Hammadi ABIDI

Département de Mathématiques Faculté des Sciences de Tunis Université de Tunis El Manar 2092 Tunis

Cours d'algèbre générale

Section : Licence fondamentale de Mathématiques troisième année

LFM3

Remerciements

J'adresse mes remerciements aux personnes qui m'ont aidé dans la réalisation de ce cours. En premier lieu, je remercie Said Zarati, professeur à Faculté des sciences de Tunis.

Table des matières

1 Groupes **7**
- 1.1 Les groupes $\mathbb{Z}/nZ$ . . . 7
  - 1.1.1 Relation binaire . . . 7
  - 1.1.2 Relation d'équivalence . . . 8
- 1.2 Groupe symétrique . . . 10
- 1.3 Sous-groupe . . . 10
- 1.4 Classes modulo un sous-groupe . . . 13
- 1.5 Morphisme de groupes . . . 16
- 1.6 Groupes quotients . . . 20
  - 1.6.1 Sous-groupe d'un groupe quotient . . . 23
  - 1.6.2 Normalisateur et centralisateur d'une partie . . . 26
- 1.7 Série numéro I . . . 28
- 1.8 Correction . . . 32

2 Actions des groupes et théorème de Sylow **43**
- 2.1 Action d'un groupe sur un ensemble . . . 43
  - 2.1.1 Orbites et stabilisateurs . . . 45
  - 2.1.2 Équation aux classes . . . 50
- 2.2 Théorème de Sylow . . . 53
- 2.3 Produits directs . . . 63
- 2.4 Série numéro II . . . 73
- 2.5 Correction . . . 76

3 Anneaux et corps **85**
- 3.1 Anneaux . . . 85
  - 3.1.1 Sous-anneaux . . . 86
  - 3.1.2 Groupe des unités . . . 87
  - 3.1.3 Morphisme d'anneaux . . . 87
- 3.2 Corps . . . 88
  - 3.2.1 Diviseurs de zéro-anneau intègre . . . 88
  - 3.2.2 Corps des fractions d'un anneau intègre . . . 90
- 3.3 Idéaux et anneaux quotients . . . 92
  - 3.3.1 Idéal premier - idéal maximal . . . 95

3.4 Anneaux principal 99
3.5 Anneaux euclidien 99
3.6 P. G. C. D et P. P. C. M 101
3.7 Série numéro III 105
3.8 Correction 109

Chapitre 1

Groupes

Définition 1.1. *On appelle groupe tout couple $(G, *)$ formé d'un ensemble non vide et d'une loi de composition $*$ vérifiant*

1. $\forall\ (x, y) \in G^2 : x * y \in G$ *(l.c.i).*
2. $\forall\ (x, y, z) \in G^3 : (x * y) * z = x * (y * z)$ *(associativité).*
3. $\exists\ e \in G$ *tel que* $\forall\ x \in G : e * x = x * e = x$ *(e l'élément neutre).*
4. $\forall\ x \in G, \exists\ x' \in G$ *tel que* $x * x' = x' * x = e$ *(x' l'inverse de x est noté x^{-1}).*

Si de plus la loi $*$ vérifie

$$x * y = y * x \qquad \forall\ (x, y) \in G^2$$

on dit que G est un groupe commutatif ou abélien.

Exemples.
- $(\mathbb{C}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Z}, +)$ *groupes abéliens.*
- $(\mathbb{C}^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{Q}^*, \times)$ *groupes abéliens ou $E^* = E \setminus \{0\}$.*
- $(\mathbb{Z}^*, +)$, $(\mathbb{N}, +)$, *ne sont pas des groupes.*

Remarques.
1. *L'élément neutre est unique : $e * e' = e = e'$.*
2. *Un élément $x \in G$ possède un seul inverse :*

$$x' * (x * x'') = x' = (x' * x) * x'' = x''.$$

3. $(x * y)^{-1} = y^{-1} * x^{-1}$.

Définition 1.2. *L'ordre d'un groupe G est le cardinal de l'ensemble G, il est noté $|G|$.*

1.1 Les groupes $\mathbb{Z}/nZ$

1.1.1 Relation binaire

Définition 1.3. *On appelle relation binaire $\mathscr{R}$ sur un ensemble E, toute propriété vraie pour certain couples (x, y) d'éléments de E et fausse pour les autres. Lorsque un couple (x, y) vérifie la relation $\mathscr{R}$, on écrit $x\mathscr{R}y$, sinon on écrit $x\not\mathscr{R}y$.*

Exemples. *1.* $=, \geq, \leq, \subset$ *sont des relations binéaires.*

2. $E = \mathbb{R} : x\mathscr{R}y \iff \sin(x) = \sin(y)$.

$$0\mathscr{R}\pi \qquad et \qquad 0\mathscr{R}\pi/2.$$

1.1.2 Relation d'équivalence

Définition 1.4. *On appelle relation d'équivalence toute relation binéaire vérifiant :*

1. $\forall\, x \in E\ x\mathscr{R}x$ *(réflexive).*

2. $\forall\, (x, y) \in E^2$ *si* $x\mathscr{R}y$*, alors* $y\mathscr{R}x$ *(symétrique).*

3. $\forall\, (x, y, z) \in E^3$ *si* $x\mathscr{R}y$ *et* $y\mathscr{R}z$*, alors* $x\mathscr{R}z$ *(transitive).*

Remarque. *Une relation d'équivalence se comprend comme une égalité modulo certains critères.*

Exemples. *1.* $E = \mathbb{R} : x\mathscr{R}y \iff \sin(x) = \sin(y)$.

2. $E = \mathbb{Z}$, $n \in \mathbb{N}^* : p\mathscr{R}q \iff p - q$ *divisible par* n.

Classe d'équivalence : Soit $\mathscr{R}$ une relation d'équivalence sur un ensemble E.

Définition 1.5. *On appelle classe d'équivalence d'un élément* $x \in E$ *pour* $\mathscr{R}$ *le sous-ensemble de* E *noté,* $\bar{x}$ *(ou bien* $cl(x)$, $\dot{x}$*)*

$$\bar{x} = \{y \in E \,|\, x\mathscr{R}y\}.$$

Exemple. $E = \mathbb{R} : x\mathscr{R}y \iff \sin(x) = \sin(y)$

$$\bar{x} = \{x + 2k\pi \,|\, k \in \mathbb{Z}\} \cup \{\pi - x + 2k\pi \,|\, k \in \mathbb{Z}\} = \{x,\, \pi - x\} + 2\pi\mathbb{Z}.$$

Définition 1.6. *On appelle ensemble quotient de* E *par* $\mathscr{R}$ *l'ensemble noté* $E/\mathscr{R}$ *des classes d'équivalence pour* $\mathscr{R}$*,*

$$E/\mathscr{R} = \{\bar{x} \,|\, x \in E\}.$$

Exemple. $E = \mathbb{Z} \times \mathbb{Z}^* : (a, b)\mathscr{R}(c, d) \iff ad = bc$

$$\overline{(a, b)} = \frac{a}{b}; \quad \frac{\mathbb{Z} \times \mathbb{Z}^*}{\mathscr{R}} = \mathbb{Q}.$$

Définition 1.7. *On définit sur* $\mathbb{Z}$ *la relation de congruence modulo* n, $n \in \mathbb{N}^*$ *par*

$$p \equiv q[n] \iff n/p - q.$$

La relation de congruence modulo n, est une relation d'équivalence sur $\mathbb{Z}$

$$\overline{p} = \{p + kn \,|\, k \in \mathbb{Z}\} = p + n\mathbb{Z}.$$

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}?$$

Pour $a, b \in \{0, 1, \cdots, n-1\} \Longrightarrow 1-n \leq b-a \leq n-1$. Donc si $\overline{a} = \overline{b} \Longrightarrow n/b-a \Longrightarrow a = b$. Ainsi $\overline{0}, \overline{1}, \cdots, \overline{n-1}$ sont deux à deux distincts et par suite

$$\{\overline{0}, \overline{1}, \cdots, \overline{n-1}\} \subset \mathbb{Z}/n\mathbb{Z}.$$

Soit $\overline{p} \in \mathbb{Z}/n/Z$, alors $p = nk + r$ avec $0 \leq r \leq n-1$, ainsi $\overline{p} = \overline{r}$. Donc

$$\mathbb{Z}/n\mathbb{Z} \subset \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\},$$

d'où

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}.$$

Exemple.

$$\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}.$$

Proposition 1.8. *Si*

$$p \equiv p'[n] \qquad et \qquad q \equiv q'[n],$$

alors

$$p + q \equiv p' + q'[n] \qquad et \qquad pq \equiv p'q'[n].$$

Démonstration : Comme

$$n/p - p' \qquad \text{et} \qquad n/q - q', \qquad \text{alors} \qquad n \Big/ p + q - (p' + q').$$

On a

$$pq - p'q' = (p - p')q + (q - q')p'$$

et par suite

$$n \Big/ pq - p'q'.$$

■

Dans $\mathbb{Z}/n\mathbb{Z}$, on définit les deux lois + et $\times$:

$$\overline{p} + \overline{q} = \overline{p+q} \qquad \text{et} \qquad \overline{p} \times \overline{q} = \overline{pq}.$$

Ces deux lois sont bien définies puisque elles sont indépandantes du choix des représentants.

Exemple. *Dans* $\mathbb{Z}/6\mathbb{Z} : \overline{3} + \overline{5} = \overline{8} = \overline{2}$ *et* $\overline{3} \times \overline{5} = \overline{15} = \overline{3}$.

Proposition 1.9. $(\mathbb{Z}/n\mathbb{Z}, +)$ *est un groupe commutatif.*

Démonstration : La loi + est une l.c.i ; $\overline{0}$ l'élément neutre ; $\overline{p}^{-1} = \overline{-p} = \overline{n-p}$. ■

Remarque. $(\mathbb{Z}/n\mathbb{Z}, \times)$ *n'est pas un groupe car* $\overline{0}$ *n'est pas inversible.*

1.2 Groupe symétrique

Définition 1.10. *Soit E un ensemble non vide, on appelle permutation de E toute bijection de E et on note $\mathcal{S}(E)$ l'ensemble des permutations de E : i.e, des bijections de E vers E.*

Exemple. *Pour $n \in \mathbb{N}^*$, $\mathcal{S}_n$ l'ensemble des permutations de $\{1, \cdots, n\}$, $|\mathcal{S}_n| = n!$.*

Proposition 1.11. *Si $E \neq \emptyset$, alors $(\mathcal{S}(E), \circ)$ est un groupe.*

Démonstration : La loi $\circ$, l.c.i : associative, Id_E, l'élément neutre, $f^{-1} \in \mathcal{S}(E)$. ■

Remarque. *Le groupe $(\mathcal{S}(E), \circ)$ n'est pas commutatif dès que $card(E) \geq 3$:*

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad et \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad on\ a \quad \sigma_1 \circ \sigma_2 \neq \sigma_2 \circ \sigma_1.$$

Définition 1.12. *Soit $(G, *)$ un groupe, d'élément neutre e, $g \in G$ et $k \in \mathbb{Z}$, alors*

$$g^k = \begin{cases} \underbrace{g * \cdots * g}_{k\ fois}, & si \quad k > 0 \\ e, & si \quad k = 0 \\ \underbrace{g^{-1} * \cdots * g^{-1}}_{-k\ fois}, & si \quad k < 0. \end{cases}$$

Proposition 1.13. *Soit $(G, *_i)_{i \in I}$ une famille de groupes. Le produit cartésien des G_i est un groupe pour la l.c.i : $*$*

$$x = (x_i)_{i \in I}, \quad y = (y_i)_{i \in I}, \qquad alors \quad x * y = (x_i *_i y_i)_{i \in I}.$$

Définition 1.14. *Soit $(G, *_i)_{i \in I}$ une famille de groupes. On appelle produit direct de cette famille le produit cartésien des G_i.*

1.3 Sous-groupe

Définition 1.15. *On appelle sous-groupe d'un groupe $(G, *)$ toute partie H de G telle que $(H, *)$ est un groupe et on note $H \leq G$.*

Exemple. *$\{e\}$ et G deux sous-groupes de G.*

Théorème 1.16. *H est un sous-groupe de G si et seulement si $H \neq \emptyset$ et $\forall\, (x, y) \in H^2;\ x * y^{-1} \in H$.*

Démonstration : "$\Longrightarrow$" Le premier sens ça démontre facilement.
"$\Longleftarrow$" Il est clair que $*$ est associative, comme $H \neq \emptyset$, alors $x * x^{-1} = e \in H$, enfin $e * x^{-1} = x^{-1} \in H$. D'où $H \leq G$. ■

Exemples. *1) Les sous-groupes de* $(\mathbb{Z},+)$ *sont de la forme* $n\mathbb{Z}$*, où* $n\in\mathbb{N}$*. En effet :*
Pour $n\in\mathbb{N}$*, on a* $(n\mathbb{Z},+)$ *est un sous-groupe de* $(\mathbb{Z},+)$*.*
Soit $H\leq\mathbb{Z}$*, si* $H=\{0\}$*, alors* $H=0\mathbb{Z}$*, sinon*

$$H^+=\{h\in H\,|\,h>0\}\neq\emptyset$$

car $H\neq\{0\}$*, et par suite il existe* $h\in H$ *tel que* $h\neq 0$*. Si* $0<h\in H^+$*, alors* $h\in H^+$*, sinon* $0<-h\in H^+$*. Ainsi* $H^+\neq\emptyset$ *et minoré donc admet une borne inf or* $H^+\subset\mathbb{N}$*. Ainsi* H^+ *admet un plus petit élément :* $n=\min H^+$*.*
On a, $n\in H^+\subset H$*, alors*

$$n\mathbb{Z}=H.$$

Soit $h\in H$*, par division euclidienne on a,* $h=qn+r$ *avec* $0\leq r<n$*, et par suite* $r=h-qn\in H$*. Si* $r>0$*, alors* $r\in H^+$ *avec* $r<n$ *absurde car* $n=\min H^+$*. Donc* $r=0$*, ainsi* $h\in n\mathbb{Z}$*, d'où*

$$H\subset n\mathbb{Z}.$$

2)

$$U_n=\{z\in\mathbb{C}\,|\,z^n=1\}\qquad\text{est un sous-groupe de }\mathbb{C}^*\text{ pour la multiplication.}$$

3)

$$O(n,\mathbb{R})=\{M\in GL_n(\mathbb{R})\,|\,\det(M)=1\}\leq GL_n(\mathbb{R}).$$

4) (Voir TD)

$$\mathcal{A}_n=\{\sigma\in\mathcal{S}_n\,|\,\varepsilon(\sigma)=1\}\leq\mathcal{S}_n$$

avec

$$\varepsilon(\sigma)=\prod_{i<j}\frac{\sigma(i)-\sigma(j)}{i-j}=\pm 1.$$

Remarque. *Pour montrer qu'un ensemble est un groupe, il suffit de prouver que c'est un sous-groupe d'un groupe connu.*

Sous-groupe engendré par un élément

Définition 1.17. *On appelle sous-groupe engendré par un élément* $g\in G$*, l'ensemble*

$$\langle g\rangle=\{g^k\,|\,k\in\mathbb{Z}\}.$$

Proposition 1.18. $\langle g\rangle\leq G$*, contenant* g*. De plus* $\langle g\rangle$ *le plus petit sous-groupe contenant* g*.*

Démonstration : On a $\langle g\rangle\neq\emptyset$, soit $(a,b)\in\langle g\rangle^2$, ainsi $a=g^k$ et $b=g^l$ et par suite

$$ab^{-1}=g^{k-|l|}\in\langle g\rangle.$$

Donc $\langle g\rangle\leq G$.
Soit $H\leq G$ tel que $g\in H$, ainsi on aura par définition $\langle g\rangle\subset H$. ∎

Exemple. $G = \mathbb{Z}/8\mathbb{Z}$; $\langle \overline{2} \rangle = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$.

Remarques. *1. $\langle g \rangle$ est toujours commutatif même si la loi $*$ n'est pas commutatif.*

2. L'ordre d'un élément g est l'ordre de $\langle g \rangle$ qui est aussi le plus petit entier $n \in \mathbb{N}^*$ tel que

$$g^n = e.$$

Proposition 1.19. *Soient G un groupe, I un ensemble non vide et $\{H_i\}_{i \in I}$ une famille de sous-groupes de G, alors*

$$H = \bigcap_{i \in I} H_i \leq G$$

c'est-à-dire, l'intersection de sous-groupes de G est un sous-groupe de G.

Remarques. *1. La reunion de sous-groupes de G n'est pas en général un sous-groupe de G. Voici un contre exemple $2\mathbb{Z} \cup 3\mathbb{Z} \nleqslant \mathbb{Z}$ car $5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.*

2. Si $H \leq G$ et $K \leq G$, alors $H \cup K$ est un sous-groupe de G si et seulement si $H \subset K$ ou $K \subset H$.

Définition 1.20. *Soit A une partie non vide d'un groupe G, l'intersection de tous les sous-groupes de G contenant A est un sous-groupe de G, on l'appelle sous-groupe engendré par la partie A : $\langle A \rangle$*

$$\langle A \rangle = \bigcap_{H \leq G,\, A \subset H} H.$$

Définition 1.21. *On appelle partie génératrice d'un groupe toute partie engendrant le groupe.*

Exemples. *1. $\{(1,0),\ (0,1)\}$ est une partie génératrice de groupe $(\mathbb{Z}^2, +)$.*

2. Pour $n \geq 2$, le groupe symétrique $\mathcal{S}_n$ est engendré par les transpositions.
On appelle transposition de $1 \leq i \leq n$ et $1 \leq j \leq n$ et on le note $\tau_{i,j}$

$$\tau_{i,j}(k) = \begin{cases} j, & si \quad k = i \\ i, & si \quad k = j \\ k, & si \quad k \neq i,\ k \neq j. \end{cases}$$

La démonstration se fait par récurrence, pour $n = 2$, $\mathcal{S}_n = \{Id, \tau_{12}\}$, on a $Id = \tau_{12} \circ \tau_{12}$.
On suppose la proriété vraie au rang $n - 1$.
Soit $\sigma \in \mathcal{S}_n$, si $\sigma(n) = n$, alors la restriction de σ à $\{1, 2, \cdots, n-1\}$ appartient à $\mathcal{S}_{n-1}$: hypothèse de récurrence.
Si $\sigma(n) = m \neq n$, alors

$$\tau_{nm} \circ \sigma(n) = n$$

et par suite

$$\sigma = \tau_{nm} \circ (\ \underbrace{\tau_{nm} \circ \sigma}_{récurrence}\ ).$$

Définition 1.22. *Un groupe ayant une partie génératrice réduite à un élément est dit monogène.*
Un groupe cyclique est tout groupe monogène fini.

Exemples. *1.* $\mathbb{Z} = \langle 1 \rangle$: *monogène.*

2. $U_n = \{z \in \mathbb{C} \,|\, z^n = 1\} = \langle \omega \rangle$ *avec* $\omega = e^{\frac{2i\pi}{n}}$: *cyclique.*

3. $(\mathbb{Z}/n\mathbb{Z}, +)$ *est un groupe cyclique dont les générateurs sont les* $\overline{m}$ *avec* $m \wedge n = 1$.
On a

$$\mathbb{Z}/n\mathbb{Z} = \langle \overline{1} \rangle = \{k\overline{1} \,|\, k \in \mathbb{Z}\} = \{\overline{k} \,|\, k \in \mathbb{Z}\}.$$

Si $\langle \overline{m} \rangle = \mathbb{Z}/n\mathbb{Z}$, *alors il existe* $k \in \mathbb{Z}$ *tel que* $k\overline{m} = \overline{1}$, *ainsi* $km \equiv 1[n]$ *et par suite* $m \wedge n = 1$ *(identité de Bézout).*
Si $m \wedge n = 1$, *alors*

$$km \equiv 1[n] \Longrightarrow k\overline{m} = \overline{1} \Longrightarrow \overline{1} \in \langle \overline{m} \rangle$$

or

$$\langle \overline{1} \rangle = \mathbb{Z}/n\mathbb{Z}$$

donc

$$\langle \overline{m} \rangle = \mathbb{Z}/n\mathbb{Z}.$$

1.4 Classes modulo un sous-groupe

Proposition 1.23. *Soient* G *un groupe et* $H \leq G$. *La relation définie par*

$$x \mathscr{R} y \Longleftrightarrow x^{-1}y \in H$$

est une relation d'équivalence sur G.
La classe d'équivalence de x *est l'ensemble* xH.

Définition 1.24. *La classe d'équivalence de* x *est appelée classe à gauche de* x *modulo* H.

Remarque. *On a les mêmes notions à droite*

$$x \mathscr{R} y \Longleftrightarrow yx^{-1} \in H$$

est une relation d'équivalence sur G. *La classe à droite de* x *modulo* H *est l'ensemble* Hx.

Ainsi les classes à gauche (reps. à droite) modulo H forment une partition de G, i.e

$$G = \coprod_{x \in G} xH$$

avec $xH \neq yH$ ($xH \neq yH \Longleftrightarrow xH \cap yH = \emptyset$).
De plus pour tout $g \in xH$ il existe un unique $h \in H$ tel que

$$g = xh$$

ainsi

$$|xH| = |H|.$$

Le nombre de classe à gauche est égal au nombre de classe à droite modulo H. Ce nombre s'appelle **l'indice du sous-groupe H**, noté $[G : H]$.

Exemples. *1.* $[G : G] = 1$, $[G : \{e\}] = |G|$.

2. $[Z, n\mathbb{Z}] = n$ *ici les classes à droite= classes à gauche car* $(\mathbb{Z}, +)$ *abélien.*

Comme

$$G = \coprod_{x \in G} xH \qquad \text{avec} \quad xH \cap yH = \emptyset \quad \text{et} \quad |xH| = |H|,$$

alors, on en dénduit le théorème suivant.

Théorème 1.25. *(de Lagrange) Soit* G *un groupe fini. Si* $H \leq G$, *alors*

$$|G| = |H|[g : H]$$

Conséquence : Si G est fini et $H \leq G$, alors $|H|$ divise $|G|$.
La réciproque n'est pas vraie.

Exemple.

$$\mathcal{A}_4 = \{\sigma \in \mathcal{S}_n \,|\, \varepsilon(\sigma) = 1\}$$

est un groupe d'ordre 12 *mais n'admet pas un sous-groupe d'ordre* 6 *(voir TD).*

Un groupe G d'ordre premier p est cyclique, en effet :
Soit $g \in G \setminus \{e\}$, alors $|\langle x \rangle| > 1$ de plus $|\langle x \rangle|$ divise p, ainsi $|\langle x \rangle| = p$ et par suite

$$\langle x \rangle = G.$$

Formule de l'indice

Théorème 1.26. *Soient* G *un groupe,* $H \leq G$ *et* $K \leq G$ *tels que* $H \subset K$ *et* $[G : H] < +\infty$. *Alors*

$$[G : K] < +\infty \qquad et \qquad [G : H] = [G : K][K : H].$$

Démonstration : Si $|G| < +\infty$, alors

$$[G : H] = \frac{|G|}{|H|} = \frac{[G : K]|K|}{|H|} = [G : K][K : H].$$

Si G est un groupe quelconque.
Soit $\{x_i\}_{i \in I}$ une famille de reprśentants des classes (à droite) distincts des éléments de G modulo K, ainsi

$$G = \coprod_{i \in I} Kx_i \qquad \text{avec} \qquad card(I) = [G : K].$$

Soit $\{y_i\}_{i\in J}$ une famille de reprśentants des classes (à droite) distincts des éléments de K modulo H, ainsi

$$K = \coprod_{j\in J} Hy_j \qquad \text{avec} \qquad card(J) = [K : H].$$

Pour tout $g \in G$ il existe un unique $i \in I$ tel que $g \in Kx_i$ et par suite il existe un unique $k \in K$ tel que

$$g = kx_i.$$

De même pour k il existe un unique $j \in J$ tel que $k \in Hy_j$, ainsi $g \in Hy_jx_i$. Donc

$$G = \coprod_{(i,j)\in I\times J} Hy_jx_i.$$

D'où les ensembles Hy_jx_i forment une partition de G. En effet :
Si

$$Hy_jx_i = Hy_{j'}x_{i'},$$

alors

$$KHy_jx_i = KHy_{j'}x_{i'},$$

comme $H \subset K$, on en déduit

$$Kx_i = Kx_{i'}$$

or Kx_i forment une partition de G, alors

$$i = i'.$$

Comme Hy_j forment une partition de K, alors

$$j = j'.$$

Ainsi

$$[G : H] = card(I \times J) = card(I)card(J) = [G : K][K : H].$$

■

Théorème 1.27. *Dans un groupe G, l'intersection d'un nombre fini des sous-groupes d'indice fini est un sous-groupe d'indice fini.*

Démonstration : Par récurrence : $n = 2$, on a

$$[G : H_1 \cap H_2] = [G : H_1][H_1 : H_1 \cap H_2]$$

or l'application

$$\begin{aligned} \varphi : \quad & H_1\big/H_1 \cap H_2 \longrightarrow G\big/H_2 \\ & x = h(H_1 \cap H_2) \longmapsto xH_2 = hH_2 \end{aligned}$$

est injective. En effet :

$$\varphi(x_1) = \varphi(x_2) \quad \Longrightarrow h_1H_2 = h_2H_2 \quad \Longrightarrow h_2^{-1}h_1 \in H_1 \cap H_2$$

et par suite

$$x_1 = h_1(H_1 \cap H_2) = h_2h_2^{-1}h_1(H_1 \cap H_2) = h_2(H_1 \cap H_2) = x_2.$$

Donc

$$[H_1 : H_1 \cap H_2] = card\Big(H_1\Big/H_1 \cap H_2\Big) \leq [G : H_2].$$

Supposons qu'il est vraie pour $(n-1)$ sous-groupes. Or

$$H_1 \cap \cdots \cap H_n = \Big(\underbrace{H_1 \cap \cdots \cap H_{n-1}}_{H}\Big) \cap H_n$$

ainsi

$$[G : H_1 \cap \cdots H_n] \leq [G : H][G : H_n] \leq \prod_{i=1}^{n}[G : H_i].$$

■

1.5 Morphisme de groupes

Définition 1.28. *Soient $(G, *)$, (G', T) deux groupes et*

$$\varphi : \quad G \longrightarrow G'$$

une application. On dit que φ est un morphisme de groupes si

$$\varphi(x * y) = \varphi(x)T\varphi(y) \qquad \forall\,(x, y) \in G^2.$$

On note $Hom(G, G')$, l'ensemble de morphisme de G vers G'.

Si de plus φ est bijective, on dit que φ est un isomorphisme, $Isom(G, G')$. Un morphisme de G dans lui même est un endomorphisme de G, $End(G)$. Un isomorphisme de G dans lui même est un automorphisme de G, $Aut(G)$.

Exemples. *1.*

$$\begin{aligned} \varphi : \quad & (\mathbb{R}, +) \longrightarrow (\mathbb{R}^*, \times) \\ & x \longmapsto e^x \end{aligned}$$

est un morphisme.

2.

$$\begin{aligned} \det : \quad & GL_n(\mathbb{C}) \longrightarrow \mathbb{C}^* \\ & M \longmapsto \det(M) \end{aligned}$$

est un morphisme.

3. *(voir TD)*

$$\begin{aligned}\varepsilon : \quad & \mathcal{S}_n \longrightarrow \{-1,1\} \\ & \sigma \longmapsto \varepsilon(\sigma)\end{aligned}$$

est un morphisme.

4. *Soit $g \in G$, alors*

$$\begin{aligned}i_g : \quad & G \longrightarrow G \\ & x \longmapsto gxg^{-1}\end{aligned}$$

est un automorphisme, appelé automorphisme intérieur de G, $Int(G)$.

5. *L'application*

$$\begin{aligned}i : \quad & G \longrightarrow Aut(G) \\ & g \longmapsto i_g\end{aligned}$$

est un morphisme.

Remarques. 1. *$(Aut(G), \circ)$ est un groupe.*

2. *Soient $f \in Hom(G, G')$ et $g \in Hom(G', G'')$, alors $g \circ f \in Hom(G, G'')$.*

Proposition 1.29. *Soit $\varphi \in Hom(G, G')$, alors*

1. $\varphi(e) = e'$.
2. $\varphi(x^{-1}) = [\varphi(x)]^{-1}$.
3. *L'image directe (reps. réciproque) d'un sous-groupe est un sous-groupe, i.e,*
   Si $H \leq G$, alors $\varphi(H) = \{\varphi(x) \,|\, x \in H\} \leq G'$.
   Si $K \leq G'$, alors $\varphi^{-1}(K) = \{x \in G \,|\, \varphi(x) \in K\} \leq G$.
4. $$\ker(\varphi) = \{x \in G \,|\, \varphi(x) = e'\} \leq G.$$
5. $$Im(\varphi) = \{\varphi(x) \,|\, x \in G\} \leq G'.$$
6. *φ injective* $\iff \ker(\varphi) = \{e\}$.
7. *φ surjective* $\iff Im(\varphi) = G'$.

Exemple. *Pour*

$$\begin{aligned}\varphi : \quad & (\mathbb{C}, +) \longrightarrow (\mathbb{C}^*, \times) \\ & z \longmapsto e^z,\end{aligned}$$

on a $\ker(\varphi) = 2i\pi\mathbb{Z}$.

Définition 1.30. *S'il existe un isomorphisme entre deux groupes, alors ces deux groupes sont dits isomorphes.*

Exemple. *$(\mathbb{Z}/4\mathbb{Z}, +)$ et $(U_4, \times)$ sont isomorphes*

$$\varphi(\overline{0}) = 1, \quad \varphi(\overline{1}) = i, \quad \varphi(\overline{2}) = -1 \quad et \quad \varphi(\overline{3}) = -i.$$

Lemme 1.31. *Soient G, G' deux groupes d'ordre fini $n \in \mathbb{N}^*$ et $\varphi : G \longrightarrow G'$ un isomorphisme. Si $g \in G$ d'ordre k, alors $\varphi(g)$ est d'ordre k dans G'.*

Démonstration : Comme $g^k = e$, ainsi $\varphi(g^k) = [\varphi(g)]^k = e'$, et par suite l'ordre de $\varphi(g)$ divise k. Si $|\varphi(g)| = k' < k$, alors

$$[\varphi(g)]^{k'} = \varphi(g^{k'}) = e' = \varphi(g^k) \quad \text{comme } \varphi \text{ est injective, alors} \quad g^k = g^{k'} = e$$

ceci est absurde car g est d'ordre k. ■

Théorème 1.32.

$$\mathbb{Z}\Big/nm\mathbb{Z} \simeq \mathbb{Z}\Big/n\mathbb{Z} \times \mathbb{Z}\Big/m\mathbb{Z} \Longleftrightarrow n \wedge m = 1.$$

Démonstration : Soit

$$\begin{aligned} f : \quad & \mathbb{Z}\Big/nm\mathbb{Z} \longrightarrow \mathbb{Z}\Big/n\mathbb{Z} \times \mathbb{Z}\Big/m\mathbb{Z} \\ & [k]_{nm} \longmapsto ([k]_n, [k]_m). \end{aligned}$$

"$\Longrightarrow$" On a $[1]_{nm}$ est d'ordre nm dans $\mathbb{Z}\Big/nm\mathbb{Z}$, ainsi $f([1]_{nm})$ est d'ordre nm. Supposons que $d = n \wedge m \neq 1$, ainsi il existe n' et m' tel que

$$n = n'd \qquad \text{et} \qquad m = m'd \qquad \text{avec} \qquad n' \wedge m' = 1.$$

Comme f est un morphisme de groupes, alors

$$n'm'\overline{f}([1]_{nm}) = (m'n[1]_n, n'm[1]_m = ([0]_n, [0]_m).$$

Donc $\overline{f}([1]_{nm})$ est d'ordre $n'm'd$, absurde. D'où $n \wedge m = 1$.
"$\Longleftarrow$" Il est clair que f est un morphisme de groupes et

$$\begin{aligned} \ker(f) =& \{[k]_{nm} \in \mathbb{Z}\Big/nm\mathbb{Z} \,|\, f([k]_{nm}) = ([0]_n, [0]_m)\} \\ &= \{[k]_{nm} \in \mathbb{Z}\Big/nm\mathbb{Z} \,|\, k \in nm\mathbb{Z}\} \qquad \text{car } n \wedge m = 1 \\ &= \{[0]_{nm}\} \end{aligned}$$

et par suite f est injectif, de plus

$$\left|\mathbb{Z}\Big/nm\mathbb{Z}\right| = nm = \left|\mathbb{Z}\Big/n\mathbb{Z} \times \mathbb{Z}\Big/m\mathbb{Z}\right|$$

Donc

$$\mathbb{Z}\Big/nm\mathbb{Z} \simeq \mathbb{Z}\Big/n\mathbb{Z} \times \mathbb{Z}\Big/m\mathbb{Z}.$$

■

Proposition 1.33. *Soient G un groupe, $g \in G$ et*

$$\begin{aligned} \varphi : \quad & (\mathbb{Z}, +) \longrightarrow (G, *) \\ & m \longmapsto g^m \end{aligned}$$

un morphisme de groupes. Alors

1. $Im(\varphi) =< g >$.
2. *Il existe un unique* $n \in \mathbb{N}$ *tel que* $\ker(\varphi) = n\mathbb{Z}$.

Démonstration : Il clair que φ est un morphisme de groupes

1. $Im(\varphi) =< g > \leq G$, engendré par g.
2. On a $\ker(\varphi) \leq \mathbb{Z}$, alors $\ker(\varphi) = n\mathbb{Z}$.

Si $\ker(\varphi) = \{0\}$, alors φ est injective. Ainsi

$$\forall\, (m,p) \in \mathbb{Z}^2 \qquad \text{tel que} \qquad m \neq p \implies g^m \neq g^p,$$

ce qui implique que

$$< g >= \{g^m \,|\, m \in \mathbb{Z}\} \qquad \text{est infini}$$

et par suite

$$< g > \simeq \mathbb{Z}.$$

Si $\ker(\varphi) = n\mathbb{Z}$, avec $n \neq 0$. Donc pour tout $m \in \mathbb{Z}$,

$$g^m = e \iff m \in n\mathbb{Z} \iff \exists\, k \in \mathbb{Z} \quad \text{tel que} \quad m = kn.$$

Soit $m \in \mathbb{Z}$, alors

$$m = kn + r \qquad \text{avec} \qquad 0 \leq r \leq n-1$$

ainsi

$$g^m = g^r,$$

d'où

$$< g >= \{g^k \,|\, 0 \leq k \leq n-1\}$$

donc

$$card(< g >) = n$$

et par suite

$$< g > \simeq \mathbb{Z}\Big/n\mathbb{Z}.$$

■

Exemples. 1. $< 2 > \simeq \mathbb{Z}$.

2. *Pour* $\omega = e^{2i\pi/n}$, *on a* $< \omega > \simeq \mathbb{Z}\Big/n\mathbb{Z}$.
3. *Si* G *est un groupe cyclique d'ordre* n, *alors* $G \simeq \mathbb{Z}\Big/n\mathbb{Z}$.

1.6 Groupes quotients

Définition 1.34. *Un sous-groupe H de G est dit distingué (ou normal ou encore invariant) si* $\forall\, g \in G$

$$gH = Hg \iff ghg^{-1} \in H \quad \forall\, (g,h) \in G \times H$$

on note $H \lhd G$.

Exemples. *1.* $\{e\}$ *et* G *sont toujours distingués dans* G.

2. Si G *est abélien, alors tout sous-groupe de* G *est distingué.*

3. $\varphi : \quad G \longrightarrow G'$ *morphisme de groupes. Alors* $\ker(\varphi) \lhd G$. *En effet :*
Soit $(h,g) \in \ker(\varphi, G)$, *alors*

$$\begin{aligned} \varphi(ghg^{-1}) &= \varphi(g)\varphi(h)\varphi(g^{-1}) \\ &= \varphi(g)[\varphi(g)]^{-1} \\ &= e'. \end{aligned}$$

Donc $ghg^{-1} \in \ker(\varphi)$.

Soient $(G, *)$ un groupe et $H \lhd G$, alors

$$xH * yH = x * y\, H \qquad \forall\, (x,y) \in G^2.$$

On définit ainsi une l.c.i sur l'ensemble les classes modulo H par

$$\overline{x} * \overline{y} = \overline{x * y}.$$

L'ensemble des classes modulo H muni de cette loi est un groupe, appelé **le groupe quotient de** G **par** H, noté G/H de plus

$$\begin{aligned} \Pi : \quad & G \longrightarrow G/H \\ & g \longmapsto \overline{g} = gH \end{aligned}$$

est un morphisme de groupes, appelé surjection canonique de G dans G/H. Remarquons que

$$\Pi(g) = \Pi(g') \iff g^{-1}g' \in H,$$

c'est-à-dire,

$$\ker(\Pi) = H.$$

Théorème 1.35. *Soit* $H \leq G$. *Les propriétés suivantes sont équivalentes*

1. $H \lhd G$.

2. $\forall\, g \in G$, *on a* $gHg^{-1} = H$.

3. $\forall\, g \in G$, *on a* $gHg^{-1} \subset H$.

4. H *est le noyau d'un morphisme de groupes* φ *de* G *dans* G'. ($\varphi = \Pi$, $G' = G/H$)

Remarques. *1. Si G abélien et $H \leq G$, alors $H \lhd G$ et G/H est abélien.*

2. Soient $H \leq G$ et $K \leq G$ tel que $H \subset K$. Si $H \lhd G$, alors $H \lhd K$.

Théorème 1.36. *(Premier théorème d'isomorphisme) Soient G, G' deux groupes et*

$$\varphi : \quad G \longrightarrow G'$$

un morphisme de groupes. Alors

$$G\Big/\ker(\varphi) \simeq Im(\varphi).$$

Démonstration : Soient $H = \ker(\varphi)$ et

$$\begin{aligned} \overline{\varphi} : \quad & G\Big/H \longrightarrow G' \\ & \overline{x} = xH \longmapsto \overline{\varphi}(\overline{x}) = \varphi(x) \end{aligned}$$

i) $\overline{\varphi}$ bien définie, en effet :
Si $\overline{x} = \overline{y}$, alors $\overline{\varphi}(\overline{x}) = \overline{\varphi}(\overline{y})$, et par suite $\overline{\varphi}(\overline{xy}^{-1}) = e'$, ainsi $\varphi(xy^{-1}) = e'$, d'où $xy^{-1} \in \ker(\varphi) = H$. Donc

$$x \in yH \implies x = yx' \quad \text{avec} \quad x' \in H \implies \varphi(x) = \varphi(y).$$

ii) $\overline{\varphi}$ injectif : soit $xH \in \ker(\overline{\varphi})$, alors

$$\overline{\varphi}(xH) = \varphi(x) = e'$$

ce qui implique que $x \in \ker(\varphi) = H$, et par suite

$$xH = H \qquad \text{qui est l'élément neutre de } G\Big/H.$$

iii) $\overline{\varphi}$ surjectif, soit $y \in Im(\varphi) = \varphi(G)$, alors il existe $x \in G$ tel que

$$y = \varphi(x) = \overline{\varphi}(xH).$$

Donc

$$\overline{\varphi} : \quad G\Big/H \longrightarrow Im(\varphi) \qquad \text{est un isomorphisme.}$$

■

Exemple.

$$\mathcal{S}_n\Big/\mathcal{A}_n \simeq \{-1, 1\} \simeq \mathbb{Z}\Big/2\mathbb{Z}.$$

Théorème 1.37. *(Deuxième théorème d'isomorphisme) Soient G un groupe, $H \lhd G$ et $K \leq G$. Alors*

1. *$H \cap K \lhd K$.*
2. *$K\Big/H \cap K \simeq KH\Big/H$.*

Démonstration : 1) Comme $H \leq G$ et $K \leq G$, alors $H \cap K \leq K$. On a

$$khk^{-1} \in K \qquad \forall\, (h,k) \in H \cap K \times K.$$

Comme $H \lhd G$ et $k \in K \subset G$, alors

$$khk^{-1} \in H,$$

et par suite

$$H \cap K \lhd K.$$

2) Montrons que

$$KH = \{kh \,|\, k \in K \text{ et } h \in H\} \leq G?$$

On a $KH \neq \emptyset$ car $H \leq G$ et $K \leq G$. Soient $k_1h_1 \in KH$ et $k_2h_2 \in KH$, montrons que $k_1h_1(k_2h_2)^{-1} \in KH$, on a

$$\begin{aligned} k_1h_1(k_2h_2)^{-1} = k_1h_1{h_2}^{-1}{k_2}^{-1} &= k_1h_1{k_2}^{-1}(k_2{h_2}^{-1}{k_2}^{-1}) \\ &= \underbrace{k_1{k_2}^{-1}}_{\in K}\underbrace{(k_2h_1{k_2}^{-1})}_{\in H}\underbrace{(k_2{h_2}^{-1}{k_2}^{-1})}_{\in H} \\ &\in KH. \end{aligned}$$

Donc $KH \leq G$. Montrons que $H \lhd KH$, tout d'abord, on a $H \leq KH$. Soit $(kh, h') \in KH \times H$, alors

$$khh'(kh)^{-1} = \underbrace{k}_{\in G}\underbrace{hh'h^{-1}}_{\in H}\underbrace{k^{-1}}_{\in G}$$

or $H \lhd G$, et par suite $khh'(kh)^{-1} \in H$, d'où

$$H \lhd KH.$$

Comme

$$\begin{aligned} j: \quad K &\longrightarrow KH \\ k &\longmapsto k \end{aligned}$$

est un morphisme de groupes injectif et

$$\begin{aligned} \sigma: \quad KH &\longrightarrow KH\Big/H \\ x &\longmapsto \overline{x} = xH \end{aligned}$$

est un morphisme de groupes, alors

$$\begin{aligned} f = \sigma \circ j: \quad K &\longrightarrow KH\Big/H \\ k &\longmapsto \overline{k} = kH \end{aligned}$$

est un morphisme de groupes. Soit $k \in \ker(f)$, alors $f(k) = kH \in H \iff k \in H$. Donc

$$k \in H \cap K.$$

f est surjectif car $(kh)H \in KH\big/H$ avec $k \in K$ et $h \in H$, ona

$$khH = f(k).$$

Ainsi le Premier théorème d'isomorphisme, implique que

$$K\big/H \cap K \simeq KH\big/H.$$

■

Théorème 1.38. *(Troisième théorème d'isomorphisme) Soient G un groupe, $H \lhd G$ et $K \lhd G$ tel que $K \subset H$. Alors*

1. $H\big/K \lhd G\big/K$.
2. $(G/K)\big/(H/K) \simeq G\big/H$.

Démonstration :

$$\begin{aligned} \varphi : \quad & G\big/K \longrightarrow G\big/H \\ & \overline{g} = gK \longmapsto gKH = gH \end{aligned}$$

est un morphisme de groupes avec $\ker(\varphi) = H\big/K \lhd G\big/K$, de plus φ est surjectif, ainsi le premième théorème d'isomorphisme, implique que

$$(G/K)\big/(H/K) \simeq G\big/H.$$

■

1.6.1 Sous-groupe d'un groupe quotient

Soient G un groupe, $H \lhd G$ et Π la surjection canonique

$$\begin{aligned} \Pi : \quad & G \longrightarrow G/H \\ & g \longmapsto \overline{g} = gH \end{aligned}$$

qui est un morphisme de groupes. Donc l'image d'un sous-groupe de G par Π est un sous-groupe de G/H.

Théorème 1.39. *1. Les sous-groupes de G contenant H sont en bijection par Π avec les sous-groupes de G/H.*

2. Les sous-groupes distingués de G contenant H sont en bijection par Π avec les sous-groupes distingués de G/H.

Démonstration : 1) Π définie sur l'ensemble des sous-groupes de G contenant H est injective. En effet :
Soient $H \subset H_1 \leq G$ et $H \subset H_2 \leq G$ tel que $\Pi(H_1) = \Pi(H_2)$, montrons que $H_1 = H_2$.

Pour tout $h_1 \in H_1$, il existe $h_2 \in H_2$ tel que $\Pi(h_1) = \Pi(h_2)$, ainsi $h_1 h_2^{-1} \in \ker(\Pi) = H$, et par suite $h_1 \in Hh_2 \subset H_2$. Donc

$$H_1 \subset H_2.$$

De même on montre que $H_2 \subset H_1$. D'où

$$H_1 = H_2.$$

Comme Π est un morphisme de groupes, alors l'image réciproque d'un sous-groupe de G/H est un sous-groupe de G. Soit $\overline{H} \leq G/H$, comme Π est surjective (donc inversible à droite), alors

$$\overline{H} = \Pi\big(\underbrace{\Pi^{-1}(\overline{H})}_{\leq G}\big).$$

Montrons que $H \subset \Pi^{-1}(\overline{H})$?
On a $\overline{H}$ contient l'élément neutre de G/H, noté $e_{G/H}$. Ainsi $\Pi^{-1}(\overline{H})$ contient $\Pi^{-1}(e_{G/H}) = \ker(\Pi) = H$. Donc Π est une bijection entre l'ensemble des sous-groupes de G contenant H et les sous-groupes de G/H.
2) Soit $H_1 \lhd G$ tel que $H \subset H_1$. Montrons que $\Pi(H_1) \lhd G/H$?
Comme Π est un morphisme de groupes, alors

$$\Pi(H_1) \leq G/H.$$

Soient $h_1 \in H_1$ et $g \in G$. Montrons que

$$gH\Pi(h_1)(gH)^{-1} \in \Pi(H_1)?$$

on a

$$gH\Pi(h_1)(gH)^{-1} = \Pi(g)\Pi(h_1)[\Pi(g)]^{-1} = \Pi(gh_1g^{-1}) \in \Pi(H_1) \qquad \text{car} \qquad H_1 \lhd G.$$

Soit $\overline{H_1} \lhd G/H$ et $H_1 = \Pi^{-1}(\overline{H_1})$, on a $H_1 \leq G$ tel que $H \subset H_1$ (d'après 1). Montrons que $H_1 \lhd G$?
Soit $(h_1, g) \in H_1 \times G$, comme

$$\Pi(gh_1g^{-1}) = \Pi(g)\Pi(h_1)[\Pi(g)]^{-1} \in \overline{H_1}$$

car $\overline{H_1} \lhd G/H$, alors

$$gh_1g^{-1} \in H_1 \implies H_1 \lhd G.$$

■

Exemple. *Les sous-groupes de* $\mathbb{Z}/4\mathbb{Z}$ *sont en bijection avec les sous-groupes de* $\mathbb{Z}$ *contenant* $4\mathbb{Z}$. *Or les sous-groupes de* $\mathbb{Z}$ *contenant* $4\mathbb{Z}$: $4\mathbb{Z}$, $\{0\}$, $\mathbb{Z}$, *et* $2\mathbb{Z}$, *et par suite les sous-groupes de* $\mathbb{Z}/4\mathbb{Z}$: $\mathbb{Z}/4\mathbb{Z}$, $2\mathbb{Z}/4\mathbb{Z}$ *et* $4\mathbb{Z}/4\mathbb{Z}$.

Proposition 1.40. *Soient G un groupe, $H \lhd G$ et $K \leq G$, alors*

$$HK \leq G, \quad H \subset HK, \quad H \lhd HK \quad et \quad \Pi(K) = HK\big/H.$$

Démonstration : Comme $H \lhd G$, alors

$$k^{-1}hk \in H \quad \forall\, (h,k) \in H \times K,$$

alors

$$\Pi(k^{-1}hk) = e_{G/H} \quad \text{car} \quad \ker(\Pi) = H$$

et par suite

$$\Pi(k) = \Pi(hk),$$

d'où

$$\Pi(K) = \Pi(HK).$$

Par définition

$$\begin{aligned}\Pi(HK) = \{\Pi(hk) \,|\, (h,k) \in H \times K\} =& \{hkH \,|\, (h,k) \in H \times K\} \\ &= HK\big/H.\end{aligned}$$

Donc

$$\Pi(K) = \Pi(HK) = HK\big/H.$$

■

Groupe simple

Définition 1.41. *Un groupe G est dit simple s'il n'a pas d'autres sous-groupes distingués que $\{e\}$ et G.*

Exemple. *Les seuls groupes abéliens simples sont les groupes cycliques d'ordre premier.*

Définition 1.42. *Soit G un groupe, on appelle centre de G, et on noté $Z(G)$ le sous-groupe*

$$Z(G) = \{z \in G \,|\, zg = gz, \forall\, g \in G\}.$$

Exemple.

$$Z(\mathcal{S}_n) = \begin{cases} \mathcal{S}_2, & si \quad n = 2 \\ \{Id\}, & si \quad n \geq 3. \end{cases}$$

En effet : pour $n = 2$ évident. Pour $n \geq 3$, soit $\sigma \in \mathcal{S}_n \setminus \{Id\}$ alors il existe $i \neq j$ tel que $\sigma(i) = j$. Comme $n \geq 3$, alors il existe $k \neq i$, $k \neq j$ et par suite

$$\sigma \circ \tau_{jk} \neq \tau_{jk} \circ \sigma.$$

Remarques. *1. $Z(G) \lhd G$.*

2. G abélien $\Longleftrightarrow Z(G) = G$.

1.6.2 Normalisateur et centralisateur d'une partie

Définition 1.43. *Soient G un groupe, $H \leq G$ et S une partie de G. Le normalisateur de S dans H*

$$N_H(S) = \{h \in H \,|\, hSh^{-1} = S\} \qquad \textit{(i.e, } hsh^{-1} \in S \textit{ pour tout } s \in S.\textit{)}$$

Le centralisateur de S dans H

$$C_H(S) = \{h \in H \,|\, hs = sh, \forall\, s \in S\}.$$

Proposition 1.44. *Soient G un groupe, $H \leq G$ et S une partie de G. Alors*

1. *$N_H(S) \leq H$ $(\leq G)$.*
2. *$C_H(S) \leq H$ $(\leq G)$.*
3. *$C_H(S) \lhd N_H(S)$.*

Démonstration : 1) Comme $e_G \in N_H(S)$, alors $N_H(S) \neq \emptyset$. Soit $(h_1, h_2) \in [N_H(S)]^2$, montrons que $h_1 {h_2}^{-1} \in N_H(S)$, i.e,

$$h_1 {h_2}^{-1} s h_2 {h_1}^{-1} \in S?$$

On a,

$$h_2 s {h_2}^{-1} = t \in S$$

et par suite

$${h_2}^{-1} t h_2 = s \in S$$

ainsi

$$h_1 s {h_1}^{-1} = h_1 {h_2}^{-1} t h_2 {h_1}^{-1} = h_1 {h_2}^{-1} h_2 s {h_2}^{-1} h_2 {h_1}^{-1} \in S.$$

Donc

$$N_H(S) \leq H.$$

2) Comme $e_G \in C_H(S)$, alors $C_H(S) \neq \emptyset$. Soit $(h_1, h_2) \in [C_H(S)]^2$, montrons que $h_1 {h_2}^{-1} \in C_H(S)$, i.e,

$$h_1 {h_2}^{-1} s = s h_1 {h_2}^{-1} \in S?$$

Comme

$$h_1 s = s h_1 \quad \text{et} \quad h_2 s = s h_2,$$

alors

$$h_1 {h_2}^{-1} s h_2 = h_1 s = s h_1$$

ainsi

$$h_1 {h_2}^{-1} s = s h_1 {h_2}^{-1}$$

et par suite

$$h_1 {h_2}^{-1} \in C_H(S).$$

Donc

$$C_H(S) \leq H.$$

Comme $C_H(S) \subset N_H(S)$, alors $C_H(S) \leq N_H(S)$. Montrons que

$C_H(S) \lhd N_H(S)$? (i.e, $hh_1h^{-1}s(hh_1h^{-1})^{-1} = s$, $\forall\ (h, h_1, s) \in N_H(S) \times C_H(S) \times S$),

on a

$$\begin{aligned} hh_1h^{-1}s(hh_1h^{-1})^{-1} = hh_1h^{-1}shh_1{}^{-1}h^{-1} &= hh_1(\underbrace{h^{-1}sh}_{=s'})h_1{}^{-1}h^{-1} \\ &= hh_1s'h_1{}^{-1}h^{-1} \\ &= hs'h^{-1} \quad \text{car } h_1 \in C_H(S) \\ &= hh^{-1}shh^{-1} \\ &= s. \end{aligned}$$

Donc

$$C_H(S) \lhd N_H(S).$$

■

Proposition 1.45. *Soient G un groupe et $H \leq G$. Alors*

1. $H \lhd N_G(H) = \{g \in G \,|\, gH = Hg\}$.
2. $H \lhd G \iff N_G(H) = G$.

1.7 Série numéro I

Exercice 1 : Soient G un groupe et $(x, y) \in G^2$.
1. Montrer que xy et yx ont même ordre.
2. Soient x d'ordre p et y d'ordre q tel que $xy = yx$.
   — On suppose p et q premiers entre eux. Montrer que $ord(xy) = pq$.
   — On ne suppose plus p et q premiers entre eux. A-t-on $ord(xy) = ppcm(p, q)$?
3. On définit l'exposant d'un groupe fini G, noté $\exp(G)$, comme le plus petit entier $n \geq 1$ tel que $g^n = e$, pour tout élément $g \in G$. Montrer qu'il existe $z \in G$ tel que $\exp(G) = ord(z)$ lorsque G est abélien.

Exercice 2 : Soient G un groupe, H un sous-groupe de G et $g \in G$. Montrer que

$$gH = \{ghg^{-1} \,|\, h \in H\}$$

est un sous-groupe de G.

Exercice 3 : On appelle centre d'un groupe G la partie $Z(G)$ de G définie par

$$Z(G) = \{g \in G \,|\, gx = xg,\ \forall\, x \in G\}.$$

1. Montrer que $Z(G)$ est un sous-groupe de G.
2. Montrer que si G possède un unique élément d'ordre 2, alors cet élément est dans $Z(G)$.

Exercice 4 : Soient $(G, *)$ un groupe et H une partie finie non vide de G stable pour $*$. Soient $h \in H$ et

$$\begin{aligned} \varphi : \quad & \mathbb{N} \longrightarrow H \\ & n \longmapsto h^n \end{aligned}$$

une application. Montrer que φ n'est pas injective. En déduire que $h^{-1} \in H$ puis que H est un sous-groupe de G.

Exercice 5 : Soit H_8 le sous-groupe de $GL_2(\mathbb{C})$ engendré par les matrices

$$I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \qquad \text{et} \qquad K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}.$$

1. Montrer que H_8 est un groupe d'ordre 8, non commutatif.
2. Déterminer les sous-groupes de H_8. Lesquels sont cycliques ? Distingués dans H_8.

Exercice 6 : Soit $(B, \circ)$ le groupe des bijections de $\mathbb{C}$ sur $\mathbb{C}$ et n un entier supérieur ou égal à 3. On désigne par r et s les deux éléments de B définis par

$$r(z) = ze^{2i\pi/n} \qquad \text{et} \qquad s(z) = \overline{z}.$$

1. Montrer que $r^n = Id_{\mathbb{C}}$, $s^2 = Id_{\mathbb{C}}$, $r \circ s \circ r = s$ et que pour tout $p \in \mathbb{Z}$, $r^p \circ s \circ r^p = s$.
2. Démontrer que

$$\mathbb{D} = \{r^k \circ s^\ell \,|\, k, \ell \in \mathbb{Z}\}$$

est un sous-groupe de B et en déduire que tout élément de $\mathbb{D}$ peut s'écrire de manière unique

$$r^k \circ s^\ell \qquad \text{avec} \qquad 0 \leq k \leq n-1 \quad \text{et} \quad 0 \leq \ell \leq 1.$$

Quel est l'ordre de $\mathbb{D}$ (le groupe $\mathbb{D}_n$ est appelé groupe diédral).
3. Montrer que $\mathbb{D}_3$ est isomorphe à S_3.

Exercice 7 : Soit E un ensemble non vide, on note $S(E)$ l'ensemble des permutations des éléments de E, c'est-à-dire, des bijections de E sur lui-même.
1. Montrer que $(S(E), \circ)$ est un groupe non abélien dès que $\text{card}(E) \geq 3$.
2. Pour $n \in \mathbb{N}^*$, on note S_n le groupe symétrique de $E = \{1, \cdots, n\}$. On dit que S_n est le groupe symétrique d'ordre n. On peut représenter un élément σ de S_n par la notation

$$\sigma = \begin{pmatrix} 1 & 2 \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

Montrer que S_n est d'ordre $n!$.
3. Le support d'une permutation $\sigma \in S_n$: $supp(\sigma) := \{1 \leq k \leq n \,|\, \sigma(k) \neq k\}$. On dit qu'une permutation $\sigma \in S_n$ est un cycle de longueur r (σ est r-cycle) on note $\sigma = (i_1, i_2, \cdots, i_r)$, si $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3, \cdots \sigma(i_r) = i_1$ (avec $i_k \neq i_l$ pour $k \neq l$) et σ laisse tout autre entier invariant. Un 2-cycle s'appelle transposition.

- Montrer que deux permutations de supports disjoints commutent.
- Soit σ un r-cycle, montrer que $\sigma^r = Id$.
- Montrer que toute permutation est un produit de cycles à supports disjointes. Calculer σ^{2015}, avec $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 7 & 1 & 5 & 12 & 6 & 3 & 9 & 4 & 2 & 11 & 8 & 10 \end{pmatrix}$.
- Montrer que toute permutation est un produit de transpositions.

4. Soit $\sigma \in S_n$, on appelle signature de σ,

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j} = \pm 1.$$

- Montrer que $\varepsilon(\sigma_1 \sigma_2) = \varepsilon(\sigma_1)\varepsilon(\sigma_2)$.
- Calculer la signature d'une transposition.
- Soit $A_n = \{\sigma \in S_n \,|\, \varepsilon(\sigma) = 1\}$. Montrer que A_n est un sous-groupe de S_n (A_n groupe alterné).
- Pour $n \geq 3$, montrer que A_n est engendré par les 3-cycles.

Exercice 8 :
1. Montrer que tout sous-groupe d'un groupe cyclique est cyclique.
2. Soit $n \geq 1$. Montrer que pour tout diviseur $d \geq 1$ de n il existe un unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d.

Exercice 9 : Soit G un groupe.
1. Montrer que si l'application $x \mapsto x^{-1}$ est un endomorphisme de G, alors G est commutatif.
2. Soit $n \geq 1$ un entier tels que l'application $x \mapsto x^n$ est un automorphisme de G. Montrer

que $\forall\, x \in G$, $x^{n-1} \in Z(G)$.

Exercice 10 : 1. Donner la liste des sous-groupes de $\mathbb{Z}$, puis de $\mathbb{Z}/n\mathbb{Z}$.
2. Montrer qu'un groupe est monogène si et seulement s'il est isomorphe soit à $\mathbb{Z}$, soit à $\mathbb{Z}/n\mathbb{Z}$ pour un entier non nul n.

Exercice 11 : 1. Montrer que l'ordre d'un élément dans un groupe est invariant par isomorphisme.
2. Montrer que $\mathbb{Z}/nm\mathbb{Z}$ isomorphe à $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ si et seulement si $n \wedge m = 1$.

Exercice 12 : Soient G un groupe fini et H un sous-groupe de G. Montrer que si $[G : H] = 2$, alors H est distingué dans G.

Exercice 13 : Soient G un groupe et A une partie non vide de G. On pose

$$N_A = \{(g_1 a_1 g_1^{-1}) \cdots (g_n a_n g_n^{-1}) \,|\, n \in \mathbb{N},\ \forall\, 1 \leq i \leq n,\ g_i \in G \text{ et } (a_i \in A \text{ ou } a_i^{-1} \in A)\}.$$

1. Montrer que N_A est un sous-groupe distingué de G contenant A.
2. Montrer que N_A est le plus petit sous-groupe distingué de G contenant A. N_A est appelé sous-groupe distingué engendré par A.

Exercice 14 : Soient G un groupe, H un sous-groupe distingué de G et f un automorphisme de G.
1. Montrer que $f(H)$ est un sous-groupe distingué de G.
2. Montrer que les groupes G/H et $G/f(H)$ sont isomorphes.

Exercice 15 : Soit G un groupe. On appelle sous-groupe dérivé de G, noté $D(G)$ le sous-groupe engendré par les commutateurs de G, c'est-à-dire par les éléments

$$[x, y] = xyx^{-1}y^{-1} \in G \qquad \text{lorsque } x \text{ et } y \text{ parcourent } G.$$

1. $D(G) = \{e\}$ si et seulement si G est commutatif.
2. Montrer que pour tout endomorphisme f de G, on a $f(D(G)) \subset D(G)$.
3. Montrer que $D(G)$ est un sous-groupe distingué de G.
4. Montrer que le groupe quotient $G/D(G)$ est commutatif.
5. Soit H un sous-groupe distingué de G. Montrer que G/H est abélien si et seulement si $D(G) \subset H$.
6. Soient G' un groupe abélien et $f : G \longrightarrow G'$ un morphisme de groupe. Montrer que $D(G) \subset \ker(f)$.
7. En déduire qu'il existe un unique morphisme $\widetilde{f} : G/D(G) \longrightarrow G'$ tel que $f = \widetilde{f} \circ \Pi$ où $\Pi : G \longrightarrow G/D(G)$ est la surjection canonique.
8. Déterminer $D(S_n)$.

Exercice 16 : Un sous-groupe H de G est dit caractéristique si pour tout automorphisme φ de G, $\varphi(H) = H$.
1. Montrer que $D(G)$ est un sous-groupe caractéristique de G.

2. Montrer que tout sous-groupe caractéristique de G est distingué dans G.
3. Soient H un sous-groupe de G et K un sous-groupe de H. Montrer que si K est caractéristique dans H et si H est caractéristique dans G alors K est caractéristique dans G.
4. Soient N un sous-groupe distingué de G et H un sous-groupe de N. Montrer que si H est caractéristique dans N alors H est un sous-groupe distingué de G.

Exercice 17 : Soient G_1 et G_2 deux groupes, H_1 un sous-groupe distingué de G_1 et H_2 un un sous-groupe distingué de G_2.
1. Montrer que $H_1 \times H_2$ est un sous-groupe distingué de $G_1 \times G_2$.
2. Montrer que $G_1 \times G_2 \Big/ H_1 \times H_2$ est isomorphe à $G_1/H_1 \times G_2/H_2$.

Exercice 18 : Soit A l'ensemble des applications affines de $\mathbb{R}$ c'est à dire l'ensemble des applications de la forme $(x \longmapsto ax + b)$ avec a réel non nul et b réel.
1. Montrer que A est un groupe pour la composition des applications.
2. Soit N l'ensemble des applications de la forme $(x \longmapsto x + b)$ avec b réel. Montrer que N est un sous-groupe distingué de A.
3. Montrer que A/N est isomorphe à $\mathbb{R}^*$.

1.8 Correction

Exercice 1 : 1. Si $ord(xy) = n < \infty$. Montrons que $ord(yx) = n$.
Nous avons

$$\underbrace{(xy)\cdots(xy)}_{n \text{ fois}} = e$$

cela peut encore s'écrire

$$x\underbrace{(yx)\cdots(yx)}_{n-1 \text{ fois}}y = e$$

ensuite en multipliant à gauche par x^{-1} et à droite par x, nous trouvons

$$\underbrace{(yx)\cdots(yx)}_{n \text{ fois}} = e.$$

Nous avons ainsi prouvé que si

$$(xy)^n = e \qquad \Longrightarrow (yx)^n = e$$

de même si

$$(yx)^m = e \qquad \Longrightarrow (xy)^m = e.$$

D'où

$$ord(xy) = ord(yx) = n.$$

De même dans le cas infini.
2. i) Soit $r = ord(xy)$. Ayant

$$(xy)^{pq} = (x^p)^q(y^q)^p = e,$$

d'où r divise pq. En outre

$$e = \Big((xy)^r\Big)^p = (x^p)^r y^{rp} = y^{rp}$$

et par suite q divise rp, or p est premier avec q donc q divise r. De façon similaire p divise r, à nouveau puisque $p \wedge q = 1$, alors pq divise r. D'où $r = pq$.
ii) Clairement non. Un contre-exemple est donné en considérant un élément x d'ordre $p \neq 1$ et $y = x^{-1}$, également d'ordre p. Alors $ord(xy) = 1 \neq n = ppcm(p, p)$.
3. Posons

$$M = ppcm\{ord(g) \,|\, g \in G\},$$

ainsi

$$g^M = e \quad \forall\, g \in G.$$

On a

$$M = \prod_{i=1}^{n} p_i^{a_i} \qquad \text{avec } p_i \text{ premier et } a_i \in \mathbb{N}^*$$

et par définition de M il existe $g_i \in G$ pour tout $1 \leq i \leq n$ tel que

$$ord(g_i) = p_i^{a_i} q_i \qquad \text{avec } p_i \text{ premier à } q_i.$$

Alors

$$z = \prod_{i=1}^{n} g_i^{q_i} \qquad \text{est d'ordre } M \text{ d'après 2).}$$

Exercice 2 : Aucune difficulté.

Exercice 3 :

1. Aucune difficulté.
2. Soit $g \in G$ l'unique élément d'ordre 2. Comme

$$\left(x^{-1}gx\right)^2 = e \qquad \forall\, x \in G$$

alors

$$x^{-1}gx = g.$$

Exercice 4 : Si φ est injective, alors H est infini absurde.
Comme φ n'est pas injective, alors il existe $(n, m) \in \mathbb{N}^2$ tels que $m > n$ et $h^m = h^n$, alors

$$h^{m-n-1}h = e,$$

soit

$$h^{-1} = h^{m-n-1} \in H.$$

D'où H est un sous-groupe de G.

Exercice 5 :

1. Le calcul des produits de deux éléments quelconques, nous donne les relations

$$I^2 = J^2 = K^2 = -I, \quad IJ = K, \quad IK = -J, \quad JI = -K,$$
$$KI = J, \quad JK = I \quad \text{et} \quad KJ = -I$$

ainsi

$$H_8 = \{I_2, I, J, K, -I_2, -I, -J, -K\}.$$

2. Il y a bien sûr le sous-groupe trivial

$$H_8 \quad \text{et} \quad \{I_2\}.$$

Le sous-groupe d'ordre 2

$$Z(H_8) = \{I_2, -I_2\}.$$

Trois sous-groupes d'ordre 4 engendrés par : I, J et K. Notons que ces sous-groupes sont respectivement ceux engendrés par $-I$, $-J$ et $-K$. Enfin, un sous-groupe engendré par deux éléments distincts a et b avec $a \neq -b$ ($a = I$ et $b = -K$) est H_8.
Donc tous les sous-groupes propres étaient cycliques. Dans n'importe quel groupe le centre est distingué. Remarquons que les sous-groupes d'ordre 4 sont d'indices 2, ce qui nous dit directement qu'ils sont distingués.

Exercice 6 :
1. Aucune difficulté.
2. On a $Id_{\mathbb{C}} \in \mathbb{D}$, ($k = n$ et $\ell = 2$) ainsi $\mathbb{D} \neq \emptyset$. Soit

$$(r^{k_1} \circ S^{\ell_1}, r^{k_2} \circ S^{\ell_2}) \in \mathbb{D}^2$$

alors

$$r^{k_1} \circ S^{\ell_1} \circ \left(r^{k_2} \circ S^{\ell_2}\right)^{-1} = r^{k_1} \circ S^{\ell_1} \circ S^{-\ell_2} \circ r^{-k_2} = r^{k_1} \circ S^{\ell_1 - \ell_2} \circ r^{-k_2}.$$

Comme

$$S^{\ell_1 - \ell_2} = \begin{cases} Id_{\mathbb{C}}, & \text{si} \quad \ell_1 - \ell_2 \in 2\mathbb{Z} \\ S, & \text{sinon,} \end{cases}$$

et par suite

$$r^{k_1} \circ S^{\ell_1 - \ell_2} \circ r^{-k_2} = \begin{cases} r^{k_1 - k_2}, & \text{si} \quad \ell_1 - \ell_2 \in 2\mathbb{Z} \\ r^{k_1} \circ S \circ r^{-k_2}, & \text{sinon} \end{cases} = \begin{cases} r^{k_1 - k_2}, & \text{si} \quad \ell_1 - \ell_2 \in 2\mathbb{Z} \\ r^{k_1 + k_2} \circ S, & \text{sinon.} \end{cases}$$

Donc

$$r^{k_1} \circ S^{\ell_1} \circ \left(r^{k_2} \circ S^{\ell_2}\right)^{-1} \in \mathbb{D},$$

d'où $\mathbb{D}$ est un sous-groupe de B.
Supposons qu'il existe $0 \leq k < \ell \leq n-1$ tel que

$$r^k \circ S = r^\ell \implies r^{\ell - k} = S \implies r^{2(\ell - k)} = S^2 = Id_{\mathbb{C}}$$

or

$$2 \leq 2(\ell - k) \leq 2n - 2$$

d'où

$$2(\ell - k) = n$$

et par suite

$$\overline{z} = -z$$

absurde. $\mathbb{D}_n$ est d'ordre $2n$.
3. Soient (ABC) triangle équilatéral, o son centre de gravité et R la rotation de centre o est d'angle $2\pi/3$. On a

$$S_3 = \{Id, \tau_{AB}, \tau_{AC}, \tau_{BC}, (ABC), (ACB)\}.$$

Soit

$$s_1,\ s_2 \text{ et } s_3 \qquad \text{les réflexions par rapport aux trois médianes}$$

ainsi

$$\mathbb{D}_3 = \{Id, R, R^2, s_1, s_2, s_3\}$$

et

$$\psi : S_3 \longrightarrow \mathbb{D}_3$$

$\psi(Id) = Id$, $\psi(\tau_{AB}) = s_1$, $\psi(\tau_{AC}) = s_2$, $\psi(\tau_{BC}) = s_3$, $\psi((ABC)) = R$ et $\psi((ACB)) = R^2$ est un isomorphisme.

Exercice 7 :
1. $\circ$ est une l.c.i : associative, Id_E, l'élément neutre, $f^{-1} \in \mathcal{S}(E)$. $(\mathcal{S}(E), \circ)$ n'est pas commutatif dès que $card(E) \geq 3$:

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \text{et} \qquad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \qquad \text{on a} \quad \sigma_1 \circ \sigma_2 \neq \sigma_2 \circ \sigma_1.$$

2. Par récurrence sur n.
3. i) Soit $(\sigma_1, \sigma_2) \in S_n^2$ deux permutations à supports disjoints. Soit $i \in \{1, \cdots, n\}$, nous voulons montrer que $\sigma_1 \circ \sigma_2(i) = \sigma_2 \circ \sigma_1(i)$. Il y a trois cas :
a) Si $i \in supp(\sigma_1)$, alors $\sigma_2(i) = i$ de plus $\sigma_1(i) \in supp(\sigma_1)$. Donc $\sigma_1 \circ \sigma_2(i) = \sigma_1(i) = \sigma_2 \circ \sigma_1(i)$.
b) Si $i \in supp(\sigma_2)$, on conclut de même que $\sigma_2 \circ \sigma_1(i) = \sigma_2(i) = \sigma_1 \circ \sigma_2(i)$.
c) Si $i \notin supp(\sigma_1) \cup supp(\sigma_2)$, alors $\sigma_2 \circ \sigma_1(i) = \sigma_1 \circ \sigma_2(i) = i$.
ii) Soit $\sigma = (i_1, \cdots, i_r)$ un r-cycle, on a

$$i_j \xrightarrow{\sigma} i_{j+1} \cdots i_r \xrightarrow{\sigma^{r-j+1}} i_1 \cdots \xrightarrow{\sigma^r} i_j$$

iii) Soit $\sigma \neq Id$. Il existe $i_1 \in \{1, \cdots, n\}$ tel que $\sigma(i_1) \neq i_1$. Pour $j \geq 2$, on pose $i_j = \sigma(i_{j-1})$. Soit k le plus petit entier tel que

$$i_{k+1} = \sigma(i_k) \in \{i_1, i_2, \cdots, i_k\}.$$

On doit avoir $\sigma(i_k) = i_1$, car sinon $\sigma(i_k) = i_j$, où $2 \leq j \leq k$, mais alors on aurait $\sigma(i_k) = \sigma(i_{j-1}) = i_j$ et $i_{j-1} \neq i_k$, ce qui contredit l'injectivité de σ. On obtient alors un cycle $\alpha_1 = (i_1, \cdots, i_k)$ de longueur k. La restriction de σ à $\{1, \cdots, n\} \setminus \{i_1, \cdots, i_k\}$ est une permutation. Par récurrence sur n, on peut écrire cette restriction comme le produit de cycles deux à deux disjoints $\alpha_2 \cdots \alpha_r$. Ces cycles sont aussi deux à deux disjoints avec α_1.
iv) On voit que

$$(i_1, \cdots, i_k) = (i_1, i_k)(i_1, i_{k-1}) \cdots (i_1, i_2).$$

4. i) On a

$$\begin{aligned} \varepsilon(\sigma_1 \circ \sigma_2) &= \prod \frac{\sigma_1\big(\sigma_2(i)\big) - \sigma_1\big(\sigma_2(j)\big)}{i - j} \\ &= \prod \frac{\sigma_1\big(\sigma_2(i)\big) - \sigma_1\big(\sigma_2(j)\big)}{\sigma_2(i) - \sigma_2(j)} \, \frac{\sigma_2(i) - \sigma_2(j)}{i - j} \\ &= \prod \frac{\sigma_1(i) - \sigma_1(j)}{i - j} \prod \frac{\sigma_2(i) - \sigma_2(j)}{i - j} \\ &= \varepsilon(\sigma_1)\varepsilon(\sigma_2). \end{aligned}$$

ii) évidant.
iii) On a

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

est un morphisme de groupes surjectif et

$$A_n = \ker(\varepsilon).$$

iv) Soit $\sigma \in A_n$ par définition de la signature,σ s'écrit donc comme un produit pair de transpositions. Or, on remarque que tout produit de deux transpositions est un produit de 3-cycle :

$$(a,b)(b,c) = (a,b,c)$$
$$(a,b)(a,c) = (a,c,b)$$
$$(a,b)(c,d) = (a,b)(b,c)(b,c)(c,d) = (a,b,c)(b,c,d).$$

Exercice 8 :

1. Comme G est cyclique, alors il existe $x \in G$ tel que

$$G = < x > .$$

Soit $H \leq G$ non trivial, soit n le plus petit entier strictement positif tel que $x^n \in H$, alors

$$< x^n > \subset H.$$

Soit $y \in H \subset G$, donc $y = x^k$ or

$$k = qn + r \qquad \text{avec} \quad 0 \leq r < n,$$

et par suite

$$yx^{-nq} = x^r \implies r = 0$$

d'où $y \in < x^n >$, ainsi

$$H = < x^n > .$$

2. Comme d divise n, alors

$$G_d = \{k(\overline{\frac{n}{d}}) \,|\, k \in \mathbb{Z}\} = < (\overline{\frac{n}{d}}) > \leq \mathbb{Z}/n\mathbb{Z}$$

d'ordre d. Par la question précédente il est isomorphe à $\mathbb{Z}/d\mathbb{Z}$ car $\mathbb{Z}/n\mathbb{Z} = < \overline{1} > .$
Inversement si $H \leq \mathbb{Z}/n\mathbb{Z}$ d'ordre d, alors pour tout $x \in H$, $dx = 0$, c'est-à-dire, si $x = \overline{a}$, alors $da \in n\mathbb{Z}$ donc a divisible par n/d donc $x \in G_d$. Ainsi $H \subset G_d$ or H et G_d ont même cardinal donc

$$H = G_d.$$

Exercice 9 :

1. On a

$$\left(x^{-1}y^{-1}\right)^{-1} = xy = yx.$$

2. On a

$$\underbrace{(xy)\cdots(xy)}_{n \text{ fois}} = x^n y^n \implies y\underbrace{(xy)\cdots(xy)}_{n-2 \text{ fois}} x = x^{n-1}y^{n-1}$$

ainsi

$$(yx)^n = yx(yx)^{n-1} = yxx^{n-1}y^{n-1} = yx^ny^{n-1},$$

et par suite

$$(yx)^n = y^nx^n = yx^ny^{n-1} \implies y^{n-1}x^n = x^ny^{n-1}$$

d'où pour tout $y \in G$, y^{n-1} commute avec tous éléments de la forme x^n avec $x \in G$, or $x \longmapsto x^n$ est surjective ainsi pour tout $z \in G$ il existe $x \in G$ tel que $z = x^n$. Donc

$$Z(G) = \{x^{n-1} \,|\, x \in G\}.$$

Exercice 10 :

1. Pour $n \in \mathbb{N}$, on a $(n\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Z}, +)$.
Soit $H \leq \mathbb{Z}$, si $H = \{0\}$, alors $H = 0\mathbb{Z}$, sinon

$$H^+ = \{h \in H \,|\, h > 0\} \neq \emptyset$$

car $H \neq \{0\}$, et par suite il existe $h \in H$ tel que $h \neq 0$. Si $0 < h \in H^+$ ok, sinon $0 < -h \in H^+$. Ainsi $H^+ \neq \emptyset$ et minioré donc admet borne inf or $H^+ \subset \mathbb{N}$. Ainsi H^+ admet un plus petit élément : $n = \min H^+$.
On a, $n \in H^+ \subset H$, alors

$$n\mathbb{Z} \subset H.$$

Soit $h \in H$, par division euclidienne on a, $h = qn + r$ avec $0 \leq r < n$, et par suite $r = h - qn \in H$. Si $r > 0$, alors $r \in H^+$ avec $r < n$ absurde car $n = \min H^+$. Donc $r = 0$, ainsi $h \in n\mathbb{Z}$, d'où

$$H \subset n\mathbb{Z}.$$

Soient $H \leq \mathbb{Z}/n\mathbb{Z}$ et

$$\begin{aligned} \Pi : \quad & \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \\ & k \longmapsto \overline{k}, \end{aligned}$$

alors $\Pi^{-1}(H) \leq \mathbb{Z}$ avec $\ker(\Pi) = n\mathbb{Z} \subset \Pi^{-1}(H)$, or le sous-groupes de $\mathbb{Z}$ contenant $n\mathbb{Z}$: $d\mathbb{Z}$ avec d divise n, comme Π surjective, alors

$$\Pi\Big(\Pi^{-1}(H)\Big) = H,$$

d'où

$$H = \Pi(d\mathbb{Z}) = < \overline{(\frac{n}{d})} > = G_d.$$

2. Soit $G = < g >$ un groupe monogène, alors

$$\begin{aligned} \varphi : \quad & \mathbb{Z} \longrightarrow G \\ & k \longmapsto g^k \end{aligned}$$

est un morphisme surjective.
Si φ injective, alors

$$\mathbb{Z} \simeq G.$$

Sinon $\ker(\varphi) = n\mathbb{Z}$, ainsi

$$\mathbb{Z}/n\mathbb{Z} \simeq G.$$

Si G isomorphe à $\mathbb{Z}$ ou $\mathbb{Z}/n\mathbb{Z}$ et comme

$$Z =< 1 > \qquad \text{et} \qquad \mathbb{Z}/n\mathbb{Z} =< \overline{1} >,$$

alors G est monogène

$$G =< \varphi(1) > \qquad \text{ou} \qquad G =< \varphi(\overline{1}) > .$$

Exercice 11 :

1. Soit g un élément d'ordre k, alors $\varphi(g^k) = [\varphi(g)]^k = e'$, et par suite l'ordre de $\varphi(g)$ est inférreur où égal à k. Si $|\varphi(g)| = k' < k$, ainsi

$$[\varphi(g)]^{k'} = \varphi(g^{k'}) = e' = \varphi(g^k) \quad \text{comme } \varphi \text{ est injective, alors} \quad g^k = g^{k'} = e$$

absurde car g est d'ordre k. De même dans le cas infini.
2. Soit

$$\begin{aligned} f: \quad & \mathbb{Z}\big/nm\mathbb{Z} \longrightarrow \mathbb{Z}\big/n\mathbb{Z} \times \mathbb{Z}\big/m\mathbb{Z} \\ & [k]_{nm} \longmapsto ([k]_n, [k]_m). \end{aligned}$$

"$\Longrightarrow$" On a $[1]_{nm}$ est d'ordre nm dans $\mathbb{Z}\big/nm\mathbb{Z}$, ainsi $f([1]_{nm})$ est d'ordre nm. Supposons que $d = n \wedge m \neq 1$, ainsi il existe n' et m' tel que

$$n = n'd \qquad \text{et} \qquad m = m'd \qquad \text{avec} \qquad n' \wedge m' = 1.$$

Comme f est un morphisme de groupes, alors

$$n'm'\overline{f}([1]_{nm}) = (m'n[1]_n, n'm[1]_m = ([0]_n, [0]_m).$$

Donc $\overline{f}([1]_{nm})$ est d'ordre $n'm'd$, absurde. D'où $n \wedge m = 1$.
"$\Longleftarrow$" Il est clair que f est un morphisme de groupes et

$$\begin{aligned} \ker(f) =& \{[k]_{nm} \in \mathbb{Z}\big/nm\mathbb{Z} \,|\, f([k]_{nm}) = ([0]_n, [0]_m)\} \\ &= \{[k]_{nm} \in \mathbb{Z}\big/nm\mathbb{Z} \,|\, k \in nm\mathbb{Z}\} \qquad \text{car } n \wedge m = 1 \\ &= \{[0]_{nm}\} \end{aligned}$$

et par suite f est injectif, de plus

$$\left|\mathbb{Z}\big/nm\mathbb{Z}\right| = nm = \left|\mathbb{Z}\big/n\mathbb{Z} \times \mathbb{Z}\big/m\mathbb{Z}\right|$$

Donc

$$\mathbb{Z}\big/nm\mathbb{Z} \simeq \mathbb{Z}\big/n\mathbb{Z} \times \mathbb{Z}\big/m\mathbb{Z}.$$

Exercice 12 :

Comme

$$[G : H] = 2,$$

alors il y a deux classes, de plus les classes forment une partition de G parmi le classe il y a H, ainsi pour tout $x \in G$

$$xH = Hx.$$

En effet : si $x \in H$, alors on obtient l'égalité, sinon xH et Hx sont égales, puisque

$$G = H \cup xH = H \cup xH.$$

Exercice 13 :

1. On a

$$N_a \neq \emptyset \qquad \text{car } A \neq \emptyset \text{ et } A \subset N_A.$$

2. Soit N un sous-groupe distingué de G tel que $A \subset N$. Soient $a \in A$ et $g \in G$, alors

$$gag^{-1} \in N$$

Si $b \in G$ tel que $b^{-1} \in A \subset N \leq G$, alors $b \in N$, et par suite

$$gbg^{-1} \in N.$$

Donc N contient tous les éléments de G de la forme

$$(g_1 a_1 g_1^{-1}) \cdots (g_n a_n g_n^{-1}) \,|\, n \in \mathbb{N},\ \forall\, 1 \leq i \leq n,\ g_i \in G \text{ et } (a_i \in A \text{ ou } a_i^{-1} \in A).$$

Exercice 14 :

1. Soient H un sous-groupe distingué de G et $f \in Aut(G)$. Montrons que

$$gf(h)g^{-1} \in f(H) \qquad \forall\, (g, h) \in G \times H?$$

Comme $g \in G$ et f surjective alors il existe $g' \in G$ tel que $g = f(g')$ et f endomorphisme, alors

$$gf(h)g^{-1} = f(g'hg'^{-1}) \in f(H) \qquad \text{car } H \text{ est distingué.}$$

2. Puisque H et $f(H)$ distingués dans G, alors G/H et $G/f(H)$ sont deux groupes. Soit

$$\begin{aligned} \overline{f} : \quad & G/H \longrightarrow G/f(H) \\ & gH \longmapsto f(g)f(H). \end{aligned}$$

$\overline{f}$ injective. En effet :

$$\overline{f}(gH) = \overline{f}(g'H),$$

alors $f(gg'^{-1})f(H) \in f(H)$, ainsi $gg'^{-1} \in H$, c'est-à-dire $gH = g'H$.
$\overline{f}$ surjective. En effet :
Soit $\overline{g} = gf(H) \in G/f(H)$ puisque f surjective donc il existe $g' \in G$ tel que $g = f(g')$ ainsi

$$\overline{g} = \overline{f}(g'H).$$

Exercice 15 :

1. Aucune difficulté.
2. Pour tout $f \in End(G)$, on a

$$f([x,y]) = [f(x), f(y)].$$

3. Soient $X = c_1 \cdots c_k \in D(G)$ et $g \in G$, avec $c_i = [x_i, y_i]$, alors

$$gXg^{-1} = (gc_1g^{-1}) \cdots (gc_kg)^{-1}$$

or

$$gc_ig^{-1} = [gx_ig^{-1}, gy_ig^{-1}]$$

d'où $gXg^{-1} \in D(G)$.

4. Comme $D(G)$ est un sous-groupe distingué de G, alors $G/D(G)$ est un groupe. Pour tout $(\overline{x}, \overline{y}) \in (G/D(G))^2$, montrons que $\overline{x}\,\overline{y} = \overline{y}\,\overline{x}$?, i.e, $\overline{x}^{-1}\overline{y}^{-1}\overline{x}\,\overline{y} = \overline{e}$, i.e, $x^{-1}y^{-1}xy \in D(G)$, or

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

5. Comme G/H est abélien, alors

$$\overline{x}^{-1}\overline{y}^{-1}\overline{x}\,\overline{y} = \overline{e},$$

et par suite

$$x^{-1}y^{-1}xy \in H,$$

d'où

$$D(G) \subset H.$$

Soit $H \leq G$ tel que $D(G) \subset H$. Montrons que H est distingué et G/H abélien ?
Pour tout $(g,h) \in G \times H$, on a

$$ghg^{-1} = ghg^{-1}h^{-1}h = [g,h]h \in H.$$

De plus

$$\begin{array}{rl} \Pi : & G \longrightarrow G/H \\ & g \longmapsto gH \end{array}$$

la surjection canonique vérifiée

$$\Pi([g,g']) = \Pi(gg'g^{-1}g'^{-1}) = \overline{e} \qquad \text{car } D(G) \subset H = \ker(\Pi)$$

or Π est un morphisme, donc

$$\Pi(gg') = \Pi(g'g) \qquad \text{i.e, } \overline{g}\,\overline{g'} = \overline{g'}\,\overline{g}.$$

On a

$$G/\ker(f) \simeq Im(f) \quad \text{qui est abélien,}$$

alors

$$D(G) \subset \ker(f).$$

7.

$$\begin{array}{lll} f: & G \longrightarrow G' & \Pi: \quad G \longrightarrow G/D(G) \\ \widetilde{f}: & G/D(G) \longrightarrow G' & \\ & gD(G) \longmapsto f(g) & \end{array}$$

$\widetilde{f}$ bien définie : Soit $(\overline{g_1}, \overline{g_2}) \in (G/D(G))^2$ tel que $\overline{g_1} = \overline{g_2}$. On a

$$\widetilde{f}(\overline{g_1}\,\overline{g_2^{-1}} = f(g_1 g_2^{-1})$$

or $g_1 g_2^{-1} \in D(G)$, ainsi $(g_1 g_2^{-1}) =$ é, et par suite

$$\widetilde{f}(\overline{g_1}) = \widetilde{f}(\overline{g_2}).$$

8. On a $D(S_2) = \{Id\} = A_2$.
Si $n \geq 3$.
Le signature d'un commutateur est 1 donc $D(S_n) \subset A_n$. Comme A_n est engendré par les 3-cycles et un 3-cycle

$$(ijk) = (jk)(ij)(jk)(ij) = [(ik), (ij)],$$

alors $A_n \subset D(S_n)$. Donc

$$D(S_n) = A_n \qquad \forall\, n \geq 2.$$

Exercice 16 :

1. On a pour tout endomorphisme $\varphi \in End(G)$

$$\varphi[g, g'] = [\varphi(g), \varphi(g')] \implies \varphi(D(G)) \subset D(G).$$

Ainsi pour tout $\varphi \in Aut(G)$

$$\varphi^{-1}(D(G)) \subset \implies D(G) \subset \varphi(D(G)).$$

D'où

$$\varphi(D(G)) = D(G).$$

2. Comme pour tout $g \in G$, on a $\varphi_g(x) = gxg^{-1}$ est un automorphisme de G, alors

$$gHg^{-1} = H.$$

3. Soit $\varphi \in Aut(G)$ puisque H es caractéristique dans G, alors $\varphi(h) \in H$ et $\varphi^{-1}(h) \in H$ pour tout $h \in H$. D'où la restriction φ_H de φ à H est un automorphisme de H. Puisque K est caractéristique dans H, alors $\varphi_H(K) = \varphi(K) \subset K$. Cette propriété étant vraie pour tout automorphisme φ, elle est vraie pour φ^{-1}. D'où $\varphi^{-1}(K) \subset (K)$, c'est-à-dire, $K \subset \varphi(K)$. Ainsi K est un sous-groupe caractéristique de G.
4. Puisque N est distingué dans G, alors pour tout $g \in G$ l'application φ_g définie par

$\varphi_g(n) = gng^{-1}$ pour tout $n \in N$ est un automorphisme de N, comme H est caractéristique dans N, alors

$$gHg^{-1} = H \quad \forall\, g \in G.$$

Exercice 17 :

1. On a $H_1 \times H_2 \leq G_1 \times G_2$ et $\forall\, (g_1, g_2, h_1, h_2) \in G_1 \times \times G_2 \times H_1 \times H_2$

$$(g_1, g_2)(h_1, h_2)(g_1^{-1}, g_2^{-1}) = (g_1 h_1 g_1^{-1}, g_2 h_2 g_2^{-1}) \in H_1 \times H_2.$$

2. On a

$$\begin{array}{rl} \varphi : & G_1 \times G_2 \longrightarrow G_1/H_1 \times G_2/H_2 \\ & (g_1, g_2) \longmapsto (g_1 H_1, g_2 H_2) \end{array}$$

est un morphisme de groupes surjectif avec $\ker(\varphi) = H_1 \times H_2$. Ainsi

$$G_1 \times G_2 \Big/ H_1 \times H_2 \simeq G_1/H_1 \times G_2/H_2.$$

Exercice 18 :

1. A Sous-groupe de $(B, \circ)$ des bijections de $\mathbb{R}$ sur $\mathbb{R}$.
On a

$$\begin{array}{rl} \varphi : & A \longrightarrow \mathbb{R}^* \\ & ax + b \longmapsto a \end{array}$$

est un morphisme de groupes surjectif avec $\ker(\varphi) = N$, alors

$$N \lhd A \qquad \text{et} \qquad A/N \simeq \mathbb{R}^*.$$

Chapitre 2

Actions des groupes et théorème de Sylow

2.1 Action d'un groupe sur un ensemble

Définition 2.1. *Soient G un groupe d'élément neutre e et X un ensemble non vide. On dit que G opère à gauche sur X s'il existe une application*

$$\begin{aligned} \varphi : \quad & G \times X \longrightarrow X \\ & (g, x) \longmapsto \varphi(g, x), \qquad \text{noté } g \cdot x \end{aligned}$$

vérifiant

1. $$\varphi(g_1 g_2, x) = \varphi\Big(g_1, \varphi(g_2, x)\Big) = (g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x) \qquad \forall\, (g_1, g_2, x) \in G^2 \times X.$$

2. $$\varphi(e, x) = e \cdot x = x \qquad \forall\, x \in X.$$

Remarques. *1. On a une définition analogue pour les opérations à droite.*

2. Si G opère sur X, alors

i) *Pour tout $g \in G$*

$$\begin{aligned} \varphi_g : \quad & X \longrightarrow X \\ & x \longmapsto \varphi_g(x) = g \cdot x \end{aligned}$$

est une bijection de X, $\varphi_g \in \mathcal{S}(X)$.

ii)

$$\begin{aligned} \phi : \quad & G \longrightarrow \mathcal{S}(X) \\ & g \longmapsto \varphi_g \end{aligned}$$

est un morphisme de groupes.

Exemples. *1. $\mathcal{S}_n$ opère sur $[\![1,n]\!]$ par :*

$$\begin{aligned}\mathcal{S}_n \times [\![1,n]\!] &\longrightarrow [\![1,n]\!]\\ (\sigma,k) &\longmapsto \sigma\cdot k = \sigma(k).\end{aligned}$$

2. Soit $\sigma \in \mathcal{S}_n$, alors $<\sigma>$ opère sur $[\![1,n]\!]$

$$\begin{aligned}<\sigma> \times [\![1,n]\!] &\longrightarrow [\![1,n]\!]\\ (\sigma^k,x) &\longmapsto \sigma^k\cdot x = \sigma^k(x).\end{aligned}$$

3. $GL_n(\mathbb{R})$ opère sur $\mathbb{R}^n$ par :

$$U\cdot x = U(x) \qquad \forall\,(U,x)\in GL_n(\mathbb{R})\times\mathbb{R}^n.$$

Remarque. *En général*

$$g_1\cdot x = g_2\cdot x \;\not\Rightarrow\; g_1 = g_2$$

dans $\mathcal{S}_4$

$$\tau_{12}(4) = \tau_{13}(4) = 4 \qquad \textit{mais } \tau_{12}\neq\tau_{13}.$$

Proposition 2.2. *G opère sur X si et seulement si il existe un morphisme de groupes de G dans $\mathcal{S}(X)$.*

Démonstration : "$\Longrightarrow$" Voir remarque précédente.
"$\Longleftarrow$" On a $\phi :\quad G\longrightarrow \mathcal{S}(X)$ un morphisme de groupes. Posons

$$\phi(g)(x) = g\cdot x$$

ainsi pour tout $(g_1,g_2,x)\in G^2\times X$, on obtient

$$g_1\cdot(g_2\cdot x) = \phi(g_1)[\phi(g_2)(x)] = \phi(g_1)\circ\phi(g_2)(x) \underbrace{=}_{\phi \text{ morphisme}} \phi(g_1g_2)(x) = (g_1g_2)\cdot x.$$

Enfin

$$e\cdot x = \phi(e)(x) = Id_X(x) = x.$$

■

Remarques. *G opère sur X.*

1. *Si $H\leq G$, alors H opère sur X (restriction de φ sur $H\times X$).*
2. *L'ensemble $\{\varphi_g \,|\, g\in G\}$ est un sous-groupe de $\mathcal{S}(X)$ appelé groupe de transformation de X.*

Action d'un groupe sur lui-même
Soit G un groupe, on peut faire opérer G sur lui-même

1. Par translation
$$G \times G \longrightarrow G$$
$$(g, x) \longmapsto gx.$$

2. Par conjugaison
$$G \times G \longrightarrow G$$
$$(g, x) \longmapsto gxg^{-1}.$$

On peut faire opérre G sur l'ensemble $\mathscr{P}(G)$ des ses parties

1.
$$G \times \mathscr{P}(G) \longrightarrow \mathscr{P}(G)$$
$$(g, X) \longmapsto gX = \{gx \,|\, x \in X\}.$$

2.
$$G \times \mathscr{P}(G) \longrightarrow \mathscr{P}(G)$$
$$(g, X) \longmapsto gXg^{-1} = \{gxg^{-1} \,|\, x \in X\}.$$

2.1.1 Orbites et stabilisateurs

Lorsque un G un groupe opère sur un ensemble X, alors la relation

$$x \sim y \iff \exists\, g \in G \quad \text{tel que} \quad y = g \cdot x$$

est une relation d'équivalence.

1. Réflexivité :
$$x = e \cdot x \qquad \text{d'où} \quad x \sim x$$

2. Symétrique
$$x \sim y \implies y = g \cdot x \implies g^{-1} \cdot y = g^{-1} \cdot g \cdot x = (g^{-1}g) \cdot x = e \cdot x = x \implies y \sim x.$$

3. Transitivité : $x \sim y$ et $y \sim z$, alors
$$z = g_2 \cdot y = g_2 \cdot g_1 \cdot x = (g_2 g_1) \cdot x \implies x \sim z.$$

Les classes d'équivalences sont appelées les orbites. L'orbite d'un $x \in X$ est notée Ω_x ou O_x ou
$$G \cdot x = \{g \cdot x \,|\, g \in G\}.$$
L'ensemble des orbites est le quotient de X par G est noté G/X.
L'ensemble
$$G_x = \{g \in G \,|\, g \cdot x = \varphi_g(x) = x\}$$
s'appelle stabilisateur (ou sous-groupe d'isotropie) de x qui est un sous-groupe de G. En effet :
$$e \in G_x \text{ car } e \cdot x = x \implies G_x \neq \emptyset.$$

Soit $(g_1, g_2) \in G_x^2$, alors

$$(g_1 {g_2}^{-1}) \cdot x = (g_1 {g_2}^{-1}) \cdot (g_2 \cdot x) = g_1 \cdot [({g_2}^{-1} g_2) \cdot x] = g_1 \cdot x = x.$$

Donc

$$g_1 {g_2}^{-1} \in G_x.$$

Soit E une partie non vide de X.

1. On appelle fixateur de E, et on note

$$Fix_G(E) = \{g \in G \,|\, g \cdot x = x, \forall\, x \in E\}.$$

2. On appelle stabilisateur de E, et on note

$$Stab_G(E) = \{g \in G \,|\, g \cdot E = E\}.$$

Si $E = \{x\}$, on noté G_x à la place de $Fix_G(\{x\}) = Stab_G(\{x\})$.

Proposition 2.3. *Soient G un groupe, X un ensemble non vide tel que G opère sur X et E une partie non vide de X. Alors*

1. $Fix_G(E) \leq G$.
2. $Stab_G(E) \leq G$.
3. $Fix_G(E) \lhd Stab_G(E)$.

Démonstration : 1) C'est évident.

2) On a

$$e \in Stab_G(E) \implies Stab_G(E) \neq \emptyset.$$

Soit $(g_1, g_2, x) \in (Stab_G(E))^2 \times E$, alors

$$(g_1 {g_2}^{-1}) \cdot x = g_1 \cdot ({g_2}^{-1} \cdot x) = g_1 \cdot [{g_2}^{-1} \cdot (g_2 \cdot y)] = g_1 \cdot y \in E$$

car $g_2 \in Stab_G(E)$ et $x \in E$ donc il existe $y \in E$ tel que $g_2 \cdot y = x$. Donc

$$g_1 {g_2}^{-1} \in G_x.$$

3) On a $Fix_G(E) \leq G$ et $Fix_G(E) \subset Stab_G(E)$, alors

$$Fix_G(E) \leq Stab_G(E).$$

Soit $(g, g_1) \in Stab_G(E) \times Fix_G(E)$. Montrons que

$$g g_1 g^{-1} \in Fix_G(E)?$$

On a

$$g g_1 g^{-1} \cdot x = g g_1 \cdot (g^{-1} \cdot x) = g g_1 \cdot y = g \cdot (g_1 \cdot y) = g \cdot y = x.$$

Donc

$$g g_1 g^{-1} \in Fix_G(E) \implies Fix_G(E) \lhd Stab_G(E).$$

■

Remarque. *Soit ϕ le morphisme de G dans $\mathcal{S}_X$ associé à l'opération, alors*

$$\begin{aligned}\ker(\phi) = \{g \in G \,|\, \phi(g) = Id_X\} &= \{g \in G \,|\, g \cdot x = x,\ \forall\, x \in X\} \\ &= Fix_G(X) \\ &= \bigcap_{x \in X} Fix_G(\{x\}) \\ &= \bigcap_{x \in X} G_x.\end{aligned}$$

Exemples. *1. Si G opère sur lui-même par translation, alors*

$$\Omega_x = G \qquad et \qquad G_x = Fix_G(\{x\}), \quad \forall\, x \in G.$$

2. Si G opère sur lui-même par conjugaison, alors pour tout $x \in G$

$$\Omega_x = \{gxg^{-1} \,|\, g \in G\} \quad et \quad Fix_G(\{x\}) = \{g \in G \,|\, gxg^{-1} = x\} = C_G(\{x\}).$$

3. Si G opère sur $\mathscr{P}(G)$ par conjugaison, alors pour tout $S \in \mathscr{P}(G)$

$$Stab_G(S) = \{g \in \ | \, gSg^{-1} = S\} = N_G(S) \quad et \quad \Omega_S = \{gSg^{-1} \,|\, g \in G\}.$$

Ainsi $S \lhd G \iff Stab_G(S) = G$.

Le normalisateur d'un sous-groupe H de G est le plus grand sous-groupe de G dans lequel H est distingué. En effet :
On a

$$H \lhd Stabl_G(H) = N_G(H).$$

Soit $K \leq G$ tel que $H \lhd K$. Montrons que $K \subset N_G(H)$?
Soit $k \in K$, alors $kHk^{-1} = H$, ainsi $k \in N_G(H)$, et par suite $k \subset N_G(H)$.

Définition 2.4. *Soit G un groupe qui opère sur X. L'opération est dite transitive s'il n'y a qu'une seule orbite (i.e, G/X est réduit à un seul élément)*

$$\forall\, (x, y) \in X^2 \quad il\ existe\ g \in G\ tel\ que\ y = g \cdot x = \varphi_g(x).$$

Exemple. *Un groupe opère sur lui-même par translation transitivement.*

En particulier on retrouve le théorème de Cauchy.

Théorème 2.5. *(Théorème de Cauchy) Si G est un groupe d'ordre n ($|G| = n$), alors G est isomorphe à un sous-groupe du groupe $\mathcal{S}_n$.*

Démonstration : Soit

$$\begin{aligned}\phi : \quad & G \longrightarrow \mathcal{S}(G) \\ & g \longmapsto \varphi_g\end{aligned}$$

le morphisme associé à l'opération de G sur lui-même par translation. ϕ est injectif

$$\ker(\phi) = Fix_G(G) = \{g \in G \,|\, g \cdot x = x \;\forall\, x \in G\} = \{e\}$$

et par suite, on en déduit grâce à la première théorème d'isomorphisme que

$$G \simeq Im(\phi) \leq \mathcal{S}(G) = \mathcal{S}_n.$$

■

Soient G un groupe et $H \leq G$ (n'est pas nécessairement distingué). On peut faire opérer G sur l'ensemble G/H des classes à gauche modulo H

$$\begin{aligned} \varphi : \quad & G \times G/H \longrightarrow G/H \\ & (g, xH) \longmapsto \varphi_g(xH) = g \cdot (xH) = gxH, \end{aligned}$$

on a

$$\Omega_{xH} = G/H \qquad \text{et} \qquad Fix_G(xH) = xhx^{-1}.$$

Donc pour tout $x \in G$

$$H \lhd G \iff xH = Hx \iff Fix_G(xH) = H.$$

De plus

$$\begin{aligned} \phi : \quad & G \longrightarrow \mathcal{S}(G/H) \\ & g \longmapsto \varphi_g \end{aligned}$$

est un morphisme de groupes.
1) Si $H \lhd G$, alors

$$\ker(\phi) = \bigcap_{x \in G} xHx^{-1} = H.$$

2) Si $H \leq G$, alors

$$\ker(\phi) = \{g \in G \,|\, \varphi_g = Id_{G/H}\}.$$

Donc

$$g \in \ker(\phi) \iff gxH = xH \iff g \in \bigcap_{x \in G} xHx^{-1} = \bigcap_{x \in G} Fix_G(xH),$$

et par suite

$$\ker(\phi) = \bigcap_{x \in G} xHx^{-1} \lhd G \qquad \text{car c'est le noyau d'un morphisme de groupes.}$$

D'autre part pour $x = e$ et $g \in \ker(\phi)$ implique que $gH = H$ et par suite $\ker(\phi) \subset H$. Donc $\ker(\phi)$ est le plus grand sous-groupe distingué de G inclus dans H. En effet :
Soit $K \lhd G$ tel que $K \subset H$ on a pour tout $g \in G$

$$K = gKg^{-1} \subset gHg^{-1} \implies K \subset \ker(\phi).$$

3) Si G est un groupe simple (i.e, les sous-groupes distingué de G sont G et $\{e\}$), alors pour tout sous-groupe H de G ($H \neq G$) le groupe G est isomorphe à un sous-groupe de $\mathcal{S}(G/H)$, car $\ker(\phi) \lhd G$ et $\ker(\phi) \subset H$, et par suite

$$\ker(\phi) = \{e\} \implies \phi \text{ est injectif} \implies G \simeq Im(\phi) \leq \mathcal{S}(G/H).$$

Proposition 2.6. *Soient G un groupe d'ordre n et $H \leq G$ tel que*

$$[G : H] = card(G/H) = k > 1.$$

Si n ne divise pas $k!$, alors G n'est pas simple.

Démonstration : Si G est simple, alors G isomorphe à sous-groupe de $\mathcal{S}_k$ qui est d'ordre $k!$, ainsi le théorème de Lagrange implique que n divise $k!$ absurde. ■

Théorème 2.7. *Soit G un groupe opérrant sur un ensemble X. Si l'action de G sur X est transitive ($\forall\,(x, y) \in X^2$ il existe $g \in G$ tel que $y = g \cdot x$), alors*

$$Fix_G(\{x\}) = G_x = \{g \in G \,|\, g \cdot x = x\} \simeq Fix_G(\{y\}) = G_y, \qquad \forall\,(x, y) \in X^2.$$

Démonstration : Soit $(x, y) \in X^2$, alors il existe $g \in G$ tel que $y = g \cdot x$, d'où $x = g^{-1} \cdot y$. Soit

$$\begin{aligned} \psi_g : \quad & G_x \longrightarrow G_y \\ & c \longmapsto gcg^{-1} \end{aligned}$$

en particulier

$$c \cdot x = x \qquad \text{car } c \in G_x,$$

c'est que implique que

$$gcg^{-1} \cdot y = gc \cdot (g^{-1} \cdot y) = gc \cdot x = g \cdot (c \cdot x) = g \cdot x = y$$

donc ψ_g bien définie. De plus

$$gcg^{-1} = h \iff c = ghg^{-1}$$

d'où ψ_g est bijective. Comme

$$\psi_g(c_1c_2) = g(c_1c_2)g^{-1} = (gc_1g^{-1})(gc_2g^{-1}) = \psi_g(c_1)\psi_g(c_2),$$

ainsi ψ_g est un morphisme de groupes. Donc

$$G_x \simeq G_y.$$

■

Remarque. *Lorsque l'action de G sur X n'est pas transitive on peut appliquer la preuve précédante à un orbite, i.e,*

$$G_x \simeq G_y, \quad \forall\,(x, y) \in \Omega_z^2.$$

2.1.2 Équation aux classes

Théorème 2.8. *Soit G un groupe opérant sur un ensemble X. Alors il existe une bijection entre $\Omega_x = \{g \cdot x \,|\, g \in G\}$ et l'ensemble quotient G/G_x (l'ensemble des classes à gauche modulo $G_x = \{g \,|\, g \cdot x = x\}$). En particulier si G est fini, alors*

$$|G| = |G_x| Card(\Omega_x).$$

Démonstration : Soit

$$\begin{aligned} f : \quad & \Omega_x \longrightarrow G/G_x \\ & gx \longmapsto gG_x \end{aligned}$$

i) f bien définie :

$$g_1 x = g_2 x \implies x = g_1^{-1} g_2 x \implies g_1^{-1} g_2 \in G_x$$

et par suite

$$g_2 G_x = g_1 g_1^{-1} g_2 G_X = g_1 G_x.$$

ii) f surjective : pour tout $gG_x \in G/G_x$ admet au moins gx comme antécédent.
iii) f injective :

$$g_1 G_X = g_2 G_x \implies g_1^{-1} g_2 \in G_X \implies g_1^{-1} g_2 x = x \implies g_1 x = g_2 x.$$

Si G est fini, alors

$$Card(\Omega_x) = [G : G_x] = Card(G/G_x) = \frac{|G|}{|G_x|}$$

d'où

$$|G| = |G_x| Card(\Omega_x).$$

■

Corollaire 2.9. *Soient X un ensemble fini et G un groupe opérrant sur X. Si $\{x_i\}_{1 \leq i \leq r}$ une famille de représentants des orbites distincts, alors*

$$Card(X) = \sum_{i=1}^{r} [G : G_{x_i}] = \sum_{i=1}^{r} Card(\Omega_{x_i}).$$

Démonstration : On a

$$X = \bigcup_{i=1}^{r} \Omega_{x_i} \quad \text{avec } \Omega_{x_i} \cap \Omega_{x_j} = \emptyset \text{ pour } i \neq j$$

et

$$[G : G_{x_i}] = Card(\Omega_{x_i}).$$

■

Corollaire 2.10. *Soit G un groupe fini opérrant sur lui-même par conjugaison. Si $\{x_i\}_{1\leq i\leq r}$ une famille de représentants des orbites distincts, alors*

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

Démonstration : On a

$$G_{x_i} = \{g \in G \,|\, gx_ig^{-1} = x_i\} = C_G(\{x_i\}) \quad \text{centralisateur de } x_i \text{ dans } G.$$

■

Remarque. *Soit G un groupe opérant sur lui-même par conjugaison et*

$$Z(G) = \{g \in G \,|\, gx = xg, \forall\, x \in G\} \lhd G$$

son centre, alors

$$x \in Z(G) \iff C_G(\{x\}) = G,$$

c'est-à-dire,

$$x \in Z(G) \iff [G : C_x(\{x\})] = 1 \iff \Omega_x = \{x\}.$$

Théorème 2.11. *(équation aux classes) Soit G un groupe fini de centre $Z(G)$. Soit $\{x_i\}_{1\leq i\leq r}$ une famille de représentants des classes de conjugaison distincts et non réduites à un point de G. Alors*

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

Application

Théorème 2.12. *(théorème de Cauchy) Soit G un groupe fini et p un diviseur premier de l'ordre de G. Alors il existe un élément d'ordre p dans G.*

Démonstration : Soit

$$X = \{(x_1, \cdots x_p) \in G^p \,|\, x_1 \cdots x_p = e\}$$

où e est l'élément neutre de G. On a $Card(X) = |G|^{p-1}$, car pour choisir un élément de X nous devons faire $p-1$ choix d'éléments de G. Soit

$$\begin{aligned} \varphi : \quad & \mathbb{Z}/pZ \times X \longrightarrow X \\ & (\overline{k}, x) \longmapsto (x_{\overline{k+1}}, \cdots, x_{\overline{k+p}}) \end{aligned}$$

que définie une action de $\mathbb{Z}/p\mathbb{Z}$ sur X.
Supposons que G ne possède aucun élément d'ordre p, alors le seul élément de X tel

que $\Omega_x = \{x\}$ est $(e, \cdots, e)$. En effet : s'il existe $x = (x_1, \cdots, x_p) \in X \setminus \{(e, \cdots, e)\}$ tel que $\Omega_x = \{x\}$, alors

$$\begin{aligned} x = (x_1, \cdots, x_p) &= (x_{\overline{1}}, \cdots, x_{\overline{p}}) \\ &= (x_{\overline{2}}, \cdots, x_{\overline{p+1}}) \\ &= (x_2, \cdots, x_p, x_1) \\ &\vdots \\ &= (x_p, x_1, \cdots, x_{p-1}), \end{aligned}$$

ainsi

$$x_1 = \cdots = x_p \implies {x_1}^p = e$$

d'où x_1 est d'ordre p absurde. Donc si G ne possède aucun élément d'ordre p, alors le seul élément de X tel que $\Omega_x = \{x\}$ est $(e, \cdots, e)$.
Soit $x \in X \setminus \{(e, \cdots, e)\}$, comme $|\mathbb{Z}/p\mathbb{Z}| = p$ est divisible par $Card(\Omega_x)$ et $Card(\Omega_x) > 1$, alors

$$Card(\Omega_x) = p$$

et par suite

$$|G|^{p-1} = Card(X) = \sum_i Card(\Omega_{x_i}) = 1 + mp$$

où m est le nombre des orbites de taille plus grand que 1. Or $|G|$ est divisible par p, d'où p divise $1 + mp$ absurde. ■

Théorème 2.13. *(Généralisation de théorème de Cauchy) Soit G un groupe fini d'ordre n et p un nombre premier tel que p^k divise n. Alors il existe $H \leq G$ tel que $|H| = p^k$.*

Démonstration : Si $p^k = n \implies H = G$.
Si $p^k = 1 \implies H = \{e\}$.
Supposons que $p^k \neq n$ et $p^k \neq 1$.
Démonstration par récurrence sur n : pour $n = 1$, c'est évident.
Supposons que pour tout groupe d'ordre $m < n$ $(n \geq 2)$ et pour tout p^k divisant m, il existe un sous-groupe d'ordre p^k.
Montrons que si $|G| = n$ tel que p^k divise n, alors il existe $H \leq G$ tel que $|H| = p^k$.
D'après l'équation aux classes, on a

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

avec $\{x_i\}_{1 \leq i \leq r}$ une famille de représentants des classes des orbites distincts et non réduit à un point. Il y a deux cas :
Première cas
Il existe $1 \leq i \leq r$ tel que p ne divise pas $[G : C_G(\{x_i\})] > 2$, or

$$|G| = |C_G(\{x_i\})|[G : C_G(\{x_i\})] \implies |C_G(\{x_i\})| < n.$$

D'autre part p^k divise n et p ne divise pas $[G : C_G(\{x_i\})]$, donc p^k divise $|C_G(\{x_i\})| < n$, ainsi d'après l'hypothèse de récurrence $C_G(\{x_i\} \subset G$ contient un sous-groupe d'ordre p^k.

Deuxième cas

Pour tout $1 \leq i \leq r$, p divise $[G : C_G(\{x_i\})]$, ce qui implique que p divise $|Z(G)|$, et par suite il existe un élément $a \in Z(G)$ d'ordre p. Soit $H =< a > \lhd G$, alors

$$\Big|G/H\Big| = \frac{|G|}{|H|} = \frac{n}{p} < n$$

comme p^k divise n (avec $k \neq 0$), alors p^{k-1} divise $\Big|G/H\Big|$. Ainsi l'hypothèse de récurrence, implique qu'il existe sous-groupe de G/H d'ordre p^{k-1} de la forme K/H avec $K \leq G$ tel que $H \subset K$, et par suite

$$|K| = \Big|K/H\Big||H| = p^k.$$

■

2.2 Théorème de Sylow

Définition 2.14. *Soit p un nombre premier. On appelle un p-groupe fini tout groupe d'ordre une puissance non nulle de p.*

Exemple. $\mathbb{Z}/8\mathbb{Z}$ *est un* 2*-groupe.*

Théorème 2.15. *(Théorème de Burnside) Le centre d'un p-groupe n'est pas trivial (i.e,* $\{e\} \subsetneq Z(G)$*).*

Démonstration : On a

$$Z(G) = \{g \in G \,|\, gx = xg, \forall\, x \in G\},$$

on fait opérer G sur lui-même par conjugaison. D'après l'équation des classes

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

Si $Z(G) = G$ ok, sinon

$$Card(\Omega_{x_i}) = [G : G_{x_i}] \geq 2$$

or $G_{x_i} \leq G$, alors $|G_{x_i}|$ divise $|G|$.
Si $|G_{x_i}| = 1$, alors

$$Card(\Omega_{x_i}) = [G : G_{x_i}] = \frac{|G|}{|G_{x_i}|} = |G|$$

et par suite l'opération est transitive ce qui est impossible, puisque G n'est pas rénduit à e (pour tout $x \in G$ il existe $g \in G$ tel que $gxg^{-1} = y = e$ est par suite $x = e$).
Si $|G_{x_i}| = |G|$, alors

$$Card(\Omega_{x_i}) = [G : G_{x_i}] = \frac{|G|}{|G_{x_i}|} = 1$$

impossible car $x_i \notin Z(G)$.
Donc pour tout $1 \leq i \leq r$ il existe $1 \leq \alpha_i \leq k$ tel que $\frac{|G|}{|G_{x_i}|} = p^{\alpha_i}$. Or

$$|G| = |Z(G)| + \sum_{i=1}^{r} \frac{|G|}{|G_{x_i}|}$$

et par suite dans $\mathbb{Z}/p\mathbb{Z}$ (i.e, modulo p)

$$\overline{0} = \overline{|Z(G)|} + \overline{0}.$$

Donc $Z(G)$ n'est pas réduit à l'élément neutre. ■

Corollaire 2.16. *Tout groupe d'ordre p^2, où p est un nombre premier est abélien.*

Démonstration : Comme $Z(G)$ est un sous-groupe d'un p-groupe, alors

$$|Z(G)| = \begin{cases} p \\ p^2. \end{cases}$$

Si $|Z(G)| = p^2$, alors $Z(G) = G$, est par suite G abélien.
Si $|Z(G)| = p$, alors $\frac{|G|}{|Z(G)|} = p$, d'où $G/Z(G)$ est cyclique. Or si $G/Z(G)$ est cyclique, alors G abélien. En effet :
Soit

$$\begin{aligned} \Pi : \quad & G \longrightarrow G/Z(G) \\ & g \longmapsto gZ(G) \end{aligned}$$

la surjection canonique, comme $G/Z(G)$ est cyclique, alors il existe $g \in G$ tel que $\Pi(g)$ est un générateur de $G/Z(G)$. Soit $(x, y) \in G^2$, alors

$$\Pi(x) = \Big(\Pi(g)\Big)^n = \Pi(g^n) \qquad \text{et} \qquad \Pi(y) = \Big(\Pi(g)\Big)^m = \Pi(g^m),$$

comme $\ker(\Pi) = Z(G)$, alors il existe $(x', y') \in Z(G)^2$ tel que

$$x = x'g^n \qquad \text{et} \qquad y = y'g^m.$$

Donc

$$xy = (x'g^n)(y'g^m) = x'y'g^ng^m = y'x'g^mg^n = y'g^mx'g^n = yx.$$

■

Proposition 2.17. *Soient G un groupe fini et $H \leq G$ ($H \subsetneq G$) tel que $[g : H] = p$ est le plus petit nombre premier divisant $|G|$, alors $H \lhd G$.*

Exemple. *Si G est un groupe d'ordre 75, alors tout sous-groupe d'indice 3 est distingué.*

Démonstration : On considère l'action de G sur G/H par translation à gauche

$$\begin{aligned}\varphi : \quad & G \times G/H \longrightarrow G/H \\ & (g, xH) \longmapsto g \cdot xH\end{aligned}$$

soit $\phi : \quad G \longrightarrow \mathcal{S}_{G/H}$ le morphisme associé. D'après le première théorème d'isomorphisme

$$G/\ker(\phi) \simeq \phi(G) \leq \mathcal{S}_p \qquad \text{car } \mathcal{S}_{G/H} \simeq \mathcal{S}_p.$$

Donc

$$\left|G/\ker(\phi)\right| \quad \text{divise } |G| = n \text{ et } p! \implies \left|G/\ker(\phi)\right| = p.$$

Comme

$$[G : H] = p = [G : \ker(\phi)] \implies |\ker(\phi)| = |H|$$

et

$$\ker(\phi) \subset H$$

en effet : soit $g \in \ker(\phi)$, alors pour tout $x \in G$, on a

$gxH = xH$ pour $x = e$, on trouve $gH = H$, ce qui implique que $g \in H$.

Donc

$$H = \ker(\phi) \lhd G.$$

■

Définition 2.18. *Soient p un nombre premier, $n \in \mathbb{N}^*$, $s \in \mathbb{N}^*$ tel que $p \wedge s = 1$ et G un groupe d'ordre $p^n s$.*
On appelle p-sous-groupe de Sylow de G, tout sous-groupe d'ordre p^n.

Exemples. *1) Pour $G = \mathbb{Z}/12\mathbb{Z}$, on a $|G| = 12 = 2^2 3$ et*

$$< \overline{3} >= \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\} \quad \textit{est 2-sous-groupe de Sylow de } \mathbb{Z}/12\mathbb{Z}.$$

$$< \overline{4} >= \{\overline{0}, \overline{4}, \overline{8}\} \quad \textit{est 3-sous-groupe de Sylow de } \mathbb{Z}/12\mathbb{Z}.$$

2) Pour

$$\mathcal{S}_3 = \{Id, \tau_{12}, \tau_{13}, \tau_{23}, (1,2,3), (1,3,2)\}$$

il y a 3, 2-sous-groupe de Sylow $\{Id, \tau_{12}\}$, $\{Id, \tau_{13}\}$ et $\{Id, \tau_{23}\}$.
Le 3-sous-groupe de Sylow $\{Id, (1,2,3), (1,3,2)\}$.
3) Pour $G = \mathbb{Z}/900\mathbb{Z}$, on a $|G| = 900 = 2^2 3^2 5^2$ et les sous-groupes de G : $n\mathbb{Z}/900\mathbb{Z}$ avec n divise 900.

$225\mathbb{Z}/900\mathbb{Z}$: 2-*sous-groupe de Sylow de* $225\mathbb{Z}/900\mathbb{Z}$.
$100\mathbb{Z}/900\mathbb{Z}$: 3-*sous-groupe de Sylow de* $225\mathbb{Z}/900\mathbb{Z}$.
$36\mathbb{Z}/900\mathbb{Z}$: 5-*sous-groupe de Sylow de* $225\mathbb{Z}/900\mathbb{Z}$.

On peut généralise la définition dans le cas où G est infini.

Définition 2.19. *Soient G un groupe, $H \leq G$ et p un nombre premier.*

1. *On dit que G est un p-groupe si*

$$\forall\, g \in G \setminus \{e\} \quad \text{il existe } n(g) \in \mathbb{N}^* \text{ tel que } | < g > | = ord(g) = p^{n(g)}.$$

2. *On dit que H est un p-sous-groupe de G si H est un p-groupe.*
3. *Un sous-groupe S de G est appelé p-sous-groupe de Sylow si S est le plus grand (pour l'inclusion) des p-sous-groupes de G.*

Remarques. 1. *Un p-sous-groupe de Sylow est un p-groupe.*

2. *L'image par un morphisme de groupes d'un p-sous-groupe est un p-sous-groupe. En effet :*
   Soient $\varphi : G \longrightarrow G'$ un morphisme de groupes et H un p-sous-groupe de G. Pour tout $y \in \varphi(H)$ il existe $h \in H$ tel que $y = \varphi(h)$, comme H est un p-sous-groupe de G, alors il existe $n \in \mathbb{N}^*$ tel que $ord(h) = p^n$,

$$y^{p^n} = e' \implies ord(y) \text{ divise } p^n \implies ord(y) = p^m.$$

3. *Si $H \lhd G$ et G un p-groupe, alors G/H est p-groupe, car*

$$\begin{aligned} \Pi : \quad & G \longrightarrow G/H \\ & g \longmapsto gH \end{aligned}$$

   est un morphisme de groupes surjectif ($G/H = \Pi(G)$).

Proposition 2.20. *Soient G un groupe fini et p un nombre fini. Alors tout p-sous-groupe de G est contenu dans un p-sous-groupe de Sylow de G.*

Démonstration : Soit H un p-sous-groupe de G. Si H est maximal (pour l'inclusion), alors H est un p-sous-groupe de Sylow de G. Sinon il existe H_1 tel que $H \subsetneq H_1$ avec H_1 est p-sous-groupe de G, on itère ce procédé qui fini car G l'est. ■

Remarque. *La proposition précédente reste vraie pour G infini. En effet :*
Soit

$$E = \{H' \leq G \,|\, H' \text{ p-sous-groupe de } G \text{ et } H \subset H'\},$$

on a $E \neq \emptyset$ car $H \in E$, et par suite le lemme de Zorn implique que E admet un élément maximal.

Ainsi on déduit l'existence des p-sous-groupe de Sylow.

Corollaire 2.21. *Tout groupe fini possède au moins un p-sous-groupe de Sylow.*

Démonstration : On a

$$|G| = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \qquad \text{avec } p_i \text{ premier, } \alpha_i \in \mathbb{N}^* \text{ et } p_i \wedge p_j = 1 \text{ pour } i \neq j.$$

Ainsi le théorème de Cauchy implique l'existence de p_i-sous-groupe et par suite la proposition précédente assurée l'existence de p_i-sous-groupe de Sylow. ■

Donc G possède des p-sous-groupes de Sylow. Nous allons maintenant voir comment liés les p-sous-groupe de Sylow entre eux et donner des indications sur leur nombre.

Proposition 2.22. *Soient G un groupe et p un nombre premier.*

1. *Tout sous-groupe conjugué d'un p-sous-groupe est un p-sous-groupe.*
2. *Tout sous-groupe conjugué d'un p-sous-groupe de Sylow est un p-sous-groupe de Sylow.*
3. *Si G possède un seul p-sous-groupe de Sylow S, alors $S \lhd G$.*

Démonstration : 1) Soit H un p-sous-groupe de G, on a pour tout $g \in G$, $gHg^{-1} \simeq H$ car

$$\begin{aligned} f : \quad & H \longrightarrow gHg^{-1} \\ & h \longmapsto ghg^{-1} \end{aligned}$$

est un isomorphisme.
2) Soit S un p-sous-groupe de Sylow, alors d'après 1) gSg^{-1} est un p-sous-groupe, supposons que gSg^{-1} n'est pas maximal, donc il existe S', p-sous-groupe de G tel que $gSg^{-1} \subsetneq S'$ et par suite

$$S \subsetneq g^{-1}S'g$$

absurde car $g^{-1}S'g$ est p-sous-groupe et S maximal.
3) Si S est un p- Sylow, ainsi 2) implique que gSg^{-1} est un p-Sylow pour tout $g \in G$. Comme S est unique, alors

$$gSg^{-1} = S \implies S \lhd G.$$

■

Théorème 2.23. *(Théorème de Sylow) Soient G un groupe fini, p un nombre premier et S un p-sous-groupe de Sylow de G. Alors*

1. *Si H est un p-sous-groupe de G, alors il existe $g \in G$ tel que*

$$H \subset gSg^{-1}.$$

2. *Les p-sous-groupes de Sylow de G sont les conjugués de S.*
3. *Les nombre de p-sous-groupe de Sylow de G : a_p*

   a_p divise $|G|$.

   $a_p = [G : N_G(S)]$.

   $a_p \equiv 1[p]$.

Démonstration : H opère sur l'ensemble G/S par translation à gauche

$$\begin{aligned}\varphi : \quad & H \times G/H \longrightarrow G/S \\ & (h, gS) \longmapsto h \cdot gS = ghS.\end{aligned}$$

Ainsi G/S se décomposer en orbites pour cette opération, d'après l'équation aux classes le cardinal de chacune des orbites divise $|H|$. Ainsi les orbites sont de cardinal 1 soit de cardinal une puissance non nulle de p.
Montrons qu'il existe au moins une orbite de cardinal 1.
Si toutes les orbites sont de cardinal une puissance non nulle de p, alors p divise $Card(G/S)$ (puisque les orbites forment une partition de G/S). Or

$$|G| = p^n s, \qquad \text{avec } (n, s) \in \mathbb{N}^{*2} \text{ tel que } p \wedge s = 1$$

et

$$Card(G/S) = [G : S] = \frac{|G|}{|S|} = s, \qquad \text{car } |S| = p^n$$

absurde car s n'est pas divisible par p. Donc il existe au moins une orbite de cardinal 1. Soit gS un reprśentant de cette orbite, ainsi pour tout $h \in H$

$$h \cdot gS = hgS = gS \implies g^{-1}hgS = S \implies g^{-1}hg \in S \implies h \in gSg^{-1} \implies H \subset gSg^{-1}.$$

2) Soit Q un p-sous-groupe de Sylow de G. Montrons qu'il existe $g \in G$ tel que

$$Q = gSg^{-1}?$$

Comme Q est un p-sous-groupe de G, alors 1) implique qu'il existe $g \in G$ tel que

$$Q \subset gSg^{-1}$$

or

$$|Q| = p^n = |gSg^{-1}| \implies Q = gSg^{-1}.$$

Pour démontrer 3) on a besoin de lemme suivant :

Lemme 2.24. *Soient G un groupe fini, p un nombre premier et S un p-sous-groupe de Sylow de G. Alors S est l'unique p-sous-groupe de Sylow de $N_G(S)$.*

3) On note $S_p(G)$ l'ensemble des p-sous-groupes de Sylow de G et on fait opère G sur sur $S_p(G)$ par conjugaison

$$\begin{aligned}\psi : \quad & G \times S_p(G) \longrightarrow S_p(G) \\ & (g, Q) \longmapsto gQg^{-1}.\end{aligned}$$

D'après 2) on a une seule orbite pour cette opération (i.e, G opère transitivement par conjugaison sur $S_p(G)$). D'où

$$a_p = Card(S_p(G)) \quad \text{divise } |G|.$$

De plus le cardinal de l'orbite est égal à l'indice du stabilisateur

$$[G : Stab_G(S)]$$

puisque pour l'action par conjugaison $Stab_G(S) = N_G(S)$, alors

$$a_p = Card(S_p(G)) = [G : N_G(S)].$$

Puisque G opère par conjugaison sur $S_p(G)$, alors S opère aussi par conjugaison sur $S_p(G)$. Donc $S_p(G)$ se décompose en orbites pour cette opération. Le cardinal de ces orbites divise l'ordre de S, donc chacune de ces orbites soit de cardinal 1 soit de cardinal une puissance non nulle de p.
$\{S\}$ **est l'unique orbite de cardinal** 1 (i.e, $\Omega_S = \{S\}$). Soit Q un p-sous-groupe de Sylow tel que l'orbite de Q est $\{Q\}$. Alors pour tout $x \in S$

$$xQx^{-1} = Q \implies x \in N_G(Q) \implies S \subset N_G(Q).$$

Ainsi S et Q sont deux p-sous-groupes de Sylow de $N_g(Q)$, d'où

$$S = Q.$$

Donc, on a une seule orbite de cardinal 1 et toutes les autres de cardinal divisible par p d'où

$$a_p \equiv 1[p].$$

■

Démonstration du Lemme 2.24
On a

$$N_G(S) = \{g \in G \,|\, gSg^{-1} = S\}$$

on sait que $N_G(S)$ est le plus grand sous-groupe de G dans lequel S est distingué. Comme

$$|G| = p^n s, \quad |S| = p^n \quad \text{et} \quad S \subset N_G(S),$$

alors

$$|N_G(S)| = p^n s' \quad \text{avec} \quad p \wedge s' = 1 \quad \text{et } s' \text{ divise } s.$$

Soit Q un p-sous-groupe de Sylow de $N_G(S)$ d'après 2) Q et S sont conjuqués dans $N_G(S)$, et par suite il existe $x \in N_G(S)$ tel que

$$Q = xSx^{-1}$$

comme $x \in N_G(S)$, alors

$$xSx^{-1} = S \implies S = Q.$$

D'où le lemme. ■

Corollaire 2.25. *a_p divise s.*

Démonstration : On a $|G| = p^n s$ avec $p \wedge s = 1$ et a_p divise $|G|$, alors $a_p = p^k s'$ avec $0 \leq k \leq n$ et $p \wedge s' = 1$, alors s' divise s. Or $a_p \equiv 1[p]$, donc $k = 0$, et par suite $a_p = s'$ divise s. ∎

Corollaire 2.26. *Soient G un groupe fini et S un p-sous-groupe de Sylow de G. Alors*

$$S \lhd G \iff S \text{ est l'unique } p\text{-sous-groupe de Sylow de } G.$$

Démonstration : "$\Longleftarrow$" voir Proposition 2.22.
"$\Longrightarrow$" Soit Q un p-sous-groupe de Sylow de G, alors il existe $g \in G$ tel que

$$Q = gSg^{-1} = S$$

d'où l'unicité. ∎

Exemples. *1. Un groupe d'ordre 63 n'est pas simple.*
On a $63 = 3^2 7$, alors

$$a_7 \equiv 1[7] \quad et \quad a_7 \text{ divise } 9.$$

Donc $a_7 = 1$, et par suite il y a un seul 7-sous-groupe de Sylow, ainsi il est distingué. D'où le groupe n'est pas simple. De même pour les groupes d'ordre 35.

2. Soit $G = \mathcal{S}_3$, alors $|G| = 2 \times 3$. Donc

$$a_2 \equiv 1[2] \quad et \quad a_2 \text{ divise } 3 \Longrightarrow a_2 = 1 \text{ ou } 3$$

$a_2 = 3$ car il y a 3, 2-sous-groupe de Sylow $\{Id, \tau_{12}\}$, $\{Id, \tau_{13}\}$ et $\{Id, \tau_{23}\}$. Par contre $a_3 = 1$.
Ainsi $\mathcal{S}_3$ n'est pas abélien car dans un groupe abélien tous les sous-groupes sont distingués.

Remarque. *Si G est un groupe abélien fini d'ordre fini divisible par un nombre premier p, alors G ne possède qu'un seul p-sous-groupe de Sylow.*

Corollaire 2.27. *Tout groupe fini d'ordre pq où p et q sont deux nombres premiers distincts n'est pas simple.*

Démonstration : Supposons que $q < p$. On a

$$a_p \equiv 1[p] \quad \text{et} \quad a_p \text{ divise } q \Longrightarrow a_p = 1 \text{ ou } q$$

comme $1 < q < p$, alors $a_p = 1$. Ainsi G possède un unique p-sous-groupe de Sylow S d'ordre p, et par suite $S \lhd G$ avec $\{e\} \subsetneq S \subsetneq G$. Donc G n'est pas simple. ∎

Avec des conditions supplémentaires, on a un meilleur résultat.

Proposition 2.28. *Soit G un groupe d'ordre pq où p et q sont deux nombres premiers distincts. Si $p \not\equiv 1[q]$ et $q \not\equiv 1[p]$, Alors G cyclique, abélien et isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \simeq \mathbb{Z}/pq\mathbb{Z}$.*

Démonstration : On a

$$a_p = 1 \quad \text{et} \quad a_q = 1,$$

d'où G possède :

Un unique p-sous-groupe de Sylow P.

Un unique q-sous-groupe de Sylow Q.

Ainsi

$$P \lhd G \quad \text{et} \quad Q \lhd G.$$

Comme P d'ordre premier, alors P cyclique $P =< x >$ de même $Q =< y >$. Montrons que

$$xy = yx?$$

Comme $P \cap Q$ est un sous-groupe de P et Q, alors lethéorème de Lagrange implique que

$$|P \cap Q| \quad \text{divise } p \text{ et } q$$

or

$$p \wedge q = 1 \Longrightarrow |P \cap Q| = 1 \Longrightarrow P \cap Q = \{e\}.$$

Comme $P \lhd Q$ et $Q \lhd G$, alors

$$xyx^{-1}y^{-1} \in P \cap Q = \{e\},$$

d'où

$$xy = yx.$$

Montrons que

$$G =< xy >?$$

On a

$$(xy)^{pq} = x^p y^q = e.$$

Soit $m \in \mathbb{N}^*$ tel que $(xy)^m = e$, alors $x^m = y^{-m} \in P \cap Q$, et par suite $x^m = y^m = e$. Donc p divise m et q divise m. Donc

$$ppcm(p, q) = pq \quad \text{divise } m$$

alors

$$| < xy > | = pq = |G|,$$

d'où G cyclique engendré par xy. Ainsi

$$G \simeq \mathbb{Z}/pq\mathbb{Z}$$

or $p \wedge q = 1$, donc

$$G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}.$$

■

Remarque. *D'après la proposition pécédente il n'y a qu'un seul groupe à isomorphisme près d'ordre pq où p et q sont deux nombres premiers distincts avec $p \not\equiv 1[q]$ et $q \not\equiv 1[p]$. Par exemple à isomorphisme près il y a un seul groupe d'ordre* $15 : \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/15\mathbb{Z}$.

Proposition 2.29. *Soient G un groupe fini, p un nombre premier divise $|G|$, $N \lhd G$ tel que p divise $|N|$ et S un p-sous-groupe de Sylow de G. Alors*

1. *$S \cap N$ est un p-sous-groupe de Sylow de N.*
2. *SN/N est un p-sous-groupe de Sylow de G/N.*

Démonstration : On a

$$|G| = p^n s \quad \text{avec } n \in \mathbb{N}^* \text{ et } p \wedge s = 1,$$

$$|N| = p^m s' \quad \text{avec } m \in \mathbb{N}^*,\ m \leq n \text{ et } s' \text{ divise } s$$

et

$$|S| = p^n.$$

1) Soit Q un p-sous-groupe de Sylow de N, ainsi Q est un p-sous-groupe de N, et par suite Q est n p-sous-groupe de G. Ainsi le théorème de Sylow implique qu'il existe un p-sous-groupe de Sylow S' de G tel que

$$Q \subset S'.$$

De nouveau le théorème de Sylow implique qu'il existe $g \in G$ tel que

$$S = gS'g^{-1}$$

comme $Q \subset S'$, alors

$$gQg^{-1} \subset S.$$

On a $N \lhd G$ et $Q \subset N$, alors

$$gQg^{-1} \subset N,$$

d'où

$$gQg^{-1} \subset S \cap N.$$

L'ordre de $S \cap N$ divise $|S|$ et $|N|$, alors

$$|S \cap N| = p^\alpha \quad \text{avec } 0 \leq \alpha \leq \inf(n, m)$$

puisque $gQg^{-1} \subset S \cap N$ et gQg^{-1} est un p-sous-groupe de Sylow de N, d'où

$$|S \cap N| \geq p^m \implies |S \cap N| = p^m.$$

Donc $S \cap N$ est un p-sous-groupe de Sylow de N.
2) Par le théorème d'isomorphisme, on a

$$SN/N \simeq S/S \cap N,$$

ainsi

$$\Big|SN/N\Big| = \Big|S/S \cap N\Big| = p^{n-m}.$$

Comme

$$\Big|G/N\Big| = \frac{s}{s'}p^{n-m},$$

donc SN/N est un p-sous-groupe de Sylow de G/N. ■

Pour classifier les groupes abéliens finis, on a besoin de définir produits directs.

2.3 Produits directs

Soient $(G_1, *_1)$ et $(G_2, *_2)$ deux groupes. On peut munir le produit cartésien $G_1 \times G_2$ d'un structure de groupe, en définisant une l.c.i $*$, par

$$(x_1, x_2) * (y_1, y_2) = (x_1 *_1 y_1, x_2 *_2 y_2)$$

Proposition 2.30. *Soient G_1 et G_2 deux groupes. Alors*

1. *$G_1 \times G_2$ abélien $\Longleftrightarrow$ G_1 et G_2 sont abéliens.*
2. *$G_1 \times G_2 \simeq G_2 \times G_1$.*
3. *Si G_1 et G_2 sont cycliques d'ordre m et n tel que $m \wedge n = 1$, alors $G_1 \times G_2$ est cyclique d'ordre mn.*

Démonstration : 1) "$\Longleftarrow$" C'est évident.
"$\Longrightarrow$" On a

$$(x_1y_1, e_2) = (x_1, e_2)(y_1, e_2) = (y_1, e_2)(x_1, e_2) = (y_1x_1, e_2).$$

Don G_1 abélien de même G_2 abélien. 2) L'application suivante

$$\begin{aligned} \varphi : \quad & G_1 \times G_2 \longrightarrow G_2 \times G_1 \\ & (x_1, x_2) \longmapsto (x_2, x_1) \end{aligned}$$

est une morphisme.
3) On a

$$G_1 =< x > \quad \text{avec } |G_1| = m \quad \text{et} \quad G_2 =< y > \quad \text{avec } |G_1| = n,$$

alors

$$(x, y)^{mn} = (x^{mn}, y^{mn}) = (e_1, e_2) = e.$$

Si (x, y) est d'ordre r, alors m divise r et n divise r, or $m \wedge n = 1$, d'où mn divise r de plus r divise mn. Donc

$$r = mn \implies G_1 \times G_2 =< (x, y) > \implies |G_1 \times G_2| = mn.$$

■

Corollaire 2.31. *Soit $n_1, \cdots, n_k$ une suite d'entiers positifs tel que*

$$n_i \wedge n_j = 1 \quad \textit{pour } i \neq j.$$

Si G_i est un groupe cyclique d'ordre n_i pour $1 \leq i \leq k$, alors

$$G = G_1 \times \cdots \times G_k$$

est un groupe cyclique d'ordre $n = n_1 \cdots n_k$.

Démonstration : Par récurrence sur k.

i) Pour $k = 1$, c'est par définition.

ii) Supposons que le résultat vrai jusque'à l'ordre $k - 1$

$$H = G_1 \times \cdots \times G_{k-1} \quad \text{est cyclique d'ordre } n_1 \cdots n_{k-1}.$$

Ainsi la proposition précédente, implique que

$$G = H \times G_k \quad \text{est cyclique d'ordre } n_1 \cdots n_k.$$

■

Remarques.

1. *Pour $G_1 = G_2 = \mathbb{Z}/2\mathbb{Z}$, alors $G_1 \times G_2$ est d'ordre 2 et se groupe n'est pas cyclique car il ne contient pas d'éléments d'ordre 4.*
2. *Soient G_1 et G_2 deux groupes. Les sous-groupes de $G_1 \times G_2$ ne sont pas tous de la forme $H_1 \times H_2$ où $H_1 \leq G_1$ et $H_2 \leq G_2$. Par exemple pour*

$$G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

H est un sous-groupe de G avec

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

et les sous-groupes de $\mathbb{Z}/2\mathbb{Z}$ sont

$$\{\overline{0}\} \quad \textit{et} \quad \mathbb{Z}/2\mathbb{Z}$$

et H n'est pas produit cartésien de ses deux sous-groupes. C'est pour cette raison le produit cartésien est parfois appelée "produit direct externe".

Définition 2.32. *Soient G un groupe, $H \leq G$ et $K \leq G$. On dit que G est le produit direct interne (ou plus simplement produit direct) de H et k si*

1. *$H \lhd G$ et $K \lhd G$.*
2. *Pour tout $g \in G$*

$$\exists!(h, k) \in H \times K \quad \textit{tel que} \quad g = hk.$$

Exemple. *Si $n \wedge m = 1$, alors $\mathbb{Z}/mn\mathbb{Z}$ est le produit direct de $n\mathbb{Z}/nm\mathbb{Z}$ et $m\mathbb{Z}/nm\mathbb{Z}$. En effet : on a $\mathbb{Z}/mn\mathbb{Z} =< \overline{1} >$. Soit*

$$H =< \overline{m} > \simeq n\mathbb{Z}/nm\mathbb{Z} \quad et \quad K =< \overline{n} > \simeq m\mathbb{Z}/nm\mathbb{Z}$$

comme $\mathbb{Z}/mn\mathbb{Z}$ est abélien, alors $H \lhd \mathbb{Z}/mn\mathbb{Z}$ et $K \lhd \mathbb{Z}/mn\mathbb{Z}$. Or

$$\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

d'où $\mathbb{Z}/mn\mathbb{Z}$ est le produit direct de H et K.

Remarque. *on peut généraliser la notion de produit direct à un famille finie : $H_1, \cdots, H_r$*

1. *$H_i \lhd G$ pour tout $1 \leq i \leq r$.*
2. *Pour tout $g \in G$*

$$\exists!(h_1 \cdots, h_r) \in H_1 \times \cdots \times H_r \quad tel\ que \quad g = h_1 \cdots h_r.$$

Proposition 2.33. *Soient G un groupe, $H \lhd G$ et $K \lhd G$ tels que*

1. *$H \cap K\{e\}$.*
2. *$G = HK$.*

Alors G est le produit direct de H et K.

Démonstration : Le deuxième point implique que pour tout $g \in G$ il existe $(h, k) \in H \times K$ tel que $g = hk$. Unicité, supposons que

$$h_1k_1 = h_2k_2,$$

alors

$$h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = \{e\} \implies h_1 = h_2 \quad \text{et} \quad k_1 = k_2.$$

■

Remarque. *On peut généraliser le résultat de la proposition précédente à une famille finie $H_i \lhd G$ pour $1 \leq i \leq r$.*

1. *$H_1 \cdots H_{i-1} \cap H_i = \{e\}$ pour $2 \leq i \leq r$.*
2. *$G = H_1 \cdots H_r$.*

Alors G est le produit direct des sous-groupes $H_1, \cdots, H_r$.

Corollaire 2.34. *Soit G un groupe. On suppose que G est le produit direct de H et K (reps. d'un nombre fini $H_1, \cdots, H_r$). Alors tout élément de H (reps. de H_i) commute avec tout élément de K (reps. de H_j pour $i \neq j$).*

Démonstration : Soit $(x, y) \in H \times K$, comme $H \lhd G$ et $K \lhd G$, alors

$$xyx^{-1}y^{-1} = x(yx^{-1}y^{-1}) = (xyx^{-1})y^{-1} \in H \cap K = \{e\},$$

alors

$$xy = yx.$$

■

Remarque. *Un produit cartésien de deux (ou d'un nombre fini) de sous-groupes n'est pas nécessairement un produit direct. Par contre un produit direct est un produit cartésien.*

Proposition 2.35. *1) Si G est un produit cartésien de deux groupes H et K ($G = H \times K$) (reps. $H_1, \cdots, H_r$), alors il existe $N \lhd G$ et $M \lhd G$ (resp. $N_1, \cdots, N_r$) tels que $H \simeq N$ et $K \simeq M$ (resp. $H_i \simeq N_i$) tel que G est le produit direct de N et M (reps. N_i).*
2) Si G est le produit direct de H et K (reps. $H_1, \cdots, H_r$), alors G est isomorphe au produit cartésien de sous-groupes isomorphes à H et K (reps. H_i)

$$G = HK \simeq H \times K$$

Démonstration : 1) On prend

$$N = H \times \{e\} \quad \text{et} \quad M = \{e\} \times K,$$

on a

$$N \lhd G \quad \text{et} \quad M \lhd G$$

et

$$N \cap M = \{(e, e)\}$$

de plus pour $g = (h, k) \in G$, on a

$$g = (h, e)(e, k).$$

Donc G est le produit direct de N et M.
2) G produit direct de H et K (rappelons que les éléments de H commutent avec les éléments de K). Soit

$$\begin{aligned} \varphi : \quad & HK \longrightarrow H \times K \\ & g = hk \longmapsto (h, k), \end{aligned}$$

on a

$$\begin{aligned} \varphi(gg') = \varphi\Big((hk)(h'k')\Big) = \varphi(hkh'k') = \varphi(hh'kk') &= (hh', kk') \\ &= (h, k)(h', k') \\ &= \varphi(g)\varphi(g') \end{aligned}$$

d'où φ est un morphisme de groupes. Il est clair que φ est surjectif. De plus

$$\varphi(g) = \varphi(g') \implies (h, k) = (h', k')$$

et par suite φ est injectif. Donc φ est un isomorphisme. ■

Théorème 2.36. *Soit G un groupe fini, dont tous les sous-groupes de Sylow sont distingués, alors*

$$\begin{aligned} G = & \text{ produit direct de ses sous-groupes de Sylow} \\ \simeq & \text{ au produit cartésien de ses sous-groupes de Sylow.} \end{aligned}$$

Exemple. *Un groupe G d'ordre 35 est cyclique*

$$G = \mathbb{Z}/5\mathbb{Z}\ \mathbb{Z}/7\mathbb{Z} \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}.$$

Démonstration : Par récurrence sur le nombre de sous-groupe de Sylow.
Si $k = 2$: H_1 et H_2 sont les deux sous-groupes de Sylow de G

$$H_1 \lhd G \quad et \quad H_2 \lhd G \quad \text{tels que } |H_1| = p_1^{\alpha_1} \text{ et } |H_2| = p_2^{\alpha_2}$$

comme $p_1 \neq p_2$, alors $H_1 \cap H_2 = \{e\}$. Donc

$$\left.\begin{array}{l} |G| = p_1^{\alpha_1} p_2^{\alpha_2} \\ H_1 H_2 \leq G \\ |H_1 H_2| = p_1^{\alpha_1} p_2^{\alpha_2} \end{array}\right\} \Longrightarrow G = H_1 H_2 \simeq H_1 \times H_2.$$

Supposons que le résultat est vrai pour $k = n$. Montons le résultat pour $k = n + 1$?
On pose

$$K = H_1 \cdots H_n,$$

on a

$$K \lhd G \quad \text{car pour tout } (g, k) \in G \times K,\ gkg^{-1} = gh_1g^{-1}gh_2g^{-1} \cdots gh_ng^{-1} \in K.$$

Ainsi l'hypothèse de récurrence, implique que

$$K \simeq H_1 \times \cdots \times H_n,$$

de plus

$$|K| = \prod_{i=1}^{n} p_i^{\alpha_i}, \quad H_{n+1} \lhd G,\ |H_{n+1}| = p_{n+1}^{\alpha_{n+1}} \quad \text{et} \quad KH_{n+1} \leq G$$

$$\text{avec} \quad |KH_{n+1}| = \prod_{i=1}^{n+1} p_i^{\alpha_i} = |G|.$$

Donc

$$G = KH_{n+1} \simeq K \times H_{n+1} \simeq H_1 \times \cdots H_{n+1}.$$

■

Remarques. *1. Soit G un groupe tel que $|G| = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ où $p_1, \cdots, p_k$ sont des nombres premiers distincts et $\alpha_i \in N^*$. Si pour $1 \leq i \leq k$, G ne possède qu'un seul p_i-sous-groupe de Sylow. Alors*

$$G = P_1 \cdots P_k \simeq P_1 \times \cdots \times P_k.$$

2. Soit G un groupe abélien tel que

$$|G| = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

où $p_1, \cdots, p_k$ sont des nombres premiers distincts et $\alpha_i \in N^*$. Alors

$$G = P_1 \cdots P_k \simeq P_1 \times \cdots \times P_k.$$

Lemme 2.37. *Soient G un groupe abélien et $(H_i)_{1\leq r\leq k}$ une famille de sous-groupes d'ordre deux à deux premiers. Alors*

$$H = H_1 \cdots H_k \simeq H_1 \times \cdots \times H_k.$$

Démonstration : On a

$$H_k \lhd G \quad \forall\, 1 \leq i \leq k \qquad \text{car } G \text{ est abélien,}$$

alors

$$H \lhd G.$$

Montrons que

$$(H_1 \cdots H_r) \cap H_{r+1} = \{e\} \quad \forall\, 1 \leq r \leq k-1?$$

Soit $d_r = |H_r|$ pour tout $1 \leq r \leq k$. On a

$$|H_1 \cdots H_r| \quad \text{divise } ppcm(d_1, \cdots, d_r),$$

alors

$$|H_1 \cdots H_r| \wedge |H_{r+1}| = 1.$$

Donc

$$(H_1 \cdots H_r) \cap H_{r+1} = \{e\} \quad \forall\, 1 \leq r \leq k-1,$$

et par suite H est le produit direct de $(H_i)_{1\leq r\leq k}$, ainsi

$$H = H_1 \cdots H_k \simeq H_1 \times \cdots \times H_k.$$

■

Proposition 2.38. *Soit G un groupe abélien d'ordre n, alors pour tout d diviseur de n, G admet un sous-groupe d'ordre d.*

Démonstration : On a

$$n = \prod_i p_i^{\alpha_i}, \qquad \text{alors} \quad d = \prod_{i=1}^{k} p_i^{\beta_i},$$

et par suite le théorème de Cauchy, implique l'existence d'un p_i-sous-groupe de G d'ordre $p_i^{\beta_i}$: H_i pour tout $1 \leq i \leq k$. Donc le lemme précédent, implique que

$$H = \prod_{i=1}^{k} H_i \simeq H_1 \times \cdots \times H_k$$

est un sous-groupe de G d'ordre d. ■

Définition 2.39. *Soit G un groupe d'élément neutre e. On appelle exposant de G le plus petit entier strictement positif n, s'il existe tel que*

$$g^n = e \quad \forall\, g \in G$$

s'il n'existe pas, on dit que l'exposant est infini. (i.e, l'exposant de G est ppcm des ordres des éléments de G).

Proposition 2.40. *Soit G un groupe abélien fini. Alors*

1. *L'exposant de G est le maximum des ordres des éléments de G.*
2. *Il existe $x \in G$ d'ordre l'exposant de G.*
3. *L'ordre de tout élément divise l'exposant de G.*
4. *L'exposant d'un groupe a les mêmes facteurs premiers que l'ordre du groupe.*
5. *L'exposant d'un groupe divise l'ordre du groupe.*

Démonstration : 1) Soit m le maximum des ordres des éléments de G et $x \in G$ tel que

$$| < x > | = m$$

Montrons que l'ordre de tout élément de G divise m?
Soit $y \in G$ tel que $| < y > | = q$, alors il existe $z \in G$ tel que

$$| < z > | = ppcm(m, q) \geq m,$$

or m est le maximum, alors

$$ppcm(m, q) = m \implies q \quad \text{divise } m.$$

2) D'après 1).
3) D'après la définition.
4) On a

$$|G| = p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

ainsi le théorème de Cauchy, implique qu'il existe $(x_1, \cdots, x_k) \in G^k$ tel que

$$| < x_i > | = p_i \quad \text{pour tout } 1 \leq i \leq k.$$

5) Comme l'exposant de G est égal à l'ordre d'un point x, d'où l'exposant divise l'ordre de G (théorème de Lagrange). ■

Proposition 2.41. *Soit G un groupe abélien fini et x un élément d'ordre maximal dans G. Alors*

1. *Il existe un morphisme de G dans $< x >$ qui envoie x sur x.*
2. *Il existe $K \leq G$ tel que*

$$G =< x > K \simeq < x > \times K.$$

Démonstration : 1) Soit $H \leq G$ tel que $x \in H$, supposons qu'il existe

$$\varphi : \quad H \longrightarrow < x >$$

tel que $\varphi(x) = x$.
Soient $y \in G \setminus H$ avec $| < y > | = n$,

$$\begin{aligned} \widetilde{\varphi} : \quad & \mathbb{Z}/n\mathbb{Z} \times H \longrightarrow < x > \\ & (\overline{k}, h) \longmapsto x^{kl}\varphi(h) \end{aligned}$$

et

$$\begin{aligned} p : \quad & \mathbb{Z}/n\mathbb{Z} \times H \longrightarrow < y, H > \\ & (\overline{k}, h) \longmapsto y^k h \end{aligned}$$

des morphismes où l est un entier à déterminer.

$$\widetilde{\varphi} \quad \text{bien définie} \iff x^{nl} = e \ (h = x)$$

or $| < x > | = m$, d'où

$$m \quad \text{divise} \quad nl. \tag{2.1}$$

Comme p est surjectif, alors

$$< y, H > \simeq \mathbb{Z}/n\mathbb{Z} \times H \Big/ \ker(p).$$

On a

$$(\overline{k}, h) \in \ker(p) \iff y^k h = e \iff h = y^{-k} \in H \cap < y >,$$

comme $< y >$ est cyclique, alors $H \cap < y > = < y^\beta >$ avec β divise n. Donc

$$\ker(p) = < (\beta, y^{-\beta}) > .$$

D'une autre côté

$$\widetilde{\varphi}(\overline{\beta}, y^{-\beta}) = x^{\beta l}\varphi(y^{-\beta})$$

or $\varphi : \quad H \longrightarrow < x >$, posons

$$\varphi(y^\beta) = x^\alpha,$$

et par suite

$$\widetilde{\varphi}(\overline{\beta}, y^{-\beta}) = x^{\beta l - \alpha}. \tag{2.2}$$

Soit $q : \quad < y, H > \longrightarrow < x >$ un morphisme de groupes tel que $\widetilde{\varphi} = q \circ p$, alors

$$\ker(p) \subset \ker(\widetilde{\varphi}),$$

ainsi l'égalité (2.2), implique que

$$\widetilde{\varphi}(\overline{\beta}, y^{-\beta}) = e \qquad \text{si } l = \tfrac{\alpha}{\beta}.$$

Vériffions que (2.2) compatible avec (2.1) et $l \in Z$.
On a β divise n et $\varphi(y^\beta) = x^\alpha$ donc

$$\begin{aligned}\varphi\Big(y^{\beta\frac{\alpha n}{\beta}}\Big) &= \varphi(y^{\alpha n}) = x^{\frac{\alpha n}{\beta}} \\ &= \varphi(e) \\ &= e,\end{aligned}$$

d'où m divise $\frac{\alpha n}{\beta} = ln$ d'où (2.1) vérifié. Comme m l'exposant de G, alors n divise m de plus m divise $\frac{\alpha n}{\beta}$, alors β divise α, c'est-à-dire, $l \in \mathbb{Z}$.
2) On a

$$\begin{aligned}\varphi : \quad & G \longrightarrow < x > \\ & g \longmapsto \varphi(g)\end{aligned}$$

tel que $\varphi(x) = x$. De plus

$$K \ker(\varphi) \lhd G \quad \text{et} \quad K \cap < x >= \{e\} \quad \text{car} \quad \varphi_{|<x>} = Id_{<x>},$$

et par suite théorème d'isomorphisme, implique que

$$G/K \simeq < x > \Longrightarrow |G| = |K|| < x > | \Longrightarrow G =< x > K \simeq < x > \times K.$$

■

Théorème 2.42. *Pour tout groupe G abélien fini non trivial, il existe r entiers : $d_1, \cdots, d_r$ tels que*

1. $d_1 \geq 2$.
2. d_i *divise* d_{i+1} *pour tout* $1 \leq i \leq r-1$.
3. $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$.

$(d_1, \cdots, d_r)$ *unique.*

Démonstration : **Existence** : G groupe abélien fini d'exposant d_r, soit $x_d \in G$ tel que $| < x_d > | = d_r$, on noté

$$H_{d_r} =< x_d > \simeq \mathbb{Z}/d_r\mathbb{Z}.$$

La proposition précédente, implique qu'il existe $K_{d_{r-1}} \leq G$ tel que

$$G =< x_d > K_{d_{r-1}} \simeq H_{d_r} \times K_{d_{r-1}}.$$

Si $K_{d_{r-1}} \neq \{e\}$, on recommence en remplaçant G par $K_{d_{r-1}}$ et portant d'un élément $x_{d_{r-1}}$ d'ordre l'exposant de $K_{d_{r-1}}$. Après un nombre fini d'étapes on a $K_0 = \{e\}$. C'est clair que d_i divise d_{i+1} pour tout $1 \leq i \leq r-1$ puisque il s'agit d'exposant.
Unicité : Si

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z} \simeq \mathbb{Z}/d'_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d'_r\mathbb{Z}$$

l'exposant de G : d_r et d'_r donc $d_r = d'_r$. Ainsi

$$\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_{r-1}\mathbb{Z} \simeq \mathbb{Z}/d'_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d'_{r-1}\mathbb{Z}$$

de même, on trouve $d_{r-1} = d'_{r-1}$, jusque'à on obtient $d_1 = d'_1$. ■

Exemple. *Soit G un groupe abélien d'ordre* 300. *On a*

$$|G| = 2^2 \cdot 3 \cdot 5^2$$

à isomorphisme près il y a 4 *groupes*

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}.$$
$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z}.$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/150\mathbb{Z}.$$
$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} \simeq \mathbb{Z}/300\mathbb{Z}.$$

Remarque. *Un groupe abélien fini dont l'ordre est sans facteur carré est cyclique, i.e, si*

$$|G| = p_1 \cdots p_r \implies G \simeq \mathbb{Z}/p_1 \cdots p_r\mathbb{Z}.$$

2.4 Série numéro II

Exercice 1 : Soit X un ensemble non vide. Vérifier que l'application $\varphi : S(X) \times X \longrightarrow X$ définie par $\varphi(\sigma, x) = \sigma(x)$ est une action de $S(X)$ sur X. Cette action est-elle transitive ?

Exercice 2 : Soit $S^1 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$. Vérifier que l'application $\varphi : \mathbb{R} \times S^1 \longrightarrow S^1$ définie par $\varphi(\lambda, (x, y)) = (x \cos\lambda + y \sin\lambda, -x \sin\lambda + y \cos\lambda)$ est une action de $\mathbb{R}$ sur S^1. Cette action est-elle transitive ?

Déterminer $G_{(1,0)}$. En déduire que $\mathbb{R}/2\pi\mathbb{Z}$ est en bijection avec S^1.

Exercice 3 : Soit G un groupe et H un sous-groupe d'indice fini n. On note par H' l'intersection des conjugués de H par les éléments de G.

1. Montrer que H' est un sous-groupe distingué de G.
2. Montrer que H' est d'indice fini dans G.
3. Montrer que H' est le plus grand sous-groupe distingué de G contenu dans H.

Exercice 4 : Soit G un groupe fini agissant sur un ensemble fini X.

1. On suppose que toute orbite contient au moins deux éléments, que $|G| = 15$ et que $\text{card}(X) = 17$. Déterminer le nombre d'orbites et le cardinal de chacune.
2. On suppose que $|G| = 33$ et $\text{card}(X) = 19$. Montrer qu'il existe au moins une orbite réduite à un élément.

Exercice 5 : Soient G un groupe d'ordre 35 et X un ensemble de cardinal 19 muni d'une action $\varphi : G \times X \longrightarrow X$ qui ne fixe aucun élément de X. Quel est le nombre d'orbites pour l'action φ.

Exercice 6 : Soit G un groupe infini admettant un sous-groupe H propre d'indice fin. Montrer que G n'est pas simple.

Exercice 7 : Soient G un groupe fini non réduit à l'élément neutre et p le plus petit nombre premier divisant $|G|$. Montrer que tout sous-groupe H de G d'indice p est distingué dans G.
Indication : Considérer l'action par translations à gauche de G sur l'ensemble quotient G/H.

Exercice 8 : Soit G un groupe fini. Soit p un diviseur premier de l'ordre de G.

1. Soit S un p-sous-groupe de Sylow de G. Montrer que les trois assertions suivantes sont équivalentes :
   - S est l'unique p-sous-groupe de Sylow de G.
   - S est stable par tout automorphisme de G.
   - S est distingué dans G.
2. Soit K un sous-groupe distingué de G tel que p divise $|K|$. Montrer que si H est un p-sous-groupe de Sylow de K, distingué dans K, alors H est distingué dans G.

Exercice 9 : Soient p et q deux nombres premiers distincts, avec $q > p$. Soit G un groupe d'ordre pq. Soit H un sous-groupe d'ordre q de G.

1. Montrer que H est distingué dans G. En déduire un morphisme de groupes de G dans $Aut(H)$.
2. Quel est l'ordre du groupe $Aut(H)$.
3. Si p ne divise pas $q - 1$, montrer que G est cyclique.

Exercice 10 : Soit G un groupe simple d'ordre 60.

1. Calculer le nombre de 5-sous-groupes de Sylow de G.
2. Montrer que G est isomorphe à un sous-groupe de S_6.
3. En déduire que G est isomorphe à un sous-groupe de A_6.

Exercice 11 : Montrer que tout groupe d'ordre 56 a au moins un sous-groupe distingué non trivial.

Exercice 12 : Soient G un groupe, p un nombre premier divisant l'ordre de G et H un sous-groupe de G. Montrer que si P est un p-sous-groupe de Sylow de G tel que $N_G(P) \subset H$, alors $N_G(H) = H$.

Exercice 13 : Montrer qu'un groupe d'ordre pqr avec p, q et r premiers distincts n'est pas simple.

Exercice 14 : Montrer qu'un groupe G d'ordre 300 n'est pas simple.

Indication : On pourra considérer le noyau de l'action de G sur $S_6(G)$.

Exercice 15 : 1. Montrer qu'il n'existe pas de groupe simple d'ordre 63.

2. Quels sont les groupes simples abéliens.

Exercice 16 : Soit p un nombre premier.

1. Montrer que tout groupe d'ordre p^2 est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.
2. Soit G un groupe abélien d'ordre p^3.
   - Montrer que si G possède un élément d'ordre p^3, alors G isomorphe à $\mathbb{Z}/p^3\mathbb{Z}$.
   - Montrer que si tous les éléments non triviaux de G sont d'ordre p, alors G est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^3$.
   - On suppose que G ne possède pas d'élément d'ordre p^3, mais un élément g d'ordre p^2. En dénombrant les éléments d'ordre p^2 dans G, montrer qu'il existe un élément d'ordre p hors de $\langle g \rangle$. En déduire que G isomorphe à $\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Exercice 17 : Soit G un groupe simple d'ordre 60.

1. Si H est un sous-groupe de G d'indice $n > 1$, montrer que $n \geq 5$ (pourra considérer l'action à gauche de G sur l'ensemble G/H).
2. Soit S un 2-sous-groupe de Sylow de G. Montrer que $[G : N_G(S)]$ est égal à 5 ou 15.
3. Dans toute cette question, on suppose $[G : N_G(S)] = 15$.
   - Montrer qu'il existe deux 2-sous-groupe de Sylow de G d'intersection non triviale. Soit τ un élément non trivial qui est dans l'intersection de deux 2-sous-groupe de Sylow distincts.
   - Soit C_τ le centralisateur de τ dans G, c'est-à-dire le sous-groupe de G formé des éléments qui commutent avec τ. Montrer que $[G : C_\tau] = 5$.
4. Montrer alors que tout groupe simple G d'ordre 60 possède un sous-groupe d'indice 5. En déduire que G est isomorphe à A_5.

Exercice 18 : Soient p, q deux nombres premiers et G un groupe d'ordre p^2q.

1. Montrer que G n'est pas simple.
2. On suppose que $p^2 - 1$ n'est pas divisible par q et $q - 1$ n'est pas divisible par p. Montrer que G est abélien.

Exercice 19 : Soit G un groupe d'ordre 30. Notons n_3 (resp. n_5) le nombre de 3-sous-groupe de Sylow de G (resp. le nombre de 5-sous-groupe de Sylow de G).

1. Donner les valeurs possibles de n_3 et n_5.
2. Supposons que $n_3 \neq 1$ et $n_5 \neq 1$.
   — Déterminer les nombres des éléments d'ordre 3 et d'ordre 5.
   — En déduire que $n_3 = 1$ ou $n_5 = 1$.
3. Soient P un 3-sous-groupe de Sylow de G et Q un 5-sous-groupe de Sylow de G. Notons $N = PQ$.
   — Montrer que N est un sous-groupe distingué de G d'ordre 15.
   — Montrer que P et Q sont distingués dans N.
   — Montrer alors que N isomorphe est à $P \times Q$. En déduire que N est cyclique.
4. Déterminer le nombre des éléments d'ordre 15 dans G :
   — Dans le cas où $n_3 \neq 1$.
   — Dans le cas où $n_5 \neq 1$.
5. En déduire que $n_3 = 1$ et $n_5 = 1$.
6. Soit R un 2-sous-groupe de Sylow de G. Montrer que $G = NR$.

2.5 Correction

Exercice 1 : Comme

$$\varphi(\sigma_1 \circ \sigma_2, x) = \sigma_1 \circ \sigma_2(x) = \sigma_1\Big(\sigma_2(x)\Big) = \varphi\Big(\sigma_1, \varphi(\sigma_2, x)\Big)$$

et

$$\varphi(Id, x) = x,$$

alors $S(X)$ opère sur X. De plus $\forall\,(x, y) \in X^2$, on a :

$$\begin{aligned} &\text{Si} \quad x = y, \quad \text{alors} \quad y = \varphi(Id, x), \\ &\text{si} \quad x \neq y, \quad \text{alors} \quad y = \varphi(\tau_{x,y}, x). \end{aligned}$$

Donc il y a une seule orbite, et par suite, $S(X)$ opère transitivement sur X.
Exercice 2 : On a

$$\begin{aligned} \varphi\Big(\lambda_1 + \lambda_2, (x, y)\Big) &= \Big(x\cos(\lambda_1 + \lambda_2) + y\sin(\lambda_1 + \lambda_2), -xsin(\lambda_1 + \lambda_2) + y\cos(\lambda_1 + \lambda_2)\Big) \\ &= \varphi\Big(\lambda_1, \varphi\Big(\lambda_2, (x, y)\Big)\Big) \end{aligned}$$

et

$$\varphi\Big(0, (x, y)\Big) = (x, y),$$

alors $\mathbb{R}$ opère sur S^1.
Est-ce que $\forall\,(x, y, z, t) \in \mathbb{R}^4$ existe-t-il $\lambda \in \mathbb{R}$ tel que

$$(z, t) = \varphi\Big(\lambda, (x, y)\Big)?$$

C'est-à-dire

$$\begin{cases} z = x\cos(\lambda) + y\sin(\lambda), \\ t = -x\sin(\lambda) + y\cos(\lambda) \end{cases}$$

ça implique

$$\begin{cases} \cos(\lambda) = xz + yt, \\ \sin(\lambda) = yz - xt. \end{cases}$$

Donc $\mathbb{R}$ opère transitivement sur S^1.
Par définition de stabilisateur, on a

$$G_{(0,1)} = \Big\{\lambda \in \mathbb{R} \,|\, \varphi\Big(\lambda, (1, 0)\Big) = (1, 0)\Big\} = 2\pi\mathbb{Z}.$$

Comme l'ensemble quotient $\mathbb{R}/G_{(x,y)}$ est en bijection avec l'orbite de (x, y) $(\Omega_{(x,y)})$ et l'action est transitive, c'est-à-dire, $\Omega_{(x,y)} = S^1$ pour tout $(x, y) \in S^1$, alors $\mathbb{R}/2\pi\mathbb{Z}$ est en bijection avec S^1.
Exercice 3 : On a

$$H' = \bigcap_{g \in G} gHg^{-1}$$

1. évident.
2. Montrons que H' est d'indice fini dans G. Pour cela considérer le morphisme de G à valeurs dans le groupe des permutations des classes à gauche de G modulo H et montrer que le noyau de ce morphisme est le groupe H'.
3. évident.

Exercice 4 : Toute orbite Ω_x est en bijection avec G/Ω_x. Donc le cardinal de Ω_x divise $|G|$. De plus la somme des longueurs des orbites est égale au cardinal de X.
1. On a

$$|G| = 15, \quad card(X) = 17 \quad \text{et} \quad card(\Omega_x) \geq 2 \; \forall \, x \in X.$$

Supposons, on a k orbites avec $card(\Omega_{x_i}) = 3$ ou 5 ou 15 avec

$$card(\Omega_{x_1}) + \cdots + card(\Omega_{x_k}) = 17$$

d'où

$$3p + 5q + 15m = 17,$$

ainsi

$$m = 0, \quad q = 1 \quad \text{et} \quad p = 4.$$

Donc il y a 4 orbites de longueur 3 et une orbite de longueur 5.
2. On a

$$k \cdot 1 + 3p + 11q + 33\lambda = 19,$$

alors

$$\lambda = 0 \quad \text{et} \quad q = 0 \text{ ou } 1.$$

Donc $k \geq 1$.

Exercice 5 : Soient k le nombre d'orbites pour l'action de φ et $x_1, \cdots, x_k$ un système de représentants des orbites de l'action de G sur X. Donc

$$Card(\Omega_{x_i}) = 1 \text{ ou } 5 \text{ ou } 7 \text{ ou } 35.$$

Comme φ ne fixe aucun élément de X, alors

$$Card(\Omega_{x_i}) \geq 2 \quad \forall \, 1 \leq i \leq k,$$

or $\Omega_{x_i} \subset X$, ainsi

$$Card(\Omega_{x_i}) = 5 \text{ ou } 7,$$

d'où

$$5n + 7m = 19$$

et par suite $n = 1$ et $m = 2$. Donc $k = 3$.

Exercice 6 : On fait opérer G sur l'ensemble G/H par translation à gauche

$$\varphi : G \times G/H \longrightarrow G/H$$
$$(g, xH) \longmapsto gxH$$

et par suite il existe un morphisme de groupes

$$\phi : \ G \longrightarrow S_{G/H} \simeq S_n$$

qui n'est pas injective car G est infini et $S_{G/H}$ fini. Donc

$$\{e\} \subsetneq \ker(\phi) \lhd G.$$

Si $\ker(\phi) = G$, alors

$$gxH = xH \quad \forall\, (g, x) \in G^2,$$

pour $x = e$, on aura $g \in H$, c'est-à-dire, $G = H$ absurde. D'où

$$\{e\} \subsetneq \ker(\phi) \subsetneq G.$$

Exercice 7 : On fait opérer G sur l'ensemble G/H par translation à gauche

$$\varphi : G \times G/H \longrightarrow G/H$$
$$(g, xH) \longmapsto gxH$$

et par suite il existe un morphisme de groupes

$$\phi : \ G \longrightarrow S_{G/H} \simeq S_p$$

$\ker(\phi)$ est un sous-groupe distingué en tant que noyau d'un morphisme. Il est inclus dans H car si $gxH = xH$, pour tout $x \in G$, en particulier $gH = H$ et donc $g \in H$. De plus $[G : \ker(\phi)]$ divise $p!$ et $|G|$. Puisque p est le plus petit diviseur premier de l'ordre de G, ainsi le plus grand commun diviseur de $p!$ et de l'ordre de G est p, et par suite $[G : \ker(\phi)]$ divise p. Puisque $\ker(\phi)$ est contenu dans H et que H est d'indice p dans G, on doit avoir $\ker(\phi) = H$, donc H est distingué dans G.

Exercice 8 :

1. i) $\Rightarrow$ ii) Soit $f \in Aut(G)$, alors $f(S)$ est un p-sous-groupe de Sylow de G car $|f(S)| = |S|$. Et par suite $f(S) = S$.
ii) $\Rightarrow$ iii) $f(x) = gxg^{-1}$ (où $g \in G$) est un automorphisme de G. Ainsi $gSg^{-1} = S$, donc S est distingué dans G.
iii) $\Rightarrow$ i) Les p-sous-groupe de Sylow de G sont tous conjuqués à S comme S est distingué dans G, alors ils sont tous égaux à S.
2. On a

$$gKg^{-1} = K \qquad \forall\, g \in G.$$

Comme H est p-sous-groupe de Sylow de K, alors gHg^{-1} est p-sous-groupe de Sylow de $gKg^{-1} = K$ por tout $g \in G$. Or H est distingué dans K, ainsi c'est le seul p-sous-groupe de Sylow de K. Donc

$$gHg^{-1} = H \qquad \forall\, g \in G.$$

Exercice 9 :

1. Le nombre de q-sous-groupe de Sylow de G divise p et congru à 1 modulo q. Donc $n_q = 1$, et par suite H distingué dans G.

$$\begin{aligned} \varphi : G &\longrightarrow Aut(H) \\ g &\longmapsto i_g \qquad \text{avec } i_g(h) = ghg^{-1}. \end{aligned}$$

2. Comme $H \backsimeq \mathbb{Z}/q\mathbb{Z}$, alors $Aut(H) \backsimeq Aut(\mathbb{Z}/q\mathbb{Z}) \backsimeq \mathbb{Z}/(q-1)\mathbb{Z}$, alors $|Aut(H)| = q-1$.
3. Comme $k = |Im(\varphi)|$ divise $q-1$ et $|G| = pq = p(q-1)+p$, alors k divise p, alors $k = 1$ ou p, or p ne divise pas $q-1$, ainsi $k = 1$, et par suite $\varphi(g) = Id$, pour tout $g \in G$. Donc $ghg^{-1} = h$, d'où $H \subset Z(G)$, alors $|G/Z(G)| = 1$ ou p, ce qui implique que $G/Z(G)$ est cyclique. Alors G abélien : En effet
Comme $G/Z(G)$ est cyclique, alors $G/Z(G) =< \overline{a} >$, alors pour tout $g \in G$ il existe $n \in \mathbb{Z}$ et $z \in Z(G)$ tel que

$$g = a^n z$$

Soit $(g_1, g_2) \in G^2$, alors

$$g_1 g_2 = a^{n_1} z_1 a^{n_2} z_2 = a^{n_1+n_2} z_1 z_2 = a^{n_2} z_2 a^{n_1} z_1 = g_2 g_1.$$

Comme $n_p = 1$, alors un p-sous-groupe de Sylow est distingué : K
Comme $p \wedge q = 1$, alors $G \backsimeq G/H \times G/K$

$$\begin{aligned} \psi : G &\longrightarrow G/H \times G/K \\ g &\longmapsto (gH, gK) \end{aligned}$$

$\ker(\psi) = H \cap K = \{e\}$, de plus $|G| = |G/H \times G/K| = pq$ donc $G \backsimeq G/H \times G/K$, de même on a $G/H \backsimeq K$ et $G/K \backsimeq H$, d'où

$$G \backsimeq H \times K \backsimeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \backsimeq \mathbb{Z}/pq\mathbb{Z}.$$

Exemple $|G| = 15$, alors $G \backsimeq \mathbb{Z}/15\mathbb{Z}$.

Exercice 10 : Soit G un groupe simple d'ordre $60 = 2^2 \times 3 \times 5$.

1. Comme $n_5 \equiv 1[5]$, n_5 divise 12 et G simple alors $n_5 = 6$.
2. Soient

$$B = \{5 - \text{sous-groupe de Sylow de } G\}$$

et

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

action de G sur B par conjugaison, alors il existe un morphisme de groupes

$$\begin{aligned} \psi : G &\longrightarrow S(B) \simeq S_6 \\ g &\longmapsto \phi(g) : \qquad \psi(g) \cdot H = gHg^{-1} \end{aligned}$$

on a $\ker(\psi) \lhd G$ comme $card(B) = 6$, alors $\ker(\psi) \neq G$. Or G simple alors $\ker(\psi) = \{e\}$ et par suite $G \simeq \psi(G)$ qui est sous-groupe de S_6.
3. Comme $A_6 \lhd S_6$, alors $\psi^{-1}(A_6) \lhd G$.
Si $\psi^{-1}(A_6) = \{e\}$, on a pour tout $g \in G$,

$$\psi(g^2) = (\psi(g))^2 \in A_6 \qquad \text{car } \varepsilon(\psi(g^2)) = 1$$

ainsi $g^2 = e$ et par suite G abélien absurde. D'où $\psi^{-1}(A_6) = G$, i.e, $\psi(G) \leq A_6$.
Exercice 11 : On a $|G| = 2^3 \times 7$ et par suite $n_2 \in \{1, 7\}$ et $n_7 \in \{1, 8\}$. Si $n_2 = 7$ et $n_7 = 8$, alors il y a 48 éléments d'ordre 7 et cardinal des sous-groupes d'ordre 8 est supérieur à 9, ainsi $48 + 9 = 57 \leq |G| = 56$ absurde, d'où $n_2 = 1$ ou $n_7 = 1$.
Exercice 12 : Rappelons que

$$H \subset N_G(H) = \{g \in G \,|\, gH = Hg\}.$$

Comme $P \subset N_G(P) \subset H$, alors P est un p-sous-groupe de Sylow de H. Soit $n \in N_G(H)$ comme $P \subset H$, alors $nPn^{-1} \subset H$ d'où nPn^{-1} est un p-sous-groupe de Sylow de H, et par suite Théorème de Sylow implique qu'il existe $h \in H$ tel que

$$h(nPn^{-1})h^{-1} = P$$

ainsi $hn \in N_G(P) \subset H$. Donc $n \in H$, i.e, $N_G(H) \subset H$.
Exercice 13 : Supposons que $r < q < p$, alors $n_p \in \{1, qr\}$, $n_q \in \{1, p, pr\}$ et $n_r \in \{1, p, pq\}$.
Si $n_p > 1$, $n_q > 1$ et $n_r > 1$, alors $n_p = qr$, $n_q \geq p$ et $n_r \geq p$.
Comme

l'intersection d'un p-sous-groupe de Sylow de G avec un q-sous-groupe de Sylow de G est $\{e\}$
l'intersection d'un p-sous-groupe de Sylow de G avec un r-sous-groupe de Sylow de G est $\{e\}$
l'intersection d'un q-sous-groupe de Sylow de G avec un r-sous-groupe de Sylow de G est $\{e\}$

alors

$$pqr \geq qr(p-1) + p(q-1) + q(r-1) + 1 = pqr + (p-1)(q-1)$$

absurde. Donc G n'est pas simple.
Exercice 14 : On a $|G| = 2 \times 3 \times 5^2$ avec $n_5 \in \{1, 6\}$. Si $n_5 = 1$, alors G n'est pas simple.
Si $n_5 = 6$, d'après l'exercice 10, on a $\ker(\psi) \lhd G$.
Si $\ker(\psi) = \{e\}$, alors G isomorphe à un sous-groupe de S_6, d'où 300 divise 720 absurde.
Si $\ker(\psi) = G$, alors pour tout $g \in G$, $\psi(g) = Id$, ainsi pour tout $P \in B$

$$gPg^{-1} = P$$

et par suite $n_5 = 1$ absurde. Donc $\ker(\psi)$ est un sous-groupe distingué propre de G.
Exercice 15 : 1. $n_7 = 1$.
2. $\mathbb{Z}/p\mathbb{Z}$ avec p premier.

Exercice 16 : Soit p un nombre premier.

1. Comme $|G| = p^2$, d'où G est abélien s'il existe $g \in G$ tel que $| < g > | = p^2$, alors $G =< g >\simeq \mathbb{Z}/p^2\mathbb{Z}$.
D'après théorème de Cauchy il existe $x \in G$ tel que $| < x > | = p$. Soit $y \in G\backslash < x >$, alors $| < y > | = p$ car on a supposé qu'il n'existe pas un élément d'ordre p^2. Comme G abélien, alors $< x > \triangleleft G$ et $< y > \triangleleft G$ avec $< x > \cap < y >= \{e\}$ et

$$G =< x >< y >\simeq < x > \times < y >\simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

2. Soit G un groupe abélien d'ordre p^3.
   - S'il existe $g \in G$ tel que $| < g > | = p^3$, alors $G =< g >\simeq \mathbb{Z}/p^3\mathbb{Z}$.
   - D'après théorème de Cauchy G possède un sous-groupe H d'ordre p^2 et d'après 1), on aura
   $$H \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$
   car G ne contient pas un élément d'ordre p^2. Soit $x \in G \setminus H$ alors $| < x > | = p$ et $H \cap < x >= \{e\}$, d'où
   $$G \simeq H \times < x >\simeq (\mathbb{Z}/p\mathbb{Z})^3.$$
   - On a $| < g > | = p^2$, d'où
   $$< g >= \{e, g, \cdots, g^p, \cdots, g^{pk}, \cdots, g^{p^2-1}\} \qquad \text{avec } 1 \leq k \leq p-1$$
   Donc $< g >$ contient $p^2 - 1 - (p-1) = p(p-1)$ éléments d'ordre p^2.
   Supposons que pour tout $x \in G\backslash < g >$ l'ordre de x est p^2. Ainsi G contient $p^3 - p^2 + p(p-1) = p^3 - p$ éléments d'ordre p^2 et par suite G contient $p-1$ éléments d'ordre p. Comme G abélien, alors
   $$\begin{aligned} \psi : G &\longrightarrow G \\ y &\longmapsto y^p \end{aligned}$$
   est un morphisme de groupes de plus l'image d'un élément d'ordre p^2 est un élément d'ordre p, ainsi un élément d'ordre p doit avoir au moins $p^3 - p$ antécédents par ψ. De plus le fait que G ne contient pas d'éléments d'ordre p^3, alors $\psi \circ \psi = e$ ainsi $\psi(G) \subset \ker(\psi)$ avec $|\ker(\psi)| = p - 1 + 1 = p$ absurde car $p^3 - p > p$. Donc il existe $x \in G\backslash < g >$ tel que $| < x > | = p$. Et par suite
   $$G \simeq \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

Exercice 17 : Soit G un groupe simple d'ordre 60.

1. G opérer sur G/H par translation à gauche et par suite il existe ψ un morphisme de groupes de G dans $S(G/H)$, avec $\ker(\psi) \triangleleft G$ et $\ker(\psi) \subset H$, ainsi ψ injectif, d'où la première théorème d'isomorphisme implique que 60 divise $n!$. Donc $n \geq 5$.
2. Rappelons que $[G : N_G(S)] = n_2$ avec $n_2 \in \{1, 3, 5, 15\}$ d'après 1) $n_2 \geq 5$ et par suite il est égal à 5 ou 15.
3. Dans toute cette question, on suppose $[G : N_G(S)] = 15 = n_2$.

— Si l'intersection de deux 2-sous-groupe de Sylow est $\{e\}$, alors G contient $15 \times 3 = 45$ éléments d'ordre 4.
Or dans G il y a 6 : 5-sous-groupe de Sylow, d'où 24 éléments d'ordre 5 mais $45+24 = 69 \geq 60 = |G|$ absurde.
— Soit τ un élément non trivial qui est dans l'intersection de deux 2-sous-groupe de Sylow distincts, comme les 2-sous-groupe de Sylow sont abéliens (car ils sont d'ordre 2^2). Donc C_τ contient ces 2-sous-groupe de Sylow, ainsi l'ordre de C_τ est un multiplie de 4 et divisant 60, on sait que ce n'est pas 4 puisqu'il contient les 2-sous-groupe de Sylow et n'est pas 20 car sinon $[G : C_\tau] = 3$ et ce n'est pas 60 car G est simple (si $C_\tau = G$, alors $< \tau > \triangleleft G$). Donc $|C_\tau| = 12$ et par suite

$$[G : C_\tau] = 5.$$

4. Si $[G : H] = 5$ OK, si $[G : H] = 15$ alors il existe τ tel que $[G : C_\tau] = 5$. Donc il existe $K \leq G$ tel que $[G : K] = 5$. Alors d'après 1) G isomorphe à un sous-groupe de S_5 or le seul sous-groupe d'ordre 60 dans S_5 est A_5, d'où

$$G \simeq A_6.$$

Exercice 18 : Soient p, q deux nombres premiers et G un groupe d'ordre p^2q.

1. Supposons que G est simple :
i) Si $p > q$, alors $n_p = q$. Soit B l'ensemble de p-sous-groupe de Sylow de G, on fait opérer G sur B par conjugaison, et par suite il existe un morphisme de groupes ψ de G dans S_q non trivial (i.e, il existe $g \in G$ tel que $\psi(g) \neq Id$) car l'action est transitive, or $\ker(\psi) \triangleleft G$, avec $\ker(\psi) \neq G$ et G simple, d'où $\ker(\psi) = \{e\}$. Donc p^2q divise $q!$, ainsi p divise un entier entre 1 er $q-1$ absurde car $p > q$.
ii) Si $p < q$, d'où $n_q = p$ ou p^2 et par suite $p-1$ ou p^2-1 divisible par q ainsi $p \equiv \pm 1[q]$, d'où $p \geq q-1$. Donc $p = 2$ et $q = 3$, ce que implique qu'il y a 4 : 3-sous-groupe de Sylow qui contiennent 8 éléments d'ordre 3, donc il y a un seul 2-sous-groupe de Sylow (car $|G| = 12$) et par suite il est distingué absurde.

il n'existe pas un groupe simple d'ordre p^2q.

2. $n_p = 1$ er $n_q = 1$. D'où il existe un unique
P : p-sous-groupe de Sylow d'ordre p^2 (P abélien).
Q : q-sous-groupe de Sylow d'ordre q (Q cyclique).
Avec $P \triangleleft G$ et $Q \triangleleft G$. Ce que implique que

$$xy = yx \quad \forall\, (x, y) \in P \times Q \qquad \text{car } P \cap Q = \{e\}$$

d'où PQ abélien et $PQ \simeq P \times Q$, or $|P \times Q| = p^2q = |G|$. D'où $G = PQ$.

Exercice 19 :

1. $n_3 \in \{1, 10\}$ et $n_5 \in \{1, 6\}$.
2. Supposons que $n_3 \neq 1$ et $n_5 \neq 1$.
— 20 éléments d'ordre 3 et 24 éléments d'ordre 5.
— $20 + 24 = 44 > |G| = 30$. Donc $n_3 = 1$ ou $n_5 = 1$.

3. Soient P un 3-sous-groupe de Sylow de G et Q un 5-sous-groupe de Sylow de G. Notons $N = PQ$.

— N est un sous-groupe de G car $n_3 = 1$ ou $n_5 = 1$ (i.e, P ou Q distingué dans G) avec $|N| = 15$ car $P \cap Q = \{e\}$ et par suite $[G : N] = 2$, d'où N distingué de G.

— P est l'unique 3-sous-groupe de Sylow de N et Q est l'unique 5-sous-groupe de Sylow de N, ainsi ils sont distingués dans N.

— On a P et Q sont distingués dans N, $P \cap Q = \{e\}$ et $N = PQ$, ainsi

$$N \simeq P \times Q \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/15\mathbb{Z}.$$

4. Déterminer le nombre des éléments d'ordre 15 dans G :

— Dans le cas où $n_3 \neq 1$. 80 éléments $> |G|$.

— Dans le cas où $n_5 \neq 1$. 48 éléments $> |G|$.

5. En déduire que $n_3 = 1$ et $n_5 = 1$. OK

6. On a R un 2-sous-groupe de Sylow de G et N distingué dans G, et par suite NR est un sous-groupe de G d'ordre 30. Donc

$$G = NR.$$

Chapitre 3

Anneaux et corps

3.1 Anneaux

Définition 3.1. *Un anneau est un ensemble non vide A muni de deux lois de composition internes, notées $+$ et $\cdot$, vérifiant les propriétés :*

1. *$(A, +)$ groupe abélien (on note 0 son élément neutre).*
2. *La multiplication est associative*

$$x(yz) = (xy)z \qquad \forall\, (x, y, z) \in A^3.$$

3. *La multiplication est distributive par rapport à l'addition à gauche et à droite*

$$x(y + z) = xy + xz \qquad et \quad (x + y)z = xz + yz \qquad \forall\, (x, y, z) \in A^3.$$

L'anneau est dit commutatif si la multiplication est commutatif, c'est-à-dire,

$$xy = yx \qquad \forall\, (x, y) \in A^2.$$

On dit que A est unitaire si la multiplication admet un élément neutre. Cet élément est appelé élément unité de A, noté 1 (1_A)

$$x \cdot 1 = 1 \cdot x = x \qquad \forall\, x \in A.$$

Exemples. 1. *$(\mathbb{Z}, +, \cdot)$ est un anneau commutatif unitaire, de même $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$.*

2. *$(\mathcal{M}_n(\mathbb{R}), +, \cdot)$ anneau non commutatif unitaire.*
3. *Soit I intervalle de $\mathbb{R}$, alors $(\mathcal{F}(I, \mathbb{R}), +, \cdot)$ commutatif unitaire.*
4. *$(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ anneau commutatif unitaire ($\overline{x} \cdot \overline{y} = \overline{xy}$).*
5. *Soit A un anneau, on noté $B = A^{\mathbb{N}}$ l'ensemble des suites d'éléments de A qui sont " à support fini", c'est-à-dire, dont tous les termes sont nuls sauf un nombre fini. On note*

$0_B = (0_A, 0_A, \cdots)$. *Pour tout* $f = (a_n)_{n\mathbb{N}}$ *distinct de* 0_B *on appelle degré de* f *le plus grand entier* $n\mathbb{N}$ *tel que* $a_N \neq 0$. *Pour tout* $f = f = (a_n)_{n\mathbb{N}} \in B$ *et* $g = (b_n)_{n\mathbb{N}} \in B$

$$f + g = (a_n + b_n)_{n\mathbb{N}} \qquad et \quad fg = (c_n)_{n\mathbb{N}} \qquad avec \quad c_n = \sum_{k=0}^{n} a_k b_{n-k}.$$

Alors B *est un anneau. Si* A *commutatif (resp. unitaire), alors* B *commutatif (resp. unitaire avec* $1_B = (1_A, 0_A, \cdots, 0_A, \cdots)$*).*
On l'appelle l'anneau des polynômes en une indéterminée à coefficients dans A : $A[X]$

i) *Pour tout* $P \in A[X]$ *avec* $P \neq 0$, *il existe un unique* $n \in \mathbb{N}^*$ *et* $(a_0, \cdots, a_n) \in A^{n+1}$ *tel que*

$$P = a_n X^n + \cdots + a_1 X + a_0$$

avec $n = cd(P)$ *coefficient dominant,* $n = deg(P)$, $deg(0) = -\infty$ *et* $cd(0) = 0$.

ii) *Si* $P = Q$ *si est seulement si* $deg(P) = deg(Q)$ *et ont mêmes coefficients.*

iii) $deg(P + Q) \leq \max(\deg(P), deg(Q))$.

iv) $deg(PQ) \leq deg(P) + deg(Q)$.

Si A *commutatif (resp. unitaire), alors* $A[X]$ *commutatif (resp. unitaire).*

Remarque. *Soit* A *un anneau, alors*

$$0 \cdot a = a \cdot 0 = 0 \qquad \forall\, a \in A.$$

Si A *unitaire, alors*

$$(-1)a = a(-1) = -a \qquad \forall\, a \in A.$$

Si $1 = 0$, *alors* $A = \{0\}$.

3.1.1 Sous-anneaux

Définition 3.2. *Soit* A *un anneau. Une partie* B *de* A *est un sous-anneau de* A *si*

i) $(B, +)$ *est un sous-groupe de* $(A, +)$.

ii) B *stable par la multiplication* ($xy \in B$ *pour tout* $(x, y) \in B^2$).

Si de plus A est unitaire et $1_A \in B$, on dit que B est un sous-anneau unitaire de A.

Remarques. **1)** *Si* B *est un sous-anneau de* A, *alors* B *est un anneau.*

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

3) *Si* A *et commutatif, alors tout sous-anneau est commutatif.*

4) *Pour montrer que* B *est un sous-anneau de* A, *il suffit de prouver que*

1. $B \neq \emptyset$.
2. $x - y \in B$, $\forall\, (x, y) \in B^2$.

3. $xy \in B$, $\forall\,(x,y) \in B^2$.

Unitaire si $1_A \in B$.

Exemples. *1. Si A est un anneau, alors $\{0\}$ et A sont sous-anneaux de A.*

2. A sous-anneau de $A[X]$.

3. Pour $n \geq 2$, $n\mathbb{Z}$ est sous-anneau de $\mathbb{Z}$.

4. $\mathbb{Z}[i] = \{a + ib \,|\, (a,b) \in \mathbb{Z}^2\}$ anneau commutatif unitaire (sous-anneau de $\mathbb{C}$).

5. Pour $d \in \mathbb{N}^*$, que l'on suppose sans facteur carrés (c'est-à-dire, d n'est pas divisible par aucun carré d'entier distinct de 1), alors

$$\mathbb{Z}[w] = \{a + wb \,|\, (a,b) \in \mathbb{Z}^2\}$$

est un anneau commutatif unitaire avec $w^2 = d$.

3.1.2 Groupe des unités

Définition 3.3. *Soit A un anneau unitaire. On appelle unité de A ou élément inversible dans A, tout élément $a \in A$ tel qu'il existe $b \in A$ vérifiant $ab = ba = 1$. On noté a^{-1} l'inverse de A et $U(A)$ l'ensemble des éléments inversibles de A.*

Proposition 3.4. *$U(A)$ est un groupe pour la multiplication.*

Démonstration : On a $U(A) \neq \emptyset$, car $1 \in U(A)$. Soit $(x,y) \in (U(A))^2$, alors

$$(xy)^{-1} = y^{-1}x^{-1} \in A \qquad \text{et} \qquad (xy)(y^{-1}x^{-1}) = 1,$$

et par suite $xy \in U(A)$. Comme la multiplication est associative dans A, alors elle l'est dans $U(A)$. L'élément neutre est 1. Pour $x \in U(A)$, alors $x^{-1} \in U(A)$ car x^{-1} est inversible d'inverse x. ■

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

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

3. $U(\mathbb{Z}/n\mathbb{Z}) = \{\overline{k} \,|\, 0 \leq k \leq n-1;\ k \wedge n = 1\}$

$\overline{k} \in U(\mathbb{Z}/n\mathbb{Z}) \iff$ il existe $u \in \mathbb{Z}$ tel que $\overline{k}\overline{u} = \overline{1} \iff$ il existe $v \in \mathbb{Z}$ tel que $ku - 1 = nv$ $\iff ku + n(-v) = 1$.

3.1.3 Morphisme d'anneaux

Définition 3.5. *Soient A et B deux anneaux. Un morphisme d'anneaux de A dans B est une application $f : A \longrightarrow B$ tel que*

— $f(x+y) = f(x) + f(y)$, $\forall\,(x,y) \in A^2$.

— $f(xy) = f(x)f(y)$, $\forall\,(x,y) \in A^2$.

Si de plus A et B sont unitaires et $f(1_A) = f(1_B)$, on dit que f est un morphisme d'anneaux unitaires.

Proposition 3.6. *Soit $f : A \longrightarrow B$ un morphisme d'anneaux. Alors*

1. $\ker(f) = \{a \in A \,|\, f(a) = 0_B\}$ *est un sous-anneau de* A.
2. $Im(f) = \{b \in A \,|\, \exists\, a \in A,\ f(a) = b\}$ *est un sous-anneau de* B.
3. C *sous-anneau de* A, *alors* $f(C)$ *est un sous-anneau de* B.
4. D *sous-anneau de* B, *alors* $f^{-1}(D)$ *est un sous-anneau de* A.

3.2 Corps

Définition 3.7. *On appelle corps tout anneau unitaire A, dont tout élément non nul est inversible, c'est-à-dire,*

$$U(A) = A^*.$$

Exemples. 1. $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$.

2. $\mathbb{Q}(i) = \{p + iq \,|\, (p, q) \in \mathbb{Q}^2\}$.
3. $\mathbb{Z}/n\mathbb{Z} \Longleftrightarrow n$ *est premier.*

Définition 3.8. *Soit $\mathbb{K}$ un corps. On appelle sous-corps de $\mathbb{K}$ tout sous-anneau unitaire F de $\mathbb{K}$ tel que l'inverse de tout élément non-nul de F appartienne à F.*

3.2.1 Diviseurs de zéro-anneau intègre

Définition 3.9. *Soit A un anneau.*

- *On dit que $a \in A$ est nilpotent s'il existe $n \in \mathbb{N}^*$ tel que $a^n = 0$.*
- *On dit que $a \in A$ est un diviseur de zéro à gauche (resp. à droite) s'il existe $b \in A^*$ tel que $ab = 0$ (resp. $ba = 0$).*
- *Un diviseur de zéro est un diviseur de zéro à gauche et à droite.*
- *On dit que A est intègre si $A \neq \{0\}$ et vérifie la propriété suivante*

$$\forall\, (a, b) \in A^2, \quad ab = 0 \Longleftrightarrow a = 0 \quad ou \quad b = 0.$$

Exemples. 1. $\mathbb{Z}$ *est un anneau intègre.*

2. *Tout corps est un anneau intègre. En effet :*

$$ab = 0 \qquad si\ a = 0\ ou\ b = 0\ ok,$$

si $a \neq 0$, alors $a^{-1}(ab) = b = 0$.

Remarques. **1)** *Si A est un anneau intègre, alors A n'est pas nécessairement un corps (contre exemple $\mathbb{Z}$).*

2) $\mathbb{Z}/5\mathbb{Z}$ *est un anneau intègre car* $\mathbb{Z}/5\mathbb{Z}$ *est un corps.*

3) $\mathbb{Z}/6\mathbb{Z}$ *n'est pas intègre car* $\overline{2}\,\overline{3} = \overline{0}$.

Proposition 3.10. **1)** *Si A est un anneau intègre, alors* $\forall\,(P,Q)\in(A[X])^2$

$$deg(Pq)=deg(P)+deg(Q)$$

et

$$cd(PQ)=cd(P)cd(Q)$$

2) *A intègre $\Longleftrightarrow$ $A[X]$ intègre.*

3) *Si $\mathbb{K}$ est un corps, alors $\mathbb{K}[X]$ est un anneau intègre.*

Démonstration : 1) Si $P=0$ et $Q=0$, le résultat est évident.
Si $P\neq 0$ et $Q\neq 0$ avec

$$P=a_nX^n+\cdots+a_0 \qquad \text{et} \qquad Q=b_mX^m+\cdots+b_0,$$

alors

$$PQ=a_nb_mX^{n+m}+\cdots$$

comme A est intègre alors $a_nb_m\neq 0$ est par suite $cd(PQ)=a_nb_m$ et $deg(PQ)=n+m$.
2) D'après 1) A intègre implique que $A[X]$ intègre. A est un sous-anneau de $A[X]$ ainsi A intègre si $A[X]$ l'est.
3) Comme $\mathbb{K}$ est un corps, alors $\mathbb{K}$ est un anneau intègre est par suite $\mathbb{K}[X]$ est un anneau intègre. ■

Corollaire 3.11. *Si A anneau unitaire intègre, alors $U(A[X])=U(A)$.*

Démonstration : Comme A est un sous-anneau de $A[X]$, alors $U(A)\subset U(A[X])$.
Soit $P\in U(A[X])$, alors il existe $Q\in A[X]$ te que $PQ=QP=1$, or ces deux polynômes sont nécessairement non nuls, ce que implique que $deg(P)+deg(Q)=0$ et par suite $deg(P)=deg(Q)=0$ ainsi $(P,Q)\in A^2$ avec $PQ=1$. D'où $P\in U(A)$. ■

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

Lemme 3.12. *Soient A, B deux ensembles tel que $card(A)=card(B)$ fini et $f:A\longrightarrow B$ une application. Alors les propriétés suivantes sont équivalentes*

1. *f injective.*
2. *f surjective.*
3. *f bijective.*

Théorème 3.13. *Tout anneau intègre unitaire de cardinal fini est un corps.*

Démonstration : Soient $a\in A^*$ et

$$\begin{aligned} f_a :& A\longrightarrow A\\ & x\longmapsto xa. \end{aligned}$$

On a f_a est injective : $xa = ya \iff (x-y)a = 0$ comme $a \neq 0$ alors $x = y$. Ainsi f_a est bijective et pr suite il existe $b \in A$ tel que $ba = 1$, d'où a inversible à gauche. De même on prouver que a inversible à droite ($x \longmapsto ax$). Donc

$$ba = ac = 1 \implies c = bac = b.$$

■

Anneaux produits

Définition et proposition Soient A_1 et A_2 deux anneaux.

1) Le produit cartésien $A_1 \times A_2 = \{(a_1, a_2) \,|\, a_i \in A_i\}$ est un anneau pour les lois définis par

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$$

et

$$(a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2)$$

cet anneau est appelé le produit direct de A_1 et A_2 on le noté $A = A_1 \times A_2$.
Si A_1 et A_2 commutatifs, alors A commutatif.
Si A_1 et A_2 unitaires, alors A unitaire avec $1_A = (1_{A_1}, 1_{A_2})$.

2)

$$\begin{aligned} p_1 : A_1 \times A_2 &\longrightarrow A_1 \\ (a_1, a_2) &\longmapsto a_1 \end{aligned}$$

morphisme d'anneaux (appelé première projection).

$$\begin{aligned} p_2 : A_1 \times A_2 &\longrightarrow A_2 \\ (a_1, a_2) &\longmapsto a_2 \end{aligned}$$

morphisme d'anneaux (appelé second projection).

Remarques. **1)** $A_1 \times A_2 \simeq A_2 \times A_1$.

2) *On définit de même façon le produit direct d'un nombre fini d'anneaux.*

3) *L'anneau $A_1 \times A_2$ n'est pas intègre (même si A_1 et A_2 le sont et même si ce sont des corps)* $(1_{A_1}, 0_{A_2})(0_{A_1}, 1_{A_2}) = 0_A$.

4)

$$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/nm\mathbb{Z} \iff n \wedge m = 1.$$

3.2.2 Corps des fractions d'un anneau intègre

On sait qu'un anneau intègre n'est pas forcément un corps ($\mathbb{Z}$). Le but est de montrer quand peut construire un corps $\mathbb{K}$ à partir d'un anneau intègre A tel que $A \subset \mathbb{K}$ avec $\mathbb{K}$ le plus petit corps qui contient A (exemple $A = \mathbb{Z}$, $\mathbb{K} = \mathbb{Q}$).
Soit A un anneau commutatif unitaire intègre. On définit dans $A \times A^*$ la relation $\mathscr{R}$ par

$$(a, b)\mathscr{R}(c, d) \iff ad = bc.$$

$\mathscr{R}$ est une relation d'équivalence :

i) Réflexive : cette propriété se démonte facilement.

ii) Symétrique : évident.

iii) Transitive

$$(a,b)\mathscr{R}(c,d) \quad \text{et} \quad (c,d)\mathscr{R}(e,f) \iff ad = bc \quad \text{et} \quad cf = de$$

et par suite $adf = bcf$ ainsi $adf = bde$, comme A commutatif, alors $d(af - be) = 0$, or $d \neq 0$ et A intègre, d'où $af = be$, c'est-à-dire, $(a,b)\mathscr{R}(e,f)$.

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

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

On note $\mathbb{K} = A \times A^*/\mathscr{R}$.
Tout couple $(c,d) \in \frac{a}{b}$ s'appelle une représentant de $\frac{a}{b}$, c'est-à-dire, $\frac{a}{b} = \frac{c}{d}$ dans $\mathbb{K} \iff (a,b)\mathscr{R}(c,d)$ dans $A \times A^* \iff ad = bc$ dans A. L'application

$$\begin{aligned} \phi : A &\longrightarrow \mathbb{K} \\ a &\longmapsto \frac{a}{1} \end{aligned}$$

est injective et est appelée injection canonique de A dans $\mathbb{K}$. En effet

$$\phi(a) = \phi(b) \iff \frac{a}{1} = \frac{b}{1} \iff a \cdot 1 = 1 \cdot b \iff a = b.$$

Ainsi on convient d'identifier A avec le sous-ensemble $\phi(A)$ de $\mathbb{K}$. Donc A est un sous-ensemble de $\mathbb{K}$ et on pose $a = \frac{a}{1}$, $\forall\, a \in A$, c'est-à-dire,

$$a = \frac{a}{1} = \{(c,d) \in A \times A^* \,|\, c = ad\} = \frac{ad}{d},\ \forall\, d \in A^*.$$

Les lois de composition interne dans $\mathbb{K}$

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

sont bien définies ? En effet : si

$$\frac{a}{b} = \frac{a'}{b'} \qquad \text{et} \qquad \frac{c}{d} = \frac{c'}{d'}$$

alors

$$ab' = a'b \qquad \text{et} \qquad cd' = c'd$$

ainsi

$$(ad + bc)b'd' = (a'd' + b'c')bd$$

d'où

$$\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$$

de même

$$\frac{ac}{bd} = \frac{a'c'}{b'd'}.$$

$\mathbb{K}$ est un anneau commutatif unitaire ($0 = \frac{0}{1}$ élément neutre pour $+$ et $1 = \frac{1}{1}$ pour multiplication). De plus

$$\phi(a+c) = \frac{a+c}{1} = \phi(a) + \phi(c) \qquad \text{et} \qquad \phi(ac) = \phi(a)\phi(c).$$

Donc A identifiant avec son image $\phi(A)$ (car ϕ injective).
Tout élément non-nul de $\mathbb{K}$ est inversible dans $\mathbb{K}$. En effet :

$$\forall\ \frac{a}{b} \in \mathbb{K}^* \qquad \text{son inverse est } \frac{b}{a} \text{ car } \frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = 1 \text{ car } A \text{ commutatif.}$$

Théorème 3.14. *Soit A un anneau commutatif unitaire intègre. Alors*

1) *$\mathbb{K} = A \times A^*/\mathscr{R}$ est un corps commutatif qui contient A (comme sous-anneau unitaire).*

2) *Si $\mathbb{K}'$ est un corps tel que $A \subset \mathbb{K}' \subset \mathbb{K}$, alors $\mathbb{K}' = \mathbb{K}$.*

Démonstration : Soit $x \in \mathbb{K}$ alors il existe $(a,b) \in A \times A^*$ tel que $x = \frac{a}{b}$, on a $b \in A \subset \mathbb{K}'$ avec $b \neq 0$ comme l'inverse de b dans $\mathbb{K}$ est $\frac{1}{b}$ et $\mathbb{K}'$ est un corps alors $\frac{1}{b} \in \mathbb{K}'$, d'où $a \cdot \frac{1}{b} = \frac{a}{b} = x \in \mathbb{K}'$, ainsi $\mathbb{K} \subset \mathbb{K}'$. Donc $\mathbb{K} = \mathbb{K}'$. ■

Exemples. *1. Le corps de fractions de l'anneau intègre $\mathbb{Z}$ est $\mathbb{Q}$.*

2. Le corps de fractions de l'anneau intègre $\mathbb{R}[X]$ est appelé corps des fractions rationnelles à coefficients réels, on noté $\mathbb{R}(X)$.
Plus généralement si A est un anneau commutatif unitaire intègre le corps de fractions de l'anneau $A[X]$ est appelé corps de fractions rationnelle à coefficients dans A. Ses éléments sont de la forme

$$F(X) = \frac{P(X)}{Q(X)} \qquad \textit{avec} \quad P \in A[X] \quad \textit{et} \quad Q \in A[X] \quad \textit{tel que} \quad Q \neq 0.$$

3. Le corps de fractions de $\mathbb{Z}[i]$ est $\mathbb{Q}(i)$.

3.3 Idéaux et anneaux quotients

Définition 3.15. *Soient A un anneau et I une partie de A.*

— *On dit que I est un idéal à gauche (resp. à droite) de A si :*

a) $I \leq A$.

b) $\forall\,(a,x)\in A\times I$, *on a,* $ax\in I$ *(resp.* $xa\in I$*).*

— *On dit que* I *est un idéal bilatère ou idéal de* A *s'il est à la fois un idéal à gauche et à droite.*

Exemples. **1)** *Si* A *est un anneau, alors* A *et* $\{0\}$ *sont deux idéaux de* A *(idéaux triviaux).*

1) $\forall\, n\in\mathbb{Z}$, $n\mathbb{Z}$ *est un idéal de* $\mathbb{Z}$.

3) *L'ensemble des fonctions qui s'annulent en* 0 *est un idéal de* $\mathcal{F}(\mathbb{R},\mathbb{R})$.

4) *Si* A *est un anneau commutatif, alors*

$(x)=xA=\{xa\,|\,a\in A\}$ *est un idéal de* A*, appelé idéal principal de* A *engendre par* x.

5) $f:A\longrightarrow B$ *morphisme d'anneau, alors*
— $\ker(f)$ *est un idéal de* A.
— *Si* I *idéal de* A*, alors* $f(I)$ *est un idéal de* $f(A)=Im(f)$.
— J *idéal de* B*, alors* $f^{-1}(J)$ *est un idéal de* A.

6) I *et* J *deux idéaux de* A*, alors*
— $I\cap J$ *est un idéal de* A *(*$\cap$ *d'une famille quelconque).*
— $I\cdot J=\{ij\,|\,i\in I,\,j\in J\}$ *est un idéal de* A *appelé produit des idéaux* I *et* J.
— $(I:J)=\{a\in A\,|\,aJ\subset I\}$ *est un idéal de* A *contenant* I*, appelé le conducteur "transporteur" de* J *dans* I.

Remarques. **1)** *Un idéal d'anneau* A *est un sous-anneau de* A.

2) *Dans le cas d'un anneau commutatif, les notions d'idéal à gauche et à droite coïncident.*

3) $\cup$ *de deux idéaux n'est pas idéal (si l'un inclus dans l'autre).*

4) *Dans un anneau unitaire* A*, si un idéal contient* 1_A*, (un élément inversible de* A*), alors il est égal à* A.

Définition 3.16. *Un idéal (à gauche, à droite ou bilatère)* I *est dit propre si* $I\neq\{0\}$ *et* $I\neq A$.

Proposition 3.17. *Soit* A *un anneau commutatif et unitaire. Alors les propriétés suivantes sont équivalentes*

1. A *est un corps*
2. A *ne possède aucun idéal propre.*

Démonstration : "$\Longrightarrow$" A corps et $I\neq\{0\}$ idéal de A. Alors il existe $a\in I\backslash\{0\}$ et par suite a inversible dans A, d'où $aa^{-1}=1_A\in I$. Donc $I=A$.
"$\Longleftarrow$" $(a)=aA$ est un idéal de A (avec $a\neq 0$), alors $aA=A$ ce que implique que $1_A\in aA$ et par suite il existe $b\in A$ tel que $ab=1_A$. D'où A est un corps. ■

Quotient d'un anneau par un idéal

Considérons un anneau A et I un idéal de A, alors $I \lhd A$ et par suite A/I est un groupe, ou A/I est l'ensemble des classes d'équivalence de la relation définie sur A par

$$x \mathscr{R} y \iff x - y \in I,$$

avec

$$\overline{a} = \{b \in A \,|\, a - b \in I\} := a + I$$

ainsi $(A/I, +)$ est un groupe avec $\overline{0} = I$ et

$$\overline{a} \underbrace{+}_{\text{dans } A/I} \overline{b} = \overline{a \underbrace{+}_{\text{dans } A} b} \qquad \forall\, (a, b) \in A^2.$$

On définit dans A/I une multiplication en posant

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b} \qquad \forall\, (a, b) \in A^2.$$

Bien définie, c'est-à-dire, indépendamment des représentants choisis. Soient $x' \in \overline{x}$ et $y' \in \overline{y}$, alors $x - x' \in I$ et $y' - y \in I$, ains $xy - x'y' = x(y - y') + (x - x')y' \in I$, d'où $\overline{xy} = \overline{x'y'}$.

Définition 3.18. *L'ensemble A/I muni de l'addition et la multiplication induites par celles de A est un anneau, appelé anneau quotient de A par I. Il est commutatif et unitaire si A l'est.*

Remarques. **1)**

$$\begin{aligned} \pi : A &\longrightarrow A/I \\ a &\longmapsto \overline{a} \end{aligned} \qquad \textit{morphisme d'anneaux surjectif}$$

2) *Si A anneau et I une partie de A, alors I idéal de $A \iff I$ noyau d'un morphisme d'anneaux.*

Proposition 3.19. *Si I idéal de A, alors les idéaux de A/I sont en bijection avec ceux de A contenant I.*

Démonstration : Si J idéal de A tel que $I \subset I$, alors $\pi(J) = J/I$ est un idéal de A/I. Si K idéal de A/I, alors $\pi^{-1}(K)$ est un idéal de A contenant I. ∎

Exemple. *Les idéaux de $\mathbb{Z}/12\mathbb{Z}$ sont :*

$$12\mathbb{Z}/12\mathbb{Z},\ 6\mathbb{Z}/12\mathbb{Z},\ 4\mathbb{Z}/12\mathbb{Z},\ 3\mathbb{Z}/12\mathbb{Z},\ 2\mathbb{Z}/12\mathbb{Z},\ \mathbb{Z}/12\mathbb{Z}.$$

Théorème 3.20. *Soient A et B deux anneaux.*

1) *Soit $f : A \longrightarrow B$ un morphisme d'anneaux, alors*

$$A/\ker(f) \simeq f(A) = Im(f).$$

2) *Soient I et J deux idéaux de A, alors*

$$\frac{I+J}{J} \simeq I/I \cap J.$$

3) *Soient I et J deux idéaux tel que $I \subset J$, alors*

$$\frac{A/I}{J/I} \simeq A/J.$$

Démonstration : 1)

$$\begin{aligned} f :& A/\ker(f) \longrightarrow f(A) \\ & \overline{x} \longmapsto f(x) \end{aligned} \qquad \text{morphisme d'anneaux injective et surjective}$$

2)

$$\begin{aligned} \varphi :& I \longrightarrow \frac{I+J}{I} \\ & x \longmapsto \overline{x} \end{aligned} \qquad \text{morphisme d'anneaux surjective } \ker(\varphi) = I \cap J$$

3)

$$\begin{aligned} \psi :& A/I \longrightarrow A/J \\ & \overline{x} = xI \longmapsto [x] = xJ \end{aligned} \qquad \text{morphisme d'anneaux surjective } \ker(\psi) = J/I$$

■

3.3.1 Idéal premier - idéal maximal

Proposition 3.21. *Soient A un anneau commutatif unitaire et $P \neq A$ un idéal de A. Alors L'anneau A/P est intègre si et seulement si $\forall\,(a,b) \in A^2$, si $ab \in P$, alors $a \in P$ ou $b \in P$.*

Démonstration : "$\Longrightarrow$" Si $ab \in P$, alors $\overline{ab} = \overline{a}\overline{b} = \overline{0}$ or A/P est intègre, d'où $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$, et par suite $a \in P$ ou $b \in P$.
"$\Longleftarrow$" Si $\overline{a}\overline{b} = \overline{0}$, alors $ab \in P$, ce que implique que $a \in P$ ou $b \in P$, c'est-à-dire, $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$, d'où A/P est intègre. ■

Définition 3.22. *Soient A un anneau P un idéal de A tel que $P \neq A$. P est dit premier s'il vérifie l'une des assertions de la proposition précédante.*

Exemples. **1)** *Si p est un nombre premier, alors $p\mathbb{Z}$ est un idéal premier de $\mathbb{Z}$.*

2) *$\{0\}$ est un idéal premier de $A \Longleftrightarrow A$ intègre.*

3) *$(X) = X\mathbb{Z}[X]$ est un idéal premier de $\mathbb{Z}[X]$.*

Définition 3.23. *Soit A un anneau, un idéal M de A est dit maximal si pout tout idéal I de A tel que $M \subset I \subset A$, on a $I = M$ ou $I = A$, c'est-à-dire, A est le seul idéal contenant M.*

Si M est un idéal maximal d'un anneau commutatif unitaire A, alors A/M ne possède aucun idéal propre est par suite A/M est un corps.
Si A/M est un corps alors A/M ne possède aucun idéal propre, et par suite A ne possède aucun idéal propre contenant M. D'où M est maximal.

Proposition 3.24. *Soit A un anneau commutatif unitaire. Un idéal propre M de A est maximal si et seulement si A/M est un corps.*

Remarques. **1)** *Un corps est un anneau intègre : si M maximal, alors A/M corps, se que implique que A/M anneau intègre et par suite M idéal premier.*

2) *La réciproque est fausse. Par exemple $(X) = X\mathbb{Z}[X]$ est un idéal premier mais n'est pas maximal car $(X) \subsetneq (2, X)$.*

3) *A anneau commutatif unitaire, I idéal de A, alors*

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

4)

$$\begin{aligned} f :&\mathbb{Z}[X] \longrightarrow \mathbb{Z} \\ &P \longmapsto a_0 \qquad \text{morphisme d'anneaux surjectif} \end{aligned}$$

on a $\ker(f) = X\mathbb{Z}[X]$, et par suite, $\mathbb{Z}[X]/\ker(f) \simeq \mathbb{Z}$.
Comme $\mathbb{Z}$ est intègre, alors $\ker(f) = X\mathbb{Z}[X]$ est premier. $\mathbb{Z}$ n'est pas corps, alors $\ker(f) = X\mathbb{Z}[X]$ n'est pas maximal.

Théorème 3.25. *(de Krull) Tout anneau a au moins un idéal maximal.*

C'est-à-dire, tout idéal I de A est contenu dans un idéal maximal de A.

Caractéristique d'un anneau
Soit A un anneau unitaire pour tout $k \in \mathbb{Z}$, on définit l'élément $k \cdot 1$

$$k \cdot 1 = \begin{cases} 0 \quad \text{si } k = 0, \\ 1 + \cdots + 1, \quad k \text{ fois si } k > 0, \\ -1 - \cdots - 1, \quad -k \text{ fois si } k < 0. \end{cases}$$

Lemme 3.26. *Soit A un anneau commutatif unitaire. Alors*

$$\begin{aligned} f :&\mathbb{Z} \longrightarrow A \\ &k \longmapsto k \cdot 1 \qquad \text{morphisme d'anneaux unitaires.} \end{aligned}$$

Définition 3.27. *Soit A un anneau commutatif unitaire. On appelle caractéristique de A, notée $Car(A)$, l'unique entier $k \in \mathbb{N}$ tel que $\ker(f) = n\mathbb{Z}$.*

Si 1 est d'ordre infini (pour l'addition), alors f est injectif, d'où $Car(A) = 0$.
Si 1 est d'ordre n, alors $\ker(f) = n\mathbb{Z}$.

Exemples. **1)** *L'anneau $\mathbb{Z}$, les corps $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont de caractéristique 0.*

2) *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est caractéristique n.*

3) *Si A est caractéristique n, alors $A[X]$ est caractéristique n.*

4) *Pour tout sous-anneau unitaire B de A, on a $Car(B) = Car(A)$.*

Proposition 3.28. *Un anneau intègre est de caractéristique 0 ou un entier premier p.*

Démonstration : Si $Car(A) = n \neq 0$, supposons que n n'est pas premier, alors $n = ab$, et par suite $n \cdot 1 = (a \cdot 1) \cdot (b \cdot 1) = 0$ avec $a \cdot 1 \neq 0$ et $b \cdot 1 \neq 0$ absurde car A intègre. ■

Remarques. **1)** *Soient A et $(a, b) \in A^2$ anneau tel que $ab = ba$, alors*

$$(a + b)^n = \sum_{k=0}^{n} C_n^k a^k b^{n-k}.$$

En particulier si a nilpotent, alors $1 - a$ est inversible.

2) *Si $Car(A) = n$, alors*

$$(a + b)^n = a^n + b^n.$$

Définition 3.29. *Soient A un anneau commutatif unitaire et $(a, b) \in A^2$.*

1) *On dit que a divise b dans A (a/b) si*

$$(b) = bA \subset (a) = aA$$

c'est-à-dire il existe $c \in A$ tel que $b = ac$. On dit que a est un diviseur de b ou b est un multiplier de a dans A.

2) *On dit que a et b sont associés dans A si a divise b et b divise a.*

3) *On dit qu'un élément non nul et non inversible $a \in A$ est un élément irréductible dans A, si ses seuls diviseur dans A sont les unités ou ses associés, c'est-à-dire, si $x = cd$ avec $(c, d) \in A^2$, alors $a \in U(A)$ ou $b \in U(A)$.*

4) *x est dit premier dans A lorsqu'il est non-nul et non inversible dans A et vérifie la condition suivante :*
Si x divise ab avec $(a, b) \in A^2$, alors x divise a ou x divise b, c'est-à-dire l'idéal $(x) = xA$ est un idéal premier de A.

5) *On dit que a et b sont étrangers (ou premier entre eux) dans A si les seuls diviseurs en commun sont les unités.*

Remarques et Exemples. **1)** *$\forall\ (x, y, z) \in A^3$ si x/y et y/z, alors x/z.*

2) *$u \in U(A) \iff uA = A \iff u/y$, $\forall\ y \in A$.*

3) *Si $u \in U(A)$ et x/u, alors $x \in U(A)$.*

4) *x et y associés (x/y et y/x) $\Longleftrightarrow xA = yA \Longleftrightarrow$ il existe $u \in U(A)$ tel que $x = uy$.*

5) *Dans $\mathbb{Z}$ deux entiers m et n sont associés $\Longleftrightarrow m = \pm n$ car $U(\mathbb{Z}) = \{\pm 1\}$.*

6) *Soit $\mathbb{K}$ un corps, deux polynômes P et Q de $\mathbb{K}[X]$ sont associés $\Longleftrightarrow$ il existe $c \in \mathbb{K}^*$ tel que $P = cQ$.*

7) *Deux éléments associés ont les mêmes multiplies et les mêmes diviseurs dans A.*

8) *Un élément de A peut être irréductible dans A mais ne plus l'être dans un anneau contenant A. Par exemple 3 irréductible dans $\mathbb{Z}$, mais dans $\mathbb{Q}$ non.*

9) *Soit A un anneau commutatif unitaire, x irréductible dans $A \Longleftrightarrow xA$ maximal parmi les idéaux principaux distincts de A. En effet :*
Comme x est irréductible, alors $x \notin U(A)$, et par suite $M = xA \neq A$. Soit $J = aA$ un idéal principal distinct de A, supposons que $M \subset J$, alors $x \in J$, ainsi il existe $b \in A$ tel que $x = ab$ comme $a \notin U(A)$ et x irréductible, alors $b \in U(A)$, d'où $a \in M$. Donc $M = J$, c'est-à-dire, M maximal.
Soit $x \in A$ tel que xA maximal parmi les idéaux principaux distinct de A. Soient $(a, b) \in A^2$, tel que $x = ab$, alors $xA \subset aA$.
Si $a \in U(A)$, alors $aA = A$. Sinon, on a $aA \neq A$ comme xA maximal, d'où $aA = xA$, et par suite x et a associés, ainsi il existe $u \in U(A)$ tel que $x = ua = ba$, donc

$$(u - b)a = 0 \qquad \text{or } A \text{ intègre et } a \neq, 0 \text{ d'où } b = u. \text{ Donc } x \text{ irréductible.}$$

10) *Soit A un anneau commutatif unitaire intègre. Alors*

1. *Tout élément de A associé à un élément irréductible dans A est encore irréductible dans A.*
2. *Tout élément associé à un élément premier dans A est encore premier dans A.*

Puisque deux éléments associés a et b

$$(a) = aA = (b) = bA.$$

Proposition 3.30. *Soit A un anneau commutatif unitaire intègre. Alors tout élément premier dans A est irréductible dans A.*

Démonstration : Soit x un élément premier, alors $x \notin U(A)$. Supposons que $x = ab$ avec $(a, b) \in A^2$, alors x/ab, et par suite x/a ou x/b.
Si x/a, alors il existe $y \in A$ tel que $a = xy$, et par suite $x = xyb$, c'est-à-dire $x(1 - yb) = 0$, comme $x \neq 0$ et A intègre, alors $yb = 1$, d'où $b \in U(A)$. On prouve de même $a \in U(A)$ si x/b. ∎

Remarque. *La réciproque est fausse en général.*

$$\mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5} \,|\, (a, b) \in \mathbb{Z}^2\}$$

qui est anneau commutatif, unitaire et intègre. 3 irréductible mais non premier.
3 irréductible, supposons que $3 = xy$ avec $x = a + ib\sqrt{5}$ et $y = c + id\sqrt{5}$, ainsi $9 = |x|^2|y|^2$ donc

$$|x|^2 = |y|^2 = 3 \quad ou \quad |x|^2 = 1 \text{ et } |y|^2 = 9 \quad ou \quad |x|^2 = 9 \text{ et } |y|^2 = 1.$$

Ainsi $x = \pm 1 \in U(\mathbb{Z}[i\sqrt{5}])$ *ou* $y = \pm 1 \in U(\mathbb{Z}[i\sqrt{5}])$.
3 *n'est pas premier, en effet :*

$$3 \text{ divise } \quad 9 = (2 + i\sqrt{5})(2 - i\sqrt{5}) \quad \text{dans } \mathbb{Z}[i\sqrt{5}] \quad \text{mais } 3 \text{ ne divise pas } 2 + i\sqrt{5} \text{ et } 2 - i\sqrt{5}.$$

3.4 Anneaux principal

Définition 3.31. *Un anneau A est dit principal s'il est commutatif, intègre, unitaire et si tout idéal est principal (c'est-à-dire I idéal de $A \Longleftrightarrow$ il existe $a \in A$ tel que $I = aA$).*

Exemples. *1. $\mathbb{Z}$ est un anneau principal.*

2. $\mathbb{Z}[X]$ n'est pas principal, car

$$I = 2\mathbb{Z}[X] + X\mathbb{Z}[X] \quad \text{idéal de } \mathbb{Z}[X] \text{ non principal.}$$

Supposons que $I = P\mathbb{Z}[X]$, alors il existe $Q \in \mathbb{Z}[X]$ tel que $2 = PQ$, d'où $P \in \mathbb{Z}$. Comme $X \in I$, alors il existe $R \in \mathbb{Z}[X]$ tel que $X = PR$. Donc $P = \pm 1$ et $R = \pm X$, ainsi $1 = \pm P \in I$, et par suite il existe $(S, T) \in (\mathbb{Z}[X])^2$ tel que

$$1 = 2S + TX \quad \text{absurde car le coefficient constant de } 2S + TX \text{ est pair.}$$

Proposition 3.32. *Dans un anneau principal tout élément irréductible est premier (notions d'élément premier et élément irréductible coïncident).*

Démonstration : Si x irréductible, alors $x \neq 0$ et $x \notin U(A)$ de plus $M = xA$ est maximal parmi les idéaux principaux de A distinct de A, or tout idéal de A est principal. Donc M est un idéal maximal dans A, et par suite M est un idéal premier dans A. Donc x premier dans A. ■

Dans un anneau principal A
p premier $\Longleftrightarrow$ p irréductible.
Un idéal est premier $\Longleftrightarrow$ est maximal.

3.5 Anneaux euclidien

Définition 3.33. *On appelle anneau euclidien un anneau commutatif, unitaire, intègre et pour lequel il existe une application $\delta : A^* \longrightarrow \mathbb{N}$ vérifient*

1. *Si a/b, alors $\delta(a) \leq \delta(b)$ (i.e, $\delta(a) \leq \delta(\alpha a)$, $\forall\, \alpha \in A^*$).*
2. *Pour tout $(a, b) \in (A^*)^2$ il existe $(q, r) \in A^2$ tel que*

$$a = bq + r \quad \text{avec } r = 0 \text{ ou } \delta(r) < \delta(b).$$

δ s'appelle stathme euclidien ou algorithme euclidien, q quotient et r reste de la division euclidienne de a par b.

Exemples. *1. $\mathbb{Z}$ est un anneau euclidien : $\delta(x) = |x|$.*

2. Si $\mathbb{K}$ corps commutatif, alors $\mathbb{K}[X]$ anneau euclidien : $\delta(P) = deg(P)$.

3. $\mathbb{Z}[i]$ est un anneau euclidien : $\delta(z) = \overline{z}$.
i) $\delta(z_1) \leq \delta(z_1 z_2)$, $\forall\,(z_1, z_2) \in (\mathbb{Z}[i] \setminus \{0\})^2$.
ii) $\frac{u}{v} = \alpha + i\beta$ avec $(\alpha, \beta) \in \mathbb{Q}^2$. Il existe $(a, b) \in \mathbb{Z}^2$ tels que $|\alpha - a| \leq 1/2$ et $|\beta - b| \leq 1/2$. Ainsi $q = a + ib$ et $r = u - qv$ avec $\delta(r) < \delta(v)$ car $|u/v - q|^2 \leq (1/2)^2 + (1/2)^2 < 1$.

Théorème 3.34. *Tout anneau euclidien est principal.*

Démonstration : A euclidien, alors A commutatif, unitaire et intègre. Montrons que tous ses idéaux sont principaux ? Soit I un idéal de A.
Si $I = \{0\}$, alors $I = 0A$.
Si $I = A$, alors $I = 1A$.
Si $I \neq \{0\}$ et $I \neq A$. Soit $E = \{\delta(x) \,|\, x \in I;\, x \neq 0\}$ qui est une partie de $\mathbb{N}$ non vide et minoré, donc E admet un plus petit élément $n = \delta(x)$ avec $x \neq 0$. Soit $a \in A$, alors $a = xq + r$ avec $r = 0$ ou $\delta(r) < \delta(x) = n$, or $r = a - xq \in I$, ainsi $r = 0$, c'est-à-dire, $a = xq \in I \subset xA$. Donc $I = xA$. ■

Remarques. *1. Si A est un anneau euclidien, alors $A[X]$ n'est pas forcement euclidien.*

2. Si A est un anneau principal, alors $A[X]$ n'est pas nécessairement principal.

3. $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}] = \{a + b\frac{1+i\sqrt{19}}{2}\ (a, b) \in \mathbb{Z}^2\}$ anneau principal qui n'est pas euclidien.

Théorème 3.35. *Soit A un anneau commutatif unitaire et intègre. Alors les propriétés suivantes sont équivalentes.*

1. A est un corps.

2. $A[X]$ est un anneau euclidien.

3. $A[X]$ est un anneau principal.

Démonstration : Si A corps, alors $A[X]$ anneau euclidien et par suite $A[X]$ anneau principal.
Si $A[X]$ anneau principal, alors $A[X]$ anneau intègre, ainsi A intègre. Soit

$$\begin{aligned} f : A[X] &\longrightarrow A \\ P &\longmapsto a_0 \end{aligned} \qquad \text{morphisme d'anneaux surjective}$$

ainsi $A[X]/\ker(f) \simeq A$, et par suite $A[X]/\ker(f)$ intègre. Donc $\ker(f)$ est idéal premier, or $A[X]$ principal, d'où $\ker(f)$ est maximal de $A[X]$. Donc $A[X]/\ker(f)$ est un corps, et par suite, A est un corps. ■

Pour montrer q'un anneau commutatif, unitaire et intègre est un anneau euclidien, il suffit de montrer qu'on peut le munir d'un algorithme euclidien. En revanche il est difficile de montrer qu'un anneau commutatif, unitaire et intègre ne peut pas être munir d'aucun algorithme euclidien.

Proposition 3.36. *Soit A un anneau euclidien. Il existe $x \notin U(A)$ tel que l'application de $U(A) \cup \{0\} \longrightarrow A/(x)$ (avec $(x) = xA$) induite par la surjection canonique soit surjective.*

Démonstration : Soit A un anneau euclidien et notons δ son algorithme euclidien.
Si A est un corps, alors $x = 0$.
Sinon, alors l'ensemble des éléments non nuls et non inversible de A est non vide. Soit $x \neq 0$ et $x \notin U(A)$ tel que $\delta(x)$ soit minimal, c'est-à-dire,

$$\delta(x) \leq \delta(y), \qquad \forall (x,y) \in \Big(A \setminus (U(A) \cup \{0\})\Big)^2,$$

x existe car $\delta\Big(A \setminus (U(A) \cup \{0\})\Big)$ est une partie non vide de $\mathbb{N}$.
Soit $a \in A$, alors $a = xq + r$ avec $r = 0$ ou $\delta(r) < \delta(x)$, c'est-à-dire, dans $A/(x)$, on a $\overline{a} = \overline{r}$ avec $r = 0$ ou $\delta(r) < \delta(x)$, or $\delta(x)$ est minimale, donc si $r \neq 0$, alors $r \in U(A)$, si $r = 0$, OK. Ainsi $r \in U(A) \cup \{0\}$. ■

Application Montrons que $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}] = \{a + b\frac{1+i\sqrt{19}}{2}\ (a,b) \in \mathbb{Z}^2\}$ n'est pas euclidien. $U(A) =?$
Soit $y \in U(A)$, alors $yy^{-1} = 1$, et par suite $|y|^2|y^{-1}|^2 = 1$ avec $|y|^2 = a^2 + 5b^2 + ab \in \mathbb{N}$. Donc $a^2 + b^2 + ab \leq |y|^2 = 1$. Mais comme $\frac{1}{2}(a^2 + b^2) \leq a^2 + b^2 + ab \leq 1$, alors $a^2 + b^2 \leq 2$. Ainsi

$$a^2 + b^2 = \begin{cases} 1 \\ \text{ou} \\ 2. \end{cases}$$

Si $a^2 + b^2 = 2$, alors $a^2 = b^2 = 1$ ou $a^2 = 2$ et $b^2 = 0$ ou $a^2 = 0$ et $b^2 = 2$. Remarquons que pour les deux dernières cas c'est impossible.
Si $a^2 = b^2 = 1$ avec $a^2 + b^2 + ab = 1$, alors $ab = -1$. Donc $a = 1$ et $b = -1$, et par suite $y = \frac{1}{2} - \frac{i}{2}\sqrt{19}$ absurde car $|y|^2 = 5$. De même si $a = -1$ et $b = 1$.
Si $a^2 + b^2 = 1$, alors $a^2 = 1$ et $b^2 = 0$ ou $a^2 = 0$ et $b^2 = 1$ deuxième cas impossible. Donc $a^2 = 1$ et $b^2 = 0$, d'où $U(A) = \{-1, 1\}$.
Supposons que A est anneau euclidien, alors il existe $x \in A \setminus \{-1, 0, 1\}$ tel que $A/(x)$ est un anneau fini de cardinal au plus 3.
Or en général $y \in U(A) \Longleftrightarrow \overline{1} = \overline{0}$ dans $A/(y)$. En effet :
Si $y \in U(A)$, alors $yy^{-1} = 1$, et par suite $\overline{y}\overline{y^{-1}} = \overline{1} = \overline{0}$ dans $A/(y)$.
Si $\overline{1} = \overline{0}$ dans $A/(y)$, alors $1 \in (y) = yA$, d'où $y \in U(A)$.
Comme $x \notin U(A)$, alors $A/(x)$ contient au moins 2 éléments. En conclusion $A/(x)$ est un anneau à 2 ou 3 éléments, c'est-à-dire

$$A/(x) \simeq \mathbb{Z}/2\mathbb{Z} \quad \text{ou à} \quad \mathbb{Z}/3\mathbb{Z}.$$

Or $X^2 - X + 5$ admet une racine dans $A/(x)$ qui est égale à la classe modulo x de l'élément $\frac{1+i\sqrt{19}}{2}$, mais $X^2 - X + 5$ n'admet pas de racine ni dans $\mathbb{Z}/2\mathbb{Z}$ ni dans $\mathbb{Z}/3\mathbb{Z}$.

3.6 P. G. C. D et P. P. C. M

Définition 3.37. *Soit A un anneau intègre et commutatif. Soit $(a,b) \in A^2$, on dit que a et b admettent un pgcd, s'il existe un $d \in A$ tel que*

1. *d/a et d/b.*
2. *Si d'/a et d'/b, alors d'/d.*

Remarque. *En général deux éléments n'ont pas nécessairement un pgcd.*

Exemple.

$$A[i\sqrt{5}] = \{n + im\sqrt{5}\} \qquad \textit{anneau commutatif et intègre.}$$

Mais 6 et $4 + 2i\sqrt{5}$ ne possèdent pas un pgcd. En effet
Soit $d = u + iv\sqrt{5}$ un diviseur de 6 et $4+2i\sqrt{5}$, alors $|d|^2 = u^2 + 5v^2$ divise 36, d'où $d = \pm 1$, $\pm(1 - i\sqrt{5})$, ± 2. Comme 2 ne divise pas $1 - i\sqrt{5}$ et que $1 - i\sqrt{5}$ ne divise pas 2, $\cdots$.

Proposition 3.38. *Soit A un anneau commutatif intègre. Soit $(a, b) \in A^2$.*

1. *Si $d = pgcd(a, b) \in A$, alors si $d' = pgcd(a, b) \in A \iff d$ et d' sont associés (ie d/d' et d'/d).*
2. *A unitaire : a et b premiers entre eux $\iff pgcd(a, b) = 1 \iff U(A) =$ l'ensemble des pgcd de a et b.*

Démonstration :

1. d'/a et d'/b, alors d'/d de même d/a et d/b, alors d/d'. D'où d et d' associés.
   Si d et d' sont associés, alors d'/a et d'/b comme d/d', donc $d' = pgcd(a, b)$.
2. Si a et b sont premiers entre eux, alors les seuls éléments de A qui divisent à la fois a et b sont les éléments de $U(A)$.
   Si $pgcd(a, b) = 1$, alors $U(A)$ diviseurs de a et b, ce que implique que a et b premiers entre eux.

■

Remarque. *On dit un pgcd et non pas le pgcd de a et b car on n'est pas unicité. Si d est un pgcd de a et b, on note*

$$d = pgcd(a, b) = a \wedge b.$$

Exemples. 1. *Dans $\mathbb{Z}$, le pgcd de 12 et 30 sont 6 et -6.*
2. *Dans $\mathbb{R}[X]$, le pgcd de $X^2 - 3X + 2$ et $X^2 - 1$ sont $\alpha(X - 1)$ où $\alpha \in \mathbb{R}^*$.*

Proposition 3.39. *Soit A un anneau commutatif, unitaire et intègre. Soit $(a, b) \in (A^*)^2$ si $d = pgcd(a, b)$, alors les éléments (a', b') tel que $a = da'$ et $b = db'$ sont premiers entre eux dans A.*

Démonstration : Soit z un diviseur commun de a' et b', alors $a' = \alpha z$ et $b' = \beta z$, et par suite $a = d\alpha z$ et $b = d\beta z$. Ce que implique que dz est un diviseur de a et b, et par suite dz divise d, d'où $d = dzu$, ainsi $d(1 - zu) = 0$, comme $d \neq 0$ (car $(a, b) \in (A^*)^2$), alors $zu = 1$. Donc $z \in U(A)$, et par suite a' et b' premiers entre eux. ■

Définition 3.40. *Soit A un anneau, un élément $m \in A$ est appelé le plus petit commun multiple de a et b si*

1. *a/m et b/m.*
2. *Si a/m' et b/m', alors m/m'.*

$$m = ppcm(a,b) = a \vee b.$$

Remarque. *Soient A un anneau intègre et $mm = ppcm(a,b)$. Alors*

$$m' = m = ppcm(a,b) \iff m \text{ et } m' \text{ sont associés.}$$

Théorème 3.41. *Soit A un anneau principal. Alors $\forall\,(a,b) \in A^2$ admettent un pgcd et un ppcm.*

1. *$d = a \wedge b \iff (a) + (b) = (d)$.*
2. *$m = a \vee b \iff (a) \cap (b) = (m)$.*

Démonstration : Si $d = a \wedge b$, alors $(a) \subset (d)$ et $(b) \subset (d)$, ce que implique que $(a) + (b) \subset (d)$. D'autre part $(a) + (b) = (c)$, d'où c/a et c/b, et par suite c/d, ainsi $(d) \subset (c)$. Donc $(d) = (c)$.
On a $(a) + (b) = (d)$, d'où $(a) \subset (a) + (b) = (d)$, ainsi d/a de même d/b. Si c/a et c/b, alors $(a) \subset (c)$ et $(b) \subset (c)$, et par suite $(d) = (a) + (b) \subset (c)$, ce que implique que c/d. Donc $d = a \wedge b$.
De même pour ppm. ■

Théorème 3.42. *(Identité de Bézout) Soient A un anneau principal et $(a,b) \in A^2$. Alors*

$$a \text{ et } b \text{ premiers entre eux dans } A \iff \text{il existe } (u,v) \in A^2 \text{ tel que } au + bv = 1.$$

Démonstration : On a $(a) + (b) = (1) = A$, comme $1 \in A$, alors il existe $(u,v) \in A^2$ tel que $au + bv = 1$.
$au + bv = 1$, alors $1 \in aA + bA$ qui est un idéal de A, d'où $aA + bA = A$. Soit $d = pgcd(a,b)$, ainsi $dA = aA + bA = A$, ce que implique que $d \in U(A)$. Donc a et b premiers entre eux dans A. ■

Corollaire 3.43. *Soit A un anneau principal pour tout $(a,b,c) \in A^3$ si a/bc et $a \wedge b = 1$, alors a/c.*

Démonstration : On a $au + bv = 1$, alors $c = cau + cbv$, comme a/bc, d'où $bc \in aA$, ce que implique que $bcv \in aA$, or $acu \in aA$, et par suite $c \in aA$. Donc a/c. ■

Remarques.
1. *Si $d = pgcd(a,b)$, alors il existe $(u,v) \in A^2$ tel que $d = au + bv$.*
   La réciproque est vraie aussi si $d = 1$ (et donc si $d \in U(A)$). Mais si $d \neq 1$, l'existence d'un couple (u,v) tel que $d = au + bv$, n'implique pas que $d = pgcd(a,b)$. Dans $\mathbb{Z}$, on a : $3 \times 10 + (-2) \times 14 = 2$, mais 2 n'est pas un pgcd de 3 et -2 dans $\mathbb{Z}$.
2. *Dans un anneau principal $a \wedge b = 1 \iff a \vee b = ab$.*

Théorème 3.44. *Soit A un anneau principal. Alors toute suite croissante d'idéaux de A est stationnaire, c'est-à-dire, si*

$$I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$$

alors il existe n_0 tel que $I_m = I_{n_0}$ pour tout $m \geq n_0$.

Démonstration : Soit $(I_n)_{n\geq 1}$ une suite croissante d'idéaux de A, comme A principal, alors il existe $b \in A$ tel que

$$\bigcup_{n\geq 1} I_n = bA,$$

or A unitaire, d'où il existe n_0 tel que $b \in I_{n_0}$, et par suite

$$\bigcup_{n\geq 1} I_n = bA \subset I_{n_0} \quad \text{or } I_n \text{ est croissante, donc } I_m = I_{n_0} \text{ pour tout } m \geq n_0.$$

■

Théorème 3.45. *Dans un anneau principal A, tout élément non nul et non inversible est le produit fini d'éléments irréductibles.*

Démonstration : Soit

$$F = \Big\{ a \in A \setminus \big(U(A) \cup \{0\}\big) \;\Big|\; a \text{ n'est pas produit fini d'éléments irréductibles} \Big\}.$$

Montrons que $F = \emptyset$?
Supposons que $F \neq \emptyset$. Soit $a_0 \in F$, alors a_0 n'est pas irréductible dans A. Si a_0 irréductible, alors $a_0 = b_0 c_0$ avec $b_0 \in U(A)$ ou $c_0 \in U(A)$. Donc il existe $(\alpha_1, \beta_1) \in A^2$ non inversibles tel que

$$a_0 = \alpha_1 \beta_1.$$

Si $(\alpha_1, \beta_1) \notin F^2$, alors $a_0 \notin F$. Donc l'un des ces deux éléments est dans F. Supposons que $\alpha_1 \in F$. Notons $\alpha_1 = a_1$, on a $a_0 A \subset a_1 A$. On répète ce procédé à l'élément a_1 et on a un élément a_2 tel que

$$a_0 A \subset a_1 A \subset a_2 A.$$

Avec ce procédé on construit une suite croissante $(a_n A)_{n\geq 0}$, ainsi elle est stationnaire, c'est-à-dire, il existe n tel que

$$a_{n+p} A = a_n A \quad \forall\, p \geq 0.$$

En particulier $a_{n+1} A = a_n A$, d'où il existe $\gamma \in A$ tel que $a_{n+1} = \gamma a_n$. Revenons à l'étape $n+1$ du procédé qui définit notre suite il existe $(\alpha_{n+1}, \beta_{n+1}) \in (A \setminus U(A))^2$ tel que

$$a_n = \alpha_{n+1} \beta_{n+1} \quad \text{avec } a_{n+1} = \alpha_{n+1},$$

ce que implique que

$$a_n = a_{n+1} \beta_{n+1} = \gamma a_n \beta_{n+1},$$

ainsi $\gamma \beta_{n+1} = 1$, et par suite $\beta_{n+1} \in U(A)$ absurde. Donc $F = \emptyset$. Ainsi tout élément non nul et non inversible est le produit fini d'éléments irréductibles. ■

Dans $\mathbb{Z}$, tout entier est produit de nombres premiers.

3.7 Série numéro III

Soit G un groupe d'ordre 285.
1. Montrer que G admet un sous-groupe H d'ordre 5.
2. Montrer que G n'est pas simple.
3. Montrer que G possède un sous-groupe K distingué d'ordre 95.
4. Montrer que G/K est cyclique.
5. Dans le cas où G possède un unique 3-sous-groupe de Sylow, déterminer le groupe G à isomorphisme près.

Exercice 1 : On dit qu'un anneau A est un anneau de Boole si, pour tout $x \in A$, $x^2 = x$. On fixe A un tel anneau.
1. Démontrer que, pour tout $x \in A$, $x = -x$.
2. Montrer que A est commutatif.
3. Montrer que A ne peut pas se réduire à trois éléments.
4. On suppose que A est **unitaire**, fini et de cardinal **strictement** supérieur à 2. Montrer que A possède des diviseurs de zéro.
5. Montrer que si A **unitaire** et $|A| = 4$, alors A est unique à un isomorphisme près.

Exercice 2 : Dans l'anneau A, on suppose que

$$(a^2 - a)b = b(a^2 - a) \qquad \forall,\ (a, b) \in A^2.$$

1. Montrer que $(xy + yx)z = z(xy + yx)$ pour tout $(x, y, z) \in A^3$.
2. Montrer que A est anneau commutatif.

Exercice 3 : Un élément x d'un anneau A est dit nilpotent s'il existe un entier $n \geq 1$ tel que $x^n = 0$. On fixe x, y deux éléments nilpotents tel que $xy = yx$.
1. Montrer que xy est nilpotent.
2. Montrer que $x + y$ est nilpotent.
3. On suppose que A unitaire, montrer que $1_A - x$ est inversible.
4. Soient $u, v \in A$ tel que uv est nilpotent. Montrer que vu est nilpotent.

Exercice 4 : On considère $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2};\ a, b \in \mathbb{Z}\}$.
1. Montrer que $(\mathbb{Z}[\sqrt{2}], +, \times)$ est un anneau.
2. On note $N(a + b\sqrt{2}) = a^2 - 2b^2$. Montrer que, pour tous x, y de $\mathbb{Z}[\sqrt{2}]$, on a $N(xy) = N(x)N(y)$.
3. En déduire que les éléments inversibles de $\mathbb{Z}[\sqrt{2}]$ sont ceux s'écrivant $a+b\sqrt{2}$ avec $a^2-2b^2 = \pm 1$.

Exercice 5 : Pour $n \in \mathbb{N}^*$, on note $\varphi(n)$ le nombre d'éléments inversibles dans $(\mathbb{Z}/n\mathbb{Z}, \times)$.
1. Calculer $\varphi(p)$ et $\varphi(p^\alpha)$ pour p premier et $\alpha \in \mathbb{N}^*$.
2. Soient n et m premiers entre eux. On considère l'application

$$\begin{aligned} f :\ & \mathbb{Z}/nm\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ & \overline{x} \longmapsto (\widetilde{x}, \widehat{x}). \end{aligned}$$

Montrer que f est un isomorphisme d'anneaux. En déduire que $\varphi(nm) = \varphi(n)\varphi(m)$.
3. Exprimer $\varphi(n)$ selon la décomposition primaire de n.

Exercice 6 : Soit $(A, +, \times)$ un anneau commutatif. Si I et J sont deux idéaux de A, on note

$$\begin{aligned} I + J &= \{i + j;\ i \in I, ; j \in J\} \\ I.J &= \{i_1 j_1 + \cdots + i_n j_n;\ n \geq 1,\ i_k \in I,\ j_k \in J\} \end{aligned}$$

On dit que deux idéaux I et J sont étrangers si $I + J = A$.
1. Montrer que $I + J$ et IJ sont encore des idéaux de A.
2. Montrer que $I.J \subset I \cap J$.
3. Montrer que $(I + J).(I \cap J) \subset I.J$.
4. Montrer que si A **unitaire** et I et J sont étrangers, alors $I.J = I \cap J$.

Exercice 7 : Soit A un anneau commutatif (unitaire). Si I est un idéal de A, on appelle radical de I l'ensemble $\sqrt{I} = \{x \in A;\ \exists\, n \geq 1,\ x^n \in I\}$.
1. Montrer que $\sqrt{I}$ est un idéal de A.
2. Soient I, J deux idéaux de A et $p \geq 1$. Montrer que

$$\sqrt{I.J} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J},\ \sqrt{\sqrt{I}} = \sqrt{I} \text{ et } \sqrt{I^p} = \sqrt{I}.$$

3. Si $A = \mathbb{Z}$ et $I = k\mathbb{Z}$, $k \geq 1$, déterminer le radical de I.

Exercice 8 : Soit A un anneau commutatif **unitaire**. On dit qu'un idéal I est premier si $xy \in I \implies x \in I$ ou $y \in I$. On dit que I est maximal si, pour tout idéal J de A tel que $I \subset J$, on a $J = I$ ou $J = A$.
1. Déterminer les idéaux premiers de $\mathbb{Z}$.
2. Soit I un idéal et $x \in A \backslash I$. Soit J l'idéal engendré par I et x. Montrer que

$$J = \{a \in A;\ \exists i \in I,\ \exists k \in \mathbb{Z},\ a = i + kx\}\,.$$

3. En déduire que tout idéal maximal est premier.
4. Montrer que si tous les idéaux de A sont premiers, alors A est un corps.
5. Montrer que si A est principal, tout idéal premier est maximal.
6. Soit I un idéal de A. Montrer que I est premier si et seulement si A/I est intègre. Montrer que I est maximal si et seulement si A/I est un corps. En déduire une autre preuve que I maximal entraine I premier.

Exercice 9 : Soient A et B des anneaux commutatifs unitaires.
1. Si $f : A \longrightarrow B$ est un morphisme d'anneaux unitaires, alors quel que soit Q un idéal premier de B, $f^{-1}(Q)$ est un idédal premier de A qui contient $\ker(f)$.
2. Si $f : A \longrightarrow B$ est un morphisme d'anneaux unitaires surjectif, alors quel que soit P un idéal premier de A contenant $\ker(f)$, $f(P)$ est un idéal premier de B.
3. Soit A un anneau commutatif unitaire et I un idéal de A, distinct de A. Les idéaux premiers de A/I sont de la forme P/I où P est un idéal premier de A contenant I.

Exercice 10 : 1. Dans $\mathbb{Q}[X]$, trouver une expression plus simple des idéaux suivants :
i) $2X\mathbb{Q}[X] + (X + 1)\mathbb{Q}[X]$.
ii) $2X\mathbb{Q}[X] \cap (X + 1)\mathbb{Q}[X]$.

iii) $2X\mathbb{Q}[X].(X+1)\mathbb{Q}[X]$.
2. Déterminer un pgcd des polynômes $P = X^4 + 1$ et $Q = X^3 + X + 1$ dans $\mathbb{Z}/2\mathbb{Z}[X]$ et $\mathbb{Z}/3\mathbb{Z}[X]$.
Dans le cas où P et Q sont premiers entre eux, trouver deux polynômes U et V tels que $UP + VQ = \overline{1}$.

Exercice 11 : Soit A un anneau commutatif. On rappelle que $a \in A^*$ est un diviseur de zéro s'il existe $b \in A^*$ tel que $ab = 0$. Montrer que si A possède exactement n ($n \geq 1$) diviseurs de zéro, alors $|A| \leq (n+1)^2$. (Indication : si $a \in A$ est un diviseur de zéro, on pourra étudier le cardinal de l'idéal $I = \{x \in A \,|\, ax = 0\}$.)

Exercice 12 : On considère l'anneau

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

1. Déterminer $U(\mathbb{Z}[i])$ et $Fr(\mathbb{Z}[i])$.
2. On considère l'application

$$\begin{aligned} f : \quad & \mathbb{Z}[i] \to \mathbb{Z}/10\mathbb{Z} \\ & a + ib \longmapsto \overline{a + 7b}. \end{aligned}$$

a) Montrer que f est un homéomorphisme d'anneaux unitaire surjectif.
b) Montrer que $\mathbb{Z}[i]/(3+i)$ isomorphe à $\mathbb{Z}/10\mathbb{Z}$.
c) $3 + i$ est-il premier dans $\mathbb{Z}[i]$?

Exercice 13 : Soit

$$\mathbb{Z}[\sqrt{-5}] = \{n + im\sqrt{5} \,|\, n, m \in \mathbb{Z}\}.$$

1. Montrer que $\mathbb{Z}[\sqrt{-5}]$ est un sous-anneau intègre de $\mathbb{C}$.
2. Si $a = n + im\sqrt{5}$, on pose $N(a) = n^2 + 5m^2$. Montrer que $N(a) = 0$ si et seulement si $a = 0$ et que $N(a) = 1$ si et seulement si $a = \pm 1$.
3. Montrer que $N(ab) = N(a)N(b)$, pour tout $a, b \in \mathbb{Z}[\sqrt{-5}]$.
4. Montrer que 2 est irréductible dans $\mathbb{Z}[\sqrt{-5}]$ mais que 2 n'est pas un élément premier (Indication : $2.3 = (1 - \sqrt{-5})(1 + \sqrt{-5})$).

Exercice 14 : 1. Soient A un anneau intègre et $(a, b) \in (A^*)^2$ ayant un ppcm noté m. Montrer qu'il existe $d \in A$ tel que $ab = md$ et que d est un pgcd de a et b.
2. Soit l'anneau

$$\mathbb{Z}[i\sqrt{5}] = \{n + im\sqrt{5} \,|\, n, m \in \mathbb{Z}\}.$$

a) Déterminer $U(\mathbb{Z}[i\sqrt{5}])$.
b) Déterminer tous les diviseurs de 9 et de $3(2 + i\sqrt{5})$.
c) Montrer que 1 est un pgcd de 3 et $2+i\sqrt{5}$ et que 3 et $2+i\sqrt{5}$ n'ont pas de ppcm. Conclure
d) Montrer que les éléments 9 et $3(2 + i\sqrt{5})$ n'ont pas de pgcd dans $\mathbb{Z}[i\sqrt{5}]$. 9 et $3(2 + i\sqrt{5})$ admettent-ils un ppcm ?
e) Montrer que l'idéal engendré par 3 et $2 + i\sqrt{5}$ n'est pas principal.

Exercice 15 : Soit A un anneau principal tel que tout suite décroissante d'idéaux est stationnaire. Montrer que A est un corps. (Indication : considérer a un élément non nul et la suite d'idéaux $I_n = (a^n)$).

Exercice 16 : Soit

$$A = \mathbb{Z}[j] = \{P(j) \mid P \in \mathbb{Z}[X]\} \quad \text{où} \quad j = \frac{-1 + i\sqrt{3}}{2}.$$

On note pour tout $z \in \mathbb{C}$, $N(z) = |z|^2$.
1. Vérifier que $\mathbb{Z}[j] = \{a + bj \mid a, b \in \mathbb{Z}\}$.
2. Montrer que A est un anneau euclidien.
3. Déterminer $U(A)$.
4. On suppose que $z, z' \in \mathbb{Z}[i\sqrt{3}] \subset A$, $z' = uz$ avec $u \in U(A)$ et $N(z)$ impair. Montrer que $\frac{z'\overline{z}}{N(Z)} = u \in \frac{1}{2}\mathbb{Z}[i\sqrt{3}]$.
5. En déduire que $u \in \mathbb{Z}[i\sqrt{3}]$ et conclure.

Exercice 17 : On note $A = \mathbb{Z}[\sqrt{2}]$ et $K = \mathbb{Q}[\sqrt{2}]$.
1. Montrer que K est le corps des fractions de A.
2. Pour tout $x = a + b\sqrt{2} \in K$, on pose $\delta(x) = |a^2 - 2b^2|$. Montrer que $\delta(xy) = \delta(x)\delta(y)$ pour tout $(x, y) \in K^2$.
3. Vérifier que pour tout $a \in \mathbb{R}$, il existe $\lfloor a \rceil \in \mathbb{Z}$ tel que $|a - \lfloor a \rceil| \leq \frac{1}{2}$.
4. Pour tout $x = a + b\sqrt{2} \in K$, on pose $[x] = \lfloor a \rceil + \lfloor b \rceil \sqrt{2}$. Montrer que $\delta(x - [x]) \leq \frac{3}{4}$.
5. Montrer que A est euclidien pour δ.

3.8 Correction

Exercice 1 : 1) Comme $x^2 = x$, alors $(x+x)^2 = x + x = x^2 + x^2 + x^2 + x^2 = x + x + x + x$, d'où $x = -x$.
2) $(x+y)^2 = x + y = x^2 + xy + yx + y^2$, ainsi $xy + yx = 0$, est par suite $xy = -yx = yx$.
3) Si $A = \{0, a, b\}$, alors $a + b = 0$, ou a ou b.
Si $a + b = 0$, alors $a = -b = b$ absurde.
Si $a + b = a$, (resp. $a + b = b$) alors $b = 0$ (resp. $a = 0$), absurde.
Donc $|A| \neq 3$. 4) A unitaire tel que $|A| = n \geq .4$ On a

$$x(1+x) = x^2 + x = x + x = 0 \quad \text{avec } x \neq 0 \text{ et } x + 1 \neq 0.$$

5) Si $A = \{0, 1, a, b\}$, alors

$$1 + a = b\,; 1 + b = a,\ a + b = 2a + 1 = 1,\ ab = a(a+1) = 0 = ba.$$

Soit $f : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow A$ avec

$$f(0,0) = 0,\ f(1,1) = 1,\ f(1,0) = a \text{ et } f(0,1) = b.$$

Exercice 2 : On a $(a^2 - a)b = b(a^2 - a)$.
1) Ainsi pour $a = x + y$ et $b = z$, on trouve

$$z(xy + yx) = (xy + yx)z.$$

2) Pour tout $(x, y) \in A^2$, on a $(xy + yx)x = x(xy + yx)$, ainsi $yx^2 = x^2y$, et par suite

$$xy = x^2y - (x^2 - x)y = yx^2 - y(x^2 - x) = yx.$$

Exercice 3 : On a $x^n = y^m = 0$ avec $n \geq 1$ et $m \geq 1$.
1) $(xy)^n = x^n y^n = 0y^n = 0$.
2) $(x+y)^{n+m} = \sum_{k=0}^{n+m} C_{n+m}^k x^k y^{n+m-k} = 0$, car $y^{n+m-k} = 0$ si $k \leq n$ et $x^k = 0$ sinon.
3) On a $1 = 1 - x^n = (1-x)(1 + x + \cdots + x^{n-1})$, et par suite

$$(1-x)^{-1} = \sum_{k=0}^{n-1} x^k.$$

4) On a $(uv)^n = 0$, alors

$$(vu)^{n+1} = v(uv)^n u = 0.$$

Exercice 4 : 1) $\mathbb{Z}[\sqrt{2}]$ sous-anneau de $\mathbb{R}$.
2) C'est évident.
3) Soit $x = a + b\sqrt{2}$ un élément inversible d'inverse y, alors $N(xy) = N(1) = 1$, et par suite $N(x)N(y) = 1$, mais $(N(x), N(y)) \in \mathbb{Z}^2$, alors $N(X) = \pm 1$. Réciproquement si $N(X) = \pm 1$, alors $\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \pm(a - b\sqrt{2})$. Donc $U(\mathbb{Z}[\sqrt{2}]) = \{x \in \mathbb{Z}[\sqrt{2}] \mid N(x) = \pm 1\}$.

Exercice 5 : 1) $\varphi(p) = p - 1$.
On a $p^\alpha \wedge q = 1 \Longleftrightarrow p \wedge q = 1$, or il y a $p^{\alpha-1}$ multiplies de p entre 1 et p^α, ce que implique que

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1).$$

2) Isomorphisme d'anneaux ok.
Les éléments inversibles de $\mathbb{Z}/nm\mathbb{Z}$ correspondent aux couples formés par un inversible de $\mathbb{Z}/n\mathbb{Z}$ est un inversible de $\mathbb{Z}/m\mathbb{Z}$, et par suite

$$\varphi(nm) = \varphi(n)\varphi(m).$$

3) On a, $n = \prod_{k=1}^{N} p_k^{\alpha_k}$, d'où

$$\varphi(n) = \prod_{k=1}^{N} p_k^{\alpha_k - 1}(p_k - 1) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_N}).$$

Exercice 6 : 1) On a $I + J \leq A$.
Pour tout $a \in A$ et $x = i + j \in I + J$, on a

$$ax = ai + aj \in I + J,$$

d'où $I + J$ est un idéal de A.
On a $I \cdot J \neq \emptyset$ car $0 \cdot 0 = 0 \in IJ$, soit $(x, y) \in (I \cdot J)^2$, alors

$$x - y = \sum_{k=1}^{n} i_k j_k - \sum_{\ell=1}^{m} i'_\ell j'_\ell = \sum_{k=1}^{n+m} i_k j_k$$

avec $i_k = -i'_{k-n}$ et $j_k = -j'_{k-n}$ pour $n + 1 \leq k \leq n + m$. Donc $I \cdot J \leq A$. De plus pour tout $a \in A$

$$ax = \sum_{k=1}^{n} (ai_k) j_k \in I \cdot J.$$

2) Soit $x = \sum_{k=1}^{n} i_k j_k \in I \cdot J$, alors pour tout k, on a $i_k j_k \in I$ car I idéal est comme $I \leq A$, alors $x \in J$, de même $x \in J$. Donc $I \cdot J \subset I \cap J$.
3) Soit $x \in (I + J) \cdot (I \cap J)$, alors

$$x = \sum_{k=1}^{n} a_k b_k \qquad \text{avec } a_k \in I + J \text{ et } b_k \in I \cap J$$

de plus $a_k = i_k + j_k$, et par suite $a_k b_k = i_k b_k + j_k b_k \in I \cdot J$. Donc $(I + J) \cdot (I \cap J) \subset I \cdot J$.
4) On a $I + J = A$ et $I \cdot J \subset I \cap J$. Soit $x \in I \cap J$, comme A unitaire, alors

$$x = 1 \cdot x = (i + j)x = ix + ij \in I \cdot J.$$

Donc $I \cdot J = I \cap J$.
Exercice 7 : 1) Comme I est un idéal de A, alors $0 \in I$, et par suite $0 \in \sqrt{I}$, ainsi $\sqrt{I} \neq \emptyset$.

Soit $(x,y) \in (\sqrt{I})^2$, d'où il exite $(n,m) \in \mathbb{N}^2$ tel que $x^n \in I$ et $y^m \in I$, montrons que $x-y \in \sqrt{I}$, en effet, on a

$$(x-y)^{n+m} = \sum_{k=0}^{n+m} C_{n+m}^k (-1)^{n+m-k} x^k (y)^{n+m-k},$$

si $k \leq n$, alors $y^{n+m-k} \in I$ et $(-1)^{n+m-k}x^k \in A$ comme I est un idéal de A, ainsi $(-1)^{n+m-k}x^k(y)^{n+m-k} \in I$, de même si $n \leq k$. Donc $I \leq A$. Soit $(a,x) \in A \times \sqrt{I}$, on a $x^n \in I$, et par suite $(ax)^n = a^n x^n \in I$. D'où $\sqrt{I}$ est un idéal de A.
2) D'après l'exercice 6, on $I \cdot J$ et $I \cap J$ sont deux idéaux de A, ainsi 1) implique que $\sqrt{I \cdot J}$ $\sqrt{I \cdot J}$ sont deux idéaux de A.
Soit $x \in \sqrt{I \cdot J}$, alors il existe n tel que $x^n \in I \cdot J$ avec

$$x^n = \sum a_k b_k \quad \text{avec } a_k \in I \text{ et } b_k \in J,$$

d'où $x^n \in I \cap J$, ce que implique que $x \in \sqrt{I \cap J}$.
Soit $x \in \sqrt{I \cap J}$, ainsi il existe n tel que $x^n \in I \cap J$, c'est-à-dire $x \in \sqrt{I} \cap \sqrt{J}$.
Soit $y \in \sqrt{I} \cap \sqrt{J}$, alors il existe n et m tel que $y^n \in I$ et $y^m \in J$, et par suite $y^{n+m} = y^n y^m \in I \cdot J$, d'où $y \in \sqrt{I \cdot J}$. En conclusion

$$\sqrt{I \cdot J} \subset \sqrt{I \cap J} \subset \sqrt{I} \cap \sqrt{J} \subset \sqrt{I \cdot J}.$$

On a $I \subset \sqrt{I}$, ainsi $\sqrt{I} \subset \sqrt{\sqrt{I}}$. Soit $x \in \sqrt{\sqrt{I}}$, alors il existe n tel que $x^n \in \sqrt{I}$, et par suite il existe m tel que $(x^n)^m = x^{nm} \in I$, d'où $x \in \sqrt{I}$. Donc $\sqrt{I} = \sqrt{\sqrt{I}}$.
3) On a $x \in \sqrt{k\mathbb{Z}}$ si et seulement si il existe n tel que $x^n \in k\mathbb{Z}$, c'est-à-dire, k divise x^n, mais comme $k = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, alors p_i divise x^n, ce que implique que p_i divise x pour tout $1 \leq i \leq r$. D'où $x \in (p_1 \cdots p_r)\mathbb{Z}$. Réciproquement si $x \in (p_1 \cdots p_r)\mathbb{Z}$, alors $x = p_1 \cdots p_r m$. Notant $n = \max_{1 \leq i \leq r} \alpha_i$, alors k divise x^n, d'où

$$\sqrt{k\mathbb{Z}} = (p_1 \cdots p_r)\mathbb{Z}.$$

Exercice 8 : 1) Soit $I = n\mathbb{Z}$ un idéal premier de $\mathbb{Z}$. Si n n'est pas premier, alors $n = ab$ avec $1 < a, b < n$, ainsi $a \in I$ ou $b \in I$, et par suite a ou b est un multiplie de n absurde. n premier.
Si n premier, soit $xy \in I$, c'est-à-dire, n divise xy, ainsi n divise x ou y ce que implique que $x \in I$ ou $y \in I$. Donc $n\mathbb{Z}$ premier si et seulement si n premier.
2) On pose

$$K = \{a \in A \,|\, \exists\, i \in I \; k \in \mathbb{Z};\; a = i + kx\},$$

on a K un idéal de A avec $I \subset K$ et $x \in K$, alors $J \subset K$.
Soit J' un idéal de A tel que $I \subset J'$ et $x \in J'$, ainsi $K \subset J'$. Donc K le plus petit idéal de A contenant I et x, d'où

$$K = J.$$

3) Soient M un idéal maximal de A et $xy \in M$ tel que $x \notin M$. Montrons que $y \in M$?
Soit J l'idéal engendré par M et x, comme M maximal et $M \subsetneq J$, alors $A = J$. Or d'après 2) tout élément de J s'écrit $i + kx$, et par suite

$$J \ni 1 = i + kx \implies y = yi + kxy \in M.$$

4) On a $\{0\}$ est un idéal premier, si $xy = 0$, alors $x = 0$ ou $y = 0$, et par suite A est intègre. Soient $x \in A^*$ et I l'idéal engendre par x^2, ainsi $x \in I$, d'où il existe $b \in A$ tel que $x = bx^2$, et par suite

$$x(1 - bx) = 0$$

comme A intègre et $x \neq 0$, alors $bx = 1$, donc A est un corps.
5) Soit I un idéal premier, mais comme A principal, alors il existe $a \in A$ tel que

$$I = (a).$$

Soit J un idéal de A tel que $I \subset J$, or A principal d'où $J = (b)$, ainsi $a = bc$ avec $c \in A$. Comme I premier, alors

$$b \in I \implies (b) \subset I \implies I = J$$

ou bien

$$c \in I \implies c = xa = bxc$$

or A principal, d'où intègre, ainsi $bx = 1$ ce que implique que $b \in U(A)$, et par suite $J = A$. Donc I maximal.
6)

$$A/I \quad \text{intègre} \iff \overline{xy} = \overline{0} \iff \overline{x} = \overline{0} \text{ ou } \overline{x} = \overline{0} \iff x \in I \text{ ou } y \in I \iff I \quad \text{premier.}$$

7) A/I est un corps si et seulement si ses seuls idéaux sont $\{\overline{0}\}$ et A/I, or les idéaux de A/I sont en bijection avec les idéaux de A contenant I, c'est-à-dire, A/I est un corps si et seulement si les seuls idéaux de A contenant I sont I et A, c'est-à-dire I maximal.
Si I maximal, alors A/I corps et par suite anneau intègre. Donc I premier.
Exercice 9 : 1) On a $\ker(f) \subset f^{-1}(Q)$, soit $ab \in f^{-1}(Q)$ tel que $a \notin f^{-1}(Q)$. Montrons que $b \in f^{-1}(Q)$. Comme $ab \in f^{-1}(Q)$, alors $f(ab) = f(a)f(b) \in Q$ avec $f(a) \notin Q$, ainsi $f(b) \in Q$ car Q premier, et par suite, $b \in f^{-1}(Q)$.
2) Comme f surjectif, alors $f(P)$ est un idéal de B. Soit $xy \in f(P)$ tel que $x \notin f(P)$, montrons que $y \in f(P)$?
On a $xy = f(a)f(b) = f(ab) \in f(P)$, ainsi $ab \in P$, or $a \notin P$, d'où $b \in P$, et par suite, $y \in f(P)$.
3) On a

$$\begin{aligned} \pi : A &\longrightarrow A/I \\ a &\longmapsto a + I \end{aligned} \qquad \text{morphisme d'anneaux surjective avec } \ker(\pi) = I.$$

Si P est un idéal premier de A tel que $I \subset A$, alors $\pi(P) = P/I$ est un idéal premier de A/I.
Exercice 10 : 1) Puisque $\mathbb{Q}[X]$ est un anneau principal, alors

$$(P)+(Q)=(p\wedge Q)\qquad\text{et}\qquad(P)\cap(Q)=(P\vee Q),$$

et par suite

$$(2X)+(X+1)=(1)=\mathbb{Q}[X],\quad(2X)\cap(X+1)=2X(X+1)\mathbb{Q}[X]$$

et d'après l'exercice 6, on a $(2X)(X+1)=(2X)\cap(X+1)=2X(X+1)\mathbb{Q}[X]$.
2) Dans $\mathbb{Z}/2\mathbb{Z}$, on a

$$P=XQ+X^2+X+\overline{1}\qquad\text{et}\qquad Q=(X^2+X+\overline{1})(X+\overline{1})+X$$

de plus

$$X^2+X+\overline{1}=X(X+\overline{1})+\overline{1},$$

d'où

$$P\wedge Q=\overline{1}$$

avec

$$\overline{1}=X^2+X+\overline{1}-X(X+\overline{1})=P-XQ-[Q-(P-XQ)][X+\overline{1}]=XP+\cdots.$$

Dans $\mathbb{Z}/3\mathbb{Z}$, on a

$$P=XQ+\overline{2}X^2+\overline{2}X+\overline{1}\qquad\text{et}\qquad Q=(\overline{2}X^2+\overline{2}X+\overline{1})(\overline{2}X+\overline{1}),$$

et par suite

$$P\wedge Q=\overline{2}X^2+\overline{2}X+\overline{1}.$$

Exercice 11 : Soient a un diviseur de zéro et

$$\begin{aligned}\varphi :A &\longrightarrow A\\ x &\longmapsto ax\end{aligned}\qquad\text{morphisme de groupes}$$

avec

$$\ker(\varphi)=\{x\in A\,|\,ax=0\}=I\quad\text{ qui est un idéal de } A.$$

Pour $y\in Im(\varphi)$, on a $y=ax$ or a est un diviseur de zéro, alors il existe $c\in A^*$ tel que $ac=0$, et par suite $yc=axc=acx=0$. Donc $Im(\varphi)$ ne contient que 0 et des diviseurs de zéro. Or A possède n diviseurs de zéro, ains $card(Im(\varphi))\leq n+1$. Mais d'après le première théorème d'isomorphisme $A/I\simeq Im(\varphi)$. Donc

$$card(A/I)\leq n+1\quad\text{et}\quad card(I)\leq n+1,$$

et par suite $card(A)\leq(n+1)^2$.
Exercice 12 : 1) Soit $x=a+ib\in U(\mathbb{Z}[i])$, alors il existe $y=c+id\in\mathbb{Z}[i]$ tel que $xy=1$, et par suite $|xy|^2=|x|^2|y|^2=1$, c'est-à-dire, $(a^2+b^2)(c^2+d^2)=1$ avec $(a,b,c,d)\in\mathbb{Z}^4$, d'où $a^2+b^2=1$, ce que implique que $a=\pm1$ ou $b=\pm1$. Donc

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

D'autre part

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

Donc

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

Par définition, on a

$$Fr(\mathbb{Z}[i]) = \{x/y \,|\, x \in \mathbb{Z}[i],\ y \in (\mathbb{Z}[i])^*\}.$$

Soit $x/y \in Fr(\mathbb{Z}[i])$, tel que $x = a + ib$ et $y = c + id$ avec $(c, d) \neq (0, 0)$. Alors

$$x/y = \frac{ac + bd}{c^2 + d^2} + i\frac{bc - ad}{c^2 + d^2} \in \mathbb{Q}[i],$$

d'où $Fr(\mathbb{Z}[i]) \subset \mathbb{Q}[i]$. Soit $\alpha + i\beta \in \mathbb{Q}[i]$, alors $\alpha = a/b$ et $\beta = c/d$, ce que implique que $\alpha + i\beta = \frac{ad+ibc}{bd} \in Fr(\mathbb{Z}[i])$. Donc

$$Fr(\mathbb{Z}[i]) = \mathbb{Q}[i].$$

2) a) On a

$$f(x + y) = f[(a + c) + i(b + d)] = \overline{a + c + 7(b + d)} = f(x) + f(y),$$

$$f(xy) = f[(ac - bd) + i(ad + bc)] = \overline{ac - bd + 7(ad + bc)} = \overline{(a + 7b)(c + 7d)} = f(x)f(y)$$

et

$$f(\overline{1}) = \overline{1},$$

ainsi f est un morphisme d'anneaux unitaire. De plus pour tout $\overline{y} \in \mathbb{Z}/10\mathbb{Z}$, on a $\overline{y} = f(y)$, d'où f surjectif.
b) On a

$$\ker(f) = \{x \in \mathbb{Z}[i] \,|\, f(x) = 0\},$$

soit $x = a + ib \in \ker(f)$, alors $\overline{a + 7b} = \overline{0}$, ainsi il existe $k \in \mathbb{Z}$ tel que $a + 7b = 10k$ et par suite

$$\begin{aligned} x = 10k - 7b + ib = (3 + i)(3 - i)k + (i - 7)b &= (3 + i)(3 - i)k + (3 + i)(i - 2)b \\ &= (3 + i)[(3 - i)k + (i - 2)b] \end{aligned}$$

ce que implique que

$$\ker(f) \subset (3 + i).$$

De plus $f(3 + i) = 0$ alors $(3 + i) \subset \ker(f)$. Donc $\ker(f) = (3 + i)$ et plus le théorème d'isomorphisme, on obtient

$$\mathbb{Z}[i]/(3 + i) \simeq \mathbb{Z}/10\mathbb{Z}.$$

c) Comme $\mathbb{Z}/10\mathbb{Z}$ n'est pas intègre ($\overline{2} \cdot \overline{5} = 0$), alors $\mathbb{Z}[i]/(3+i)$ n'est pas intègre, et par suite $(3 + i)$ n'est pas idéal premier, d'où $3 + i$ n'est pas premier.
Exercice 13 : 1) Évident.
2) Évident.

3) Évident.
4) Supposons que $2 = ab$, alors $N(ab) = N(a)N(b) = N(2) = 4$, ainsi $N(a) = N(b) = 2$ (non) ou $N(a) = 4$ et $N(b) = 1$ ou $N(a) = 1$ et $N(b) = 4$. D'où $N(a) = 1$ ou $N(b) = 1$. Donc $a \in U(\mathbb{Z}[\sqrt{-5}])$ ou $b \in U(\mathbb{Z}[\sqrt{-5}])$, ainsi 2 irréductible.
2 n'est pas premier car 2 divise $(1-i\sqrt{5})(1+i\sqrt{5})$ avec 2 ne divise pas $(1-i\sqrt{5})$ et $(1+i\sqrt{5})$ car $N(1-i\sqrt{5}) = N(1+i\sqrt{5}) = 6$.

Exercice 14 : 1) Comme a/ab et b/ab, alors m/ab, et par suite il existe $d \in A$ tel que $ab = md$. Montrons que $d = a \wedge b$?
Comme a/m et b/m, alors $m = \alpha a = \beta b$, ce que implique que $ab = md = \alpha ad = \beta bd$ et le fait que A intègre, on obtient $b = \alpha d$ et $a = \beta d$, d'où d/a et d/a. Soit $c \in A$ tel que c/a et c/b, c'est-à-dire, $a = cu$ et $b = cv$. Comme a/cuv et b/cuv, alors m/cuv, ainsi $cuv = mt = \alpha at$. Donc $v = \alpha t$, or $acv = ab = md = \alpha ad$, et par suite $cv = \alpha d = c\alpha t$, d'où $ct = d$. Donc c/d.
2) a)

$$U(\mathbb{Z}[i\sqrt{5}]) = \{-1, 1\}.$$

b) Soit $x = a + ib\sqrt{5}$ tel que $x/9$, alors il existe y tel que

$$(a^2 + 5b^2)(c^2 + 5d^2) = 81,$$

et par suite

$$a^2 + 5b^2 \in \{1, 9, 81\} \qquad \text{car } a^2 + 5b^2 \neq 3 \text{ et de } 27.$$

Donc les diviseurs de 9 sont : ± 1, ± 3, ± 9, $\pm(2 + i\sqrt{5})$ et $\pm(2 - i\sqrt{5})$.
De même on montre que les diviseurs de $3(2+i\sqrt{5})$ sont ± 1, ± 3, $\pm(2+i\sqrt{5})$ et $\pm 3(2+i\sqrt{5})$.
c) Soit $x \in \mathbb{Z}[i\sqrt{5}]$ tel que $x/3$ et $x/(2 + i\sqrt{5})$, or les diviseurs de 3 : ± 1 et ± 3 puisque ± 3 ne divise pas $x/2 + i\sqrt{5}$, alors $x = \pm 1$. Donc $1 = 3 \wedge 2 + i\sqrt{5}$.
Supposons que $m = ppcm(3, 2 + i\sqrt{5})$, alors m divise $3(2 + i\sqrt{5})$ (car $1 = 3 \wedge 2 + i\sqrt{5}$) et m divise 9, puisque $3/9$ et $2 + i\sqrt{5}/9$ (d'après b)) avec $1 = 3 \wedge 2 + i\sqrt{5}$, ainsi $m/3(2 + i\sqrt{5})$. D'après b)

$$m \in \{\pm 1, \pm 3, \pm(2 + i\sqrt{5})\},$$

mais 3 ne divise pas ± 1 et $\pm(2+i\sqrt{5})$ aussi $\pm(2+i\sqrt{5})$ ne divise pas ± 3. Donc 3 et $2+i\sqrt{5}$ n'ont pas de ppcm dans $\mathbb{Z}[i\sqrt{5}]$. D'où $\mathbb{Z}[i\sqrt{5}]$ n'est pas principal.
d) Supposons que $d = 9 \wedge 3(2 + i\sqrt{5})$, ainsi d'après b)

$$d \in \{\pm 1, \pm 3, \pm(2 + i\sqrt{5})\},$$

on $d \neq \pm 1$ car $3/d$, $d \neq \pm 3$ puisque $(2 + i\sqrt{5})/d$ et $d \neq \pm(2 + i\sqrt{5})$ car $3/d$. Donc 9 et $3(2+i\sqrt{5})$ n'ont pas de pgcd et par suite 1) implique que 9 et $3(2+i\sqrt{5})$ n'ont pas un ppcm.
e) Supposons que $(3, 2+i\sqrt{5}) = (x)$, alors $x/3$ et $x/(2+i\sqrt{5})$ ainsi d'après c) $x = \pm 1$. Donc $(3, 2 + i\sqrt{5}) = \mathbb{Z}[i\sqrt{5}]$, en particulier, on aura

$$1 = 3(a + ib\sqrt{5}) + (2 + i\sqrt{5})(c + id\sqrt{5}),$$

d'où

$$3a = 2c - 5d = 1 \quad \text{et} \quad 3b + 2d + c = 0$$

ainsi

$$1 = 3(a+b+c-d) \quad \text{absurde car } (a,b,c,d) \in \mathbb{Z}^4.$$

Exercice 15 : Soient $a \in A^*$ et $I_n = (a^n)$, alors $I_{n+1} \subset I_n$, ainsi il existe p tel que $I_{p+1} = I_p$. En particulier

$$a^p = a^{p+1}u \implies a^p(1-au) = 0$$

comme A intègre et $a^p \neq 0$, alors a inversible. Donc A corps.

Exercice 16 : 1) On a $j^3 = 1$, $1 + j + j^2 = 0$ et pour tout $P \in \mathbb{Z}[X]$, on a

$$P = Q(X^2+X+1) + R \qquad \text{avec } R = aX + b.$$

2) Soit $N(a+bj) = a^2 - ab + b^2 = (a+bj)(a+bj^2) \in N$. Soit $(x,\alpha) \in \mathbb{Z}[j] \times \mathbb{Z}[j]^*$, alors

$$\alpha x = (a+bj)(c+dj) = ac-bd+j(bc+ad-bd) \implies N(\alpha x) = N(x)N(\alpha) \geq N(x) \quad \text{car } N(\alpha) \geq 1.$$

Soit $(z,z') \in (\mathbb{Z}[j]^*)^2$, alors $\xi = z/z' = x + yj \in \mathbb{Q}[j]$, et par suite il existe $(a,b) \in \mathbb{Z}^2$ tel que $|x-a| \leq 1/2$ et $|y-b| \leq 1/2$, ainsi

$$N(x-a+(y-b)j) = (x-a)^2 + (y-b)^2 - (x-a)(y-b) \leq 3/4 < 1$$

et

$$z = z'(a+bj) + z'(x-a+(y-b)j).$$

Donc $\mathbb{Z}[j]$ est un anneau euclidien.

3) Soit $a + bj = x \in U(\mathbb{Z}[j])$, alors $N(x) = 1$ si et seulement si $a^2 + b^2 - ab = 1$. Donc $(2a-b)^2 + 3b^2 = 4$, d'où $U(\mathbb{Z}[j]) \subset \{\pm 1 + bj \,|\, b \in \{0,1,-1\}\}$, de plus l'autre inclusion est évident. Donc

$$U(\mathbb{Z}[j]) = \{\pm 1 + bj \,|\, b \in \{0,1,-1\}\}.$$

4) On a $\frac{z'\overline{z}}{N(z)} = \frac{z'}{z} = u \in A \subset 1/2\mathbb{Z}[i\sqrt{3}]$.

5) On a $u = \frac{z'\overline{z}}{N(z)} = \frac{a}{2}$ avec $a \in \mathbb{Z}[i\sqrt{3}]$, d'où 2 divise $aN(z)$ or $2 \wedge N(z) = 1$. Donc 2 divise a, et par suite $u \in \mathbb{Z}[i\sqrt{3}]$.

Exercice 17 : 1) $\mathbb{K}$ corps contient A et que s'injecte dans tous corps qui contient A. Donc $\mathbb{K} = Fr(A)$.

2) Évident.

3) Évident.

4) On a

$$\delta(x - [x]) = \delta(a - \lfloor a \rceil + \sqrt{2}(b - \lfloor b \rceil)) \leq 1/4 + 2 \cdot 1/4 \leq 3/4.$$

5) Soit $(z,z') \in ((\mathbb{Z}[\sqrt{2}])^*)^2$, alors $z/z' \in \mathbb{K}$ avec

$$z/z' = [z/z'] + (z/z' - [z/z']),$$

et par suite $z = qz' + r$ avec $q = [z/z'] \in \mathbb{Z}[\sqrt{2}]$ et $r = z'(z/z' - [z/z'])$, de plus $N(r) < N(z')$. Donc A est un anneau euclidien pour δ.