. Il en résulte que $r \leq n-\alpha \leq n$, c'est-à-dire $r \leq \beta \leq n$, donc p^r divise p^β, et donc p^r divise $|H|$.

Par ailleurs, par définition du stabilisateur $G_{A_h} = H$, on a $gA_h = A_h$ pour tout $g \in H$. Ceci permet de considérer, pour un élément $a \in A_h$ fixé quelconque, l'application $f : H \to A_h$ définie par $f(g) = ga$ pour tout $g \in H$. Elle est clairement injective, donc $|H| \leq |A_h|$. Mais $|A_h| = p^r$ puisque $A_h \in E$. Ainsi $|H| \leq p^r$. On a vu précédemment que p^r divise $|H|$. On conclut que $|H| = p^r$. □

COROLLAIRE (dit théorème de Cauchy). *Soit G un groupe fini. Pour tout nombre premier p divisant $|G|$, il existe dans G un élément d'ordre p.*

Preuve. On applique le théorème précédent pour $r = 1$. Il existe dans G un sous-groupe H d'ordre p. Comme H est d'ordre premier, il est cyclique, engendré par un élément d'ordre p. □

1.2 Sous-groupes de Sylow.

DÉFINITIONS. Soit G un groupe fini. Soit p un nombre premier divisant $|G|$. Notons $|G| = sp^n$ avec $n \in \mathbb{N}^*$ et $s \in \mathbb{N}^*$ non divisible par p.

1. On appelle p-sous-groupe de G tout sous-groupe de G dont l'ordre est une puissance de p, c'est-à-dire tout sous-groupe H de G tel que $|H| = p^r$ avec $0 \leq r \leq n$.
2. On appelle p-sous-groupe de Sylow de G tout p-sous-groupe de G d'ordre maximal, c'est-à-dire tout sous-groupe H de G tel que $|H| = p^n$.

EXEMPLE. Soit G un groupe fini d'ordre 72. Il existe dans G des sous-groupes d'ordre 2, 4 et 8. Parmi eux, les 2-sous-groupes de Sylow sont ceux d'ordre 8. Il existe aussi dans G des sous-groupes d'ordre 3 et 9. Parmi eux, les 3-sous-groupes de Sylow sont ceux d'ordre 9.

Le théorème suivant a pour objet de préciser la structure des p-sous-groupes de Sylow dont le théorème précédent a établi l'existence.

1.3 Second théorème de Sylow.

LEMME 1. *Si G est un p-groupe non trivial opérant sur un ensemble fini non-vide E, alors: $|E^G| \equiv |E| \bmod p$.*

Preuve. Démontré au 2.3 du chapitre 2. □

LEMME 2. *Soit G un groupe. Soit p un nombre premier. On suppose qu'il existe dans G un sous-groupe K d'ordre p^n, avec $n \geq 1$, et un sous-groupe H d'indice r non divisible par p. Alors K est inclus dans un conjugué de H.*

Preuve. Soit Q_H l'ensemble des classes à gauche modulo H; donc $Q_H = \{xH\,;\, x \in G\}$. Considérons l'action de K sur Q_H par translation à gauche:

$$\begin{array}{ccc} K \times Q_H & \longrightarrow & Q_H \\ (g\,,\, xH) & \longmapsto & gxH. \end{array}$$

En appliquant le lemme 1 au p-groupe K, on déduit: $|(Q_H)^K| \equiv |Q_H| \bmod p$. Or $|Q_H| = [G : H] = r$, qui par hypothèse n'est pas divisible par p. On en tire: $|(Q_H)^K| \neq 0$, c'est-à-dire $(Q_H)^K \neq \emptyset$. Il existe donc $x \in G$ tel que la classe à gauche xH soit un point fixe de l'action. On a:

$$(xH \in (Q_H)^K) \;\Leftrightarrow\; (\forall\, g \in K,\; gxH = xH) \;\Leftrightarrow\; (\forall\, g \in K,\; gx \in xH) \;\Leftrightarrow\; (\forall\, g \in K,\; g \in xHx^{-1}).$$

On conclut que $K \subseteq xHx^{-1}$. □

LEMME 3. *Soient G un groupe fini, et p un nombre premier divisant $|G|$. Si H est un p-sous-groupe de Sylow de G, alors H est l'unique p-sous-groupe de Sylow de son normalisateur.*

Preuve. Notons $|G| = sp^n$ avec $n \geq 1$ et $s \geq 1$ non divisible par p. On a donc $|H| = p^n$. Considérons le normalisateur $N_G(H)$ de H dans G. C'est un sous-groupe de G, donc son ordre divise $|G| = sp^n$. Posons $|N_G(H)| = s'p^\alpha$ avec $s' \in \mathbb{N}^*$ non divisible par p et $0 \leq \alpha \leq n$. Par ailleurs, H est un sous-groupe de $N_G(H)$, donc $|H| = p^n$ divise $|N_G(H)| = s'p^\alpha$. On a donc finalement $|N_G(H)| = s'p^n$, d'où $[N_G(H) : H] = s'$.

Soit K un p-sous-groupe de Sylow de $N_G(H)$. On a donc $|K| = p^n$. En appliquant le lemme 2 aux sous-groupes H et K du groupe $N_G(H)$, on déduit qu'il existe $x \in N_G(H)$ tel que $K \subseteq xHx^{-1}$. Mais $H \lhd N_G(H)$, de sorte que $xHx^{-1} = H$. On conclut que $K \subseteq H$, ce qui, comme les deux groupes sont de même ordre p^n, permet de conclure que $K = H$. □

THÉORÈME (dit second théorème de Sylow). *Soit G un groupe fini. Soit p un nombre premier divisant $|G|$. Notons $|G| = sp^n$ avec $n \in \mathbb{N}^*$ et $s \in \mathbb{N}^*$ non divisible par p. Alors:*

(i) *tout p-sous-groupe de G est contenu dans un p-sous-groupe de Sylow;*

(ii) *les p-sous-groupes de Sylow de G sont conjugués dans G;*

(iii) *le nombre N_p des p-sous-groupes de Sylow de G vérifie:*

$$N_p \text{ divise } s, \qquad \text{et} \qquad N_p \equiv 1 \bmod p.$$

Preuve. (i). Soit K un p-sous-groupe de G non trivial; notons $|K| = p^r$ avec $1 \leq r \leq n$. Soit H un p-sous-groupe de Sylow de G; donc $|H| = p^n$, d'où $[G : H] = s$. Comme p ne divise pas s, on peut appliquer le lemme 2: il existe $x \in G$ tel que $K \subseteq xHx^{-1}$. Mais $|xHx^{-1}| = |H| = p^n$, de sorte que xHx^{-1} est lui-même un p-sous-groupe de Sylow de G. Ce qui prouve (i).

(ii). Si H et H' sont deux p-sous-groupes de Sylow de G, le raisonnement ci-dessus appliqué à $K = H'$ montre que $H' \subseteq xHx^{-1}$ pour un certain $x \in G$. Mais $|H'| = p^n = |H| = |xHx^{-1}|$, donc $H' = xHx^{-1}$. Ce qui prouve (ii).

(iii). Notons $\mathcal{S}$ l'ensemble des p-sous-groupes de Sylow de G, et $N_p = |\mathcal{S}|$. Il résulte du point (ii) ci-dessus que G opère transitivement par conjugaison sur $\mathcal{S}$. Il n'y a donc qu'une seule orbite:

$$\text{pour tout } H \in \mathcal{S}, \text{ on a } \mathcal{S} = \Omega_H \text{ et } N_p = |\mathcal{S}| = |\Omega_H| = [G : G_H].$$

Fixons un p-sous-groupe de Sylow $H \in \mathcal{S}$. Le stabilisateur G_H est ici $\{x \in G\,;\, xHx^{-1} = H\}$, qui n'est autre que le normalisateur $N_G(H)$ de H dans G. D'où: $N_p = [G : N_G(H)] = \frac{|G|}{|N_G(H)|}$. Comme $|H|$ divise $|N_G(H)|$, l'entier $\frac{|G|}{|N_G(H)|}$ divise l'entier $\frac{|G|}{|H|} = s$. On a ainsi montré que N_p divise s.

Par ailleurs, il est clair que H opère sur $\mathcal{S}$ par conjugaison. En appliquant le lemme 1, on obtient $|\mathcal{S}^H| \equiv |\mathcal{S}| \bmod p$, c'est-à-dire $N_p \equiv |\mathcal{S}^H| \bmod p$. Or $\mathcal{S}^H$ est l'ensemble des éléments $H' \in \mathcal{S}$ tels que $H' = xH'x^{-1}$ pour tout $x \in H$, c'est-à-dire tels que $H \subset N_G(H')$. Mais d'après le lemme 3, le seul p-sous-groupe de Sylow de G contenu dans $N_G(H')$ est H'. On conclut que $H' = H$, donc $|\mathcal{S}^H| = 1$. Ce qui achève la preuve du point (iii). □

COROLLAIRE. *Soient G un groupe fini et p un diviseur premier de $|G|$.*

(i) *Soit H un p-sous-groupe de Sylow de G; alors H est le seul p-sous-groupe de Sylow de G si et seulement si H est normal dans G.*

(ii) *Si G est abélien, il n'existe dans G qu'un seul p-sous-groupe de Sylow.*

Preuve. Le point (i) est une conséquence immédiate du point (ii) du théorème précédent. Le point (ii) découle immédiatement de (i). □

2. Exemples d'applications.

2.1 Cas des groupes abéliens.

REMARQUE PRÉLIMINAIRE. On a défini au chapitre 1 la notion de produit direct de deux sous-groupes d'un groupe. Cette notion se généralise aisément à un nombre fini quelconque de sous-groupes, de la façon suivante:
soient G un groupe, et $H_1, \ldots, H_k$ des sous-groupes de G; on dit que G est le produit direct des sous-groupes $H_1, \ldots, H_k$ lorsque:
(1) $G = H_1 H_2 \ldots H_k$,
(2) $H_i \cap (H_1 \ldots H_{i-1} H_{i+1} \ldots H_k) = \{e\}$ pour tout $1 \leq i \leq k$;
(3) $h_i h_j = h_j h_i$ pour tous $h_i \in H_i, h_j \in H_j$, quels que soient $1 \leq i \neq j \leq k$.

Dans ce cas, tout élément de G s'écrit de façon unique comme un produit $h_1 h_2 \ldots h_k$ avec $h_1 \in H_1, h_2 \in H_2, \ldots, h_k \in H_k$.

Il est clair que, si $G_1, \ldots, G_k$ sont k groupes quelconques, un groupe G est isomorphe au produit direct (externe) $G_1 \times \cdots \times G_k$ si et seulement s'il existe dans G des sous-groupes $H_1, \ldots, H_k$ tels que G soit le produit direct (interne) des sous-groupes $H_1, \ldots, H_k$ et tels que $H_i \simeq G_i$ pour tout $1 \leq i \leq k$.

LEMME. *Soit G un groupe fini non trivial. Soit $|G| = p_1^{n_1} \ldots p_k^{n_k}$ la décomposition en facteurs premiers de l'ordre de G, avec les p_i premiers deux à deux distincts et les n_i entiers ≥ 1. Si G admet pour tout $1 \leq i \leq k$ un unique p_i-sous-groupe de Sylow H_i, alors G est le produit direct des H_i.*

Preuve. Remarquons d'abord que, pour tous $1 \leq i \neq j \leq k$, on a $H_i \cap H_j = \{e\}$ d'après le théorème de Lagrange. De plus $H_i \triangleleft G$ pour tout $1 \leq i \leq k$ d'après le point (ii) du dernier corollaire de 1.3. Dès lors, pour tous $h_i \in H_i$ et $h_j \in H_j$:

$$\underbrace{(h_i h_j h_i^{-1})}_{\in H_j} h_i = h_i h_j = h_j \underbrace{(h_j^{-1} h_i h_j)}_{\in H_i} \implies h_j^{-1} h_i h_j h_i^{-1} \in H_i \cap H_j \implies h_j^{-1} h_i h_j h_i^{-1} = e,$$

ce qui signifie que $h_i h_j = h_j h_i$. Les autres conditions assurant que G est le produit direct $H_1 H_2 \dots H_k$ sont alors claires en raisonnant sur les ordres. □

THÉORÈME. *Tout groupe abélien fini non trivial est produit direct de ses sous-groupes de Sylow.*

Preuve. D'après le point (ii) du dernier corollaire de 1.3, on est dans les conditions d'application du lemme précédent, qui donne immédiatement le résultat voulu. □

REMARQUE: Soit G un groupe abélien fini non trivial. Soit $|G| = p_1^{n_1} \dots p_k^{n_k}$ la décomposition en facteurs premiers de l'ordre de G, avec les p_i premiers deux à deux distincts et les n_i entiers ≥ 1. Fixons $1 \leq i \leq k$ quelconque. Le p_i-sous-groupe de Sylow H_i de G, qui est d'ordre $p_i^{n_i}$, s'exprime d'après le théorème 3.4 du chapitre 1 comme un produit de groupes cycliques $C_{p_i^{r_1}} C_{p_i^{r_2}} \cdots C_{p_i^{r_m}}$ pour des entiers $1 \leq r_1 \leq r_2 \leq \cdots \leq r_m$ uniques, satisfaisant $r_1 + r_2 + \cdots + r_m = n_i$.

2.2 Quelques résultats de non-simplicité.

PROPOSITION 1. *Tout groupe d'ordre pq avec p et q deux nombres premiers distincts n'est pas simple.*

Preuve. Soit G un groupe d'ordre pq. Quitte à échanger les rôles de p et q, on peut sans restriction supposer que $p > q$. On sait par le second théorème de Sylow que le nombre N_p de p-sous-groupes de Sylow de G divise q, et vérifie $N_p \equiv 1 \bmod p$. Comme q est premier, on ne peut avoir que $N_p = 1$ ou $N_p = q$. Si l'on avait $N_p = q$, on aurait $q \equiv 1 \bmod p$, donc p diviserait $q - 1$, ce qui contredit l'hypothèse $p > q$. C'est donc que $N_p = 1$. Il y a un seul p-sous-groupe de Sylow; on sait qu'il est alors normal dans G, et donc G n'est pas simple. □

PROPOSITION 2. *Tout groupe d'ordre $p^2 q$ avec p et q deux nombres premiers distincts n'est pas simple.*

Preuve. Soit G un groupe d'ordre $p^2 q$. D'après le second théorème de Sylow, le nombre N_q de q-sous-groupes de Sylow de G divisant p^2, trois cas sont possibles.

Si $N_q = 1$, l'unique q-sous-groupe de Sylow est normal (voir dernier corollaire de 1.3). Donc G n'est pas simple.

Si $N_q = p$, il résulte de la condition $N_q \equiv 1 \bmod q$ qu'il existe $\lambda \in \mathbb{N}$ tel que $p = \lambda q + 1$. Comme $p \neq 1$, on a $\lambda \geq 1$, donc $p \geq q + 1$. Par ailleurs, le nombre N_p de p-sous-groupes de Sylow divise q, donc vaut 1 ou q. Supposons que l'on ait $N_p = q$. La condition $N_p \equiv 1 \bmod p$ devenant $q \equiv 1 \bmod p$, on déduit comme ci-dessus que $q \geq p + 1$, d'où une contradiction avec l'inégalité $p \geq q + 1$ précédente. C'est donc que $N_p = 1$; l'unique p-sous-groupe de Sylow est alors normal, donc G n'est pas simple.

Si $N_q = p^2$, notons $(S_i)_{1 \leq i \leq p^2}$ les q-sous-groupes de Sylow. Chacun est d'ordre q premier, donc cyclique, donc formé du neutre e et de $(q-1)$ éléments d'ordre q. Comme les S_i sont d'intersection deux à deux réduite à $\{e\}$, (cela résulte immédiatement du théorème de Lagrange), la réunion des S_i comprend $p^2 \times (q-1)$ éléments d'ordre q, (plus le neutre e d'ordre 1). Le cardinal de l'ensemble des éléments de G qui ne sont pas d'ordre q est donc: $|G| - p^2(q-1) = p^2 q - p^2(q-1) = p^2$. Ce cardinal p^2 ne permet dans G que l'existence d'un seul p-sous-groupe de Sylow. Ce dernier est alors normal, donc G n'est pas simple. □

PROPOSITION 3. *Tout groupe d'ordre pqr avec p, q et r trois nombres premiers distincts n'est pas simple.*

Preuve. Soit G un groupe d'ordre pqr. Quitte à permuter, on peut sans restriction supposer que $p > q > r$. Soit N_p, N_q, N_r les nombres respectifs de p-sous-groupes, q-sous-groupes et r-sous-groupes de Sylow de G.

Montrons d'abord que l'on a l'inégalité: (*) $pqr \geq N_p(p-1) + N_q(q-1) + N_r(r-1)$.

Désignons par S_i, pour $1 \leq i \leq N_p$ les p-sous-groupes de Sylow de G. Chacun d'eux est d'ordre p, donc contient $p-1$ éléments d'ordre p (plus le neutre e qui est d'ordre 1). Comme les S_i sont d'intersection deux à deux réduite à $\{e\}$, (cela résulte immédiatement du théorème de Lagrange), la réunion des S_i comprend $N_p \times (p-1)$ éléments d'ordre p, (plus le neutre e d'ordre 1). Donc G contient $N_p(p-1)$ éléments d'ordre p, et de même bien sûr $N_q(q-1)$ éléments d'ordre q et $N_r(r-1)$ éléments d'ordre r. Comme $|G| = pqr$, on obtient l'inégalité (*) voulue.

Faisons maintenant l'hypothèse: (H) $N_p > 1$ et $N_q > 1$ et $N_r > 1$.

(1) On sait que N_p divise qr. D'après (H), le cas $N_p = 1$ est exclu. Supposons que $N_p = q$; on aurait alors $q \equiv 1 \bmod p$, ce qui impliquerait (comme on l'a vu dans la preuve de la proposition 2) que $q \geq p+1$. Ceci est contraire aux hypothèses de départ, ce qui prouve que $N_p = q$ est impossible. De même $N_p = r$ conduirait à $r \geq p+1$ et une contradiction. On conclut donc finalement que: $N_p = qr$.
(2) On sait que N_q divise pr. D'après (H), le cas $N_q = 1$ est exclu. Supposons que $N_q = r$; on aurait alors $r \equiv 1 \bmod q$, ce qui impliquerait (comme on l'a vu dans la preuve de la proposition 2) que $r \geq q+1$. Ceci est contraire aux hypothèses de départ, ce qui prouve que $N_q = r$ est impossible. Donc, $N_q = p$ ou pr. Dans les deux cas, on a: $N_q \geq p$.
(3) On sait que N_r divise pq. D'après (H), le cas $N_r = 1$ est exclu. Donc, $N_r = p$ ou q ou pq. Dans les trois cas, on a: $N_r \geq q$.

Il résulte de (1), (2) et (3) que $N_p(p-1)+N_q(q-1)+N_r(r-1) \geq qr(p-1)+p(q-1)+q(r-1) = pqr + pq - p - q$. L'inégalité (*) implique alors $p + q \geq pq$. Ceci est impossible, ce qui prouve que la condition (H) est absurde. On a donc $N_p = 1$ ou $N_q = 1$ ou $N_r = 1$. On sait que l'unique sous-groupe de Sylow est alors normal, et donc G n'est pas simple. □

LEMME 4. *Soit G un groupe d'ordre $p^n q$ avec p et q deux nombres premiers distincts et $n \geq 2$. Si $p > q$, ou si p^n ne divise pas $(q-1)!$, alors G n'est pas simple.*

Preuve. Supposons d'abord $p > q$. Soit N_p le nombre de p-sous-groupes de Sylow de G. On sait que N_p divise q, donc vaut q ou 1. Si $N_p = q$, la condition $N_p \equiv 1 \bmod p$ devient $q \equiv 1 \bmod p$, et il existe donc $\lambda \in \mathbb{N}$ tel que $q = \lambda p + 1$. L'entier λ est non-nul car $q \neq 1$, donc $q > p$, ce qui contredit l'hypothèse $p > q$. C'est donc que $N_p = 1$; l'unique p-sous-groupe de Sylow est alors normal, donc G n'est pas simple. (On peut aussi utiliser directement le théorème de Frobenius).

Supposons maintenant que p^n ne divise pas $(q-1)!$. Soit H un p-sous-groupe de Sylow de G. Il est d'ordre p^n donc $[G : H] = |G||H|^{-1} = p^n q p^{-n} = q \geq 2$. Par ailleurs l'hypothèse faite implique que $p^n q = |G|$ ne divise pas $q!$. On applique alors le corollaire du 3.2 du chapitre 2 pour conclure que G n'est pas simple. □

PROPOSITION 5. *Les groupes abéliens simples sont les groupes cycliques d'ordre premier.*

Preuve. Soit G un groupe abélien simple. Il n'admet donc aucun sous-groupe hormis $\{e\}$ et G. Soient x un élément quelconque de G distinct de e, et $\langle x \rangle$ le sous-groupe monogène engendré par x. Comme $\langle x \rangle \neq \{e\}$, on a nécessairement $G = \langle x \rangle$, de sorte que G est monogène. Si G était infini, il serait isomorphe au groupe additif $\mathbb{Z}$, qui n'est évidemment pas simple (tout $n\mathbb{Z}$ avec $n \in \mathbb{Z}$ est un sous-groupe). C'est donc que G est fini. On conclut que G est cyclique. Soit $p = |G| = |x|$. Pour tout diviseur d de p dans $\mathbb{N}$, l'élément x^d engendre un sous-groupe de G d'ordre pd^{-1}. La simplicité de G implique que $d = 1$ ou $d = p$, ce qui prouve que p est premier. Il est clair réciproquement que tout groupe cyclique d'ordre premier est abélien simple. □

COROLLAIRE 6. *Tout groupe d'ordre p^n avec p premier et $n \geq 2$ n'est pas simple.*

Preuve. Par l'absurde, supposons que G soit simple d'ordre p^n avec p premier et $n \geq 2$. On sait (2.3 du chapitre 2) que son centre $Z(G)$ n'est pas réduit à $\{e\}$. Comme $Z(G) \lhd G$, la simplicité de G implique alors $Z(G) = G$. Donc G est abélien. Mais alors la proposition 6 implique que G est d'ordre premier, d'où la contradiction puisque $n \geq 2$. □

EXERCICE 7. *Soit G un groupe d'ordre $p^n q^m$ avec p et q deux nombres premiers distincts et $n, m \geq 1$. Si $p^n < q + 1$, alors G n'est pas simple.*

Solution. Soit N_q le nombre de q-sous-groupes de Sylow de G. On sait que N_q divise p^n; il existe donc un entier $0 \leq \alpha \leq n$ tel que $N_q = p^\alpha$. De plus la condition $N_q \equiv 1 \bmod q$ implique qu'il existe $\lambda \in \mathbb{N}$ tel que $N_q = \lambda q + 1$. Ainsi $p^\alpha = \lambda q + 1$. Mais $p^\alpha \leq p^n$ qui est, par hypothèse, strictement inférieur à $q + 1$. Donc $\lambda q < q$, c'est-à-dire $\lambda = 0$. On conclut que $N_q = 1$; l'unique q-sous-groupe de Sylow est alors normal, et donc G n'est pas simple. □

EXERCICE 8. Montrer que tout groupe d'ordre 36, 40, ou 56, n'est pas simple.

Solution. Observons d'abord que ces trois entiers ne satisfont les hypothèses d'aucun des résultats précédents, et nécessitent donc une étude particulière.

Si $|G| = 40 = 5 \times 2^3$, on a N_5 qui divise 2^3, donc vaut $1, 2, 4$ ou 8. La condition $N_5 \equiv 1 \bmod 5$ n'est vérifiée que pour $N_5 = 1$. L'unique 5-sous-groupe de Sylow est alors normal dans G. Donc G n'est pas simple.

Si $|G| = 56 = 7 \times 2^3$, on a N_7 qui divise 2^3, donc vaut $1, 2, 4$ ou 8. La condition $N_7 \equiv 1 \bmod 7$ n'est vérifiée que pour $N_7 = 1$ ou $N_7 = 8$. Si $N_7 = 1$, l'unique 7-sous-groupe de Sylow est normal donc G n'est pas simple. Supposons maintenant que $N_7 = 8$. Notons $S_1, \ldots, S_8$ les 7-sous-groupes de Sylow de G. Chaque S_i comprend 6 éléments d'ordre 7 plus le neutre d'ordre 1. Comme $S_i \cap S_j = \{e\}$ si $i \neq j$, le groupe G contient donc $8 \times 6 = 48$ éléments d'ordre 7. Il reste alors $56 - 48 = 8$ éléments disponibles et, comme les 2-sous-groupes de Sylow de G sont d'ordre 8, il ne peut exister qu'un seul 2-sous-groupe de Sylow. Il est donc normal, et G n'est pas simple.

Si $|G| = 36 = 3^2 \times 2^2$, on a N_3 qui divise 2^2, donc vaut $1, 2$ ou 4. La condition $N_3 \equiv 1 \bmod 3$ n'est vérifiée que pour $N_3 = 1$ ou $N_3 = 4$. Si $N_3 = 1$, l'unique 3-sous-groupe de Sylow est normal donc G n'est pas simple. Supposons maintenant que $N_3 = 4$. Notons $S_1, \ldots, S_4$ les 3-sous-groupes de Sylow de G. On sait qu'ils sont tous conjugués; notons $\Omega_{S_1} = \{S_1, S_2, S_3, S_4\}$ la classe de conjugaison qu'ils forment. Son cardinal est $|\Omega_{S_1}| = [G : N_1]$ où le stabilisateur N_1 est ici le normalisateur $N_1 = N_G(S_1)$. Ainsi, $[G : N_1] = 4$ et $|G| = 36$ ne divise pas $4! = 24$; on conclut avec le corollaire du 3.2 du chapitre 2 que G n'est pas simple. □

THÉORÈME. *Il n'existe pas de groupes simples non abéliens d'ordre < 60.*

Preuve. Soit G un groupe fini d'ordre $n < 60$.

Si $n = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53$ ou 59, G est d'ordre premier, donc cyclique d'ordre premier, donc abélien simple d'après la proposition 5.

Si $n = 4, 8, 9, 16, 25, 27, 32$ ou 49, le corollaire 6 montre que G n'est pas simple.

Si $n = 6, 10, 14, 15, 21, 22, 26, 33, 34, 35, 38, 39, 46, 51, 55, 57$ ou 58, la proposition 1 montre que G n'est pas simple.

Si $n = 12, 18, 20, 28, 44, 45, 50$ ou 52, la proposition 2 montre que G n'est pas simple.

Si $n = 24$ ou 48, le second cas du lemme 4 montre que G n'est pas simple. Si $n = 54$, le premier cas du lemme 4 montre que G n'est pas simple. Si $n = 30$ ou 42, la proposition 3 montre que G n'est pas simple. Les seuls cas restants sont $n = 36, 40$ ou 56, qui font l'objet de l'exercice 8. □

REMARQUE. Le groupe alterné A_5 est non-abélien, d'ordre 60, et on verra dans le chapitre suivant qu'il est simple.

2.3 D'autres applications.

PROPOSITION. *Tout groupe d'ordre pq avec p et q premiers distincts tels $q \not\equiv 1 \bmod p$ et $p \not\equiv 1 \bmod q$ est cyclique.*

Preuve. On a: N_p divise q, donc $N_p = q$ ou $N_p = 1$, et $N_p \equiv 1 \bmod p$. L'hypothèse $q \not\equiv 1 \bmod p$ implique alors $N_p = 1$; notons S l'unique p-sous-groupe de Sylow de G, qui est donc normal dans G. De même G admet un unique q-sous-groupe de Sylow T, et il est normal dans G. Comme $|S| = p$ et $|T| = q$, il est clair par le théorème de Lagrange que $S \cap T = \{e\}$, donc $|ST| = pq$, et donc $G = ST$ est produit direct de $S \simeq C_p$ et $T \simeq C_q$. On conclut par le théorème chinois que $G \simeq C_{pq}$. □

PROPOSITION. *Tout groupe d'ordre $2p$ avec p premier impair est cyclique ou diédral.*

Preuve. Comme $p > 2$, la preuve de la proposition 1 de 2.2. avec $q = 2$ montre que G admet un unique p-sous-groupe de Sylow. Notons-le S; il est normal dans G et d'ordre p.

Par ailleurs, le nombre N_2 de 2-sous-groupes de Sylow de G divisant p, il ne peut valoir que 1 ou p. Si $N_2 = 1$, l'unique 2-sous-groupe de Sylow T de G est normal dans G, d'ordre 2, et en reprenant la preuve de la proposition précédente, on conclut que $G \simeq C_{2p}$.

Supposons donc maintenant $N_2 = p$. Soit $y \in G$ tel que $y \notin S$. L'ordre de y divise $2p$, ne peut pas valoir 1 (car sinon $y = e \in S$), ne peut pas valoir p (car sinon $\langle y \rangle$ est un sous-groupe d'ordre p, donc égal à S par unicité de S, d'où $y \in S$), et ne pas valoir $2p$ (car sinon $\langle y \rangle$ est un sous-groupe d'ordre $2p$, donc égal à G, d'où $G \simeq C_{2p}$, ce qui contredit $N_2 = p$ puisque C_{2p} admet un unique sous-groupe d'ordre 2). On conclut donc que les p éléments de G qui ne sont pas dans S sont tous d'ordre 2. On conclut que $G \simeq D_p$. □

THÉORÈME. *Tous les groupes d'ordre ≤ 15 sont, à isomorphisme près, donnés dans le tableau suivant:*

ordre du groupe	*groupes abéliens*	*groupes non abéliens*
$n = 1$	groupe trivial $C_1 = \{e\}$	
$n = 2$	groupe cyclique C_2	
$n = 3$	groupe cyclique C_3	
$n = 4$	groupe cyclique C_4 groupe de Klein $C_2 \times C_2$ = groupe diédral D_2	
$n = 5$	groupe cyclique C_5	
$n = 6$	groupe cyclique C_6	groupe symétrique S_3 = groupe diédral D_3
$n = 7$	groupe cyclique C_7	
$n = 8$	groupe cyclique C_8 produit direct $C_2 \times C_4$ produit direct $C_2 \times C_2 \times C_2$	groupe diédral D_4 groupe quaternionique Q_8
$n = 9$	groupe cyclique C_9 produit direct $C_3 \times C_3$	
$n = 10$	groupe cyclique C_{10}	groupe diédral D_5
$n = 11$	groupe cyclique C_{11}	
$n = 12$	groupe cyclique C_{12} produit direct $C_2 \times C_6$	groupe diédral D_6 groupe quaternionique Q_{12} groupe alterné A_4
$n = 13$	groupe cyclique C_{13}	
$n = 14$	groupe cyclique C_{14}	groupe diédral D_7
$n = 15$	groupe cyclique C_{15}	

Preuve. Le fait que tout groupe d'ordre premier soit cyclique, que tout groupe d'ordre p^2 avec p premier soit abélien (voir 2.3 du chapitre 2), et les deux propositions précédentes, permettent de conclure immédiatement dans tous les cas sauf 8 et 12. Ces derniers doivent faire l'objet d'une étude technique détaillée, basée sur l'utilisation fine des théorèmes de Sylow, qui pourra être menée en travaux dirigés. □

2.4 Exercices.

1. LEMME DE FRATTINI. Soient G un groupe, H un sous-groupe fini normal dans G, et S un p-sous-groupe de Sylow de H. Montrer que: $G = HN_G(S)$.
   En déduire que, si G est un groupe fini et si S est un p-sous-groupe de Sylow de G, alors on a pour tout sous-groupe H de G:
   $$N_G(S) \text{ sous-groupe de } H \implies N_G(H) = H.$$

2. Soient G un groupe fini non trivial, p un diviseur premier de $|G|$, et H l'intersection de tous les p-sous-groupes de Sylow de G. Montrer que H est un p-sous-groupe normal dans G. Montrer que tout p-sous-groupe normal de G est un sous-groupe de H.

Chapitre 4

Groupes finis: compléments sur le groupe symétrique

1. Décomposition en cycles disjoints.

1.1 Rappels et notations.

Fixons un entier $n \geq 1$. On note S_n le groupe symétrique des permutations sur un ensemble fini à n éléments, c'est-à-dire à isomorphisme près le groupe des permutations de $\mathbb{N}_n := \{1, 2, \ldots, n\}$.
S_n est un groupe fini, d'ordre $n!$, non abélien dès lors que $n \geq 3$.

On a vu que les transpositions engendrent le groupe S_n, mais d'une part la décomposition d'une permutation en produit de transpositions n'est en général pas unique, et d'autre part les transpositions ne commutent pas entre elles dans une telle décomposition.

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

On va donner dans ce qui suit une décomposition canonique de toute permutation en éléments de type particulier (appelés cycles), qui est unique, avec commutation des facteurs.

1.2 Support.

Définition. Pour tout $\sigma \in S_n$, on appelle support de σ l'ensemble des éléments de $\mathbb{N}_n$ qui ne sont pas fixés par σ:

$$\operatorname{Supp}\sigma = \{i \in \mathbb{N}_n \,;\, \sigma(i) \neq i\}.$$

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

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

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

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

1.3 Orbites

Définition. Pour toute $\sigma \in S_n$, le sous-groupe cyclique $\langle\sigma\rangle$ engendré par σ dans S_n opère sur $\mathbb{N}_n$ par:

$$\begin{array}{ccc}\langle\sigma\rangle \times \mathbb{N}_n & \longrightarrow & \mathbb{N}_n \\ (\sigma^k, i) & \longmapsto & \sigma^k(i)\end{array}.$$

On appelle σ-orbite toute orbite d'un élément de $\mathbb{N}_n$ pour cette action. On note:

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

Remarque. Soit p l'ordre de l'élément σ dans S_n, c'est-à-dire l'ordre du sous-groupe $\langle\sigma\rangle$. Le cardinal d'une orbite divisant l'ordre du groupe, $|\Omega_\sigma(i)|$ divise p, et donc $1 \leq |\Omega_\sigma(i)| \leq p$. En outre:

$$\begin{cases} i \notin \operatorname{Supp}\sigma & \Leftrightarrow \quad \Omega_\sigma(i) = \{i\} \ \text{(orbite ponctuelle)}, \\ i \in \operatorname{Supp}\sigma & \Leftrightarrow \quad 2 \leq |\Omega_\sigma(i)| \leq p. \end{cases}$$

1.4 Cycles.

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: $\Omega_2 = \{2\}$, $\Omega_3 = \{3\}$, $\Omega_1 = \{1,5,4,6\} = \Omega_5 = \Omega_4 = \Omega_6$.

PROPOSITION, DÉFINITION, NOTATION. *Soit $\sigma \in S_n$ un cycle. On note r 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 r de σ.*

(iii) *Il existe $j_1, j_2, \ldots, j_r$ distincts dans $\mathbb{N}_n$ tels que:*

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

On dit que σ est un r-cycle, ou un cycle d'ordre r. On note: $\sigma = [j_1, j_2, \ldots, j_r]$.
On a aussi: $\sigma = [j_k, j_{k+1}, \ldots, j_r, j_1, \ldots, j_{k-1}]$ pour tout $1 < k \leq r$.

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

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

les éléments étant deux à deux distincts. On a alors $\sigma^p(j_1) = j_1$, et ceci étant vrai pour tout représentant j_1 choisi dans $\Omega = \operatorname{Supp}\sigma$, on a $\sigma^p(i) = i$ pour tout $i \in \operatorname{Supp}\sigma$. Mais l'égalité $\sigma^p(i) = i$ est claire si $i \notin \operatorname{Supp}\sigma$ puisqu'alors $\sigma(i) = i$. Ainsi $\sigma^p = e$ dans S_n. L'ordre r de σ dans S_n est donc un diviseur de p. Par ailleurs, dans l'action de $G = \langle\sigma\rangle$ sur $\mathbb{N}_n$, le cardinal de l'orbite $\Omega = \Omega_\sigma(j_1)$ doit diviser l'ordre de G; donc p divise $|G| = r$. On conclut que $p = r$. □

REMARQUES.

1. Le seul 1-cycle est e.
2. Les 2-cycles sont les transpositions $[i, j]$.
3. Le n-cycle $[1, 2, \ldots, n] = \left(\begin{smallmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 2 & 3 & 4 & \cdots & n & 1 \end{smallmatrix}\right)$ s'appelle la permutation circulaire de S_n. Il existe des n-cycles qui ne sont pas la permutation circulaire, par exemple $[1, 3, 4, 2] \in S_4$.
4. L'inverse d'un r-cycle est un r-cycle: $[j_1, j_2, \ldots, j_r]^{-1} = [j_r, j_{r-1}, \ldots, j_1]$.
5. 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.

Le lemme suivant, bien qu'évident, est d'une utilisation fréquente et précieuse dans de nombreuses preuves.

LEMME (CONJUGUÉ D'UN CYCLE). *Pour tout r-cycle $\gamma = [j_1, j_2, \ldots, j_r]$ de S_n et tout $\sigma \in S_n$, le conjugué $\sigma\gamma\sigma^{-1}$ est égal au r-cycle $[\sigma(j_1), \sigma(j_2), \ldots, \sigma(j_r)]$.*

Preuve. Soit $i \in \mathbb{N}_n$. Si $\sigma^{-1}(i) \in \operatorname{Supp}\gamma$, il existe $1 \leq k \leq r$ tel que $i = \sigma(j_k)$. On a $\sigma\gamma\sigma^{-1}(i) = \sigma\gamma(j_k) = \sigma(j_{k+1})$ si $1 \leq k < r$, et $\sigma\gamma\sigma^{-1}(i) = \sigma\gamma(j_r) = \sigma(j_1)$ si $k = r$. 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 r-cycle $[\sigma(j_1), \sigma(j_2), \ldots, \sigma(j_r)]$. □

On peut montrer plus précisément que l'action par conjugaison de S_n sur l'ensembles des r-cycles est transitive (à faire en exercice).

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 $\gamma_k : \mathbb{N}_n \longrightarrow \mathbb{N}_n$ 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, de support égal à Ω_k (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 $j \in \Omega_k$). 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 $j \in \mathbb{N}_n$; 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 $j \notin \Omega_i = \operatorname{Supp}\gamma_i$; 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 $j \notin \operatorname{Supp}\gamma_k$ 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 $\sigma = \gamma'_1\gamma'_2\dots\gamma'_p$ en produit de cycles à supports deux à deux disjoints (donc commutant deux à deux). Pour tout $1 \leq i \leq p$, notons $\Omega'_i = \operatorname{Supp}\gamma'_i$. 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 $\sigma = \gamma'_k\gamma'_1\dots\gamma'_{k-1}\gamma'_{k+1}\dots\gamma'_p$, 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:

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

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 $\sigma = \gamma'_1\gamma'_2\dots\gamma'_p$ 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 $\{\gamma_1, \dots, \gamma_p\} = \{\gamma'_1, \dots, \gamma'_p\}$. □

COROLLAIRE. *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.*

Preuve. En exercice □

1.5 Groupe alterné.

RAPPELS. On a défini la signature d'une permutation $\sigma \in S_n$ comme le signe $\varepsilon(\sigma) = (-1)^m$, où m désigne le nombre de transpositions d'une décomposition quelconque de σ en produit de transpositions (la décomposition en produit de transpositions n'est pas unique, mais la parité du nombre de transpositions est la même dans les différentes décompositions). L'ensemble des permutations de signature 1 (c'est-à-dire des permutations qui se décomposent en un nombre pair de transpositions) est un sous-groupe du groupe S_n appelé groupe alterné, noté A_n. Ce n'est autre que le noyau du morphisme signature $\varepsilon : S_n \to \{-1, 1\}$. En particulier:

$$A_n \lhd S_n \quad \text{et} \quad |A_n| = \tfrac{n!}{2}.$$

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

En effet, si $\gamma = [j_1, j_2, \dots, j_r]$, alors $\gamma = [j_1, j_r][j_1, j_{r-1}]\cdots[j_1, j_2]$. □

REMARQUE. On peut donner de la signature d'autres définitions équivalentes:

EXERCICE. 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.

EXERCICE. Montrer que, pour toute permutation $\sigma \in S_n$, la signature de σ vérifie $\varepsilon(\sigma) = \displaystyle\prod_{1 \leq i < k \leq n} \frac{\sigma(k) - \sigma(i)}{k - i}$.

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

Preuve. On a vu ci-dessus que tout 3-cycle est de signature $(-1)^{3-1} = 1$, donc appartient à A_n. Réciproquement, tout élément de A_n est un produit d'un nombre pair de transpositions, donc A_n est engendré par les produits de deux transpositions. Or un produit de deux transpositions est nécessairement de l'un des deux types suivants (où i, j, k, l sont distincts deux à deux): $[i, j][i, k] = [i, k, j]$, ou bien $[i, j][k, l] = [i, l, k][i, j, k]$. Donc tout élément de A_n est un produit de 3-cycles. □

REMARQUE. On peut donner des ensembles de générateurs plus restreints de A_n:

EXERCICE. Soit $n \geq 4$. Montrer que A_n est engendré par l'ensemble des 3-cycles de la forme $[1, i, j]$, où $2 \leq i \neq j \leq n$. Montrer que A_n est engendré par l'ensemble des 3-cycles de la forme $[1, 2, j]$, où $3 \leq j \leq n$.

2. Simplicité de A_n pour $n \geq 5$.

2.1 Introduction.

On a $A_1 = A_2 = \{e\}$. Le groupe A_3 est d'ordre 3, donc est cyclique d'ordre premier, donc simple. Le groupe A_4 n'est pas simple car contient le sous-groupe normal V isomorphe au groupe de Klein vu au chapitre 1. Le théorème suivant est fondamental pour la théorie des corps, en raison d'une de ses conséquences que l'on démontrera dans la partie 3 de ce chapitre.

2.2 Le résultat principal.

Théorème. *Le groupe alterné A_n est simple pour $n \geq 5$.*

Preuve. On divise la démonstration en plusieurs étapes.

(1) Remarque préliminaire: quel que soit un 3-cycle $[i,j,k] \in A_n$, il existe $\sigma \in A_n$ tel que $\sigma[1,2,3]\sigma^{-1} = [i,j,k]$. Par conséquent, deux 3-cycles quelconques sont toujours conjugués dans A_n.

En effet: donnons-nous dans $\mathbb{N}_n$ cinq éléments deux à deux distincts i,j,k,ℓ,m et considérons dans S_n les permutations:

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \dots & n \\ i & j & k & l & m & \dots & ? \end{pmatrix} \quad \text{et} \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \dots & n \\ i & j & k & m & l & \dots & ? \end{pmatrix} = [l,m]\sigma_1.$$

On a: $\sigma_1[1,2,3]\sigma_1^{-1} = [i,j,k] = \sigma_2[1,2,3]\sigma_2^{-1}$, et comme $\sigma_2 = [\ell,m]\sigma_1$, l'une des deux permutations σ_1 et σ_2 est dans A_n.

(2) Soit H un sous-groupe non trivial de A_n, normal dans A_n. Si H contient un 3-cycle, alors $H = A_n$.

En effet: si γ_0 est un 3-cycle dans H, tout 3-cycle de S_n (qui appartient à A_n) est d'après (1) de la forme $\sigma\gamma_0\sigma^{-1}$ pour un $\sigma \in A_n$. Comme H est normal dans A_n, on déduit que H contient tous les 3-cycles, d'où $H = A_n$ d'après la proposition de 1.5.

(3) Fixons un sous-groupe non trivial H de A_n, normal dans A_n, et montrons que H contient un 3-cycle.

Partons de $\mu \in H, \mu \neq e$. Il existe $i \in \mathbb{N}_n$ tel que $\mu(i) \neq i$. Notons $j = \mu(i)$. Comme $n \geq 5$, il est clair qu'on peut choisir $k \in \mathbb{N}_n$ distinct de i et de j tel que $\mu(k) \neq i$. Notons $\ell = \mu(k)$. En résumé i,j,k sont deux à deux distincts, et donc $\mu(i) = j, \mu(j), \mu(k) = \ell$ sont deux à deux distincts. (En revanche, rien n'empêche a priori que $\mu(j) = i$ ou $\mu(j) = k$).

On peut donc considérer le 3-cycle $\gamma = [i,j,k] \in A_n$. D'après le lemme de conjugaison de 1.4, on a: $\mu\gamma\mu^{-1} = [\mu(i),\mu(j),\mu(k)] = [j,\mu(j),\ell]$. Rappelons également que $\gamma^{-1} = [i,k,j]$.

Notons $\sigma = \gamma^{-1}\mu\gamma\mu^{-1} = [i,k,j][j,\mu(j),\ell]$. Remarquons que cette écriture n'est pas la décomposition canonique de σ, car les deux 3-cycles qui interviennent ne sont pas disjoints.

On a $\sigma \in H$ (car d'une part $\gamma^{-1}\mu\gamma \in H$ puisque $\mu \in H$ et H normal dans A_n, et d'autre part $\mu^{-1} \in H$).

On a $\sigma \neq e$ (car sinon $[j,\mu(j),\ell] = \gamma = [i,j,k] = [j,k,i]$, d'où $i = \ell$, ce qui est contraire aux données).

Par définition de σ, σ permute au plus 5 éléments (en d'autres termes, $|\operatorname{Supp}\sigma| \leq 5$). La décomposition canonique de σ en produit de cycles disjoints ne peut donc être que de l'une des formes suivantes: un 5-cycle, un 4-cycle, un 3-cycle, une transposition, le produit d'un 3-cycle par une transposition disjointe, le produit de deux transpositions disjointes. Mais comme σ doit être paire, seuls les trois cas suivants sont à retenir:

• si σ est un 3-cycle, c'est fini, on a montré que H contient un 3-cycle.

• si σ est un 5-cycle, notons $\sigma = [x,y,z,s,t]$; introduisons $\nu = [x,y,z]$; on calcule en utilisant le lemme de conjugaison de 1.4: $\nu^{-1}\sigma\nu\sigma^{-1} = [x,y,z]^{-1}[\sigma(x),\sigma(y),\sigma(z)] = [x,z,y][y,z,s] = [x,z,s]$. Comme H normal dans A_n, $\nu \in A_n$ et $\sigma \in H$, on a $\nu^{-1}\sigma\nu \in H$ et finalement $\nu^{-1}\sigma\nu\sigma^{-1} \in H$. Donc H contient un 3-cycle.

• si σ est le produit de deux transpositions disjointes, notons $\sigma = [x,y][z,s]$; posons $\nu = [x,y,t]$ où t est un élément quelconque de $\mathbb{N}_n$ choisi distinct de x,y,z,s (ce qui est possible parce que $n \geq 5$). Alors $\nu^{-1}\sigma\nu\sigma^{-1} = [x,y,t]^{-1}[\sigma(x),\sigma(y),\sigma(t)] = [x,t,y][y,x,t] = [x,y,t]$. On conclut comme dans le cas précédent que H contient un 3-cycle.

Bilan: si H est un sous-groupe non trivial de A_n normal dans A_n, il contient un 3-cycle d'après (3), donc $H = A_n$ d'après (2). On conclut que A_n est un groupe simple. □

3. Une approche directe des questions de résolubilité.

3.1 Rappels et notations. Pour tout $n \in \mathbb{N}$, on connaît comme sous-groupe normal de S_n, distinct de $\{e\}$ et S_n, le groupe alterné A_n. De plus, dans le cas particulier où $n = 4$, le groupe A_4 contient le sous-groupe $V = \{e, a, b, c\}$ avec: $a = [1,2][3,4]$, $b = [1,3][2,4]$ et $c = [1,4][2,3]$. Il vérifie: $V \lhd S_4$.

Rappelons-en la preuve: d'après le lemme de conjugaison de 1.4, on a pour tout $\sigma \in S_4$:

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

On montre de même que $\sigma b \sigma^{-1} \in V$ et $\sigma c \sigma^{-1} \in V$ pour tout $\sigma \in S_4$. □

Le groupe quotient S_4/V est d'ordre 6 (car $|S_4| = 24$ et $|V| = 4$). Il n'est pas abélien (et donc $S_4/V \simeq S_3$).

En effet, si l'on prend par exemple $\tau = [1,2]$ et $\sigma = [1,3]$, on a $\tau\sigma\tau^{-1}\sigma^{-1} = [1,2,3] \notin V$, de sorte que $\overline{\tau}\,\overline{\sigma} \neq \overline{\sigma}\,\overline{\tau}$ dans S_4/V. □

Le but du théorème suivant est de montrer qu'il s'agit des seuls sous-groupes normaux de S_n.

3.2 Sous-groupes normaux de S_n.

Théorème. *Soit n un entier ≥ 2.*

(i) *Si $n \neq 4$, les seuls sous-groupes normaux de S_n sont $\{e\}$, A_n et S_n.*

(ii) *Si $n = 4$, les seuls sous-groupes normaux de S_4 sont $\{e\}$, V, A_4 et S_4.*

Preuve. Soit G un sous-groupe de S_n normal dans S_n. On divise la démonstration en plusieurs étapes.

(1) Si G contient une transposition, alors ils les contient toutes, et $G = S_n$.

Soit $[i,j]$ une transposition appartenant à G. Soit $[k,\ell]$ une transposition quelconque. On peut toujours trouver $\varphi \in S_n$ telle que $\varphi(i) = k$ et $\varphi(j) = \ell$. D'après le lemme de conjugaison de 1.4, on calcule alors $\varphi[i,j]\varphi^{-1} = [\varphi(i),\varphi(j)] = [k,\ell]$. Comme $[i,j] \in G$ et $G \lhd S_n$, on en déduit que $[k,\ell] \in G$. Ceci prouve que G contient toutes les transpositions, et comme les transpositions engendrent S_n, on conclut que $G = S_n$.

(2) Si G contient un 3-cycle, alors il les contient tous, et $G = S_n$ ou $G = A_n$.

Soit $[i,j,k]$ un 3-cycle appartenant à G. Soit $\gamma = [i',j',k']$ un 3-cycle quelconque. On peut toujours trouver $\varphi \in S_n$ telle que $\varphi(i) = i'$, $\varphi(j) = j'$ et $\varphi(k) = k'$. D'après le lemme de conjugaison de 1.4, on calcule alors $\varphi[i,j,k]\varphi^{-1} = [\varphi(i),\varphi(j),\varphi(k)] = \gamma$. Comme $[i,j,k] \in G$ et $G \lhd S_n$, on en déduit que $\gamma \in G$. Ceci prouve que G contient tous les 3-cycles, et comme les 3-cycles engendrent A_n, on conclut que $A_n \subseteq G \subseteq S_n$. Ainsi $|S_n|/|G| \leq |S_n|/|A_n| = 2$, d'où $G = S_n$ ou $G = A_n$.

(3) Si G contient un cycle, alors il les contient tous, et $G = S_n$ ou $G = A_n$.

Soit $\gamma = [j_1, j_2, \ldots, j_r]$ un r-cycle appartenant à G. Si $r = 2$, alors $G = S_n$ d'après (1). Si $r = 3$, alors $G = S_n$ ou $G = A_n$ d'après (2). On suppose donc maintenant que $r \geq 4$. Considérons le 3-cycle $\omega = [j_1, j_2, j_3]$ et formons le commutateur $\beta := \omega\gamma\omega^{-1}\gamma^{-1}$. Parce que $\gamma \in G$ et $G \lhd S_n$, on a $\alpha := \omega\gamma\omega^{-1} \in G$, et donc $\beta = \alpha\gamma^{-1} \in G$ comme produit de deux éléments de G. Par ailleurs, on calcule avec le lemme de conjugaison de 1.4:

$$\gamma\omega^{-1}\gamma^{-1} = \gamma[j_3,j_2,j_1]\gamma^{-1} = [\gamma(j_3),\gamma(j_2),\gamma(j_1)] = [j_4,j_3,j_2],$$

d'où l'on tire que $\beta = [j_1,j_2,j_3][j_4,j_3,j_2] = [j_1,j_2,j_4]$, qui est donc un 3-cycle. On conclut que G contient un 3-cycle, et on applique alors (2).

(4) Si G contient le produit de deux transpositions à supports disjoints, alors $G = S_n$ ou $G = A_n$ lorsque $n \geq 5$, et $G = S_4, A_4$ ou V lorsque $n = 4$.

Soit $\sigma = [i,j][k,\ell]$ un produit de transpositions appartenant à G et tel que i,j,k,ℓ sont deux à deux distincts. Supposons $n \geq 5$. On peut alors considérer un entier $m \in \mathbb{N}_n$ distincts de i,j,k,ℓ. Notons $\nu = [i,j,m]$. En utilisant le lemme de conjugaison de 1.4, on calcule:

$$\nu^{-1}\sigma\nu\sigma^{-1} = [i,j,m]^{-1}[\sigma(i),\sigma(j),\sigma(m)] = [m,j,i][j,i,m] = [i,j,m] = \nu.$$

Or $\lambda := \nu^{-1}\sigma\nu \in G$ car $\sigma \in G$ et $G \lhd S_n$, d'où $\nu = \lambda\sigma^{-1} \in G$. On applique alors (2) pour conclure que $G = S_n$ ou A_n.

Supposons maintenant que $n = 4$. Quels que soient $x,y,z,t \in \mathbb{N}_4$ deux à deux distincts, il existe $\varphi \in S_4$ tel que $\varphi(i) = x$, $\varphi(j) = y$, $\varphi(k) = z$ et $\varphi(\ell) = t$. En utilisant le lemme de conjugaison de 1.4, on calcule:

$$\varphi\sigma\varphi - 1 = \varphi[i,j]\varphi^{-1}\varphi[k,\ell]\varphi^{-1} = [\varphi(i),\varphi(j)][\varphi(k),\varphi(\ell)] = [x,y][z,t].$$

Or $\varphi\sigma\varphi^{-1} \in G$ puisque $\sigma \in G$ et $G \lhd S_4$. On a ainsi prouvé que G contient tous les produits de deux transpositions à supports disjoints; mais dans S_4 il n'y en a que trois, que l'on a noté a,b,c, et qui avec e forment le sous-groupe V. Donc $V \subseteq G$. Si $G \not\subset V$, alors G contient nécessairement un cycle (car tous les éléments de S_4 sont des cycles à part a,b,c), et l'on applique (3) pour conclure que $G = S_4$ ou A_4. Si $G \subseteq V$, alors $G = V$.

(5) On achève alors la preuve de la façon suivante. Supposons $G \neq \{e\}$. Soit $\varphi \in G$ tel que $\varphi \neq e$. Si φ est un cycle, c'est fini d'après l'étape (3). Sinon, la décomposition canonique de φ en produit de cycles disjoints contient au moins deux cycles disjoints σ_1 et σ_2. Fixons $i \in \operatorname{Supp}\sigma_1$ et $j \in \operatorname{Supp}\sigma_2$. Ils vérifient $i \neq j$ puisque σ_1 et σ_2 sont disjoints. On a $\varphi(i) = \sigma_1(i)$, et donc $\varphi(i) \neq i$ (car $\sigma_1(i) \neq i$). On a aussi $\varphi(i) \neq j$ (car on aurait sinon $\sigma_1(i) = \varphi(i) = j = \sigma_1(j)$, ce qui contredirait $i \neq j$). Ainsi les trois éléments $i, j, \varphi(i)$ sont deux à deux distincts, ce qui permet de considérer le 3-cycle $\gamma = [i, \varphi(i), j]$. Formons le commutateur $\theta = \gamma\varphi\gamma^{-1}\varphi^{-1}$. Il appartient à G comme produit de $\gamma\varphi\gamma^{-1} \in G$ (car $\varphi \in G$ et $G \lhd S_n$) par $\varphi^{-1} \in G$. En utilisant le lemme de conjugaison de 1.4, on peut préciser le calcul de θ:

$$\theta = [i, \varphi(i), j]\varphi[i, \varphi(i), j]^{-1}\varphi^{-1} = [i, \varphi(i), j]\varphi[j, \varphi(i), i]\varphi^{-1} = [i, \varphi(i), j][\varphi(j), \varphi^2(i), \varphi(i)].$$

Si $\varphi^2(i) \neq i$, alors les cinq éléments $i, \varphi(i), \varphi^2(i), j, \varphi(j)$ sont deux à deux distincts, et on calcule $\theta = [i, \varphi(i), j][\varphi(j), \varphi^2(i), \varphi(i)] = [i, \varphi(i), \varphi(j), \varphi^2(i), j]$ qui est un 5-cycle. Ainsi G contient un cycle; on applique (3) pour conclure.

Si $\varphi^2(i) = i$, on calcule $\theta = [i, \varphi(i), j][\varphi(j), i, \varphi(i)] = [i, j][\varphi(i), \varphi(j)]$. Ainsi G contient un produit de deux transpositions à supports disjoints; on applique (4) pour conclure. □

Exercice (centre et groupe dérivé). Montrer que:

(i) Pour tout $n \geq 3$, le centre de S_n est $\{e\}$ et le groupe dérivé de S_n est A_n.

(ii) Pour tout $n \geq 5$, le centre de A_n est $\{e\}$ et le groupe dérivé de A_n est A_n.

(iii) Pour $n = 4$, le centre de A_4 est $\{e\}$ et le groupe dérivé de A_4 est V.

3.3 Suites normales.

Grâce au théorème de 3.2, on peut expliciter toutes les suites normales de S_n, c'est-à-dire les suites strictement décroissantes de sous-groupes normaux de S_n commençant à S_n et finissant à $\{e\}$.

	suites normales	*groupes quotients*
$n = 1$	$S_1 = \{e\}$	
$n = 2$	$S_2 \supset \{e\} = A_2$	$S_2/\{e\} \simeq C_2$ abélien
$n = 3$	$S_3 \supset \{e\}$	$S_3/\{e\} \simeq S_3$ non abélien
	$S_3 \supset A_3 \supset \{e\}$	$S_3/A_3 \simeq C_2$ abélien, et $A_3/\{e\} \simeq C_3$ abélien
$n = 4$	$S_4 \supset \{e\}$	$S_4/\{e\} \simeq S_4$ non abélien
	$S_4 \supset A_4 \supset \{e\}$	$S_4/A_4 \simeq C_2$ abélien, et $A_4/\{e\} \simeq A_4$ non abélien
	$S_4 \supset V \supset \{e\}$	$S_4/V \simeq S_3$ non abélien, et $V/\{e\} \simeq V$ abélien
	$S_4 \supset A_4 \supset V \supset \{e\}$	$S_4/A_4 \simeq C_2$ abélien, et $A_4/V \simeq C_3$ abélien, et $V/\{e\} \simeq V$ abélien
$n \geq 5$	$S_n \supset \{e\}$	$S_n/\{e\} \simeq S_n$ non abélien
	$S_n \supset A_n \supset \{e\}$	$S_n/A_n \simeq C_2$ abélien, et $A_n/\{e\} \simeq A_n$ non abélien

En résumé:

(i) si $n \leq 4$, il existe une suite normale de S_n telles que tous les quotients de deux termes successifs soient abéliens,

(ii) si $n \geq 5$, il n'existe pas de telles suites.

On traduit cette propriété en disant que S_n est résoluble si $n \leq 4$, et non résoluble si $n \geq 5$. Cette propriété importante, liée à la résolubilité des équations par radicaux (voir cours ultérieur de théorie des corps) sera étudiée en détail au chapitre suivant.

Chapitre 5

Groupes résolubles

1. Suites normales et groupes résolubles.

1.1 Groupes dérivés successifs.

Rappel. Soient G un groupe et $D(G)$ son groupe dérivé. On a:

- $D(G) \lhd G$ et $G/D(G)$ abélien,
- pour tout $N \lhd G$, (G/N abélien $\Leftrightarrow$ $D(G) \subseteq N$).

Notation. Soit G un groupe; on pose: $D_0(G) = G$, $D_1(G) = D(G)$ le groupe dérivé de G, $D_2(G) = D(D_1(G)$ le groupe dérivé de $D_1(G)$, et par récurrence:

$$D_{i+1}(G) = D(D_i(G)) \text{ le groupe dérivé de } D_i(G), \text{ pour tout } i \in \mathbb{N}.$$

Proposition. *Pour tout $i \in \mathbb{N}$, on a: $D_{i+1}(G) \lhd D_i(G)$, et $D_i(G)/D_{i+1}(G)$ est abélien,*

Preuve. Résulte immédiatement du rappel ci-dessus. □

On considère la suite des groupes dérivés successifs $(D_i(G))_{i\in\mathbb{N}}$, que l'on note aussi:

$$D_0(G) = G \rhd D_1(G) = D(G) \rhd D_2(G) \rhd D_3(G) \rhd \cdots \rhd D_i(G) \rhd D_{i+1}(G) \rhd \cdots.$$

Théorème. *Pour tout $i \in \mathbb{N}$, on a: $D_i(G) \lhd G$.*

Preuve. Montrons d'abord que l'image de $D(G)$ par tout automorphisme de G est égal à $D(G)$. Soit $\alpha \in \operatorname{Aut} G$. Pour tous $x, y \in G$, on a $\alpha(xyx^{-1}y^{-1}) = \alpha(x)\alpha(y)\alpha(x)^{-1}\alpha(y)^{-1} \in D(G)$. Comme $D(G)$ est engendré par les commutateurs, on déduit que $\alpha(D(G)) \subseteq D(G)$. En considérant l'automorphisme α^{-1}, on obtient de même $\alpha^{-1}(D(G)) \subseteq D(G)$, donc $D(G) \subseteq \alpha(D(G))$, et finalement $\alpha(D(G)) = D(G)$.

Montrons maintenant que $\alpha(D_i(G)) = D_i(G)$ pour tout $\alpha \in \operatorname{Aut} G$ et tout $i \in \mathbb{N}$. La propriété est vraie pour $i = 1$ d'après la première étape. Par récurrence, supposons-la vraie jusqu'à un rang $i \geq 1$. Soit $\alpha \in \operatorname{Aut} G$. Par hypothèse de récurrence, $\alpha(D_i(G)) = D_i(G)$, donc la restriction de α à $D_i(G)$ détermine un automorphisme α' de $D_i(G)$. En appliquant la première étape au groupe $D_i(G)$ et à $\alpha' \in \operatorname{Aut} D_i(G)$, on a: $\alpha'(D(D_i(G)) = D(D_i(G))$. Mais $D_{i+1}(G) = D(D_i(G))$, de sorte que cette dernière égalité s'écrit encore $\alpha(D_{i+1}(G)) = D_{i+1}(G)$. Ce qui montre la propriété voulue au rang $i + 1$.

Dès lors, soient $x \in G$ quelconque et $i \in \mathbb{N}$. D'après la seconde étape ci-dessus, l'automorphisme intérieur $\alpha : g \mapsto xgx^{-1}$ vérifie $\alpha(D_i(G)) = D_i(G)$, donc $xD_i(G)x^{-1} = D_i(G)$, ce qui prouve que $D_i(G) \lhd G$. □

Remarquons que la preuve du théorème montre une propriété plus forte que la normalité des sous-groupes $D_i(G)$, à savoir qu'ils sont stables par tout automorphisme de G, propriété que l'on traduit en disant que ce sont des sous-groupes caractéristiques de G.

1.2 Notion de groupe résoluble.

Définition. Un groupe G est dit *résoluble* s'il existe un rang $n \in \mathbb{N}$ à partir duquel on a $D_n(G) = \{e\}$.

Remarque. Cela signifie donc que la suite des groupes dérivés successifs est stationnaire:

$$G = D_0(G) \rhd D_1(G) \rhd D_2(G) \rhd D_3(G) \rhd \cdots \rhd D_n(G) = \{e\}.$$

Proposition. *Si G est un groupe résoluble, tout sous-groupe de G et tout quotient de G est résoluble.*

Preuve. Soit G un groupe résoluble. Soit $n \in \mathbb{N}$ tel que $D_n(G) = \{e\}$. Considérons un sous-groupe H de G; il est clair que $D(H)$ est un sous-groupe de $D(G)$ et donc, par une récurrence évidente, que $D_i(H)$ est un sous-groupe de $D_i(G)$ pour tout $i \in \mathbb{N}$. En particulier pour $i = n$, on a $D_n(H)$ sous-groupe de $D_n(G) = \{e\}$, donc $D_n(H) = \{e\}$, ce qui prouve que H est résoluble.

Considérons $N \lhd G$ et le groupe quotient G/N. Notons π la surjection canonique $G \to G/N$. Pour tout sous-groupe H de G, un commutateur quelconque du groupe $\pi(H)$ est de la forme:

$$\pi(x)\pi(y)\pi(x)^{-1}\pi(y)^{-1} = \pi(xyx^{-1}y^{-1}), \text{ avec } x, y \in H,$$

d'où il résulte que $D(\pi(H)) = \pi(D(H))$. On en déduit que $D(\pi(G)) = D(G/N) = \pi(D(G))$, puis $D_2(G/N) = D(\pi(D(G))) = \pi(D_2(G))$, et par une réurrence évidente, $D_i(G/N) = \pi(D_i(G))$ pour tout $i \in \mathbb{N}$. En particulier pour $i = n$, on a $D_n(G/N) = \pi(D_n(G)) = \pi(\{e\}) = \{\pi(e)\}$, ce qui prouve que G/N est résoluble. □

1.3 Caractérisation de la résolubilité par les suites de compositions et les suites normales.

DÉFINITIONS. Soit G un groupe.

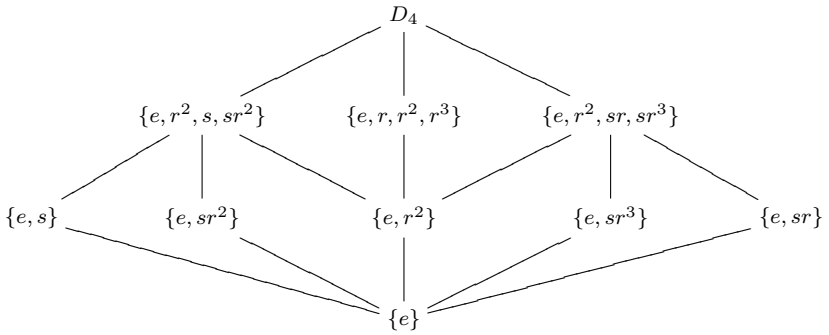
1. On appelle *suite de composition* de G toute chaîne finie de sous-groupes
$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_i \rhd G_{i+1} \rhd \cdots \rhd G_n = \{e\},$$
où $G_i \rhd G_{i+1}$ signifie que G_{i+1} est un sous-groupe de G_i normal dans G_i. Les groupes G_i/G_{i+1} sont appelés les *quotients* de la suite, et le nombre n de quotients est appelé la *longueur* de la suite.
2. On dit que la suite est strictement décroissante lorsque $G_i \neq G_{i+1}$ pour tout $0 \leq i \leq n-1$.
3. On dit que la suite est normale lorsque $G_i \lhd G$ pour tout $0 \leq i \leq n-1$.

Attention ! Certains auteurs appellent suite normale ce que nous appelons suite de composition, suite de composition ce que nous appelerons suite de Jordan-Hölder, ou encore suite de composition ce que nous appelons suite de composition strictement décroissante.

EXEMPLE 1. Considérons le groupe symétrique S_4, le sous-groupe alterné A_4, leur sous-groupe $V = \{e, a, b, c\}$ où $a = [1,2][3,4]$, $b = [1,3][2,4]$, $c = [1,4][2,3]$, et le sous-groupe $H = \{e, a\}$. D'après les résultats vus au chapitre 1:

- $S_4 \rhd A_4 \rhd V \rhd \{e\}$ est une suite normale,
- $S_4 \rhd A_4 \rhd V \rhd H \rhd \{e\}$ est une suite de composition, mais pas une suite normale, car H n'est pas normal dans S_4.

EXEMPLE 2. Considérons le groupe diédral $D_4 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$, avec $r^4 = s^2 = e$ et $rs = sr^3$. Les sous-groupes de D_4 sont:



Tout chemin à 4 sommets de D_4 à $\{e\}$ dans ce diagramme est une suite de composition.

- $D_4 \rhd \{e, r^2, s, sr^2\} \rhd \{e, r^2\} \rhd \{e\}$ est une suite normale, (car de plus $\{e, r^2\} \lhd D_4$),
- $D_4 \rhd \{e, r^2, sr, sr^3\} \rhd \{e, sr^3\} \rhd \{e\}$ n'est pas une suite normale, (car $s(sr^3)s^{-1} = r^3 s = sr \notin \{e, sr^3\}$, de sorte que $\{e, sr^3\}$ n'est pas normal dans D_4).

THÉORÈME. *Soit G un groupe. Les propriétés suivantes sont équivalentes:*

(i) *G est résoluble;*

(ii) *G admet une suite normale dont tous les quotients sont abéliens;*

(iii) *G admet une suite de composition dont tous les quotients sont abéliens.*

Preuve. Supposons G résoluble, et considérons la suite (finie) des groupes dérivés successifs:
$$G = D_0(G) \rhd D_1(G) \rhd D_2(G) \rhd D_3(G) \rhd \cdots \rhd D_n(G) = \{e\}.$$
Elle est normale d'après le théorème de 1.1, et tous ses quotients sont abéliens d'après la proposition de 1.1. Ceci prouve que (i) implique (ii). Il est trivial que (ii) implique (iii). Supposons maintenant que G vérifie (iii). On considère donc une suite de composition:
$$G = H_0 \rhd H_1 \rhd H_2 \rhd \cdots \rhd H_i \rhd H_{i+1} \rhd \cdots \rhd H_m = \{e\},$$
telle que H_i/H_{i+1} abélien pour tout $0 \leq i \leq m-1$. Quitte à supprimer certains H_i, on peut sans restriction supposer que les H_i sont deux à deux distincts, c'est-à-dire que la suite de composition est strictement décroissante. Pour $i = 0$, l'abélianité de $H_0/H_1 = G/H_1$ implique que $D(G) \subset H_1$ (voir le rappel au début de ce chapitre). De plus, $D(G) \subset H_1$ implique $D(D(G)) = D_2(G) \subset D(H_1)$, et comme l'abélianité de H_1/H_2 implique que $D(H_1) \subseteq H_2$, on déduit que $D_2(G) \subseteq H_2$. Une récurrence évidente permet ainsi de vérifier que $D_{i+1}(G) \subseteq H_{i+1}$ pour tout $0 \leq i \leq m-1$. En particulier $D_m(G) \subseteq H_m = \{e\}$, ce qui montre que G est résoluble. □

1.4 Exemples de groupes résolubles.

PROPOSITION 1. *Tout groupe abélien est résoluble.*

Preuve. Evident puisqu'alors $D(G) = \{e\}$. □

PROPOSITION 2. *Les seuls groupes simples résolubles sont les groupes cycliques d'ordre premier.*

Preuve. Si G est simple, sa seule suite de composition est $G \rhd \{e\}$. Si de plus G est résoluble, le théorème de 1.3 implique que l'unique quotient $G/\{e\}$ de cette suite est abélien, c'est-à-dire que G est abélien. D'où le résultat d'après la proposition 5 du 2.2 du chapitre 3. □

PROPOSITION 3. *Pour tout $n \geq 2$, le groupe diédral D_n est résoluble.*

Preuve. Considérons dans le groupe diédral $D_n = \{e, r, r^2, r^3, \ldots, r^{n-1}, s, sr, sr^2, sr^3, \ldots, sr^{n-1}\}$ le sous-groupe $C_n = \{e, r, r^2, r^3, \ldots, r^{n-1}\}$. On a la suite normale $D_n \rhd C_n \rhd \{e\}$ avec $G/C_n \simeq C_2$ abélien, et $C_n/\{e\} \simeq C_n$ abélien, donc D_n est résoluble d'après le théorème 1.3. □

PROPOSITION 4. *Pour $n \geq 5$, le groupe symétrique S_n et le groupe alterné A_n ne sont pas résolubles.*

Preuve. Soit $n \geq 5$. Si S_n était résoluble, A_n le serait d'après la proposition 1.2. Or on a vu au chapitre 4 (théorème 2.2) que A_n est simple. D'après la proposition ci-dessus, A_n serait cyclique d'ordre premier, ce qui est évidemment faux. □

REMARQUE. La non résolubilité des S_n pour $n \geq 5$ a des conséquences fondamentales en théorie des corps. On l'avait déjà montrée par une preuve directe à la fin du chapitre 4. Rappelons que S_2, S_3 et S_4 sont résolubles.

THÉORÈME. *Pour tout nombre premier p, tout p-groupe est résoluble.*

Preuve. Soit G fini d'ordre p^n, avec $n \in \mathbb{N}^*$. Si G est abélien, il est résoluble. Supposons donc G non abélien. Notons $C_1 = Z(G)$ son centre. On sait qu'il est normal dans G (voir 2.4 du chapitre 1), strictement inclus dans G (puisque G non abélien), et distinct de $\{e\}$ (d'après la proposition 2.3 du chapitre 2). On a donc une suite normale strictement décroissante: $G \rhd C_1 \rhd \{e\}$.

Le groupe quotient G/C_1 est un p-groupe (évident); son centre $Z(G/C_1)$ est normal dans G/C_1, donc de la forme C_2/C_1 pour un certain sous-groupe C_2 de G contenant C_1 (voir chapitre 1, résultat 5 de 2.4), qui vérifie $C_1 \lhd C_2$ (puisque plus généralement $C_1 \lhd G$), et tel que $C_2 \lhd G$ (car $C_2/C_1 \lhd G/C_1$). On a $C_1 \neq C_2$, car sinon $Z(G/C_1) = C_2/C_1$ serait trivial, ce qui est exclu puisque G/C_1 est un p-groupe.

- OU $G = C_2$. Alors $G/C_1 = Z(G/C_1)$, donc G/C_1 est abélien. On a donc construit une suite normale $G \rhd C_1 \rhd \{e\}$ dont tous les quotients sont abéliens. On conclut que G est résoluble.
- OU $G \neq C_2$. On a donc une suite normale strictement décroissante: $G \rhd C_2 \rhd C_1 \rhd \{e\}$. Le groupe G/C_2 est un p-groupe non trivial. Son centre $Z(G/C_2)$ est normal dans G/C_2, donc de la forme C_3/C_2 pour un certain sous-groupe C_3 de G contenant C_2 (voir chapitre 1, résultat 5 de 2.4), qui vérifie $C_2 \lhd C_3$ (puisque plus généralement $C_2 \lhd G$), et tel que $C_3 \lhd G$ (car $C_3/C_2 \lhd G/C_2$). On a $C_2 \neq C_3$, car sinon $Z(G/C_2) = C_3/C_2$ serait trivial, ce qui est exclu puisque G/C_2 est un p-groupe.
  - OU $G = C_3$. Alors $G/C_2 = Z(G/C_2)$, donc G/C_2 est abélien. On a donc construit une suite normale $G \rhd C_2 \rhd C_1 \rhd \{e\}$ dont tous les quotients sont abéliens. On conclut que G est résoluble.
  - OU $G \neq C_3$. On réitère le raisonnement en considérant $Z(G/C_3) = C_4/C_3$.

On construit ainsi de proche en proche une suite croissante (C_i) de sous-groupes normaux de G telle que $C_1 = Z(G)$ et $C_{i+1}/C_i = Z(G/C_i)$ pour tout $i \geq 1$. Comme G est fini, le processus s'arrête, c'est-à-dire qu'il existe un plus petit entier k tel que $C_k = G$. On a alors obtenu la suite normale strictement décroissante: $G = C_k \rhd C_{k-1} \rhd \cdots \rhd C_2 \rhd C_1 \rhd \{e\}$, dont tous les quotients sont abéliens, et on conclut que G est résoluble. □

EXERCICE. Montrer que tout groupe fini d'ordre pq ou p^2q, avec p, q premiers distincts, est résoluble.

Indication: utiliser le fait, vu au 2.2 du chapitre 3, qu'il n'y a pour un tel groupe qu'un seul p-sous-groupe de Sylow ou qu'un seul q-sous-groupe de Sylow.

Ce résultat simple est un cas particulier d'un théorème beaucoup plus profond de W. Burnside, selon lequel tout groupe fini dont l'ordre n'admet que deux diviseurs premiers est résoluble.

1.5 Quelques compléments sur la notion de groupes résolubles.

THÉORÈME. *Un groupe G est résoluble si et seulement s'il admet un sous-groupe normal N tel que N et G/N soient résolubles.*

Preuve. Supposons G résoluble. Le groupe dérivé $N = D(G)$ est normal dans G et distinct de G (car sinon $D_i(G) = G$ pour tout $i \in \mathbb{N}^*$, ce qui contredirait la résolubilité). D'après la proposition 1.2, N et G/N sont résolubles.

Supposons réciproquement qu'il existe un sous-groupe normal propre N de G tel que N et G/N soient résolubles. D'après le théorème 1.3, il existe deux suites de composition:

$$N = K_0 \rhd K_1 \rhd \cdots \rhd K_r = \{e\} \qquad \text{et} \qquad G/N = T_0 \rhd T_1 \rhd \cdots \rhd T_s = \{\overline{e}\},$$

avec K_i/K_{i+1} abélien pour tout $0 \leq i \leq r-1$, et T_i/T_{i+1} abélien pour tout $0 \leq i \leq s-1$.

Chaque T_i étant un sous-groupe de G/N, il est de la forme $T_i = G_i/N$ pour un certain sous-groupe G_i de G contenant N (voir 2.4 du chapitre 1). Comme $T_{i+1} \lhd T_i$, on a $G_{i+1} \lhd G_i$, et par application du troisième théorème d'isomorphisme: G_i/G_{i+1} est isomorphe à T_i/T_{i+1}, donc abélien. En outre, pour $i = s$, le fait que $T_s = \{\overline{e}\}$ implique $G_s = N$. On peut alors considérer la suite de composition:

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_{s-1} \rhd G_s = N = K_0 \rhd K_1 \rhd \cdots \rhd K_r = \{e\},$$

dont tous les quotients sont abéliens. Donc G est résoluble. □

COROLLAIRE. *Soient G un groupe, H et K deux sous-groupes normaux et résolubles de G. Alors HK est un sous-groupe normal et résoluble de G.*

Preuve. Il est clair que HK est un sous-groupe normal de G. Par application du second théorème d'isomorphisme (voir 2.4 du chapitre 1), on a: $H \cap K \lhd K$ et $H \lhd HK$, et l'isomorphisme $HK/H \simeq K/(H \cap K)$. Comme K est résoluble, $K/(H \cap K)$ est résoluble par application de la proposition 1.2, et donc HK/H est résoluble. Puisque H est un sous-groupe normal et résoluble dans HK, on déduit avec le théorème précédent que HK est résoluble. □

COROLLAIRE. *Le produit direct de deux groupes résolubles est résoluble.*

Preuve. Soient G_1 et G_2 deux groupes résolubles, et $G = G_1 \times G_2$ leur produit direct. Les sous-groupes $H = G_1 \times \{e_2\}$ et $K = \{e_1\} \times G_2$ vérifient: $H \simeq G_1$, $K \simeq G_2$, $H \lhd G$, $K \lhd G$, et $G = HK$. On applique le corollaire ci-dessus pour conclure que G est résoluble. □

2. Suites de Jordan-Hölder et groupes résolubles.

2.1 Notion de suite de Jordan-Hölder.

DÉFINITION. Soient G un groupe, et (Σ) une suite de composition de G strictement décroissante:

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_n = \{e\}.$$

On dit que (Σ) admet un *raffinement propre* lorsqu'il existe $1 \leq i \leq n-1$ et un sous-groupe K tel que $G_{i+1} \lhd K \lhd G_i$ avec $G_{i+1} \neq K \neq G_i$.

REMARQUE. Comme $G_{i+1} \lhd G_i$, tout sous-groupe K tel que $G_{i+1} \subset K \subset G_i$ vérifie $G_{i+1} \lhd K$. En conséquence, dire que (Σ) n'admet pas de raffinement propre signifie que, quel que soit $1 \leq i \leq n-1$, on ne peut pas trouver de sous-groupe K tel que $G_{i+1} \subset K \lhd G_i$ avec $G_{i+1} \neq K \neq G_i$, c'est-à-dire que G_{i+1} est normal maximal dans G_i.

LEMME. *Soient G un groupe, et (Σ) une suite de composition de G strictement décroissante:*

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_n = \{e\}.$$

Les assertions suivantes sont équivalentes:

(i) *(Σ) est sans raffinement propre;*

(ii) *G_{i+1} est normal maximal dans G_i, pour tout $0 \leq i \leq n-1$;*

(iii) *G_i/G_{i+1} est un groupe simple, pour tout $0 \leq i \leq n-1$.*

Preuve. L'équivalence de (i) et (ii) résulte de la remarque précédente. Pour (iii), rappelons d'abord que tout sous-groupe normal H de G_i/G_{i+1} est de la forme $H = K/G_{i+1}$ avec K un sous-groupe normal de G_i contenant G_{i+1}. Dès lors:

$$\begin{aligned}(G_i/G_{i+1} \text{ simple}) &\Leftrightarrow G_i/G_{i+1} \neq \{\overline{e}\} \text{ et, si } H \lhd G_i/G_{i+1}, \text{ alors } H = \{\overline{e}\} \text{ ou } H = G_i/G_{i+1} \\ &\Leftrightarrow G_i \neq G_{i+1} \text{ et, si } G_{i+1} \subseteq K \lhd G_i, \text{ alors } K = G_{i+1} \text{ ou } K = G_i,\end{aligned}$$

d'où l'équivalence de (ii) et (iii). □

DÉFINITION. Une suite de composition satisfaisant l'une des conditions équivalentes du lemme ci-dessus s'appelle une *suite de Jordan-Hölder* de G.

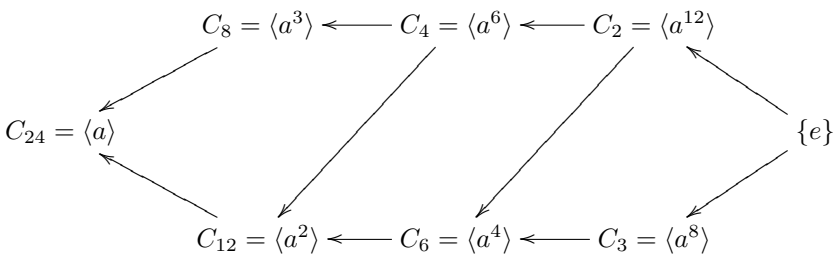
2.2 Exemples.

EXEMPLE 1. La suite $S_5 \rhd A_5 \rhd \{e\}$ est de Jordan-Hölder car $S_5/A_5 \simeq C_2$ qui est simple, et $A_5/\{e\} \simeq A_5$ qui est simple (chapitre 4, théroème 2.2).

EXEMPLE 2. La suite $S_4 \rhd A_4 \rhd \{e\}$ n'est pas de Jordan-Hölder car $A_4/\{e\} \simeq A_4$ n'est pas simple.

- Elle admet le raffinement propre $S_4 \rhd A_4 \rhd V \rhd \{e\}$, qui n'est pas de Jordan-Hölder car $V/\{e\} \simeq V$ n'est pas simple.
- Elle admet le raffinement propre $S_4 \rhd A_4 \rhd V \rhd H \rhd \{e\}$, qui est de Jordan-Hölder car tous les quotients $S_4/A_4 \simeq C_2$, $A_4/V \simeq C_3$, $V/H \simeq C_2$ et $H/\{e\} \simeq C_2$ sont simples (puisque cycliques d'ordre premier). On ne peut pas raffiner davantage.

EXEMPLE 3. Considérons le groupe cyclique $C_{24} = \{e, a, a^2, \ldots, a^{23}\}$ d'ordre 24. Ses sous-groupes sont:



On obtient quatre suites de Jordan-Hölder:

$$C_{24} \rhd C_{12} \rhd C_6 \rhd C_3 \rhd \{e\}, \qquad C_{24} \rhd C_8 \rhd C_4 \rhd C_2 \rhd \{e\},$$
$$C_{24} \rhd C_{12} \rhd C_4 \rhd C_2 \rhd \{e\}, \qquad C_{24} \rhd C_{12} \rhd C_6 \rhd C_2 \rhd \{e\}.$$

EXEMPLE 4. Le groupe additif $\mathbb{Z}$ n'admet aucune suite de Jordan-Hölder.

En effet, considérons une suite de composition $G_0 = \mathbb{Z} \rhd G_1 \rhd \cdots \rhd G_{n-1} \rhd G_n = \{0\}$ strictement décroissante. Rappelons que tout sous-groupe de $\mathbb{Z}$ est de la forme $k\mathbb{Z}$ avec $k \in \mathbb{N}$. Il existe donc ici $k \in \mathbb{N}^*$ tels que $G_{n-1} = k\mathbb{Z} \rhd G_n = \{0\}$. Soit alors le sous-groupe $H = 2k\mathbb{Z}$ de $\mathbb{Z}$. C'est un sous-groupe de $G_{n-1} = k\mathbb{Z}$, distinct de $k\mathbb{Z}$ et de $\{0\}$, de sorte que la suite de composition $G_0 = \mathbb{Z} \rhd G_1 \rhd \cdots \rhd G_{n-1} \rhd H \rhd G_n = \{0\}$ est un raffinement propre de la suite (quelconque) donnée au départ. Cette dernière n'est donc pas une suite de Jordan-Hölder.

PROPOSITION 1. *Tout groupe fini non-trivial admet au moins une suite de Jordan-Hölder.*

Preuve. Si G est simple, alors $G = G_0 \rhd G_1 = \{e\}$ est une suite de Jordan-Hölder (et c'est la seule suite de composition strictement décroissante). On suppose donc maintenant que G n'est pas simple. L'ensemble $\mathcal{H}$ des sous-groupes normaux dans G distincts de G et $\{e\}$ est alors non-vide. Il est fini (puisque G est fini). Il admet donc (au moins) un élément maximal H_1. Ce sous-groupe H_1 étant normal maximal dans G, il résulte du lemme 2.1 que G/H_1 est simple. Si H_1 est simple, c'est fini car $G \rhd H_1 \rhd \{e\}$ est alors une suite de Jordan-Hölder. Sinon, l'ensemble $\mathcal{H}_1$ des sous-groupes normaux dans H_1 distincts de H_1 et $\{e\}$ est fini non-vide, donc admet (au moins) un élément maximal H_2, et il résulte du lemme 2.1 que H_1/H_2 est simple. Si H_2 est simple, c'est fini car $G \rhd H_1 \rhd H_2 \rhd \{e\}$ est alors une suite de Jordan-Hölder. Sinon, on réitère. Comme G n'a qu'un nombre fini de sous-groupes, le processus s'arrête: il existe un rang k à partir duquel on obtient nécessairement un sous-groupe H_k simple, et la suite strictement décroissante $G \rhd H_1 \rhd H_2 \rhd \cdots \rhd H_k \rhd \{e\}$ est alors de Jordan-Hölder. □

PROPOSITION 2. *Un groupe abélien admet au moins une suite de Jordan-Hölder si et seulement s'il est fini non trivial.*

Preuve. Un sens est clair d'après la proposition précédente. Pour la réciproque, donnons-nous un groupe abélien G admettant une suite de Jordan-Hölder $G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{e\}$. Pour tout $0 \leq i \leq n-1$, le groupe G_i/G_{i+1} est simple (par définition d'une suite de Jordan-Hölder) et abélien (car G l'est), et donc (d'après la proposition 5 du 2.2 du chapitre 3) cyclique d'ordre premier. Notons $p_{i+1} = |G_i/G_{i+1}| = [G_i : G_{i+1}]$.

D'après la formule des indices (rappelée au 2.4 du chapitre 1), les égalités $[G : G_1] = p_1$ et $[G_1 : G_2] = p_2$ implique que G_2 est d'indice fini dans G, et $[G : G_2] = [G : G_1][G_1 : G_2] = p_1 p_2$. De même, $[G : G_2] = p_1 p_2$ et $[G_2 : G_3] = p_3$ impliquent $[G : G_3] = p_1 p_2 p_3$. En itérant, on obtient ainsi $[G : G_n] = p_1 p_2 \cdots p_n$, ce qui, comme $G_n = \{e\}$, montre que G est fini d'ordre $p_1 p_2 \cdots p_n$. □

2.3 Caractérisation de la résolubilité d'un groupe fini par les suites de Jordan-Hölder.

Nous avons défini la notion de groupe résoluble par le caractère stationnaire de la suite des groupes dérivés. Nous avons donné au théorème 1.3 une définition équivalente en termes de suite de composition ou en terme de suites normales. Le théorème suivant donne une autre définition équivalente, dans le cas des groupes finis, en termes cette fois de suites de Jordan-Hölder.

THÉORÈME. *Soit G un groupe fini non trivial. Le groupe G est résoluble si et seulement s'il existe une suite de Jordan-Hölder de G dont tous les quotients sont (cycliques) d'ordre premier.*

> *Preuve.* Supposons qu'il existe une suite de Jordan-Hölder de G dont tous les quotients sont d'ordre premier. Chaque quotient est alors cyclique, donc abélien, de sorte que la résolubilité de G découle directement du théorème 1.3. Réciproquement, supposons que G est résoluble. Comme G est supposé fini, il résulte de la proposition 1 de 2.2 qu'il existe une suite de Jordan-Hölder $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{e\}$. Donc, pour tout $0 \leq i \leq n-1$, le quotient G_i/G_{i+1} est simple. Puisque G est résoluble, il en est de même de chaque sous-groupe G_i et de chaque quotient G_i/G_{i+1}, par application de la proposition 1.2. Ainsi, tous les quotients G_i/G_{i+1} sont simples et résolubles, donc cycliques d'ordre premier d'après la proposition 2 de 1.4. □

2.4 A propos du théorème de Jordan-Hölder.

DÉFINITION. Deux suites de composition $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{e\}$ et $G = K_0 \triangleright K_1 \triangleright \cdots \triangleright K_p = \{e\}$ d'un groupe G sont dites équivalentes lorsque $n = p$ et qu'il existe une permutation $\sigma \in S_n$ telle que $G_i/G_{i+1} \simeq K_{\sigma(i)}/K_{\sigma(i)+1}$ pour tout $0 \leq i \leq n-1$.

EXEMPLE. Reprenons l'exemple 3 de 2.2. Les quatre suites de Jordan-Hölder de C_{24} sont équivalentes, car les quotients correspondants sont respectivement isomorphes à:

suites	quotients
$C_{24} \triangleright C_{12} \triangleright C_6 \triangleright C_3 \triangleright \{e\}$	$C_2,\ C_2,\ C_2,\ C_3$
$C_{24} \triangleright C_8 \triangleright C_4 \triangleright C_2 \triangleright \{e\}$	$C_3,\ C_2,\ C_2,\ C_2$
$C_{24} \triangleright C_{12} \triangleright C_4 \triangleright C_2 \triangleright \{e\}$	$C_2,\ C_3,\ C_2,\ C_2$
$C_{24} \triangleright C_{12} \triangleright C_6 \triangleright C_2 \triangleright \{e\}$	$C_2,\ C_2,\ C_3,\ C_2$

Cette propriété est un cas d'application du théorème général suivant (que nous citons pour mémoire, mais ne démontrerons pas ici).

THÉORÈME (dit de Jordan-Hölder). *Si G est un groupe admettant une suite de Jordan-Hölder (en particulier si G est un groupe fini), alors toutes les suites de Jordan-Hölder de G sont équivalentes.*

> *Preuve.* Voir ouvrage de référence. □

REMARQUE. En particulier, toutes les suites de Jordan-Hölder d'un groupe G admettant des suites de Jordan-Hölder sont de même longueur. On appelle cette longueur commune la longueur de G. Par exemple, il résulte de l'exemple précédent que C_{24} est de longueur 4. En reprenant la preuve du théorème 1.4, on vérifie aisément que tout groupe d'ordre p^n (avec p premier et $n \geq 1$) est de longueur n.

Chapitre 6

Anneaux de polynômes: rappels et compléments sur les polynômes en une indéterminée

Dans tout ce chapitre, le mot "anneau" désigne toujours un anneau commutatif unitaire.

1. Rappel de quelques notions générales.

1.1 Données et notations.

On fixe un anneau A. On note $A[X]$ l'anneau des polynômes en une indéterminée à coefficients dans A. Il contient A comme sous-anneau. Son neutre pour l'addition est 0_A. Son neutre pour la multiplication est 1_A. Pour tout élément non-nul P de $A[X]$, il existe un unique entier naturel n et un unique $(n+1)$-uplet $(a_0, a_1, \dots, a_n)$ 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 $\deg 0 = -\infty$. On vérifie aisément 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 Groupe des unités, intégrité, corps de fractions.

Définition et proposition. Soit A un anneau. Un élément $a \in A$ est dit inversible dans A s'il existe un élément b dans A tel que $ab = 1_A$. L'ensemble des éléments de A qui sont inversibles dans A est un groupe pour la multiplication, noté $U(A)$ ou A^* et appelé groupe des unités de l'anneau A.

Définition. Un anneau A est un corps lorsque tout élément non-nul de A est inversible dans A, c'est-à-dire lorsque $U(A) = A \setminus \{0\}$.

Définition. Un anneau A est intègre lorsque, pour tous $a, b \in A$, l'égalité $ab = 0$ implique $a = 0$ ou $b = 0$.

Proposition. Tout corps est un anneau intègre. La réciproque est fausse, mais, pour tout anneau intègre A, il existe un corps $K(A)$, appelé le corps de fractions de A qui est le plus petit corps contenant A (c'est-à-dire A est un sous-anneau de $K(A)$, et si F est un corps tel que A soit un sous-anneau de F, alors $K(A)$ est un sous-corps de F).

Exemples

- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des corps.
- L'anneau $\mathbb{Z}$ des entiers est intègre, vérifie $U(\mathbb{Z}) = \{-1, 1\}$, et donc n'est pas un corps. Son corps de fractions est $K(\mathbb{Z}) = \mathbb{Q}$.
- L'anneau $\mathbb{Z}[i]$ des entiers de Gauss est intègre, vérifie $U(\mathbb{Z}[i]) = \{-1, 1, i, -i\}$, et donc n'est pas un corps. Son corps de fractions est $K(\mathbb{Z}[i]) = \mathbb{Q}[i]$.
- L'anneau $\mathcal{F}$ des fonctions $\mathbb{R} \to \mathbb{R}$ n'est pas intègre (le produit de deux fonctions peut être la fonction nulle sans qu'aucune des deux ne soit la fonction nulle). Le groupe $U(\mathcal{F})$ est formé des fonctions qui ne s'annulent en aucun point de $\mathbb{R}$.
- L'anneau $\mathbb{Z}/n\mathbb{Z}$, où n est un entier ≥ 2, est intègre si et seulement si n est un nombre premier, ce qui est encore équivalent au fait que $\mathbb{Z}/n\mathbb{Z}$ est un corps. Le groupe $U(\mathbb{Z}/n\mathbb{Z})$ est formé des éléments $\overline{x}$ tels que $0 \leq x \leq n-1$ soit premier avec n.

Lemme. *Si A est intègre, alors on a:* $\begin{cases} \deg(PQ) = \deg P + \deg Q & \text{pour tous } P, Q \in A[X], \\ \mathrm{cd}(PQ) = \mathrm{cd}(P)\,\mathrm{cd}(Q) & \text{pour tous } P, Q \in A[X] \text{ non-nuls.} \end{cases}$

Preuve. L'égalité $\deg(PQ) = \deg P + \deg Q$ est trivialement vérifiée si P ou Q est nul. Supposons-les tous les deux non-nuls, et écrivons $P = a_n X^n + \cdots + a_1 X + a_0$ et $Q = b_m X^m + \cdots + b_1 X + b_0$, avec $\mathrm{cd}(P) = a_n \neq 0$ et $\mathrm{cd}(Q) = b_m \neq 0$. Alors:

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

L'intégrité de A impliquant $a_n b_m \neq 0$, le résultat voulu est établi. □

PROPOSITION. *$A[X]$ est intègre si et seulement si A est intègre.*

Preuve. Le fait que A intègre implique $A[X]$ intègre résulte immédiatement du lemme précédent. Récipoquement, si A n'est pas intègre, $A[X]$ ne peut pas l'être puisqu'il contient A comme sous-anneau. □

Remarque. En particulier, si K est un corps, alors $K[X]$ est intègre.

PROPOSITION. *Si A est intègre, on a: $U(A[X]) = U(A)$.*

Preuve. L'inclusion $U(A) \subset U(A[X])$ est claire. 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 lemme ci-dessus 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. □

PROPOSITION ET DÉFINITION. *Si A est intègre, le corps de fractions de $A[X]$ est égal au corps de fractions de l'anneau $K[X]$, où K désigne le corps de fractions de A; on l'appelle le corps des fractions rationnelles en une indéterminée à coefficients dans K, et on le note $K(X)$.*

Preuve. Evidente. □

1.3 Idéaux.

DÉFINITION. Soit A un anneau (commutatif). On appelle idéal de A tout sous-ensemble I de A vérifiant:
(1) I est un sous-groupe de A pour l'addition,
(2) pour tous $x \in I$ et $a \in A$, on a $ax \in I$.

EXEMPLES.
(1) A et $\{0\}$ sont toujours des idéaux de A. Rappelons les trois propriétés immédiates suivantes:
   - Un idéal I de A est égal à A si et seulement si $1_A \in I$.
   - Un idéal I de A est égal à A si et seulement s'il contient un élément de $U(A)$.
   - A et $\{0\}$ sont les seuls idéaux de A si et seulement si A est un corps

(2) Pour tout $a \in A$, l'ensemble $aA = \{ab\,;\, b \in A\}$ est un idéal de A. C'est le plus petit idéal de A contenant a, on l'appelle l'idéal principal engendré par a.
(3) Si f est un morphisme d'un anneau A dans un anneau B, le noyau $\operatorname{Ker} f = \{a \in A\,;\, f(a) = 0_B\}$ est un idéal de A.
(4) Si I et J sont deux idéaux de A, alors $I \cap J$ et $I + J = \{x + y\,;\, x \in I, y \in J\}$ sont des idéaux de A.

Un exemple intéressant. Montrons que, dans l'anneau $A = \mathbb{Z}[X]$, 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.

1.4 Anneaux quotients.

Soit I un idéal d'un anneau commutatif A. Comme I est un sous-groupe du groupe abélien A pour l'addition, 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 $\pi : A \to A/I$, qui à tout élément a de A associe sa classe $\overline{a}$ est alors un morphisme de groupes pour l'addition.
Il est facile de vérifier que l'on peut munir A/I d'une multiplication, définie indépendamment des représentants choisis par:

$$\overline{a}.\overline{b} = \overline{ab} \quad \text{pour tous } a, b \in A,$$

et l'on montre alors que:

THÉORÈME. *A/I est un anneau commutatif, et $\pi : A \to A/I$ est un morphisme d'anneaux.*

On a pour les anneaux quotients des résultats de même nature que pour les groupes quotients, en particulier:

THÉORÈME (dit premier théorème d'isomorphisme). *Soient A et A' deux anneaux commutatifs, et $f : A \to A'$ un morphisme d'anneaux. 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:* $A/\operatorname{Ker} f \simeq \operatorname{Im} f$.

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 idéal de A contenant I.

PROPOSITION. *Soient A un anneau et I un idéal de A. Dans $A[X]$, on pose $I[X]$ l'ensemble des éléments qui sont de la forme $\sum_{i=0}^{n} a_i X^i$ pour un entier $n \geq 0$ et des éléments $a_0, a_1, \ldots, a_n$ de I. Alors:*

(i) *$I[X]$ est un idéal de $A[X]$;* (ii) *les anneaux $(A/I)[X]$ et $A[X]/I[X]$ sont isomorphes.*

Preuve. Le point (i) est clair. Pour le (ii), considérons la surjection canonique $\pi : A \to A/I$ et son extension canonique en un morphisme d'anneaux $f : A[X] \to (A/I)[X]$, consistant à envoyer tout polynôme $P = \sum_{i=0}^{n} a_i X^i$ sur $f(P) = \sum_{i=0}^{n} \pi(a_i) X^i$. Il est clair que f est surjective et que son noyau est $\operatorname{Ker} f = I[X]$. L'isomorphisme $A[X]/\operatorname{Ker} f \simeq \operatorname{Im} f$ devient donc $A[X]/I[X] \simeq (A/I)[X]$. □

1.5 Idéaux premiers, idéaux maximaux.

DÉFINITION. Un idéal P d'un anneau commutatif A est dit premier si $P \neq A$ et s'il vérifie:
quels que soient deux éléments x et y de A, si $xy \in P$, alors $x \in P$ ou $y \in P$.

DÉFINITION. Un idéal M d'un anneau commutatif A est dit maximal si $M \neq A$ et s'il vérifie:
quel que soit I un idéal de A, si M est strictement inclus dans I, alors $I = A$.

THÉORÈME. *Soit I un idéal d'un anneau commutatif A. On a les implications suivantes:*

$$\begin{array}{ccc} I \text{ maximal} & \Longleftrightarrow & A/I \text{ corps} \\ \Downarrow & & \Downarrow \\ I \text{ premier} & \Longleftrightarrow & A/I \text{ intègre} \end{array}$$

PROPOSITION (idéaux premiers ou maximaux d'un quotient). *Soit A un anneau commutatif 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. Les idéaux maximaux de A/I sont de la forme M/I où M est un idéal maximal de A contenant I.*

PROPOSITION. *Soient A un anneau et I un idéal de A. Alors $I[X]$ est un idéal premier de $A[X]$ si et seulement si I est un idéal premier de A.*

Preuve. I est premier si et seulement si A/I est intègre, ce qui équivaut d'après 1.2 à $(A/I)[X]$ intègre, c'est-à-dire $A[X]/I[X]$ intègre d'après la proposition de 1.4, ce qui équivaut à dire que $I[X]$ est premier dans $A[X]$. □

1.6 Euclidianité.

LEMME (division euclidienne des polynômes). *Soit K un corps. Quels que soient des polynômes P et S dans $K[X]$ tels que $S \neq 0$, il existe Q et R uniques dans $K[X]$ tels que:*

$$P = SQ + R \quad \text{et} \quad \deg R < \deg S.$$

Preuve. Supposée connue; à réviser. □

DÉFINITION. Un anneau A est dit euclidien lorsqu'il est intègre et qu'il existe une application $\delta : A\backslash\{0\} \to \mathbb{N}$ vérifiant les deux conditions:

(i) quels que soient a, b non-nuls dans A, si a divise b, alors $\delta(a) \leq \delta(b)$,

(ii) quels que soient $a, b \in A$ avec $b \neq 0$, il existe $q, r \in A$ tels que: $a = bq + r$, avec $r = 0$ ou $\delta(r) < \delta(b)$.

L'application δ est appelé stathme euclidien.

Exemples

- L'anneau $\mathbb{Z}$ des entiers est euclidien, pour le stathme $\delta : \mathbb{Z}^* \to \mathbb{N}$ défini par $\delta(x) = |x|$.
- L'anneau $\mathbb{Z}[i]$ des entiers de Gauss est euclidien, pour le stathme $\delta : \mathbb{Z}[i]^* \to \mathbb{N}$ défini par $\delta(x + iy) = x^2 + y^2$.

COROLLAIRE. *Si K est un corps, l'anneau $K[X]$ est euclidien, pour le stathme défini par le degré.*

1.7 Principalité.

DÉFINITION. Un anneau intègre A est dit principal lorsque tout idéal de A est principal, c'est-à-dire de la forme aA pour un élément a de A.

THÉORÈME. *Tout anneau euclidien est principal.*

Exemples. En particulier, $\mathbb{Z}$ et $\mathbb{Z}[i]$ sont principaux.

Remarque. La réciproque du théorème est fausse. Il existe des anneaux principaux non euclidiens. Un des exemples classiques, élémentaire mais non immédiat, est $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$.

PROPOSITION. *Dans un anneau principal, tout idéal premier non-nul est maximal (et donc les notions d'idéal premier non-nul et d'idéal maximal coïncident).*

COROLLAIRE. *Si K est un corps, l'anneau $K[X]$ est principal.*

Remarque fondamentale. On a vu en 1.3 un exemple d'idéal de $\mathbb{Z}[X]$ qui n'est pas principal. Ceci prouve que l'anneau $\mathbb{Z}[X]$ n'est pas principal (et donc a fortiori non euclidien), bien que l'anneau $\mathbb{Z}$ des coefficients soit euclidien (et donc a fortiori principal). On retiendra que:

$$(\ A \text{ euclidien} \not\Rightarrow A[X] \text{ euclidien}\ ) \text{ et } (\ A \text{ principal} \not\Rightarrow A[X] \text{ principal}\ ).$$

Le théorème suivant précise cette observation.

THÉORÈME. *Soit A un anneau. Les 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) ⇒ (ii) ⇒ (iii). Supposons donc maintenant $A[X]$ principal. En particulier, $A[X]$ est intègre, et donc (voir 1.2), 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 conduit à $A[X]/\operatorname{Ker} f \simeq A$. L'intégrité de A implique que $A[X]/\operatorname{Ker} f$ est intègre, donc $\operatorname{Ker} f$ est un idéal premier de $A[X]$. Mais comme $A[X]$ est supposé principal, $\operatorname{Ker} f$ est alors un idéal maximal de $A[X]$, donc $A[X]/\operatorname{Ker} f$ est un corps; on conclut via l'isomorphisme $A[X]/\operatorname{Ker} f \simeq A$ que A est un corps. □

2. Factorialité des anneaux de polynômes

2.1 Divisibilité

Définitions. Soient a et b deux éléments d'un anneau intègre A.
On dit que b divise a lorsqu'il existe un élément c de A tel que $a = bc$. On note $b|a$.
On dit que b est associé à a lorsqu'il existe un élément u de $U(A)$ tel que $a = bu$. On note $b \sim a$.

Proposition (traduction en terme d'idéaux principaux). *Soient a et b deux éléments d'un anneau A.*

(1) $b|a \Leftrightarrow a \in bA \Leftrightarrow aA \subseteq bA$.

(2) $b \sim a \Leftrightarrow a \sim b \Leftrightarrow (b|a \text{ et } a|b) \Leftrightarrow aA = bA$.

Exemple. Dans le cas où $A = \mathbb{Z}$, on retrouve la notion de diviseur de l'arithmétique élémentaire.

Application. 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 $P = cQ$ (et alors $Q = c^{-1}P$). 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 $P = cQ$.

Définition. Un polynôme de $A[X]$ est dit unitaire lorsque son coefficient dominant est égal à 1.

Remarque. Si K est un corps, tout polynôme non-nul est associé à un polynôme unitaire.

Définition. Soient a et b deux éléments non-nuls d'un anneau A. On dit qu'un élément non-nul d de A est un pgcd de a et b lorsque: $d|a$, $d|b$ et tout élément de A qui divise a et b divise aussi d.

Remarque. Deux pgcd de a et b sont nécessairement associés.

Définition. Deux éléments non-nuls a et b de A sont dits premiers entre eux lorsque leurs seuls diviseurs communs sont les inversibles de A, ce qui équivaut à dire que 1 est un pgcd de a et b.

Proposition. *Soient a et b deux éléments non-nuls d'un anneau A admettant un pgcd d. Alors il existe deux éléments non-nuls a' et b' de A tels que $a = da'$, $b = db'$, et a' et b' sont premiers entre eux.*

Question. Pour quels types d'anneaux deux éléments quelconques a et b non-nuls dans A admettent-ils toujours des pgcd ? Le théorème suivant montre que c'est le cas pour les anneaux principaux. On verra plus loin que c'est aussi le cas plus généralement pour les anneaux factoriels.

Théorème. *Soit A un anneau principal. Soient a et b deux éléments non-nuls de A. Alors:*

(i) *l'idéal $aA + bA$ est principal et tout générateur de $aA + bA$ est un pgcd de a et b;*

(ii) *pour tout $d \in A$, on a: (d est un pgcd de a et b) $\Rightarrow$ (il existe $u, v \in A$ tels que $d = au + bv$);*

(iii) *(a et b sont premiers entre eux) $\Leftrightarrow$ (il existe $u, v \in A$ tels que $au + bv = 1$).*

Remarques.

(1) La propriété (iii) est connue sous le nom de théorème de Bézout dans un anneau principal (elle est donc vraie en particulier dans $\mathbb{Z}$).

(2) Dans le cas particulier d'un anneau euclidien (en particulier dans $\mathbb{Z}$), on dispose pour calculer les pgcd d'un moyen algorithmique basé sur la division euclidienne, l'algorithme d'Euclide (à réviser).

(3) On généralise sans difficultés les notions de pgcd et d'éléments premiers entre eux rappelées ci-dessus pour deux éléments à un nombre fini quelconque d'éléments de A.

Application. Si K un corps, $A = K[X]$ est euclidien et donc principal, et tout ce qui précède s'applique (pgcd de polynômes, polynômes premiers entre eux, théorème de Bézout, algorithme d'Euclide,...)

Contre-exemple. Dans l'anneau $A = \mathbb{Z}[X]$, il est facile de vérifier que les éléments 2 et X sont premiers entre eux, mais que $1 \notin 2A + XA$; donc la propriété de Bézout n'est pas vérifiée dans $\mathbb{Z}[X]$ (ce qui donne une autre preuve du fait que $\mathbb{Z}[X]$ n'est pas principal).

Exercice. Soit K un corps de caractéristique nulle. Soient m, n, d trois entiers strictement positifs. Montrer:
(1) d divise m dans $\mathbb{Z}$ si et seulement si $X^d - 1$ divise $X^m - 1$ dans $K[X]$;
(2) d est un pgcd de m et n dans $\mathbb{Z}$ si et seulement si $X^d - 1$ est un pgcd de $X^m - 1$ et $X^n - 1$ dans $K[X]$.

2.2 Irréductibité

Définition. Un élément r d'un anneau intègre A est dit irréductible dans A lorsqu'il n'est pas inversible dans A et vérifie la condition:

si $r = ab$ avec $a, b \in A$, alors $a \in U(A)$ ou $b \in U(A)$.

Remarques.

(1) r irréductible dans $A \Leftrightarrow rA$ maximal dans l'ensemble des idéaux principaux propres de A.
(2) Tout élément de A associé à un élément irréductible est encore irréductible.
(3) 0 n'est pas irréductible dans A.
(4) 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 $\mathbb{Q}$.

Définition. Un élément p d'un anneau intègre A est dit premier dans A lorsqu'il est non nul, non inversible dans A, et vérifie la condition:

si p divise ab avec $a, b \in A$, alors p divise a ou p divise b.

Remarques.

(1) p premier dans $A \Leftrightarrow pA$ idéal premier non-nul de $A \Leftrightarrow pA \neq (0)$ et A/pA intègre.
(2) Tout élément de A associé à un élément premier est encore premier.

Proposition. *Tout élément premier dans A est irréductible dans A.*

Remarque. La réciproque est fausse en général. Par exemple, il est facile de montrer que, dans $A = \mathbb{Z}[i\sqrt{5}]$, l'élément 3 est irréductible, mais il n'est pas premier car il divise $9 = (2+i\sqrt{5})(2-i\sqrt{5})$ sans diviser $(2+i\sqrt{5})$ ni $(2-i\sqrt{5})$. Néanmoins, on a le théorème suivant:

Théorème. *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.*

Exemple. Dans $\mathbb{Z}$, les éléments premiers (ou irréductibles) sont les nombres premiers et leurs opposés.

Proposition. *Soit K un corps.*

(i) *Les polynômes de degré un sont irréductibles dans $K[X]$.*
(ii) *Si $K = \mathbb{C}$, les éléments irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré un.*
(iii) *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 négatifs.*

Preuve. Le point (i) est évident en raisonnant sur le degré. Les points (ii) et (iii) ont été vus précédemment (à réviser). □

2.3 Factorialité

Définition. Un anneau intègre A est dit factoriel lorsque 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:

(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 *la* 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). Plus généralement, on a:

Théorème. *Tout anneau principal est factoriel.*

Remarque. La réciproque est fausse. On verra plus loin que $A[X]$ est factoriel dès lors que A est factoriel, donc par exemple $\mathbb{Z}[X]$ est factoriel, alors qu'il n'est pas principal comme on l'a vu plus haut. Ainsi, les anneaux factoriels forment une classe d'anneaux plus vaste que celle des anneaux principaux, importante pour les applications (car stable par passage aux polynômes, voir plus loin), et dans laquelle on peut facilement faire de l'arithmétique, en particulier grâce aux résultats résumés dans le théorème suivant.

THÉORÈME. *Soit A un anneau factoriel.*

(i) *Les diviseurs d'un élément a non-nul de A sont tous les produits par un élément de $U(A)$ de certains des éléments irréductibles apparaissant dans une décomposition de a.*

(ii) *Deux éléments non-nuls quelconques a et b admettent toujours des pgcd dans A, dont on obtient la décomposition en facteurs irréductibles en prenant les facteurs irréductibles apparaissant à la fois dans la décomposition de a et celle de b.*

(iii) *Quels que soient a, b, c non-nuls dans A, on a:*
$$(a \text{ divise } bc) \text{ et } (a \text{ et } b \text{ premiers entre eux}) \Rightarrow (a \text{ divise } c)$$

Remarque. La propriété (iii) est connue sous le nom de théorème de Gauss.

THÉORÈME. *Si A est un anneau factoriel, tout élément irréductible est premier, et donc les notions d'élément premier et d'élément irréductible coïncident dans ce cas.*

2.4 Irréductibilité des polynômes à coefficients dans un anneau factoriel

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'au produit par un inversible de A près. Lorsque l'on écrit $c(P) = a$, on a aussi $c(P) = ua$ pour tout $u \in U(A)$.

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, c'est-à-dire lorsque $c(P) = 1$ (ou encore, d'après la remarque précédente, lorsque $c(P) \in U(A)$).

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.

LEMME 1. *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, ont 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) 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. □

LEMME 2. (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 1 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 élément inversibles près $c(PQ) = c(P)c(Q)$. □

LEMME 3. *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 $P = qP_1$ où $q \in K^*$ et $P_1 \in A[X]$ est 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. □

THÉORÈME. *Soient A un anneau factoriel et K son corps de fractions. Soit R un élément non-nul de $A[X]$.*

(i) *Ou bien $R \in A$; alors R est irréductible dans $A[X]$ si et seulement si R est irréductible dans A.*

(ii) *Ou bien $R \notin A$; alors R est irréductible dans $A[X]$ si et seulement si R est primitif dans $A[X]$ et irréductible dans $K[X]$.*

Preuve. Rappelons d'abord que $U(A[X]) = U(A)$ puisque A est intègre.

(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 $U(K[X]) = K \setminus \{0\}$. Mais P et Q étant à coefficients dans A, cela signifie que P ou Q appartient à $A \setminus \{0\}$. 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 1 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 3 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 2. En appliquant le lemme 1, 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 $K[X]$. □

2.5 Première application: critère d'irréductibilité d'Eisenstein

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 2 implique que Q et R le sont. Posons $Q = \sum_{i=0}^{q} b_i X^i$ et $R = \sum_{i=0}^{r} c_i X^i$, avec $b_i, c_i \in A$, et $0 < q < n$ et $0 < r < n$. On a $a_n = b_q c_r \neq 0$, 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 $a_0 = b_0 c_0$, et donc par hypothèse p divise $b_0 c_0$ mais p^2 ne divise pas $b_0 c_0$, 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 $k \in \{1, \dots, r\}$ tel que p ne divise pas c_k. Par construction, p ne divise pas $b_0 c_k$, et p divise $b_i c_{k-i}$ pour tout $i \in \{1, \dots, k\}$. Il en résulte que p ne divise pas $a_k = b_0 c_k + b_1 c_{k-1} + \cdots + b_k c_0$. 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 $a'_0, a'_1, \dots, a'_n$ premiers entre eux dans leur ensemble tels que $a_i = c(P)a'_i$ pour tout $0 \leq i \leq n$. Donc $P_1 = a'_n X^n + \cdots + a'_1 X + a'_0$. 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). 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 de 2.4, 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 $c(P)P_1 = P$. □

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.

2.6 Seconde application: factorialité de l'anneau des polynômes sur un anneau factoriel

On commence par prouver le lemme général suivant, qui donne une autre définition équivalente de la notion d'anneau factoriel, et dont un sens a déjà été cité à la fin du rappel du 2.3.

Lemme (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 iréductible 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. □

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 2.4. 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 irréductibles de P_1 pour en déduire une décomposition de P). On raisonne par récurrence sur n. Si $n = 1$, on écrit $P = u(X - a)$ avec $u \in U(A)$ et $a \in A$. Il est clair que $X - a$ est irréductible dans $A[X]$, donc il en est de même pour P. 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 2 de 2.4, 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 2.4), donc premier dans A puisque A est factoriel (lemme ci-dessus). 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 2.4, 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 le lemme ci-dessus, 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 3 de 2.4, 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 2 de 2.4). On en déduit avec le lemme 1 de 2.4 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 que $A[X]$ est factoriel. □

EXEMPLE: $\mathbb{Z}[X]$ est factoriel (rappelons qu'il n'est pas principal).

EXEMPLE: Si A est factoriel, alors $A[X, Y]$ est factoriel car isomorphe à $A[X][Y]$ avec $A[X]$ factoriel. Plus généralement on obtient ainsi (voir au chapitre suivant) la factorialité de l'anneau des polynômes en n indéterminées à coefficients dans un anneau factoriel A.

Chapitre 7

Anneaux de polynômes: polynômes en plusieurs indéterminées

Dans tout ce chapitre, le mot "anneau" désigne toujours un anneau commutatif unitaire.

1. Quelques notions générales.

1.1 Données, notations, définitions.

• On fixe un anneau A, et un entier naturel $n \geq 1$. Considérons une application f:

$$\begin{array}{ccc} \mathbb{N}^n & \to & A \\ (i_1, i_2, \ldots, i_n) & \mapsto & a_{i_1,i_2,\ldots,i_n} \end{array}$$

que l'on notera sous forme de suite (indexée sur $\mathbb{N}^n$), c'est-à-dire $(a_{i_1,i_2,\ldots,i_n})_{(i_1,i_2,\ldots,i_n)\in\mathbb{N}^n}$. On dit que f est à support fini lorsque $a_{i_1,i_2,\ldots,i_n} = 0$ sauf pour un nombre fini d'éléments $(i_1, i_2, \ldots, i_n)$ de $\mathbb{N}^n$. On note $\mathcal{R}_n(A)$ l'ensemble de toutes les suites f de ce type qui sont à support fini.

• Il est technique mais élémentaire de vérifier que $\mathcal{R}_n(A)$ est un anneau commutatif pour la somme et le produit définis par

$$(a_{i_1,i_2,\ldots,i_n})_{(i_1,i_2,\ldots,i_n)\in\mathbb{N}^n} + (b_{i_1,i_2,\ldots,i_n})_{(i_1,i_2,\ldots,i_n)\in\mathbb{N}^n} = (a_{i_1,i_2,\ldots,i_n} + b_{i_1,i_2,\ldots,i_n})_{(i_1,i_2,\ldots,i_n)\in\mathbb{N}^n},$$

$$(a_{i_1,i_2,\ldots,i_n})_{(i_1,i_2,\ldots,i_n)\in\mathbb{N}^n} \times (b_{i_1,i_2,\ldots,i_n})_{(i_1,i_2,\ldots,i_n)\in\mathbb{N}^n} = (c_{i_1,i_2,\ldots,i_n})_{(i_1,i_2,\ldots,i_n)\in\mathbb{N}^n},$$

avec

$$c_{i_1,i_2,\ldots,i_n} = \sum_{r=1}^{n} \sum_{j_r+k_r=i_r} a_{j_1,j_2,\ldots,j_n} b_{k_1,k_2,\ldots,k_n}.$$

Pour tout $a \in A$, on note encore a la suite $(a_{i_1,i_2,\ldots,i_n})_{(i_1,i_2,\ldots,i_n)\in\mathbb{N}^n}$ dont tous les termes $a_{i_1,i_2,\ldots,i_n}$ sont nuls, sauf $a_{0,0,\ldots,0} = a$. La définition du produit dans $\mathcal{R}_n(A)$ permet de vérifier que:

$$a \times (b_{i_1,i_2,\ldots,i_n})_{(i_1,i_2,\ldots,i_n)\in\mathbb{N}^n} = (ab_{i_1,i_2,\ldots,i_n})_{(i_1,i_2,\ldots,i_n)\in\mathbb{N}^n},$$

de sorte que A peut être identifié à un sous-anneau de $\mathcal{R}_n(A)$. En particulier, le neutre additif et le neutre multiplicatif de l'anneau $\mathcal{R}_n(A)$ sont (via l'identification ci-dessus) le zéro et le un de l'anneau A.

• Pour tout $(j_1, j_2, \ldots, j_n) \in \mathbb{N}^n$, on note $X_1^{j_1} X_2^{j_2} \ldots X_n^{j_n}$ la suite $(a_{i_1,i_2,\ldots,i_n})_{(i_1,i_2,\ldots,i_n)\in\mathbb{N}^n}$ dont tous les termes sont nuls, sauf $a_{j_1,j_2,\ldots,j_n} = 1$. La définition du produit dans $\mathcal{R}_n(A)$ permet de vérifier que:

$$(X_1^{j_1} X_2^{j_2} \ldots X_n^{j_n})(X_1^{k_1} X_2^{k_2} \ldots X_n^{k_n}) = X_1^{j_1+k_1} X_2^{j_2+k_2} \ldots X_n^{j_n+k_n}.$$

En particulier, $X_1^0 X_2^0 \ldots X_n^0 = 1$ et tout élément de l'anneau $\mathcal{R}_n(A)$ s'écrit comme une somme finie:

$$(a_{i_1,i_2,\ldots,i_n})_{(i_1,i_2,\ldots,i_n)\in\mathbb{N}^n} = \sum_{(i_1,i_2,\ldots,i_n)\in\mathbb{N}^n} a_{i_1,i_2,\ldots,i_n} X_1^{i_1} X_2^{i_2} \ldots X_n^{i_n}.$$

Définition. L'anneau $\mathcal{R}_n(A)$ est appelé l'anneau des polynômes en n indéterminées à coefficients dans A. On le note $A[X_1, X_2, \ldots, X_n]$.

Définitions. Un polynôme de la forme $aX_1^{i_1} X_2^{i_2} \ldots X_n^{i_n}$, avec $a \in A$, est appelé un monôme. Si $a \neq 0$, l'entier $i_1 + i_2 + \cdots + i_n$ est appelé le degré total de ce monôme. Tout polynôme est une somme de monômes, et on appelle degré total d'un polynôme non-nul le maximum des degrés totaux des monômes dont il est la somme. Par convention, le degré total du polynôme nul est strictement inférieur au degré total de tout polynôme non-nul; on le note $-\infty$.

Définitions. Un polynôme non-nul de $A[X_1, X_2, \ldots, X_n]$ est dit homogène de degré d (où d est un entier naturel) s'il est une somme de monômes qui sont tous de même degré total d. Pour tout polynôme P non-nul de $A[X_1, X_2, \ldots, X_n]$ et tout entier naturel d, on appelle composante homogène de degré d de P la somme des monômes de P de degré total d.

• Si $n = 1$, on note $X = X_1$ et on retrouve l'anneau $A[X]$ bien connu, étudié au chapitre précédent. Le degré total est le degré usuel.

• Si $n = 2$, on note souvent $X = X_1$ et $Y = X_2$; un élément de $A[X, Y]$ est une somme finie:

$$P = \sum_{(i,j)\in\mathbb{N}^2} a_{i,j} X^i Y^j, \quad \text{avec } a_{i,j} \in A.$$

EXEMPLE. Considérons par exemple dans $\mathbb{Z}[X, Y]$ les polynômes:

$$P = 3X^3Y + 5X^3 - 2XY + 7 \quad \text{et} \quad Q = XY + 5X - 6Y + 1.$$

Le degré total de P est 4, celui de Q est 2. Dans Q, la composante homogène de degré 2 est XY, la composante homogène de degré 1 est $5X - 6Y$, la composante homogène de degré 0 est 1. On calcule:

$$PQ = \underbrace{3X^4Y^2}_{6} + \underbrace{20X^4Y - 18X^3Y^2}_{5} + \underbrace{25X^4 - 27X^3Y - 2X^2Y^2}_{4} + \underbrace{5X^3 - 10X^2Y + 12XY^2}_{3} + \underbrace{5XY}_{2} + \underbrace{35X - 42Y}_{1} + \underbrace{7}_{0}.$$

• Si $n = 3$, on note souvent $X = X_1$, $Y = X_2$ et $Z = X_3$; un élément de $A[X, Y, Z]$ est une somme finie:

$$P = \sum_{(i,j,k)\in\mathbb{N}^3} a_{i,j,k} X^i Y^j Z^k, \quad \text{avec } a_{i,j,k} \in A.$$

EXEMPLE. Considérons par exemple dans $\mathbb{Z}[X, Y, Z]$ les polynômes:

$$P = X^3 + XYZ + X^2Z \quad \text{et} \quad Q = X + Y - Z.$$

P est homogène de degré 3 et Q est homogène de degré 1.

Leur produit $PQ = X^4 + X^3Y + 2X^2YZ - X^2Z^2 + XY^2Z - XYZ^2$ est homogène de degré 4.

1.2 Premières propriétés de l'anneau $A[X_1, X_2, \ldots, X_n]$.

LEMME (propriété universelle des anneaux de polynômes). *Soient A et B deux anneaux et φ un morphisme d'anneaux $A \to B$. Alors, quels que soient un entier $n \geq 1$ et des éléments $b_1, b_2, \ldots, b_n$ de B, il existe un unique morphisme d'anneaux $\Phi : A[X_1, X_2, \ldots, X_n] \to B$ qui prolonge φ (c'est-à-dire $\Phi(a) = \varphi(a)$ pour tout $a \in A$), et tel que $\Phi(X_i) = b_i$ pour tout $1 \leq i \leq n$.*

Preuve. Si Φ existe, il est nécessairement défini par:

$$\Phi\big(\sum a_{i_1,i_2,\ldots,i_n} X_1^{i_1} X_2^{i_2} \ldots X_n^{i_n}\big) = \sum \varphi(a_{i_1,i_2,\ldots,i_n}) b_1^{i_1} b_2^{i_2} \ldots b_n^{i_n},$$

ce qui réciproquement définit bien un morphisme d'anneaux $A[X_1, X_2, \ldots, X_n] \to B$. □

PROPOSITION (fondamentale). *Soit A un anneau.*

(i) *Pour tout entier $n \geq 2$, il existe dans $A[X_1, X_2, \ldots, X_n]$ un sous-anneau isomorphe à $A[X_1, X_2, \ldots, X_{n-1}]$, et l'on a alors $A[X_1, X_2, \ldots, X_n] \simeq A[X_1, X_2, \ldots, X_{n-1}][X_n]$.*

(i) *En particulier, $A[X, Y] \simeq A[X][Y]$, et $A[X, Y, Z] \simeq A[X, Y][Z] \simeq A[X][Y][Z]$.*

Preuve. Dans $B = A[X_1, X_2, \ldots, X_n]$, considérons l'ensemble C des polynômes $P = \sum a_{i_1,i_2,\ldots,i_n} X_1^{i_1} X_2^{i_2} \ldots X_n^{i_n}$ tels que $a_{i_1,i_2,\ldots,i_n} = 0$ pour tout multi-indice $(i_1, i_2, \ldots, i_n) \in \mathbb{N}^n$ tel que $i_n \neq 0$. Il est clair que C est un sous-anneau de A isomorphe à $A[X_1, X_2, \ldots, X_{n-1}]$. D'après le lemme précédent (appliqué avec $n = 1$), l'injection canonique $\varphi : C \to B$ se prolonge en un unique morphisme d'anneaux $\Phi : C[X] \to B$ tel que $\Phi(P) = \varphi(P) = P$ pour tout $P \in C$ et $\Phi(X) = X_n$, qui réalise de façon évidente un isomorphisme $C[X] \simeq B$, d'où le résultat en revenant aux notations de l'énoncé. □

THÉORÈME. *Soit A un anneau. Soit n un entier naturel non-nul.*

(i) *Si A est intègre, alors $A[X_1, X_2, \ldots, X_n]$ est intègre.*

(ii) *Si A est factoriel, alors $A[X_1, X_2, \ldots, X_n]$ est factoriel.*

Preuve. On raisonne par récurrence grâce à la proposition précédente, en utilisant la proposition d'intégrité du paragraphe 1.2 du chapitre 6 pour le point (i), et le théorème 2.6 du chapitre 6 pour le point (ii). □

Remarque. On n'a pas de propriétés analogues pour les notions d'anneau principal ou euclidien. Même si K est un corps, $K[X, Y] \simeq K[X][Y]$ n'est pas principal (d'après le théorème 1.7 du chapitre 6).

2. Polynômes symétriques.

Dans toute cette partie, on fixe un entier $n \geq 2$ et un anneau A intègre, et on se place dans l'anneau de polynômes $A[X_1, X_2, \ldots, X_n]$.

2.1 Action canonique du groupe symétrique sur l'anneau des polynômes.

• *Notations.* Pour tout polynôme $P \in A[X_1, X_2, \ldots, X_n]$ et toute permutation $\sigma \in S_n$, on note P_σ le polynôme de $A[X_1, X_2, \ldots, X_n]$ obtenu en permutant les indéterminées $X_1, X_2, \ldots, X_n$ suivant σ, c'est-à-dire:

$$P_\sigma(X_1, X_2, \ldots, X_n) = P(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}).$$

• *Exemple.* $n = 3$, $\sigma = (1, 3, 2)$, $P(X, Y, Z) = X^2 + YZ - 3XY$, alors $P_\sigma(X, Y, Z) = Z^2 + XY - 3ZX$.

• *Remarque.* Si P est constant (c'est-à-dire de degré nul), alors $P = P_\sigma$ pour toute $\sigma \in S_n$.

• Proposition.

(i) *Le groupe S_n opère sur $A[X_1, X_2, \ldots, X_n]$ par l'action:*

$$\begin{array}{ccc} S_n \times A[X_1, X_2, \ldots, X_n] & \to & A[X_1, X_2, \ldots, X_n] \\ (\sigma, P) & \mapsto & P_\sigma \end{array}.$$

(ii) *Quelle que soit $\sigma \in S_n$, l'application:*

$$\begin{array}{ccc} A[X_1, X_2, \ldots, X_n] & \to & A[X_1, X_2, \ldots, X_n] \\ P & \mapsto & P_\sigma \end{array}$$

est un automorphisme de l'anneau $A[X_1, X_2, \ldots, X_n]$.

Preuve. Simple vérification, sans aucune difficulté. □

2.2 Notion de polynôme symétrique.

Définition. Un polynôme $P \in A[X_1, X_2, \ldots, X_n]$ est dit symétrique si $P_\sigma = P$ pour toute $\sigma \in S_n$.

Remarque. L'ensemble des polynômes symétriques n'est autre que l'ensemble des points fixes pour l'action du groupe S_n sur l'ensemble $A[X_1, X_2, \ldots, X_n]$.

Proposition. *L'ensemble des polynômes symétriques est un sous-anneau de l'anneau $A[X_1, X_2, \ldots, X_n]$.*

Preuve. Simple vérification, sans aucune difficulté, utilisant le point (ii) de la proposition précédente. □

Exemples avec $n = 2$. Les polynômes suivants sont des polynômes symétriques dans $A[X, Y]$:

(1) $S_1 = X + Y, \quad S_2 = X^2 + Y^2, \quad S_3 = X^3 + Y^3, \quad \ldots$

(2) $W_1 = X + Y, \quad W_2 = X^2 + XY + Y^2, \quad W_3 = X^3 + X^2Y + XY^2 + Y^3, \quad \ldots$

(3) $D = (X - Y)^2$.

(4) $\Sigma_1 = X + Y, \quad \Sigma_2 = XY$.

Exemples avec $n = 3$. Les polynômes suivants sont des polynômes symétriques dans $A[X, Y, Z]$:

(1) $S_1 = X + Y + Z, \quad S_2 = X^2 + Y^2 + Z^2, \quad S_3 = X^3 + Y^3 + Z^3, \quad \ldots$

(2) $W_1 = X + Y + Z, \quad W_2 = X^2 + XY + XZ + Y^2 + YZ + Z^2,$
$W_3 = X^3 + Y^3 + Z^3 + X^2Y + XY^2 + X^2Z + XZ^2 + Y^2Z + YZ^2 + XYZ, \quad \ldots$

(3) $D = (X - Y)^2(X - Z)^2(Y - Z)^2$.

(4) $\Sigma_1 = X + Y + Z, \quad \Sigma_2 = XY + XZ + YZ, \quad \Sigma_3 = XYZ$.

Ces exemples sont des cas particuliers des exemples classiques suivants.

EXEMPLES avec n quelconque. Les polynômes suivants sont des polynômes symétriques dans $A[X_1, X_2, \ldots, X_n]$:

(1) les sommes de Newton: $\boxed{S_k = X_1^k + X_2^k + \cdots + X_n^k}$ pour tout $k \in \mathbb{N}$;

(2) les polynômes de Wronski: $\boxed{W_k = \sum_{i_1+i_2+\cdots+i_n=k} X_1^{i_1} X_2^{i_2} \ldots X_n^{i_n}}$ pour tout $k \in \mathbb{N}$;

(3) le discriminant des indéterminées: $\boxed{D = \prod_{1\leq i<j\leq n} (X_i - X_j)^2}$;

(4) les polynômes symétriques élémentaires:

$\Sigma_1 = X_1 + X_2 + \cdots + X_n$,

$\Sigma_2 = X_1X_2 + X_1X_3 + \cdots + X_1X_n + X_2X_3 + \cdots + X_2X_n + \cdots + X_{n-1}X_n$,

$\ldots$

$\boxed{\Sigma_k = \sum_{1\leq i_1<i_2<\cdots<i_k\leq n} X_{i_1} X_{i_2} \ldots X_{i_k}}$ pour tout $1 \leq k \leq n$, (somme de C_n^k termes),

$\ldots$

$\Sigma_n = X_1X_2 \ldots X_n$.

REMARQUE. Dans l'anneau $A[X_1, X_2, \ldots, X_n][Z]$, le polynôme $P(Z) = (Z - X_1)(Z - X_2)\ldots(Z - X_n)$ vérifie:

$$P(Z) = Z^n - \Sigma_1 Z^{n-1} + \Sigma_2 Z^{n-2} - \cdots + (-1)^{n-1}\Sigma_{n-1}Z + (-1)^n\Sigma_n.$$

2.3 Le théorème fondamental.

On reprend toutes les notations et hypothèses de 2.1 et 2.2. En particulier, on note $\Sigma_1, \Sigma_2, \ldots, \Sigma_n$ les polynômes symétriques élémentaires.

• *Premier exemple introductif.*

Considérons dans $\mathbb{Z}[X, Y, Z]$ le polynôme symétrique: $P(X, Y, Z) = X^2Y + XY^2 + Y^2Z + YZ^2 + Z^2X + ZX^2$.

On calcule:

$\Sigma_1\Sigma_2 = (X + Y + Z)(XY + YZ + ZX) = X^2Y + XYZ + X^2Z + XY^2 + Y^2Z + XYZ + XYZ + YZ^2 + Z^2X$
$= P(X, Y, Z) + 3XYZ = P(X, Y, Z) + 3\Sigma_3$.

On conclut que: $P(X, Y, Z) = \Sigma_1\Sigma_2 - 3\Sigma_3$,

ou encore: $P(X, Y, Z) = F(\Sigma_1, \Sigma_2, \Sigma_3)$, avec $F = XY - 3Z \in \mathbb{Z}[X, Y, Z]$.

• *Second exemple introductif.*

Considérons dans $\mathbb{Z}[X, Y, Z]$ le polynôme symétrique: $P(X, Y, Z) = (2X - Y - Z)(2Y - Z - X)(2Z - X - Y)$.

On calcule:

$P(X, Y, Z) = (3X - \Sigma_1)(3Y - \Sigma_1)(3Z - \Sigma_1)$
$= (9XY - 3X\Sigma_1 - 3Y\Sigma_1 + \Sigma_1^2)(3Z - \Sigma_1)$.
$= 27XYZ - 9XY\Sigma_1 - 9XZ\Sigma_1 + 3X\Sigma_1^2 - 9YZ\Sigma_1 + 3Y\Sigma_1^2 + 3Z\Sigma_1^2 - \Sigma_1^3$
$= 27XYZ - 9(XY + XZ + YZ)\Sigma_1 + 3(X + Y + Z)\Sigma_1^2 - \Sigma_1^3$.

On conclut que: $P(X, Y, Z) = 27\Sigma_3 - 9\Sigma_2\Sigma_1 + 2\Sigma_1^3$,

ou encore: $P(X, Y, Z) = F(\Sigma_1, \Sigma_2, \Sigma_3)$, avec $F = 27Z - 9XY + 2X^3 \in \mathbb{Z}[X, Y, Z]$.

THÉORÈME. *Soit $n \geq 2$ un entier. Soit A un anneau intègre. Pour tout polynôme symétrique $P \in A[X_1, X_2, \ldots, X_n]$, il existe un unique polynôme $F \in A[X_1, X_2, \ldots, X_n]$ tel que:*

$$P(X_1, X_2, \ldots, X_n) = F(\Sigma_1, \Sigma_2, \ldots, \Sigma_n),$$

où $\Sigma_1, \Sigma_2, \ldots, \Sigma_n$ sont les polynômes symétriques élémentaires en les X_i, $1 \leq i \leq n$.

La preuve de ce théorème est relativement longue et technique. On la donnera en détail plus loin dans le chapitre. Auparavant, on développe quelques applications des polynômes symétriques à des questions concrètes d'algèbre.

2.4 Formules de Newton.

On reprend toutes les notations et hypothèses de 2.1 et 2.2. En particulier, on note $\Sigma_1, \Sigma_2, \ldots, \Sigma_n$ les polynômes symétriques élémentaires, et $S_1, S_2, \ldots$ les sommes de Newton.

THÉORÈME. *Soit $n \geq 2$ un entier. Soit A un anneau intègre. On a dans l'anneau $A[X_1, X_2, \ldots, X_n]$ les relations suivantes:*

(i) $S_k - \Sigma_1 S_{k-1} + \Sigma_2 S_{k-2} - \cdots + (-1)^{k-1}\Sigma_{k-1}S_1 + (-1)^k k\Sigma_k = 0$, *pour tout* $1 \leq k \leq n$,

(ii) $S_\ell - \Sigma_1 S_{\ell-1} + \Sigma_2 S_{\ell-2} + \cdots + (-1)^n \Sigma_n S_{\ell-n} = 0$, *pour tout* $\ell > n$.

Preuve. Considérons dans l'anneau $A[X_1, X_2, \ldots, X_n][Z]$ le polynôme $P(Z) = (Z - X_1)(Z - X_2)\ldots(Z - X_n)$. Comme on l'a vu à la fin de 2.2, on a:

$$P(Z) = Z^n - \Sigma_1 Z^{n-1} + \Sigma_2 Z^{n-2} - \cdots + (-1)^{n-1}\Sigma_{n-1}Z + (-1)^n\Sigma_n.$$

• Par définition de P, on a $P(X_i) = 0$ pour tout $1 \leq i \leq n$, et donc:

$$X_i^n - \Sigma_1 X_i^{n-1} + \Sigma_2 X_i^{n-2} - \cdots + (-1)^{n-1}\Sigma_{n-1}X_i + (-1)^n\Sigma_n = 0.$$

On fait la somme membre à membre de ces n égalités pour $1 \leq i \leq n$; il vient:

$$S_n - \Sigma_1 S_{n-1} + \Sigma_2 S_{n-2} - \cdots + (-1)^{n-1}\Sigma_{n-1}S_1 + (-1)^n n\Sigma_n = 0,$$

ce qui est l'assertion (i) pour $k = n$.

• Pour $\ell > n$, on considère dans $A[X_1, X_2, \ldots, X_n][Z]$ le polynôme $Z^{\ell-n}P(Z)$. Pour tout $1 \leq i \leq n$, il vérifie $X_i^{\ell-n}P(X_i) = 0$, donc:

$$X_i^{\ell-n}\big(X_i^n - \Sigma_1 X_i^{n-1} + \Sigma_2 X_i^{n-2} - \cdots + (-1)^{n-1}\Sigma_{n-1}X_i + (-1)^n\Sigma_n\big) = 0,$$

ou encore:

$$X_i^\ell - \Sigma_1 X_i^{\ell-1} + \Sigma_2 X_i^{\ell-2} - \cdots + (-1)^{n-1}\Sigma_{n-1}X_i^{\ell-n+1} + (-1)^n\Sigma_n X_i^{\ell-n} = 0.$$

On fait la somme membre à membre de ces n égalités pour $1 \leq i \leq n$; on obtient exactement l'assertion (ii).

• Pour $k = 1$, la formule (i) est triviale, puisque $S_1 = \Sigma_1$.

• Il reste à prouver (i) pour $1 < k < n$. On raisonne pour cela par récurrence sur le nombre n d'indéterminées. C'est clair pour $n = 3$, car alors $k = 2$ et l'on a bien: $S_2 - \Sigma_1 S_1 + 2\Sigma_2 = 0$. On suppose maintenant la relation (i) vraie dans $A[X_1, X_2, \ldots, X_{n-1}]$, et on fixe $1 < k < n$.

On considère dans $A[X_1, X_2, \ldots, X_n]$ le polynôme $S_k - \Sigma_1 S_{k-1} + \Sigma_2 S_{k-2} - \cdots + (-1)^{k-1}\Sigma_{k-1}S_1 + (-1)^k k\Sigma_k$. Notons-le $Q(X_1, X_2, \ldots, X_{n-1}, X_n)$. Il est clairement homogène de degré k.

Introduisons enfin dans $A[X_1, X_2, \ldots, X_{n-1}]$ le polynôme $Q_0(X_1, \ldots, X_{n-1}) = Q(X_1, \ldots, X_{n-1}, 0)$.

Il est clair que, pour tout $1 \leq i \leq n-1$, on a: $\Sigma_i(X_1, \ldots, X_{n-1}, 0) = \Sigma_i(X_1, \ldots, X_{n-1})$, le i-ième polynôme symétrique élémentaire dans $A[X_1, X_2, \ldots, X_{n-1}]$. Et de même $S_i(X_1, \ldots, X_{n-1}, 0) = S_i(X_1, \ldots, X_{n-1})$. L'hypothèse de récurrence se traduit donc par: $Q_0(X_1, \ldots, X_{n-1}) = 0$ dans $A[X_1, X_2, \ldots, X_{n-1}]$.

En d'autres termes, $Q(X_1, \ldots, X_{n-1}, 0) = 0$ dans $A[X_1, X_2, \ldots, X_{n-1}, X_n]$. On en déduit que Q est divisible par X_n dans $A[X_1, X_2, \ldots, X_{n-1}, X_n]$. Comme Q est symétrique, cela implique que Q est aussi divisible par X_i pour tout $1 \leq i \leq n-1$. Finalement Q est divisible par le produit $X_1X_2\ldots X_n$. Comme Q est homogène de degré $k < n$, ce n'est possible que si $Q = 0$, ce qui prouve le résultat voulu, et achève la preuve. □

APPLICATION 1 (*expression des sommes de Newton en fonction des polynômes symétriques élémentaires*). Soit $n \geq 2$ un entier. Soit A un anneau intègre. On a dans l'anneau $A[X_1, X_2, \ldots, X_n]$ les relations suivantes:

$$S_1 = \Sigma_1, \qquad S_2 = S_1\Sigma_1 - 2\Sigma_2 = \Sigma_1^2 - 2\Sigma_2, \qquad S_3 = S_2\Sigma_1 - S_1\Sigma_2 + 3\Sigma_3 = \Sigma_1^3 - 3\Sigma_1\Sigma_2 + 3\Sigma_3, \quad \cdots$$

et ainsi, de proche en proche, l'expression de tous les S_i comme des polynômes en les Σ_j.

APPLICATION 2 (*expression des polynômes symétriques élémentaires en fonction des sommes de Newton; cas d'un corps de caractéristique zéro*). Soit $n \geq 2$ un entier. Soit K un corps de caractéristique zéro. On a dans l'anneau $K[X_1, X_2, \ldots, X_n]$ les relations suivantes:

$$\Sigma_1 = S_1, \qquad \Sigma_2 = \tfrac{1}{2}S_1^2 - \tfrac{1}{2}S_2, \qquad \Sigma_3 = \tfrac{1}{6}S_1^3 - \tfrac{1}{2}S_1S_2 + \tfrac{1}{3}S_3, \quad \cdots$$

et, de proche en proche, l'expression de tous les Σ_j comme des polynômes en les S_i, à coefficients dans K.

COROLLAIRE (une autre forme du théorème fondamental; cas d'un corps de caractéristique zéro). *Soit $n \geq 2$ un entier. Soit A un anneau intègre de caractéristique nulle. Soit K son corps de fractions. Pour tout polynôme symétrique $P \in A[X_1, X_2, \ldots, X_n]$, il existe un unique polynôme $G \in K[X_1, X_2, \ldots, X_n]$ tel que:*

$$P(X_1, X_2, \ldots, X_n) = G(S_1, S_2, \ldots, S_n),$$

où $S_1, S_2, \ldots, S_n$ sont les n premières sommes de Newton en les X_i, $1 \leq i \leq n$.

Preuve. Il suffit de combiner la seconde remarque ci-dessus avec le théorème fondamental de 2.3. □

2.5 Application aux relations entre coefficients et zéros d'un polynôme de $K[X]$.

On fixe un corps K algébriquement clos. Soit $P = \sum_{i=0}^{n} a_i X^i$ un polynôme de $K[X]$, de degré $n \geq 1$. Il a alors n zéros dans K, que l'on notera $\alpha_1, \alpha_2, \ldots, \alpha_n$, et se factorise en:

$$P(X) = \sum_{i=0}^{n} a_i X^i = a_n \prod_{j=1}^{n} (X - \alpha_j), \quad \text{avec } a_n \neq 0.$$

Pour tout $1 \leq k \leq n$, notons $\Sigma_k = \Sigma_k(\alpha_1, \alpha_2, \ldots, \alpha_n)$ le k-ième polynôme symétrique élémentaire en les α_i. On a alors (voir remarque finale de 2.2):

$$\prod_{j=1}^{n} (X - \alpha_i) = X^n - \Sigma_1 X^{n-1} + \Sigma_2 X^{n-2} - \cdots + (-1)^{n-1} \Sigma_{n-1} X + (-1)^n \Sigma_n.$$

On en déduit par identification que:

$$a_{n-1} = -a_n \Sigma_1, \quad a_{n-2} = a_n \Sigma_2, \quad \ldots, \quad a_1 = (-1)^{n-1} a_n \Sigma_{n-1}, \quad a_0 = (-1)^n a_n \Sigma_n.$$

On a ainsi établi:

PROPOSITION. *Si K est un corps algébriquement clos, alors pour tout polynôme $P(X) = \sum_{i=0}^{n} a_i X^i$ de degré $n \geq 1$, les n zéros $\alpha_1, \alpha_2, \ldots, \alpha_n$ de P vérifient:*

$$\Sigma_k(\alpha_1, \alpha_2, \ldots, \alpha_n) = (-1)^k \frac{a_{n-k}}{a_n}, \quad \text{pour tout } 1 \leq k \leq n.$$

COROLLAIRE. *Soit K un corps. Soient $\alpha_1, \alpha_2, \ldots, \alpha_n$ des éléments quelconques de K. Pour tout $1 \leq i \leq n$, posons $\lambda_i = \Sigma_i(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Alors $\alpha_1, \alpha_2, \ldots, \alpha_n$ sont les zéros du polynôme:*

$$X^n - \lambda_1 X^{n-1} + \lambda_2 X^{n-2} - \cdots + (-1)^n \lambda_n.$$

Exemple 1. Pour $P(X) = aX^2 + bX + c \in \mathbb{C}[X]$, avec $a \neq 0$, on retrouve le résultat bien connu:

$$\Sigma_1 = \alpha_1 + \alpha_2 = -\frac{b}{a} \quad \text{et} \quad \Sigma_2 = \alpha_1 \alpha_2 = \frac{c}{a}.$$

Exemple 2. Pour $P(X) = X^3 + pX + q \in \mathbb{C}[X]$, on retrouve le résultat bien connu:

$$\Sigma_1 = \alpha_1 + \alpha_2 + \alpha_3 = 0, \quad \Sigma_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = p \quad \text{et} \quad \Sigma_3 = \alpha_1\alpha_2\alpha_3 = -q.$$

3. RÉSULTANT ET DISCRIMINANT

3.1. Position du problème.

DONNÉES, QUESTION, REMARQUES. Dans toute cette partie, K est un corps algébriquement clos. On cherche à résoudre la question suivante:

> étant donnés deux polynômes P et Q de degré ≥ 1 dans $K[X]$, distincts, trouver une condition nécessaire et suffisante pour qu'ils admettent au moins un zéro commun.

Dire que P et Q admettent un zéro commun $\alpha \in K$ équivaut à dire que le polynôme $X - \alpha$ divise à la fois P et Q dans $K[X]$, ce qui équivaut à dire que leur pgcd dans l'anneau $K[X]$ est de degré ≥ 1.

PROPOSITION. *Soit K un corps algébriquement clos. Soient P et Q deux polynômes dans $K[X]$ de degrés respectifs $m \geq 1$ et $n \geq 1$. Ils admettent un zéro commun dans K si et seulement s'il existe des polynômes R et S dans $K[X]$ tels que:*

$$\deg R \leq m - 1, \qquad \deg S \leq n - 1, \qquad RQ = SP.$$

Preuve. Supposons les trois conditions de la proposition vérifiées. Appelons $\alpha_1, \alpha_2, \ldots, \alpha_m$ les zéros (non nécessairement distincts) de P dans K. Alors, pour tout $1 \leq i \leq m$, le polynôme $X - \alpha_i$ divise P, donc divise RQ, dans $K[X]$. Puisque $X - \alpha_i$ est premier (car irréductible dans l'anneau principal $K[X]$), on a donc $X - \alpha_i$ divise R ou $X - \alpha_i$ divise Q, et ceci quel que soit $1 \leq i \leq m$. Comme $\deg R < m$, on ne peut pas avoir R divisible par $(X - \alpha_1)(X - \alpha_2) \ldots (X - \alpha_m)$. C'est donc qu'il existe au moins un indice $1 \leq i_0 \leq m$ tel que $X - \alpha_{i_0}$ divise Q. Ainsi α_{i_0} est un zéro commun à P et Q dans K.

Réciproquement, supposons que P et Q aient un zéro commun $\alpha \in K$. Si D est un pgcd de P et Q dans $K[X]$, on a donc $\deg D \geq 1$, et il existe des polynômes non-nuls R et S dans $K[X]$ tels que $P = RD$ et $Q = SD$, avec $\deg R < \deg P$ et $\deg S < \deg Q$. On a alors l'égalité $RQ = RSD = SP$. □

3.2 Notion de résultant de deux polynômes.

DÉFINITION. Soit K un corps algébriquement clos. Soient P et Q deux polynômes non-nuls dans $K[X]$ de degrés respectifs $m \geq 1$ et $n \geq 1$. Notons:

$$P = \sum_{i=0}^{m} a_i X^i \quad \text{et} \quad Q = \sum_{i=0}^{n} b_i X^i, \qquad a_i, b_i \in K, \ \ a_m \neq 0, \ \ b_n \neq 0.$$

On appelle résultant de P et Q le déterminant d'ordre $m + n$ suivant:

$$R(P,Q) = \begin{vmatrix} a_m & 0 & . & 0 & 0 & b_n & 0 & . & 0 & 0 \\ a_{m-1} & a_m & . & . & . & b_{n-1} & b_n & . & . & . \\ a_{m-2} & a_{m-1} & . & . & . & b_{n-2} & b_{n-1} & . & . & . \\ . & . & . & . & . & . & . & . & . & . \\ . & . & . & a_m & 0 & . & . & . & . & . \\ a_{m-n+1} & a_{m-n+2} & . & a_{m-1} & a_m & b_1 & . & . & . & . \\ a_{m-n} & a_{m-n+1} & . & a_{m-2} & a_{m-1} & b_0 & b_1 & . & . & . \\ a_{m-n-1} & a_{m-n} & . & . & a_{m-2} & 0 & b_0 & . & . & . \\ . & . & . & . & . & 0 & 0 & . & . & . \\ . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & 0 & . \\ a_2 & a_3 & . & a_n & a_{n+1} & 0 & . & . & b_n & 0 \\ a_1 & a_2 & . & a_{n-1} & a_n & 0 & . & . & b_{n-1} & b_n \\ a_0 & a_1 & . & a_{n-2} & a_{n-1} & 0 & . & . & b_{n-2} & b_{n-1} \\ 0 & a_0 & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . \\ . & . & . & a_0 & a_1 & . & . & . & b_0 & b_1 \\ 0 & 0 & . & 0 & a_0 & 0 & 0 & . & 0 & b_0 \end{vmatrix} \begin{matrix} \leftarrow 1 \\ \leftarrow 2 \\ \leftarrow 3 \\ \\ \\ \leftarrow n \\ \leftarrow n+1 \\ \leftarrow n+2 \\ \\ \\ \\ \leftarrow m-1 \\ \leftarrow m \\ \leftarrow m+1 \\ \\ \\ \\ \leftarrow m+n \end{matrix}$$

$\underbrace{\qquad\qquad\qquad\qquad\qquad}_{n}$ $\underbrace{\qquad\qquad\qquad\qquad\qquad}_{m}$

Remarque. On a ci-dessus, pour fixer clairement l'écriture du déterminant, supposé que $m > n$. Mutatis mutandis, l'analogue pour $m \leq n$ s'en déduit de façon évidente.

THÉORÈME. *Soit K un corps algébriquement clos. Deux polynômes de $K[X]$ non-nuls et non constants ont au moins un zéro commun dans K si et seulement si leur résultant est nul.*

Preuve. Soient $P = \sum_{i=0}^{m} a_i X^i$ et $Q = \sum_{i=0}^{n} b_i X^i$ dans $K[X]$, de degrés respectifs $m \geq 1$ et $n \geq 1$. D'après la proposition de 3.1, l'existence d'un zéro commun à P et Q équivaut à l'existence de deux polynômes non-nuls $R = \sum_{i=0}^{m-1} \lambda_i X^i$, de degré $\leq m-1$, et $S = \sum_{i=0}^{n-1} \mu_i X^i$, de degré $\leq n-1$, tels que $RQ = SP$. Par identification, cette égalité équivaut aux relations:

$$\begin{cases} a_m\mu_{n-1} & = & b_n\lambda_{m-1} \\ a_{m-1}\mu_{n-1} + a_m\mu_{n-2} & = & b_{n-1}\lambda_{m-1} + b_n\lambda_{m-2} \\ a_{m-2}\mu_{n-1} + a_{m-1}\mu_{n-2} + a_m\mu_{n-3} & = & b_{n-2}\lambda_{m-1} + b_{n-1}\lambda_{m-2} + b_n\lambda_{m-3} \\ \cdots & \cdots & \cdots \\ a_0\mu_1 + a_1\mu_0 & = & b_0\lambda_1 + b_1\lambda_0 \\ a_0\mu_0 & = & b_0\lambda_0 \end{cases}$$

En faisant "tout passer" dans le premier membre, on obtient un système linéaire homogène, de $m + n$ équations à $m + n$ inconnues, ces inconnues étant $\mu_{n-1}, \mu_{n-2}, \ldots, \mu_0, -\lambda_{m-1}, -\lambda_{m-2}, \ldots, -\lambda_0$. Il admet une solution non-nulle si et seulement si son déterminant est nul. Or ce dernier n'est autre que le résultant $R(P,Q)$, d'où le résultat. □

COROLLAIRE. *Soit K un corps algébriquement clos. Deux polynômes de $K[X]$ non-nuls et non constants sont premiers entre eux dans $K[X]$ si et seulement si leur résultant est non-nul.*

Preuve. On a déjà observé en 3.1 que l'existence d'un zéro commun à P et Q équivaut au fait que leur pgcd est de degré ≥ 1, c'est-à-dire que P et Q ne sont pas premiers entre eux. D'où le résultat d'après le théorème précédent. □

Exemples en petits degrés.

- Si $P = aX + b$ et $Q = cX + d$, alors $R(P,Q) = ad - bc$.
- Si $P = aX^2 + bX + c$ et $Q = pX + q$, alors $R(P,Q) = p^2c + q^2a - pqb$.
- Si $P = aX^2 + bX + c$ et $Q = pX^2 + qX + r$, alors $R(P,Q) = (ar - cp)^2 - (aq - bp)(br - cq)$.

Exercice. Soit $a \in K$ un paramètre quelconque. Montrer qu'il existe au plus 7 valeurs de a pour lesquelles les polynômes $P = X^4 + X^3 + X + a + 1$ et $Q = aX^3 + X + a$ ont un zéro commun. (Indication: vérifier que $R(P,Q) = a^7 + 2a^4 + 3a^3 + a^2 + a + 1$.)

3.3 Expression du résultant en fonction des zéros.

THÉORÈME. *Soit K un corps algébriquement clos. Soient P et Q deux polynômes non-nuls dans $K[X]$ de degrés respectifs $m \geq 1$ et $n \geq 1$. Notons:*

$$P = \sum_{i=0}^{m} a_i X^i = a_m \prod_{j=1}^{m} (X - \alpha_j) \quad \text{et} \quad Q = \sum_{i=0}^{n} b_i X^i = b_n \prod_{j=1}^{n} (X - \beta_j),$$

où les a_i $(0 \leq i \leq m)$ et les b_i $(0 \leq i \leq n)$ sont les coefficients dans K de P et Q respectivement, avec $a_m \neq 0$ et $b_n \neq 0$, et où les α_j $(1 \leq j \leq m)$ et les β_j $(1 \leq j \leq n)$ sont les zéros dans K de P et Q respectivement.

Alors le résultant $R(P,Q)$ est donné par:

$$R(P,Q) = a_m^n b_n^m \prod_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} (\alpha_i - \beta_j).$$

Preuve. On raisonne en plusieurs étapes.
Première étape. Soient P_1 et Q_1 les polynômes unitaires dans $K[X]$ définis par $P = a_m P_1$ et $Q = b_n Q_1$. On a:

$$P_1 = \prod_{j=1}^{m} (X - \alpha_j) \qquad \text{et} \qquad Q_1 = \prod_{j=1}^{n} (X - \beta_j).$$

Notons $\Sigma_1, \ldots, \Sigma_m$ les fonctions symétriques élémentaires en les zéros $\alpha_1, \ldots, \alpha_m$ de P, et $\Sigma'_1, \ldots, \Sigma'_n$ les fonctions symétriques élémentaires en les zéros $\beta_1, \ldots, \beta_n$ de Q. D'après les résultats de 2.5, on a:

$$\Sigma_1 = -\frac{a_{m-1}}{a_m}, \quad \Sigma_2 = \frac{a_{m-2}}{a_m}, \quad \ldots, \quad \Sigma_m = (-1)^m \frac{a_0}{a_m}, \quad \Sigma'_1 = -\frac{b_{n-1}}{b_n}, \quad \Sigma'_2 = \frac{b_{n-2}}{b_n}, \quad \ldots, \quad \Sigma'_n = (-1)^n \frac{b_0}{b_n},$$

et donc:

$$P_1 = X^m - \Sigma_1 X^{m-1} + \Sigma_2 X^{m-2} - \ldots + (-1)^{m-1} \Sigma_{m-1} X + (-1)^m \Sigma_m,$$
$$Q_1 = X^n - \Sigma'_1 X^{n-1} + \Sigma'_2 X^{n-2} - \ldots + (-1)^{n-1} \Sigma'_{n-1} X + (-1)^n \Sigma'_n.$$

Deuxième étape. Reprenons maintenant les expressions développées $P = \sum_{i=0}^{m} a_i X^i$ et $Q = \sum_{i=0}^{n} b_i X^i$.
L'expression du déterminant $R(P,Q)$ vu en 3.2 permet de voir $R(P,Q)$ comme un polynôme en les $n + m + 2$ indéterminées $a_0, a_1, \ldots, a_m, b_0, b_1, \ldots, b_n$. Plus précisément, la forme du déterminant permet d'observer que ce polynôme est homogène de degré n en les indéterminées $a_0, a_1, \ldots, a_m$ et homogène de degré m en les indéterminées $b_0, b_1, \ldots, b_n$. Dans l'anneau $K[a_0, a_1, \ldots, a_m, b_0, b_1, \ldots, b_n]$, notons:

$$R(P,Q) = F(a_0, a_1, \ldots, a_m, b_0, b_1, \ldots, b_n).$$

D'après les observations précédentes:

$$R(P,Q) = a_m^n b_n^m F(\frac{a_0}{a_m}, \frac{a_1}{a_m}, \ldots, \frac{a_{m-1}}{a_m}, 1, \frac{b_0}{b_n}, \frac{b_1}{b_n}, \ldots, \frac{b_{n-1}}{b_n}, 1).$$

Cette relation appliquée aux polynômes P_1 et Q_1 développés comme à la fin de la première étape s'écrit:

$$R(P_1, Q_1) = F(\ (-1)^m \Sigma_m,\ (-1)^{m-1} \Sigma_{m-1},\ \ldots,\ -\Sigma_1,\ 1,\ (-1)^n \Sigma'_n,\ (-1)^{n-1} \Sigma'_{n-1},\ \ldots,\ -\Sigma'_1,\ 1\ ).$$

On en déduit d'abord que $R(P_1, Q_1)$ est un polynôme symétrique en $\alpha_1, \alpha_2, \ldots, \alpha_m$ d'une part, et en $\beta_1, \beta_2, \ldots, \beta_n$ d'autre part (c'est le sens évident du théorème 2.3).

On en déduit d'autre part que $R(P,Q) = a_m^n b_n^m R(P_1,Q_1)$, d'où $R(P_1,Q_1) = 0$ si et seulement si $R(P,Q) = 0$, c'est-à-dire d'après le théorème 3.2 si et seulement s'il existe un couple (i,j) avec $1 \leq i \leq m$ et $1 \leq j \leq n$ tel que $\alpha_i = \beta_j$.

Ces deux remarques impliquent que, dans $K[\alpha_1,\ldots,\alpha_m,\beta_1,\ldots,\beta_n]$, le polynôme $R(P_1,Q_1)$ est divisible par $(\alpha_i - \beta_j)$ pour tous $1 \leq i \leq m$ et $1 \leq j \leq n$, et donc par le produit $\Pi = \prod_{1\leq i\leq m, 1\leq j\leq n}(\alpha_i - \beta_j)$. En comparant pour chacun des polynômes $R(P_1,Q_1)$ et Π les degrés en $\alpha_1,\alpha_2,\ldots,\alpha_m$ et en $\beta_1,\beta_2,\ldots,\beta_n$, ainsi que le coefficient de $(\alpha_1\alpha_2\cdots\alpha_m)^n$, on conclut finalement que $R(P_1,Q_1) = \Pi$.

On en tire que $R(P,Q) = a_m^n b_n^m \Pi$, ce qui achève la preuve. □

Remarque. On a donc du résultant les expressions suivantes:

$$R(P,Q) = a_m^n b_n^m \prod_{\substack{1\leq i\leq m\\ 1\leq j\leq n}} (\alpha_i - \beta_j) = a_m^n \prod_{1\leq i\leq m} Q(\alpha_i) = (-1)^{mn} b_n^m \prod_{1\leq j\leq n} P(\beta_j).$$

qui rendent explicite la conclusion du théorème 3.2.

3.4 Discriminant d'un polynôme.

DÉFINITION. Soit K un corps algébriquement clos. On appelle discriminant d'un polynôme P de degré au moins égal à 2 dans $K[X]$ le résultant de P et de son polynôme dérivé P'. On note:

$$\Delta(P) = R(P,P').$$

THÉORÈME. *Soit K un corps algébriquement clos. Soient P un polynôme de degré au moins égal à 2 dans $K[X]$ et P' son polynôme dérivé. Les conditions suivantes sont équivalentes.*

(i) *Le polynôme P a au moins un zéro multiple dans K.*

(ii) *Les polynômes P et P' ne sont pas premiers entre eux.*

(iii) *Les polynômes P et P' ont au moins un zéro commun dans K.*

(iv) *Le discriminant $\Delta(P)$ du polynôme P est nul.*

Preuve. L'équivalence de (ii) et (iii) résulte de la remarque préliminaire de 3.1. Par définition même du discriminant, l'équivalence de (iii) et (iv) est une conséquence du théorème 3.2. Il suffit donc de montrer l'équivalence de (i) et (ii).

Supposons d'abord que P a un zéro multiple α. Alors il existe un polynôme Q de degré $n-2$, où n désigne le degré de P, tel que $P(X) = (X-\alpha)^2 Q(X)$. On a alors $P'(X) = 2(X-\alpha)Q(X) + (X-\alpha)^2 Q'(X)$, de sorte que $X - \alpha$ est un diviseur commun de P et P' de degré non-nul. Donc P et P' ne sont pas premiers entre eux.

Supposons réciproquement que P et P' ne sont pas premiers entre eux. Leur pgcd D est de degré strictement positif. Comme K est algébriquement clos, il admet au moins un zéro $\alpha \in K$. Le polynôme $X - \alpha$ divise D, donc divise P et P'. Il existe en particulier un polynôme Q de degré $n-1$, où n désigne le degré de P, tel que $P(X) = (X-\alpha)Q(X)$. On a alors $P'(X) = Q(X) + (X-\alpha)Q'(X)$. Mais comme $X - \alpha$ divise aussi P', on en déduit qu'il divise Q. Et donc P est divisible par $(X-\alpha)^2$, ce qui achève la preuve. □

COROLLAIRE. *Soit K un corps algébriquement clos. Un polynôme P de degré au moins égal à 2 dans $K[X]$ n'admet que des zéros simples dans K si et seulement si son discriminant est non-nul.*

EXEMPLE 1. Dans $\mathbb{C}[X]$, considérons $P(X) = aX^2 + bX + c$, avec $a \neq 0$. On a $P'(X) = 2aX + b$, et donc:

$$\Delta(P) = R(P,P') = \begin{vmatrix} a & 2a & 0 \\ b & b & 2a \\ c & 0 & b \end{vmatrix} = a(4ac - b^2).$$

L'application du corollaire ci-dessus montre que P n'a que des zéros simples si et seulement si $b^2 - 4ac \neq 0$, résultat bien connu !

EXEMPLE 2. Dans $\mathbb{C}[X]$, considérons $P(X) = X^3 + pX + q$. On a $P'(X) = 3X^2 + p$, et donc:

$$\Delta(P) = R(P,P') = \begin{vmatrix} 1 & 0 & 3 & 0 & 0 \\ 0 & 1 & 0 & 3 & 0 \\ p & 0 & p & 0 & 3 \\ q & p & 0 & p & 0 \\ 0 & q & 0 & 0 & p \end{vmatrix} = 4p^3 + 27q^2.$$

Supposons que $\Delta(P) = 0$, et notons α le zéro multiple de P dans K (il est forcément unique puisque P est de degré 3). Comme α est alors aussi zéro de P', on a $\alpha^2 = -\frac{p}{3}$.

Si $p = 0$, alors la nullité de $\Delta(P) = 4p^3 + 27q^2$ implique que l'on a aussi $q = 0$, donc $P(X) = X^3$, qui admet 0 comme zéro triple.

Si $p \neq 0$, alors la nullité de $\Delta(P) = 4p^3 + 27q^2$ implique que l'on a $p = -\frac{27q^2}{4p^2}$, d'où $\alpha^2 = -\frac{p}{3} = \frac{9q^2}{4p^2}$. On vérifie que seul $\alpha = -\frac{3q}{2p}$ est zéro de P, et c'est un zéro double.

PROPOSITION (expression du discriminant en fonction des zéros). *Soit K un corps algébriquement clos. Soit $P = a_n X^n + \cdots + a_1 X + a_0$ un polynôme de degré $n \geq 2$ dans $K[X]$. Soient $\alpha_1, \ldots, \alpha_n$ les zéros de P dans K. Alors le discriminant de P est donné par:*

$$\Delta(P) = (-1)^{\frac{n(n-1)}{2}} a_n^{2n-1} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

Preuve. On a: $P(X) = a_n \prod_{1 \leq k \leq n} (X - \alpha_k)$, donc: $P'(X) = a_n \sum_{1 \leq j \leq n} \Big(\prod_{1 \leq k \leq n, k \neq j} (X - \alpha_k) \Big)$

d'où, pour tout $1 \leq i \leq n$, l'égalité: $P'(\alpha_i) = a_n(\alpha_i - \alpha_1)(\alpha_i - \alpha_2) \ldots (\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1}) \ldots (\alpha_i - \alpha_n)$.

On calcule alors en utilisant les expressions de la remarque suivant le théorème 3.3:

$$\begin{aligned}
\Delta(P) = R(P, P') &= a_n^{n-1} \prod_{1 \leq i \leq n} P'(\alpha_i) \\
&= a_n^{n-1} \prod_{1 \leq i \leq n} a_n(\alpha_i - \alpha_1)(\alpha_i - \alpha_2) \ldots (\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1}) \ldots (\alpha_i - \alpha_n) \\
&= a_n^{2n-1} \prod_{1 \leq i \leq n} (\alpha_i - \alpha_1)(\alpha_i - \alpha_2) \ldots (\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1}) \ldots (\alpha_i - \alpha_n) \\
&= a_n^{2n-1} \prod_{1 \leq i \leq n} (-1)^{i-1} (\alpha_1 - \alpha_i)(\alpha_2 - \alpha_i) \ldots (\alpha_{i-1} - \alpha_i)(\alpha_i - \alpha_{i+1}) \ldots (\alpha_i - \alpha_n) \\
&= a_n^{2n-1} (-1)^{n(n-1)/2} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.
\end{aligned}$$

□

Remarque. Cette relation justifie le nom de discriminant des indéterminées donné à l'exemple (3) du paragraphe 2.2.