DÉPARTEMENT DE MATHÉMATIQUES
FACULTÉ DES SCIENCES
UNIVERSITÉ MOULAY ISMAÏL-MEKNÈS

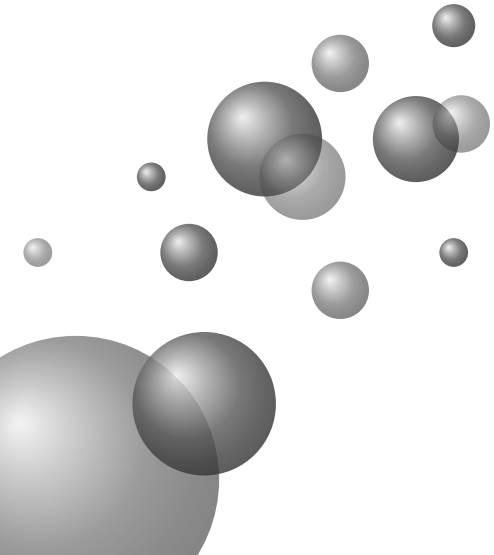
COURS D'ALGÈBRE 7

FILIÈRE : SMA

(SEMESTRE IV)

(Ce document ne peut en aucun cas remplacer les séances de cours en présentiel)

MOHAMMED TAMEKKANTE



Année universitaire :2017-2018.

Table des matières

Chapitre 1

Groupe opérant sur un ensemble

1.1 Notion de groupe opérant sur un ensemble

Dans ce qui suit, les groupes seront notés multiplicativement, sauf mention explicite du contraire. L'élément neutre d'un groupe sera noté 1.

Définition 1.0.1. Soient G un groupe et E un ensemble non vide. On dit que G opère à gauche sur E, s'il existe une application de $G \times E$ dans E ; $(g, x) \mapsto g.x$ satisfaisant aux deux conditions suivantes :

1. $(\forall g, h \in G)(\forall x \in E),\ g.(h.x) = (gh).x$.
2. $(\forall x \in E),\ 1.x = x$.

Remarque 1.0.1. On définit de façon analogue la notion de groupe opérant à droite sur un ensemble (non vide). Dans la suite (sauf indication contraire), nous conviendrons de dire qu'un groupe G opère sur un ensemble E, si G opère à gauche sur E. Dans ce cas, E sera appelé un G-ensemble (un G-ensemble sera toujours non vide).

Proposition 1.1

Soit G un groupe opérant sur un ensemble E.

1. Pour tout $g \in G$, l'application $\gamma_g : E \to E$; $x \mapsto g.x$ est une permutation de E.
2. S_E désignant le groupe des permutations de E, l'application $\gamma : G \to S_E$; $g \to \gamma_g$ est un morphisme de groupes et $\ker\gamma$ est appelé : noyau de l'action de G sur E.

Démonstration. 1. Montrons que $\gamma_g \in S_E$, c'est-à-dire que γ_g est une bijection.

γ_g est surjective, car, pour tout $x \in E$, $x = g.(g^{-1}.x)$.

γ_g est injective. En effet, soient x et y dans E tels que $\gamma_g(x) = \gamma_g(y)$, c'est-à-dire $g.x = g.y$, alors $x = g^{-1}.(g.x) = g^{-1}.(g.y) = y$.

2. Soient g_1 et g_2 dans G. Pour tout $x \in E$, on a

$$\gamma_{g_1} \circ \gamma_{g_2}(x) = \gamma_{g_1}(g_2.x) = g_1.(g_2.x) = (g_1g_2).x = \gamma_{g_1g_2}(x).$$

Donc, $\gamma_{g_1} \circ \gamma_{g_2} = \gamma_{g_1g_2}$. C'est-à-dire que $\gamma(g_1g_2) = \gamma(g_1) \circ \gamma(g_2)$. Ce qui prouve que γ est un morphisme de groupes.

□

Remarque 1.1.1. D'après ce qui précède, à toute action de G sur un ensemble E, correspond un morphisme de groupes, γ, de G dans S_E.
Réciproquement, à tout $\lambda \in Hom(G, S_E)$, on peut associer l'action de G sur E définie par $g.x = \lambda(g)(x)$. On a en effet, quels que soient g_1 et g_2 dans G et x dans E :

— $g_1.(g_2.x) = \lambda(g_1)(\lambda(g_2)(x)) = \lambda(g_1) \circ \lambda(g_2)(x) = \lambda(g_1g_2)(x) = (g_1g_2).x$, et
— $1.x = \lambda(1)(x) = \mathrm{Id}_E(x) = x$.

***Exemples* 1.1.1.**

1. Soient G un groupe, E un ensemble. En posant $g.x = x$ pour tout $g \in G$ et tout $x \in E$, on obtient une action, dite triviale, de G sur E. Le morphisme associé est le morphisme trivial de G dans $S(E)$ ($g \mapsto \mathrm{Id}_E$).
2. Soit E un ensemble. Pour tous $s \in S(E)$ et $x \in E$, posons $s.x := s(x)$. Nous obtenons une action, dite naturelle, du groupe $(S(E), \circ)$ sur E. Le morphisme associé est l'application identité de $S(E)$.
3. Sot $(g, x) \mapsto g.x$ une action de G sur E. Soit H un sous groupe de G. La restriction de cette action sur H est une action de H sur E dont le morphisme associé est la rastriction de γ sur H.
4. Voici un exemple théorique important. Soit G un groupe. La multiplication $G \times G \mapsto G$ est une action du groupe G sur l'ensemble G. En effet, posons ici $g.x := gx$ pour tous $g, x \in G$. Dans la définition, la propriété (1) est vérifiée (c'est l'associativité de la loi de G), la propriété (2) aussi (elle traduit le fait que 1 est élément neutre de G). Dans cet exemple, G joue un rôle double : celui du groupe qui agit et celui de l'ensemble sur lequel ce groupe agit. Cette action est appelée action par translation à gauche du groupe G sur lui-même. Cette terminologie est justifiée : pour tout $g \in G$ fixé, la permutation $\gamma(g)$ de G associée à g est la translation à gauche $x \mapsto gx$ de G.
5. Soit G un groupe multiplicatif. Pour tous $g, x \in G$, posons $g.x := gxg^{-1}$. Nous obtenons encore une action du groupe G sur l'ensemble G. En effet, si $g, h, x \in G$, il vient :

$$g.(h.x) = g.(hxh^{-1}) = ghxh^{-1}g^{-1} = (gh)x(gh)^{-1}$$

d'où la propriété 1 de la définition. La propriété 2 est clairement vérifiée.
L'action obtenue est appelée conjugaison, on dit que G agit sur lui-même par conjugaison. Notons γ le morphisme associé à cette action. Soit $g \in G$. Par définition, on a donc : $\gamma(g)(x) = g.x = gxg^{-1}$. Nous savons que $\gamma(g)$ n'est pas seulement une permutation de l'ensemble G, c'est un automorphisme du groupe G. Ainsi γ est à valeurs dans le groupe $\mathrm{Aut}(G)$ des automorphismes de G, Le γ est un morphisme de G dans $\mathrm{Aut}(G)$.
Le noyau de γ est le centre $\mathrm{Z}(G)$ de G, formé des $g \in G$ commutant avec tout élément x de G. En particulier, l'action par conjugaison de G sur lui-même est triviale si, et seulement si, G est commutatif.

Soient G un groupe et H un sous-groupe de G. Alors la relation ${}_H\mathcal{R}$ (resp. $\mathcal{R}_H$) définie par $a\,{}_H\mathcal{R}\,b \Leftrightarrow a^{-1}b \in H$ (resp. $a\mathcal{R}_H b \Leftrightarrow ab^{-1} \in H$) est une relation d'équivalence sur G compatible à gauche (resp. à droite) avec la loi interne ; la classe d'équivalence de $a \in G$ est sa classe à gauche aH (resp. sa classe à droite Ha). Les relations d'équivalence ${}_H\mathcal{R}$ et $\mathcal{R}_H$ coïncident si et seulement si H est distingué dans G ($H \trianglelefteq G$). Les ensembles quotients $G/{}_H\mathcal{R}$ et $R/\mathcal{R}_H$ seront respectivement notés $(G/H)_g$ et $(G/H)_d$. Dans le cas où H est distingué dans G, l'ensemble G/H menu de la loi $\overline{g_1}.\overline{g_2} = \overline{g_1 g_2}$ est un groupe.

***Exemple* 1.1.1.** Soit H un sous-groupe de G ; alors G opère par translation à gauche, sur l'ensemble $(G/H)_g$. Pour voir cela, il suffit de vérifier que la correspondance $G \times (G/H)_g \to (G/H)_g$; $(g, xH) \to gxH$ est une application. Supposons $xH = yH$. Donc, $x^{-1}y \in H$. Ainsi, $(gx)^{-1}(gy) \in H$. D'où, $gxH = gyH$. Ainsi G opère sur $(G/H)_g$ par translation à gauche.

Théoreme 1.2 (Premier théorème d'isomorphisme)

Pour tout morphisme f d'un groupe G dans un groupe G', on a : $G/\ker f \cong \mathrm{Im}(f)$.

Démonstration. Notons tout d'abord que $\ker(f)$ est distingué dans G. Pour obtenir le résultat désiré, il suffit de vérifier que l'application $G/\ker(f) \to \mathrm{Im}(f)$; $\overline{x} \mapsto f(x)$ est un isomprhisme de groupes. □

Proposition 1.3

Soit $\mathrm{Int}(G)$ le groupe des automorphismes intérieurs d'un groupe G. Alors $\mathrm{Int}(G) \cong G/\mathrm{Z}(G)$.

Démonstration. On considère le morphisme γ associé à l'action par conjugaison de G. On a $\mathrm{Im}(\gamma) = \mathrm{Int}(G)$ et $\ker(\gamma) = \mathrm{Z}(G)$. Donc, d'après le premier théorème d'isomorphisme on a le résultat désiré. □

Théoreme 1.4 (de Cayley)

Tout groupe est isomorphe à un sous-groupe de permutations.

Démonstration. Le morphisme $\gamma : G \mapsto S(G)$ associé à l'action de G sur lui-même par translations à gauche est injectif. Par ailleurs, G est isomorphe à $\gamma(G)$ qu'est une sous groupe de $S(G)$. □

Remarque 1.4.1. Soit $G = \{x_1, \ldots, x_n\}$ une ensemble fini. Soit $f : G \to \{1, \ldots, n\}$ la bijection définie par $f(x_i) = i$. Alors,l'application $\psi : S(G) \to S_n$ définie par $\psi(s) = f \circ s \circ f^{-1}$ est un isomorphisme de groupe entre $(S(G), \circ)$ et $(S_n, \circ)$. Donc du théorème précédent, on déduit que tout groupe fini d'ordre n est isomorphe à un sous-groupe du groupe symétrique S_n.

1.2 Sous-groupe d'isotropie ou stabilisateur et Orbite

Définition 1.4.1. Soient G un groupe et E un G-ensemble.

1. Pour tout $x \in E$, On appelle stabilisateur de x le sous groupe de G

$$G_x := \{g \in G \mid g.x = x\}.$$

2. On considère dans E la relation binaire

$$x \mathcal{R} y \Leftrightarrow \exists g \in G; \quad x = g.y.$$

$\mathcal{R}$ est clairement une relation d'équivalence. Pour tout $x \in E$, la classe de x modulo $\mathcal{R}$ est appelée G-orbite de x et est notée Ω_x. C'est à dire,

$$\Omega_x = \{g.x \mid g \in G\} = G.x.$$

***Exemples* 1.4.1.**

1. On considère l'action par traslation à gauche sur le groupe G. Pour tout $x \in G$, on a

$$G_x = \{e\} \qquad \text{et} \qquad \Omega_x = G.$$

2. On considère l'action par conjugaison sur le groupe G. Pour tout $x \in G$, on a

$$G_x = \{g \in G \mid gx = xg\} = C_G(x) \quad \text{(le centralisateur de } x \text{ dans } G)$$

et

$$\Omega_x = \{gxg^{-1} \mid g \in G\} \quad \text{(la classe de } x \text{ par conjugaison).}$$

3. On considère l'action de G sur $P(G)$ par conjugaison. Pour tout $S \in P(G)$ avec $S \neq \emptyset$, on a

$$G_S = \{g \in G \mid gS = Sg\} = N_G(S) \quad \text{(le normalisation de } S \text{ dans } G)$$

et

$$\Omega_S = \{gSg^{-1} \mid g \in G\}.$$

Aussi, $G_\emptyset = G$ et $\Omega_\emptyset = \emptyset$.

4. On considère l'action de G sur $(G/H)_g$ par translation à gauche. Pour tout $x \in G$, on a

$$G_{xH} = \{g \in G \mid gxH = xH\} = \{g \in G \mid g \in xHx^{-1}\} = xHx^{-1}.$$

5. Soit $\sigma \in S_n$. Rappelons que le σ-orbite de $1 \leq i \leq n$ est $\Omega_\sigma(i) = \{\sigma^r(i) \mid r \in \mathbb{Z}\}$. On pose $H = (\sigma)$ et on considère l'action naturelle de H sur $\{1, \ldots, n\}$ ($\sigma^r.i = \sigma^r(i)$). Alors, pour tout $1 \leq i \leq n$,

$$\Omega_i = \{\sigma^r(i) \mid r \in \mathbb{Z}\} = \Omega_\sigma(i)$$

ce qui justifie les appellations des deux notions.

Proposition 1.5

Le noyau, $\ker(\gamma)$, de l'action de G sur $\left(\frac{G}{H}\right)_g$ est le plus grand sous groupe de G distingué contenu dans H.

Démonstration. On a

$$\begin{aligned}
\ker(\gamma) &= \{g \in G \mid gxH = xH \text{ pour tout } x \in G\} \\
&= \{g \in G \mid g \in xHx^{-1} \text{ pour tout } x \in G\} \\
&= \bigcap_{x \in G} xHx^{-1} \\
&= \bigcap_{x \in G} G_{xH}
\end{aligned}$$

$\ker(\gamma)$ est distingué dans G car c'est le noyau d'un morphisme de groupe de G vers un autre groupe. En plus $\ker(\gamma) \subseteq G_H = H$. Soit maintenant un $N \trianglelefteq G$ tel que $N \subseteq H$. Alors, pour tout $x \in G$, on a $N = xNx^{-1} \subseteq xHx^{-1}$. Donc, $N \subseteq \ker(\gamma)$. □

Pour tout sous-groupe H d'un groupe G, la correspondance

$$\begin{array}{rccc} \theta : & (G/H)_g & \longrightarrow & (G/H)_d \\ & xH & \longmapsto & Hx^{-1} \end{array}$$

est une application bijective. Cela se traduit par la relation

$$\text{Card}\left((G/H)_g\right) = \text{Card}\left((G/H)_d\right).$$

Ce cardinal commun est noté $[G : H]$ est appelé l'indice de H dans G. En particulier, si G est fini, alors $[G; H] = \dfrac{|G|}{|H|}$.

Remarques 1.5.1.

1. Si $H \trianglelefteq G$, alors $\ker(\gamma) = H$.
2. Un groupe qui n'a pas de sous-groupe distingués autre que les sous-groupes triviaux est dit simple. Si G est simple alors pour tout $H < G$, G est isomorphe à un sous groupe de $S_{\left(\frac{G}{H}\right)_g}$. En effet, $\ker(\gamma) = \{1\}$, et donc γ injective. Si de plus $[G : H]$ est fini alors G est isomorphe à un sous groupe de $S_{[G:H]}$.

Exercice 1. Soit G un groupe agissant sur deux ensembles X et Y. On dit que ces deux actions sont isomorphes s'il existe une bijection f de X sur Y telle que $f(g.x) = g.f(x)$ pour tous $g \in G$, $x \in X$ et $y \in Y$.
Soient H et H' deux sous-groupes de G. Montrer que les actions de G sur les quotients $(G/H)_g$ et $(G/H')_g$ sont isomorphes si et seulement si H et H' sont conjugués.

Solution.
On suppose qu'il existe $g \in G$ tel que $H' = gHg^{-1}$. On considère l'application f de $(G/H)_g$ vers $(G/H')_g$ définie par $f(xH) = xg^{-1}H' = xHg^{-1}$. L'application f est

— clairement bien définie,
— injective, en effet $xHg^{-1} = yHg^{-1}$ implique que $xH = yH$.
— surjective, en effet pour tout $x \in G$, $xH' = xgHg^{-1} = f(xgH)$.

Donc, f est bijective. En plus, $f(x.yH) = f(xyH) = xyHg^{-1} = x.f(yH)$. Par conséquent, les actions de G sur les quotients $(G/H)_g$ et $(G/H')_g$ sont isomorphes.
Inversement, on suppose que les actions de G sur les quotients $(G/H)_g$ et $(G/H')_g$ sont isomorphes via le bijection f. On pose $f(H) = gH'$. Donc, pour tout $h \in H$, on a $gH' = f(H) = f(hH) = hgH'$. Ainsi, $g^{-1}Hg \subseteq H'$. Aussi, pour tout $h' \in H'$, on a $f(h'g^{-1}H) = h'g^{-1}gH' = H' = f(g^{-1}H)$. Par injectivité de f, on obtient $h'g^{-1}H = g^{-1}H$. Alors, $H' \subseteq g^{-1}Hg$. D'où, $H' = g^{-1}Hg$.

Exercice 2.

1. Montrer qu'un sous-groupe d'indice 2 dans un groupe est toujours distingué dans ce groupe.
2. Soient H et K deux sous-groupes d'un groupe G.

(a) Formule des indices : On suppose que H est d'indice fini dans G, et que $H \subseteq K$. Montrer que $[G : H] = [G : K][K : H]$.

(b) Théorème de Poincaré : On suppose que H et K sont tous deux d'indices finis. Montrer que $[G : H \cap K] \leq [G : H][G : K]$. Donner un exemple où la relation est une inégalité stricte, puis où la relation est une égalité.

(c) Monter que si $[G : H]$ et $[G : K]$ sont finis et premiers entrer eux alors $[G : H \cap K] = [G : H][G : K]$.

Solution.

1. Soient G un groupe et $H \leq G$ tel que $[G : H] = 2$. Soit $x \in G$. Si $x \in H$ alors $xH = Hx = H$. Sinon, $H \neq xH$ et $H \neq Hx$. Donc, $(G/H)_g = \{H, xH\}$ et $(G/H)_g = \{H, Hx\}$. Par suite, $G = H \cup xH = H \cup Hx$ avec $H \cap xH = \emptyset$ et $H \cap Hx = \emptyset$. Ainsi, $xH = Hx$. Donc, H est distingué dans G.

2. Soient H et K deux sous-groupes d'un groupe G.

   (a) Soit $\{g_i\}_{i\in I}$ une famille de représentants des classes de G modulo K et que $\{k_j\}_{j\in J}$ une famille de représentants des classes de K modulo H. Alors,

   $$G = \bigcup_{i\in I} g_i K = \bigcup_{i\in I} g_i \left(\bigcup_{j\in J} k_j H \right) = \bigcup_{(i,j)\in I\times J} g_i k_j H.$$

   Par ailleurs, si $g_i k_j H = g_{i'} k_{j'} H$ alors $g_{i'}^{-1} g_i \in K$. Donc, $g_i K = g_{i'} K$. Ainsi, $g_i = g_{i'}$. On a alors $k_j H = k_{j'} H$. D'où, $k_j = k_{j'}$. On en déduit que la famille $\{g_i k_j\}_{(i,j)\in I\times J}$ est une famille de représentants des classes de G modulo H. Et donc, si l'indice $[G : H]$ est fini, le cardinal de $I \times J$ est fini, I et J sont finis et $[G : H] = [G : K][K : H]$.

   (b) Soit $f : (G/H \cap K)_g \to (G/H)_g \times (G/K)_g$ définie par $f(g(H \cap K)) = (gH, gK)$. L'application f est bien définie, car si $g' = gh$, où $h \in H \cap K$, alors $gH = g'H$ et $gK = g'K$. Elle est injective, car si $gH = g'H$ et $gK = g'K$, on a $g' = gh = gk$ où $h \in H$ et $k \in K$, ce qui donne $h = k \in H \cap K$. Par conséquent, $[G : H \cap K] \leq [G : H][G : K]$. Pour que l'inégalité soit stricte, il suffit de prendre $H = K \neq G$. Pour un cas d'égalité, on peut prendre, par exemple, $G = \mathbb{Z}$, $H = 2\mathbb{Z}$ et $K = 3\mathbb{Z}$.

   (c) Supposons que $[G : H]$ et $[G : K]$ sont finis et premiers entrer eux. D'après (2)(a) $[G : H]$ et $[G : K]$ divisent $[G : H \cap K]$. Donc, $[G : H][G : K]$ divise $[G : H \cap K]$. Alors, $[G : H \cap K] \geq [G : H][G : K]$. Vu la question (2)(b), on a le résultat désiré.

Théoreme 1.6

Soit E un G-ensemble. Pour tous $x, y \in G$ on a

$$\Omega_x = \Omega_y \Rightarrow G_x \text{ et } G_y \text{ sont conjugués dans } P(G).$$

Démonstration. Supposons $\Omega_x = \Omega_y$. Donc, il existe $g \in G$ tel que $x = g.y$. Donc,

$$\begin{aligned} G_x &= \{h \in G \mid h.x = x\} \\ &= \{h \in G \mid h.(g.y) = g.y\} \\ &= \{h \in G \mid g^{-1}hg.y = y\} \\ &= \{h \in G \mid g^{-1}hg \in G_y\} \\ &= \{h \in G \mid h \in gG_yg^{-1}\} \\ &= gG_yg^{-1}. \end{aligned}$$

□

Théoreme 1.7

Soit E un G-ensemble. Pour tout $x \in E$, on a

$$\mid \Omega_x \mid = [G : G_x].$$

Démonstration. Soient $g, g' \in G$ tels que $g.x = g'.x$. Alors, $g'^{-1}g \in G_x$. D'où, $gG_x = g'G_x$. On peut alors définir l'application $\phi : \Omega_x \to (G/G_x)_g$ avec $\phi(g.x) = gG_x$. ϕ est surjective par construction et $\phi(g.x) = \phi(g'.x)$ implique que $g^{-1}g' \in G_x$ et ainsi $g'.x = g.x$. D'où ϕ est injective. Par suite Ω_x et $(G/G_x)_g$ sont équipotenets. □

Corollaire 1.8

Soient E un G-ensemble fini et $\{x_1, \ldots, x_k\}$ une famille de représentants des G-orbites distinctes. Alors,

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

Démonstration. Les Ω_{x_i} forment une partition de E. Donc,

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

□

Corollaire 1.9 (Équation aux classes)

Soient G un groupe fini et $\{x_1, \ldots, x_k\}$ une famille de représentants des classes de conjugaisons distinctes. Alors

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

Démonstration. On considère l'action par conjugaison sur le groupe G. Pour tout $x \in G$, Ω_x est la classe de conjugaison de x et G_x est le centralisateur de x dans G ; $C_G(x)$. Donc,

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

□

Définition 1.9.1. Soit E un G-ensemble. La partie de E définie par

$$E_G = \{x \in E \mid g.x = x \text{ pour tout } g \in G\}$$

est appelée le sous ensemble des points fixes de E par l'action de G.

Remarques 1.9.1.

1. $E_G = \{x \in E \mid G = G_x\} = \{x \in E \mid \Omega_x = \{x\}\}$.
2. Il est clair que $E_G = E$ si et seulement si l'action est triviale.
3. L'ensemble E_G peut être vide. En effet si l'action est transitive (c-à-d, pour tous $x, y \in E$ il existe $g \in G$ tel que $x = g.y$; en d'autre terme l'action admet une seule orbite qu'est E) alors pour tout $x \in E_G$ (s'il existe) et tout $y \in E$, $y = g.x = x$ pour un certain $g \in G$. Donc, $E = \{x\}$ ou $E_G = \emptyset$.

***Exemples* 1.9.1.**

1. Opération de G sur lui même par conjugaison : Pour tout $x \in G$, $x \in G_G$ si et seulement si $x \in Z(G)$. Donc, $G_G = Z(G)$.
2. Soit $G \leq S_4$ opérant de façon naturelle sur $E = \{1, 2, 3, 4\}$.
   Si $G =< (1, 2, 3) >= \{e, (1, 2, 3), (1, 3, 2)\}$ alors $\Omega_1 = \Omega_2 = \Omega_3 = \{1, 2, 3\}$ et

$\Omega_4 = \{4\}$. Donc, $E_G = \{4\}$
Si $G =< (1,2)(3,4) >= \{e, (1,2)(3,4)\}$, alors $\Omega_1 = \Omega_2 = \{1,2\}$ et $\Omega_3 = \Omega_4 = \{3,4\}$. Donc, $E_G = \emptyset$.

Proposition 1.10

Soit E un G-ensemble fini. Alors,

$$|E| = |E_G| + \sum_{i=1}^{k} |\Omega_{x_i}| = |E_G| + \sum_{i=1}^{k} [G : G_{x_i}]$$

avec $\{\Omega_{x_i}\}$ est l'ensemble des orbites non ponctuelles de E (c-à-d, $|\Omega_{x_i}| > 1$).
En particulier si G est fini,

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

ou les x_i sont des représentants des classes de conjugaisons non ponctuelles.

Démonstration. On a $\Omega_x = \{x\}$ si et seulement si $x \in E_G$. Donc, les orbites des éléments de E_G sont des singletons. Maintenant soient $x_1, \ldots, x_k$ les représentants des orbites non ponctuelles ($x_i \notin E_G$) alors les reprsentants des orbites sont $E_G \cup \{x_1, \ldots, x_k\}$. Ainsi,

$$|E| = \sum_{x \in E_G} |\Omega_x| + \sum_{i=1}^{k} |\Omega_{x_i}| = |E_G| + \sum_{i=1}^{k} |\Omega_{x_i}|.$$

Si G est fini et opère sur lui même par conjugaison alors $G_G = Z(G)$, les orbites sont les classes de conjugaisons et $G_{x_i} = C_G(x_i)$. D'où le résultat. □

Exercice 3. On considère l'ensemble

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in M_2(\mathbb{R}) \mid ac \neq 0 \right\}.$$

1. Vérifier que G est un sous-groupe de $\mathbf{GL}(2,\mathbb{R})$ et que G opère sur $\mathbb{R}$ par l'application
$$\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, x \right) \mapsto \frac{ax+b}{c}.$$
2. Déterminer le noyau de l'action de G sur $\mathbb{R}$, ainsi que le stabilisateur et la G-orbite de 0.

Solution.

1. Pour tous $a, b, c \in \mathbb{R}$, on pose

$$M(a,b,c) = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}.$$

Pour tout $M(a,b,c) \in G$, $\det(M(a,b,c)) = ac \neq 0$, donc $G \subseteq \mathbf{GL}(2,\mathbb{R})$. L'ensemble G est non vide, car il contient la matrice identité $I_2 = M(1,0,1)$. Soient $M(a,b,c)$ et $M(a_0,b_0,c_0)$ deux éléments de G. On a $(M(a,b,c))^{-1} = M(1/a, -b/ac, 1/c) \in G$ et $M(a,b,c)M(a_0,b_0,c_0) = M(aa_0, ab_0 + bc_0, cc_0) \in G$. Donc G est un sous-groupe de $\mathbf{GL}(2,\mathbb{R})$.
L'application donnée est une action de G sur $\mathbb{R}$. En effet, pour tous $M = M(a,b,c)$, $M_0 = M(a_0,b_0,c_0) \in G$ et $x \in \mathbb{R}$, on a

$$M.(M_0.x) = M.\frac{a_0x + b_0}{c_0} = \frac{a\frac{a_0x+b_0}{c_0} + b}{c} = \frac{aa_0x + ab_0 + bc_0}{cc_0} = M(aa_0, ab_0+bc_0, cc_0) = (MM_0).x$$

et

$$I_2.x = x.$$

2. Soit N le noyau de l'action de G sur $\mathbb{R}$. On a

$$N = \left\{ M(a,b,c) \in G \mid \frac{ax+b}{c} = x \; \forall x \in \mathbb{R} \right\} = \{M(a,0,a) \mid a \in R\} = \mathbb{R}I_2.$$

Le stabilisateur de 0 est

$$G_0 = \{M(a,b,c) \in G \mid M.0 = 0\} = \{M(a,b,c) \in G \mid b = 0\} = \{M(a,0,c) \mid ac \neq 0\}.$$

et la G-orbite de 0 est

$$\Omega_0 = \{M(a,b,c).0 \mid M(a,b,c) \in G\} = \{b/c \mid b \in \mathbb{R}, c \neq 0\} = \mathbb{R}.$$

Exercice 4. Soit $G = \mathrm{SL}(2,\mathbb{R})$ le groupe des matrices 2×2 à coefficients réels et de déterminant égal à 1 .

1. Montrer que G opère sur le demi-plan de Poincaré (l'ensemble des complexes de partie imaginaire strictement positive) par l'application

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, z \right) \mapsto \frac{az+b}{cz+d}.$$

2. Déterminer le stabilisateur et la G-orbite de i.

Solution.

1. Soient $M := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ et $z \in \mathbb{C}$ tel que $\mathrm{Im}(z) > 0$. On

$$M.z = \frac{az+b}{cz+d} = \frac{ac|z|^2 + bd + adz + bc\bar{z}}{|cz+d|^2}.$$

Comme par hypothèse, le déterminant de M est l, on voit que $\mathrm{Im}(M.z) = \dfrac{\mathrm{Im}(z)}{|cz+d|^2} > 0$. De plus, avec des notations évidentes, on a

$$M'.(M.z) = M.\frac{az+b}{cz+d} = \frac{(aa'+b'c)z + a'b + b'd}{(c'a+d'c)z + c'b + d'd} = (M'M).z$$

et

$$I_2.z = z.$$

2. Le stabilisateur de i est

$$G_i = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \mid a = d\,, b = -c \right\} = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in G \mid a^2 + b^2 = 1 \right\}$$

et la G-orbite de i est

$$\Omega_i = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}.i \mid a,b,c,d \in \mathbb{R},\ ad - bc = 1 \right\} = \left\{ \frac{ai+b}{ci+d} \mid a,b,c,d \in \mathbb{R},\ ad - bc = 1 \right\}.$$

On a, pour $a, b, c, d \in \mathbb{R}$ tels que $ad - bc = 1$,

$$\frac{ai+b}{ci+d} = \frac{i + ac + bd}{c^2 + d^2}.$$

Donc, Ω_i est inclus dans le demi-plan de Poincaré. Inversement, pour tout $z = xi + y \in \mathbb{C}$ tel que $\mathrm{Im}(z) = x > 0$, on a

$$z = \begin{pmatrix} \sqrt{x} & \dfrac{y}{\sqrt{x}} \\ 0 & \dfrac{1}{\sqrt{x}} \end{pmatrix}.i.$$

Donc, Ω_i est exactement le demi-plan de Poincaré.

Exercice 5. Soit G un groupe fini opérant sur un ensemble fini E.

1. On suppose que l'action de G sur E est telle que $E_G = \emptyset$. Si $|G| = 15$ et $|E| = 17$,

trouver le nombre de G-orbites et le cardinal de chacune d'elles.

2. Montrer que, si $|G| = 33$ et $|E| = 19$, alors nécessairement E_G est non vide.

Solution.

1. Comme $E_G = \emptyset$, alors aucune orbite n'est ponctuelle. Donc, $|\Omega_x| > 1$ pour tout $x \in E$. Soient $x_1, \ldots, x_k$ des représentants des orbites distinctes. Alors, $|\Omega_{x_i}| = [G, G_{x_i}]$ divise $|G| = 15$. Donc, c'est ou bien 3, 5, ou 15. Soient alors a le nombre des orbites de cardinal 3, et b celles de cardinal 5, et c celles de cardinal 15. Donc, $17 = 3a + 5b + 15c$. La seule solution est $a = 4$, $b = 1$ et $c = 0$. Donc, on a 5 orbites.
2. Supposons que E_G est vide. Le cardinal d'une orbite est ou bien 3, ou 11, ou 33. Soient alors a le nombre des orbites de cardinal 3, et b celles de cardinal 11, et c celles de cardinal 33. Donc, $19 = 3a + 11b + 33c$. Alors, $c = 0$ et $19 = 3a + 11b$. Si $b = 1$, alors $8 = 3a$, ce qu'est impossible. Donc, $b = 0$, et $19 = 3a$ ce qu'est aussi impossible. Donc, $E_G \neq \emptyset$.

Exercice 6. Soit E un ensemble fini à n éléments. On considère l'action naturelle de $S(E)$ sur E.

1. Donner les orbites de cette action.
2. Pour $x \in E$ fixé, montrer que $S(E)_x \cong S(F)$ où $S(E)_x$ est le stabilisateur de x et $F = E - \{x\}$.
3. Déduire que $\text{card}(S(E)) = n!$.

Solution.

1. Soit $x \in E$. On a
$$\Omega_x = \{s(x) \mid s \in S(E)\} = E.$$
Donc, cette action admet une seule orbite qu'est E.
2. On a $S(E)_x = \{s \in S(E) \mid s(x) = x\}$. On considère l'application de $S(E)_x$ vers $S(F)$ qui associe a chaque élément s de $S(E)_x$ sa restriction s/F sur F. L'application est bien défini car $s(F) = F$, et elle est isomorphisme de groupes.
3. On a pour $x \in E$ fixé, $|E| = |\Omega_x| = [S(E) : S(E)_x]$. Donc,
$$|S(E)| = |E|\,|S(E)_x| = |E|\,|S(F)|$$
Par récurrence, on obtient le résultat désiré.

Exercice 7 (Formule de Burnside)**.** Soit G un groupe fini opérant sur un ensemble fini E. Pour tout $g \in G$, on note $\mathrm{Fix}(g) = \{x \in E \mid g.x = x\}$. On note aussi r le nombre d'orbites de E sous l'action de G, et on pose

$$F = \{(g, x) \in G \times E \mid g.x = x\}.$$

1. Montrer que $\mathrm{card}(F) = r\,\mathrm{card}(G)$.
2. Déduire que $r = \dfrac{1}{\mathrm{card}(G)} \displaystyle\sum_{g \in G} \mathrm{card}(\mathrm{Fix}(g))$.

Solution.

1. On a
$$F = \bigcup_{x \in E} \{(g, x) \in G \times E \mid g.x = x\}.$$
Donc,
$$|F| = \sum_{x \in E} |G_x| = \sum_{i=1}^{r} \sum_{x \in \Omega_{x_i}} |G_{x_i}| = \sum_{i=1}^{r} \sum_{x \in \Omega_{x_i}} \left| \frac{|G|}{|\Omega_{x_i}|} \right| = r|G|.$$
2. On a
$$|F| = \left| \bigcup_{g \in G} \{(g, x) \in G \times E \mid g.x = x\} \right| = \left| \bigcup_{g \in G} \mathrm{Fix}(g) \right|$$
Donc,
$$r = \frac{1}{\mathrm{card}(G)} \sum_{g \in G} \mathrm{card}(\mathrm{Fix}(g))$$

Théoreme 1.11

Soit G un groupe fini d'ordre p^n avec p premier et $n \geq 1$. Alors, p divise $|Z(G)|$.

Démonstration. Si G est abélien, le résultat est trivial. On suppose donc que G n'est pas abélien. Il existe $g, h \in G$ tels que $gh \neq hg$, et donc $ghg^{-1} \neq h$. Ainsi, la classe de conjugaison de h contient au moins deux éléments distincts h et ghg^{-1}. Soient $x_1, \ldots, x_k$ les représentants des classes de conjugaisons non ponctuelles. Il est clair que $[G : C_G(x_i)] > 1$ sinon $G = C_G(x_i)$ (et donc $x_i \in Z(G)$). Donc, comme $[G : C_G(x_i)]$ divise $|G| = p^n$, on a $[G : C_G(x_i)] = p^{k_i}$ avec $0 < k_i < n$. De l'équation aux classes

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

on déduit que

$$|Z(G)| = p^n - \sum_{i=1}^{k} p^{k_i}$$

Ainsi, p divise $|Z(G)|$. D'où le résultat. □

Théoreme 1.12

Tout groupe d'ordre p^2 (avec p premier) est abélien. Dans, ce cas $G \cong \mathbb{Z}/p^2\mathbb{Z}$ ou $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Démonstration. On a $|Z(G| = p$ ou $|Z(G)| = p^2$. Supposons que $|Z(G)| = p$. Alors, $\left|\frac{G}{Z(G)}\right| = p$. Donc, $G/Z(G)$ est cyclique. Posons $G/Z(G) = (\overline{a})$. Alors, pour tous $g_1, g_2 \in G$, on a $g_1 = a^{k_1}z_1$ et $g_2 = a^{k_2}z_2$ avec $z_1, z_2 \in Z(G)$. Donc, $g_1g_2 = a^{k_1+k_2}z_1z_2 = g_2g_1$. Ainsi, G est abélien, ce qu'est absurde. Donc, $|Z(G)| = p^2$, et donc G est abélien.
Si $G = (a)$ est cyclique alors $G \cong \mathbb{Z}/p^2\mathbb{Z}$ par le morphisme $a^k \mapsto \overline{k}$. Sinon, soit $x \in G$ d'ordre p. Donc, $G/(x)$ est cyclique d'ordre p. Posons $G/(x) = (\overline{y})$ (avec $(x) \cap (y) = \{e\}$). Alors, tout $g \in G$ s'écrit de la forme $g = x^iy^j$. Cette écriture est unique. En effet, $x^iy^j = x^ny^m$ implique que $x^{i-n} = y^{m-j} = e$. Par suite, $G = (x, y)$. Dans ce cas, $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ via le morphisme $x^iy^j \mapsto (\overline{i}, \overline{j})$. □

1.3 Produit semi-direct

Définition 1.12.1 (Produit semi-direct d'un sous-groupe normal par un autre sous–groupe)**.** Etant donné un groupe G et deux sous-groupes H et N. On dira que G est produit semi-direct de N par H, et on écrit $G = N \rtimes H$, si :

1. $N \trianglelefteq G$.
2. $G = NH$.
3. $N \cap H = \{1\}$.

H est appelé complément de N dans G. L'application du second théorème d'isomorphisme donne $G/N \cong H$.

***Exemple* 1.12.1.** On considère le groupe S_3. On pose

$$N =< a = (1,2,3) > \quad \text{et} \quad H =< b = (2,3) > .$$

On a

$$N = \{1, a, a^2 = (1,3,2)\}, \quad H = \{1, b\} \quad \text{et} \quad S_3 = \{1, a, a^2, b, ab = (1,2), a^2b = (1,3)\}.$$

Donc, $N \cap H = \{1\}$, $S_3 = NH$ et $N \trianglelefteq S_3$ (car $[S_3, N] = 2$). Donc, S_3 est produit semi-direct de N par H.

Proposition 1.13 (et Définition)

Soient H et N deux groupes et $\varphi \in \mathrm{Hom}(H, \mathrm{Aut}(N))$ un morphisme de groupes. L'ensemble $N \times H$ muni de la loi de composition interne (multiplicative) définie par :

$$(n, h)(n', h') = (n\varphi(h)(n'), hh')$$

est un groupe (non abélien en général) noté $N \times_\varphi H$, et appelé produit semi-direct de N par H relativement à φ.

Démonstration. Associativité : Soient $(n, h), (n', h'), (n'', h'') \in N \times H$. On a

$$\begin{aligned}
\big((n, h)(n', h')\big)(n'', h'') &= (n\varphi(h)(n'), hh')(n'', h'') \\
&= (n\varphi(h)(n')\varphi(hh')(n''), hh'h'') \\
&= (n\varphi(h)(n')\varphi(h) \circ \varphi(h')(n''), hh'h'') \\
&= (n\varphi(h)(n')\varphi(h)(\varphi(h')(n'')), hh'h'') \\
&= (n\varphi(h)(n'\varphi(h')(n'')), hh'h'') \\
&= (n, h)(n'\varphi(h')(n''), h'h'') \\
&= (n, h)\big((n', h')(n'', h'')\big)
\end{aligned}$$

L'élément neutre est $(1_N, 1_H)$ et $(n, h)^{-1} = (\varphi(h^{-1}(n^{-1}), h^{-1})$. □

Remarque 1.13.1.

1. Avec les notations du Proposition précédente, on pose $N' = \{(n, 1_H) \mid n \in N\}$ et $H' = \{(1_N, h) \mid h \in H\}$. On peut vérifier facilement que N' et H' sont des sous groupes de $N \times_\varphi H$ et que $N \times_\varphi H$ est produit semi-direct de N' par H'.
2. Si $\varphi(h) = \mathrm{Id}_N$ pour tout $h \in H$, alors $N \times_\varphi H$ est le groupe $N \times H$.

***Exemple* 1.13.1.** On pose $N = U(\mathbb{Z}/5\mathbb{Z}) = \{1, 2, 3, 4\}$ et $H = U(\mathbb{Z}/3\mathbb{Z}) = \{1, 2\}$. On considère $\varphi \in \mathrm{Hom}(H, Aut(N))$ définie par $\varphi(1) = \mathrm{Id}_N$ et $\varphi(2)(x) = x^{-1}$ pour tout $x \in N$. Dans $N \times_\varphi H$ on a $(1, 2)(2, 1) = (3, 2)$ et $(2, 1)(1, 2) = (2, 2)$. Ainsi, même si N et H sont commutatifs, le produit semi-direct de N par H relativement à φ n'est pas commutatif.

Exercice 8.

1. Soit G un groupe engendré par deux éléments a et b tels que

$$(*) : \quad o(a) = n \quad (n > 2), \quad o(b) = 2, \quad \text{et} \quad ba = a^{-1}b.$$

Montrer que G est non abélien d'ordre $2n$.

2. On appelle groupe diédral de degré $n \in \mathbb{N}^*$, noté D_n, le sous groupe de S_n engendré par $\sigma = (1, 2, \ldots, n)$ et

$$\nu = \begin{pmatrix} 1 & 2 & 3 & \ldots & i & \ldots & n-2 & n-1 & n \\ 1 & n & n-1 & \ldots & n+2-i & \ldots & 4 & 3 & 2 \end{pmatrix}.$$

   (a) Montrer que, pour tout $n > 2$, $D_n \cong G$.

   (b) Donner les ordres de tous les éléments de D_4.

3. Montrer que l'on peut écrire le groupe diédral D_n comme un produit semi-direct naturel $\mathbb{Z}_n \times_\phi \mathbb{Z}_2$.

Solution.

1. Le groupe G est non abélien, sinon $ab = ba = a^{-1}b$ et donc $a^2 = e$ (ce qu'est absurde).
   Par hypothèse $G =< a, b >$, par suite tout élément de G est un produit de puissances entières (positives, négatives ou nulles) de a et de b. Le groupe G peut donc être considéré comme engendré par $< a > \cup < b >$. Par hypothèse aussi,

$$< a >= \{a^0 = e, a, a^2, \cdots, a^{n-1}\} \text{ et } < b >= \{b^0 = e, b\}.$$

   — Pour tout $0 \leq k \leq n-1$, les éléments $a^k b$ sont deux à deux distincts et $b \notin < a >$ implique qu'aucun d'eux n'appartient à $< a >$.
   — De plus, pour tout $0 \leq k \leq n-1$,

$$ba^k = a^{-1}ba^{k-1} = \cdots = a^{-k}b.$$

   On en déduit que $< a >< b >=< b >< a >$ est un sous-groupe de G et c'est alors le sous-groupe de G engendré par $< a > \cup < b >$, par suite $G =< a >< b >$. D'où $G = \{e, a, ..., a^{n-1}, b, ab, ..., a^{n-1}b\}$. Le groupe G est donc d'ordre $2n$.

2. (a) Les ordres de σ et ν sont n et 2, respectivement. En plus, pour tout $2 \leq i \leq n-1$, on a $3 \leq i+1 \leq n$ et $3 \leq n+2-i \leq n$ et donc

$$\nu\sigma(i) = \nu(i+1) = n+2-(i+1) = n+1-i \quad et \quad \sigma^{-1}\nu(i) = \sigma^{-1}(n+2-i) = n+1-i.$$

   Aussi,

$$\nu\sigma(1) = \nu(2) = n, \quad \sigma^{-1}\nu(1) = \sigma^{-1}(1) = n, \quad \nu\sigma(n) = \nu(1) = 1, \quad \sigma^{-1}\nu(n) = \sigma^{-1}(2) = 1.$$

Donc, $\nu\sigma = \sigma^{-1}b$.

Par suite un morphisme φ tel $\varphi(a) = \sigma$ et $\varphi(b) = \nu$ est nécessairement un isomorphisme de D_n sur G.

(b) Pour $n = 4$, $G = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$. Les éléments a et a^3 sont d'ordre 4 et les éléments a^2, b, ab, a^2b et a^3b sont d'ordre 2.

3. Soit le morphisme $\phi : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_n)$ défini par $\phi(1) = -\mathrm{Id}_{\mathbb{Z}_n}$. On considère, dans $\mathbb{Z}_n \times_\phi \mathbb{Z}_2$, les éléments $a = (1, 0)$ et $b = (0, 1)$. On a pour tout $1 \leq k \leq n$, $a^k = (1, 0)^k = (k, 0)$, $a^k b = (k, 1)$ et $b^2 = (0, 1)^2 = (0, 0)$. Donc, a est d'ordre n, b est d'ordre 2 et $\mathbb{Z}_n \times_\phi \mathbb{Z}_2$ est engendré par a et b. En plus,

$$ba = (0, 1)(1, 0) = (-1, 1) \text{ et } a^{-1}b = (-1, 0)(0, 1) = (-1, 1).$$

Donc, d'après 2(a), $D_n \cong \mathbb{Z}_n \times_\phi \mathbb{Z}_2$.

Exercice 9. Soit G un groupe et soient N et H des sous-groupes de G tels que $G = N \rtimes H$.

1. Vérifier que l'application $\iota : H \to \mathrm{Aut(N)}$ définie par $\iota(h)(n) = hnh^{-1}$ est un morphisme de groupes.
2. Montrer que $G \cong N \times_\iota H$.
3. Quand le produit semi-direct se révèle-t-il être un produit direct ?
4. À quelle condition un produit semi-direct est-il commutatif ?

Solution.

1. C'est évident (ι est bien définie car N est distingué dans G).
2. L'application
$$\begin{array}{rccc} f : & N \times_\iota H & \longrightarrow & G \\ & (n, h) & \longmapsto & nh \end{array}$$
est un morphisme de groupes. L'hypothèse $NH = G$ assure que f est surjectif, et l'hypothèse $N \cap H = \{e\}$ assure que le noyau de f est trivial. Donc f est un isomorphisme.
3. Un produit semi-direct $N \times_\phi H$ est direct si $(nn', hh') = (n\phi(h)(n'), hh')$ pour tous $n, n' \in N$ et $h, h' \in H$. Donc, pour $n = e_N$, on a $\phi(h)(n') = n'$. Ainsi, ϕ est trivial. Inversement, si ϕ est trivial, on obtient un produit direct.
4. Un produit semi-direct $N \times_\phi H$ est abélien si $(n\phi(h)(n'), hh') = (n'\phi(h')(n), h'h)$ pour tous $n, n' \in N$ et $h, h' \in H$. Donc, pour $n = e$, on obtient $\phi(h)(n') = n'$. Ainsi, ϕ est trivial, et le produit semi-direct est maintenant un produit direct. Ainsi, N et H sont nécessairement abélien. Par suite, pour qu'un produit semi-direct $N \times_\phi H$ soit abélien il faut que ϕ soit trivial et N et H soient abélien. Le sens inverse est trivial.

Exercice 10. Démontrer que pour qu'il existe un produit semi-direct non direct, $\mathbb{Z}_n \times_\phi \mathbb{Z}_m$, il faut qu'il existe r premier avec n, tel que $r^m = 1\,[n]$. Existe t-il un produit semi-direct non trivial de la forme $\mathbb{Z}_4 \times_\phi \mathbb{Z}_3$

Solution.
Le morphisme $\phi(\overline{1})$ est définie par $\phi(\overline{1})(\hat{1}) = \hat{r}$ avec r premier avec n. Donc,

$$\hat{1} = \phi(\overline{0})(\hat{1}) = \phi(\overline{m})(\hat{1}) = \phi(\overline{1})^m(\hat{1}) = \hat{r}^m.$$

D'où le résultat.
Il n'existe aucun produit semi-direct non trivial de la forme $\mathbb{Z}_4 \times_\phi \mathbb{Z}_3$. En effet, l'équation $r^3 = 1\,[4]$ avec r premier avec 4 n'admet pas de solution.

Exercice 11. Une suite courte de morphismes de groupes

$$1 \to N \xrightarrow{\iota} G \xrightarrow{\pi} H \to 1$$

est dite exacte si ι est injectif, π est surjectif et $\mathrm{Im}(\iota) = \ker(\pi)$.

1. Montrer que, si G est le produit direct de N par H, alors on a une telle suite exacte.
2. Soit une telle suite exacte. Montrer que s'il existe un morphisme de groupes $s : H \to G$ tel que $\pi \circ s = \mathrm{Id}_H$ alors G est le produit semi-direct de $\iota(N)$ par $s(H)$.
3. En utilisant une suite exacte convenable, montrer que le groupe symétrique est produit semi-direct du groupe alterné et du groupe engendré par une transposition.

Solution.

1. On pose $G = N \times_\phi H$. On considère $\iota : N \to G$ défini par $\iota(n) = (n, e_H)$ et $\pi : G \to H$ défini par $\pi(n, h) = h$. Il est facile de voir que la suite $1 \to N \xrightarrow{\iota} G \xrightarrow{\pi} H \to 1$ est exacte.
2. Soit $1 \to N \xrightarrow{\iota} G \xrightarrow{\pi} H \to 1$ une suite exacte. On suppose qu'il existe un morphisme de groupes $s : H \to G$ tel que $\pi \circ s = \mathrm{Id}_H$.
   — Soient $g \in G$ et $n \in N$. On a $\pi(g\iota(n)g^{-1}) = \pi(g)e_H\pi(g^{-1}) = e_H$. Donc, $g\iota(n)g^{-1} \in \ker(\pi) = \mathrm{Im}(\iota)$. Ainsi, $g\iota(n)g^{-1} \in \iota(N)$. Par suite, $\iota(N) \trianglelefteq G$.
   — Soit $g \in \iota(N) \cap s(H)$. Donc, $\iota(n) = g = s(h)$, et alors $e_H = \pi(g) = \pi(s(h)) = h$. Ainsi, $g = s(e_H) = e_G$. Par conséquent, $\iota(N) \cap s(H) = \{e_G\}$.
   — Soit $g \in G$. On pose $h = s \circ \pi(g) \in s(H)$ et $n = gh^{-1}$. On a $\pi(n) = \pi(g)\pi(g)^{-1} = e_H$. Donc, $n \in \iota(N)$ et $g = nh$. Alors, $G = \iota(N)s(H)$.
   On en déduit alors que G est le produit semi-direct de $\iota(N)$ par $s(H)$.
3. On pose $\sigma = (1, 2)$ et $s : \{-1, 1\} \to S_n$ le morphisme défini par $s(-1) = \sigma$. On considère ensuite la suite exacte $1 \to A_n \hookrightarrow G \xrightarrow{\varepsilon} \{-1, 1\} \to 1$ avec ε est le

morphisme signature. On a clairement $\varepsilon \circ s = \mathrm{Id}_{\{-1,1\}}$. Donc, comme $\mathrm{Im}(s) =< \sigma >$, on a $S_n = A_n \rtimes < \sigma >$.

Exercice 12. Soit $G = N \rtimes H$ et soit K un sous-groupe de G contenant N. Montrer que $K = N \rtimes (K \cap H)$.

Solution.

On a

— $N \trianglelefteq K$ (car $N \trianglelefteq G$),

— $N \cap (K \cap H) = K \cap (N \cap H) = \{e\}$, et

— pour tout $k \in K$, on a $k = nh$ avec $n \in N$ et $h \in H$. Donc, $h = n^{-1}k \in K$. Ainsi, $h \in K \cap H$ et $K = N(K \cap H)$.

On en déduit alors que $K = N \rtimes (K \cap H)$.

Exercice 13. Soient H et N deux groupes et soient $\psi, \phi : H \to \mathrm{Aut}(N)$ des morphismes. On veut trouver des conditions nécessaires et suffisantes pour que $N \times_\psi H$ et $N \times_\phi H$ soient isomorphes.

1. S'il existe un automorphisme α de H tel que $\psi = \phi \circ \alpha$, montrer que l'on a la conclusion attendue.
2. S'il existe un automorphisme u de N tel que, pour tout $h \in H$ on a $\phi(h) = u\psi(h)u^{-1}$, montrer que la conclusion attendue vaut encore.
3. Si H est cyclique et $\psi(H) = \phi(H)$, montrer qu'on a encore l'isomorphisme désiré.

Solution.

Soient H et N deux groupes et soient $\psi, \phi : H \to \mathrm{Aut}(N)$ des morphismes. On veut trouver des conditions nécessaires et suffisantes pour que $N \times_\psi H$ et $N \times_\phi H$ soient isomorphes.

1. Le morphisme
$$\begin{array}{ccc} N \times_\psi H & \longrightarrow & N \times_\phi H \\ (n,h) & \longmapsto & (n, \alpha(h)) \end{array}$$
est un isomorphisme.
2. Le morphisme
$$\begin{array}{ccc} N \times_\psi H & \longrightarrow & N \times_\phi H \\ (n,h) & \longmapsto & (u(n), h) \end{array}$$
est un isomorphisme.
3. On pose $H =< x >$ et $|H| = n$. Alors, $K = \psi(H) =< \psi(x) >$ est aussi un groupe cyclique d'ordre m avec m divise n. Or, $\phi(x)$ est aussi un générateur de K. Donc, $\phi(x) = \psi(x)^d$ avec d premier avec m. Soient $m = \prod_{i=1}^{k} p_i^{\alpha_i}$ et $n = \prod_{i=1}^{k} p_i^{\beta_i} \prod_{j=1}^{r} q_j^{\gamma_j}$ les décompositions de m et n en produits de facteurs premiers. D'après le lemme de

Chinois, il existe $a \in \{1, \cdots, n\}$ tel que $a \equiv d\,[p_i^{\beta_i}]$ et $a \equiv 1\,[q_j^{\beta_j}]$. On a alors a est premier avec n et $a - d \in m\mathbb{Z}$. On considère le morphisme $\alpha : H \to H$ tel que $\alpha(x) = x^a$. On a

$$\phi \circ \alpha(x) = \phi(x^a) = \phi(x)^a = \phi(x)^d = \psi(x).$$

Donc, d'après la première question, on a le résultat désiré.

Exercice 14. 1. Montrer que le groupe $\mathbb{H}_8$, appelé groupe quaternionique, défini par :

$$\mathbb{H}_8 = \left\langle a, b \mid a^4 = e,\ a^2 = b^2,\ ba = a^{-1}b \right\rangle$$

est non abélien et admet huit éléments. Quels sont les ordres de ses éléments ?

2. Montrer que $\mathbb{H}_8$ est isomorphe au groupe engendré par les matrices complexes

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

3. Dire pourquoi $\mathbb{H}_8$ n'est pas un produit semi-direct ?
4. Vérifier que $\mathbb{H}_8 \ncong D_4$.

Solution.

1. Le groupe $\mathbb{H}_8$ est non abélien, sinon $ab = ba = a^{-1}b$ et donc $a^2 = e$ (ce qu'est absurde).
Par hypothèse $\mathbb{H}_8 =< a, b >$, par suite tout élément de $\mathbb{H}_8$ est un produit de puissances entières de a et de b. Le groupe $\mathbb{H}_8$ peut donc être considéré comme engendré par $< a > \cup < b >$. Par hypothèse aussi,

$$< a >= \{a^0 = e, a, a^2, a^3\} \text{ et } < b >= \{b^0 = e, b, b^2, b^3\}.$$

— Pour tout $0 \leq k \leq 3$, les éléments $a^k b$ sont deux à deux distincts et $b \notin < a >$ implique qu'aucun d'eux n'appartient à $< a >$.
— De plus, pour tout $0 \leq k \leq n - 1$,

$$ba^k = a^{-1}ba^{k-1} = \cdots = a^{-k}b, \quad b^2a^k = a^{k+2}, \quad b^3a^k = ba^{k+2} = a^{-k-2}.$$

On en déduit que $< a >< b >=< b >< a >$ est un sous-groupe de $\mathbb{H}_8$ et c'est alors le sous-groupe de G engendré par $< a > \cup < b >$, par suite $\mathbb{H}_8 =< a >< b >$. D'où $G = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$. Le groupe G est donc d'ordre 8. Le seul élément d'ordre 2 est $a^2 = b^2$ et les éléments d'ordre 4 sont a, a^3, b, ab, a^2b et a^3b.

2. On a $A^2 = B^2 = -I_2$ et $A^{-1}B = -AB = BA$. Par suite un morphisme φ tel $\varphi(a) = A$ et $\varphi(b) = B$ est nécessairement un isomorphisme de $\mathbb{H}_8$ sur le groupe $G =< A, B >$.
3. Supposons que $\mathbb{H}_8 = N \rtimes H$. Donc, $|N|\,|H| = 8$. Ainsi, $|N| = 2$ ou 4.
   — Si $|N| = 2$, alors $|H| = 4$ et donc $H \trianglelefteq \mathbb{H}_8$. Par suite, $\mathbb{H}_8 \cong N \times H$. Or, les groupes N et H doivent être abélien (en effet, ils sont de cardinaux 2 et 4). Par contre $\mathbb{H}_8$ n'est pas abélien, et donc cette situation est impossible.
   — Si $|N| = 4$, alors $|H| = 2$. Le seul élément d'ordre 2 est $a^2 = b^2$. Donc, $H =< a^2 >$. Comme a^2 commute avec a et b, il commute avec tous les éléments de G, et donc $H \trianglelefteq \mathbb{H}_8$. Ce cas est aussi impossible comme dans le premier cas.

   Par conséquent, $\mathbb{H}_8$ n'est pas un produit semi-direct.
4. Cela découle dut fait que D_4 est produit semi-direct par contre $\mathbb{H}_8$ ne l'est pas.
   On peut aussi raisonner suivant les éléments d'ordre 2. On sait que D_4 admet 5 éléments d'ordre 2, alors que $\mathbb{H}_8$ n'admet qu'un seul.

1.4 Théorèmes de Sylow

Plusieurs des notions et résultats précédents permettent de caractériser les sous-groupes d'un groupe fini donné. En particulier, on a vu que l'ordre d'un sous-groupe doit diviser l'ordre du groupe, ce qui réduit considérablement les possibilités. Cependant, cette contrainte n'est pas suffisante en général pour caractériser l'ordre possible des sous-groupes. Par exemple, pour le groupe alterné A_4 d'ordre $12 = 2.6$, on n'a pas de sous-groupe d'ordre 6. Nous allons chercher à déterminer (en partie) quand un groupe donné admet un sous-groupe d'ordre d, pour d divisant son ordre. En toute généralité, cette question est peut-être trop difficile. Cependant, en la restreignant au cas où $d = p^n$, avec p premier, on a les résultats remarquables de Sylow. Afin de les énoncer, on se donne la définition suivante.

Définition 1.13.1.
1. Si G est un groupe fini, on dit que G est un p-groupe, si $|G| = p^n$, où p est un nombre premier et $n \in N$.
2. Soit G un groupe fini d'ordre $|G| = p^n.m$, avec $n \in N^*$ et p premier ne divisant pas m. On dit qu'un sous-groupe de G est un sous-groupe de Sylow si son ordre est p^n. Autrement dit, c'est un p-sous-groupe (c'est à dire son ordre est une puissance de p) d'ordre le plus grand possible.

Théoreme 1.14 (Premier théorème de Sylow)

Soit G un groupe fini d'ordre $|G| = p^n.m$, avec $n \in N^*$ et p premier ne divisant pas m. Alors le groupe G possède un sous-groupe d'ordre p^s pour tout $0 \leq s \leq n$. En particulier, G contiens un p-sous-groupe de Sylow.

Démonstration. On a

$$C_{mp^n}^{p^s} = \frac{mp^n.(mp^n-1)\dots(mp^n-p^s+1)}{p^s.(p^s-1)\dots.1} = mp^{n-s}.\frac{mp^n-1}{1}.\frac{mp^n-2}{2}.\dots.\frac{mp^n-(p^s-1)}{p^s-1}.$$

Pour tout $1 \leq k \leq p^s-1$, on pose $k = p^{\alpha_k}q_k$ avec p ne divise pas q_k. Donc,

$$\frac{mp^n-k}{k} = \frac{mp^n-p^{\alpha_k}q_k}{p^{\alpha_k}q_k} = \frac{mp^{n-\alpha_k}-q_k}{q_k}.$$

Ainsi,

$$C_{mp^n}^{p^s} = mp^{n-s}.\prod_{k=1}^{p^s-1}\frac{mp^{n-\alpha_k}-q_k}{q_k}.$$

Alors,

$$\left(\prod_{k=1}^{p^s-1}q_k\right)C_{mp^n}^{p^s} = mp^{n-s}\prod_{k=1}^{p^s-1}mp^{n-\alpha_k}-q_k.$$

L'entier $\prod_{k=1}^{p^s-1}q_k$ est premier avec p, et donc p^{n-s} divise $C_{mp^n}^{p^s}$. En plus, $\prod_{k=1}^{p^s-1}mp^{n-\alpha_k}-q_k$ est premier avec p, et donc $n-s$ est exactement l'ordre de p dans la décomposition en facteurs premiers de $C_{mp^n}^{p^s}$. Par suite, $C_{mp^n}^{p^s} = ap^{n-s}$ avec p ne divise pas a.
Soit $\mathcal{F}$ l'ensemble des partie de G de cardinal p^s. Donc, $|\mathcal{F}| = ap^{n-s}$. En outre, pour tout $g \in G$ et $A \in \mathcal{F}$, on a $|gA| = |A|$, et donc $gA \in \mathcal{F}$. Donc, G opère sur F par translation à gauche. Soient $A_1, \dots, A_k$ les representants des différentes orbites. On a alors $|\mathcal{F}| = \sum_{i=1}^{k}[G : G_{A_i}]$. Il existe $1 \leq i \leq k$ tel que p^{n-s+1} ne divise pas $[G : G_{A_i}]$. On pose $H = G_{A_i}$, $[G : G_{A_i}] = cp^{\beta}$ avec $\beta \leq n-s$ et p ne divise pas β. Donc, $|H| = bp^{n-\beta}$ avec p ne divise pas b et $\alpha = n-\beta \geq s$. Donc, p^s divise $|H|$. Soit $x \in A_i$, on a $g \neq g'$ implique $gx \neq g'x$ pour tout $g, g' \in G$, et donc $|Hx| = |H|$. Or, pour tout $g \in H$, $gx \in gA_i = A_i$. Donc, $Hx \subseteq A_i$. Ainsi, $|H| \leq |A_i| = p^s$. Donc, $|H| = p^s$. □

En appliquant le théorème précédent dans le cas $s = 1$, puis dans le cas $s = n$, on obtient les deux résultats suivants :

Corollaire 1.15 (Théorème de Cauchy)

G étant un groupe fini, si p est un nombre premier divisant l'ordre de G, alors G a au moins un élément d'ordre p.

Corollaire 1.16

Si G est un groupe fini d'ordre sp^n, où p est un nombre premier ne divisant pas s, alors G contient au moins un sous-groupe d'ordre p^n.

Lemme 1.17

Soient G un groupe fini d'ordre p^n et E un G-ensemble fini. Alors,

$$|E| \equiv |E_G| \, [p].$$

Démonstration. On a

$$|E| = |E_G| + \sum_{i=1}^{k} [G : G_{x_i}]$$

où les x_i sont les représentants des orbites non ponctuelles distinctes de cette action. On sai que les $[G : G_{x_i}] > 1$ sont des puisance de p, et donc on a le résultat. □

Lemme 1.18

Soient H et K deux sous groupes d'un groupe G tels que $[G : H] = s$ et $|K| = p^n$ avec p ne divise pas s et $n \geq 1$. Alors, il existe $x \in G$ tel que $K \subseteq xHx^{-1}$. En d'autres termes, si $[G : H] = s$ alors tout p-sous groupe de G avec p ne divise pas s est inclus dans un conjugué de H.

Démonstration. On considère l'action de K par translation à gauche sur $(G/H)_g$. On a

$$[G : H] = s \equiv |E_K| \, [p].$$

Comme p ne divise pas s, alors $E_K \neq \emptyset$. Soit $xH \in E_K$. On a $K(xH) = xH$. Donc, $Kx \subseteq xH$ et ainsi $K \subseteq xHx^{-1}$. □

Lemme 1.19

G étant un groupe fini, si S est un p-sous-groupe de Sylow de G, alors S est l'unique p-sous-groupe de Sylow de $N_G(S) = \{g \in G \mid gS = Sg\}$ (c'est le stabilisateur de S pour l'action de G sur $P(G)$ par conjugaison).

Démonstration. Posons $|G| = m.p^s$. On a S est un sous groupe de $N_G(S)$ et $|S| = p^s$. Donc, $|N_G(S)| = a.p^s$ (avec a divise m et p ne divise pas a). Soit K un p-sous groupe de

Sylow de $N_G(S)$. Alors, $[N_G(S) : K] = [N_G(S) : S] = a$. Alors, il existe $x \in N_G(S)$ tel que $K \subseteq xSx^{-1} = S$. Donc, $K = S$. □

Théoreme 1.20 (Second théorème de Sylow)

Soient G un groupe fini et p un nombre premier divisant l'ordre de G ; alors,

1. tout p-sous-groupe de G est contenu dans un p-sous-groupe de Sylow de G ;
2. les p-sous-groupes de Sylow de G sont conjugués ;
3. le nombre n_p des p-sous-groupes de Sylow de G est congru à 1 modulo p et divise l'ordre de G.

Démonstration. On pose $|G| = mp^s$.

1. Soit H un p-sous groupe de G et soit S un p-sous groupe de Sylow. On a $[G : S] = m$. D'après le lemme 1.18, il existe $x \in G$ tel que $H \subseteq xSx^{-1}$. Or, xSx^{-1} est aussi un p-sous groupe de Sylow car $|xSx^{-1}| = |S|$.

2. Soient S et S' deux p-sous groupe de Sylow de G. Alors, d'après le lemme 1.18, il existe $x \in G$ tel que $S' \subseteq xSx^{-1}$, et d'où $S' = xSx^{-1}$.

3. On considère l'action de G sur $\mathcal{S}$; l'ensemble des p-sous groupes de Sylow de G, par conjugaison. Il est bien définie. Soit $S \in \mathcal{S}$. Tous les éléments de $\mathcal{S}$ sont conjugués à S, et donc cette action admet une seule orbite qu'est donc $\mathcal{S}$. En plus,

$$G_S = \{g \in G \mid gS = Sg\} = N_G(S).$$

Donc,

$$|\mathcal{S}| = |\Omega_S| = [G : G_S] = [G : N_G(S)].$$

Alors, $|\mathcal{S}|$ divise $|G|$. En outre, S opère par conjugaison sur $\mathcal{S}$, et

$$\mathcal{S}_S = \{S' \in \mathcal{S} \mid xS'x^{-1} = S' \ \forall x \in S\}.$$

Ainsi, si $S' \in \mathcal{S}_S$, on a $S \subseteq N_G(S')$, et donc d'après le lemme 1.19, $S = S'$. Donc, $|\mathcal{S}_S| = 1$. En outre, d'après le lemme 1.17, $|S| \equiv |\mathcal{S}_S| = 1[p]$.

□

Corollaire 1.21

Un groupe fini G a un unique p-sous-groupe de Sylow S, si et seulement si S est distingué dans G. En particulier, dans un groupe fini abélien G, pour tout nombre premier p divisant l'ordre de G, il n'existe qu'un seul p-sous-groupe de Sylow.

Démonstration. Si S est unique alors $xSx^{-1} = S$ pour tout $x \in G$, et donc S est distingué. Inversement, si S est distingué il est unique car tous les p-sous groupe de Sylow sont conjugués. □

Corollaire 1.22

Si $G \neq (e)$ est un groupe abélien fini, d'ordre $p_1^{\alpha_1} \dots p_k^{\alpha_k}$, $k \geq 1$, les p_i $(1 \leq i \leq k)$ étant des nombres premiers distincts et les α_i des entiers positifs non nuls, alors G est isomorphe au produit direct de ses p_i-sous-groupes de Sylow distincts.

Démonstration. G étant abélien, il admet un seul p_i-sous groue de Sylow pour tout i qu'on note H_i. On pose $K = H_2 \cdots H_k$. Soit $x \in H_1 \cap K$. Posons $x = x_1 = x_2 \cdots x_k$. Alors $x^{p_2^{\alpha_2} \cdots p_k^{\alpha_k}} = e$. Donc, si $x \neq e$, p_1 divise $p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, ce qu'est absurde. Donc $H_1 \cap K = \{e\}$. Donc, $H_1K \cong H_1 \times K$. On a $|H_1K| = |H_1||K|$, et donc par induction $|H_1 \cdots H_k| = |H_1| \cdots |H_k| = |G|$. Donc, $G = H_1 \cdots H_k$. Par induction encore $G = H_1 \cdots H_k \cong H_1 \times \cdots \times H_k$. □

Exercice 15. Soient p et q deux entiers premiers avec $p < q$. Soit G un groupe d'ordre pq.

1. Montrer que $n_q = 1$.
2. Montrer que si $q \not\equiv 1\ [p]$, alors G est isomorphe à $\mathbb{Z}_{pq}$, et est donc cyclique.
3. On suppose que $q \equiv 1\ [p]$.
   (a) Montrer que G est soit cyclique, isomorphe à $\mathbb{Z}_{pq}$, ou est produit semidirect (non direct) de la forme $\mathbb{Z}_q \times_\phi \mathbb{Z}_p$.
   (b) Montrer que, à isomorphisme près, il y a deux groupes distincts de cardinal pq.
4. Déduire que tout groupe G d'ordre $2q$ avec $q > 2$ un nombre premier est isomorphe à $\mathbb{Z}_{2q}$ ou à D_q.

Solution.

1. On a $n_q \equiv 1\ [q]$ et n_q divise p. Donc, puisque $p < q$, on a nécessairement $n_q = 1$.

2. Supposons que $q \not\equiv 1\,[p]$. Alors, $n_p = 1$. Il n'y a alors qu'un seul p-Sylow S_p et un seul q-Sylow S_q qui sont distingués dans G. Donc,

$$G = S_p S_q \cong S_p \times S_q \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}.$$

3. On suppose que $q \equiv 1\,[p]$.
   (a) Comme $q \equiv 1\,[p]$, alors il peut y avoir plusieurs p-Sylow. Soit H un de ces groupes, et N l'unique q-Sylow. Ces deux groupes satisfont le critère du produit semi-direct, et donc $G \cong N \times_\phi H$. Étudions maintenant l'existence de ϕ. L'ordre de $\mathrm{Im}(\phi)$ est soit 1 soit p. Si c'est 1, alors ϕ est trivial, et donc $G \cong N \times H \cong \mathbb{Z}_{pq}$. Sinon, $G \cong \mathbb{Z}_q \times_\phi \mathbb{Z}_p$ (car $N \cong \mathbb{Z}_q$ et $H \cong \mathbb{Z}_p$).
   (b) Si ϕ est non trivial, alors $\mathrm{Im}(\phi)$ est un sous groupe de $Aut(\mathbb{Z}_q)$ d'ordre p. Or, $Aut(\mathbb{Z}_q) \cong \mathbb{Z}_{q-1}$. Vérifions que $\mathbb{Z}_{q-1}$ admet un seul sous groupe d'ordre p. On pose $q - 1 = ap$. On se donne un sous groupe $K =< \overline{x} >$ de $\mathbb{Z}_{q-1}$ d'ordre p. Alors $q - 1$ divise px. Donc, a divise x. Ainsi, $\overline{x} \in < \overline{a} >$. Or, $< \overline{a} >$ est un sous groupe de $\mathbb{Z}_{q-1}$ d'ordre p. D'où, vu leur cardinal, on a $K =< \overline{a} >$. Donc, d'après la question (3) de l'exercice 13, il existe, à isomorphisme près, un seul groupe d'ordre pq de la forme $\mathbb{Z}_q \times_\phi \mathbb{Z}_p$.
4. D'après ce qui précède, il existe exactement deux types de groupes d'ordre $2q$, le premier est $\mathbb{Z}_{2q}$, et l'autre est non abélien. Or, on sait que D_q est non abélien d'ordre $2q$.

Exercice 16. Soit G un groupe d'ordre 8.

1. Vérifier que, si G est abélien, alors G est isomorphe à l'un des groupes : $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, $(\mathbb{Z}_2)^3$.
2. On suppose que G est non abélien.
   (a) Démontrer qu'il existe un élément a d'ordre 4.
   (b) On pose $N = (a)$. Prouver que $N \lhd G$ et en déduire que $b \in G - N$ implique $b^2 = e$ ou $b^2 = a^2$.
   (c) Démontrer que, dans le premier cas $G \cong D_4$ et dans le second cas $G \cong \mathbb{H}_8$.

Solution.

1. — Si G admet un élément d'ordre 8, alors G est cyclique et est isomorphe à $\mathbb{Z}_8$.
   — Supposons que tout élément de G est d'ordre 2. Soient $a, b \in G$ avec $a \neq b$. On pose $H =< a >< b >$ et on considère $c \in G - H$. Donc, $G = H < c > \cong H \times < c > \cong < a > \times < b > \times < c > \cong (\mathbb{Z}_2)^3$.

— Soit maintenant a un élément d'ordre 4 et posons $N =< a >$. Supposons que tout élément de $G - N$ est d'ordre 4. Soit $b \in G - N$. Alors, $ab \in G - N$. Donc, ab est d'ordre 4 et ainsi a^2b^2 est d'ordre 2. Or le seul élément de G d'ordre 2 est a^2.Donc, $a^2 = a^2b^2$, et par suite $b^2 = e$, ce qu'est absurde. Donc, $G - N$ contient un élément d'ordre 2 qu'on va noter b. Comme $< a > \cap < b >= \{e\}$, on en déduit que $G =< a > \times < b > \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

2. On suppose que G est non abélien.

   (a) Si G contient un élément d'ordre 8, alors G est abélien. De même si tout élément est d'ordre 2, alors G est abélien. Donc, il existe au moins un élément a d'ordre 4.

   (b) On a $[G : N] = 2$, et donc $N \lhd G$. Soit $b \in G - N$. Alors, bN est un générateur de G/N. Or, ce dernier est d'ordre 2, et ainsi $b^2N = N$. Donc, $b^2 \in N$. Cela implique que $b^2 = e$ ou $b^2 = a^2$. En effet, $b^2 \neq a$ et $b^2 \neq a^{-1}$. Sinon, $a^2 = e$.

   (c) On a $bab^{-1} \in N$. Donc, comme bab^{-1} a le même ordre que a (i.e., d'ordre 4), on a deux possibilités. Soit que $bab^{-1} = a$ ou $bab^{-1} = a^{-1}$. Le premier cas st impossible car $G =< a, b >$ et G non abélien. Donc, on a $bab^{-1} = a^{-1}$.
   — Si $b^2 = e$, alors $G \cong D_4$.
   — Si $b^2 = a^2$, alors $G \cong \mathbb{H}_8$.

Exercice 17. Soit A_n le groupe alterné de degré n.

1. Montrer A_n est distingué dans S_n d'indice 2.
2. Montrer que le produit de deux transpositions est un 3-cycle ou le produit de deux 3-cycles. En déduire que A_n est enegendré par les 3-cycles de S_n.
3. Montrer que les trois cycles sont des carrés. En déduire que A_n est engendré par les carrés des éléments de S_n.
4. Montrer que A_n est le seul sous groupe de S_n d'ordre $n!/2$.
5. Montrer que A_n ne contient aucun sous groupe d'indice 2.

Solution.

1. On sait que l'application signature $\varepsilon : S_n \to \{-1, 1\}$ est un morphise surjectif avec $A_n = \ker(\varepsilon)$. Donc, A_n est distingué. En plus, $\{-1, 1\} \cong S_n/A_n$. Donc, $n! = |S_n| = 2|A_n|$.
2. Soit (i, j) et (k, l) deux transpositions. Si $j = k$, alors $(i, j)(j, l) = (i, j, l)$ et si $j \neq k$ alors,
$$(i, j)(k, l) = (i, j)(j, k)(j, k)(k, l) = (i, j, k)(j, k, l).$$

Soit $\sigma \in A_n$. Alors, σ est le produit d'un nombre pair de permutation. Chaque produit de deux permutations successives, on le remplace par un cycle ou le produit de deux cycles. Inversement A_n contient tous les 3-cycles. Par suite, A_n est engendré par les 3-cycles de S_n.

3. Soit σ un 3-cycle. Donc, $(\sigma^2)^2 = \sigma^4 = \sigma$. Donc, les trois cycles sont des carrés. Ainsi, A_n est inclus dans le sous groupe engendré par les carrés. Inversement, un carré dans S_n est toujours pair. Donc, A_n est engendré par les carrés des éléments de S_n.
4. Soit H un sous groupe de S_n d'ordre $n!/2$. Donc, H est d'indice 2, et donc distingué. Alors, pour tout $\sigma \in S_n$, $\sigma^2 \in H$. Donc, $A_n \subseteq H$, d'où l'égalité.
5. Soit H un sous groupe de A_n d'indice 2. Alors, pour tout $\sigma \in A_n$, $\sigma^2 \in H$. Or, les 3-cycle sont des carrés, et donc $H = A_n$, ce qu'est absurde.

Exercice 18. 1. Montrer que le groupe

$$\mathcal{T} = \left\langle a, b \mid a^6 = e,\ a^3 = b^2,\ ba = a^{-1}b \right\rangle$$

admet douze éléments.

2. Montrer que $\mathcal{T}$ est isomorphe au groupe engendré par les matrices complexes

$$A = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \omega = e^{i\pi/3}.$$

3. Montrer qu'il existe un seul produit semi-direct non abélien de la forme $\mathbb{Z}_3 \times_\phi \mathbb{Z}_4$, et que celui la est isomorphe à $\mathcal{T}$.
4. Vérifier que $\mathcal{T}$ n'est isomorphe ni à D_6 ni à A_4.

Solution.

1. Le groupe $\mathcal{T}$ est non abélien, sinon $ab = ba = a^{-1}b$ et donc $a^2 = e$ (ce qu'est absurde).
   Par hypothèse $\mathcal{T} =< a, b >$, par suite tout élément de $\mathcal{T}$ est un produit de puissances entières de a et de b. Le groupe $\mathcal{T}$ peut donc être considéré comme engendré par $< a > \cup < b >$. Par hypothèse aussi,

$$< a >= \{a^0 = e, a, a^2, a^3, a^4, a^5\} \text{ et } < b >= \{b^0 = e, b, b^2, b^3\}.$$

   — Pour tout $0 \leq k \leq 5$, les éléments $a^k b$ sont deux à deux distincts et $b \notin < a >$ implique qu'aucun d'eux n'appartient à $< a >$.

— De plus, pour tout $0 \leq k \leq 5$,

$$ba^k = a^{-1}ba^{k-1} = \cdots = a^{-k}b, \quad b^2a^k = a^{k+3}, \quad b^3a^k = ba^{k+3} = a^{-k-3}.$$

On en déduit que $< a >< b >=< b >< a >$ est un sous-groupe de $\mathcal{T}$ et c'est alors le sous-groupe de $\mathcal{T}$ engendré par $< a > \cup < b >$, par suite $\mathcal{T} =< a >< b >$. D'où

$$|\mathcal{T}| = | < a > || < b > |/| < a > \cap < b > | = 12$$

et

$$\mathcal{T} = \{e, a, a^2, a^3, a^4, a^5, b, ab, a^2b, a^3b, a^4b, a^5b\}.$$

2. On a $A^3 = B^2 = -I_2$ et

$$A^{-1}B = -A^2B = \begin{pmatrix} 0 & -\omega^2 \\ \omega^{-2} & 0 \end{pmatrix} = \begin{pmatrix} 0 & \omega^{-1} \\ -\omega & 0 \end{pmatrix} = BA.$$

Par suite un morphisme φ tel $\varphi(a) = A$ et $\varphi(b) = B$ est nécessairement un isomorphisme de $\mathcal{T}$ sur le groupe $G =< A, B >$.

3. Soit $\phi : \mathbb{Z}_4 \to \mathrm{Aut}(\mathbb{Z}_3) = \{\mathrm{Id}_{\mathbb{Z}_3}, -\mathrm{Id}_{\mathbb{Z}_3}\}$. Alors, $\phi(1) = \mathrm{Id}_{\mathbb{Z}_3}$ ou $\phi(1) = -\mathrm{Id}_{\mathbb{Z}_3}$. Dans le premier cas, ϕ est trivial, et donc $\mathbb{Z}_3 \times_\phi \mathbb{Z}_4 = \mathbb{Z}_3 \times \mathbb{Z}_4$ (qu'est abélien). Donc, le cas non abélien provient de $\phi(1) = -\mathrm{Id}_{\mathbb{Z}_3}$. On considère dans $\mathbb{Z}_3 \times_\phi \mathbb{Z}_4$, les éléments $a = (\bar{1}, \hat{2})$ et $b = (\bar{0}, \hat{1})$. On a pour tout $1 \leq k \leq 3$,

$$(\bar{0}, \hat{k}) = b^k, \quad (\bar{1}, \hat{k}) = ab^{i-2}, \quad (\bar{2}, \hat{k}) = a^2b^k.$$

Ainsi, $\mathbb{Z}_3 \times_\phi \mathbb{Z}_4 =< a, b >$. En plus, l'ordre de a est 6, $a^3 = b^2$ et $ba = a^{-1}b$. Donc, d'après (1) et (2), $\mathcal{T} \cong \mathbb{Z}_n \times_\phi \mathbb{Z}_2$.

4. Le groupe $\mathcal{T}$ admet un élément d'ordre 6, alors que A_4 ne l'admet pas. Donc, $\mathcal{T} \ncong A_4$. Ensuite, le groupe

$$D_6 = \left\langle a, b \mid a^6 = b^2 = e,\ ba = a^{-1}b \right\rangle$$

admet au moins deux éléments d'ordre 2. Par contre $\mathcal{T}$ n'admet qu'un seul élément d'ordre 2. Donc, $\mathbb{T} \ncong D_6$.

Exercice 19. Soit G un groupe d'ordre 12.

1. Montrer que si G est abélien alors G est isomorphe à $\mathbb{Z}_{12}$ ou à $\mathbb{Z}_3 \times (\mathbb{Z}_2)^2$.
2. On suppose que G n'est pas abélien et soit $H = (a)$ un 3-sous groupe de Sylow de G.
   (a) Montrer que le morphisme de l'action de G sur $\left(\frac{G}{H}\right)_g$ est injective si et seulement si H n'est pas distingué dans G.

(b) Déduire que si H n'est pas distingué dans G alors $G \cong A_4$.

3. On suppose que H est distingué.

(a) Montrer que $[G : C_G(a)] \leq 2$, en déduire que G admet un élément d'ordre 6.

(b) Déduire que $G \cong D_6$ ou $G \cong \mathcal{T}$.

Solution.

1. Soient S_2 le seul 2-Sylow et S_3 le seul 3-Sylow. On a, $G \cong S_2 \times S_3$. En plus, $S_3 \cong \mathbb{Z}_3$. Or, $S_2 \cong \mathbb{Z}_4$ ou $S_2 \cong (\mathbb{Z}_2)^2$. Donc, G est isomorphe à $\mathbb{Z}_{12}$ ou à $\mathbb{Z}_3 \times (\mathbb{Z}_2)^2$.

2. (a) Notons N le noyau de l'action de G sur $\left(\frac{G}{H}\right)_g$. On a $N = \bigcap_{x \in G} xHx^{-1}$. Si $H \trianglelefteq G$, alors $N = H \neq \{e\}$. Donc, le morphisme de l'action n'est pas injectif. Si maintenant H n'est pas distingué dans G, alors il existe $x \in G$ tel que $H' = xHx^{-1} \neq H$. Or, $|H| = |H'| = 3$ implique que $H' \cap H = \{e\}$. Donc, $N = \{e\}$. D'où le morphisme de l'action est injectif.

(b) Si H n'est pas distingué dans G alors G est isomorphe à un sous groupe de S_4 d'ordre 12 (et donc distingué). Ce sous groupe ne peut être que A_4.

3. On suppose que H est distingué.

(a) On considère l'action par conjugaison de G sur lui même. On a $G_a = C_G(a)$. Donc, $[G : C_G(a)] = |\Omega_a| = |\{gag^{-1} \mid g \in G\}|$. Or tous les éléments de Ω_a sont d'ordre 3, et G ne contient que deux éléments d'ordre 3 (a et a^2). Donc, $[G : C_G(a)] \leq 2$. Par suite, $|C_G(a)| = 6$ ou 12. Dans le deux cas, $C_G(a)$ contient un élément d'ordre 2 qu'on note b. Il est clair que $x = ab$ est d'ordre 6.

(b) On pose $K = (x)$. L'indice de K est 2, et donc K est distingué dans G. Soit $y \in G - K$. On a $G =< x, y >$ et $y^2 \in K$. On sait aussi que yxy^{-1} est un élément de K d'ordre 6. Ainsi, c'est ou bien x ou x^{-1}. Le premier cas est exclu, sinon G est abélien. On pose $y^2 = x^i$ avec $i \in \{0, 1, 2, 3, 4, 5\}$. Donc, $x^i = yx^iy^{-1} = x^{-i}$, ce qui implique que 6 divise $2i$. Donc, $i = 0$ ou $i = 3$. Dans le premier cas $G \cong D_6$, et dans le second cas $G \cong \mathcal{T}$.

Le tableau suivant présente, à isomorphisme près, les groupes ayant moins de 15 éléments.

$\|G\|$	Nombre de groupes	cas abélien	cas non abélien
2	1	$\mathbb{Z}_2$	
3	1	$\mathbb{Z}_3$	
4	2	$\mathbb{Z}_4$ $\mathbb{Z}_2 \times \mathbb{Z}_2$	
5	1	$\mathbb{Z}_5$	
6	2	$\mathbb{Z}_6$	D_3
7	1	$\mathbb{Z}_7$	
8	5	$\mathbb{Z}_8$ $\mathbb{Z}_4 \times \mathbb{Z}_2$ $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	D_8 $\mathbb{H}_8$
9	2	$\mathbb{Z}_9$ $\mathbb{Z}_3 \times \mathbb{Z}_3$	
10	2	$\mathbb{Z}_{10}$	D_5
11	1	$\mathbb{Z}_{11}$	
12	5	$\mathbb{Z}_{12}$ $\mathbb{Z}_6 \times \mathbb{Z}_2$	A_4 D_6 $\mathcal{T}$
13	1	$\mathbb{Z}_{13}$	
14	2	$\mathbb{Z}_{14}$	D_7
15	1	$\mathbb{Z}_{15}$	

Chapitre 2

Anneaux euclidiens, principaux, factoriels

Dans tout le chapitre, les anneaux considérés sont commutatifs.

2.1 Anneaux euclidiens et principaux

On peut faire des divisions euclidiennes dans les anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$ où $\mathbb{K}$ est un corps. Ici, Nous allons généraliser cette situation.

Définition 2.22.1. Soient A un anneau et $a, b \in A$. On dit que a divise b, et on note a/b, s'il existe $c \in A$ tel que $b = ac$.

Définition 2.22.2 (Anneau euclidien)**.** Un anneau intègre A muni d'une application $\nu : A^* \to \mathbb{N}$, appelée stathme ou mesure, telle que :

1. pour tous $a, b \in A^*$, a/b implique $\nu(a) \leq \nu(b)$, et
2. pour tous $a, b \in A$ avec b non nul, il existe des éléments $q, r \in A$ tels que $a = bq+r$ avec $r = 0$ ou $\nu(r) < \nu(b)$,

est dit anneau euclidien.

***Exemples* 2.22.1.**

1. $\mathbb{Z}$ est un anneau euclidien pour le stathme $\nu : \mathbb{Z}^* \to \mathbb{N}$; $\nu(n) = |n|$.
2. $\mathbb{R}[X]$ est un anneau euclidien pour le stathme $\nu : \mathbb{R}[X]^* \to \mathbb{N}$; $\nu(P) = \deg(P)$.
3. $\mathbb{Z}\left[i\sqrt{2}\right]$ est un anneau euclidien pour le stathme $\nu : \mathbb{Z}\left[i\sqrt{2}\right]^* \to \mathbb{N}$; $\nu(z) = |z|^2$.
4. $\mathbb{Z}[i]$ est un anneau euclidien pour le stathme $\nu : \mathbb{Z}[i]^* \to \mathbb{N}$; $\nu(z) = |z|^2$.

Remarque 2.22.1. Dans la définition d'un anneau euclidien, on ne demande pas l'unicité de la division avec reste. En effet, même dans $\mathbb{Z}$, cette division n'est pas unique. Par exemple, si l'on prend $a = 8$ et $b = 3$, $8 = 3.2 + 2$ et $8 = 3.3 + (-1)$ sont deux divisions avec reste possibles.

Exercice 20. Soit A un anneau intègre qui n'est pas un corps muni d'une application $\varphi : A^* \to \mathbb{N}$ telle que, pour $a \in A$ et $b \in A^*$, il existe de manière unique un couple $(q, r) \in A^2$ tel que $a = bq + r$ avec $r = 0$ ou $\varphi(r) < \varphi(b)$.

L'objectif de cet exercice est de montrer qu'il existe un corps K tel que $A \cong K[X]$.

1. Montrer que :
   (a) si $a, b \in A^*$ et a/b alors $\varphi(a) \leq \varphi(b)$.
   (b) si $a, b \in A^*$ sont associés alors $\varphi(a) = \varphi(b)$.
2. On pose $m_0 = \varphi(1)$. Montrer que $m_0 = \min \varphi$ et que $U(A) = \{x \in A^* \mid \varphi(x) = m_0\}$.
3. On pose $K = U(A) \cup \{0\}$. Montrer que K est corps commutatif.
4. Soit $x_0 \in A$ tel que $\varphi(x_0) := m_1 = \min_{x \in A \setminus K} \varphi(x)$. On considère le morphisme d'anneaux défini par :
$$\begin{array}{rccc} \Psi : & K[X] & \longrightarrow & A \\ & P(X) & \longmapsto & P(x_0). \end{array}$$
   (a) Montrer (par récurrence sur le degré de P) que Ψ est injective.
   (b) Soient $u \in A \setminus K$ et $a \in K$. Montrer que $\varphi(1 + u) = \varphi(u)$, et en déduire que $\varphi(a + u) = \varphi(u)$.
   (c) Soit $x \in A^*$. Montrer que $\varphi(xx_0) > \varphi(x)$.
   (d) Montrer par récurrence que pour tout $n \in \mathbb{N}$ que si $x \in A^*$ et $\varphi(x) \leq n$ alors il existe $P \in K[X]$ tel que $x = P(x_0)$.
   (e) Conclure.

Solution.

1. (a) Suposons que $b = ac$ avec $c \in A$. Cette écriture est une division euclidienne de b par a. Donc, par unicité de la division euclidienne, l'écriture $b = a \times 0 + b$ n'est pas une division euclidienne, et donc $\varphi(b) \geq \varphi(a)$.
   (b) si $a, b \in A$ sont associés alors a/b et b/a, et donc $\varphi(a) = \varphi(b)$.
2. Pour tout $x \in A^*$, on a $1/x$, et donc $m_0 = \varphi(1) \leq \varphi(x)$. On a donc $m_0 = \min \varphi$. Puisque 1 est associé a tout $a \in U(A)$, on a $m_0 = \varphi(1) = \varphi(a)$. Ainsi, $U(A) \subseteq \{x \in A^* \mid \varphi(x) = m_0\}$. Inversemement, soit $x \in A^*$ tel que $\varphi(x) = m_0$. Soit $1 = xq + r$ la division eulidienne de 1 par x. Si $r \neq 0$ alors $\varphi(r) < \varphi(x) = m_0$, ce qu'est absure. Donc, $r = 0$ et $x \in U(A)$. On conclut que $U(A) = \{x \in A^* \mid \varphi(x) = m_0\}$.
3. On sait que $(K^*, \times) = (U(A), \times)$ est un groupe commutatif. Donc, il suffit de montrer que K est un sous anneau de A.
   — K^* et donc K sont stables par multiplications.
   — $1 \in K$, et si $a \in K$ alors $-a \in K$

— Soient $a, b \in K$. Montrons que $a + b \in K$. Si $a = 0$ ou $b = 0$ ou $a + b = 0$, le resultat est clair. On suppose donc que $a \neq 0$ et $b \neq 0$ et $a + b \neq 0$. Pour montrer que $a + b \in K$, il suffit de vérifier que $\varphi(a + b) = m_0$. Comme $a+b = a(1+a^{-1}b)$, les éléments $a+b$ et $1+a^{-1}b$ sont associés. Donc, il suffit de montrer que $\varphi(1+u) = m_0$ avec $m_0 = a^{-1}b \in K^*$. On a $1 = (1+u)\times 0+1$ et aussi $1 = (1+u)u^{-1} + (-u^{-1})$. Donc, si $\varphi(1+u) > m_0 = \varphi(1) = \varphi(-u^{-1})$, on obtient deux divisions euclidiennes différentes, ce qu'est asurde. Donc, $\varphi(1+u) = m_0$.

(a) Soit $P \in K[X]$. Montrons par récurrence sur $n = \deg(P)$ que $P(x_0) = 0$ implique $P = 0$.
— Si $P = 0$ ou $\deg(P) = 0$ alors $P = 0$.
— Supposons que la propriété est vrai pour $n \geq 1$. Soit $P = a_{n+1}X^{n+1} + \cdots + a_0$ un polynôme de degré $n+1$. L'hypothèse $P(x_0) = 0$ s'écrit comme suit

$$(\star) \quad 0 = P(x_0) = (a_{n+1}x_0^n + a_n x_0^{n-1} + \cdots + a_1)x_0 + a_0.$$

Si $a_0 \neq 0$ alors $\varphi(a_0) = m_0 < m_1 = \varphi(x_0)$, et donc $(\star)$ est une division euclidienne de 0 par x_0. Mais cela ne peut pas être vrai car $0 = x_0 \times 0 + 0$ est aussi une division eulcienne. Donc, nécéssairement $a_0 = 0$ et $a_{n+1}x_0^n + a_n x_0^{n-1} + \cdots + a_1 = 0$. On pose $Q(X) = a_{n+1}X^n + a_n X^{n-1} + \cdots + a_1$. On a $\deg(Q) = n$ et $Q(x_0) = 0$. Par suite, $Q = 0$. Enfin, on obtient $P = 0$.

On peut alors conclure que Ψ est injective.

(b) Soit $u \in A \setminus K$. Montrons que $\varphi(1 + u) = \varphi(u)$. On a $1 + u \neq 0$ sinon $u \in K$. En plus, $1 = (1 + u) \times 0 + 1$ est une division euclidienne de 1 par $1 + u$. En effet, $1 + u \notin K$, et donc $\varphi(1 + u) > \varphi(1) = m_0$. Ainsi, l'écritue $1 = (1 + u) \times 1 + (-u)$ n'est pas une division euclidienne (car $-u \neq 1$). Donc, $\varphi(u) = \varphi(-u) \geq \varphi(1+u)$. De même, pour $u' = -(1 + u) \notin K$, $\varphi(1 + u) = \varphi(-u') \geq \varphi(1 + u') = \varphi(-u) = \varphi(u)$. On en déduit que $\varphi(1 + u) = \varphi(u)$.
Si $a = 0$, le résultat est clair. Sinon,

$$\varphi(a + u) = \varphi(a(1 + a^{-1}u)) = \varphi(1 + a^{-1}u) = \varphi(a^{-1}u) = \varphi(u).$$

(c) Raisonnnons par l'absurde et supposons $\varphi(xx_0) \geq \varphi(x)$. Comme x division xx_0, on $\varphi(x) \leq \varphi(xx_0)$. Donc, $\varphi(xx_0) = \varphi(x)$. Divisons, x par x_0x, il existe $q, r \in A$ tels que $x = xx_0q + r$ et $r = 0$ ou $\varphi(r) < \varphi(xx_0) = \varphi(x)$. On remarque que x/r, et donc si $r \neq 0$, on a $\varphi(x) \geq \varphi(r)$, ce qu'est absurde. Donc, $r = 0$, et $1 = x_0q$, ce qu'est aussi impossible car $x_0 \notin K$. Donc, $\varphi(xx_0) > \varphi(x)$.

(d) C'est vrai pour $n = m_0$. En effet, si $\varphi(x) = m_0$ alors $x \in K$. Supposons que la propriété est vraie jusqu'à n. Soit $x \in A^*$ tel que $\varphi(x) \leq n+1$. On peut supposer que $\varphi(x) = n + 1$ et donc $x \notin K$. Soit $x = qx_0 + r$ la division euclidienne de

x par x_0. Donc, $r = 0$ or $\varphi(r) < \varphi(x_0) = m_1$. Donc, $r \in K$. D'après (4)(b) et (4)(c), on a $\varphi(q) < \varphi(qx_0) = \varphi(x - r) = \varphi(x)$. Donc, $\varphi(q) \leq n$. Ainsi, il existe $P \in K[X]$ tel que $q = P(x_0)$. On pose $Q = XP + r$. On a $Q \in K[X]$ et $Q(x_0) = x$. Donc, la propriété est vraie pour $n + 1$. D'où le résultat.

(e) La dérnière quesion veut dire que le morphisme Ψ est surjectif. Donc, c'est un isomorphisme d'anneaux. Par conséquent, $A \cong K[X]$.

Définition 2.22.3. Un anneau intègre est dit principal si tout idéal de A est principal ; c'est à dire que pour tout idéal I de A il existe $x \in A$ tel que $I = Ax = \{ax \mid a \in A\}$.

***Exemples* 2.22.2.**

1. Les idéaux de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$ avec n un entier positif ou nul, l'anneau $\mathbb{Z}$ est donc principal.
2. Les idéaux de l'anneau $\mathbb{Z}_4$ sont le $\{\overline{0}\}$, $2\mathbb{Z}_4$ et $\mathbb{Z}_4$. Donc, tout idéal de $\mathbb{Z}_4$ est principal. Cependant, l'anneau $\mathbb{Z}_4$ n'est pas intègre, et donc l'anneau n'est pas principal.
3. L'anneau $\mathbb{Z}[X]$ est intègre mais pas principal. Pour voir cela, on pose $I =< 2, X >= 2\mathbb{Z}[X] + X\mathbb{Z}[X]$. On suppose que $I =< P >$ avec $P \in \mathbb{Z}[X]$. Donc, $2 = PQ$ pour un certain $Q \in \mathbb{Z}[X]$. Cela implique que P et Q sont des polynômes constants dans $\mathbb{Z}[X]$, et $P = \pm 1$ ou $P = \pm 2$. De même, $X = PS$ avec $S \in \mathbb{Z}[X]$, ce qui implique que $S = \alpha X$ avec $\alpha \in \mathbb{Z}$. Donc, $1 = P\alpha$. Ainsi, P est inversible dans $\mathbb{Z}$. Alors, $P = \pm 1$. Donc, $1 \in I$, et cela entraîne l'existence de $T, R \in \mathbb{Z}[X]$ tels que $1 = 2T + XR$. Ainsi, $1 = 2T(0)$, ce qu'est impossible.

Théoreme 2.23

Tout anneau euclidien est principal.

Démonstration. Soit A un anneau euclidien pour le stathme ν, et soit $(0) \subsetneq I \subsetneq A$ un idéal de A. On considère l'ensemble $F = \{\nu(x) \mid x \in I\}$. L'ensemble $F \subseteq \mathbb{N}$ est non vide, et donc admet un plus petit élément a. Soit $x \in I$. Il existe $q, r \in A$ tels que $x = aq + r$ avec $r = 0$ ou $\nu(r) < \nu(a)$. En plus, $r = x - aq \in I$, et donc, si $r \neq 0$, on a $\nu(r) \geq \nu(a)$, ce qu'est impossible car $\nu(r) < \nu(a)$. Ainsi, $r = 0$, et par suite, $x \in Aa$. Par conséquent, $I \subseteq Aa \subseteq I$. D'où, I est principal. □

Remarque 2.23.1.

1. La réciproque du théorème précédent est fausse. En effet, l'anneau $\mathbb{Z}\left[\dfrac{1 + \sqrt{19}i}{2}\right]$ est principal mais pas euclidien.
2. A principal $\not\Longrightarrow A[X]$ principal et A euclidien $\not\Longrightarrow A[X]$ euclidien. Un simple contre-exemple est donné par l'anneau $\mathbb{Z}$ qu'est euclidien (et donc principal) mais $\mathbb{Z}[X]$ n'est pas principal (et donc n'est pas euclidien).

Lemme 2.24

Dans un anneau principal, tout idéal premier non nul est maximal

Démonstration. Soit A un anneau principal et $I = Ax$ un idéal premier. On suppose que $I \subseteq J = Ay$. Dans, $x = ay$ avec $a \in A$. Comme I est premier, on a $a \in I$ ou $y \in I$. Si $y \in I$, alors $J = Ay \subseteq I$. D'où, $I = J$. Si maintenant $a \in I$, alors $a = bx$ avec $b \in A$. Donc, $x = xby$, ce qui implique que $1 = by$ (car A est intègre), et donc y est inversible. Par suite $J = A$. D'où, I est maximal. □

Théoreme 2.25

Soit A un anneau. Alors,

$$A[X] \text{ euclidien } \Leftrightarrow A[X] \text{ principal } \Leftrightarrow A \text{ corps.}$$

Démonstration. Il suffit de montrer que si $A[X]$ est principal alors A est un corps. Les autres implications sont claires.

L'application

$$\begin{array}{rccc} f: & A[X] & \longrightarrow & A \\ & P & \longmapsto & P(0) \end{array}$$

est un morphisme d'anneaux surjectif, et $\ker(f) = \{P \in A[X] \mid P(0) = 0\} = XA[X]$. En utilisant le premier théorème d'isomorphisme, on obtient $A \cong A[X]/ < X >$. Comme $A[X]$ est principal, il est intègre. Donc, A l'est aussi. Ainsi, $< X >$ est premier dans $A[X]$ et donc maximal. Par conséquent, A est un corps. □

2.2 Divisibilité

Soient A un anneau et a, b deux éléments de A. Rappelons que a divise b, noté a/b, s'il existe $c \in A$ tel que $b = ac$. Les diviseurs de 1 sont les unités de l'anneau ; ce sont les éléments inversibles pour la multiplication. Ils forment un groupe noté $U(A)$.

Définition 2.25.1. Soient A un anneau et a, b deux éléments de A. On dit que a est associé à b, s'il existe une unité u de A tel que $a = ub$. Il est facile de voir qu'« être associé » est une relation d'équivalence sur A.

Définition 2.25.2. Soit A un anneau.

1. Un élément p de A est premier si $p \neq 0$ et $< p >$ est un idéal premier de A. De façon équivalente, p est premier si et seulement si $p \neq 0$, p n'est pas une unité et pour tous $a, b \in A$ si p/ab, alors p/a ou p/b.
2. Un élément q de A est irréductible si $q \neq 0$, q n'est pas une unité de A et si pour tous $a, b \in A$ tels que $q = ab$, on a $a \in U(A)$ ou $b \in U(A)$.

Remarque 2.25.1. Un élément associé à un élément premier (resp. irréductible) est aussi premier (resp. irréductible).

Proposition 2.26

Soient A un anneau intègre et q un élément de A. Alors, q est irréductible si et seulement si $< q >$ est un idéal maximal dans l'ensemble des idéaux principaux de A différent de A.

Démonstration. Supposons que q est irréductible. Soit $x \in A$ tel que $< q > \subseteq < x > \subsetneq A$. Montrons que $< q > = < x >$ (c'est à dire que x et q sont associés). Le fait que $< x > \subsetneq A$ veut dire que $x \notin U(A)$. Aussi, $q \in < x >$ et donc il existe $y \in A$ tel que $q = xy$. Comme q est irréductible, on déduit que $y \in U(A)$, et donc x et y sont associés.

Inversement, supposons que $< q >$ est un idéal maximal dans l'ensemble des idéaux principaux de A différent de A. Posons $q = xy$ avec $x, y \in A$ et $x \notin U(A)$. On a $< q > \subseteq < x > \subsetneq A$, et donc $< q > = < x >$. Par suite, q et x sont associés. Alors, il existe $u \in U(A)$ tel que $q = ux$. Comme A est intègre et $x \neq 0$, on déduit que $y = u$. □

Proposition 2.27

Soit A un anneau intègre. Tout élément premier de A est irréductible.

Démonstration. Soit p un élément premier de A. Alors, $p \neq 0$ et p n'est pas une unité. Soient $a, b \in A$ tels que $p = ab$. Donc, p/a ou p/b. Si par exemple p/a, alors $a = ps$ avec $s \in A$. Donc, $p = psb$. Par intègrité de A, on obtient $1 = sb$, et donc $b \in U(A)$. De même, si p/b on obtient $a \in U(A)$ Par suite, p est irréductible. □

La réciproque de cette proposition est vraie pour certains anneaux mais ce n'est pas toujours le cas.

***Exemple* 2.27.1.** Dans $A = \mathbb{Z}\left[\sqrt{5}i\right]$ l'élément 2 est irréductible mais pas premier.

Démonstration. — Montrons que 2 est irréductible. Supposons que $2 = z_1 z_2$ avec $z_1, z_2 \in A$. On a $4 = |z_1 z_2|^2 = |z_1|^2 |z_2|^2$. Or, $|z_1|^2, |z_2|^2 \in \mathbb{N}$. Donc, $|z_1|^2 = 1, 2 ou 4$. On pose $z_1 = a + b\sqrt{5}i$ avec $a, b \in \mathbb{Z}$. Donc, $|z_1|^2 = a^2 + 5b^2$. Si $|z_1|^2 = 1$ alors $z = \pm 1$, et donc $z_1 \in U(A)$. De même, si $|z_1|^2 = 4$ alors $|z_2|^2 = 1$ et donc $z_2 \in U(A)$. Le dérnier cas $|z_1|^2 = a^2 + 5b^2 = 2$ est impossible.

— Montrons que 2 n'est pas premier. On a $6 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$. Si 2 était un élément premier, il diviserait $1 + \sqrt{5}i$ ou $1 - \sqrt{5}i$. Considérons par exemple le premier cas. Il existe un élément z de A tel que $1 + \sqrt{5}i = 2z$. Donc, $6 = |1 + \sqrt{5}i|^2 = 4|z|^2$, ce qui est impossible.

□

Proposition 2.28

Soient A un anneau principal. Alors, tout élément irréductible de A est premier.

Démonstration. Soit q un élément irréductible de A. On sait que $< q >$ est un idéal maximal dans l'ensemble des idéaux principaux de A (différent de A). Mais comme A est principal, tout idéal est principal, et donc $< q >$ est un idéal maximal. Par suite, $< q >$ est un idéal premier, et donc q est premier. □

Exercice 21. On définit la norme de $z = x + yi \in \mathbb{C}$ par $N(z) = z\bar{z} = x^2 + y^2$.

1. Soit p un nombre premier. Montrer que les assertions suivantes sont équivalentes :
   (a) p est irréductible dans $\mathbb{Z}[i]$.
   (b) $p \equiv 3\,[4]$.
   (c) il n'existe pas $a \in \mathbb{Z}[i]$ tel que $p = N(a)$.
   On admettra que —1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si p n'est pas congru à 3 modulo 4.
2. En déduire tous les irréductibles de $\mathbb{Z}[i]$.
3. Parmi les éléments $1 + i, 2 + i, 2, 3, 5 \in \mathbb{Z}[i]$ lesquels sont irréductibles dans $\mathbb{Z}[i]$?

Solution.

1. $(a) \Rightarrow (b)$. Si $p \not\equiv 3\,[4]$, alors -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ et il existe $x \in \mathbb{Z}$ tel que $-1 = x^2\,[p]$. On obtient alors que p divise $x^2 + 1 = (x + i)(x - i)$ dans $\mathbb{Z}[i]$. Puisque p est irréductible, il est donc un élément premier car $\mathbb{Z}[i]$ est euclidien. Donc, p divise $x + i$ ou $x - i$. Dans le premier cas $x + i = p(a + ib)$ pour $a, b \in \mathbb{Z}$. Ainsi, $1 = pa = pb$ ce qu'est absurde. Donc, p ne divise pas $x + i$. De même p ne divise pas $x - i$, ce qu'est absurde. Par conséquent, $p \equiv 3\,[4]$.

$(b) \Rightarrow (c)$. Si $p = N(x)$. Alors $p = u^2 + v^2$, où u et v sont deux entiers tels que $x = u + iv$. Mais un carré étant toujours congru à 0 ou 1 (mod 4). Donc, p est congru à 0,1 ou 2 (mod 4), ce qui contredit (b). Par conséquent, il n'existe aucun $x \in \mathbb{Z}[i]$ tel que $p = N(x)$.
$(c) \Rightarrow (a)$. Soit a et b dans $\mathbb{Z}[i]$ tels que $p = ab$. On a $p^2 = N(p) = N(a)N(b)$. Si ni a ni b est inversibles, alors $N(a)$ et $N(b)$ sont différents de 1. On obtient, puisque p est premier, $N(a) = N(b) = p$, ce qui contredit l'hypothèse. On conclut que a ou b est inversible, et donc p est irréductible.

2. Les irréductibles de $\mathbb{Z}[i]$:
   D'après la question précédente, les entiers premiers congrus à 3 modulo 4 sont irréductibles dans $\mathbb{Z}[i]$. On montre aussi facilement que les éléments a de $\mathbb{Z}[i]$ tels que $N(a)$ soit premier sont irréductibles.
   On sait aussi que $U\Big(\mathbb{Z}[i]\Big) = \{\pm 1, \pm i\}$. Donc, si p est un entier premier congrus à 3 modulo 4 alors $\pm p$ et $\pm ip$ sont irréductibles (car ils sont associés à un élément irréductible) et si a de $\mathbb{Z}[i]$ tel que $N(a)$ soit premier alors $\pm a$ et $\pm ia$ sont irréductibles (car ils sont associés à un élément irréductible).

   Montrons que ce sont les seuls éléments irréductibles de $\mathbb{Z}[i]$.
   Soit x un élément irréductible de $\mathbb{Z}[i]$. On remarque que x divise $N(x) = x\overline{x} > 1$. L'entier $N(x)$ est un produit d'entiers premiers. Puisque x est irréductible (et donc premier car $\mathbb{Z}[i]$ est principal), il divise (dans $\mathbb{Z}[i]$) un de ces entiers premiers, appelons le p. Il existe $y \in \mathbb{Z}[i]$ tel que $p = xy$ et donc $p^2 = N(x)N(y)$. Si y est inversible, x est associé à p et nécessairement p est congru à 3 modulo 4, d'après la question 5. Sinon, on a, puisque $N(x) > 1$, $N(x) = p$ et x est un irréductible.

3. Parmi les éléments $1 + i, 2 + i, 2, 3, 5 \in \mathbb{Z}[i]$ lesquels sont irréductibles dans $\mathbb{Z}[i]$?
   — On a $N(1 + i) = 2$ et $N(2 + i) = 5$ sont premiers. Donc, $1 + i$ et $2 + i$ sont irréductibles.
   — On a $2 \equiv 2\,[4]$, $3 \equiv 3\,[4]$ et $5 \equiv 1\,[4]$. Donc, 3 est irréductible dans $\mathbb{Z}[i]$ mais ni 2 ni 5 est irréductible dans $Z[i]$.

Définition 2.28.1. Soit A un anneau intègre. Deux éléments a et b de A sont dits premiers entre eux si les seuls diviseurs en commun sont les unités de A.

Proposition 2.29

Soit A un anneau intègre. Alors, tout élément irréductible est premier avec tout élément qu'il ne divise pas.

Démonstration. Soit q un élément irréductible de A et soit $a \in A$ tel que q ne divise pas a. Soit aussi d un diviseur en commun de q et x. Donc, $d \in U(A)$ ou d est associé à q. Dans

le second cas, $x \in < d >=< q >$, et donc q divise x, ce qu'est absurde. Donc, $d \in U(A)$, et q et x sont premiers entre eux. □

Définition 2.29.1. Soient A un anneau intègre et a et b deux éléments de A. On dit que a et b admettent un plus grand commun diviseur (pgcd) si :

1. il existe $d \in A$ tel que d divise a et b, et
2. si $d' \in A$ divise a et b alors d' divise d.

Remarque 2.29.1. Soient A un anneau intègre et a et b deux éléments de A.

1. Si a divise b alors a est un pgcd de a et b.
2. Il existe des anneaux dans lesquels le pgcd de deux éléments n'existe pas toujours. Notamment, dans l'anneau $A = \mathbb{Z}\left[\sqrt{5}i\right]$ les éléments $z_1 = 2(1 + \sqrt{5}i)$ et $z_2 = 6 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$ n'ont pas de pgcd. En effet, supposons que d soit un pgcd de ces deux éléments. Comme d divise z_1 et z_2, sa norme $|d|^2$ divise $|z_1|^2 = 24$ et $|z_2|^2 = 36$. D'autre part comme 2 et $(1 + \sqrt{5}i)$ sont des diviseurs communs, $|d|^2$ est divisible par 4 et 6. On en déduit facilement que $|d|^2 = 12$. Ceci est impossible car l'équation $a^2 + 5b^2 = 12$ n'a pas de solution dans $\mathbb{Z}$.

Proposition 2.30

Soient A un anneau intègre et a et b deux éléments de A admettant un pgcd d. Alors, $d' \in A$ est un pgcd de a et b si et seulement si d' est associé à d.

Démonstration. ($\Rightarrow$) Par définition de pgcd, d divise d' et d' divise d. Donc, d et d' sont associés.

($\Leftarrow$) On pose $d' = ud$ avec $u \in U(A)$. On a $d \in A$ tel que d divise a et b, et donc d' divise a et b. Soit d" $\in A$ tel que d" divise a et b. Donc, d" divise d, et par suite d" divise d'. Par conséquent, d' est un pgcd de a et b. □

Exercice 22. On considère l'anneau $\mathbb{Z}[i\sqrt{2}] = \left\{a + bi\sqrt{2} \mid a, b \in \mathbb{Z}\right\}$ sur lequel on définit l'application norme N donnée par $N(a + bi\sqrt{2}) = |a + bi\sqrt{2}|^2 = a^2 + 2b^2 \in \mathbb{N}$.

1. Vérifier que N est multiplicative (c-à-d, $N(xy) = N(x)N(y)$ pour tous $x, y \in Z[i\sqrt{2}]$)
2. Déterminer les éléments inversibles de $\mathbb{Z}[i\sqrt{2}]$.
3. Soit $z \in \mathbb{Z}[i\sqrt{2}]$. Montrer que si $N(z)$ est un nombre premier alors x est irréductible dans $\mathbb{Z}[i\sqrt{2}]$.
4. Soient $x, y \in \mathbb{Z}[i\sqrt{2}]$ avec $y \neq 0$.
   (a) Montrer qu'il existe $q \in \mathbb{Z}[i\sqrt{2}]$ tel que $\left|q - \frac{x}{y}\right| < 1$.
   (b) On pose $r = x - qy$. Vérifier que $|r| < |y|$.

(c) Conclure que l'anneau $\mathbb{Z}[i\sqrt{2}]$ est Euclidien.

5. Donner tous les diviseurs de $2 + i\sqrt{2}$ dans $\mathbb{Z}[i\sqrt{2}]$.
6. Donner la liste des diviseurs communs de $2 + i\sqrt{2}$ et 3 dans $\mathbb{Z}[i\sqrt{2}]$.
7. Donner tous les pgcd de $2 + i\sqrt{2}$ et 3 dans $\mathbb{Z}[i\sqrt{2}]$

Solution.

1. Vérifions que N est multiplicative : Soient $z, z' \in \mathbb{Z}[i\sqrt{2}]$. On a

$$N(zz') = |zz'|^2 = |z|^2|z'|^2 = N(z)N(z').$$

Donc, N est multiplicative.

2. Les éléments inversibles de $\mathbb{Z}[i\sqrt{2}]$: Soit $z \in U\big(\mathbb{Z}[i\sqrt{2}]\big)$. Il existe $z' \in \mathbb{Z}[i\sqrt{2}]$ tel que $zz' = 1$. Donc, $N(z)N(z') = 1$. Comme $N(z), N(z') \in \mathbb{N}$, on a nécessairement $N(z) = 1$. Ainsi, $a^2 + 2b^2 = 1$. Par suite, $a = \pm 1$ et $b = 0$.Donc, $z = \pm 1$. Inversement, 1 et -1 sont inversibles. Par conséquent,

$$U(\mathbb{Z}[i\sqrt{2}]) = \{\pm 1\}.$$

3. Soit $z \in \mathbb{Z}[i\sqrt{2}]$. Montrer que si $N(z)$ est un nombre premier alors z est irréductible dans $\mathbb{Z}[i\sqrt{2}]$:
Soit $z \in \mathbb{Z}[i\sqrt{2}]$ tel que $N(z) = p$ soit un entier premier.
— $z \neq 0$ (sinon $N(z) = 0$).
— $z \notin U(\mathbb{Z}[i\sqrt{2}])$ car $N(z) \neq 1$.
— Soient $z_1, z_2 \in \mathbb{Z}[i\sqrt{2}]$ tels que $z = z_1 z_2$. Donc, $p = N(z) = N(z_1)N(z_2)$. Comme p est premier, on a nécessairement $N(z_1) = 1$ ou $N(z_2) = 1$. Donc, $z_1 = \pm 1$ ou $z_2 = \pm$. Alors, z_1 est inversible ou z_2 est inversible.
On en déduit donc que z est irréductible.

4. Soient $x, y \in \mathbb{Z}[i\sqrt{2}]$ avec $y \neq 0$.
(a) Montrer qu'il existe $q \in \mathbb{Z}[i\sqrt{2}]$ tel que $\left|q - \frac{x}{y}\right| < 1$:
On pose $\frac{x}{y} = \alpha + i\sqrt{2}\beta$ avec $\alpha, \beta \in \mathbb{R}$. Soient u et v les entiers les plus proches de α et β respectivement. On a

$$|u - \alpha| \leq 1/2 \text{ et } |v - \beta| \leq 1/2.$$

Alors, pour $q = u + iv\sqrt{2} \in \mathbb{Z}[i\sqrt{2}]$, on a

$$\left|q - \frac{x}{y}\right|^2 = \left|(u - \alpha) + (v - \beta)i\sqrt{2}\right|^2 = (u-\alpha)^2 + 2(v-\beta)^2 \leq 1/4 + 2.1/4 = 3/4 < 1.$$

Donc,

$$\left|q - \frac{x}{y}\right| < 1.$$

(b) On pose $r = x - qy$. Vérifions que $|r| < |y|$:
On a

$$|r| = |x - qy| = |y|\left|\frac{x}{y} - q\right| < |y|.$$

(c) Montrons que l'anneau $\mathbb{Z}[i\sqrt{2}]$ est Euclidien :
— L'anneau $\mathbb{Z}[i\sqrt{2}]$ est intègre (car c'est un sous anneau du corps $\mathbb{C}$).
— On considère l'application $N : \mathbb{Z}[i\sqrt{2}]^* \to \mathbb{N}$ définie par $N(a + ib\sqrt{2}) = |a + ib|^2 = a^2 + 2b^2$ avec $a, b \in \mathbb{Z}$.
— Soient $x, y \in \mathbb{Z}[i]^*$ tels que y divise x. Donc, il existe $z \in \mathbb{Z}[i]^*$ tel que $x = yz$. Comme $z \neq 0$ on a $N(z) \geq 1$. Donc, $N(x) = N(yz) = N(y)N(z) \geq N(y)$.
— Soient $x, y \in \mathbb{Z}[i]$ avec $y \neq 0$. D'après ce qui précède, il existe $q, r \in \mathbb{Z}[i\sqrt{2}]$ tel que $x = qy + r$ avec $r = 0$ ou $N(r) < N(y)$.
Ceci montre que $\mathbb{Z}[i\sqrt{2}]$ est euclidien.

5. Les diviseurs de $2 + i\sqrt{2}$ dans $\mathbb{Z}[i\sqrt{2}]$:
Soit $x = a + ib\sqrt{2} \in \mathbb{Z}[i\sqrt{2}]$ un diviseur de $2 + i\sqrt{2}$ dans $\mathbb{Z}[i\sqrt{2}]$. Il existe $y \in \mathbb{Z}[i\sqrt{2}]$ tel que $2 + i\sqrt{2} = xy$. Donc, $6 = N(2 + i\sqrt{2}) = N(x)N(y)$. Ainsi, $N(x) \in \{1, 2, 3, 6\}$.
— Si $N(x) = 1$ alors $x = \pm 1$.
— Si $N(x) = 2$ alors $a^2 + 2b^2 = 2$. Donc, $a^2 = 0$ et $b^2 = 1$. Alors, $x = \pm\sqrt{2}i$. Inversement $\sqrt{2}i$ et $-\sqrt{2}i$ sont des diviseurs de $2 + i\sqrt{2}$. En effet,

$$2 + i\sqrt{2} = \sqrt{2}i(1 - \sqrt{2}i) = -\sqrt{2}i(-1 + \sqrt{2}i).$$

— Si $N(x) = 3$ alors $N(y) = 2$. Donc, $y = \pm\sqrt{2}i$. Par suite, $x = \pm(1 - \sqrt{2}i)$.
— Si $N(x) = 6$ alors $N(y) = 1$. Donc, $y = \pm 1$ et $x = \pm(2 + i\sqrt{2})$.
On conclut donc que les diviseurs de $2 + i\sqrt{2}$ sont exactement :

$$\pm 1, \quad \pm\sqrt{2}i, \quad \pm(1 - \sqrt{2}i), \quad \pm(2 + i\sqrt{2}).$$

6. La liste des diviseurs communs de $2 + i\sqrt{2}$ et 3 dans $\mathbb{Z}[i\sqrt{2}]$:
Soit $x = a + ib\sqrt{2} \in \mathbb{Z}[i\sqrt{2}]$ un diviseur de 3 dans $\mathbb{Z}[i\sqrt{2}]$. Il existe $y \in \mathbb{Z}[i\sqrt{2}]$ tel que $3 = xy$. Donc, $9 = N(3) = N(x)N(y)$. Ainsi, $N(x) \in \{1, 3, 9\}$.
Les seuls diviseur de $2 + i\sqrt{2}$ qui vérifient cette condition sont : ± 1 et $\pm(1 - \sqrt{2}i)$. Il est clair que ± 1 divisent 3.Aussi, $3 = (1 - \sqrt{2}i)(1 + \sqrt{2}i)$. Donc, $\pm(1 - \sqrt{2}i)$ divisent aussi 3. Par conséquent, les diviseurs communs de $2 + i\sqrt{2}$ et 3 dans $\mathbb{Z}[i\sqrt{2}]$ sont exactement : ± 1 et $\pm(1 - \sqrt{2}i)$.

7. Donner tous les pgcd de $2+i\sqrt{2}$ et 3 dans $\mathbb{Z}[i\sqrt{2}]$: D'après la question précédente, les pgcd de $2+i\sqrt{2}$ et 3 dans $\mathbb{Z}[i\sqrt{2}]$ sont $\pm(1-\sqrt{2}i)$.

2.3 Anneaux factoriels

Définition 2.30.1 (Décomposition unique en produit de facteurs irréductibles)**.** Soit A un anneau intègre. On dit qu'un élément non nul a de A admet une décomposition unique en produit de facteurs irréductibles si les deux conditions suivantes sont satisfaites.

1. Il existe une unité $u \in A$, un entier $r \geq 1$, des éléments irréductibles $p_1, \cdots, p_r$ de A, des entiers $k_1, ..., k_r \geq 1$ tels que
$$a = up_1^{k_1} \cdots p_r^{k_r}.$$
2. Si a admet une seconde décomposition du même type : $a = vq_1^{l_1} \cdots q_s^{l_s}$, alors $r = s$ et il existe une permutation σ des indices telle qu'on ait $p_{\sigma(i)}$ associé à q_i et $k_{\sigma(i)} = l_i$ pour $i = 1, ..., r$.

Il est souvent utile de normaliser la décomposition en facteurs irréductibles. Pour cela, on choisit une famille $(p_i)_{i\in I}$ d'éléments irréductibles de A telle que :

1. tout élément irréductible de A est associé à l'un des p_i,
2. si $i \neq j$, p_i et p_j ne sont pas associés.

Ce choix étant effectué, la définition précédente s'énonce : a s'écrit de manière unique sous la forme
$$a = u\prod_{i\in I} p_i^{r_i}.$$
où u est un élément inversible de A et où les r_i sont des entiers positifs, nuls sauf un nombre fini d'entre eux.

Définition 2.30.2 (Anneau factoriel)**.** Un anneau A est dit factoriel s'il est intègre et si tout élément non nul admet une décomposition unique en produit de facteurs irréductibles.

Dans un anneau factoriel, un élément $a = u\prod_{i\in I} p_i^{r_i}$ divise donc un élément $b = v\prod_{i\in I} p_i^{s_i}$ si et seulement si pour tout i on a $r_i \leq s_i$. En effet, si $c \in A$ tel que $b = ac$, on écrit $c = w\prod_{i\in I} p_i^{t_i}$ puis on observe que l'on a $v\prod_{i\in I} p_i^{s_i} = uw\prod_{i\in I} p_i^{r_i+t_i}$. D'où, par unicité, que $s_i = r_i + t_i$ pour tout i. Inversement, il suffit de prendre $c = u^{-1}v\prod_{i\in I} p_i^{s_i-r_i}$.

Lemme 2.31

Dans un anneau factoriel, tout élément irréductible est premier.

Démonstration. On va montrer que si a est irréductible et si a/bc alors a/b ou a/c. Pour simplifier on va supposer avoir normalisé la décomposition en facteurs irréductibles dans A. Comme a est irréductible, on a $a = up_j$ pour un $j \in I$. On pose aussi $b = v\prod_{i\in I} p_i^{s_i}$ et $c = w\prod_{i\in I} p_i^{t_i}$ les décompositions en facteurs irréductibles de b et c. Comme a divise bc, on sait que $s_j + t_j \geq 1$. Mais alors $s_j \geq 1$ ou $t_j \geq 1$. En particulier, a divise b ou c. □

Proposition 2.32

Soit A un anneau factoriel et $a = u\prod_{i\in I} p_i^{r_i}$ et $b = v\prod_{i\in I} p_i^{s_i}$ deux élément de A, alors $d = \prod_{i\in I} p_i^{\inf\{r_i,s_i\}}$ est un pgcd de a et b.

Démonstration. Il est clair que d divise a et b. Si $d' = w\prod_{i\in I} p_i^{t_i}$ divise a et b alors, $t_i \leq \inf\{r_i, s_i\}$, et donc d' divise d. □

Lemme 2.33

Dans un anneau principal, toute suite croissante d'idéaux est stationnaire.

Démonstration. Supposons par l'absurde qu'il existe une suite $(a_1) \subset (a_2) \subset \cdots$ une suite strictement croissante d'idéaux. On pose $J = \bigcup_{i\geq 1}(a_i)$. Montrons que J est un idéal. Il est clairement non vide. Si $x, y \in J$ alors il existe $i, j \geq 1$ tel que $x \in (a_i)$ et $y \in (a_j)$. Si par exemple $i \leq j$ alors $x \in (a_i) \subset (a_j)$ et donc $x - y \in (a_j) \subset J$. En plus, pour tout $a \in A$, $ax \in (a_i) \subset J$. Par suite, J est un idéal de A, et donc principal. On pose $J = (a)$. Alors, il existe $i \geq 1$ tel que $a \in (a_i)$, et donc pour tout $j \geq i$, $J \subset (a_i) \subset (a_j) \subset (a_j) \subset J$. Par conséquent, $(a_i) = (a_j)$ ce qu'est absurde. □

Lemme 2.34

Soit A un anneau principal et $a \in A$ non nul et non inversible. Alors il existe $n \geq 0$, des éléments irréductibles $p_1, \cdots, p_n$ de A et un inversible u de A tels que $a = up_1 \cdots p_n$.

Démonstration. Supposons par l'absurde qu'il existe un élément a non nul de A qui n'est pas produit d'éléments irréductibles. Soit $a_1 = a$. L'élément a n'est pas inversible (sinon $a = u$ avec u inversible serait une décomposition), ni irréductible (sinon $a = p$ avec p irréductible serait une décomposition). Soit $a = bc$ avec b et c non inversibles. Comme a n'est pas produit fini d'éléments irréductibles, b ou c n'est pas produit fini d'éléments irréductibles. Soit a_2 cet élément. L'idéal (a_2) contient donc strictement l'idéal (a_1). On construit ainsi, par récurrence, une suite $a_1, a_2, \cdots$ d'éléments de A tels que la suite d'idéaux $(a_1) \subset (a2) \subset \cdots$. soit strictement croissante, ce qu'est impossible. Tout élément non nul d'un anneau principal admet donc une décomposition en éléments irréductibles. □

Théoreme 2.35

Tout anneau principal est factoriel.

Démonstration. Soit $a \in A$ non nul. L'existence de la décomposition de a en éléments irréductibles est assurée par le lemme précédent. Donc, il suffit de prouver l'unicité. Supposons que $a = up_1^{k_1} \cdots p_r^{k_r} = vp_1^{l_1} \cdots p_r^{l_r}$ avec des k_i et l_i pas tous égaux. Effectuons toutes les simplifications possibles. S'il reste dans le membre de gauche un facteur p irréductible, il divise le produit de facteurs irréductibles de droite, et comme il est premier, il en divise l'un des termes qui est donc associé à p, contrairement aux simplifications effectuées. Il ne peut donc rester aucun facteur irréductible dans l'un des membres, ce qui montre l'unicité. □

2.4 Théorème de Gauss

L'objectif de cette section est de démontrer le théorème de Gauss suivant :

Théoreme 2.36

Si l'anneau A est factoriel alors l'anneau $A[X]$ est factoriel

Définition 2.36.1. Soit A un anneau factoriel et soit $P \in A[X]$. Le contenu de P, noté $c(P)$, est un pgcd des coefficients de P. On dira que P est primitif si $c(P)$ est inversible.

Proposition 2.37

Soit A un anneau factoriel et soient $P, Q \in A[X]$. Alors, $c(PQ) \sim c(P)c(Q)$.

Démonstration. Soient P et Q des polynômes primitifs. Supposons que PQ ne soit pas un polynôme primitif, autrement dit que $c(PQ)$ soit non inversible dans A. Soit $p \in A$ un facteur irréductible de $c(PQ)$. L'idéal $I = pA$ est un idéal premier et l'anneau A/I est intègre. Notons $\pi : A[X] \to (A/I)[X]$ l'homomorphisme de changement d'anneau induit par la projection canonique $A \to A/I$. Comme $\pi(PQ) = \pi(P)\pi(Q)$ est nul, $\pi(P)$ ou $\pi(Q)$ est nul, donc P ou Q est divisible par p. Le contenu de l'un des deux polynômes, divisible par p, n'est pas inversible, ce qui donne une contradiction et montre que PQ est un polynôme primitif.

Supposons maintenant que P et Q ne sont pas primitif, et posons $P = c(P)P'$ et $Q = c(Q)Q'$ avec P' et Q' sont primitifs. Donc, $c(PQ) = c(P)c(Q)c(P'Q') \sim c(P)c(Q)$. □

Proposition 2.38

Soit A un anneau factoriel et K son corps de fractions. Alors les éléments irréductibles de $A[X]$ sont exactement :

- les éléments irréductibles de A ;
- les polynômes primitifs de $A[X]$, irréductibles en tant que polynômes de $K[X]$.

Démonstration. Montrons d'abord que les éléments en question sont bien irréductibles. Soit donc $a \in A$ irréductible et supposons que $P, Q \in A[X]$ sont tels que $a = PQ$. Comme A est intègre, on a $\deg(P) + \deg(Q) = \deg(PQ) = 0$, donc P et Q sont nécessairement de degré 0, ou autrement dit des éléments de A. L'élément a étant irréductible dans A, la relation est banale dans A et donc aussi dans $A[X]$. L'élément a est donc bien irréductible dans l'anneau $A[X]$.

Soit maintenant $P \in A[X]$ primitif, irréductible dans $K[X]$ et supposons $P = QR$ avec Q et R dans $A[X]$. Vu dans $K[X]$ cette relation doit être banale ou autrement dit, Q ou R est inversible dans $K[X]$, c'est-à-dire constant. Supposons que cela soit Q. Nous avons $c(P) = c(Q)c(R) = Qc(R)$, puisque Q est constant. Comme P est primitif, $c(P) \sim 1$ et l'élément Q est nécessairement inversible dans A donc dans $A[X]$. Ainsi, P est irréductible dans $A[X]$.

Montrons maintenant que les éléments en question sont les seuls éléments irréductibles. Pour cela, soit P un élément irréductible de $A[X]$ et écrivons $P = c(P)P'$ avec P' primitif. Cette relation doit être banale, donc $c(P) \sim 1$ ou P' est inversible dans $A[X]$. On va montrer que dans le premier cas, P est irréductible dans $K[X]$ et que dans le second cas $c(P)$ est irréductible.

Dans le premier cas, P est primitif. Soit $P = QR$ une factorisation avec $Q, R \in K[X]$. On peut écrire $Q = qQ'$ et $R = rR'$, où q et r sont dans K et où Q' et R' sont deux polynômes primitifs de $A[X]$. En effet, on sort d'abord le dénominateur commun des

coefficients, puis on sort le contenu. On a ainsi $P = (qr)Q'R'$. La fraction qr s'écrit $\frac{a}{b}$ où $a, b \in A$. On obtient $bP = aQ'R'$ dans $A[X]$. Ces deux polynômes ont donc le même contenu, a et b respectivement. Par conséquent, $a \sim b$, d'où $qr = u \in U(A)$, ce qui donne la relation $P = uQ'R'$ dans $A[X]$. Comme P est irréductible dans $A[X]$, $Q' \in U(A)$ ou $Q' \in U(A)$. D'où, $Q \in K$ ou $R \in K$.

Dans le second cas, P' est constant, inversible dans A. On observe alors qu'une relation non banale $c(P) = ab$ dans A nous donnerait une relation non banale $P = a(bP')$ dans $A[X]$, ce qui contredit l'hypothèse que P est irréductible. □

Comme on voit dans la proposition ci-dessus, le corps de fraction K de l'anneau factoriel A joue un rôle important dans la description des éléments irréductibles de $A[X]$. Comme K est un corps, l'anneau $K[X]$ est principal et donc en particulier factoriel d'après le théorème. On va utiliser cette observation pour démontrer le théorème de Gauss.

Démonstration du théorème de Gauss. Notons K le corps de fraction de A. Il faut montrer que tout polynôme P de $A[X]$ admet une décomposition unique en produit de facteurs irréductibles. Nous allons montrer l'existence de la décomposition au (1) et (2), l'unicité au (4) à l'aide d'un lemme donné au (3).

1. Supposons P primitif. Comme $K[X]$ est euclidien, donc factoriel, il existe une décomposition de P en produit de facteurs irréductibles dans $K[X]$: $P = \prod_{i=1}^{r} P_i$. En réduisant les coefficients de chacun des P_i au même dénomidinateur, on peut écrire $Pi = \frac{a_i}{b_i} Q_i$, avec Q_i primitif et irréductible dans $A[X]$. On a $\left(\prod_{i=1}^{r} b_i\right) P = \prod_{i=1}^{r} a_i Q_i$, d'où, en simplifiant par les contenus des deux membres, $P = v \prod_{i=1}^{r} Q_i$ où v est une unité de A ; ceci montre l'existence d'une décomposition de P dans $A[X]$ en produit de facteurs irréductibles dans le cas où P primitif.
2. Si P n'est primitif, écrit $P = c(P)P_1$ et décompose $c(P)$ dans A et P_1 comme précédemment pour obtenir une décomposition de P.
3. Montrons qu'un élément irréductible F de $A[X]$ est premier dans $A[X]$. Si F est un élément irréductible p de A (et donc premier dans A), on a $\frac{A[X]}{pA[X]} \cong \frac{A}{pA}[X]$. Comme ce dernier anneau est intègre, p est premier dans $A[X]$. Si F n'est pas dans A, on a vu que $c(F) \sim 1$ et que F est irréductible dans $K[X]$. Si F divise dans $A[X]$ un produit GH de deux polynômes de $A[X]$, F divise GH dans $K[X]$; comme $K[X]$ est factoriel, F divise G, par exemple, et il existe un polynôme G' de $K[X]$ tel que $FG' = G$. Écrivons $G' = (a/b)G_1$ avec G_1 dans $A[X]$ primitif et $a, b \in A$ premiers entre eux. On a alors $bG = bFG' = aFG_1$. En prenant le contenu de chaque côté, on voit $bc(G) = a$ d'où $a/b = c(G) \in A$. On a donc $G' \in A[X]$, ce qui montre que F divise Q dans A[X].

4. 4) Supposons que P admet deux décompositions en produit de facteurs irréductibles dans $A[X]$: $P = u\prod_{i=1}^{r} P_i = u\prod_{j=1}^{s} T_j$. Après avoir simplifié par les facteurs associés des deux membres, s'il reste un facteur P_i, il est premier d'après (3), donc divise un des facteurs de droite T_j ; ces deux facteurs sont associés, contradiction et fin de la démonstration.

□