GROUPES ET ANNEAUX 2

Notations générales : sauf indication contraire, G sera toujours un *groupe*, A sera toujours un *anneau commutatif* (on utilisera le terme *anneau* à la place d'anneau commutatif), et $\Bbbk$ sera toujours un *corps* (qui sera typiquement choisi parmi $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ou $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ pour un nombre premier $p \in \mathbb{N}$).

1. Pré-requis

1.1. **Groupes.** Les notions suivantes doivent être connues.

◇ Sous-groupe. **Notation :** $H < G$ signifie "H est un sous-groupe de G", et $\langle g_1, \dots, g_n \rangle$ dénote le sous-groupe de G engendré par $g_1, \dots, g_n \in G$.

◇ Morphisme (ou homomorphisme) de groupes, isomorphisme, endomorphisme, automorphisme.

◇ Noyau $\ker f$ et image $\operatorname{im} f$ d'un momorphisme de groupes $f : G \to G'$.

◇ Ordre d'un élément. **Notation :** $\operatorname{ord}(g) \in \mathbb{N}$ dénote l'ordre de $g \in G$.

Les résultats suivants doivent être connus.

Proposition 1.1.1 (Propositions 3.3.8 & 3.3.9 de HAX501X)**.** *Si $f : G \to G'$ est un morphisme de groupes, alors* $\ker f$ *est un sous-groupe de G, et* $\operatorname{im} f$ *est un sous-groupe de G'. De plus, f est injectif si et seulement si* $\ker f = \{e\}$.

Proposition 1.1.2 (Propositions 3.4.5 & 3.4.7, Exercice 50 de HAX501X)**.** *Soit G un groupe et $g \in G$ un élément.*

(i) Si $\operatorname{ord}(g) = m$*, alors $\langle g \rangle$ est un sous-groupe d'ordre m isomorphe à $\mathbb{Z}/m\mathbb{Z}$.*

(ii) Si $g^n = e$, alors $\operatorname{ord}(g)$ *divise n.*

(iii) Si $\operatorname{ord}(g) = m$*, alors* $\operatorname{ord}(g^n) = \frac{m}{\operatorname{pgcd}(m,n)}$ *pour tout $n \in \mathbb{N}$.*

Théorème 1.1.3 (Théorème de Lagrange, Théorème 3.4.12 de HAX501X)**.** *Si G est un groupe fini et H est un sous-groupe de G, alors $|H|$ divise $|G|$.*

1.2. **Anneaux.** Les notions suivantes doivent être connues.

◇ Anneau intègre.

◇ Sous-anneau, idéal. **Notation :** $(a_1, \dots, a_n)$ dénote l'idéal de A engendré par $a_1, \dots, a_n \in A$.

◇ Éléments inversibles, irréductibles. **Notation :** $A^\times$ est le groupe multiplicatif des éléments inversibles de A.

◇ Morphisme (ou homomorphisme) d'anneaux, isomorphisme, endomorphisme, automorphisme.

Les résultats suivants doivent être connus.

Proposition 1.2.1 (Proposition 4.1.16 de HAX501X)**.** *Tout corps est intègre.*

Proposition 1.2.2 (Proposition 4.5.6 de HAX501X)**.** *Si A est un anneau intègre, alors $(A[X])^\times = A^\times$.*

Proposition 1.2.3 (Proposition 4.8.6 de HAX501X)**.** *Si $f : A \to A'$ est un morphisme d'anneaux, alors* $\ker f$ *est un idéal de A, et* $\operatorname{im} f$ *est un sous-anneau de A'.*

2. Groupes

2.1. **Exemples de groupes.** On rappelle d'abord des exemples importantes de groupes.

Exemple 2.1.1. (*i*) Muni de la multiplication usuelle entre nombres complexes, $\mathbb{C}^\times$ est un groupe. Le sous-groupe

$$\boldsymbol{\mu}_n := \{z \in \mathbb{C}^\times \mid z^n = 1\}$$

est le *groupe des racines n-èmes de l'unité*. Il est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ via l'isomorphisme

$$\begin{aligned} f : \mathbb{Z}/n\mathbb{Z} &\to \boldsymbol{\mu}_n \\ [k] &\mapsto e^{\frac{2k\pi\mathrm{i}}{n}}. \end{aligned}$$

(*ii*) Soit $\mathrm{GL}_n(\Bbbk)$ le *groupe général linéaire de dégré n de* $\Bbbk$, qui est par définition le groupe des matrices inversibles de taille $n \times n$ à coefficients dans $\Bbbk$. Si $\Bbbk = \mathbb{F}_p$, alors $\mathrm{GL}_n(\Bbbk)$ est un groupe fini. Pour déterminer son cardinal, on remarque qu'une matrice $X \in \mathrm{GL}_n(\mathbb{F}_p)$ n'est rien d'autre qu'une liste ordonnée de n vecteurs colonne $X_1, \dots, X_n$ tels que

$$X_1 \neq 0, \quad X_2 \notin \mathbb{F}_p X_1, \quad X_3 \notin \mathrm{vect}_{\mathbb{F}_p}(X_1, X_2), \quad \dots, \quad X_n \notin \mathrm{vect}_{\mathbb{F}_p}(X_1, \dots, X_{n-1}).$$

En particulier :

- ◇ Pour X_1 nous avons $|\mathbb{F}_p^n \smallsetminus \{0\}| = p^n - 1$ choix ;
- ◇ Pour X_2 nous avons $|\mathbb{F}_p^n \smallsetminus \mathbb{F}_p X_1| = p^n - p$ choix ;
- ◇ Pour X_3 nous avons $|\mathbb{F}_p^n \smallsetminus \mathrm{vect}_{\mathbb{F}_p}(X_1, X_2)| = p^n - p^2$ choix ;

⋮

- ◇ Pour X_n nous avons $|\mathbb{F}_p^n \smallsetminus \mathrm{vect}_{\mathbb{F}_p}(X_1, X_2, \dots, X_{n-1})| = p^n - p^{n-1}$ choix.

Donc

$$|\mathrm{GL}_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p)(p^n - p^2) \cdots (p^n - p^{n-1}) = \prod_{k=0}^{n-1} (p^n - p^k).$$

En particulier, pour $p = n = 2$, on trouve $|\mathrm{GL}_2(\mathbb{F}_2)| = 6$. On verra dans la suite que $\mathrm{GL}_2(\mathbb{F}_2) \cong \mathfrak{S}_3$.

(*iii*) On fixe $n > 1$. Soit $R \in \mathrm{GL}_2(\mathbb{R})$ la rotation d'un angle $\frac{2\pi}{n}$ dans le sens anti-horaire autour de l'origine. Soit S la réflexion par rapport à l'axe des abscisses. En identifiant $\mathbb{R}^2$ avec $\mathbb{C}$, on obtient

$$R(z) = e^{\frac{2\pi\mathrm{i}}{n}} z, \qquad S(z) = \bar{z}.$$

On en déduit que $SR^kS = R^{-k}$ pour tout $k \in \mathbb{Z}$, car

$$S(R^k(S(z))) = S(R^k(\bar{z})) = S(e^{\frac{2k\pi\mathrm{i}}{n}} \bar{z}) = e^{-\frac{2k\pi\mathrm{i}}{n}} z = R^{-k}(z)$$

pour tout $z \in \mathbb{C}$. On prétend que

$$\mathscr{D}_n = \{I, R, \dots, R^{n-1}\} \cup \{S, RS, \dots, R^{n-1}S\}$$

est un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$. On remarque que

$$R^iR^j = R^{i+j}, \quad R^i(R^jS) = R^{i+j}S, \quad (R^iS)R^j = R^{i-j}S, \quad (R^iS)(R^jS) = R^{i-j}.$$

Donc $\mathscr{D}_n$ est clos par multiplication. De plus, le premier et le dernier produit impliquent respectivement que

$$(R^i)^{-1} = R^{-i}, \qquad (R^iS)^{-1} = R^iS.$$

Donc $\mathscr{D}_n$ est clos par inversion. Ce groupe s'appelle le *groupe diédral de* $2n$ *éléments*. Si $n > 2$, alors $\mathscr{D}_n$ n'est pas commutatif.

2.2. **Actions.** Soit X ensemble et G un groupe.

Définition 2.2.1. Une *action* de G sur X est une fonction

$$G \times X \to X$$
$$(g, x) \mapsto g \cdot x$$

telle que

(*i*) $e \cdot x = x$ pour tout $x \in X$;

(*ii*) $(gg') \cdot x = g \cdot (g' \cdot x)$ pour tout $g, g' \in G$ et $x \in X$.

De temps en temps, un ensemble muni d'une action d'un groupe G sera appelé un *G-ensemble*.

Exercice 2.2.2. Si X est un ensemble muni d'une action d'un groupe G, alors la fonction $\rho : G \to \mathfrak{S}_X$ définie par $\rho(g)(x) := g \cdot x$ pour tout $g \in G$ et $x \in X$ est un morphisme de groupes, où $\mathfrak{S}_X$ désigne le groupe des bijections de X. Réciproquement, si $\rho : G \to \mathfrak{S}_X$ est un morphisme de groupes, alors $g \cdot x := \rho(g)(x)$ définit une action de G sur X.

Exemple 2.2.3. (*i*) Le groupe $\mathfrak{S}_n$ agit naturellement sur l'ensemble $\{1, \dots, n\}$.

(*ii*) On identifie $\Bbbk^n$ avec l'ensemble des vecteurs colonne à coefficients dans $\Bbbk$. Le groupe $\mathrm{GL}_n(\Bbbk)$ agit alors sur $\Bbbk^n$ par produit matriciel, en posant $A \cdot v = Av$ pour tout $A \in \mathrm{GL}_n(\Bbbk)$ et $v \in \Bbbk^n$.

(*iii*) Pour tout $g \in \mathscr{D}_n$ et $\zeta \in \boldsymbol{\mu}_n$, l'élément $g(\zeta)$ est encore une racine n-ème de l'unité. Afin de le voir, il suffit de le vérifier pour les générateurs $R, S \in \mathscr{D}_n$:

$$(R(\zeta))^n = \left(e^{\frac{2\pi \mathrm{i}}{n}} \zeta\right)^n = e^{\frac{2n\pi \mathrm{i}}{n}} \zeta^n = 1, \qquad (S(\zeta))^n = \left(\bar{\zeta}\right)^n = \zeta^{-n} = 1.$$

On obtient donc une action de $\mathscr{D}_n$ sur $\boldsymbol{\mu}_n$.

(*iv*) Soit H un sous-groupe d'un groupe G.

(a) H agit sur G par le morphisme de groupes $\rho_{\mathrm{L}} : H \to \mathfrak{S}_G$ obtenu en posant $\rho_{\mathrm{L}}(h)(g) := hg$ pour tout $h \in H$ et $g \in G$. Cela est l'*action de H sur G par translation à gauche*.

(b) H agit sur G par le morphisme de groupes $\rho_{\mathrm{R}} : H \to \mathfrak{S}_G$ obtenu en posant $\rho_{\mathrm{R}}(h)(g) := gh^{-1}$ pour tout $h \in H$ et $g \in G$. Cela est l'*action de H sur G par translation à droite*. Le lecteur devra vérifier que la formule précédente est bien cohérente, et qu'en posant $h \cdot g = gh$ **on n'obtient pas une action**.

Dans l'exemple précédent, on a vu qu'un sous-groupe $H < G$ peut agir de deux manières différentes. Finalement, ces actions ne sont pas si différentes que ça. Pour exprimer cela de façon précise, on a besoin d'une définition.

Définition 2.2.4. Soient X et Y deux G-ensembles. Une fonction $f : X \to Y$ est dite *G-équivariante*, ou une *G–fonction*, si $f(g \cdot x) = g \cdot (f(x))$ pour tout $g \in G$ et $x \in X$.

On peut maintenant exprimer le fait que les actions par translation à droite et à gauche sont "les mêmes".

Exercice 2.2.5. Soit $H < G$ un sous-groupe. Soit G_{L} l'ensemble G muni de l'action par translations à gauche de H, à savoir, $\rho_{\mathrm{L}}(h)(g) = hg$ pour tout $h \in H$ et $g \in G_{\mathrm{L}}$. Soit G_{R} l'ensemble G muni de l'action par translations à droite de H, à savoir, $\rho_{\mathrm{R}}(h)(g) = gh^{-1}$ pour tout $h \in H$ et $g \in G_{\mathrm{R}}$. Montrer que la fonction $\_^{-1} : G_{\mathrm{L}} \to G_{\mathrm{R}}$ est une bijection H-équivariante.

Si l'ensemble X est muni d'une structure additionnelle, on s'intéresse souvent aux actions qui préservent cette structure.

Définition 2.2.6. Soit G un groupe.

(i) Soit Γ un groupe et $G \times \Gamma \to \Gamma$ une action. On dit que G *agit par homomorphismes* si

$$g \cdot (\gamma\gamma') = (g \cdot \gamma)(g \cdot \gamma')$$

pour tout $g \in G$ et $\gamma, \gamma' \in \Gamma$. Cela arrive si et seulement si la bijection $\rho(g)$ définie dans l'Exercice 2.2.2 est un morphisme de groupes pour tout $g \in G$. Dans ce cas, $\operatorname{im}\rho < \operatorname{Aut}(\Gamma)$, donc, sans changer de nom, l'action de G sur Γ est donnée par un homomorphisme $\rho : G \to \operatorname{Aut}(\Gamma)$.

(ii) Soit V un espace vectoriel sur un corps $\Bbbk$ et $G \times V \to V$ une action. On dit que cette action est *linéaire* si

$$g \cdot (v + v') = g \cdot v + g \cdot v', \qquad g \cdot (\lambda v) = \lambda(g \cdot v)$$

pour tout $g \in G$, $v, v' \in V$ et $\lambda \in \Bbbk$. Cela arrive si et seulement si la bijection $\rho(g)$ définie dans l'Exercice 2.2.2 est une application linéaire pour tout $g \in G$. Dans ce cas, $\operatorname{im}\rho < \mathrm{GL}_{\Bbbk}(V)$, donc, sans changer de nom, l'action de G sur V est donnée par un homomorphisme $\rho : G \to \mathrm{GL}_{\Bbbk}(V)$.

Exemple 2.2.7. (i) L'action d'un sous-groupe $H < G$ sur G par translation à gauche est une action par homomorphismes si et seulement si $H = \{e\}$. En effet,

$$\begin{aligned} & h \cdot (gg') = (h \cdot g)(h \cdot g') && \forall\, h \in H \\ \Leftrightarrow \quad & hgg' = hghg' && \forall\, h \in H \\ \Leftrightarrow \quad & e = (hg)^{-1}(hgg')(g')^{-1} = (hg)^{-1}(hghg')(g')^{-1} = h && \forall\, h \in H. \end{aligned}$$

(ii) L'action de $\mathrm{GL}_n(\Bbbk)$ sur $\Bbbk^n$ est clairement linéaire.

L'un des exemples les plus importantes d'actions par homomorphismes est le suivant.

Exemple 2.2.8. Si $H < G$ est un sous-groupe, alors H agit sur G par le morphisme de groupes $\rho_{\mathrm{C}} : H \to \operatorname{Aut}(G) < \mathfrak{S}_G$ obtenu en posant $\rho_{\mathrm{C}}(h)(g) := hgh^{-1}$ pour tout $h \in H$ et $g \in G$. Cela est l'*action de H sur G par conjugaison.* Il s'agit d'une action par homomorphismes, car

$$h \cdot (gg') = hgg'h^{-1} = hgh^{-1}hg'h^{-1} = (h \cdot g)(h \cdot g')$$

pour tout $h \in H$ et $g, g' \in G$.

L'idée même d'action donne directement des résultats non-triviaux.

Théorème 2.2.9 (Théorème de Cayley)**.** *Si G est un groupe d'ordre n, alors G est isomorphe à un sous-groupe de $\mathfrak{S}_n$.*

Démonstration. On considère l'action de G sur lui même par translation à gauche. D'après l'Exercice 2.2.2, on obtient un morphisme de groupes $\rho_{\mathrm{L}} : G \to \mathfrak{S}_G \cong \mathfrak{S}_n$. Il est clair que

$$g \in \ker\rho_{\mathrm{L}} \Rightarrow \rho_{\mathrm{L}}(g)(e) = e \Rightarrow g = e.$$

Donc ρ_{L} est injectif, et $\rho_{\mathrm{L}} : G \to \operatorname{im}\rho_{\mathrm{L}} < \mathfrak{S}_n$ est isomorphisme. □

Malgré son apparence spectaculaire, le Théorème 2.2.9 n'est pas si puissant que ça. En effet, les sous-groupes d'un groupe symétrique ne sont pas faciles à déterminer.

Exemple 2.2.10. Posons $\zeta_n = e^{\frac{2\pi\mathrm{i}}{n}}$. On a $\boldsymbol{\mu}_n = \{\zeta_n^k \mid 1 \leqslant k \leqslant n\}$. En faisant agir $\boldsymbol{\mu}_n$ par translation à gauche sur lui même, on obtient un homomorphisme injectif

$$\begin{aligned} \rho_{\mathrm{L}} : \boldsymbol{\mu}_n &\hookrightarrow \mathfrak{S}_{\boldsymbol{\mu}_n} \cong \mathfrak{S}_n \\ \zeta_n^k &\mapsto (1\ 2\ \cdots\ n)^k. \end{aligned}$$

Définition 2.2.11. Soit X un ensemble muni d'une action d'un groupe G, et soit $x \in X$ un élément.

(*i*) Un sous-ensemble $Y \subset X$ est *stable par* G si $G \cdot Y \subset Y$, où $G \cdot Y$ dénote l'ensemble $\{g \cdot y \mid g \in G, y \in Y\}$.

(*ii*) L'*orbite de* x est $\mathrm{orb}(x) = \{g \cdot x \mid g \in G\} \subset X$. On écrira parfois $G \cdot x$ pour $\mathrm{orb}(x)$. Clairement, $\mathrm{orb}(x)$ est stable par G.

(*iii*) Le *stabilisateur de* x est $\mathrm{st}(x) = \{g \in G \mid g \cdot x = x\}$. On écrira parfois G_x pour $\mathrm{st}(x)$. Clairement, $\mathrm{st}(x)$ est un sous-groupe de G.

(*iv*) On dit que x est un *point fixe* si $g \cdot x = x$ pour tout $g \in G$, c'est-à-dire si $G_x = G$. L'ensemble des points fixes est noté X^G.

(*v*) On dit que l'action est *transitive* si X consiste en une seule orbite, c'est-à-dire si $X = G \cdot x$ pour quelque (en fait pour tout) $x \in X$. Dans ce cas, X est appelé aussi un *espace homogène*.

(*vi*) On dit que l'action est *libre* si tous les stabilisateurs sont triviaux, c'est à dire si $G_x = \{e\}$ pour tout $x \in X$.

Exemple 2.2.12. (*i*) Le groupe $G = \mathrm{GL}_n(\Bbbk)$ agit naturellement sur $\Bbbk^n$. Si $n = 2$, et si $\{e_1, e_2\}$ dénote la base standard de $\Bbbk^2$, alors $G \cdot e_1 = \Bbbk^2 \smallsetminus \{0\}$, car

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{cases} \begin{pmatrix} x & 0 \\ y & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} & \text{si } x \neq 0, \\ \begin{pmatrix} x & 1 \\ y & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} & \text{si } y \neq 0 \end{cases} \in G \cdot e_1 \qquad \forall \begin{pmatrix} x \\ y \end{pmatrix} \in \Bbbk^2 \smallsetminus \{0\},$$

et $G \cdot 0 = \{0\}$. L'action est donc transitive sur $\Bbbk^2 \smallsetminus \{0\}$, et 0 est l'unique point fixe. De plus,

$$G_{e_1} = \left\{ \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \;\middle|\; b, d \in \Bbbk, d \neq 0 \right\}.$$

Il suit que $\Bbbk^2$ n'est pas un espace homogène, et que l'action n'est pas libre.

(*ii*) Soit H un sous-groupe d'un groupe G. En faisant agir H par translation à gauche/droite, les stabilisateurs sont triviaux, c'est-à-ride $\mathrm{st}(g) = \{e\}$ pour tout $g \in G$, et les orbites sont les classes à droite/gauche, $\mathrm{orb}(g) = Hg = \{hg \mid h \in H\}$, pour la translation à gauche, et $\mathrm{orb}(g) = gH = \{gh \mid h \in H\}$, pour la translation à droite. Donc ces deux actions sont libres, et elles sont transitives si et seulement si $H = G$.

Exercice 2.2.13 (Exercice 1.(*ii*), TD1)**.** Soit $\mathbb{P}^{n-1}(\Bbbk)$ l'*espace projectif de dimension* $n-1$ *sur* $\Bbbk$, qui est par définition l'ensemble des droites vectorielles de $\Bbbk^n$. De manière équivalente, $\mathbb{P}^{n-1}(\Bbbk)$ peut être défini comme le quotient de $\Bbbk^n \smallsetminus \{0\}$ par la relation d'équivalence

$$v \sim v' \Leftrightarrow \exists\, \lambda \in \Bbbk^\times : v' = \lambda v.$$

Le groupe $G = \mathrm{GL}_n(\Bbbk)$ agit naturellement sur $\mathbb{P}^{n-1}(\Bbbk)$ par $A \cdot [v] = [Av]$ pour tout $[v] \in \mathbb{P}^1(\Bbbk)$ et $A \in G$. En prenant $n = 2$, montrer que cette action n'est pas libre, mais qu'elle est transitive.

Exercice 2.2.14 (Exercice 5, TD1)**.** En utilisant l'action de $\mathrm{GL}_2(\mathbb{F}_2)$ sur l'espace projectif $\mathbb{P}^1(\mathbb{F}_2)$, montrer que $\mathrm{GL}_2(\mathbb{F}_2) \cong \mathfrak{S}_3$.

Il s'avère que les actions transitives et libres sont "uniques".

Exercice 2.2.15. Soit X un ensemble muni d'une action libre et transitive d'un groupe G, et soit $x \in X$ un de ses éléments. Alors la fonction $\varphi : G \to X$ définie par $\varphi(g) = g \cdot x$ est une bijection G-équivariante.

2.3. **Quotients.** Soit X un G-ensemble.

Définition 2.3.1. Le *quotient de X par G* est l'ensemble X/G des orbites de G. La *projection canonique* est la fonction $\pi : X \twoheadrightarrow X/G$ qui à tout $x \in X$ associe son orbite $\mathrm{orb}(x) \in X/G$.

Exemple 2.3.2. (*i*) Considérons l'action naturelle de $G = \mathrm{GL}_2(\Bbbk)$ sur $X = \Bbbk^2$. Alors, comme vu dans l'Exemple 2.2.12, on a $X/G = \{\{0\}, \Bbbk^2 \smallsetminus \{0\}\}$.

(*ii*) Le groupe $G = \Bbbk^\times$ agit sur $X = \Bbbk^n \smallsetminus \{0\}$ par multiplication scalaire, en posant $\lambda \cdot v = \lambda v$ pour tout $\lambda \in G$ et $v \in X$. Toute orbite est alors une droite vectorielle privée de l'origine, et $X/G \cong \mathbb{P}^{n-1}(\Bbbk)$.

(*iii*) Soit H un sous-groupe d'un groupe G. En utilisant la notation introduite dans l'Exercice 2.2.5 pour les actions par translation à gauche/droite, on obtient les ensembles quotients des classes à droite $G_{\mathrm{L}}/H = \{Hg \mid g \in G\}$ et celui des classes à gauche $G_{\mathrm{R}}/H = \{gH \mid g \in G\}$. On écrira parfois $H\backslash G$ pour G_{L}/H et G/H pour G_{R}/H.

Proposition 2.3.3. *Si H est un sous-groupe d'un groupe G, alors il existe une bijection $H\backslash G \to G/H$.*

Démonstration. On a vu dans l'Exercice 2.2.5 que l'inversion $\_^{-1} : G_{\mathrm{L}} \to G_{\mathrm{R}}$ définit une bijection H-équivariante. Les orbites sont alors en bijection. □

Exemple 2.3.4. Pour $G = \mathscr{D}_3$ et $H = \langle S \rangle$, on trouve

$$H\backslash G = \{\{I, S\}, \{R, R^2S\}, \{R^2, RS\}\},$$
$$G/H = \{\{I, S\}, \{R, RS\}, \{R^2, R^2S\}\}.$$

Définition 2.3.5. L'*indice de H dans G* est $[G : H] := |H\backslash G| = |G/H|$.

On en profite pour rappeler le Théorème 1.1.3 : si G est fini, alors

$$[G : H] = |G|/|H|,$$

car chacune des orbites gH contient exactement $|H|$ éléments, et il y a, par définition, $[G : H]$ orbites.

Voilà la propriété universelle satisfaite par les quotients, dont la preuve est tautologique. Ce résultat est parfois appelé le *Théorème de factorisation*.

Proposition 2.3.6. *Si X est un G-ensemble et Y est un ensemble, alors, pour toute fonction $f : X \to Y$ qui est constante sur les orbites, il existe une unique fonction*

$$\bar{f} : X/G \to Y$$

telle que $\bar{f}(\mathrm{orb}(x)) = f(x)$ pour tout $x \in X$, c'est-à-dire telle que $\bar{f} \circ \pi = f$ pour la projection canonique $\pi : X \twoheadrightarrow X/G$.

Si H est un sous-groupe d'un groupe G, alors une propriété très importante du quotient G/H est le fait qu'il admet encore une action naturelle de G par translation à gauche. En effet, si on pose $g \cdot g'H = gg'H$ pour tout $g \in G$ et $g'H \in G/H$, on peut vérifier facilement qu'il s'agit d'une action. Dans la théorie, cette action joue un rôle de premier plan, car elle est le prototype d'une action transitive.

Lemme 2.3.7. *Soit X un G-ensemble, et soit $x \in X$ un de ses éléments.*

(*i*) *La fonction $\varphi_x : G/G_x \to G \cdot x$ définie par $\varphi_x(gG_x) = g \cdot x$ pour tout $g \in G$ est une bijection.*

(*ii*) *La bijection $\varphi_x : G/G_x \to G \cdot x$ est G-équivariante par rapport aux actions de G sur G/G_x (par translation à gauche) et sur $G \cdot x$ (par restriction de l'action sur X).*

(*iii*) *Les stabilisateurs des éléments d'une même orbite sont tous conjugués par* $G_{g\cdot x} = gG_xg^{-1}$.

Démonstration. La preuve est évidente, mais on la reproduit ici pour aider le lecteur à retenir les définitions.

(*i*) Si $g'G_x = gG_x$, alors $g' = gs$ pour quelque $s \in G_x$, et

$$g' \cdot x = (gs) \cdot x = g \cdot (s \cdot x) = g \cdot x.$$

Donc la fonction φ_x est bien définie. Elle est surjective par définition d'orbite. Elle est injective car

$$\begin{aligned}\varphi_x(gG_x) = \varphi_x(g'G_x) &\Leftrightarrow g \cdot x = g' \cdot x \Leftrightarrow g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (g' \cdot x)\\ &\Leftrightarrow x = (g^{-1}g') \cdot x \Leftrightarrow g^{-1}g' \in G_x \Leftrightarrow gG_x = g'G_x.\end{aligned}$$

(*ii*) Pour tout $g \in G$ et $g'G_x \in G/G_x$ on a

$$\varphi_x(g \cdot g'G_x) = \varphi_x(gg'G_x) = (gg') \cdot x = g \cdot (g' \cdot x) = g \cdot \varphi_x(g'G_x).$$

(*iii*) Pour tout $g \in G$ on a

$$\begin{aligned}s \in G_{g\cdot x} \Leftrightarrow s \cdot (g \cdot x) = g \cdot x \Leftrightarrow g^{-1} \cdot (s \cdot (g \cdot x)) = g^{-1} \cdot (g \cdot x) \Leftrightarrow (g^{-1}sg) \cdot x = x\\ \Leftrightarrow g^{-1}sg \in G_x \Leftrightarrow s \in gG_xg^{-1}.\end{aligned}$$

□

Corollaire 2.3.8. *Si X est un G-espace homogène, c'est-à-dire un G-espace constitué d'une seule orbite, alors il existe un sous-groupe $H < G$ et une bijection G-équivariante $\varphi : G/H \to X$.*

Démonstration. On choisit $x \in X$, on pose $H = G_x$, et on applique le Lemme 2.3.7. □

Corollaire 2.3.9 (Formule des classes)**.** *Soit G un groupe fini et X un G-espace fini.*

(*i*) *Pour tout $x \in X$ on a*

$$|G \cdot x| = [G : G_x].$$

(*ii*) *Si $X = (G \cdot x_1) \sqcup \ldots \sqcup (G \cdot x_n)$, alors*

$$|X| = \sum_{i=1}^{n} |G \cdot x_i| = \sum_{i=1}^{n} \frac{|G|}{|G_{x_i}|}.$$

Démonstration. L'énoncé est une conséquence directe du Lemme 2.3.7.(*ii*).

(*i*) La fonction

$$\begin{aligned}\varphi_x : G/G_x &\to G \cdot x\\ gG_x &\mapsto g \cdot x\end{aligned}$$

est une bijection, donc $|G \cdot x| = |G/G_x|$. Mais $|G/G_x| = [G : G_x]$ par définition.

(*ii*) Comme $X = (G \cdot x_1) \sqcup \ldots \sqcup (G \cdot x_n)$, on a

$$|X| = \sum_{i=1}^{n} |G \cdot x_i|.$$

En utilisant la bijection φ_x on déduit que $|G \cdot x_i| = |G/G_{x_i}| = |G|/|G_{x_i}|$ pour tout entier $1 \leqslant i \leqslant n$. □

Exemple 2.3.10. (i) Considérons l'espace projectif $\mathbb{P}^1(\Bbbk)$, sur lequel le groupe général linéaire $\mathrm{GL}_2(\Bbbk)$ agit transitivement, comme vu dans l'Exercice 2.2.13.(iii). En utilisant le Lemme 2.3.7, on obtient une bijection $\mathrm{GL}_2(\Bbbk)$-équivariante

$$\mathrm{GL}_2(\Bbbk)/B \to \mathbb{P}^1(\Bbbk),$$

où $B = \mathrm{st}([e_1])$ est le groupe des matrices triangulaires supérieures inversibles.

(ii) Le groupe additif $\mathbb{R}$ agit sur le cercle $S^1 \cong \{z \in \mathbb{C} \mid |z| = 1\}$ par rotations, en posant $t \cdot z = e^{2t\pi \mathrm{i}} z$. Clairement, cette action est transitive. De plus, $\mathrm{st}(1) = \mathbb{Z}$. Alors la fonction

$$\begin{aligned} \mathbb{R} &\to S^1 \\ \vartheta &\mapsto e^{2t\pi \mathrm{i}} \end{aligned}$$

définit une bijection entre $\mathbb{R}/\mathbb{Z}$ et S^1.

Définition 2.3.11. Soit $p \in \mathbb{N}$ un nombre premier. Un *p-groupe fini* est un groupe d'ordre p^n pour quelque entier $n > 0$.

Exercice 2.3.12 (Exercice 7, TD1)**.** Soit G un p-groupe fini et X un G-ensemble fini. Montrer que

$$|X| \equiv |X^G| \pmod{p}.$$

Démonstration. Si $x \in X$ n'est pas un point fixe, alors, grâce au Lemme 2.3.7, on a que

$$1 < |\mathrm{orb}(x)| = |G/\mathrm{st}(x)| = |G|/|\mathrm{st}(x)| \mid |G|.$$

Cela implique que

$$|\mathrm{orb}(x)| \equiv 0 \pmod{p}$$

pour tout $x \in X \smallsetminus X^G$. Si $X = \mathrm{orb}(x_1) \sqcup \ldots \sqcup \mathrm{orb}(x_n)$ et $X^G = \{x_1, \ldots, x_m\}$ pour quelque $1 \leqslant m \leqslant n$, alors la formule des classes nous permet de déduire que

$$|X| = \sum_{i=1}^{m} |\mathrm{orb}(x_i)| + \sum_{j=m+1}^{n} |\mathrm{orb}(x_j)| \equiv m = |X^G| \pmod{p}. \qquad \square$$

Théorème 2.3.13 (Théorème de Cauchy, Exercice 8, TD1)**.** *Si un nombre premier p divise l'ordre d'un groupe G, alors G admet un élément d'ordre p.*

Démonstration. Considérons l'ensemble F des fonctions $f : \mathbb{Z}/p\mathbb{Z} \to G$. Pour chaque $a \in \mathbb{Z}/p\mathbb{Z}$ et $f \in F$, soit $a \cdot f \in F$ la fonction définie par $(a \cdot f)(b) := f(a+b)$ pour tout $b \in \mathbb{Z}/p\mathbb{Z}$. Cela définit une action de $\mathbb{Z}/p\mathbb{Z}$ sur F, car

$$(0 \cdot f)(a) = f(0 + a) = f(a)$$

pour tout $a \in \mathbb{Z}/p\mathbb{Z}$ implique que $(0 \cdot f) = f$, et

$$(a \cdot (b \cdot f))(c) = (b \cdot f)(a + c) = f(a + b + c) = ((a + b) \cdot f)(c)$$

pour tout $c \in \mathbb{Z}/p\mathbb{Z}$ implique que $a \cdot (b \cdot f) = (a + b) \cdot f$ pour tout $a, b \in \mathbb{Z}/p\mathbb{Z}$. On remarque que l'ensemble des points fixes de cette action est l'ensemble $F^{\mathbb{Z}/p\mathbb{Z}}$ des fonctions constantes, car

$$a \cdot f = f \quad \forall\, a \in \mathbb{Z}/p\mathbb{Z} \quad \Leftrightarrow \quad f(a) = f(0) \quad \forall\, a \in \mathbb{Z}/p\mathbb{Z}.$$

Considérons maintenant l'ensemble

$$X = \left\{ f \in F \;\middle|\; \prod_{a=0}^{p-1} f(a) = e \right\}.$$

On peut remarquer que X est stable par l'action de $\mathbb{Z}/p\mathbb{Z}$. En effet, si $f \in X$ et $a \in \mathbb{Z}/p\mathbb{Z}$, alors $a \cdot f \in X$, car l'élément

$$g_a := \prod_{b=0}^{p-1}(a \cdot f)(b) = \prod_{b=0}^{p-1} f(a+b) = \left(\prod_{c=a}^{p-1} f(c)\right)\left(\prod_{d=0}^{a-1} f(d)\right) \in G$$

satisfait $g_a^2 = g_a$, ce qui implique $g_a = e$. Donc l'ensemble des points fixes de l'action de $\mathbb{Z}/p\mathbb{Z}$ sur X est l'ensemble $X^{\mathbb{Z}/p\mathbb{Z}}$ des fonctions constantes qui appartiennent à X. La fonction

$$\begin{aligned} \varphi : F &\to G \\ f &\mapsto f(0) \end{aligned}$$

se restreint alors à une bijection entre $X^{\mathbb{Z}/p\mathbb{Z}}$ et l'ensemble des éléments $g \in G$ qui satisfont $g^p = e$. Comme $e \in \varphi(X^{\mathbb{Z}/p\mathbb{Z}})$, on doit montrer que $|X^{\mathbb{Z}/p\mathbb{Z}}| > 1$. Mais, grâce à l'Exercice 2.3.12, on a que

$$|X^{\mathbb{Z}/p\mathbb{Z}}| \equiv |X| \pmod{p}.$$

Il suffit alors de compter les éléments de X. Pour ce faire, on remarque que, afin de définir une fonction $f \in X$, on peut choisir arbitrairement $f(a)$ pour tout entier $0 \leqslant a \leqslant p-2$, à condition que

$$f(p-1) = \left(\prod_{a=1}^{p-2} f(a)\right)^{-1}.$$

On a donc $|G|$ possibilités pour l'image de tout $0 \leqslant a \leqslant p-2$, ce qui implique

$$|X| = |G|^{p-1} \equiv 0 \pmod{p}. \qquad \square$$

Remarque 2.3.14. Soit p un nombre premier et G un p-groupe fini d'ordre p^n. On fait agir G sur lui même par conjugaison, c'est-à-dire $g \cdot x = gxg^{-1}$ pour tout $g, x \in G$. C'est facile de voir que l'ensemble des points fixes G^G coïncide avec le centre $\mathrm{Z}(G)$. Grâce à l'Exercice 2.3.12 on déduit

$$|G| \equiv |\mathrm{Z}(G)| \pmod{p}.$$

Par conséquent, $|\mathrm{Z}(G)| \equiv 0 \pmod{p}$. En particulier, $|\mathrm{Z}(G)| \neq 1$.

Exercice 2.3.15 (Exercice 8, TD2)**.** Montrer que tout groupe d'ordre p^2 est abélien.

Soit X un ensemble muni d'une action d'un groupe G, et soit $g \in G$ un élément. L'*ensemble points fixes de* g est $\mathrm{fix}(g) := \{x \in X \mid g \cdot x = x\}$. On écrira parfois X^g pour $\mathrm{fix}(g)$.

Lemme 2.3.16 (Lemme de Burnside, Exercice 11, TD1)**.** *Soit X un ensemble fini muni d'une action d'un groupe fini G. Montrer que*

$$|X/G| = \frac{1}{|G|}\sum_{g \in G} |X^g|.$$

Démonstration. Soit $S = \{(g, x) \in G \times X \mid g \cdot x = x\}$, et soient $p_G : S \to G$ et $p_X : S \to X$ les projections naturelles. D'une part, on a

$$S = \bigsqcup_{g \in G} p_G^{-1}(g) = \bigsqcup_{g \in G} \{g\} \times X^g,$$

et, d'autre part, on a

$$S = \bigsqcup_{x \in X} p_X^{-1}(x) = \bigsqcup_{x \in X} G_x \times \{x\}.$$

On en déduit que

$$\sum_{g\in G}|X^g| = \sum_{x\in X}|G_x|.$$

Grâce au Lemme 2.3.7.(i), on a que

$$\sum_{x\in X}|G_x| = \sum_{x\in X}\frac{|G|}{|G\cdot x|} = |G|\sum_{x\in X}\frac{1}{|G\cdot x|}.$$

En réorganisant la somme par orbites, on obtient

$$\begin{aligned}\sum_{x\in X}|G_x| &= |G|\sum_{G\cdot y\in X/G}\left(\sum_{x\in G\cdot y}\frac{1}{|G\cdot x|}\right) = |G|\sum_{G\cdot y\in X/G}\left(\frac{1}{|G\cdot y|}\sum_{x\in G\cdot y}1\right)\\ &= |G|\sum_{G\cdot y\in X/G}\frac{|G\cdot y|}{|G\cdot y|} = |G||X/G|,\end{aligned}$$

où on a utilisé le fait que, pour tout $x\in G\cdot y$, on a $G\cdot x = G\cdot y$. □

2.4. **Sous-groupes distingués.** Soit H un sous-groupe d'un groupe G. Il est facile de voir que, si G est abélien, alors les classes à droite et les classes à gauche coïncident. Les sous-groupes ayant cette propriété ont une importance capitale dans la théorie.

Proposition 2.4.1. *Soit H un sous-groupe d'un groupe G. Les énoncés suivants sont tous équivalents.*

(i) *Pour tout $g\in G$, les classes gH et Hg coïncident.*

(ii) *Pour tout $g\in G$, le sous-groupe conjugué gHg^{-1} coïncide avec H.*

(iii) *Pour tout $g\in G$, le sous-groupe conjugué gHg^{-1} est contenu dans H.*

Démonstration. $(i)\Rightarrow(ii)$ Clairement $gH = Hg$ implique $gHg^{-1} = Hgg^{-1} = H$ pour tout $g\in G$.

$(ii)\Rightarrow(iii)$ L'implication est directe.

$(iii)\Rightarrow(i)$ D'une part $gHg^{-1}\subset H$ implique $gH = gHg^{-1}g\subset Hg$, et d'autre part $g^{-1}Hg\subset H$ implique $Hg = gg^{-1}Hg\subset gH$ pour tout $g\in G$. □

Définition 2.4.2. Un sous-groupe H d'un groupe G est *distingué* si $gHg^{-1}\subset H$ pour tout $g\in G$. Dans ce cas, on écrira $H\triangleleft G$.

Exemple 2.4.3. On a vu dans l'Exemple 2.3.4 que

$$\begin{aligned}\langle S\rangle\backslash\mathscr{D}_3 &= \{\{I,S\},\{R,R^2S\},\{R^2,RS\}\},\\ \mathscr{D}_3/\langle S\rangle &= \{\{I,S\},\{R,RS\},\{R^2,R^2S\}\}.\end{aligned}$$

En effet, $R\langle S\rangle R^{-1} = \{I,R^2S\}$, et $\langle S\rangle$ n'est pas distingué.

Le prototype de sous-groupe distingué est le noyau d'un homomorphisme. On verra que cela est essentiellement la seule façon de produire des sous-groupes distingués.

Lemme 2.4.4. *Si $f: G\to G'$ est un morphisme de groupes, alors* $\ker f\triangleleft G$.

Démonstration. Pour tout $x\in\ker f$ et $g\in G$, on a

$$f(gxg^{-1}) = f(g)f(x)f(g^{-1}) = f(g)f(g)^{-1} = e',$$

donc $gxg^{-1}\in\ker f$. □

Exemple 2.4.5. (i) Si G est abélien, alors tout sous-groupe de G est distingué.

(*ii*) Le *groupe linéaire spécial* $\mathrm{SL}_n(\Bbbk) = \{A \in \mathrm{GL}_n(\Bbbk) \mid \det A = 1\}$ est un sous-groupe distingué de $\mathrm{GL}_n(\Bbbk)$, car il coïncide avec le noyau de l'homomorphisme $\det : \mathrm{GL}_n(\Bbbk) \to \Bbbk^\times$.

(*iii*) Si $H < G$ est un sous-groupe d'indice 2 dans G, alors $H \triangleleft G$. En effet, dans ce cas, $|H\backslash G| = |G/H| = [G : H] = 2$. Comme, pour les deux actions de H par translation sur G, une des deux orbites est toujours $He = H = eH$, il suit que

$$H\backslash G = \{H, G \smallsetminus H\} = G/H.$$

En particulier, pour chaque $n > 1$, le sous-groupe $\mathscr{R} = \langle R \rangle$ de $\mathscr{D}_n$ engendré par R est distingué.

(*iv*) Pour tout $n > 1$, la signature $\mathrm{sgn} : \mathfrak{S}_n \to \{+1, -1\} = \boldsymbol{\mu}_2$ est un homomorphisme surjectif. Son noyau $\mathfrak{A}_n := \ker \mathrm{sgn}$ est appelé le *groupe alterné*. Il peut être caractérisé comme le sous-groupe des permutations qui s'expriment comme produit d'un nombre pair de transpositions.

Remarque 2.4.6. L'énoncé réciproque du point (*i*) de l'Exemple 2.4.5 est faux. Un groupe G dont tout sous-groupe est distingué est un *groupe de Dedekind*. Un groupe de Dedekind non abélien est un *groupe hamiltonien*. Un exemple de groupe hamiltonien est le *groupe des quaternions*

$$\mathrm{Q} = \langle i, j, k, -1 \mid (-1)^2 = 1, i^2 = j^2 = k^2 = ijk = -1 \rangle.$$

La propriété la plus importante des sous-groupes distingués est qu'on peut munir l'ensemble quotient d'une structure de groupe. On se donne ainsi un sous-groupe H d'un groupe G. Si xH et yH sont deux classes distinctes, on peut naïvement définir leur produit par

$$xHyH = xyH. \tag{1}$$

Cependant, si $h, k \in H$, alors $xhH = xH$ et $ykH = yH$. L'équation (1) implique

$$xHyH = xhykH.$$

Cette définition est donc cohérente seulement si

$$xyH = xhykH \tag{2}$$

pour tout $x, y \in G$ et $h, k \in H$.

Lemme 2.4.7. *Si $H \triangleleft G$, alors l'équation (2) est satisfaite pour tout $x, y \in G$ et $h, k \in H$.*

Démonstration. Comme $H \triangleleft G$, alors

$$xhyk = xy(y^{-1}hy)k \in xyH$$

pour tout $x, y \in G$ et $h, k \in H$, car $y^{-1}hy \in H$ pour tout $y \in G$ et $h \in H$. Comme deux classes distinctes sont soit disjointes, soit coïncidentes, on en déduit que $xhykH = xyH$. □

On peut ainsi énoncer le résultat le plus important concernant les sous-groupes distingués.

Théorème 2.4.8. *Soit H un sous-groupe distingué d'un groupe G.*

(*i*) *Avec l'opération définie par l'équation (1), l'ensemble G/H est un groupe. L'élément neutre est la classe eH, et l'inverse de xH est $x^{-1}H$.*

(*ii*) *Soit $\pi : G \twoheadrightarrow G/H$ la projection canonique, qui à $x \in G$ associe son orbite $xH \in G/H$. Alors π est un morphisme de groupes surjectif, et son noyau est H.*

La preuve du Théorème 2.4.8 est une conséquence directe du Lemme 2.4.7, et elle est laissée au lecteur.

Exemple 2.4.9. Soit X un ensemble muni d'une action d'un groupe G, et soit $H \triangleleft G$ un sous-groupe distingué satisfaisant $h \cdot x = x$ pour tout $h \in H$ et $x \in X$. Cela signifie que, si $\rho : G \to \mathfrak{S}_X$ est l'homomorphisme défini dans l'Exercice 2.2.2, alors $H < \ker \rho$. On en déduit ainsi une action du groupe G/H en utilisant le morphisme $\bar{\rho} : G/H \to \mathfrak{S}_X$. Une classe $gH \in G/H$ agit donc sur $x \in X$ par $gH \cdot x = g \cdot x$.

Quelques groupes importants sont naturellement décrits comme quotients.

Exemple 2.4.10. Soit $\Bbbk^\times I_n = \{\lambda I_n \mid \lambda \in \Bbbk^\times\} < \mathrm{GL}_n(\Bbbk)$ le sous-groupe des multiples non-nuls de l'identité. Comme $\Bbbk^\times I_n = \mathrm{Z}(\mathrm{GL}_n(\Bbbk))$, il suit que $\Bbbk^\times I_n \triangleleft \mathrm{GL}_n(\Bbbk)$. Le quotient $\mathrm{PGL}_n(\Bbbk) := \mathrm{GL}_n(\Bbbk)/\Bbbk^\times I_n$ est le *groupe projectif général*. De même, $(\Bbbk^\times I_n \cap \mathrm{SL}_n(\Bbbk)) \triangleleft \mathrm{SL}_n(\Bbbk)$, et $\mathrm{PSL}_n(\Bbbk) := \mathrm{SL}_n(\Bbbk)/(\Bbbk^\times I_n \cap \mathrm{SL}_n(\Bbbk))$ est le *groupe projectif spécial*.

Le résultat suivant est simple mais important. Il est connu également comme *Théorème de factorisation pour les groupes*, ou *Théorème fondamental d'homomorphisme*, ou parfois *Premier théoreme d'isomorphisme*.

Théorème 2.4.11 (Noyau et image)**.** *Si $f : G \to G'$ est un morphisme de groupes, alors $G/\ker f$ est isomorphe à $\operatorname{im} f$.*

Démonstration. Soit $K = \ker f$ et $H = \operatorname{im} f$. D'après la Proposition 2.3.6, on déduit l'existence d'une fonction $\bar{f} : G/K \to H$ telle que $\bar{f}(xK) = f(x)$ pour toute classe $xK \in G/K$. En effet, puisque $f(k) = e$ pour tout $k \in K$, la fonction f est constante sur toute classe $xK \in G/K$. En munissant G/K de la structure de groupe construite ci-dessus, $\bar{f}$ devient un morphisme de groupes, car

$$\bar{f}(xKyK) = \bar{f}(xyK) = f(xy) = f(x)f(y) = \bar{f}(xK)\bar{f}(yK).$$

De plus, comme $\ker \bar{f} = \{eK\}$, l'homomorphisme $\bar{f}$ est injectif, et comme $\operatorname{im} \bar{f} = H$, il est surjectif. □

Ce résultat est très utile pour déterminer efficacement les groupes quotients, dans le sens que cela nous permet souvent de les exprimer en terme de groupes qu'on connaît déjà.

Exemple 2.4.12. (*i*) Le quotient $\mathfrak{S}_n/\mathfrak{A}_n$ est isomorphe à $\boldsymbol{\mu}_2$. En effet, $\mathfrak{A}_n$ n'est rien d'autre que le noyau de la signature $\mathrm{sgn} : \mathfrak{S}_n \to \boldsymbol{\mu}_2$, qui est un homomorphisme surjectif.

(*ii*) Le quotient $\mathrm{GL}_n(\Bbbk)/\mathrm{SL}_n(\Bbbk)$ est $\Bbbk^\times$, car $\mathrm{SL}_n(\Bbbk)$ est le noyau du déterminant $\det : \mathrm{GL}_n(\Bbbk) \to \Bbbk^\times$.

(*iii*) On a vu dans l'Exemple 2.4.5 que $\mathscr{R} = \langle R \rangle \triangleleft \mathscr{D}_n$, car $[\mathscr{D}_n : \mathscr{R}] = 2$. Le quotient $\mathscr{D}_n/\mathscr{R}$ est un groupe d'ordre 2, qui est donc isomorphe à $\boldsymbol{\mu}_2$. Cela peut être également montré en remarquant que $\det : \mathscr{D}_n \to \boldsymbol{\mu}_2$ est un homomorphisme surjectif dont le noyau est $\mathscr{R}$, et que

$$\begin{aligned} \mathscr{D}_n/\mathscr{R} &\to \boldsymbol{\mu}_2 \\ g\mathscr{R} &\mapsto \det(g) \end{aligned}$$

est donc un isomorphisme.

(*iv*) Soit S^1 le groupe $\{z \in \mathbb{C} \mid |z| = 1\}$. Pour déterminer le quotient $S^1/\boldsymbol{\mu}_n$, on utilise l'homomorphisme

$$\begin{aligned} \_^n : S^1 &\to S^1 \\ z &\mapsto z^n. \end{aligned}$$

Comme $\ker(\_^n) = \boldsymbol{\mu}_n$ et $\operatorname{im}(\_^n) = S^1$, on déduit que $S^1/\boldsymbol{\mu}_n \cong S^1$.

Le résultat suivant est parfois connu comme *Théorème de correspondance pour les groupes.*

Théorème 2.4.13. *Soit N un sous-groupe distingué d'un groupe G, avec projection canonique $\pi : G \to \bar{G} = G/N$.*

(i) Pour tout $H < G$, l'image $\pi(H) < \bar{G}$ est isomorphe à $H/(H \cap N)$. Si $H \triangleleft G$, alors $\pi(H) \triangleleft \bar{G}$.

(ii) Pour tout $\bar{H} < \bar{G}$, la préimage $\pi^{-1}(\bar{H}) < G$ est l'unique sous-groupe $H < G$ satisfaisant $N \subset H$ et $\pi(H) = \bar{H}$. Si $\bar{H} \triangleleft \bar{G}$, alors $\pi^{-1}(\bar{H}) \triangleleft \bar{G}$.

(iii) L'ensemble des sous-groupes de G contenants N est en bijection avec l'ensemble des sous-groupes de $\bar{G}$.

Démonstration. *(i)* Comme la restriction de π à H a comme noyau $H \cap N$ et comme image $\pi(H)$, le Théorème 2.4.11 implique que $\pi(H) \cong H/(H \cap N)$. Pour montrer que, si $H \triangleleft G$, alors $\pi(H) \triangleleft \bar{G}$, on considère $\bar{g} \in \bar{G}$ et $\pi(h) \in \pi(H)$. Soit $g \in G$ tel que $\pi(g) = \bar{g}$. Il suit que

$$\bar{g}\pi(h)\bar{g}^{-1} = \pi(g)\pi(h)\pi(g)^{-1} = \pi(ghg^{-1}) \in \pi(H).$$

(ii) Soit $H < G$ un sous-groupe contenant N et tel que $\pi(H) = \bar{H}$. On remarque que, si $h \in H$, alors $\pi(h) \in \bar{H}$, et donc $h \in \pi^{-1}(\bar{H})$ par définition. On obtient que $H < \pi^{-1}(\bar{H})$. Ensuite, si $g \in \pi^{-1}(\bar{H})$, il existe $h \in H$ tel que $\pi(h) = \pi(g)$. Par conséquent, $gh^{-1} \in \ker \pi = N \Rightarrow g = gh^{-1}h \in H$. On conclut que $\pi^{-1}(\bar{H}) < H$, et l'unicité est donc prouvée. Pour montrer que, si $\bar{H} \triangleleft \bar{G}$, alors $\pi^{-1}(\bar{H}) \triangleleft G$, on considère $g \in G$ et $h \in \pi^{-1}(\bar{H})$. Comme

$$\pi(ghg^{-1}) = \pi(g)\pi(h)\pi(g)^{-1} \in \bar{H},$$

il suit que $ghg^{-1} \in \pi^{-1}(\bar{H})$.

(iii) Cela est une conséquence directe des points *(i)* & *(ii)*. □

Une autre propriété importante des sous-groupes distingués est que le sous-groupe engendré par une paire de sous-groupes dont au moins un est distingué est facile à décrire.

Proposition 2.4.14. *Soit G un groupe, $K \triangleleft G$ un sous-groupe distingué et $H < G$ un sous-groupe.*

(i) L'ensemble $KH := \{kh \mid h \in H, k \in K\}$ est un sous-groupe.

(ii) Si K et H sont finis, alors

$$|KH| = \frac{|K||H|}{|K \cap H|}.$$

Démonstration. *(i)* Le fait que K soit un sous-groupe distingué de G permet de déduire la "règle de commutation" suivante : pour tout $k \in K$ et $h \in H$ il existe $c_h(k) \in K$ tel que

$$hk = c_h(k)h.$$

En effet, il suffit de prendre $c_h(k) = hkh^{-1} \in K$. Alors, pour tout $kh, k'h' \in KH$, on a

$$khk'h' = kc_h(k')hh' \in KH.$$

De même, pour tout $kh \in KH$, on a

$$(kh)^{-1} = h^{-1}k^{-1} = c_{h^{-1}}(k^{-1})h^{-1} \in KH.$$

Donc KH est bien un sous-groupe de G.

(*ii*) Considérons

$$\mu : K \times H \to KH$$
$$(k, h) \mapsto kh.$$

Par définition, μ est surjective. Dans chaque image réciproque $\mu^{-1}(kh)$, il y a précisément $|K \cap H|$ éléments. Pour le montrer, il suffit de vérifier que

$$\delta : K \cap H \to \mu^{-1}(kh)$$
$$g \mapsto (kg, g^{-1}h)$$

est une bijection. En effet, si $k'h' = kh$, alors $k^{-1}k' = hh'^{-1} \in K \cap H$, et pour $g := k^{-1}k' = hh'^{-1}$ on trouve $\delta(g) = (k', h')$, ce qui implique que δ est surjective. De plus, si $\delta(g) = \delta(g')$, alors en particulier $kg = kg'$ et donc $g = g'$, ce qui implique que δ est injective. Comme

$$K \times H = \bigsqcup_{kh \in KH} \mu^{-1}(kh),$$

on déduit que

$$|K \times H| = |KH||K \cap H|. \qquad \square$$

Exemple 2.4.15. (*i*) Considérons $G = \mathscr{D}_n$ pour $n > 1$, avec $K = \langle R \rangle$ et $H = \langle S \rangle$. La définition du groupe diédral $\mathscr{D}_n$ qu'on a donné dans l'Exemple 2.1.1.(*iii*) montre que $G = KH$. Dans ce cas, $K \cap H = \{I_2\}$.

(*ii*) Considérons $G = \mathrm{GL}_n(\mathbb{C})$, $K = \mathrm{SL}_n(\mathbb{C})$ et $H = \{\lambda I_n \in G \mid \lambda \in \mathbb{C}^\times\}$. Alors $G = KH$, mais $K \cap H = \{\lambda I_n \mid \lambda^n = 1\} \cong \boldsymbol{\mu}_n$.

2.5. **Produits semi-directs.** On introduit maintenant une généralisation de la notion de produit direct.

Définition 2.5.1. Soit G un groupe, $K \triangleleft G$ un sous-groupe distingué et $H < G$ un sous-groupe. Si $G = KH$ et $K \cap H = \{e\}$, on dira que G est le *produit semi-direct* de K et H. Pour indiquer que G est produit semi-direct de K (qui est distingué) et H, on écrira

$$G = K \rtimes H.$$

Exemple 2.5.2. $\mathscr{D}_n = \langle R \rangle \rtimes \langle S \rangle$.

Une autre façon de voir les produit semi-directs est la suivante.

Théorème 2.5.3. *Soit G un groupe, $K \triangleleft G$ un sous-groupe distingué et $H < G$ un sous-groupe.*

(*i*) *Si $G = K \rtimes H$, alors la projection canonique $\pi : G \to G/K$ se restreint à un isomorphisme $\pi : H \to G/K$.*

(*ii*) *Si la projection canonique $\pi : G \to G/K$ se restreint à un isomorphisme $\pi : H \to G/K$, alors $G = K \rtimes H$.*

Avant de prouver le Théorème 2.5.3, on remarque que le fait de demander que $\pi : H \to G/K$ soit un isomorphisme est équivalente à demander que H soit à la fois un quotient et un sous-groupe de G, et que dans ce cas K sera un "complément" de H dans G.

Démonstration. (*i*) On sait que $\ker \pi = K$. Comme, par hypothèse, $K \cap H = \{e\}$, on déduit que la restriction de π à H est injective. De plus, comme chaque élément de G est de la forme kh avec $k \in K$ et $h \in H$, il suit que la restriction de π à H est surjective, et $\pi : H \to G/K$ est un isomorphisme.

(*ii*) On commence par montrer que $K \cap H = \{e\}$. En effet, si $h \in K \cap H$, alors $\pi(h) = [e]$, et puisque $\pi : H \to G/K$ est injectif, alors $h = e$. Ensuite, pour tout $g \in G$, comme $\pi : H \to G/K$ est surjectif, il existe $h \in H$ tel que $\pi(g) = \pi(h)$. On déduit que $Kg = Kh$, donc il existe $k \in K$ tel que $g = kh$. □

De ce point de vue, il est souvent facile d'identifier d'autres produits semi-directs.

Exemple 2.5.4. Comme vu dans l'Exemple 2.4.12.(*ii*), l'homomorphisme surjectif $\det : \mathrm{GL}_n(\Bbbk) \to \Bbbk^\times$ induit un isomorphisme $\mathrm{GL}_n(\Bbbk)/\mathrm{SL}_n(\Bbbk) \cong \Bbbk^\times$. Si on pose

$$H := \left\{ \begin{pmatrix} \lambda & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix} \;\middle|\; \lambda \in \Bbbk^\times \right\},$$

alors $\det : H \to \Bbbk^\times$ est un isomorphisme, et donc $\mathrm{GL}_n(\Bbbk) = \mathrm{SL}_n(\Bbbk) \rtimes H$.

Exemple 2.5.5. Un *drapeau de* $\Bbbk^n$ est un n-uplet $(F_1, \dots, F_n)$ de sous-espaces vectoriels de $\Bbbk^n$ tel que :

(*i*) $F_i \subset F_{i+1}$ pour tout $1 \leqslant i \leqslant n-1$;

(*ii*) $\dim F_i = i$ pour tout $1 \leqslant i \leqslant n$.

Soit X l'ensemble des drapeaux de $\Bbbk^n$. Si $(F_1, \dots, F_n) \in X$ est un drapeau et $g \in \mathrm{GL}_n(\Bbbk)$ est un endomorphisme inversible, alors $(g(F_1), \dots, g(F_n))$ est encore un drapeau. On obtient ainsi une action de $\mathrm{GL}_n(\Bbbk)$ sur X. La base canonique de $\Bbbk^n$ induit un drapeau canonique $(E_1, \dots, E_n)$, où $E_i = \mathrm{vect}_\Bbbk\{e_1, \dots, e_i\}$. C'est facile de voir que $\mathrm{st}_{(E_1,\dots,E_n)}$ est le sous-groupe

$$B := \left\{ \begin{pmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,n} \\ 0 & b_{2,2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & b_{n-1,n} \\ 0 & \cdots & 0 & b_{n,n} \end{pmatrix} \;\middle|\; \begin{array}{ll} b_{i,j} \in \Bbbk & \forall\, 1 \leqslant i < j \leqslant n \\ b_{i,i} \in \Bbbk^\times & \forall\, 1 \leqslant i \leqslant n \end{array} \right\} < \mathrm{GL}_n(\Bbbk)$$

des matrices triangulaires supérieures inversibles. Ensuite, on considère le sous-groupe

$$T := \left\{ \begin{pmatrix} t_1 & 0 & \cdots & 0 \\ 0 & t_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & t_n \end{pmatrix} \;\middle|\; t_i \in \Bbbk^\times \quad \forall\, 1 \leqslant i \leqslant n \right\} < B < \mathrm{GL}_n(\Bbbk)$$

des matrices diagonales inversibles. Un simple calcul montre que

$$\pi : B \to T$$
$$\begin{pmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,n} \\ 0 & b_{2,2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & b_{n-1,n} \\ 0 & \cdots & 0 & b_{n,n} \end{pmatrix} \mapsto \begin{pmatrix} b_{1,1} & 0 & \cdots & 0 \\ 0 & b_{2,2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & b_{n,n} \end{pmatrix}$$

est un homomorphisme qui se restreint à l'identité sur T, avec noyau

$$U := \left\{ \begin{pmatrix} 1 & b_{1,2} & \cdots & b_{1,n} \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & b_{n-1,n} \\ 0 & \cdots & 0 & 1 \end{pmatrix} \;\middle|\; b_{i,j} \in \Bbbk \quad \forall\, 1 \leqslant i < j \leqslant n \right\} < B < \mathrm{GL}_n(\Bbbk).$$

On en déduit que $B = U \rtimes T$.

Jusqu'ici, on n'a parlé de produit semi-direct que pour des sous-groupes d'un groupe donné. En revanche, pour construire le produit direct $K \times H$ de deux groupes K et H, on a le droit d'utiliser deux groupes abstraits. Il s'avère que le produit semi-direct peut être construit dans le même esprit, à partir de deux groupes K et H et d'une action par homomorphismes de H sur K, induite par un morphisme de groupes

$$\begin{aligned} \varphi : H &\to \mathrm{Aut}(K) \\ h &\mapsto \varphi_h. \end{aligned}$$

Proposition 2.5.6. *Soient K et H deux groupes, et soit $\varphi : H \to \mathrm{Aut}(K)$ un morphisme de groupes.*

(i) L'ensemble $K \times H$ admet une structure de groupe avec multiplication

$$(k,h)(k',h') := (k\varphi_h(k'), hh') \in K \times H$$

pour tout $(k,h),(k',h') \in K \times H$, élément neutre

$$(e,e) \in K \times H,$$

et inverse

$$(k,h)^{-1} := (\varphi_{h^{-1}}(k^{-1}), h^{-1}) \in K \times H$$

pour tout $(k,h) \in K \times H$. Ce groupe est noté $K \rtimes_\varphi H$.

(ii) Si $\tilde{K} := K \times \{e\}$ et $\tilde{H} := \{e\} \times H$, alors $\tilde{K} \lhd K \rtimes_\varphi H$ et $\tilde{H} < K \rtimes_\varphi H$, et si $\tilde{k} := (k,e)$ et $\tilde{h} := (e,h)$ pour tout $k \in K$ et $h \in H$, alors

$$\begin{aligned} K &\to \tilde{K}, & H &\to \tilde{H} \\ k &\mapsto \tilde{k} & h &\mapsto \tilde{h} \end{aligned}$$

sont des isomorphismes de groupes, et $K \rtimes_\varphi H = \tilde{K} \rtimes \tilde{H}$ au sens de la Définition 2.5.1. En particulier, la projection $\pi : K \rtimes_\varphi H \to \tilde{H}$ est un morphisme de groupes surjectif, et $\tilde{K}$ est son noyau.

(iii) Soient K' et H' deux groupes, $\varphi' : H \to \mathrm{Aut}(K')$ un morphisme de groupes, et $f : K \to K'$ et $g : H \to H'$ deux isomorphismes de groupes satisfaisants

$$\varphi'_{g(h)}(f(k)) = f(\varphi_h(k))$$

pour tout $k \in K$ et $h \in H$. Alors

$$\begin{aligned} f \rtimes g : K \rtimes_\varphi H &\to K' \rtimes_{\varphi'} H' \\ (k,h) &\mapsto (f(k), g(h)) \end{aligned}$$

est un isomorphisme de groupes.

Démonstration. *(i)* Montrons l'associativité du produit de $K \rtimes_\varphi H$. D'une part, pour tout $k,k',k'' \in K$ et $h,h',h'' \in H$ on a

$$((k,h)(k',h'))(k'',h'') = (k\varphi_h(k'), hh')(k'',h'') = (k\varphi_h(k')\varphi_{hh'}(k''), hh'h'').$$

D'autre part, on a

$$\begin{aligned} (k,h)((k',h')(k'',h'')) &= (k,h)(k'\varphi_{h'}(k''), h'h'') = (k\varphi_h(k'\varphi_{h'}(k'')), hh'h'') \\ &= (k\varphi_h(k')\varphi_h(\varphi_{h'}(k'')), hh'h'') = (k\varphi_h(k')\varphi_{hh'}(k''), hh'h''). \end{aligned}$$

Le reste de l'énoncé est laissé comme exercice pour le lecteur.

(*ii*) Montrons d'abord l'équation

$$\tilde{h}\tilde{k} = \tilde{\varphi}_h(k)\tilde{h}, \tag{3}$$

où $\tilde{\varphi}_h(k) = (\varphi_h(k), e)$ pour tout $k \in K$ et $h \in H$. D'une part, pour tout $k \in K$ et $h \in H$ on a

$$\tilde{k}\tilde{h} = (k, e)(e, h) = (k\varphi_e(e), eh) = (k, h).$$

D'autre part, on a

$$\tilde{h}\tilde{k} = (e, h)(k, e) = (e\varphi_h(k), he) = (\varphi_h(k), h).$$

Clairement, $\tilde{K}$ et $\tilde{H}$ sont deux sous-groupes de $K \rtimes_\varphi H$. De plus, l'équation (3) implique que

$$\tilde{h}\tilde{k}\tilde{h}^{-1} = \tilde{\varphi}_h(k)\tilde{h}\tilde{h}^{-1} = \tilde{\varphi}_h(k)$$

pour tout $k \in K$ et $h \in H$. Cela nous permet de déduire que $\tilde{K} \triangleleft K \rtimes_\varphi H$. Maintenant c'est facile de montrer que la projection canonique $\pi : K \rtimes_\varphi H \twoheadrightarrow (K \rtimes_\varphi H)/\tilde{K}$ se restreint à un isomorphisme $\pi : \tilde{H} \to (K \rtimes_\varphi H)/\tilde{K}$. Alors, grâce au Théorème 2.5.3, on obtient que $K \rtimes_\varphi H = \tilde{K} \rtimes \tilde{H}$.

(*iii*) La preuve est laissée comme exercice pour le lecteur. □

Exemple 2.5.7. On sait que $\mathscr{D}_n = \langle R \rangle \rtimes \langle S \rangle$ et que $SRS^{-1} = R^{-1}$. Considérons alors

$$\begin{aligned} \varphi : \boldsymbol{\mu}_2 &\to \mathrm{Aut}(\mathbb{Z}) \\ -1 &\mapsto -\mathrm{id}_{\mathbb{Z}}. \end{aligned}$$

On définit le *groupe diédral infini* $\mathscr{D}_\infty := \mathbb{Z} \rtimes_\varphi \boldsymbol{\mu}_2$.

Exemple 2.5.8. On a déjà rencontré de nombreux exemples de groupes finis : groupes cycliques, groupes abéliens, groupes symétriques, groupes alternés, groupes diédraux. À partir de ces groupes, grâce à la Proposition 2.5.6, on peut en construire d'autres. Le premier exemple de produit semi-direct entre groupes de ce type qui ne figure pas lui même dans la liste des groupes ci-dessus est un groupe d'ordre 12. Pour le voir, regardons les groupes d'ordre 12. On en connaît déjà plusieurs :

- ◇ $\boldsymbol{\mu}_{12} \cong \boldsymbol{\mu}_4 \times \boldsymbol{\mu}_3$;
- ◇ $\boldsymbol{\mu}_2 \times \boldsymbol{\mu}_2 \times \boldsymbol{\mu}_3 \cong \boldsymbol{\mu}_2 \times \boldsymbol{\mu}_6$;
- ◇ $\mathscr{D}_6 \cong \boldsymbol{\mu}_2 \times \mathscr{D}_3$;
- ◇ $\mathfrak{A}_4$.

Ce n'est pas difficile de voir que les groupes dans cette liste sont deux-à-deux non-isomorphes. Par exemple, les deux premier sont abéliens, tandis que les deux autres ne le sont pas. Parmi les deux premiers, seulement $\boldsymbol{\mu}_{12}$ est cyclique. Parmi les deux derniers, seulement $\mathscr{D}_6$ admet d'éléments d'ordre 6. Maintenant, essayons de construire des nouveaux groupes d'ordre 12 à l'aide de la Proposition 2.5.6. Pour ce faire, on pose $\zeta_k := e^{\frac{2\pi \mathrm{i}}{k}}$, et on fait la remarque suivante : $|\mathrm{Aut}(\boldsymbol{\mu}_k)| = \varphi(k)$, où φ est la fonction indicatrice d'Euler. En effet, $\boldsymbol{\mu}_k = \langle \zeta_k \rangle$ et, pour construire un automorphisme de $\boldsymbol{\mu}_k$, il suffit de choisir un élément d'ordre k dans $\boldsymbol{\mu}_k$ comme image de ζ_k. Comme il y en a exactement $\varphi(k)$, on peut conclure.

◇ *Produits semi-directs* $\boldsymbol{\mu}_3 \rtimes_\varphi \boldsymbol{\mu}_4$ *:* comme $\mathrm{Aut}(\boldsymbol{\mu}_3) = \{\mathrm{id}, \_^{-1}\} \cong \boldsymbol{\mu}_2$, on a un seul morphisme de groupes non trivial de $\boldsymbol{\mu}_4$ vers $\mathrm{Aut}(\boldsymbol{\mu}_3)$, c'est-à-dire

$$\begin{aligned} \varphi : \boldsymbol{\mu}_4 &\to \mathrm{Aut}(\boldsymbol{\mu}_3) \\ \zeta_4 &\mapsto \_^{-1}. \end{aligned}$$

Soit alors $k := (\zeta_3, 1) \in \boldsymbol{\mu}_3 \rtimes_\varphi \boldsymbol{\mu}_4$ et $h := (1, \zeta_4) \in \boldsymbol{\mu}_3 \rtimes_\varphi \boldsymbol{\mu}_4$. La règle de commutation est alors

$$hk = k^{-1}h.$$

Comme $\boldsymbol{\mu}_3 \rtimes_\varphi \boldsymbol{\mu}_4$ n'est pas abélien, il n'est pas isomorphe ni à $\boldsymbol{\mu}_{12}$, ni à $\boldsymbol{\mu}_2^2 \times \boldsymbol{\mu}_3$. En calculant les ordres de tous les éléments de $\boldsymbol{\mu}_3 \rtimes_\varphi \boldsymbol{\mu}_4$, on déduit qu'il en existe un unique d'ordre 2, à savoir h^2. Donc $\boldsymbol{\mu}_3 \rtimes_\varphi \boldsymbol{\mu}_4$ n'est pas isomorphisme ni à $\mathscr{D}_6$ (car $R^i S$ est d'ordre 2 pour tout $0 \leqslant i < 6$), ni à $\mathfrak{A}_4$ (car les 3 éléments non triviaux du groupe de Klein $\mathfrak{V}$ ont tous ordre 2). On a ainsi trouvé un nouveau groupe d'ordre 12.

◇ *Produits semi-directs $\boldsymbol{\mu}_2^2 \rtimes_\varphi \boldsymbol{\mu}_3$:* si on identifie $\boldsymbol{\mu}_2^2 \cong \mathfrak{V}$, est si on pose

$$x := (1\ 2)(3\ 4), \qquad y := (1\ 4)(2\ 3), \qquad z := (1\ 3)(2\ 4),$$

alors il est facile de voir que $\mathrm{Aut}(\mathfrak{V}) \cong \mathfrak{S}_{\{x,y,z\}} \cong \mathfrak{S}_3$. Considérons le morphisme de groupes

$$\begin{aligned} \varphi : \boldsymbol{\mu}_3 &\to \mathrm{Aut}(\mathfrak{V}) \cong \mathfrak{S}_{\{x,y,z\}} \\ \zeta_3 &\mapsto (x\ y\ z). \end{aligned}$$

On se demande si $\mathfrak{V} \rtimes_\varphi \boldsymbol{\mu}_3$ est déjà dans la liste. On remarque alors que $\mathfrak{V} \rtimes_\varphi \boldsymbol{\mu}_3$ contient un sous-groupe distingué isomorphe à $\mathfrak{V}$, tout comme $\mathfrak{A}_4$. De plus, il est facile de voir que la projection canonique $\pi : \mathfrak{A}_4 \twoheadrightarrow \mathfrak{A}_4/\mathfrak{V}$ induit un isomorphisme $\pi : \langle (1\ 2\ 3) \rangle \to \mathfrak{A}_4/\mathfrak{V}$. Grâce au Théorème 2.5.3, on déduit que $\mathfrak{A}_4 = \mathfrak{V} \rtimes \langle (1\ 2\ 3) \rangle$. On peut alors trouver un isomorphisme entre $\mathfrak{V} \rtimes_\varphi \boldsymbol{\mu}_3$ et $\mathfrak{A}_4$ en utilisant la Proposition 2.5.6.(*iii*) et en prenant comme $f : \mathfrak{V} \to \mathfrak{V}$ l'identité, en posant

$$\begin{aligned} g : \boldsymbol{\mu}_3 &\to \langle (1\ 2\ 3) \rangle \\ \zeta_3^k &\mapsto (1\ 2\ 3)^k, \end{aligned}$$

et on vérifiant que

$$(1\ 2\ 3)x(1\ 3\ 2) = y, \qquad (1\ 2\ 3)y(1\ 3\ 2) = z, \qquad (1\ 2\ 3)z(1\ 3\ 2) = x.$$

Donc $\mathfrak{V} \rtimes_\varphi \boldsymbol{\mu}_3$ est isomorphe à $\mathfrak{A}_4$, qui est déjà dans la liste, et il est facile de voir que le même vaut pour le seul autre morphisme de groupes de $\boldsymbol{\mu}_3$ vers $\mathrm{Aut}(\mathfrak{V})$.

On peut en effet montrer (mais on ne le fera pas) que les 5 groupes d'ordre 12 qu'on a trouvé jusqu'ici forment une liste complète des classes d'isomorphisme de groupes d'ordre 12, qui sont donc

$$\boldsymbol{\mu}_{12}, \qquad \boldsymbol{\mu}_2^2 \times \boldsymbol{\mu}_3, \qquad \mathscr{D}_6, \qquad \mathfrak{A}_4, \qquad \boldsymbol{\mu}_3 \rtimes \boldsymbol{\mu}_4.$$

2.6. **Théorèmes de Sylow.** On a introduit la notion de p-groupe fini dans la Section 2.3, voir la Définition 2.3.11.

Définition 2.6.1. Un p-groupe fini P est un *p-sous-groupe de Sylow* d'un groupe fini G, ou simplement un *p-Sylow* de G, si $P < G$ et $[G : P]$ est premier avec p. Autrement dit, si $|G| = p^a m$ avec $\mathrm{pgcd}(p, m) = 1$, alors $P < G$ est un p-Sylow de G si $|P| = p^a$.

Exemple 2.6.2. Le groupe U introduit dans l'Exemple 2.5.5 est un p-sous-groupe de Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$. En effet, il est facile de construire une bijection

$$\mathbb{F}_p^{n-1} \times \mathbb{F}_p^{n-2} \times \ldots \times \mathbb{F}_p \to U,$$

d'où $|U| = p^{\frac{n(n-1)}{2}}$. Ensuite, on sait que

$$|\mathrm{GL}_n(\mathbb{F}_p)| = p^{\frac{n(n-1)}{2}} \prod_{k=1}^{n} (p^k - 1),$$

voir l'Exercice 7.(*i*) du TD2. Comme clairement $\mathrm{pgcd}(p^k - 1, p) = 1$ pour tout $1 \leqslant k \leqslant n$, on peut conclure.

Théorème 2.6.3 (Théorèmes de Sylow)**.** *Soit G un groupe d'ordre $p^a m$ avec p premier et* $\mathrm{pgcd}(p,m)=1$.

(*i*) *G admet un p-Sylow.*

(*ii*) *Tous les p-Sylows de G sont conjugués entre eux.*

(*iii*) *Si $H<G$ est un p-groupe, alors H est contenu dans un p-Sylow.*

Soit $\mathrm{Syl}_p(G)$ l'ensemble des p-Sylows de G, et soit $n_p=|\mathrm{Syl}_p(G)|$ son cardinal.

(*iv*) $n_p \mid m$.

(*v*) $n_p \equiv 1 \pmod p$.

La preuve de l'existence d'un sous-groupe de Sylow sera conséquence du résultat suivant.

Proposition 2.6.4. *Si G est sous-groupe d'un groupe fini $\tilde{G}$, et si $\tilde{P}$ est un est un p-Sylow de $\tilde{G}$, alors il existe $\tilde{g}\in\tilde{G}$ tel que $P=\tilde{g}\tilde{P}\tilde{g}^{-1}\cap G$ est un p-Sylow de G.*

En revanche, la Proposition 2.6.4 sera une conséquence du résultat suivant.

Lemme 2.6.5. *Soit X un G-ensemble fini. Si $|X|$ est premier avec p, alors il existe une orbite dont le cardinal est premier avec p.*

Démonstration. Soient $G\cdot x_1,\dots,G\cdot x_k$ les orbites distinctes. Si, par l'absurde, on avait $|G\cdot x_i|\equiv 0 \pmod p$ pour tout $1\leqslant i\leqslant k$, on aurait

$$|X|=\sum_{i=1}^{k}|G\cdot x_i|\equiv 0 \pmod p,$$

ce qui serait une contradiction. □

Démonstration de la Propostion 2.6.4. On considère le $\tilde{G}$-ensemble $X=\tilde{G}/\tilde{P}$. On sait que $p\nmid|X|$ et que le stabilisateur d'un point $\tilde{g}\tilde{P}$ est $\tilde{g}\tilde{P}\tilde{g}^{-1}$, voir l'Exercice 10 du TD1. Maintenant, on fait agir G sur X et on considère une orbite $G\cdot\tilde{g}\tilde{P}$ telle que $p\nmid|G\cdot\tilde{g}\tilde{P}|$, qui existe grâce au Lemme 2.6.5. Si P désigne le stabilisateur $G_{\tilde{g}\tilde{P}}$, alors $p\nmid[G:P]$ et $P=\tilde{g}\tilde{P}\tilde{g}^{-1}\cap G$. Cela implique que P est un p-Sylow. □

Démonstration du Théorème 2.6.3. (*i*) Grâce au Théorème 2.2.9, tout groupe fini est isomorphe à un sous-groupe d'un groupe de permutations $\mathfrak{S}_n$ pour quelque $n\in\mathbb{N}$. En revanche, $\mathfrak{S}_n$ est isomorphe à un sous-groupe de $\mathrm{GL}_n(\mathbb{F}_p)$. En effet, soit

$$\begin{aligned} w:\mathfrak{S}_n &\to \mathrm{GL}_n(\mathbb{F}_p)\\ \sigma &\mapsto w_\sigma \end{aligned}$$

la fonction qui envoie toute permutation sur la matrice de permutation correspondante, définie par

$$w_\sigma(e_i)=e_{\sigma(i)}$$

pour tout $1\leqslant i\leqslant n$. On peut voir facilement que w est un morphisme de groupes injectif, et donc que $w:\mathfrak{S}_n\to w(\mathfrak{S}_n)<\mathrm{GL}_n(\mathbb{F}_p)$ est un isomorphisme. On peut alors appliquer la Proposition 2.6.4 à l'Exemple 2.6.2 et poser $\tilde{G}=\mathrm{GL}_n(\mathbb{F}_p)$ et $\tilde{P}=U$ pour montrer que G possède un p-Sylow.

(*ii*) Soient P et P' des p-Sylows de G. Grâce à la Proposition 2.6.4, il existe $g\in G$ tel que $gPg^{-1}\cap P'$ est un p-Sylow de P'. Mais P' est l'unique p-Sylow de P'. Il suit donc que $P'\subset gPg^{-1}$. Comme $|gPg^{-1}|=|gPg^{-1}|=p^a=|P'|$, on déduit que $gPg^{-1}=P'$.

(*iii*) Soit P un p-Sylow de G. Alors il existe $g\in G$ tel que $gPg^{-1}\cap H$ est un p-Sylow de H. Mais H est l'unique p-Sylow de H. Il suit donc que $H\subset gPg^{-1}$, et comme gPg^{-1} est un p-Sylow, on peut conclure.

(*iv*) On considère l'action par conjugaison de G sur $\mathrm{Syl}_p(G)$. D'après le point (*ii*), cette action est transitive. Soit $P \in \mathrm{Syl}_p(G)$ un p-Sylow de G quelconque. Clairement, on a $P < G_P$, et donc

$$|\mathrm{Syl}_p(G)| = [G : G_P] = \frac{[G : P]}{[G_P : P]} = \frac{m}{[G_P : P]},$$

ce qui implique que $|\mathrm{Syl}_p(G)|$ divise m.

(*v*) Cette fois on considère l'action par conjugaison de P sur $\mathrm{Syl}_p(G)$. Clairement, $P \in \mathrm{Syl}_p(G)$ est un point fixe de cette action, donc $P \cdot P = \{P\}$. Soit $P' \in \mathrm{Syl}_p(G)$ un autre p-Sylow de G. On sait que $|P \cdot P'| = |P|/|P_{P'}|$ est un diviseur de $|P|$. En particulier, soit $|P \cdot P'| \equiv 0 \pmod p$, soit $|P \cdot P'| = 1$. Si $|P \cdot P'| = 1$, alors

$$gP'g^{-1} = P' \qquad \forall\, g \in P.$$

Soit $\mathrm{N}_G(P') = \{g \in G \mid gP'g^{-1} = P'\} < G$ le normalisateur de P'. Il suit que P et P' sont contenus dans $\mathrm{N}_G(P')$, et donc ils sont des p-Sylows de $\mathrm{N}_G(P')$. D'après le point (*ii*), il existe $x \in \mathrm{N}_G(P')$ tel que $xP'x^{-1} = P$. Mais, par définition de $\mathrm{N}_G(P')$, on a que $xP'x^{-1} = P'$, et donc $P = P'$. Alors, si $P \neq P'$, on a forcement $|P \cdot P'| \equiv 0 \pmod p$. La conclusion suit de l'Exercice 2.3.12. □

Les groupes finis où tous les Sylows sont distingués sont assez simples. Pour le montrer, on a besoin d'un résultat préliminaire.

Lemme 2.6.6. *Si H et K sont des sous-groupes distingués d'un groupe G tels que $H \cap K = \{e\}$, alors $hk = kh$ pour tout $h \in H$ et $k \in K$.*

Démonstration. Il suffit de remarquer que, pour tout $h \in H$ et $k \in K$, on a

$$[h, k] := hkh^{-1}k^{-1} \in H \cap K,$$

car $kh^{-1}k^{-1} \in H \lhd G$ et $hkh^{-1} \in K \lhd G$. On déduit alors que $[h, k] = e$. □

Théorème 2.6.7. *Si $|G| = p_1^{a_1} \cdots p_\ell^{a_\ell}$ avec $\ell, a_1, \ldots, a_\ell \in \mathbb{N}$ et $p_1, \ldots, p_\ell$ premiers distincts, et si $\mathrm{Syl}_{p_i}(G) = \{P_i\}$ pour tout $1 \leqslant i \leqslant \ell$, alors*

$$\varphi : P_1 \times \ldots \times P_\ell \to G$$
$$(x_1, \ldots, x_\ell) \mapsto x_1 \cdots x_\ell$$

est un isomorphisme de groupes.

Démonstration. Si $i \neq j$, alors clairement $P_i \cap P_j = \{e\}$. Ensuite, comme on sait que tous les p_i-Sylows sont conjugués entre eux, $P_i \lhd G$. Le Lemme 2.6.6 implique que, pour tout $x_i \in P_i$ et $x_j \in P_j$, on a $x_i x_j = x_j x_i$.

Pour commencer, φ est un morphisme de groupes, car

$$\varphi((x_1, \ldots, x_\ell)(y_1, \ldots, y_\ell)) = \varphi(x_1y_1, \ldots, x_\ell y_\ell) = x_1y_1 \cdots x_\ell y_\ell = x_1 \cdots x_\ell y_1 \cdots y_\ell$$
$$= \varphi(x_1, \ldots, x_\ell)\varphi(y_1, \ldots, y_\ell).$$

Ensuite, φ est injectif. En effet, si $(x_1, \ldots, x_\ell) \in \ker \varphi$, alors $x_1 \cdots x_\ell = e$. Si on pose

$$q_i := \frac{|G|}{p_i^{a_i}},$$

alors $p_i \nmid q_i$ et $p_j^{a_j} \mid q_i$ pour tout $j \neq i$. En particulier, on a

$$e = e^{q_i} = (x_1 \cdots x_\ell)^{q_i} = x_1^{q_i} \cdots x_\ell^{q_i} = x_i^{q_i}.$$

Donc $\mathrm{ord}(x_i) \mid q_i$ et $\mathrm{ord}(x_i) \mid p_i^{a_i}$, ce qui implique que $\mathrm{ord}(x_i) = 1$.

Pour finir, φ est surjectif, car

$$|\mathrm{im}\, \varphi| = |P_1 \times \ldots \times P_\ell| = |G|.$$

□

On termine cette section avec un exemple d'application du Théorème 2.6.3. Pour ce faire, on rappelle d'abord que $|\mathrm{Aut}(\boldsymbol{\mu}_n)| = \varphi(n)$, où φ est la fonction indicatrice d'Euler, comme déjà vu dans l'Exemple 2.5.8. En effet, si on pose $\zeta_n = e^{\frac{2\pi \mathrm{i}}{n}}$, et si on considère, pour tout $k \in \mathbb{Z}/n\mathbb{Z}$, le morphisme de groupes

$$\begin{aligned} f_k : \boldsymbol{\mu}_n &\to \boldsymbol{\mu}_n \\ \zeta_n &\mapsto \zeta_n^k, \end{aligned} \tag{4}$$

alors

$$\begin{aligned} f : (\mathbb{Z}/n\mathbb{Z})^\times &\to \mathrm{Aut}(\boldsymbol{\mu}_n) \\ k &\mapsto f_k \end{aligned}$$

est un isomorphisme de groupes.

Exemple 2.6.8. Si $|G| = 10$, alors $n_2 \mid 5$, donc $n_2 \in \{1, 5\}$, et $n_5 \mid 2$, donc $n_5 \in \{1, 2\}$. Mais $2 \not\equiv 1 \pmod 5$, ce qui implique que $n_5 = 1$. Soit alors $P_5 \lhd G$ l'unique 5-Sylow, et soit $P_2 < G$ un 2-Sylow. On a $G = P_5 \rtimes P_2$, car $P_5 \cap P_2 = \{e\}$ et car, par la Proposition 2.4.14,

$$|P_5 P_2| = \frac{|P_5||P_2|}{|P_5 \cap P_2|} = 10.$$

En choisissant des générateurs $P_5 = \langle x \rangle$ et $P_2 = \langle y \rangle$, on obtient un isomorphisme

$$\begin{aligned} P_5 \rtimes P_2 &\to \boldsymbol{\mu}_5 \rtimes_\varphi \boldsymbol{\mu}_2 \\ (x^i, y^j) &\mapsto (\zeta_5^i, \zeta_2^j) \end{aligned}$$

avec $\varphi : \boldsymbol{\mu}_2 \to \mathrm{Aut}(\boldsymbol{\mu}_5)$ déterminé par $\varphi_{\zeta_2}(\zeta_5) = \zeta_5^k$, où $yxy^{-1} = x^k$. En suivant la notation de l'équation (4), si on pose $f := f_2$ on obtient que $f^2 = f_4$ et que $f^3 = f_3$. Comme $\mathrm{id} = f_1$, on a que

$$\mathrm{Aut}(\boldsymbol{\mu}_5) = \{f_1, f_2, f_3, f_4\} = \{\mathrm{id}, f, f^2, f^3\} = \langle f \rangle \cong \boldsymbol{\mu}_4.$$

De plus, comme $\mathrm{ord}(\varphi(y)) \mid \mathrm{ord}(y) = 2$, on a que $\varphi \in \{\mathrm{id}, f^2\}$. Si $\varphi = \mathrm{id}$, alors $yxy^-1 = x$, et $G \cong P_5 \times P_2 \cong \boldsymbol{\mu}_{10}$. Par contre, si $\varphi = f^2$, alors $yxy^{-1} = x^4 = x^{-1}$, et $G \cong \mathscr{D}_5$.

3. Anneaux

3.1. **Exemples d'anneaux.** On rappelle d'abord des exemples importantes d'anneaux.

Exemple 3.1.1. (i) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des exemples d'anneaux intègres qu'on a déjà rencontré. À part $\mathbb{Z}$, ils sont tous des corps. Par contre, $\mathbb{Z}/n\mathbb{Z}$ est un corps si n est premier, et il n'est pas intègre autrement.

(ii) Si A est un anneau, alors les ensembles $A[X]$ et $A[X_1, \ldots, X_n]$ des polynômes à coefficients dans A sont des anneaux. On rappelle que, si $P, P' \in A[X]$ s'écrivent comme

$$P = \sum_{i=0}^{m} a_i X^i, \qquad P' = \sum_{i=0}^{m'} a'_i X^i$$

avec $a_1, \ldots, a_m, a'_1, \ldots, a'_{m'} \in A$, alors le produit $PP' \in A[X]$ est défini par

$$PP' = \sum_{i=0}^{m+m'} \sum_{j=0}^{i} a_j a'_{i-j} X^i.$$

Cela permet de définir récursivement le produit dans $A[X_1, \ldots, X_n]$ comme celui de $(A[X_1, \ldots, X_{n-1}])[X_n]$.

(*iii*) Si X est un ensemble et A est un anneau, alors l'ensemble $\mathscr{F}(X, A)$ de fonctions de X vers A est un anneau, avec

$$(f+g)(x) := f(x) + g(x), \qquad (fg)(x) := f(x)g(x)$$

pour tout $f, g \in \mathscr{F}(X, A)$ et $x \in X$.

On rappelle également des exemples importantes de morphismes d'anneaux.

Exemple 3.1.2. (*i*) Si A est un sous-anneau d'un anneau B, alors naturellement l'inclusion $\iota : A \hookrightarrow B$ est un morphisme d'anneau.

(*ii*) Si A est un anneau, alors le morphisme caractéristique $\chi : \mathbb{Z} \to A$ est l'unique morphisme d'anneau de $\mathbb{Z}$ vers A, vu que

$$\chi(n) = \chi(1 + \ldots + 1) = \chi(1) + \ldots + \chi(1) = 1 + \ldots + 1, \qquad \chi(-n) = -\chi(n)$$

pour tout $n \in \mathbb{N}$.

(*iii*) Si A est un anneau, alors pour tout $a \in A$ l'évaluation

$$\begin{aligned} \varepsilon_a : \mathbb{Z}[X] &\to A \\ P(X) &\mapsto P(a) \end{aligned}$$

est un morphisme d'anneaux.

3.2. **Algèbres.** Soit A un anneau.

Définition 3.2.1. Une *A-algèbre* est un anneau B muni d'un morphisme d'anneaux $f : A \to B$.

Exemple 3.2.2. (*i*) Si A est un sous-anneau d'un anneau B, alors B est une A-algèbre grâce à l'inclusion $\iota : A \hookrightarrow B$.

(*ii*) Si A est un anneau, alors A est une $\mathbb{Z}$-algèbre grâce au morphisme caractéristique $\chi : \mathbb{Z} \to A$.

(*iii*) $\mathbb{Z}/2\mathbb{Z}$ **n'est pas une $\mathbb{Q}$-algèbre**, car il n'existe aucun morphisme d'anneaux $f : \mathbb{Q} \to \mathbb{Z}/2\mathbb{Z}$. En effet, si f était un tel morphisme, alors on aurait

$$f(1) = f(2)f\left(\frac{1}{2}\right) = (f(1) + f(1))f\left(\frac{1}{2}\right) = (1+1)f\left(\frac{1}{2}\right) = 0,$$

ce qui est interdit.

Dans une A-algèbre B, on peut multiplier les éléments de B par des scalaires de A, en posant

$$ab := f(a)b$$

pour tout $a \in A$ et $b \in B$. On supprimera alors souvent le morphisme $f : A \to B$ de la notation, et on traitera les éléments de A comme des éléments de B en le confondant avec leurs images par f (même si f pourrait ne pas être injectif).

Définition 3.2.3. Si B et B' sont deux A-algèbres, un *morphisme de A-algèbres* est un morphisme d'anneaux $g : B \to B'$ satisfaisant $g \circ f = f'$.

Remarque 3.2.4. Un morphisme d'anneaux $g : B \to B'$ entre A-algèbres est un morphisme de A-algèbres si et seulement si il est A-linéaire, c'est-à-dire si et seulement si

$$g(ab) = ag(b) \tag{5}$$

pour tout $a \in A$ et $b \in B$.

Voilà la propriété universelle satisfaite par les anneaux des polynômes.

Théorème 3.2.5. *Si B est une A-algèbre, et si $\mathrm{Hom}_A(A[X_1,\dots,X_n],B)$ est l'ensemble des morphismes de A-algèbres de $A[X_1,\dots,X_n]$ vers B, alors*

$$\begin{aligned}\Phi : \mathrm{Hom}_A(A[X_1,\dots,X_n],B) &\to B\times\dots\times B\\ \varphi &\mapsto (\varphi(X_1),\dots,\varphi(X_n))\end{aligned}$$

est une bijection.

Grâce à ce résultat, pour définir un morphisme de A-algèbres de $A[X_1,\dots,X_n]$ vers B il suffit de choisir l'image $b_i\in B$ du monôme $X_i\in A[X_1,\dots,X_n]$ pour tout $1\leqslant i\leqslant n$. En effet, cela va déterminer uniquement l'image de tout polynôme $P\in A[X_1,\dots,X_n]$, et tout choix est possible.

Démonstration. Montrons d'abord que Φ est injective. Si $\Phi(\varphi)=\Phi(\varphi')$, alors $\varphi(X_i)=\varphi'(X_i)$ pour tout $1\leqslant i\leqslant n$. Il suit que, pour tout $\underline{i}=(i_1,\dots,i_n)\in\mathbb{N}^n$, on a

$$\varphi(X)^{\underline{i}} := \varphi(X_1)^{i_1}\cdots\varphi(X_n)^{i_n} = \varphi'(X_1)^{i_1}\cdots\varphi'(X_n)^{i_n} =: \varphi'(X)^{\underline{i}}.$$

Alors, pour tout

$$P=\sum_{\underline{i}} a_{\underline{i}}X^{\underline{i}}\in A[X_1,\dots,X_n],\qquad \underline{i}=(i_1,\dots,i_n)\in\mathbb{N}^n,\qquad X^{\underline{i}}=X_1^{i_1}\cdots X_n^{i_n},$$

on a

$$\begin{aligned}\varphi(P)=\varphi\left(\sum_{\underline{i}} a_{\underline{i}}X^{\underline{i}}\right)&=\sum_{\underline{i}}\varphi\left(a_{\underline{i}}X^{\underline{i}}\right)=\sum_{\underline{i}}a_{\underline{i}}\varphi\left(X^{\underline{i}}\right)=\sum_{\underline{i}}a_{\underline{i}}\varphi(X)^{\underline{i}}\\ &=\sum_{\underline{i}}a_{\underline{i}}\varphi'(X)^{\underline{i}}=\dots=\varphi'(P),\end{aligned}$$

où on utilise, dans l'ordre, le fait que tout morphisme de A-algèbres préserve l'addition, la multiplication par scalaire, et le produit. Cela implique que $\varphi=\varphi'$, donc Φ est injective.

Pour montrer que Φ est surjective, considérons $\underline{b}=(b_1,\dots,b_n)\in B\times\dots\times B$. On va montrer que l'évaluation

$$\begin{aligned}\varepsilon_{\underline{b}} : A[X_1,\dots,X_n] &\to B\\ P(X_1,\dots,X_n) &\mapsto P(b_1,\dots,b_n)\end{aligned}$$

est un morphisme de A-algèbres. On aura alors que $\underline{b}=\Phi(\varepsilon_{\underline{b}})\in\mathrm{im}\,\Phi$. On remarque tout d'abord que, pour tout $1\leqslant k\leqslant n$ et

$$P=\sum_{i=0}^{m}a_iX_k^i\in A[X_1,\dots,X_k]=(A[X_1,\dots,X_{k-1}])[X_k],\quad a_i\in A[X_1,\dots,X_{k-1}],$$

on a la relation de récurrence

$$\varepsilon_{(b_1,\dots,b_k)}(P)=\sum_{i=0}^{m}\varepsilon_{(b_1,\dots,b_{k-1})}(a_i)b_k^i.$$

On peut montrer alors que $\varepsilon_{(b_1,\dots,b_k)}$ est un morphisme de A-algèbres par récurrence sur k. Pour l'initialisation en $k=0$, l'énoncé est évident, car $\mathrm{ev}_{\varnothing}(a)=a\in B$ pour tout $a\in A$ (en identifiant, comme d'habitude, tout élément de A avec son image dans B par le morphisme d'anneau $f:A\to B$, qui est en particulier un morphisme de A-algèbres). Pour l'hérédité de l'énoncé, et pour tout

$$P=\sum_{i=0}^{m}a_iX_k^i,P'=\sum_{i=0}^{m'}a_i'X_k^i\in(A[X_1,\dots,X_{k-1}])[X_k],\quad a_i,a_i'\in A[X_1,\dots,X_{k-1}],$$

et $a \in A$, on a clairement que

$$\begin{aligned}
\varepsilon_{(b_1,\ldots,b_k)}(P+P') &= \varepsilon_{(b_1,\ldots,b_k)}\left(\sum_{i=0}^{\max(m,m')}(a_i+a'_i)X_k^i\right)\\
&= \sum_{i=0}^{\max(m,m')}\varepsilon_{(b_1,\ldots,b_{k-1})}(a_i+a'_i)b_k^i\\
&= \sum_{i=0}^{\max(m,m')}\varepsilon_{(b_1,\ldots,b_{k-1})}(a_i)+\varepsilon_{(b_1,\ldots,b_{k-1})}(a'_i)b_k^i\\
&= \varepsilon_{(b_1,\ldots,b_k)}(P)+\varepsilon_{(b_1,\ldots,b_k)}(P'),\\
\varepsilon_{(b_1,\ldots,b_k)}(PP') &= \varepsilon_{(b_1,\ldots,b_k)}\left(\sum_{i=0}^{m+m'}\sum_{j=0}^{i}(a_ja'_{i-j})X_k^i\right)\\
&= \sum_{i=0}^{m+m'}\sum_{j=0}^{i}\varepsilon_{(b_1,\ldots,b_{k-1})}(a_ja'_{i-j})b_k^i\\
&= \sum_{i=0}^{m+m'}\sum_{j=0}^{i}\varepsilon_{(b_1,\ldots,b_{k-1})}(a_j)\varepsilon_{(b_1,\ldots,b_{k-1})}(a'_{i-j})b_k^i\\
&= \varepsilon_{(b_1,\ldots,b_k)}(P)\varepsilon_{(b_1,\ldots,b_k)}(P'),\\
\varepsilon_{(b_1,\ldots,b_k)}(1) &= 1,\\
\varepsilon_{(b_1,\ldots,b_k)}(aP) &= \varepsilon_{(b_1,\ldots,b_k)}\left(\sum_{i=0}^{m}aa_iX_k^i\right)\\
&= \sum_{i=0}^{m}\varepsilon_{(b_1,\ldots,b_{k-1})}(aa_i)b_k^i\\
&= \sum_{i=0}^{m}a\varepsilon_{(b_1,\ldots,b_{k-1})}(a_i)b_k^i\\
&= a\varepsilon_{(b_1,\ldots,b_k)}(P),
\end{aligned}$$

où on utilise, dans l'ordre, le fait que tout morphisme de A-algèbres préserve l'addition, le produit, l'unité, et la multiplication par scalaire. □

Définition 3.2.6. Soit B une A-algèbre, soit $\underline{b} = (b_1, \ldots, b_n) \in B \times \ldots \times B$, et soit

$$\begin{aligned}
\varepsilon_{\underline{b}} : A[X_1, \ldots, X_n] &\to B\\
X_i &\mapsto b_i
\end{aligned}$$

l'évaluation correspondante. L'anneau

$$A[b_1, \ldots, b_n] := \operatorname{im} \varepsilon_{\underline{b}}$$

est la *sous-A-algèbre* de B engendrée par $b_1, \ldots, b_n$.

Exemple 3.2.7. Plein d'anneaux peuvent être décrits de cette manière, comme par exemple $\mathbb{Z}[\sqrt{2}], \mathbb{Z}[\sqrt{3}] \subset \mathbb{R}$, ou même $\mathbb{Z}[\sqrt{-5}] \subset \mathbb{C}$.

3.3. **Quotients.** Si A est un anneau et $I \subset A$ est un idéal, alors A/I est naturellement un groupe par rapport à l'addition. En effet, I est automatiquement un sous-groupe distingué de A, car A est un groupe abélien. De plus, A/I admet une structure naturelle d'anneau.

Théorème 3.3.1. *Soit I un idéal d'un anneau A.*

(i) Le groupe A/I est un anneau, avec multiplication

$$(a+I)(b+I) = ab+I$$

pour tout $a, b \in A$, et unité $1+I$.

(ii) La projection canonique $\pi : A \twoheadrightarrow A/I$ est un morphisme d'anneaux surjectif, et son noyau est I.

Démonstration. Si $a+I = a'+I$ et $b+I = b'+I$, alors ils existent $x, y \in I$ tels que $a' = a+x$ et $b' = b+y$. Cela implique

$$a'b' = (a+x)(b+y) = ab + ay + bx + xy \in ab + I.$$

En particulier, $ab+I = a'b'+I$, et la multiplication est bien définie. Le reste de la preuve est laissée au lecteur. □

Le résultat suivant est parfois connu comme *Théorème de factorisation pour les anneaux*.

Théorème 3.3.2. *Si $f : A \to A'$ est un morphisme d'anneaux, alors $A/\ker f$ est isomorphe à $\operatorname{im} f$.*

Démonstration. Si $I = \ker f$ et $B = \operatorname{im} f$, alors le Théorème 2.4.11 fournit un isomorphisme de groupes additifs $\bar{f} : A/I \to B$, défini par $\bar{f}(a+I) = f(a)$ pour tout $a \in A$. Il s'agit en plus d'un morphisme d'anneaux, car

$$\bar{f}((a+I)(b+I)) = \bar{f}(ab+I) = f(ab) = f(a)f(b) = \bar{f}(a+I)\bar{f}(b+I),$$
$$\bar{f}(1+I) = f(1) = 1.$$ □

Tout comme pour les groupes, on a un *Théorème de correspondance pour les anneaux* aussi.

Théorème 3.3.3. *Soit I un idéal d'un anneau A, et soit $\pi : A \to \bar{A} = A/I$ la projection canonique. Pour tout idéal $\bar{J} \subset \bar{A}$, la préimage $\pi^{-1}(\bar{J}) \subset A$ est l'unique idéal $J \subset A$ satisfaisant $I \subset J$ et $\pi(J) = \bar{J}$. En particulier, l'ensemble des idéaux de A contenants I est en bijection avec l'ensemble des idéaux de $\bar{A}$.*

Le preuve est identique à celle du Théorème 2.4.13, et elle est laissée au lecteur.

3.4. **Idéaux premiers et maximaux.**

Définition 3.4.1. Un idéal I d'un anneau A satisfaisant $I \neq A$ est *premier* si A/I est intègre, et il est *maximal* si A/I est un corps.

Remarque 3.4.2. Tout idéal premier est maximal.

Remarque 3.4.3. Un anneau A est un corps si et seulement si ses seuls idéaux sont $\{0\}$ et A. En effet, d'une part, si A est un corps et $I \subset A$ est un idéal, alors soit $I = \{0\}$, soit il existe $x \in I \setminus \{0\}$, ce qui implique $1 = xx^{-1} \in I$. D'autre part, si les seuls idéaux de A sont $\{0\}$ et A, alors pour tout $x \neq 0$ on a $(x) = A$, ce qui implique qu'il existe $y \in A$ tel que $1 = xy \in I$. Une conséquence directe de cette caractérisation est que tout morphisme d'anneaux $f : \Bbbk \to A$ est injectif, car $f(1) = 1$ implique $\ker f \neq \Bbbk$.

Exercice 3.4.4 (Exercice 1, TD4)**.** Soit I un idéal d'un anneau A satisfaisant $I \neq A$.

(i) Montrer que I est premier si et seulement si, pour tout $x, y \in A$, on a $xy \in I \Rightarrow x \in I$ ou $y \in I$.

(ii) Montrer que I est maximal si et seulement si, pour tout idéal $J \subset A$, on a $I \subset J \Rightarrow J = I$ ou $J = A$.

Proposition 3.4.5. *Si $P \in \Bbbk[X]$ est un polynôme de degré $m > 0$, alors l'anneau $A := \Bbbk[X]/(P)$ est une $\Bbbk$-algèbre de dimension m, et une base est donnée par*

$$\{1 + (P), X + (P), \dots, X^{m-1} + (P)\}.$$

De plus, les conditions suivantes sont équivalentes.

(*i*) *L'anneau A est un corps (c'est-à-dire, (P) est maximal).*

(*ii*) *L'anneau A est intègre (c'est-à-dire, (P) est premier).*

(*iii*) *Le polynôme P est irréductible.*

Démonstration. L'anneau A est le quotient du $\Bbbk$-espace vectoriel $\Bbbk[X]$ par le sous-espace vectoriel (P), donc il est naturellement une $\Bbbk$-algèbre. De plus, pour tout $P' \in \Bbbk[X]$, on peut considérer la division euclidienne par $P \in \Bbbk[X]$, ce qui assure l'existence de $Q, R \in \Bbbk[X]$ avec $\deg R < \deg P = m$ tels que $P' = PQ + R$. Mais alors $P' + (P) = R + (P)$, et une base de A est donnée par

$$\{1 + (P), X + (P), \dots, X^{m-1} + (P)\},$$

car tout $P' \in \Bbbk[X]$ admet un représentant de degré au plus $m - 1$ dans A.

Pour ce qui concerne le deuxième énoncé, on a les implications suivantes.

(*i*) $\Rightarrow$ (*ii*) Tout corps est intègre.

(*ii*) $\Rightarrow$ (*iii*) Si $P \in \Bbbk[X]$ n'est pas irréductible, alors il existent $Q, R \in \Bbbk[X]$ avec $\deg Q, \deg R < \deg P = m$ tels que $P = QR$. Il suit que $(Q+(P))(R+(P)) = 0+(P)$ dans A, donc A n'est pas intègre.

(*iii*) $\Rightarrow$ (*i*) Il suffit de montrer que (P) est maximal. Soit $I \subset \Bbbk[X]$ un idéal contenant (P). Comme $\Bbbk[X]$ est principal, alors il admet un générateur $Q \in \Bbbk[X]$ de I. On déduit que $Q \mid P$, donc il existe un $R \in \Bbbk[X]$ tel que $P = QR$. Soit Q est inversible, et $I = \Bbbk[X]$, soit R est inversible, et $(Q) = (P)$. □

Pour énoncer le prochain résultat, on a besoin de la définition suivante.

Définition 3.4.6. Un nombre $\alpha \in \mathbb{C}$ est *algébrique* s'il est racine d'un polynôme $P \in \mathbb{Q}[X] \setminus \{0\}$.

Corollaire 3.4.7. *Soit $\alpha \in \mathbb{C}$ un nombre algébrique. Alors l'anneau $\mathbb{Q}[\alpha] \subset \mathbb{C}$ est un corps.*

Démonstration. Soit

$$\begin{aligned} \varepsilon_\alpha : \mathbb{Q}[X] &\to \mathbb{C} \\ X &\mapsto \alpha \end{aligned}$$

le morphisme d'évaluation, et soit $(P) = \ker \varepsilon_\alpha$. Par définition de nombre algébrique, P n'est pas une constante, et donc $\deg P > 0$. Comme $\mathbb{Q}[\alpha] \cong \operatorname{im} \varphi$ est un sous-anneau de $\mathbb{C}$, ils est intègre, et donc un corps. □

3.5. **Opérations sur les idéaux.**

Exercice 3.5.1 (Exercice 4, TD4)**.** Soient I et J deux idéaux d'un anneau A.

(*i*) Montrer que

$$I + J = \{x + y \mid x \in I, y \in J\}$$

est un idéal de A qui contient $I \cup J$. Non seulement, il est le plus petit idéal de A ayant cette propriété : si K est un idéal de A et $I \cup J \subset K$, alors $I + J \subset K$.

(*ii*) Montrer que

$$IJ = \left\{ \sum_{i=1}^{n} x_i y_i \;\middle|\; n \in \mathbb{N}, x_1, \dots, x_n \in I, y_1, \dots, y_n \in J \right\}$$

est un idéal de A contenu dans $I \cap J$.

Deux idéaux I et J de A sont dit *co-maximaux* si $I + J = A$.

Théorème 3.5.2 (Théorème des restes chinois)**.** *Soient $I_1, \dots, I_n \subset A$ des idéaux d'un anneau A. Si I_i et I_j sont co-maximaux pour tout $i \neq j$, alors*

$$A/(I_1 \cdots I_n) \cong A/I_1 \times \ldots \times A/I_n.$$

Démonstration. L'énoncé peut être montré par récurrence sur $n \geqslant 2$. Pour $n = 2$, considérons le morphisme d'anneaux

$$\begin{aligned} \varphi : A &\to A/I_1 \times A/I_2 \\ a &\mapsto (a + I_1, a + I_2). \end{aligned}$$

Son noyau est $\ker \varphi = I_1 \cap I_2$. D'une part, grâce à l'Exercice 3.5.1.(ii), on a que $I_1 I_2 \subset I_1 \cap I_2$. D'autre part, comme $I_1 + I_2 = A$, ils existent $x_1 \in I_1$ et $x_2 \in I_2$ tels que $1 = x_1 + x_2$. Cela implique que $a = x_1 a + a x_2 \in I_1 I_2$ pour tout $a \in I_1 \cap I_2$, donc $I_1 \cap I_2 \subset I_1 I_2$. En d'autres termes, $\ker \varphi = I_1 I_2$. Mais $\operatorname{im} \varphi = A/I_1 \times A/I_2$ car, pour tout $a, b \in A$, on a

$$\begin{aligned} (a + I_1, b + I_2) &= (a(x_1 + x_2) + I_1, b(x_1 + x_2) + I_2) = (a x_2 + I_1, b x_1 + I_2) \\ &= \varphi(a x_2 + b x_1) \in \operatorname{im} \varphi. \end{aligned}$$

Cela établit l'initialisation. Pour ce qui concerne l'hérédité, il suffit de montrer que I_1 et $I_2 \cdots I_n$ sont co-maximaux. Par hypothèse, pour tout $2 \leqslant i \leqslant n$, il existent $x_i \in I_1$ et $y_i \in I_i$ tels que $1 = x_i + y_i$. Alors $1 + I_1 = y_i + I_1$ pour tout $2 \leqslant i \leqslant n$, ce qui implique que

$$1 + I_1 = y_2 \cdots y_n + I_1.$$

Donc il existe $x_1 \in I_1$ tel que $1 = x_1 + y_2 \cdots y_n \in I_1 + I_2 \cdots I_n$. □

Annexe A. Résultats complémentaires

A.1. **Racines de l'unité en caractéristique positive.** Dans cet annexe, on va considérer le groupe

$$\boldsymbol{\mu}_n(\mathbb{F}_p) = \{\lambda \in \mathbb{F}_p \mid \lambda^n = 1\},$$

et on va compter ses éléments, voir le Corollaire A.1.4. Pour ce faire, on aura besoin d'un peu de préparation. On commence par considérer, pour tout groupe fini G d'ordre n et tout entier naturel k, l'ensemble

$$G(k) := \{g \in G \mid \operatorname{ord}(g) = k\}.$$

Comme

$$G = \bigsqcup_{k|n} G(k),$$

on déduit que

$$n = \sum_{k|n} |G(k)|. \tag{6}$$

Lemme A.1.1. *Si $|\mathbb{F}_p^\times(k)| > 0$, alors $|\mathbb{F}_p^\times(k)| = \varphi(k)$, où φ est la fonction indicatrice d'Euler.*

Démonstration. Si $x \in \mathbb{F}_p^\times(k)$, alors tous les éléments du sous-groupe $\langle x \rangle$ engendré par x sont des racines du polynôme $X^k - 1$ dans $\mathbb{F}_p$. Comme un polynôme de degré k à coefficients dans un corps $\Bbbk$ a au plus k racines dans $\Bbbk$, et comme $|\langle x \rangle| = k$, alors $\langle x \rangle$ est l'ensemble de toutes les racines de $X^k - 1$ dans $\mathbb{F}_p$. Cela implique que $\mathbb{F}_p^\times(k) \subset \langle x \rangle$. Grâce à la Proposition 1.1.2, on a $\operatorname{ord}(x^m) = \frac{k}{\operatorname{pgcd}(k,m)}$, qui vaut k si et seulement si $\operatorname{pgcd}(k, m) = 1$. Comme $\varphi(k)$ compte exactement le nombre d'entiers $1 \leqslant m \leqslant k - 1$ tels que $\operatorname{pgcd}(k, m) = 1$, on peut conclure. □

Gâce au Lemme A.1.1, on déduit que $|\mathbb{F}_p^\times(k)| \leqslant \varphi(k)$. Alors, pour $G = \mathbb{F}_p^\times$, l'équation (6) implique

$$p-1 = \sum_{k|p-1} |\mathbb{F}_p^\times(k)| \leqslant \sum_{k|p-1} \varphi(k). \tag{7}$$

Lemme A.1.2. *Pour tout $n \in \mathbb{N}$, on a*

$$n = \sum_{k|n} \varphi(k).$$

Démonstration. Considérons l'ensemble

$$\left\{ \frac{i}{n} \;\middle|\; 1 \leqslant i \leqslant n \right\} = \bigsqcup_{k|n} \left\{ \frac{i}{k} \;\middle|\; 1 \leqslant i \leqslant k,\ \operatorname{pgcd}(k,i) = 1 \right\}.$$

De cette partition, on déduit

$$n = \left| \left\{ \frac{i}{n} \;\middle|\; 1 \leqslant i \leqslant n \right\} \right| = \sum_{k|n} \left| \left\{ \frac{i}{k} \;\middle|\; 1 \leqslant i \leqslant k,\ \operatorname{pgcd}(k,i) = 1 \right\} \right| = \sum_{k|n} \varphi(k). \quad \square$$

Théorème A.1.3. *Le groupe $\mathbb{F}_p^\times$ est cyclique.*

Démonstration. L'équation (7) et le Lemme A.1.2 impliquent que

$$p-1 = \sum_{k|p-1} |\mathbb{F}_p^\times(k)| \leqslant \sum_{k|p-1} \varphi(k) = p-1.$$

Donc $|\mathbb{F}_p^\times(k)| = \varphi(k)$ pour tout $k \mid p-1$. En particulier, $|\mathbb{F}_p^\times(p-1)| = \varphi(p-1) > 0$, et $\mathbb{F}_p^\times$ admet un élément d'ordre $p-1$. $\square$

La preuve qu'on a donné du Théorème A.1.3 est non constructive, c'est-à-dire qu'elle ne produit pas une formule de forme close pour exprimer un générateur de $\mathbb{F}_p^\times$ en fonction de p. Un tel élément de $\mathbb{F}_p^\times$ s'appelle une *racine primitive modulo n*.

Corollaire A.1.4. $|\boldsymbol{\mu}_n(\mathbb{F}_p)| = \operatorname{pgcd}(n, p-1)$.

Démonstration. Soit $r \in \mathbb{F}_p^\times$ une racine primitive modulo n, et soient $k, \ell \in \mathbb{Z}$ tels que $n = k \operatorname{pgcd}(n, p-1)$ et $p-1 = \ell \operatorname{pgcd}(n, p-1)$. En particulier, $\operatorname{pgcd}(k, \ell) = 1$. On a alors

$$\begin{aligned} (r^m)^n \equiv 1 \pmod{p} \quad &\Leftrightarrow \quad mn \equiv 0 \pmod{p-1} \\ &\Leftrightarrow \quad mk \equiv 0 \pmod{\ell} \\ &\Leftrightarrow \quad m \equiv 0 \pmod{\ell}. \end{aligned}$$

Donc il y a exactement $\operatorname{pgcd}(n, p-1)$ solutions pour cette équation. $\square$