Cours d'Algèbre 1 de L3MAG, Orsay, année 2020-2021

Nicolas Ratazzi [1]

1. nicolas.ratazzi@math.u-psud.fr

Table des matières

Bibliographie

J'indique ici quelques ouvrages de références en lien avec le cours correspondant à ce polycopié.

1. : *Algebra* de Serge Lang : ouvrage de référence en algèbre. Existe aussi en version française. Il contient tout le programme d'algèbre de L3, M1 voire un peu de M2... C'est une très jolie référence bibliographique mais assez inaccessible à votre niveau.
2. *Cours d'Algebre* de Daniel Perrin : autre ouvrage de référence ; absolument parfait pour les parties "groupes distingués et quotients, actions de groupes, théorèmes de Sylow" et "groupe symétrique". Ceci est traité dans chapitre 1 de ce livre. Le reste de ce livre est consacré à des sujets qui seront plutôt vu en M1 ou lors de la préparation à l'agrégation.
3. *Éléments de théorie des groupes* de Josette Calais. Ce classique couvre tout le cours et est d'un niveau qui me semble le bon pour le L3MAG. Seuls les chapitres 7 : "suites de composition, Jordan-Holder" et 9 : "Groupes libres, générateurs et relations, produit libre de groupes" ne seront pas traités en L3 MAG.

Chapitre 1

Entiers et congruences modulo n

1.1 Rappels ensemblistes, relation d'équivalence

Notation 1.1.1 : Soit E un ensemble. On note $\mathcal{P}(E)$ l'ensemble des parties de E. Notons que

$$X \subset E \iff X \in \mathcal{P}(E).$$

Exemple 1.1.2 $\emptyset \in \mathcal{P}(E)$; $E \in \mathcal{P}(E)$; $x \in E \Rightarrow \{x\} \in \mathcal{P}(E)$.

Définition 1.1.3 Soit E un ensemble. Une collection $\{X_i\}_{i\in I}$ de sous-ensembles de E est une *partition de E* si

1. $\forall i \neq j$, $X_i \cap X_j = \emptyset$.
2. $\bigcup_{i\in I} X_i = E$
3. $\forall i \in I, \quad X_i \neq \emptyset$.

Définition 1.1.4 Soit E un ensemble non vide. Une relation binaire $\mathcal{R}$ est une *relation d'équivalence (sur E)* si

1. (symétrie) $\forall x, y \in E, \quad x\mathcal{R}y \Rightarrow y\mathcal{R}x$.
2. (réflexivité) $\forall x \in E, \quad x\mathcal{R}x$.
3. (transitivité) $\forall x, y, z \in E, \quad (x\mathcal{R}y \text{ et } y\mathcal{R}z \Rightarrow x\mathcal{R}z)$.

Exemples 1.1.5

1. La relation d'égalité est une relation d'équivalence.
2. Sur l'ensemble $\mathbb{Z}$, si $n \in \mathbb{N}$, la relation de congruence modulo n, notée "$x = y \bmod n$", définie par $(\exists k \in \mathbb{Z}, \quad x = y + kn)$ est d'équivalence.

Définition 1.1.6 Soit E un ensemble non vide, soit $\mathcal{R}$ une relation d'équivalence sur E et soit $x \in E$. On appelle *classe d'équivalence de x* et on note $C(x)$ le sous-ensemble de E, définie par

$$C(x) := \{y \in E \mid x\mathcal{R}y\}.$$

Remarque 1.1.7 Pour tout $x \in E$, l'élément x appartient à la classe d'équivalence x.

Définition 1.1.8 Avec les notations précédentes, on note $E/\mathcal{R}$ l'ensemble des classes d'équivalence de E pour $\mathcal{R}$. C'est un sous-ensemble de $\mathcal{P}(E)$ (autrement dit un élément de $\mathcal{P}(\mathcal{P}(E))$). On appelle cet ensemble, *l'ensemble quotient (de E pour $\mathcal{R}$)*.

Notons que par construction même de $E/\mathcal{R}$, il existe une application surjective, appelée *projection canonique* (ou surjection canonique) définie par :

$$\pi \ : \ E \to E/\mathcal{R}, \quad x \mapsto \pi(x) := C(x).$$

Proposition 1.1.9 *Soit E un ensemble non vide. Une relation d'équivalence $\mathcal{R}$ étant donné, l'ensemble des classes d'équivalence pour $\mathcal{R}$ forme une partition de E. Réciproquement si on se donne une partition $(X_i)_{i\in I}$ de E, alors les X_i forment les classes d'équivalence de E pour la relation $\mathcal{R}$ définie par*

$$x\mathcal{R}y \text{ si } (\exists i \in I, \ x \in X_i \text{ et } y \in X_i)\,.$$

Démonstration : Évident □

Exemples 1.1.10

1. Soit $n \in \mathbb{N}$. Sur $E = \mathbb{Z}$, avec $x\mathcal{R}y \iff x = y \bmod n$, on a

$$C(x) = \{y \in \mathbb{Z} \mid y = x \bmod n\} = \{y \in \mathbb{Z} \mid y \in x + n\mathbb{Z}\} = x + n\mathbb{Z}.$$

   On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient. On parle de l'ensemble des *nombres entiers congrus modulo n*.

2. Deux cas particuliers au point précédent :
   (a) Si $n = 0$, alors pour tout entier $x \in \mathbb{Z}$, on a $C(x) = \{x\}$ et $\mathbb{Z}/0\mathbb{Z} = \{\{x\} \mid x \in \mathbb{Z}\}$ est naturellement en bijection avec $\mathbb{Z}$.
   (b) Si $n = 1$, alors $C(0) = \mathbb{Z}$ et donc $\mathbb{Z}/1\mathbb{Z} = \{C(0)\}$ est réduit à un élément.

   Si $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est la projection canonique, l'image d'un élément x sera notée, suivant le contexte, $x \bmod n$, $C(x)$, $\pi(x)$, voire $\bar{x}$.

3. Sur $E = \mathbb{Z} \times \mathbb{Z}^*$, avec $\mathcal{R}$ donnée par $(a, b)\mathcal{R}(c, d) \iff ad = bc$, on a

$$C((a, b)) = \{(c, d) \mid ad = bc\}.$$

   On note $\mathbb{Q}$ l'ensemble quotient. On l'appelle l'ensemble des *nombres rationnels* et on a une injection $i \ : \ \mathbb{Z} \hookrightarrow \mathbb{Q}$ donnée par $a \mapsto C((a, 1))$. Partant d'un anneau intègre commutatif A (cf. plus loin), cette construction permet de construire son corps des fractions $\mathrm{Frac}(A)$. On peut vérifier que les lois d'additions et de multiplications sur $\mathbb{Z}$ (ou A) s'étendent à $\mathbb{Q}$ (ou $\mathrm{Frac}(A)$) de sorte que l'injection i est un morphisme d'anneaux (cf. plus loin).

4. Sur $E = \{\text{suites de Cauchy } (u_n) \text{ à valeurs dans } \mathbb{Q}\}$, on définit la relation $u\mathcal{R}v$ par $\lim u_n - v_n = 0$. C'est une relation d'équivalence. On a

$$C(u) = \{u + \varepsilon \mid \varepsilon \text{ suite de rationnels tels que } \lim \varepsilon_n = 0\}.$$

   On note $\mathbb{R}$ l'ensemble quotient et on peut prouver qu'il s'agit bien de l'ensemble des réels vérifiant les propriétés que l'on lui connait. Là encore on a une injection de $\mathbb{Q}$ dans $\mathbb{R}$ fournie par $r \mapsto C((r_n))$ où (r_n) est la suite constante égale à r.

5. Soit $n \geq 1$. Sur $E = \mathbb{R}^n - \{0\}$ on pose $x\mathcal{R}y \iff \exists \lambda \in \mathbb{R}^*,\ x = \lambda y$. Cette fois on voit que
$$C(x) = \text{droite vectorielle de } \mathbb{R}^n, \text{ passant par } x, \text{ privée de } 0.$$
L'ensemble quotient est noté $\mathbb{P}^{n-1}(\mathbb{R})$ et s'appelle *l'espace projectif de dimension* $n-1$. Par exemple on a $\mathbb{P}^0(\mathbb{R}) = \{1\}$ et $\mathbb{P}^1(\mathbb{R}) = \mathbb{R} \cup \{\infty\}$ (la direction infinie étant donnée par la droite verticale, axe des ordonnées).
6. Soit $n \geq 1$, sur $E = \mathcal{M}_n(\mathbb{R})$ on peut considérer la relation d'équivalence $A\mathcal{R}B \iff \exists P \in \mathrm{GL}_n(\mathbb{R}),\ A = P^{-1}BP$. Si $A\mathcal{R}B$ on dit que A *est semblable à* B.

1.2 Le quadruplet $(\mathbb{N}, +, \times, \leq)$

Définition 1.2.1 Soit E un ensemble non vide. Une relation binaire $\mathcal{R}$ est une *relation d'ordre (sur E)* si

1. (anti-symétrie) $\forall x, y \in E,\ \ x\mathcal{R}y$ et $y\mathcal{R}x \Rightarrow x = y$.
2. (réflexivité) $\forall x \in E,\ \ x\mathcal{R}x$.
3. (transitivité) $\forall x, y, z \in E,\ \ (x\mathcal{R}y$ et $y\mathcal{R}z \Rightarrow x\mathcal{R}z)$.

Exemple 1.2.2 la relation $\leq$ est une relation d'ordre sur $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ mais la relation $<$ n'en n'est pas une (pourquoi ?).

Définition 1.2.3 Un *ensemble ordonné* est la donnée d'un couple $(E, \leq)$ constitué d'un ensemble non vide et d'une relation d'ordre. On dit que la relation $\leq$ est *totale* (et que E est *totalement ordonné*) si

$$\forall x, y \in E,\ \ x \leq y \text{ ou } y \leq x.$$

Exemple 1.2.4

1. La relation $\leq$ est une relation d'ordre totale sur $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$.
2. La relation de divisibilité $a|b$ sur $\mathbb{N}$, définie par $\exists k \in \mathbb{N},\ b = ka$ est une relation d'ordre qui n'est pas totale (par exemple 2 ne divise pas 5 et 5 ne divise pas 2).
3. Attention, la relation de divisibilité n'est pas une relation d'ordre sur $\mathbb{Z}$ (car par exemple $-1|1$ et $1|-1$ mais $1 \neq -1$).

1.2.1 Une construction axiomatique de $\mathbb{N}$

Définition 1.2.5 Soit $(E, \leq)$ un ensemble ordonné et F un sous-ensemble non vide de E. On dit que m est un *plus petit élément de* F si
$$\forall x \in F,\ m \leq x \ \text{ et } \ m \in F.$$
On définit de même la notion de *plus grand élément*. De tels éléments sont nécessairement uniques (exercice).

Pour pouvoir faire de l'arithmétique il est nécessaire de présupposer existant un ensemble ordonné $(\mathbb{N}, \leq)$ vérifiant les 3 axiomes suivants :

1. Toute partie non vide admet un plus petit élément.
2. L'ensemble $\mathbb{N}$ n'est pas majoré.
3. Toute partie majorée non vide de $\mathbb{N}$ admet un plus grand élément.

Proposition 1.2.6 *L'ensemble* $\mathbb{N}$ *est totalement ordonné.*

Démonstration : Soient $x, y \in \mathbb{N}$. L'ensemble $\{x, y\}$ étant non vide, il admet un plus petit élément donc soit $x \leq y$ soit $y \leq x$. □

Notation 1.2.7 On note 0 le plus petit élément de $\mathbb{N}$. L'ensemble $\mathbb{N}$ n'étant pas majoré on voit en particulier que $\mathbb{N} - \{0\}$ est non vide, donc admet un plus petit élément : on note 1 cet élément. Plus généralement, pour tout entier $n \in \mathbb{N}$, l'ensemble
$$S_n := \{k \in \mathbb{N} \mid n \leq k \text{ et } k \neq n\}$$
est non vide (sinon $\mathbb{N}$ serait majoré par n) donc admet un plus petit élément, strictement plus grand que n : on le note $s(n)$ et on l'appelle le *successeur de* n.

1.2.2 Principe de Récurrence

Théorème 1.2.8 *Soit $E \subset \mathbb{N}$ tel que $0 \in E$ et tel que*

$$\forall n \in \mathbb{N},\ (n \in E \Rightarrow s(n) \in E)\,.$$

Alors $E = \mathbb{N}$.

Démonstration : Par l'absurde, supposons que $E \neq \mathbb{N}$ et posons F l'ensemble non vide $\mathbb{N} - E$. Cet ensemble F admet un plus petit élément : n_0. Posons

$$P_{n_0} := \{k \in \mathbb{N} \mid k \leq n_0 \text{ et } k \neq n_0\}.$$

Comme $0 \in E$, on a $n_0 \geq 1$, donc $0 \in P_{n_0}$ et de plus P_{n_0} est visiblement majoré par n_0, donc il admet un plus grand élément : notons le $p(n_0)$ (prédécesseur de n_0). Par construction $p(n_0) < n_0$ donc $p(n_0) \notin F$, donc $p(n_0) \in E$, donc $s(p(n_0)) \in E$. On vérifie que $s(p(n_0)) = n_0$ [En effet, par définition du successeur, $s(p(n_0))$ est strictement plus grand que $p(n_0)$ donc par définition de $p(n_0)$, on a $s(p(n_0)) \geq n_0$. De plus $n_0 > p(n_0)$ et $s(p(n_0))$ est le plus petit élément k tel que $k > p(n_0)$, donc $n \geq s(p(n_0))$.] et ceci permet de conclure par l'absurde. □

Remarque 1.2.9 On a prouvé en cours de route que $s \circ p = \mathrm{Id}_{\mathbb{N}^*}$. On vérifie de même que $p \circ s = \mathrm{Id}_{\mathbb{N}}$.

1.2.3 Addition, multiplication et unicité de $\mathbb{N}$

On définit l'addition $+$ par récurrence par la formule :

$$\forall n \in \mathbb{N},\ n + 0 := n \quad n + 1 := s(n) \text{ et } \quad \forall m \in \mathbb{N}^*, n + m := (n + p(m)) + 1.$$

Nous pouvons réinterpréter le principe de récurrence sous la forme suivante : si $\mathcal{P}(n)$ est une propriété des entiers $n \in \mathbb{N}$ telle que $\mathcal{P}(0)$ est vraie et telle que $\forall n \in \mathbb{N}$, $\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$, alors pour tout entier $n \in \mathbb{N}$ la propriété $\mathcal{P}(n)$ est vérifiée [il suffit de poser $E = \{n \in \mathbb{N} \mid \mathcal{P}(n)\}$ et d'appliquer le principe de récurrence prouver précédemment].

Théorème 1.2.10 *Il existe, à bijection croissante près, un unique ensemble ordonné vérifiant les axiomes 1,2 et 3 donnés pour $\mathbb{N}$.*

Démonstration : Notons $\mathbb{N}'$ un ensemble ordonné vérifiant les mêmes axiomes. On définit par récurrence l'application suivante

$$\varphi : \mathbb{N} \to \mathbb{N}',\ \text{par la formule } \varphi(0) = 0' \text{ et } \forall n \in \mathbb{N},\ \varphi(n+1) = \varphi(n) +' 1',$$

øù $0', 1', +'$ désigne les analogues dans $\mathbb{N}'$ de $0, 1, +$ dans $\mathbb{N}$. Il est aisé de vérifier que φ est une bijection croisante. □

On définit la multiplication de la même façon que l'addition, par récurrence :

$$\forall n \in \mathbb{N},\ 0 \times n = 0,\ \text{et } \forall m \in \mathbb{N},\ (m+1) \times n = m \times n + n.$$

Il est à partir de là possible de prouver par récurrence toutes les propriétés usuelles de $+$ et $\times$ sur les entiers. Notamment la commutativité de $+$ et de $\times$, la compatibilité de $\leq$ avec $+$, la propriété de *régularité pour* $+$: $x + n = y + n \Rightarrow x = y$, la même propriété pour la loi $\times$, l'associativité de $+$ et de $\times$ et enfin la distributivité de $\times$ sur $+$. Nous laissons ceci en exercices au lecteur motivé.

1.2.4 Division euclidienne sur $\mathbb{N}$

Théorème 1.2.11 *Soit $(a, b) \in \mathbb{N} \times \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{N}^2$ tel que*

$$a = bq + r \quad \text{et} \quad 0 \leq r < b.$$

Démonstration : Commençons par prouver l'existence. On effectue pour cela une récurrence sur a : si $a = 0$ ou plus généralement si $a < b$ alors le couple $(q, r) = (0, a)$ convient. Si la propriété est vraie au rang $a - 1 \geq 0$: soit b un élément quelconque de $\mathbb{N}^*$. Si $a < b$ il n'y a rien à prouver par ce qui précède. Sinon $a - b \geq 0$ et de plus $a - b \leq a - 1$ donc on peut appliquer l'hypothèse de récurrence à $a - b$. On obtient l'existence d'un couple (q, r) tel que :

$$a - b = bq + r \text{ et } 0 \leq r < b,\ \text{donc } a = b(q+1) + r.$$

le couple $(q + 1, r)$ permet donc de conclure la récurrence.

Prouvons maintenant l'unicité. Supposons pour cela donné deux couples (q, r) et (q', r') tels que

$$bq + r = a = bq' + r' \text{ et } 0 \leq r, r' < b.$$

quitte à échanger les roles de (q, r) et de (q', r'), on peut supposer (et on le fait !) que $r' \geq r$. On a donc dans $\mathbb{N}$ l'égalité suivante :

$$b(q - q') = r' - r.$$

Si $r = r'$ ceci permet d'en déduire que $q = q'$. Sinon $r' > r$, donc l'égalité précédente donne visiblement $q > q'$ et la même égalité implique alors que $r' - r \geq b$ donc que $r' \geq b$ ce qui est impossible. Finalement par l'absurde ceci prouve que $r = r'$ et permet de conclure. □

Corollaire 1.2.12 ***(Écriture en base** g**)*** *Soit $g \geq 2$ un entier. On a :*

$$\forall a \in \mathbb{N}\ \exists r \in \mathbb{N}\ \exists a_0, \ldots, a_r \in \{0, \ldots, g-1\}, \text{ tels que } a = a_0 + \cdots + a_r g^r.$$

Démonstration : On effectue une récurrence sur a : si $a = 0$ c'est évident. Si la propriété est vraie jusqu'au rang $a-1 \geq 0$, montrons la au rang a. On effectue la division euclidienne de a par g : $\exists (q, r)$ tels que $a = gq + r$ et $0 \leq r < g$. Si q était au moins égal à a, on aurait $gq \geq 2a$ donc $a = gq + r \geq 2a + r \geq 2a > a$ ce qui est impossible. Donc $q < a$ et on peut lui appliquer l'hypothèse de récurrence : $q = q_0 + \cdots + q_n g^n$ donc $a = r + q_0 g + \cdots + q_n g^{n+1}$. □

Remarque 1.2.13 Si les derniers a_i dans l'écriture en base g sont nuls, on peut les supprimer de l'écriture. De même on peut ajouter des a_i nuls à droite dans l'écriture. L'énoncé suivant indique qu'à part ces deux cas, il y a unicité de l'écriture en base g.

Proposition 1.2.14 *Soit $a \in \mathbb{N}$ et soit $g \geq 2$ un entier. S'il existe $a_0, \ldots, a_r, b_0, \ldots, b_s \in \{0, \ldots, g-1\}$ avec $s \geq r$, alors*

$$a_0 = b_0\ ;\ \ldots\ ;\ a_r = b_r \text{ et } b_{r+1} = \cdots = b_s = 0.$$

Démonstration : Exercice □

1.3 Nombres premiers et valuation p-adique

Définition 1.3.1 Un entier n est dit *composé* s'il est de la forme $n = ab$ avec $a, b \geq 2$ deux entiers. Un entier n est dit *premier* si $n \geq 2$ et si n n'est pas composé.

Remarque 1.3.2 On voit sur la définition qu'un entier composé vérifie toujours $n \geq 4$. De même on voit aisément sur la définition qu'un nombre premier pair est nécessairement égal à 2.

Théorème 1.3.3 ***(Existence et unicité de la décomposition en facteurs premiers)*** *Soit $n \geq 2$ un entier.*

1. *L'entier n peut s'écrire comme un produit $\prod_{i=1}^{r} p_i$ de facteurs premiers (les p_i pouvant se répéter).*
2. *S'il existe deux décompositions $\prod_{i=1}^{r} p_i = n = \prod_{i=1}^{s} q_i$ (avec p_i, q_i des nombres premiers et $r, s \geq 1$), alors $r = s$ et il existe une bijection σ de $\{1, \ldots, r\}$ sur lui même, telle que*

$$\forall i \leq r,\ q_i = p_{\sigma(i)}.$$

Démonstration : Le point 1 se prouve par récurrence sur n : si n est premier (notamment si $n = 2$) l'existence d'une décomposition en facteurs premiers est évidente. Si $n \geq 4$ est composé. Supposons la propriété vraie jusquàu rang $n-1$. Par définition d'être composé, $n = ab$ avec $a, b \geq 2$ donc également $a, b < n$. L'hypothèse de récurrence appliquée à a et à b permet de conclure.

Pour ce qui est de l'unicité : quitte à réindexer les divers facteurs premiers, on peut supposer qu'ils sont ordonnés de la façon suivante :

$$p_1 \leq \ldots \leq p_r \text{ et } q_1 \leq \ldots \leq q_s.$$

De plus quitte à échanger les rôles de (p_i) et (q_i), on peut supposer que $p_1 \leq q_1$. Nous allons maintenant montrer le point 2 par récurrence sur n.

Si $p_1 = q_1$ alors $m := p_2 \ldots p_r = q_2 \ldots q_s < n$ donc l'hypothèse de récurrence apppliquée à m entraîne que $r - 1 = s - 1$ et que les $(q_i)_{i \geq 2}$ sont obtenus par permutation des $(p_i)_{i \geq 2}$. La

même chose est *a fortiori* vraie pour les $(q_i)_{i\geq 1}$ et les $(p_i)_{i\geq 1}$.

Si par l'absurde on a $p_1 < q_1$, alors posons $m := n - p_1 q_2 \dots q_s$. Il y a deux façons d'écrire ce nombre :

$$m = p_1 \left(\prod_{i=2}^{r} p_i - \prod_{i=2}^{s} q_i \right) = (q_1 - p_1) \prod_{i=2}^{s} q_i.$$

Par construction $m < n$ et de plus $m > 1$ (sinon on voit sur l'écriture $1 = m = (q_1 - p_1) \prod_{i=2}^{s} q_i$ que ceci impliquerait que $s = 1$ et $1 = q_1 - p_1$ donc $q_1 = 1 + p_1$ ou p_1 serait pair mais la remarque précédant l'énoncé du théorème nous indique que dans ce cas p_1 ou q_1 vaudrait 2, donc $p_1 = 2$ et $q_1 = 3$ et $3 = q_1 = n = \prod p_i$ serait donc pair : impossible !). On peut décomposer en facteurs premiers les nombres $q_1 - p_1$ ainsi que $\prod_{i=2}^{s} p_i - \prod_{i=2}^{s} q_i$ et l'hypothèe de récurrence (concernant l'unicité de l'écriture) appliquée à m donne que p_1 est l'un des facteurs premiers de $q_1 - p_1$ (en effet, p_1 est strictement plus petit que tout les q_i et p_1 est l'un des facteurs premiers de $m = (q_1 - p_1) \prod_{i=2}^{s} q_i$). Finalement p_1 divise $q_1 - p_1$ donc $p_1 \geq 2$ divise q_1 et est strictement plus petit que ce dernier. Ceci contredit le fait que q_1 est premier et conclut la preuve. □

Remarque 1.3.4 Lorsque l'on disposera d'un peu plus d'outils, nous verrons ultérieurement dans le cours une preuve plus simple de ce résultat.

Soit $n \in \mathbb{N}^*$. Nous noterons désormais toujours $\mathcal{P}$ l'ensemble des nombres premiers.

Proposition 1.3.5 *L'ensemble $\mathcal{P}$ est infini.*

Démonstration : Par l'absurde sinon on aurait $\mathcal{P} = \{p_1, \dots, p_r\}$ pour un certain entier $r \geq 1$. Dans ce cas on pourrait considérer l'entier $N = 1 + \prod_{i=1}^{r} p_i$.C'est un entier plus grand que 2 donc on peut le décomposer en facteurs premiers. Soit p divisant N un tel facteur premier. Par définition $p \in \mathcal{P}$, donc on doit avoir $p|1$ ce qui est impossible. □

Définition 1.3.6 Soit $n \geq 2$ un entier. Décomposons n en facteurs premiers :

$$n = \prod_{p \in \mathcal{P}} p^{v_p(n)}.$$

Par l'unicité de la décomposition en facteurs premiers le nombre $v_p(n)$ est bien défini et n étant fixé, la suite $(v_p(n))_{p\in\mathcal{P}}$ est nulle pour tout nombre premier sauf un nombre fini d'entre eux. On dit que $v_p(n)$ est la *valuation p-adique de n*. On pose $v_p(1) = 0$ pour tout $p \in \mathcal{P}$.

Lemme 1.3.7 *Soit $a, b \geq 1$ on a pour tout $p \in \mathcal{P}$, $v_p(ab) = v_p(a) + v_p(b)$.*

Démonstration : Cela résulte immédiatement de l'existence et de l'unicité de la décomposition en facteurs premiers pour a, b et ab. □

1.4 Entiers relatifs, groupes et anneaux

1.4.1 Groupes, définitions

Définition 1.4.1 Un *groupe* est la donnée d'un couple $(G, \cdot)$ où G est un ensemble non vide et où $\cdot$ est une application de $G \times G$ dans G, appelée *loi de composition interne* vérifiant :

1. (Associativité) $\forall x, y, z \in G$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
2. (Existence d'un élément neutre) $\exists e \in G$, $\forall z \in G$ on a $g \cdot e = e \cdot g$.
3. (Existence d'un inverse) $\forall x \in G$, $\exists y \in G$ tel que $x \cdot y = y \cdot x = e$.

Lemme 1.4.2 ***(Unicité du neutre et de l'inverse)*** *Si e et e' sont deux éléments neutres pour la loi $\cdot$ alors $e = e'$. De même si $x \in G$ et si y et y' sont deux inverses pour x alors $y = y'$.*

Démonstration : Pour la première assertion, on a $e \cdot e' = e$ par définition de l'élément neutre e'. De même par définition de l'élément neutre e, on a $e \cdot e' = e'$. Donc $e = e'$. Concernant la seconde assertion, on voit que $x \cdot y = e$. Multipliant cette égalité par y' on obtient $y' \cdot (x \cdot y) = y' \cdot e = y'$ et par associativité de la loi $\cdot$ on en déduit que $(y' \cdot x) \cdot y = y'$. Or $y' \cdot x = e$ donc $y = y'$. □

Remarque 1.4.3 Quelques commentaires sur la définition :

1. Le plus souvent, la notation $\cdot$ pour la loi de composition sera sous-entendue : on écrira xy au lieu de $x \cdot y$. On parlera dans ce cas de *notation multiplicative* (par opposition à la *notation additive* consistant à écrire $x + y$).
2. On fera le plus souvent l'abus de langage consistant à parler du groupe G plutôt que du groupe $(G, \cdot)$.
3. Le neutre pour la notation multiplicative est noté traditionnellement 1 (au lieu de e) et le neutre en notation additive se note traditionnellement 0.
4. L'inverse d'un élément x pour la notation multiplicative est noté traditionnellement x^{-1} et l'inverse en notation additive se note traditionnellement $-x$ et est appelé l'opposé.

Proposition 1.4.4 *Soit G un groupe et $x, y \in G$. On a $(xy)^{-1} = y^{-1}x^{-1}$.*

Démonstration : On calcule $z = (xy)y^{-1}x^{-1}$ et on voit en utilisant l'associativité que $z = 1$. De même on vérifie que $y^{-1}x^{-1}(xy) = 1$. □

Définition 1.4.5 Un groupe G est dit *commutatif* (ou *abélien*) si

$$\forall x, y \in G, \quad xy = yx.$$

Exemple 1.4.6

1. $(\mathbb{Z}, +)$ est un groupe (mais $(\mathbb{Z}, \cdot)$ ou $(\mathbb{Z}^*, \cdot)$ ou $(\mathbb{N}, +)$ n'en sont pas). Il est commutatif.
2. L'ensemble des matrices inversibles $\mathrm{GL}_n(\mathbb{R})$ est un groupe pour la multiplcation matricielle, de neutre I_n. Il n'est pas commutatif (exercice).
3. L'ensemble des matrices carrées de taille $n \times n$, noté $\mathcal{M}_n(\mathbb{R})$ est un groupe pour l'addition.
4. L'ensemble des bijections d'un ensemble X sur lui même est un groupe pour la composition. On le note $(S(X), \circ)$.

1.4.2 Anneaux

Définition 1.4.7 Un *anneau* est un triplet $(A, +, \times)$ tel que $(A, +)$ est un groupe commutatif et vérifiant de plus les propriétés suivantes :

1. La multiplication admet un neutre (que l'on note 1).
2. La loi $\times$ est associative.
3. (distributivité) $\forall a, b, c \in A$, $(a+b)c = ac + bc$ et $a(b+c) = ab + ac$.

Proposition 1.4.8 *Si A est un anneau et $a \in A$, on a $0 \cdot a = 0$. On dit que 0 est absorbant.*

Démonstration : On a $0 \cdot a = (0+0) \cdot a = (0 \cdot a) + (0 \cdot a)$. En additionnant l'opposé de $0 \cdot a$ dans cette égalité on obtient le résultat. □

Remarque 1.4.9 Étant donné un anneau $(A, +, \cdot)$ on munit naturellement A^n d'une structure d'anneau pour tout $n \geq 1$ en définissant l'addition et la multiplication dans A^n composante par composante.

Définition 1.4.10 Un anneau est *commutatif* si la loi $\times$ est commutative. Un anneau A est dit *intègre* si il est commutatif, si $A \neq \{0\}$ et si

$$\forall x, y \in A, \quad xy = 0 \Rightarrow x = 0 \text{ ou } y = 0.$$

Exemple 1.4.11

1. $(\mathbb{Z}, +, \cdot)$ est un anneau commutatif intègre.
2. si $n \geq 2$, $(\mathcal{M}_n(\mathbb{R}), +, \cdot)$ est un anneau non commutatif et il existe des matrices A, B non nulles telles que $AB = 0$ (exercice).
3. Si A est un anneau commutatif (intègre ou non), alors A^n n'est jamais intègre si $n \geq 2$ (exercice).

Définition 1.4.12 Soit A un anneau et $x \in A$. L'élément x est dit *inversible* s'il existe $y \in A$ tel que $xy = yx = 1$. On note $A^\times$ l'ensemble des éléments inversibles de A.

Proposition 1.4.13 *Si $A \neq \{0\}$ alors l'ensemble $A^\times$ est un groupe pour la multiplication de A.*

Démonstration : L'élément neutre $1 \in A$ pour la loi $\cdot$ sur A est évidemment inversible donc $A^\times$ est non vide. De plus la loi $\cdot$ est associative sur A donc *a fortiori* sur $A^\times$ qui est un sous-ensemble de A. Si $x, y \in A^\times$ alors la proposition 1.4.4 nous assure que $xy \in A^\times$ d'inverse $y^{-1}x^{-1}$. Notamment la loi $\cdot$ est bien définie sur $A^\times \times A^\times$ à valeurs dans $A^\times$. Les autres propriétés sont immédiatement vérifiées. □

1.4.3 Corps

Définition 1.4.14 Un *corps* est un anneau commutatif $A \neq \{0\}$ tel que $A^\times = A - \{0\}$.

Exemple 1.4.15 $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, le corps des fractions rationnelles $K(X)$ d'un corps K sont des corps. Par contre $\mathbb{Z}$, $\mathcal{M}_n(\mathbb{R})$ avec $n \geq 2$, K^n si K est un corps et $n \geq 2$, ne sont pas des corps.

1.4.4 Division euclidienne sur $\mathbb{Z}$

Proposition 1.4.16 *Pour tout couple $(a,b) \in \mathbb{Z} \times \mathbb{Z}^\times$, il existe un unique couple $(q,r) \in \mathbb{Z}^2$ tel que*

$$a = bq + r \quad \text{avec} \quad 0 \leq r < |b|.$$

Démonstration : Nous laissons l'unicité en exercice. Pour l'existence : si a et b sont tout deux positifs, le résultat est déjà connu. Si $b > 0$ et $a < 0$ alors $-a > 0$ et on peut appliquer le résultat au couple $(-a, b)$. Si $b < 0$ alors $-b > 0$ et on peut reprendre l'argument qui précède. □

1.4.5 Premières applications à la théorie des groupes

Soit G un groupe et $g \in G$. On définit la puissance g^n, pour $n \geq 0$ par réccurrence (sur n) en posant

$$g^0 := 1, \quad \text{et} \quad \forall n \geq 0,\ g^{n+1} = g^n \cdot g.$$

Proposition 1.4.17 *Soit $g \in G$. Pour tout entier $n, m \geq 0$ on a*

$$g^{n+m} = g^n g^m \text{ et } (g^n)^m = g^{nm}.$$

Démonstration : C'est une simple récurrence. □

Définition 1.4.18 Soient $(G, \cdot)$ et $(H, \star)$ deux groupes et soit $\varphi : G \to H$ une application. On dit que φ est un *morphisme* de groupes si

$$\forall x, y \in G \quad \varphi(x \cdot y) = \varphi(x) \star \varphi(y).$$

Exemple 1.4.19 Nous donnons trois exemples avec des lois diverses de morphismes de groupes :

1. Soit $a \in \mathbb{Z}$, $\varphi_a : \mathbb{Z} \to \mathbb{Z}$ donné $x \mapsto ax$.
2. L'application exponentielle de $(\mathbb{R}, +)$ vers $(\mathbb{R}_+^*, \cdot)$.
3. L'application logarithme de $(\mathbb{R}_+^*, \cdot)$ vers $(\mathbb{R}, +)$.

Proposition 1.4.20 *Si $\varphi : G \to H$ est un morphisme de groupes, on a $\varphi(1_G) = 1_H$. Et si $x \in G$ on a $\varphi(x^{-1}) = \varphi(x)^{-1}$.*

Démonstration : On a $\varphi(1_G) = \varphi(1_G \cdot 1_G) = \varphi(1_G) \star \varphi(1_G)$. En multipliant cette égalité par l'inverse de $\varphi(1_G)$ on en déduit que $1_H = \varphi(1_G)$. concernant la seconde assertion, notons que l'on a $1 = \varphi(1) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1})$. En multipliant par l'inverse de $\varphi(x)$ on peut conclure. □

Proposition 1.4.21 *Soit G un groupe. Les morphismes de groupes $\varphi : \mathbb{Z} \to G$ sont exactement les $\varphi_g : n \mapsto g^n$ quand g décrit G.*

Démonstration : Tout d'abord on vérifie aisément que si $g \in G$, l'application φ_g est un morphisme de groupes : en effet soit $a, b \in \mathbb{Z}$ on a $\varphi_g(a+b) = g^{a+b} = g^a g^b = \varphi_g(a)\varphi_g(b)$. Soit maintenant φ un morphisme quelconque de $\mathbb{Z}$ dans G. Par la proposition précédente, on sait que $\varphi(0) = 1_G$ (le neutre de $\mathbb{Z}$ étant 0). De plus, si $n \in \mathbb{N}$ on a $\varphi(n+1) = \varphi(n)\varphi(1)$ et par récurrence on voit donc que $\varphi(n+1) = g^n g = g^{n+1}$ en posant $g := \varphi(1)$. Enfin, si $n < 0$ on a $-n > 0$ et $\varphi(n) = \varphi(-n)^{-1} = (g^{-n})^{-1} = g^n$. Ceci prouve que $\varphi = \varphi_g$. □

Définition 1.4.22 Soit $(G, \cdot)$ un groupe et H un sous ensemble de G. On dit que H est un *sous-groupe* de G si H muni de la loi $\cdot$ est un groupe.

Proposition 1.4.23 *Soient $(G, \cdot)$ un groupe et $H \subset G$. On a*

$$H \text{ est un sous-groupe de } G \iff \forall x, y \in H, \quad xy^{-1} \in H \text{ et } H \neq \emptyset.$$

Démonstration : L'implication de gauche à droite découle facilement des définitions. Réciproquement

1. L'élément neutre 1 est dans H : en effet on sait que H est non vide, donc admet un élément h_0 ; de plus par hypothèse $1 = h_0 h_0^{-1}$ est également dans H.
2. pour tout $x \in H$, on a $x^{-1} = 1 \cdot x^{-1} \in H$.
3. Pour tout $x, y \in H$ on a y^{-1} dans H par ce qui précède et donc $x \cdot y = x \cdot (y^{-1})^{-1} \in H$.

La loi $\cdot$ étant associative sur G l'est *a fortiori* sur H. Ceci prouve que H est un sous-groupe de G. □

Définition 1.4.24 Soit $\varphi : G \to H$ un morphisme de groupes. On note

$$\mathrm{Im}(\varphi) := \{h \in H \mid \exists x \in G, \ \varphi(x) = h\} \ \textit{l'image de } \varphi,$$

et

$$\mathrm{Ker}(\varphi) := \{g \in G \mid \varphi(g) = 1\} \ \textit{le noyau de } \varphi.$$

Proposition 1.4.25 *Les sous-ensembles* $\mathrm{Im}(\varphi)$ *et* $\mathrm{Ker}(\varphi)$ *sont des sous-groupes de G et de H respectivement.*

Démonstration : Faisons la preuve pour l'image et laissons en exercice la preuve pour le noyau. Le groupe G n'étant pas vide, il contient l'élément neutre 1_G, donc l'image contient l'élément $1_H = \varphi(1_G)$. De plus si $x, y \in \mathrm{Im}(\varphi)$ alors $\exists a, b \in G$ tels que $\varphi(a) = x$ et $\varphi(b) = y$. Donc on a

$$xy^{-1} = \varphi(a)\varphi(b)^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1}) \in \mathrm{Im}(\varphi).$$

Par la proposition précédente nous pouvons conclure. □

Proposition 1.4.26 *Si $\varphi : G \to H$ est un morphisme de groupes, on a*

$$\varphi \text{ injectif} \iff \mathrm{Ker}(\varphi) = \{1\}.$$

Démonstration : Supposons que φ est injectif et soit $g \in \mathrm{Ker}(\varphi)$. On a $\varphi(g) = 1 = \varphi(1)$. Par injectivité ceci implique que $g = 1$ donc que $\mathrm{Ker}(\varphi) \subset \{1\}$. L'élément 1 étant visiblement dans le noyau on conclut que $\mathrm{Ker}(\varphi) = \{1\}$. Réciproquement supposons que $\mathrm{Ker}(\varphi) = \{1\}$. Soient $x, y \in G$ tels que $\varphi(x) = \varphi(y)$. En multipliant à droite par l'inverse de $\varphi(y)$ on obtient :

$$\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = \varphi(x)\varphi(y)^{-1} = \varphi(y)\varphi(y)^{-1} = 1.$$

Par hypothèse on en déduit que $xy^{-1} = 1$ donc que $x = y$ en multipliant à droite par y. □

Proposition 1.4.27 *Les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$ quand n décrit l'ensemble des entiers naturels.*

Démonstration : Notons tout d'abord que si $n \in \mathbb{N}$ alors l'ensemble $n\mathbb{Z}$ est visiblement un sous-groupe de $\mathbb{Z}$ (exercice). Réciproquement : soit $G \subset \mathbb{Z}$ un sous-groupe de $\mathbb{Z}$. Si $G = \{0\}$ alors G est de la forme $n\mathbb{Z}$ avec $n = 0$. Sinon, en prenant un élément non nul dans G et quitte à considérer son opposé,on voit qu'il existe un élément dans $G \cap \mathbb{N}^*$. Cette partie $G \cap \mathbb{N}^*$ est donc une partie non vide de $\mathbb{N}$ et admet donc un plus petit élément : notons le g_0. Les multiples de g_0 sont donc tous dans G (pour tout entier n, l'élément $ng_0 = g_0 + \cdots + g_0 \in G$ car G est stable par addition) donc $g_0\mathbb{Z} \subset G$. Soit maintenant $g \in G$ un élément quelconque. La division euclidienne de g par g_0 nous donne : il existe $(q, r) \in \mathbb{Z}^2$ tels que $g = g_0 q + r$ et $0 \leq r < g_0$. Donc $r = g - qg_0$ est dans G comme différence de deux éléments du groupe G. Or $r \in G \cap \mathbb{N}$ est strictement plus petit que le plus petit élément de $G \cap \mathbb{N}^*$, donc $r = 0$. Ainsi $g = qg_0$ est dans $g_0\mathbb{Z}$ donc $G \subset g_0\mathbb{Z} \subset G$. Autrement dit $G = g_0\mathbb{Z}$, ce que l'on voulait prouver. □

Définition 1.4.28 Soit φ un morphisme de groupes. On dit que φ est un *isomorphisme* si φ est bijectif.

Proposition 1.4.29 *Un isomorphisme est tel que sa bijection réciproque est automatiquement un morphisme de groupes.*

Démonstration : Notons $\varphi : G \to H$ l'isomorphisme dont on part et posons $\psi : H \to G$ sa bijection réciproque. On veut montrer que ψ est un morphisme de groupes. Soit donc $a, b \in H$, on a

$$\psi(ab) = \psi(a)\psi(b) \iff \varphi\left(\psi(ab)\right) = \varphi\left(\psi(a)\psi(b)\right) \iff ab = \varphi\left(\psi(a)\psi(b)\right).$$

Par ailleurs φ est un morphisme de groupes donc

$$ab = \varphi\left(\psi(a)\psi(b)\right) \iff ab = \varphi(\psi(a))\varphi(\psi(b)) \iff ab = ab.$$

La dernière assertion dans la série d'équivalences étant vraie, la première l'est également, autrement dit, ψ est un morphisme de groupes. □

1.4.6 Ordre d'un élément dans un groupe

Soient G un groupe et $g \in G$. Notons $\varphi_g : \mathbb{Z} \to G$ le morphisme $n \mapsto g^n$. Le noyau de φ_g est un sous-groupe de $\mathbb{Z}$, donc de la forme $d\mathbb{Z}$ pour un certain entier $d \geq 0$.

1. Si $d = 0$: les g^n sont deux à deux distincts lorsque n est variable. On dit que g est *d'ordre infini.*
2. Si $d > 0$: on dit que g est *d'ordre d.*

Proposition 1.4.30 *Si g est d'ordre $d > 0$, alors $\exists k \geq 1$ tel que $g^k = 1$ et d est le plus petit tel entier k. De plus : $g^n = 1 \iff d|n$ et $\mathrm{Im}(\varphi_g) = \{1, g, \ldots, g^{d-1}\}$.*

Démonstration : Par définition de l'ordre, le nombre $k := d$ assure l'existence d'un k comme voulu. Si $g^k = 1$ et si $k \geq 1$, alors $k \in d\mathbb{Z}$ donc en particulier $k \geq d$. Par ailleurs, $g^k = 1 \iff k \in \mathrm{Ker}\varphi_g \iff k \in d\mathbb{Z} \iff d|k$. □

Définition 1.4.31 Soit G un groupe et $g \in G$. On appelle *sous-groupe engendré par g* le groupe $\mathrm{Im}\varphi_g$. On le note $\langle g \rangle$.

1. Si $d = 0$, l'ordre de g est infini et le cardinal du groupe $\langle g \rangle$ est infini.
2. Si $d > 0$, l'ordre de g est d et le cardinal du groupe $\langle g \rangle$ est d.

Remarque 1.4.32 Si le cardinal de G est fini, alors tout les éléments de G sont d'ordre fini (en effet sinon φ_g aurait une image infini tout en étant inclus dans G, ce qui est impossible).

Théorème 1.4.33 ***(Lagrange)*** *Soit G un groupe fini et H un sous-groupe de G. Alors*

$$\mathrm{Card}(G) = \mathrm{Card}(G/H) \times \mathrm{Card}(H).$$

En particulier, le cardinal de H divise celui de G.

Pour prouver le théorème nous introduisons la relation déquivalence suivante, appelée *relation de congruence modulo H*, sur G en posant :

$$x \equiv y \bmod H \text{ si par définition } \exists h \in H \ x = yh.$$

Vérifions tout d'abord que cette relation est bien une relation d'équivalence :

1. réflexivité : on a $x = x \cdot 1$ et $1 \in H$ donc $x \equiv x \bmod H$.
2. symétrie : si $x = y \bmod H$, il existe $h \in H$ tel que $x = yh$, donc $y = xh^{-1}$. En posant $k = h^{-1}$ on voit qu'il existe $k \in H$ tel que $y = xk$, donc $y \equiv x \bmod H$.
3. transitivité : si $x \equiv y \bmod H$ et $y \equiv z \bmod H$, alors il existe $h_1, h_2 \in H$ tels que $x = yh_1$ et $y = zh_2$. Donc $x = yh_1 = (zh_2)h_1 = z(h_2h_1)$. Donc $x \equiv z \bmod H$.

Définition 1.4.34 les classes d'équivalences pour cette relation sont appelées les *classes à gauche* et l'ensemble quotient se note G/H. On a

$$\mathrm{Cl}(x) = \{y \in G \mid \exists h \in H \ y = xh\} = xH.$$

Remarque 1.4.35 Notons que l'on aurait pu également introduire une relation très similaire donnée par

$$x \equiv y \bmod H \text{ si par définition } \exists h \in H \ x = hy.$$

Il s'agit également d'une relation d'équivalence et les classes d'équivalences sont appelées les classes à droite et l'ensemble quotient se note $H\backslash G$. On a $\mathrm{Cl}(x) = Hx$. Sauf mention contraire, nous travaillerons toujours avec les classes à gauche plutôt qu'avec les classes à droite.

Notons que si le groupe G est fini, toutes les classes à gauche on le même cardinal : celui de H. En effet on a pour tout $x \in G$, une bijection de H vers $\mathrm{Cl}(x) = xH$ donnée par $h \mapsto xh$.

Preuve du théorème 1.4.33 : On considère la relation de congruence d'ensemble quotient G/H. Les classes déquivalences forment une partition de G, elles ont toutes le même cardinal ($\mathrm{Card}(H)$) et il y en a $\mathrm{Card}(G/H)$ (rappelons que par définition, l'ensemble quotient G/H est l'ensemble des classes d'équivalences). On obtient ainsi la formule suivante :

$$\mathrm{Card}(G) = \mathrm{Card}(G/H) \times \mathrm{Card}(H).$$

Ceci prouve le théorème. □

Corollaire 1.4.36 *Si $\mathrm{Card}(G) = n \in \mathbb{N}^*$, alors tout élément de G est d'ordre $d|n$.*

Démonstration : Soit $g \in G$. On sait que l'ordre d de g est fini car G est fini. Or $d = \mathrm{Card}(\langle g \rangle)$. Donc le théorème de Lagrange assure que d divise n. □

Corollaire 1.4.37 *Soit $\varphi : G \to F$ un morphisme de groupes avec G fini. Alors* $\mathrm{Im}(\varphi)$ *est un groupe fini et*

$$\mathrm{Card}(\mathrm{Im}(\varphi)) \times \mathrm{Card}(\mathrm{Ker}(\varphi)) = \mathrm{Card}(G).$$

Démonstration : Posons $H = \mathrm{Ker}(\varphi)$. c'est un sous-groupe de G donc le théorème de Lagrange nous assure que $\mathrm{Card}(G/H) \times \mathrm{Card}(\mathrm{Ker}(\varphi)) = \mathrm{Card}(G)$. Il reste pour conclure à prouver que $\mathrm{Im}(\varphi)$ est en bijection avec l'ensemble quotient $G/\mathrm{Ker}(\varphi)$. condiérons pour cela l'application suivante :

$$\bar{\varphi} : G/\mathrm{Ker}(\varphi) \to \mathrm{Im}(\varphi) \subset F,\ g\mathrm{Ker}(\varphi) \mapsto \varphi(g).$$

Notons tout d'abord que cette application est bien définie (autrement dit ce que l'on écrit à un sens et la valeur $\varphi(g)$ ne dépend par du choix d'un réprésentant de la classe déquivalence $g\mathrm{Ker}(\varphi)$). Soit donc $x, y \in G$ tels que $x\mathrm{Ker}(\varphi) = y\mathrm{Ker}(\varphi)$. Nous voulons montrer que $\varphi(x) = \varphi(y)$. Or on a

$$\varphi(x) = \varphi(y) \iff \varphi(y^{-1})\varphi(x) = 1 \iff y^{-1}x \in \mathrm{Ker}\varphi \iff x \in y\mathrm{Ker}(\varphi).$$

Finalement la dernière condition est équivalente à dire que $x\mathrm{Ker}(\varphi) \subset y\mathrm{Ker}(\varphi)$. Par symétrie des rôles de x et de y (dans la condition $\varphi(x) = \varphi(y)$), on voit que ceci est également équivalent à $y\mathrm{Ker}(\varphi) \subset x\mathrm{Ker}(\varphi)$. Donc finalement nous voyons que $\varphi(x) = \varphi(y)$ si et seulement si $x\mathrm{Ker}(\varphi) = y\mathrm{Ker}(\varphi)$. Ceci prouve non seulement que l'application $\bar{\varphi}$ est bien définie mais également qu'elle est injective. La surjectivité est claire sur la définition de l'ensemble image. □

Lemme 1.4.38 *Soit G un groupe et $(H_i)_{i\in I}$ une famille quelconque de sous-groupes de G. Notons H l'intersection des H_i quand i parcourt I. Alors H est un sous-groupe de G.*

Démonstration : Notons que 1 est dans H_i pour tout $i \in I$ donc 1 est dans l'intersection. Par ailleurs, si $x, y \in H$ alors en particulier x et y sont dans H_i pour tout $i \in I$. Comme les H_i sont des sous-groupes, on en déduit que xy^{-1} est dans H_i pour tout $i \in I$ donc xy^{-1} est dans H qui est donc un sous-groupe de G. □

Définition 1.4.39 Soit G un groupe et S une partie non-vide de G. On note $< S >$ et on appelle *sous-groupe engendré par S* le plus petit sous-groupe de G contenant S. C'est le groupe

$$< S >= \bigcap_{S\subset H, H sous-gr. de G} H.$$

Proposition 1.4.40 *Soit G un groupe et S une partie non-vide de G. On a la description ensembliste suivante de $< S >$:*

$$< S >= \left\{ g \in G \mid \exists r \geq 1,\ \exists n_1, \ldots, n_r \in \mathbb{Z},\ \exists s_1, \ldots, s_r \in S,\ g = \prod_{i=1}^{r} s_i^{n_i} \right\}.$$

Démonstration : Notons A l'ensemble du membre de droite dans l'égalité précédente. On vérifie très facilement que c'est un sous-groupe de G. De plus en prenant $r = 1$ on voit que A contient S. On en déduit que A contient $< S >$ le groupe engendré par S. Par ailleurs si H est un sous-groupe de G contenant S alors H contient tous les produits de puissances d'éléments de S, donc H contient A. En particulier le groupe $< S >$ contient A. □

1.5 Congruences modulo n

1.5.1 Définition et premiers résultats

Définition 1.5.1 Soit $n \geq 0$ un entier et soient $a, b \in \mathbb{Z}$. On dit que *a est congru à b modulo n*, et on note $a = b \bmod n$ si par définition n divise $a - b$.

Remarque 1.5.2 $a = b \bmod n \iff \exists k \in \mathbb{Z}\ a = b + kn \iff a \in b + n\mathbb{Z}$. Notons $\mathrm{Cl}(x)$ la classe d'équivalence d'un élément x pour cette relation de congruence modulo n. C'est un cas particulier de la relation de congruence modulo un sous groupe comme on le voit en posant $G = \mathbb{Z}$ et $H = n\mathbb{Z}$ et en travaillant en notations additives. On note donc naturellement $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient. On voudrait munir cet ensemble d'une structure d'anneau, qui soit de plus raisonnablement compatible avec celle provenant de $\mathbb{Z}$. C'est ce que nous allons nous attacher à faire dans la suite de ce paragraphe.

Proposition 1.5.3 *Soient $a, b, x, y \in \mathbb{Z}$ tels que $a = x \bmod n$ et $b = y \bmod n$. Alors on a :*

$$a + b = x + y \bmod n \text{ et } ab = xy \bmod n.$$

Démonstration : Nous faisons la preuve pour l'addition eet laissons au lecteur le soin de faire la preuve pour la multiplication. Dire que $a+b = x+y \bmod n$ équivaut à dire $\exists \lambda \in \mathbb{Z},\ a+b = x+y+n\lambda$. Or par hypothèses, il existe $\alpha, \beta \in \mathbb{Z}$ tels que $a = x + n\alpha$ et $b = y + n\beta$. Donc $a + b = x + y + n(\alpha + \beta)$. □

Corollaire 1.5.4 *Soit $r \geq 1$ et soient $\{a_i\}_{1 \leq i \leq r}, \{x_i\}_{1 \leq i \leq r} \in \mathbb{Z}^r$ tels que pour tout i, on a $a_i = x_i \bmod n$. Alors on a*

$$\sum_{i=1}^{r} x_i = \sum_{i=1}^{r} a_i \bmod n \text{ et } \prod_{i=1}^{r} a_i = \prod_{i=1}^{r} x_i \bmod n.$$

Démonstration : Immédiat à partir de la proposition, par récurrence sur le nombre r de termes. □

Corollaire 1.5.5 *Si $a = b \bmod n$ alors pour tout entier $k \in \mathbb{N}$ on a $a^k = b^k \bmod n$.*

Démonstration : Il suffit d'appliquer le corollaire précédent avec $r := k$, $a_i := a$ et $x_i := b$. □

Exemple 1.5.6 On a $10 = 1 \bmod 9$ donc $10^k = 1 \bmod 9$ pour tout entier $k \geq 0$. Si $x = a_r a_{r-1} \ldots a_0$ est l'écriture de x en base 10 on voit donc que $x = a_0 + \cdots + a_r \bmod 9$. Ce résultat est ce que l'on appelle *la preuve par* 9.

1.5.2 L'anneau $\mathbb{Z}/n\mathbb{Z}$, $n \geq 0$

Notation 1.5.7 Dans $\mathbb{Z}/n\mathbb{Z}$, la classe d'un élément $a \in \mathbb{Z}$ est notée $a \bmod n$ (ou $\bar{a}$ ou $\pi(a)$, l'appication $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ étant la surjection canonique).

Proposition 1.5.8 *Soient $a, b \in \mathbb{Z}$. On a*

$$a \bmod n = b \bmod n \iff a = b \bmod n.$$

Démonstration : Supposons tout d'abord que $a \bmod n = b \bmod n$. L'élément a appartient à la classe $a \bmod n$ donc à la classe $b \bmod n = \{b + kn \in \mathbb{Z} \mid k \in \mathbb{Z}\}$. Notamment il existe $k \in \mathbb{Z}$ tel que $a = b + kn$ ce qui équivaut à dire que $a = b \bmod n$. Réciproquement Si $a = b \bmod n$, il existe $k \in \mathbb{Z}$ tel que $a = b + kn$ donc $a \in b \bmod n$ et donc visiblement l'ensemble $a \bmod n$ est inclus dans $b \bmod n$. De même par symétrie des rôles de a et b, on a $b \bmod n \subset a \bmod n$, donc $a \bmod n = b \bmod n$. □

Remarque 1.5.9 En fait l'énoncé précédent vaut en fait pour toute relation d'équivalence $\mathcal{R}$ sur un ensemble E. Précisément on a dans ce cas :

$$x\mathcal{R}y \iff C(x) = C(y).$$

Par division euclidienne on voit que $\mathbb{Z}/n\mathbb{Z}$ est de cardinal n (pour $n \geq 1$) et que les classes $\bar{0}, \bar{1}, \ldots, \overline{n-1}$ sont deux à deux distinctes et forment donc l'ensemble $\mathbb{Z}/n\mathbb{Z}$. On munit cet ensemble d'une structure d'anneau commutatif en posant :

$$\forall a, b \in \mathbb{Z}, \quad (a \bmod n) + (b \bmod n) := (a + b) \bmod n \text{ et } (a \bmod n) \cdot (b \bmod n) := ab \bmod n.$$

Ceci est bien défini par ce qui précède (cf la proposition 1.5.3). On vérifie que ces opérations définissent sur $\mathbb{Z}/n\mathbb{Z}$ un structure d'anneau commutatif, de neutre $0 \bmod n$ pour l'addition, de neutre $1 \bmod n$ pour la multiplication, tels que $-a \bmod n$ est l'opposé de $a \bmod n$. De plus, la projection canonique est un *morphisme d'anneaux*, *ie* vérifie les propriétés suivantes :

1. C'est un morphisme de groupes, *ie* $\forall x, y \in \mathbb{Z}$ on a $\pi(x + y) = \pi(x) + \pi(y)$.
2. Il est compatible à la multiplication : $\forall x, y \in \mathbb{Z}$ on a $\pi(xy) = \pi(x) \cdot \pi(y)$.
3. $\pi(1) = 1 \bmod n$.

Ceci est évident sur la définition des lois $+$ et $\cdot$ sur $\mathbb{Z}/n\mathbb{Z}$.

Remarque 1.5.10 Notons que si un morphisme de groupes envoie automatiquement le neutre sur le neutre, la condition 3. précédente n'est pourtant pas impliquée par les deux précédentes. Par exemple l'application nulle vérifie trivialement les points 1 et 2 mais pas 3. Donnons deux exemples un peu moins naifs :

1. Considérons l'application $\varphi : \mathbb{Z}^2 \to \mathbb{Z}^2$ donnée par $(x, y) \mapsto (x, 0)$. Elle vérifie les points 1. et 2. mais $\varphi(1, 1) = (1, 0) \neq (1, 1)$.
2. Considérons l'application $\varphi : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ qui envoie 0 sur 0 et 1 sur $3 \bmod 6$. Elle est bien définie, stable par addition et multiplication mais $3 \bmod 6 \neq 1 \bmod 6$.

En fait si l'on considère un morphisme non nul $\varphi : A \to B$ entre deux anneaux, on a

$$\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1) = \varphi(1)^2.$$

Donc l'élément $\varphi(1)$ est solution dans B de l'équation $X(X - 1) = 0$ et est non nul (sinon $\varphi(a) = \varphi(a \cdot 1) = \varphi(a) \cdot \varphi(1) = 0$ pour tout $a \in A$ et φ serait le morphisme nul). Notamment si l'anneau B est intègre on voit que dans ce cas $\varphi(1)$ doit bien être égal à 1.

Exemple 1.5.11 Déterminons les inversibles de $\mathbb{Z}/4\mathbb{Z}$. On a $(\mathbb{Z}/4\mathbb{Z})^\times = \{1 \bmod 4 \ ; \ 3 \bmod 4\}$ (nous mettrons ceci dans un contexte plus global un peu plus loin dans ce cours). Par ailleurs on a $(2 \bmod 4) \cdot (2 \bmod 4) = 4 \bmod 4 = 0 \bmod 4$. Or $2 \neq 0 \bmod 4$, donc l'anneau $\mathbb{Z}/4\mathbb{Z}$ n'est pas intègre. Plus généralement si $n = n_1 n_2 \geq 2$ est composé dans $\mathbb{Z}$ alors l'anneau $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre comme on le voit en considérant le produit $(n_1 \bmod n) \cdot (n_2 \bmod n) = 0 \bmod n$.

Lemme 1.5.12 *Soit A un anneau commutatif intègre fini. Alors A est un corps.*

Démonstration : Il s'agit de prouver que tout élément $a \in A$ non nul est inversible. Soit a un tel élément. L'application $\varphi_a : A \to A$, $x \mapsto ax$ est injective (car A est intègre : $ax = ay \Rightarrow a(x-y) = 0 \Rightarrow x = y$). L'ensemble A étant de plus fini, elle est donc automatiquement surjective par cardinalité. Notamment il existe $b \in A$ tel que $\varphi_a(b) = 1$, donc $ab = 1$ et par commutativité ceci prouve que b est l'inverse de a. □

Théorème 1.5.13 *Soit $p \geq 2$ un entier on a*

$$p \text{ est premier} \iff \mathbb{Z}/p\mathbb{Z} \text{ est un corps} \iff \mathbb{Z}/p\mathbb{Z} \text{ est intègre.}$$

Démonstration : Si $\mathbb{Z}/p\mathbb{Z}$ est un corps, c'est en particulier un anneau intègre (si $ab = 0$ et $a \neq 0$ on multiplie par a^{-1} pour obtenir $b = 0$). Si $p \geq 2$ n'est par premier, il est composé donc par l'exemple précédent, on en déduit que $\mathbb{Z}/p\mathbb{Z}$ n'est pas intègre, ce qui prouve par la contraposée que si $\mathbb{Z}/p\mathbb{Z}$ est intègre alors p est premier. Il nous suffit donc de prouver que si p est premier, alors $\mathbb{Z}/p\mathbb{Z}$ est un corps pour conclure. En fait le lemme 1.5.12 précédent nous indique qu'il suffit de prouver que $\mathbb{Z}/p\mathbb{Z}$ est intègre pour conclure. Considérons donc $p \geq 2$ un nombre premier et $a, b \in \mathbb{Z}$ tels que $ab \bmod p = 0 \bmod p$. On a $ab = 0 \bmod p$ donc p divise ab. l'unicité de la décomposition en facteurs premiers implique que p est un facteur premier de a ou de b. On a donc $a = 0 \bmod p$ ou $b = 0 \bmod p$. □

1.6 Sous-groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$

Soit $n \geq 2$ un entier. On sait par le théorème de Lagrange que si H est un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ alors son cardinal divise n.

Définition 1.6.1 Soit G un groupe. On dit que G est *monogène* s'il existe $g \in G$ tel que $G = \{g^k \mid k \in \mathbb{Z}\}$. Si de plus G est fini, on dit qu'il est *cyclique*. Un élément g comme précédemment est appelé un *générateur* de G. On note $\langle g \rangle$ le groupe engendré par g.

Lemme 1.6.2 *Soit G un groupe cyclique et H un sous-groupe de G. Alors H est cyclique.*

Démonstration : Le sous-groupe H est inclus dans G donc est fini. Montrons qu'il est monogène. Notons n le cardinal de G. On introduit par ailleurs un générateur g_0 de G. On a ainsi $G = \{1 = g_0^0, g_0, \ldots, g_0^{n-1}\}$. Considérons k le plus petit élément non nul tel que $g_0^k \in H$. On va montrer que H est le groupe engendré par $x = g_0^k$. Tout d'abord notons que x étant dans H, toutes les puissances de x sont dans H, donc le groupe $\langle x \rangle \subset H$. Réciproquement, soit $h \in H$. L'élément h est dans G donc il existe $d \geq 0$ tel que $h = g_0^d$. On peut effectuer la division euclidienne de d par k : il existe (q, r) tels que $d = kq + r$ et $0 \leq r < k$. On a $g_0^d = (g_0^k)^q \cdot g_0^r$ donc en divisant par x^q on obtient

$$g_0^r = g_0^d (x^q)^{-1} = h(x^q)^{-1} \in H.$$

Par définition du plus petit élément k, ceci implique que $r = 0$ donc que h est un multiple de x *ie* que $H \subset \langle x \rangle$. □

Exemple 1.6.3 Soit $n \geq 2$, l'élément $1 \bmod n$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$. Donc les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont tous cycliques.

Théorème 1.6.4 *Pour tout diviseur d de $n \geq 2$, il existe un et un seul sous-groupe de cardinal d de $\mathbb{Z}/n\mathbb{Z}$: l'ensemble $\frac{n}{d}\mathbb{Z}/n\mathbb{Z}$ des multiples de $\frac{n}{d}$ dans $\mathbb{Z}/n\mathbb{Z}$.*

Démonstration : Soit d un entier divisant n. Notons tout d'abord que l'ensemble $H := \{k\frac{n}{d} \mid k \in \{0, \ldots, d-1\}\}$ est visiblement un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ de cardinal d. Si E est un sous-groupe de cardinal d. Il est cyclique par le lemme précédent, engendré par un élément x_0 (d'ordre d). On a en particulier $dx_0 = 0 \bmod n$ donc il existe $k \in \mathbb{N}$ tel que $dx_0 = kn$. En divisant par k on constate que x_0 est dans H. Donc E est inclus dans H et par cardinalité on conclut que $E = H$, d'où l'unicité. □

Chapitre 2

Groupes distingués et quotients, actions de groupes, groupes de Sylow

2.1 Sous-groupes distingués, Quotient de groupes

On voudrait généraliser la construction du groupe $\mathbb{Z}/n\mathbb{Z}$ à partir de $\mathbb{Z}$ au cas d'un groupe quelconque G et d'un sous-groupe H de G. On a déjà vu lors de la preuve du théorème de Lagrange la construction de l'ensemble quotient G/H (construction généralisant celle de $\mathbb{Z}/n\mathbb{Z}$). Toutefois cet ensemble quotient ne peut pas, en général être muni d'une structure de groupe raisonnable (cf. plus loin). Il convient pour cela de restreindre la classe de sous-groupes H autorisés.

Définition 2.1.1 Soit G un groupe et H un sous-groupe de G. On dit que H *est distingué dans* G et on note $H \triangleleft G$, si

$$\forall g \in G, \forall h \in H, \quad ghg^{-1} \in H.$$

Remarque 2.1.2 Notons que $H \triangleleft G$ ssi $\forall g \in G, \quad gHg^{-1} \subset H$.

Exemple 2.1.3 Donnons tout de suite quelques exemples de sous-groupes distingués :

1. G et $\{1\}$ sont distingués dans G.
2. Si $(G, +)$ est abélien, alors tout les sous-groupes de G sont abéliens
3. Si $\varphi : G \to F$ est un morphisme de groupes, alors $\mathrm{Ker}(\varphi)$ est distingué dans G.

Définition 2.1.4 On appelle *centre de* G, noté $Z(G)$ l'ensemble

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

Proposition 2.1.5 *Le centre est un sous-groupe distingué de* G.

Démonstration : Visiblement $1 \in Z(G)$ qui est donc non vide. Si $x, y \in Z(G)$ soit $g \in G$. On a

$$\begin{aligned} g(xy^{-1}) &= (gx)y^{-1} = (xg)y^{-1} = x(gy^{-1}) = x((g^{-1})^{-1}y^{-1}) \\ &= x(yg^{-1})^{-1} = x(g^{-1}y)^{-1} = x(y^{-1}g) \\ &= (xy^{-1})g. \end{aligned}$$

Ceci prouve que $Z(G)$ est un sous-groupe de G. Montrons qu'il est distingué : soit $x \in Z(G)$ et soit $g \in G$. On a

$$gxg^{-1} = (gx)g^{-1} = (xg)g^{-1} = x(gg^{-1}) = x.$$

En particulier gxg^{-1} est bien dans $Z(G)$. □

Proposition 2.1.6 *Si $\varphi : G \to G'$ est un morphisme de groupes, alors le noyau de φ est distingué dans G.*

Démonstration : Soit $x \in \mathrm{Ker}(\varphi)$ et soit $g \in G$. Comme φ est un morphisme, on a

$$\varphi(g^{-1}xg) = \varphi(g)^{-1}\varphi(x)\varphi(g) = \varphi(g)^{-1}\varphi(g) = 1$$

Ceci prouve que $\mathrm{Ker}(\varphi) \triangleleft G$. □

Armé de cette notion de sous-groupe distingué nous pouvons maintenant passer à la notion de groupe quotient généralisant celle de $\mathbb{Z}/n\mathbb{Z}$.

Soit G un groupe et H un sous-groupe de G. On cherche une condition (nécessaire et) suffisante pour pouvoir mettre une structure de groupe sur le quotient G/H de sorte que la projection canonique $\pi_H : G \to G/H$ soit un morphisme de groupes. C'est en ce sens que l'on dit que la structure de groupe que l'on met sur G/H est *raisonnable*. Rappelons que l'ensemble quotient $G/H := \{xH \mid x \in G\}$ est l'ensemble des classes d'équivalences pour la relation de congruence modulo H définie par

$$\forall x, y \in G, \quad x \equiv y \bmod H \overset{\text{définition}}{\iff} y^{-1}x \in H.$$

Proposition 2.1.7 *Si G/H est un groupe tel que π_H est un morphisme de groupes, alors $H \triangleleft G$.*

Démonstration : Dire que π_H est un morphisme équivaut à dire que :

$$\forall x, y \in G, \quad xH \cdot yH = \pi_H(x) \cdot \pi_H(y) = \pi_H(xy) = xyH.$$

De plus cette loi doit être bien définie donc on a

$$\forall x, y, a, b \in G\, (a = x \bmod H \text{ et } b = y \bmod H) \Rightarrow ab = xy \bmod H.$$

Or par définition on a

$$\begin{aligned} ab = xy \bmod H &\iff abH = xyH \\ &\iff y^{-1}x^{-1}abH = H \\ &\iff y^{-1}x^{-1}ab \in H \end{aligned}$$

Appliquons ceci avec $b := y$ et $a := xh$ où $h \in H$ est un élément quelconque. On obtient que

$$\forall y \in G,\ \forall h \in H, \quad y^{-1}hy \in H,$$

autrement dit que H est distingué dans G. □

Réciproquement :

Proposition 2.1.8 *Soit $H \triangleleft G$. On peut munir G/H d'une structure de groupe, unique, telle que π_H est un morphisme de groupes.*

Démonstration : Pour que π_H soit un morphisme de groupes, on voit que l'on n'a pas le choix : si $X = \pi_H(x)$ et $Y = \pi_H(y)$ sont deux éléments quelconques de G/H, il faut poser

$$X \cdot Y := \pi_H(xy).$$

Comme H est distingué dans G cette loi est bien définie sur $G/H \times G/H$. En effet, soient $x, y, u, v \in G$ tels que $x = u \bmod H$ et $y = v \bmod H$. On veut montrer que $xy = uv \bmod H$. Or on a

$$(uv)^{-1}(xy) = v^{-1}u^{-1}xy = v^{-1}yy^{-1}u^{-1}xy.$$

Or $v^{-1}y \in H$ d'une part et d'autre part $u^{-1}x \in H$, donc en conjuguant par y et car H est distingué dans G, on a aussi $y^{-1}u^{-1}xy \in H$. Ainsi $(uv)^{-1}(xy) \in H$ donc $xy = uv \bmod H$.

On vérifie ensuite immédiatement que cette loi munit G/H d'une structure de groupe ; l'inverse de $X := \pi_H(x)$ étant $X^{-1} := \pi_H(x^{-1})$ et l'élément neutre est $1 := \pi_H(1)$. □

Remarque 2.1.9 Traduisons ceci dans le cas d'un groupe commutatif $(A, +)$ avec une loi notée additivement. Soit B un sous-groupe de A. On a donc : *x est congru à y modulo B* si par définition $x - y \in B$, ce que l'on écrit :

$$\forall x, y \in A, \quad x = y \bmod B \iff x - y \in B.$$

L'ensemble quotient A/B est formé des classes d'équivalence $\mathrm{Cl}(x) = x + B := x \bmod B$. Enfin on note $\pi_B : A \to A/B$ la surjection canonique. Le groupe A étant commutatif, le sous-groupe B est automatiquement distingué et on peut donc munir A/B d'une structure de groupe telle que la projection canonique est un morphisme de groupes. On définit donc une loi $+$ sur A/B telle que

$$\forall x, y \in A, \quad \pi_B(x + y) = \pi_B(x) + \pi_B(y).$$

En traduisant en notation additive ce qui était noté multiplicativement précédemment on voit que :

$$\forall x, y \in A, \quad (x \bmod B) + (y \bmod B) := (x + y) \bmod B.$$

Avec ces notations additives l'inverse de $a \bmod B$ (qui s'appelle l'opposé dans ce cadre additif) est $-a \bmod B$ et le neutre qui se note 0 dans ce cadre additif est $0 := \pi_B(0)$. Enfin le groupe A étant commutatif, on voit que la loi sur A/B est également automatiquement commutative.

Nous pouvons maintenant passer à la *factorisation canonique* des morphismes qui permet de décomposer un morphisme de groupes en composée de projection canonique, isomorphisme et inclusion.

Théorème 2.1.10 *Soit $\varphi : G \to E$ un morphisme de groupes et soit $H \triangleleft G$. Si $H \subset \mathrm{Ker}(\varphi)$, alors il existe un unique morphisme $\bar{\varphi} : G/H \to E$ tel que $\varphi = \bar{\varphi} \circ \pi_H$.*

Démonstration : Le sous-groupe H est distingué dans G donc G/H est un groupe tel que π_H est un morphisme de groupes. Soient $f, g : G/H \to E$ deux morphismes de groupes tels que $g \circ \pi_H = \psi = f \circ \pi_H$. Vérifions que $g = f$: on va voir que f et g coincident point par point.

Soit donc X un élément quelconque de G/H. Par définition (et surjectivité de π_H) il existe $x \in G$ tel que $X = (x \bmod H) = \pi_H(x)$. Donc on a

$$g(X) = g(x \bmod H) = g(\pi_H(x)) = \psi(x) = f(\pi_H(x)) = f(x \bmod H) = f(X).$$

Ceci prouve que $f = g$ et donc l'unicité de l'aplication $\bar{\psi}$. Reste à prouver qu'il existe un tel morphisme de groupes $\bar{\psi}$ satisfaisant $\psi = \bar{\psi} \circ \pi_H$. Supposons pour l'instant qu'il existe une telle application $\bar{\psi}$ et vérifions que c'est un morphisme de groupes. Soient $X, Y \in G/H$. Il existe $x, y \in G$ tels que $X = (x \bmod H)$ et $Y = (y \bmod H)$. On a de plus :

$$\begin{aligned}
\bar{\psi}(XY) &= \bar{\psi}((x \bmod H) \cdot (y \bmod H)) \\
&= \bar{\psi}(\pi_H(x) \cdot \pi_H(y)) \text{ d'où en utilisant que } \pi_H \text{ est un morphisme (car } H \lhd G), \\
&= \bar{\psi}(\pi_H(xy)) \text{ d'où par définition de } \bar{\psi}, \\
&= \psi(xy) \text{ et } \psi \text{ étant un morphisme}, \\
&= \psi(x) \cdot \psi(y) \\
&= \bar{\psi}(X) \cdot \bar{\psi}(Y).
\end{aligned}$$

Finalement si la fonction $\bar{\psi}$ existe, c'est automatiquement un morphisme de groupes. Reste à prouver l'existence de la fonction $\bar{\psi}$. Soit $X = \pi_H(x) = x \bmod H \in G/H$, on pose pour cela : $\bar{\psi}(X) := \psi(x)$. La seule chose à vérifier est que cette application est bien définie : on se donne donc $y \in G$ tel que $x = y \bmod H$ et il reste à voir que $\psi(x) = \psi(y)$. Or

$$\psi(x) = \psi(y) \iff \psi(y^{-1}x) = 0 \iff y^{-1}x \in \mathrm{Ker}(\psi).$$

Par hypothèse H est inclus dans $\mathrm{Ker}(\psi)$ donc $x = y \bmod H$ entraîne que $y^{-1}x \in H \subset \mathrm{Ker}(\psi)$ et l'identité précédente implique que $\bar{\psi}$ est bien définie. □

Corollaire 2.1.11 ***(Factorisation Canonique)*** *Soit $\psi : G \to F$ un morphisme de groupes. Alors ψ se factorise de la façon suivante :*

$$\psi : G \xrightarrow{\pi} G/\mathrm{Ker}(\psi) \xrightarrow{\bar{\psi}} \mathrm{Im}(\psi) \xhookrightarrow{i} F,$$

où π est la projection canonique sur $G/\mathrm{Ker}(\psi)$ et où $i(x) = x$ est l'inclusion naturelle de $\mathrm{Im}(\psi)$ dans F.

De plus le morphisme $\bar{\psi}$ est un isomorphisme de groupes entre $G/\mathrm{Ker}(\psi)$ et $\mathrm{Im}(\psi)$.

Démonstration : On applique la proposition précédente avec $H = \mathrm{Ker}(\psi)$. La seule chose restant à vérifier est l'injectivité de $\bar{\psi}$: soit donc $a \bmod \mathrm{Ker}(\psi)$ dans le noyau de $\bar{\psi}$. On a

$$1 = \bar{\psi}(a \bmod \mathrm{Ker}(\psi)) = \psi(a).$$

Donc a est dans le noyau de ψ. En particulier $a = 1 \bmod \mathrm{Ker}\psi$ d'où l'injectivité de $\bar{\psi}$. □

Corollaire 2.1.12 *Soient $\psi : G \to F$ un morphisme de groupes. Si G est fini alors on a*

$$\mathrm{Card}(G) = \mathrm{Card}(\mathrm{Im}(\psi)) \cdot \mathrm{Card}(\mathrm{Ker}(\psi)).$$

Exemple 2.1.13 Soit $\mathbb{K}$ un corps et soit $n \geq 2$. Notons $\mathrm{GL}_n(\mathbb{K})$ le groupe des matrices carrées inversibles et notons $\mathrm{SL}_n(\mathbb{K})$ le noyau du morphisme déterminant $\det : \mathrm{GL}_n(\mathbb{K}) \to \mathbb{K}^\times$. Ce morphisme étant visiblement surjectif (un élément $x \in \mathbb{K}^\times$ ayant par exemple comme antécédent la matrice diagonale $\mathrm{diag}(x, 1, \ldots, 1)$), on obtient par le corollaire précédent l'isomorphisme

$$\mathrm{GL}_n(\mathbb{K})/\mathrm{SL}_n(\mathbb{K}) \simeq \mathbb{K}^\times.$$

Proposition 2.1.14 *Soit G un groupe, soit $H \triangleleft G$ et soit $\pi_H : G \to G/H$ la projection canonique. Il y a une bijection entre les sous-groupes de G/H et les sous-groupes de G contenant H. Elle est donnée par $E \mapsto \pi_H(E)$ de réciproque $\mathcal{E} \mapsto \pi_H^{-1}(\mathcal{E})$.*

Démonstration : Cf. DM 1 et son corrigé. □

La proposition précédente permet, connaissant les sous-groupes de $\mathbb{Z}$, de retrouver les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$.

2.2 Actions de groupes

Définition 2.2.1 Soit X un ensemble. On note $\mathcal{S}(X)$ l'ensemble des bijections de X dans X. On appelle cet ensemble l'*ensemble des permutations de X*.

Lemme 2.2.2 *Muni de la loi de composition, $\mathcal{S}(X)$ est un groupe de neutre Id_X et l'inverse de f est sa bijection réciproque.*

Démonstration : Immédiat. □

On reviendra plus loin sur l'étude de $\mathcal{S}(X)$ quand $X = \{1, \ldots, n\}$, avec $n \in \mathbb{N}^*$.

Théorème 2.2.3 ***(Cayley)*** *Soit G un groupe. Considérons l'application $\sigma : G \to \mathcal{S}(G)$, $g \mapsto \sigma_g$ avec $\sigma_g(h) := gh$ pour tout $h \in G$. Alors σ est un mrophisme de groupes injectif, autrement dit, G est isomorphe à un sous groupe d'un groupe de permutations.*

Démonstration : Pour tout g, il est clair que σ_g est bijectif (de bijection réciproque $\sigma_{g^{-1}}$) donc l'application est bien définie. C'est visiblement un morphisme de groupes et si $\sigma_g = \mathrm{Id}_G$ alors $g = \sigma_g(1) = 1$ d'où l'injectivité. □

Définition 2.2.4 Soit G un groupe et X un ensemble non vide. Supposons donnée un application

$$G \times X \to X, \ \ (g, x) \mapsto g \cdot x \ \text{ telle que } \ \forall x \in X, \ 1 \cdot x = x \ \text{ et } \ \forall g, g' \in G, \ g \cdot (g' \cdot x) = (gg') \cdot x.$$

On dit que G *opère sur X* ou qu'on a *une action de G sur X*.

Exemple 2.2.5

1. *Action par translation de G sur G : $G \times G \to G$, $(g, x) \mapsto gx$.*
2. *Action par conjuguaison de G sur $H \triangleleft G$: $G \times H \to H$, $(g, h) \mapsto ghg^{-1}$*

Théorème 2.2.6 *Il y a une bijection entre les actions de groupe de G sur X et les morphismes de G dans $\mathcal{S}(X)$, donnée par*

$$(G \times X \to X, \ (g, x) \mapsto g \cdot x) \ \mapsto (G \to \mathcal{S}(X), \ g \mapsto (x \mapsto g \cdot x)).$$

Démonstration : Il suffit d'expliciter la bijection réciproque : c'est l'application qui à un morphisme φ de G dans $\mathcal{S}(X)$ associe l'action $(g,x) \mapsto g \cdot x := (\varphi(g))(x)$. □

Définition 2.2.7 Une action est dite *fidèle* si le morphisme de G dans $\mathcal{S}(X)$ associé à l'action est injectif.

Définition 2.2.8 Une action est dite *transitive* si

$$\forall x, y \in X, \quad \exists g \in G, \ g \cdot x = y.$$

Exemple 2.2.9 : l'action par translation est fidèle et transitive. L'action par conjuguaison de $G \neq \{1\}$ sur son centre n'est pas fidèle ni transitive.

Définition 2.2.10 Soit G un groupe agissant sur un ensemble X et soit $x \in X$. On appelle *orbite de* x, l'ensemble

$$\omega(x) := \{y \in X \mid \exists g \in G \ g \cdot x = x\} = G \cdot x.$$

Notons que l'orbite de x contient toujours l'élément x.

Remarque 2.2.11 Si G agit sur X on peut considérer la relation d'équivalence donnée par

$$\forall x, y \in X, \ x \mathcal{R} y \iff \exists g \in G, \quad g \cdot x = y.$$

Par construction les classes d'équivalences pour cette relation sont les orbites de X pour l'action. En particulier on en déduit :

Proposition 2.2.12 *Les orbites forment une partition de* X.

Définition 2.2.13 Soit G un groupe agissant sur un ensemble X et soit $x \in X$. On appelle stabilisateur de x l'ensemble

$$\mathrm{Stab}(x) := \{g \in G \mid g \cdot x = x\}.$$

Proposition 2.2.14 *Pour tout* $x \in X$, *l'ensemble* $\mathrm{Stab}(x)$ *est un sous groupe de* G. *De plus, l'application surjective de* G *dans* $\omega(x)$, *définie par* $g \mapsto g \cdot x$, *induit par passage au quotient une bijection de* $G/\mathrm{Stab}(x)$ *sur* $\omega(x)$.

Démonstration : On vérifie immédiatement que $\mathrm{Stab}(x)$ est un sous groupe. L'application considérée est surjective par définition de $\omega(x)$. Il suffit de prouver qu'elle est injective et bien définie par passage au quotient. Or on a

$$g \cdot x = g' \cdot x \iff (g'^{-1} g) \cdot x = x \iff g'^{-1} g \in \mathrm{Stab}(x).$$

Ceci prouve à la fois que l'aplication passe au quotient et qu'elle est injective sur le quotient. □

Corollaire 2.2.15 ***Équation aux classes*** *Soit* G *agissant sur un ensemble* X *fini non vide. On a*

$$\mathrm{Card}(X) = \sum_x \mathrm{Card}\omega(x) = \sum_x \mathrm{Card}G/\mathrm{Stab}(x),$$

la somme portant sur un système de représentants des orbites.

Démonstration : On utilise que les orbites forment une partition de X ainsi que la proposition précédente. □

Proposition 2.2.16 *Soit G agissant sur un ensemble X. Soient $x \in X$ et $g \in G$. On a*

$$\mathrm{Stab}(g \cdot x) = g\mathrm{Stab}(x)g^{-1}.$$

Démonstration : On raisonne par équivalences :

$$\begin{aligned} \alpha \in \mathrm{Stab}(g \cdot x) &\iff \alpha \cdot (g \cdot x) = g \cdot x \\ &\iff (\alpha g) \cdot x = g \cdot x \\ &\iff (g^{-1}\alpha g) \cdot x = x \\ &\iff g^{-1}\alpha g \in \mathrm{Stab}(x) \\ &\iff \alpha \in g\mathrm{Stab}(x)g^{-1}. \end{aligned}$$ □

Proposition 2.2.17 *Si G agit sur X et G et X sont finis alors, pour tout $x \in X$, on a : $\omega(x)|\mathrm{Card}G$.*

Démonstration : On utilise que $\omega(x)$ est de même cardinal que $G/\mathrm{Stab}(x)$ et que, G étant fini, ce cardinal est le quotient du cardinal de G par celui de $\mathrm{Stab}(x)$. □

2.3 Groupes de Sylows et p-groupes

2.3.1 Les p-groupes

Définition 2.3.1 Soit G un groupe fini de cardinal p^n avec p premier et $n \geq 0$. On dit que G *est un p-groupe.*

Lemme 2.3.2 *Soit G un p-groupe, opérant sur un ensemble fini X. Notons*

$$X^G := \{x \in X \mid \forall g \in G,\ g \cdot x = x\}.$$

On a

$$\mathrm{Card}(X) = \mathrm{Card}(X^G) \bmod p.$$

Démonstration : On voit que $x \in \omega(x) \iff \omega(x) = \{x\}$. On peut ensuite appliquer l'équation aux classes :

$$\mathrm{Card}(X) = \sum_{x \in I_1} \mathrm{Card}(\omega(x)) + \sum_{x \in I_2} \mathrm{Card}(\omega(x)),$$

où I_1 est un système de représentants des orbites de cardinal 1 et I_2 de celles de cardinal au moins 2. On obtient donc

$$\mathrm{Card}(X) = \mathrm{Card}(X^G) + \sum_{x \in I_2} \mathrm{Card}(\omega(x)).$$

Or on sait que le cardinal de l'orbite divise $p^n = \mathrm{Card}(G)$, donc si l'orbite est de cardinal au moins 2, alors son cardinal est nul modulo p. Ceci permet de conclure. □

Proposition 2.3.3 *Soit G un p-groupe non trivial. Alors le centre de G n'est pas réduit à $\{1\}$.*

Démonstration : On fait agir G sur lui même par conjuguaison. Pour cette action, l'ensemble X^G est exactement $Z(G)$. Donc le lemme précédent entraîne que $Z(G)$ est un multiple de p. Or $1 \in Z(G)$ donc le cardinal de $Z(G)$ est au moins p. □

2.3.2 Les p-Sylows : énoncé du théorème et applications

Dans tout ce paragraphe, G est un groupe fini de cardinal n. On se donne p un nombre premier et on écrit la décomposition de n : $n = p^r m$ avec m premier à p et $r \geq 0$.

Définition 2.3.4 Un sous-groupe de G de cardinal p^r est appelé un *p-Sylow de G.*

Théorème 2.3.5 *Avec les notations précédentes, on a*

1. *Il existe au moins un p-Sylow dans G. Si n_p est le nombre de p-Sylow, alors*
$$n_p = 1 \bmod p \quad \text{et} \quad n_p | m.$$
2. *Les p-Sylows sont deux à deux conjugués (ie pour tout p-Sylows P et Q, il existe $g \in G$ tel que $P = gQg^{-1}$).*

Corollaire 2.3.6 *Soit P un p-Sylow de G. Alors,*
$$P \triangleleft G \iff n_p = 1.$$

Démonstration : Si P est distingué dans G, alors comme les p-Sykow sont conjugués, ils sont en fait tous égaux à P, donc $n_p = 1$. Réciproquement, si $n_p = 1$ alors pour tout $g \in G$, on a gPg^{-1} est un p-Sylow, donc est égal à P, donc P est distingué dans G. □

2.3.3 Les p-Sylows : preuve du théorème

Commençons par traiter un cas particulier et prouvons qu'il existe dans $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ un p-sylow (que l'on va même décrire explicitement). Nous verrons ensuite comment nous ramener dans le cas général à ce cas particulier. Dans toute la suite p est un nombre premier et $n \in \mathbb{N}^*$.

Lemme 2.3.7 *Le cardinal de $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ est $\prod_{i=0}^{n-1}(p^n - p^i)$.*

Démonstration : Se donner un matrice inversible à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ équivaut à se donner une application linéaire de $(\mathbb{Z}/p\mathbb{Z})^n$ dans lui même, qui est bijective. Ceci équivaut donc à se donner l'image $(f_1, \ldots, f_n)$ de la base canonique, de sorte que la famille $(f_1, \ldots, f_n)$ est une base. Ainsi le cardinal recherché est exactement le cardinal de l'ensemble des bases de l'espace vectoriel $(\mathbb{Z}/p\mathbb{Z})^n$. Il nous reste à dénombrer l'ensemble des bases possibles :

Pour le premier vecteur, f_1 : tout élément de $(\mathbb{Z}/p\mathbb{Z})^n$ sauf zéro convient ; il y a donc $p^n - 1$ possibilités.

Pour le second vecteur, f_2 : tout élément qui n'est pas sur la droite engendrée par f_1, $\mathbb{Z}/p\mathbb{Z}f_1$ convient ; il a donc $p^n - p$ possibilités.

On itère l'argument et pour le dernier vecteur : tout élément qui n'est pas dans l'hyperplan $\mathbb{Z}/p\mathbb{Z}f_1 \oplus \cdots \oplus \mathbb{Z}/p\mathbb{Z}f_{n-1}$ engendré par $f_1, \ldots, f_{n-1}$ convient : il y a donc $p^n - p^{n-1}$ possibilités.

En prenant le produit des diverses possibilités on conclut. □

Finalement en factorisant chaque terme $p^n - p^i$ sous la forme $p^i(p^{n-i} - 1)$, on voit que la cardinal de $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ peut se réécrire :

$$\mathrm{Card}\,(\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})) = p^{\sum_{i=0}^{n-1} i}\left(\prod_{i=1}^{n}(p^i - 1)\right) = p^{\frac{n(n-1)}{2}} m \quad \text{avec } m \wedge p = 1.$$

IL s'agit donc de trouver un sous-groupe de $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ de cardinal $p^{\frac{n(n-1)}{2}}$.

Lemme 2.3.8 *L'ensemble* $P := \{(a_{ij}) \in M_n(\mathbb{Z}/p\mathbb{Z}) \mid \forall i,\ a_i i = 1, \quad \text{et} \quad \forall j < i,\ a_{ij} = 0\}$ *est un* p*-Sylow de* $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$.

Démonstration : Tous les éléments de P sont de déterminant 1. Il est clair que c'est un sous-groupe de $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$. De plus pour chaque a_{ij} avec $j > i$, on a p valeurs possibles. Il y a donc $p^{\sum_{i=1}^{n-1} i} = p^{\frac{n(n-1)}{2}}$ matrices dans P qui est donc un p-Sylow de $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$. □

Nous voulons utiliser ceci pour prouver l'existence d'un p-Sylow dans un groupe quelconque.

Lemme 2.3.9 *Soit* G *un groupe fini de cardinal* n *et soit* p *un nombre premier. Alors,* G *est isomorphe à un sous-groupe de* $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$.

Démonstration : Par le théorème de Cayley, on sait que G est isomorphe à un sous-groupe de $\mathcal{S}_n$. Il suffit de prouver que S_n est isomorphe à un sous-groupe de $GL_n(\mathbb{Z}/p\mathbb{Z})$ pour conclure. Pour cela on considère l'application φ de $\mathcal{S}_n$ dans $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ qui à une permutation σ associe la matrice de permutation M_σ définie par son action sur la base canonique par $e_i \mapsto e_{\sigma(i)}$. On vérifie que φ est un morphisme de groupes. De plus le noyau de φ est l'ensemble des σ tels que $M_\sigma = I_n$ ie tels que $e_{\sigma(i)} = e_i$ pour tout i, ie tels que $\sigma(i) = i$ pour tout i, ie tels que $\sigma = \mathrm{Id}$. Donc φ est injectif et ceci conclut. □

Le lemme suivant nous indique que si l'on connait un p-Sylow dans un groupe, on peut trouver un p-Sylow dans tous ses sou-groupes.

Lemme 2.3.10 *Soit* $\mathcal{G}$ *un groupe de cardinal* $p^\alpha m$ *avec* $p \wedge m = 1$ *et* $\alpha \geq 1$. *Soit* $\mathcal{H}$ *un sous-groupe de* $\mathcal{G}$ *et soit* S *un* p*-Sylow de* $\mathcal{G}$. *Il existe* $a \in \mathcal{G}$ *tel que* $aSa^{-1} \cap \mathcal{H}$ *est un* p*-Sylow de* $\mathcal{H}$.

Démonstration : On considère l'action de $\mathcal{G}$ sur $\mathcal{G}/S$ par translation : $(g, xS) \mapsto gxS$. Déterminons son stablisateur :

$$\begin{aligned} \mathrm{Stab}(xS) &= \{g \in \mathcal{G} \mid gxS = xS\} \\ &= \{g \in \mathcal{G} \mid \forall s \in S\ gxs \in xS\} \\ &= \{g \in \mathcal{G} \mid gx \in xS\} \\ &= \{g \in \mathcal{G} \mid g \in xSx^{-1}\} = xSx^{-1}. \end{aligned}$$

De plus on peut considérer la restriction de cette action du sous-groupe H sur l'ensemble $\mathcal{G}/S$. Dans ce cas le même calcul montrer que le stablisateur (que l'on note Stab_H) est

$$\mathrm{Stab}_H(xS) = xSx^{-1} \cap H.$$

Visiblement $\mathrm{Stab}_H(xS)$ est un sous-groupe de xSx^{-1} qui est un p-Sylow (car conjugué à S). Donc $\mathrm{Stab}_H(xS)$ est un p-groupe. Il est de plus inclus dans H. On cherche un x tel que $\mathrm{Stab}_H(xS)$ soit un p-groupe de cardinal maximal, ie tel que $\frac{|H|}{|\mathrm{Stab}_H(xS)|} \wedge p = 1$. Or on sait que $H/Stab_H(xS)$ est en bijection avec l'orbite $\omega_H(xS)$ de xS pour l'action de H sur $\mathcal{G}/S$. En appliquant l'equation aux classes, on a

$$|\mathcal{G}/S| = \sum_x |\omega_H(xS)|$$

où x varie dans un système de représentants des orbites. Si par l'absurde pour tout x on a : p divise $|\omega_H(xS)|$; alors p divise donc $|\mathcal{G}/S|$. Mais S est un p-Sylow de $\mathcal{G}$, donc p est premier avec $\mathcal{G}/S$. Ceci conclut. □

Preuve de l'existence d'un p-Sylow dans un groupe G : On plonge G de cardinal n dans $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ et on applique le lemme précédent avec $\mathcal{G} = \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ et $\mathcal{H} = G$. □

Théorème 2.3.11 ***(Complément à Sylow)*** *Si H est un sous groupe de G et si H est un p-groupe, alors il existe un p-Sylow de G contenant H.*

Preuve de ce théorème et du point (2) du théorème de Sylow : On introduit un p-Sylow S (dont on sait maintenant qu'il existe). Le lemme précédent nous donne l'existence d'un élément $a \in G$ tel que $aSa^{-1} \cap H$ est un p-Sylow de H. Mais H est un p-groupe, c'est donc son propre p-Sylow. Ainsi, $H \subset aSa^{-1}$ qui est un p-Sylow de G. Ceci prouve le théorème. Si on suppose de plus que H est lui même un p-Sylow, alors par cardinalité on voit que $H = aSa^{-1}$ donc tout les p-Sylow sont conjugués. □

Il nous reste maintenant à prouver l'assertion sur le nombre n_p de p-Sylow : on introduit pour cela l'ensemble X de tout les p-Sylow de G. On a $n_p = |X|$. On considère l'action de G sur X par conjuguaison : $(g, S) \mapsto gSg^{-1}$. Soit P un p-sylow de G. Ce groupe induti par restriction une action par conjuguaison de P sur X. De plus P est un p-groupe, donc en notant $X^P := \{S \in X \mid \forall g \in P,\ gSg^{-1} = S\}$, on a

$$n_p = |X| = |X^P| \bmod p.$$

De plus on a $gPg^{-1} = P$ pour tout $g \in P$ donc P est dans X^P. Montrons que c'est le seul élément :

soit S un p-Sylow et G tel que $\forall g \in P$, on a$gSg^{-1} = S$. Soit N le sous-groupe de G engendré par les éléments de S et ceux de P (un élément de N sécrit donc comme un produit de puissances (à coefficients dnas $\mathbb{Z}$) d'éléments de S et de P). Les groupes S et P sont inclus dans N. Ce sont donc des p-Sylow de N (car $N \subset G$), mais par définition, S est stable par conjugaison par tout élément de P et évidemment aussi également par tout élément de S. Donc

$$\forall g \in N,\ gSg^{-1} = S.$$

Autrement dit S est distingué dans N, c'est donc son unique p-Sylow. Donc $S = P$, ie $|X^P| = 1$ donc $n_p = 1 \bmod p$. De plus, les p-Sylow sont conjugués donc

$$|X| = |\omega(P)| = \frac{|G|}{|\mathrm{Stab}(P)|} \mid |G|.$$

Donc n_p divise $|G|$ et est premier avec p, donc n_p divise m. □

2.3.4 Quelques applications de Sylow

Corollaire 2.3.12 *Soit G un groupe de cardinal $n = p^r m$ avec p premier, $r \geq 1$ et m premier à p.*

1. *Pour tout $i \leq r$ il existe un sous-groupe H_i de G de cardinal p^i.*
2. *Si G est de plus un p-groupe, on peut même choisir les H_i distingués dans G.*

Démonstration : Nous allons démontrer le résultat en nous appuyant sur un théorème qui sera prouvé dans un chapitre suivant (le théorème de structure des groupes abéliens finis). Dans G il existe un p-Sylow P. Nous allons travailler dans P (qui est de cardinal p^r) et construire une suite de sous-groupes H_i, distingués dans P de cardinal p^i. Ceci prouvera les deux énoncés. On fait une preuve par récurrence sur r.

Si P est abélien, le théorème de structure des groupes abéliens finis (que l'on prouvera dans un chapitre suivant) nous assure que P est isomorphe à un produit $\prod_{i=1}^{s} \mathbb{Z}/p^{a_i}\mathbb{Z}$ avec $1 \leq a_1 \leq \ldots \leq a_s$. Dans un tel groupe il est facile de construire les groupes H_i.

Si P n'est pas abélien, alors son centre $Z(P)$ est non trivial (car P est un p-groupe) et différent de P, donc de cardinal p^s avec $1 \leq s \leq r-1$. Par hypothèse de récurrence on en déduit l'existence de $H_0, \ldots, H_s$, sous-groupes distingués dans $Z(P)$ (donc dans P vue la définition du centre) de cardinal respectif $p^0, \ldots, p^s$.

Par ailleurs, on peut considérer la projection canonique $\pi : P \to P/Z(P)$ (qui est un morphisme de groupes car $Z(P)$ est distingué dans P). Le groupe quotient $P/Z(P)$ est de cardinal p^{r-s} avec $1 \leq r-s \leq r-1$. En appliquant l'hypothèse de récurrence à $P/Z(P)$ on trouve des groupes $\mathcal{H}_{s+1}, \ldots, \mathcal{H}_{s+(r-s)} = \mathcal{H}_r$ de cardinal respectif $p^1, \ldots, p^{r-s}$, distingués dans $P/Z(P)$. En posant $H_{s+i} := \pi^{-1}(\mathcal{H}_{s+i})$ on obtient ainsi des sous-groupes contenant $Z(P)$, (dont on vérifie aisément qu'ils sont distingués dans P) de cardinal p^{s+i}. Le dernier point découle par factorisation canonique : le projection π restreinte à H_i est surjective sur $\mathcal{H}_i$ et de noyau $Z(P)$ (facile), donc le cardinal de H_i est la produit de celui de $Z(P)$ par celui de $\mathcal{H}_i$.

Finalement on a bien obtenu des H_i comme annoncé. □

Corollaire 2.3.13 *Soit G un groupe de cardinal $n = p^r m$ avec p premier, $r \geq 1$ et m premier à p. Il existe $x \in G$ d'ordre p.*

Démonstration : On applique le corollaire précédent avec $i = 1$. □

2.3.5 Un exemple

Lemme 2.3.14 *Soient P, Q deux sous-groupes distingués d'un groupe fini G, tels que $P \cap Q = \{1\}$ et $|P| \cdot |Q| = |G|$. Alors l'application*

$$\varphi : P \times Q \to G,\ (x, y) \mapsto xy$$

est un isomorphisme de groupes.

Démonstration : Si φ est un morphisme, il suffit par cardinalité de prouver que φ est injectif pour conclure. Or $xy = 1$ implique $x = y^{-1}$. Mais x est dans P et y^{-1} est dans Q. Donc $1 = x = y$, ie φ est injectif. Reste à prouver que φ est un morphisme : soit (a, b) et (x, y) deux couples de $P \times Q$.

$$\varphi((a,b)(x,y)) = \varphi(ax, by) = axby \quad \text{et} \quad \varphi(a,b)\varphi - x, y) = abxy = ax(x^{-1}bx)y.$$

Montrons que $x^{-1}bx = b$ ce qui concluera. On a

$$x^{-1}bxb^{-1} = (x^{-1}bx)b^{-1} \in Q \text{ car } Q \text{ est distingué dans } G,$$

et

$$x^{-1}bxb^{-1} = x^{-1}(bx)b^{-1}) \in P \text{ car } P \text{ est distingué dans } G.$$

Finalement cet élément est dans $P \cap Q = \{1\}$ donc égal à 1. □

Corollaire 2.3.15 *Soit G un groupe de cardinal p^2. Alors G est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou à $(\mathbb{Z}/p\mathbb{Z})^2$.*

Démonstration : Si il y a dans G un élément d'ordre p^2. Alors G est cyclique engendré par cet élément, donc isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$. Sinon tous les éléments sauf 1_G sont d'ordre p. Soit $x \neq 1$ d'ordre p. Notons P le groupe qu'il engendre. Soit $y \in G - P$: il est d'ordre p et on note Q le groupe qu'il engendre. Le groupe G est d'ordre p^2 donc abélien (cf. TD) donc P et Q sont distingués dans G. De plus $|P| \cdot |Q| = p^2 = |G|$. Enfin, si z est dans l'intersection de P et Q : soit $z = 1$, soit z est d'ordre p et engendre donc un sous-groupe de P d'ordre p, donc est égal à P et est de même égal à Q, donc $P = Q$ ce qui est impossible. Donc $P \cap Q = \{1\}$. Le lemme donne donc un isomorphisme entre G et $(\mathbb{Z}/p\mathbb{Z})^2$. □

Exemple : *Soit G un groupe de cardinal 245, alors G est cyclique isomorphe à $\mathbb{Z}/245\mathbb{Z}$ ou est isomorphe à $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/35\mathbb{Z}$.*
Démonstration : Cf. au chapitre suivant, après la preuve du théorème des restes Chinois. □

Chapitre 3

Retour sur $\mathbb{Z}$, divisibilité

3.1 Pgcd dans $\mathbb{Z}$

Lemme 3.1.1 *Soient $a, b \in \mathbb{Z}$. Alors $a|b \iff b\mathbb{Z} \subset a\mathbb{Z}$.*

Démonstration : On a $a|b$ si et seulement si $\exists n \in \mathbb{Z}$ tel que $b = an$ ce qui implique que $\forall \lambda \in \mathbb{Z}$, $b\lambda = an\lambda$. Donc $b\mathbb{Z} \subset a\mathbb{Z}$. Réciproqument, si $b\mathbb{Z} \subset a\mathbb{Z}$, alors $b \times 1$ est dans $a\mathbb{Z}$ donc $\exists n \in \mathbb{Z}$ tel que $b = an$ autrement dit $a|b$. □

Corollaire 3.1.2 *Soient $a, b \in \mathbb{Z}$. On a ($a|b$ et $b|a$) si et seulement si $a\mathbb{Z} = b\mathbb{Z}$ ssi $a = \pm b$.*

Démonstration : Immédiat. □

Définition 3.1.3 Soit $n \in \mathbb{N}^*$ et soient $a_1, \ldots, a_n$ des entiers relatifs non tous nuls. On appelle $\text{pgcd}(a_1, \ldots, a_n)$ *le plus grand diviseur commun positif* des a_i. On le note aussi $a_1 \wedge \ldots \wedge a_n$.

Remarque 3.1.4 Pour tout $i \leq n$ l'entier 1 divise a_i. De plus les a_i étant non tous nuls, on peut supposer que $a_1 \neq 0$ quitte à renuméroter. On voit alors que l'ensemble $D := \{d \in \mathbb{N}^* \mid \forall i \leq n,\ d|a_i\}$ est inclus dans $\{d \in \mathbb{N}^* \mid d|a_1\}$ donc dans $\{1, \ldots, |a_1|\}$. En particulier l'ensemble D est une partie majorée non-vide de $\mathbb{N}$, donc admet un plus grand élément. Ceci justifie l'existence du pgcd.

Notation 3.1.5 Par convention nous poserons $\text{pgcd}(0, \ldots, 0) := 0$.

Proposition 3.1.6 *Soit $n \in \mathbb{N}^*$ et soient $a_1, \ldots, a_n$ des entiers relatifs tous non nuls. On a*

$$\text{pgcd}(a_1, \ldots, a_n) = \prod_{p \in \mathcal{P}} p^{\min\{v_p(a_1), \ldots, v_p(a_n)\}}.$$

Démonstration : Notons $\delta := \text{pgcd}(a_1, \ldots, a_n)$. On a

$$\forall i,\ \delta|a_i \Rightarrow \forall i,\ \forall p \in \mathcal{P},\ v_p(\delta) \leq v_p(a_i) \Rightarrow \forall p \in \mathcal{P},\ v_p(\delta) \leq \min\{v_p(a_i) \mid 1 \leq i \leq n\}.$$

De plus on voit que $p^\alpha | p^\beta \iff \alpha \leq \beta$ donc l'inégalité précédente entraîne :

$$\delta | \prod_{p \in \mathcal{P}} p^{\min\{v_p(a_1), \ldots, v_p(a_n)\}} =: d.$$

Réciproquement pour tout i, on a $\min\{v_p(a_1), \ldots, v_p(a_n)\} \leq v_p(a_i)$ ce qui implique que $d|a_i$ pour tout i. De plus $d \geq 0$, donc $d \leq \delta$ et $\delta|d$ ce qui conclut. □.

Proposition 3.1.7 *Soit $r \in \mathbb{N}^*$ et soient $n, a_1, \ldots, a_r$ des entiers relatifs. On a*

1. $\mathrm{pgcd}(na_1, \ldots, na_r) = |n|\mathrm{pgcd}(a_1, \ldots, a_r)$.
2. *si $\delta := \mathrm{pgcd}(a_1, \ldots, a_r) \neq 0$, alors pour tout i on a, $\frac{a_i}{\delta} \in \mathbb{Z}$ et $\mathrm{pgcd}(\frac{a_i}{\delta} \mid 1 \leq i \leq r) = 1$.*

Démonstration : Donnons une preuve de la première assertion. Quitte à supprimer tous les indices i tels que $a_i = 0$, on peut supposer (et on le fait) que les a_i sont tous non nuls. Si $n = 0$ le résultat est évident. On peut donc supposer $n \neq 0$ et, quitte à remplacer n par son opposé, on peut même supposer que $n \geq 1$. On a par la proposition précédente :

$$\mathrm{pgcd}(na_1, \ldots, na_r) = \prod_{p \in \mathcal{P}} p^{\min\{v_p(na_1), \ldots, v_p(na_r)\}}.$$

Par le lemme 1.3.7 on obtient donc

$$\begin{aligned} \mathrm{pgcd}(na_1, \ldots, na_r) &= \prod_{p \in \mathcal{P}} p^{\min(v_p(n) + v_p(a_i) \mid 1 \leq i \leq r)} \\ &= \prod_{p \in \mathcal{P}} p^{v_p(n)} \prod_{p \in \mathcal{P}} p^{\min(v_p(a_i) \mid 1 \leq i \leq r)} \\ &= |n|\mathrm{pgcd}(a_1, \ldots, a_r). \end{aligned}$$

Nous laissons le second point en exercice. □

3.2 Algorithme d'Euclide sur $\mathbb{Z}$

Étant donnés deux entiers relatifs $a, b \in \mathbb{Z}$ on donne ici un algorithme permettant de calculer leur pgcd $a \wedge b$.

On a $a \wedge b = |a| \wedge |b|$, donc on peut dans la suite supposer que a et b sont positifs.

On a $a \wedge b = b \wedge a$, donc on peut supposer que $a \geq b \geq 0$.

Si $b = 0$ alors par définition $a \wedge b = a$.

Sinon : on pose $(A_0, U_0, V_0) := (a, 1, 0)$ de sorte que $A_0 = aU_0 + bV_0$ et $(A_1, U_1, V_1) = (b, 0, 1)$ de sorte que $A_1 = aU_1 + bV_1$.

Supposons écrit (A_n, U_n, V_n) de sorte que $A_n = aU_n + bV_n$. Alors deux possibilités : si $A_n = 0$ alors $a \wedge b = A_{n-1} = aU_{n-1} + bV_{n-1}$; sinon on effectue la division euclidienne de A_{n-1} par A_n pour obtenir :

$$A_{n-1} = A_n Q_n + A_{n+1} \text{ avec } 0 \leq A_{n+1} < A_n.$$

Posons $U_{n+1} = U_{n-1} - U_n Q_n$ et $V_{n+1} = V_{n-1} - V_n Q_n$. On a alors

$$A_{n+1} = aU_{n+1} + bV_{n+1}.$$

Il reste pour conclure à vérifier deux choses :

1. Tout d'abord que l'algorithme ci-dessus termine au bout d'un nombre fini d'étapes. Or la suite A_i est une suite d'entiers positifs qui est visiblement strictement décroissante.
2. Ensuite que si $A_n = 0$ on a bien $a \wedge b = A_{n-1}$. Montrons pour se faire par récurrence sur n que $d(:= a \wedge b) = A_n \wedge A_{n+1}$ si n est tel que $A_n \neq 0$.

(a) Si $n = 0$ on a $A_0 = a$ et $A_1 = b$ d'où le résultat.

(b) Si la propriété est vraie au rang $n-1$ et si n est tel que $A_n \neq 0$. On a dans ce cas $A_{n+1} = A_{n-1} - A_n Q_n$ donc les diviseurs de A_n et de A_{n-1} sont les mêmes que ceux de A_n et A_{n+1}. Donc le pgcd d de a et b est le même par hypothèse de récurrence que celui de A_n et de A_{n-1} donc que celui de A_n et A_{n+1}.

Remarque 3.2.1 Cet algorithme permet d'une part de calculer le pgcd de a et b, mais il donne par ailleurs une relation (dite *de Bézout*) : $d = au + bv$.

Proposition 3.2.2 ***(Bézout)*** *Soient $a, b \in \mathbb{Z}$. On a*

$$d = \text{pgcd}(a, b) \Rightarrow \exists u, v \in \mathbb{Z} \quad d = au + bv.$$

Démonstration : C'est l'algorithme ci-dessus. □

Définition 3.2.3 Deux éléments $a, b \in \mathbb{Z}$ sont dits *premiers entre eux* si $a \wedge b = 1$.

Théorème 3.2.4 ***(Bézout)*** *On a*

$$a \wedge b = 1 \iff \exists u, v \in \mathbb{Z} \quad au + bv = 1.$$

Démonstration : Le sens $\Rightarrow$ est donné par l'implication précédente. Réciproquement, si $d = a \wedge b$ alors d divise a et b donc d divise $au + bv = 1$. Or d est positif, donc $d = 1$. □

3.3 Applications

3.3.1 Résolution de $ax + by = c$, $a, b, c \in \mathbb{Z}$ en les inconnues $x, y \in \mathbb{Z}$

Lemme 3.3.1 ***(Gauss)*** *Soit $a, b \in \mathbb{Z}$ tels que $a \wedge b = 1$ et tels que a divise bc. Alors a divise c.*

Démonstration : Les nombres a et b étant premiers entre eux, on a une relation de Bézout : il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$. De plus il existe $k \in \mathbb{Z}$ tel que $ak = bc$ donc on obtient :

$$c = (au + bv)c = auc + bvc = auc + akv = a(uc + kv).$$

Autrement dit, a divise c. □

Nous pouvons utiliser ce lemme pour résoudre les équations diophantiennes du type donné dans le titre de ce paragraphe :

Théorème 3.3.2 *Soient $a, b, c \in \mathbb{Z}$. Si $a \wedge b$ ne divise pas c, l'équation $ax + by = c$ n'a pas de solution dans $\mathbb{Z}^2$. Sinon l'ensemble des solutions de cette équation est l'ensemble*

$$\left\{(x, y) \in \mathbb{Z}^2 \mid \exists k \in \mathbb{Z}, \quad x = c'u_0 - b'k, \ y = c'v_0 + a'k\right\},$$

où a', b' et c' sont définis par $a = (a \wedge b)a'$, $b = (a \wedge b)b'$, $c = (a \wedge b)c'$, et où u_0, v_0 sont tels que $au_0 + bv_0 = a \wedge b$.

Démonstration : Si le $\text{pgcd}(a,b)$ ne divise pas c, il n'y a visiblement pas de solution (évident par l'absurde). Sinon

$$\exists u_0, v_0 \text{ tels que } au_0+bv_0 = d \text{ et } \exists a', b', c' \text{ tels que } c'd = c,\ a'd = d,\ b'd = b \text{ et } \text{pgcd}(a', b') = 1.$$

Notons (x, y) un couple solution. On a donc $ac'u_0+bc'v_0 = ax+by$, donc $a(c'u_0-x) = b(y-c'v_0)$ soit encore

$$a'(c'u_0 - x) = b'(y - c'v_0).$$

En appliquant le lemme de Gauss à cette dernière identité on voit que a' divise $y - c'v_0$, donc il existe $k \in \mathbb{Z}$ tel que $y = c'v_0 + a'k$. En remplaçant dans l'équation on en tire $x = c'u_0 - b'k$. Réciproquement on vérifie que tout les couples de cette forme sont solution de l'équation. □

3.3.2 Inversibles et générateurs dans $\mathbb{Z}/n\mathbb{Z}$

Proposition 3.3.3 *Soient $n \geq 2$ et $x \in \mathbb{Z}$. On a équivalence entre les trois propriétés suivantes :*

1. *Le groupe engendré par $x \bmod n$ est $(\mathbb{Z}/n\mathbb{Z}, +)$.*
2. *$x \bmod n$ est inversible (pour la multiplication).*
3. $\text{pgcd}(x, n) = 1$.

Démonstration : Prouvons tout d'abord que (2) équivaut à (3) :

$$\begin{aligned}
\bar{x} \text{ est inversible} &\iff \exists y \in \mathbb{Z},\ \bar{x} \cdot \bar{y} = \bar{1} \\
&\iff \exists y \in \mathbb{Z},\ n | xy - 1 \\
&\iff \exists y \in \mathbb{Z},\ \exists a \in \mathbb{Z},\ an = xy - 1 \\
&\iff \exists y \in \mathbb{Z},\ \exists a \in \mathbb{Z},\ xy - an = 1 \\
&\iff \text{pgcd}(x, n) = 1.
\end{aligned}$$

Soit maintenant $x \in \mathbb{Z}$ tel que $x \bmod n$ est inversible. Soit $y \in \mathbb{Z}$ tel que $y \bmod n$ est l'inverse de $x \bmod n$. On a pour tout entier $k \in \mathbb{Z}$

$$\begin{aligned}
k \bmod n &= k \times (1 \bmod n) \\
&= k \times (yx \bmod n) \\
&= ky \times (x \bmod n).
\end{aligned}$$

On voit sur cette dernière écriture que cet élément apartient au groupe engendré par $x \bmod n$, autrement dit que $\mathbb{Z}/n\mathbb{Z} = \langle x \bmod n \rangle$. Réciproquement si $\mathbb{Z}/n\mathbb{Z} = \langle x \bmod n \rangle$, alors il existe un entier k tel que $k \times (x \bmod n) = 1 \bmod n$. Donc $kx \bmod n = 1 \bmod n$ autrement dit $k \bmod n$ est l'inverse de $x \bmod n$. □

Définition 3.3.4 Étant donnés deux éléments $a, b \in \mathbb{Z}$, on définit le $\text{ppcm}(a, b)$ comme étant le plus petit entier positif, multiple commun de a et b. On définit de même le ppcm d'une famille finie d'éléments.

Proposition 3.3.5 *On a* $\text{ppcm}(a_1,\dots,a_r) = \prod_{p\in\mathcal{P}} p^{\sup\{v_p(a_1),\dots,v_p(a_r)\}}$.

Démonstration : Même preuve que pour le pgcd. □

Remarque 3.3.6 Si $n \in \mathbb{Z}$ et $a, b \in \mathbb{Z}$ on a $\text{ppcm}(na, nb) = |n|\text{ppcm}(a, b)$.

Proposition 3.3.7 *Si* $n \in \mathbb{Z}$ *et* $a, b \in \mathbb{Z}$ *on a* $\text{pgcd}(a, b) \times \text{ppcm}(a, b) = |ab|$.

Démonstration : On peut par exemple le prouver en utilisant les interprétations des pgcd et ppcm en terme de valuations. □

3.4 Lemme Chinois

Lemme 3.4.1 *Si* A, B *sont deux anneaux, alors* $A \times B$ *est un anneau (pour les lois définies coordonnées par coordonnées) et* $(A \times B)^\times = A^\times \times B^\times$.

Démonstration : Évident. □

Lemme 3.4.2 *Soit* $d, n \in \mathbb{N} - \{0\}$ *tels que* d *divise* n. *Alors la fonction* $\varphi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ *définie par* $\varphi(x \bmod n) := x \bmod d$ *est bien définie et est un morphisme d'anneaux.*

Démonstration : Le seul point non trivial est de vérifier que l'application φ est bien définie. Soient donc $x, y \in \mathbb{Z}$ tels que $x \bmod n = y \bmod n$. Il existe $k \in \mathbb{Z}$ tel que $x = y + kn$. Or d divise n donc il existe $\lambda \in \mathbb{Z}$ tel que $n = \lambda d$, donc en particulier $x = y + (k\lambda)d$ donc $x = y \bmod d$, autrement dit, φ ne dépend pas du choix d'un représentant modulo n donc est bien définie.□

Théorème 3.4.3 ***(Restes Chinois)*** *Soient* $a, b \in \mathbb{N} - \{0, 1\}$. *L'application* $\varphi : \mathbb{Z}/ab\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ *définie par* $\varphi(x \bmod ab) = (x \bmod a, x \bmod b)$ *est un morphisme d'anneaux. De plus, si* a *et* b *sont premiers entre eux alors* φ *est un isomorphisme de bijection réciproque :*

$$\psi(x \bmod a, y \bmod b) = bvx + auy \bmod ab \quad \text{où} \quad au + bv = 1 \ \text{ est une relation de Bézout.}$$

Si a *et* b *ne sont pas premiers entre eux, alors les anneaux* $\mathbb{Z}/ab\mathbb{Z}$ *et* $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ *ne sont pas isomorphes.*

Démonstration : Par le lemme 3.4.2 l'application φ est bien définie et est clairement un morphisme d'anneaux. En terme de cardinalité, on a $ab = \text{Card}(\mathbb{Z}/ab\mathbb{Z}) = \text{Card}(\mathbb{Z}/a\mathbb{Z}) \times \text{Card}(\mathbb{Z}/b\mathbb{Z})$ et la relation $|\text{Ker}(\varphi)| \times |\text{Im}(\varphi)| = ab$ implique donc que φ et un isomorphisme si et seulement si φ est injective. Or ceci se vérifie aisément : si $x = 0 \bmod a$ et $x = 0 \bmod b$ alors a et b divisent x et étant premiers entre eux, on en déduit que ab divise x autrement dit que $x = 0 \bmod ab$. On pourrait également vérifier à la main que $\varphi \circ \psi = \text{Id}$ et que $\psi \circ \varphi = \text{Id}$. Concernant le dernier point notons $d = \text{pgcd}(a, b) \geq 2$ et supposons par l'absurde qu'il existe un morphisme d'anneaux f de $\mathbb{Z}/ab\mathbb{Z}$ vers le produit $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. Alors il existe a_1, b_1 tels que $a_1 d = a$ et $b_1 d = b$ et $\text{pgcd}(a_1, b_1) = 1$. De plus $f(1) = (1, 1)$ et

$$f(a_1 b_1 d \bmod ab) = (a_1 d b_1 \bmod a, a_1 b_1 d \bmod b) = (ab_1 \bmod a, a_1 b \bmod b) = (0, 0).$$

Or $1 \leq a_1 b_1 d < ab$ car $d \geq 2$ donc $a_1 b_1 d \neq 0 \bmod ab$ ce qui donne une contradiction avec l'injectivité de f. □

Remarque 3.4.4 En modifiant légèrement l'argument donné pour la preuve du second point du théorème précédent, on pourrait même montrer que : "Si a et b ne sont pas premiers entre eux, alors les groupes $\mathbb{Z}/ab\mathbb{Z}$ et $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ ne sont pas isomorphes." Nous laissons ceci en exercice.

Corollaire 3.4.5 *Soient a, b deux entiers premiers entre eux. Alors l'isomorphisme φ précédent induit un isomorphisme de groupes entre les inversibles*

$$\varphi : (\mathbb{Z}/ab\mathbb{Z})^\times \to (\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times .$$

Exemple : *Soit G un groupe de cardinal 245, alors G est cyclique isomorphe à $\mathbb{Z}/245\mathbb{Z}$ ou est isomorphe à $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/35\mathbb{Z}$.*
Démonstration : En appliquant le théorème de Sylow on voit que $n_7 = n_5 = 1$ donc l'unique 7-Sylow : P_7 est distingué dans G et de même, l'unique 5-Sylow, P_5 est distingué dans G. Si $x \in P_5 \cap P_7$ alors l'ordre de x divise 5 et divise 7^2 donc est égal à 1. Donc $\mathcal{P}_5 \cap P_7 = \{1\}$. Nous pouvons donc appliquer le lemme 2.3.14 : G est isomorphe au produit $P_5 \times P_7$. De plus P_5 est de cardinal le nombre premier 5, donc est cyclique isomorphe à $\mathbb{Z}/5\mathbb{Z}$. Le groupe P_7 est de cardinal 7^2 donc on peut appliquer le corollaire 2.3.15 : P_7 est isomorphe à $(\mathbb{Z}/7\mathbb{Z})^2$ ou à $\mathbb{Z}/7^2\mathbb{Z}$. Finalement en appliquant le lemme des restes Chinois on peut conclure. □

3.5 Fonction indicatrice d'Euler

Théorème 3.5.1 ***(Petit théorème de Fermat)*** *Soit p un premier et soit $a \in \mathbb{Z}$. On a $a^p = a \bmod p$. De plus, si $\mathrm{pgcd}(a, p) = 1$ alors $a^{p-1} = 1 \bmod p$.*

Démonstration : Soit $a \in \mathbb{Z}$. Si $\mathrm{pgcd}(a, p) \neq 1$ alors $p|a$ donc $a \bmod p = a^p \bmod p = 0 \bmod p$. Sinon $a \bmod p \neq 0$ donc $\bar{a}$ est inversible dans le corps $\mathbb{Z}/p\mathbb{Z}$ donc son ordre divise $p - 1$ donc $a^{p-1} = 1 \bmod p$. □

Exemple 3.5.2 Calculons le reste de la division euclidienne de 666^{999} par 13 : $666 = 51 \times 13 + 3 = 3 \bmod 13$ donc $666^{999} = 3^{999} \bmod 13$. Or le petit théorème de Fermat nous dit que $3^{12} = 1 \bmod 13$ car 13 est premier. On effectue donc la division euclidienne de 999 par 12 : $999 = 83 \times 12 + 3$ pour en déduire que $666^{999} = 3^{999} = 3^3 = 1 \bmod 13$. □

Définition 3.5.3 On appelle *fonction indicatrice d'Euler* la fonction $\varphi : \mathbb{N}^* \to \mathbb{N}$ donnée par $n \mapsto \mathrm{Card}(\mathbb{Z}/n\mathbb{Z})^\times$.

Remarque 3.5.4 On a

$$\varphi(n) = \mathrm{Card}\{x \bmod n \mid x \text{ engendre } \mathbb{Z}/n\mathbb{Z}\} = \{x \in \mathbb{Z} \mid 1 \leq x \leq n \text{ et } \mathrm{pgcd}(x, n) = 1\}.$$

La formule suivante nous permet de calculer la valeur de $\varphi(n)$:

$$\text{Si } n = \prod_{p \in \mathcal{P}} p^{v_p(n)} \text{ alors } \varphi(n) = \prod_{p \in \mathcal{P}} p^{v_p(n)-1}(p-1).$$

Démonstration : Ceci se prouve par récurrence sur le nombre de facteurs permiers intervenant dans la décomposition en facteurs premiers de l'entier n.

1. Si $n = p^d$ alors

$$\begin{aligned}\varphi(n) &= \text{Card}\{x \in \{1, \dots, p^d\} \mid \text{pgcd}(x, p^d) = 1\} \\ &= p^d - \text{Card}\{p, 2p, \dots, p^{d-1}p\} = p^d - p^{d-1} \\ &= p^{d-1}(p-1).\end{aligned}$$

2. Si $n = \prod_{i=1}^{d+1} p_i^{a_i}$. On a $n = \alpha\beta$ avec $\text{pgcd}(\alpha, \beta) = 1$ et $\alpha := \prod_{i=1}^{d} p_i^{a_i}$ et $\beta := p_{d+1}^{a_{d+1}}$. Le corollaire 3.4.5 précédent nous donne l'égalité de cardinaux

$$\text{Card}\,(\mathbb{Z}/ab\mathbb{Z})^\times = \text{Card}\,(\mathbb{Z}/a\mathbb{Z})^\times \times \text{Card}\,(\mathbb{Z}/b\mathbb{Z})^\times .$$

Donc $\varphi(n) = \varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$. L'hypothèse de récurrence et l'initialisation de la récurrence nous permettent alors de conclure. □

Lemme 3.5.5 ***(Euclide)*** *Soient $a, b \in \mathbb{Z}$ et soit p premier.*

$$p|ab \Rightarrow p|a \quad \text{ou} \quad p|b.$$

Démonstration : On peut donner trois preuves de ce résultat :

1. Un calcul de valuation p-adique.
2. On sait que $\mathbb{Z}/p\mathbb{Z}$ est intègre donc $ab = 0 \bmod p$ implique que a ou b est nul modulo p.
3. Si p ne divise pas a alors, comme $p|ab$ et que $\text{pgcd}(p, a) = 1$ le lemme de Gauss implique que $p|b$. □

Remarque 3.5.6 On déduit immédiatement de ce résultat l'unicité de la décomposition en facteurs premiers d'un entier.

Application : le système de cryptographie RSA.

Corollaire 3.5.7 *Soit $n \geq 2$. Il y a exactement $\varphi(d)$ éléments d'ordre d dans $(\mathbb{Z}/n\mathbb{Z}, +)$ pour tout les diviseurs d de n.*

Démonstration : Soit d un diviseur de n et soit $x \in \mathbb{Z}/n\mathbb{Z}$ d'ordre d. On sait que le groupe H engendré par x est l'unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ de cardinal d (par le théorème 1.6.4). Il est cyclique isomorphe à $\mathbb{Z}/d\mathbb{Z}$. Dans $\mathbb{Z}/d\mathbb{Z}$ il y a exactement $\varphi(d)$ éléments d'ordre d et l'ordre est conservé par isomorphisme. Ceci conclut. □

3.6 Structure de $(\mathbb{Z}/n\mathbb{Z})^\times$

Théorème 3.6.1 *Soit p premier. Le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.*

Démonstration : Nous allons utiliser le résultat suivant (qui se prouve par récurrence et en utilisant de la division euclidienne) : si k est un corps et $P \in k[X]$ un polynôme de degré $d \geq 1$ alors P admet au plus d racines. Notamment le polynôme $X^d - 1$ admet au plus d racines dans $\mathbb{Z}/p\mathbb{Z}$ si $d \geq 1$.

Posons G le groupe des inversibles de $\mathbb{Z}p\mathbb{Z}$, de cardinal $p-1$ et pour tout entier $d|p-1$, notons $G_d = \{x \in G \mid x \text{ est d'ordre } d\}$. On a : G est la réunion disjointe des G_d donc

$$p-1 = |G| = \sum_{d|p-1} |G_d|.$$

Nous voulons prouver que $|G_{p-1}| \geq 1$. Fixons un entier d divisant $p-1$. Soit G_d est vide, soit il existe $x_0 \in G_d$. Dans ce second cas, le groupe H_d engendré par x_0 ; étant isomorphe à $\mathbb{Z}/d\mathbb{Z}$, possède exactement $\varphi(d)$ éléments d'ordre d. Donc

$$|G_d| = 0 \quad \text{ou} \quad |G_d| \geq \varphi(d).$$

Par ailleurs, $\mathbb{Z}/(p-1)\mathbb{Z}$ est la réunion disjointe des $A_d := \{x \in \mathbb{Z}/(p-1)\mathbb{Z} \mid x \text{ est d'ordre d}\}$. Par le corollaire 3.5.7 on sait que A_d est de cardinal exactement $\varphi(d)$, d'où la formule :

$$p-1 = \sum_{d|p-1} \varphi(d). \tag{3.1}$$

Enfin on sait que $|H_d| = d$ et donc que pour tout $y \in H_d$, on a $y^d = 1$. Si $z \in G_d$ est d'ordre d alors $z^d = 1$. Or les racines du polynôme $X^d - 1$ sont toutes dans H_d, donc $z \in H_d$. Donc $|G_d| \leq \varphi(d)$ et par ce qui précède on en déduit que

$$|G_d| = 0 \quad \text{ou} \quad |G_d| = \varphi(d).$$

Autrement dit, $G_d = \varepsilon(d)\varphi(d)$ où $\varepsilon(d) \in \{0, 1\}$. Finalement on tire de ceci que

$$\sum_{d|p-1} \varphi(d) = p-1 = |G| = \sum_{d|p-1} |G_d| = \sum_{d|p-1} \varepsilon(d)\varphi(d).$$

On en conclut que pour tout d (et notamment pour $d = p-1$) on a $\varepsilon(d) = 1$. □

Remarque 3.6.2 Attention $(\mathbb{Z}/4\mathbb{Z})^\times$ est cyclique de cardinal 2, mais le groupe des inversibles de $\mathbb{Z}/8\mathbb{Z}$ n'est pas cyclique : il est composé de 4 éléments, tous d'ordre divisant 2, donc ne peut être isomorphe à $\mathbb{Z}/4\mathbb{Z}$ (il est en fait isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$). Plus généralement on a le théorème suivant.

Théorème 3.6.3 *Soit p un nombre premier.*

1. *Le groupe $(\mathbb{Z}/p^r\mathbb{Z})^\times$ est cyclique (isomorphe à $(\mathbb{Z}/p^{r-1}(p-1)\mathbb{Z})$) si p est premier impair et $r \geq 2$.*
2. *Le groupe $(\mathbb{Z}/2^r\mathbb{Z})^\times$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z}$ si $r \geq 3$.*

Nous commençons par la preuve dans le cas impair :

Lemme 3.6.4 *Soit p premier impair, $k \in \mathbb{N}^*$. On a*

$$(1+p)^{p^k} = 1 + \lambda p^{k+1} \quad \text{avec } \lambda \in \mathbb{N}^* \text{ premier à } p.$$

Démonstration : La preuve se fait par récurrence sur $k \geq 1$. Pour $k = 1$ on développe

$$(1+p)^p = \sum_{j=0}^{p} C_p^j p^j.$$

Ainsi il existe un entier u tel que $(1+p)^p = 1 + p^2 + up^3 = 1 + p^2(1+up)$ qui est bien de la forme voulue.
Supposons le résultat vrai jusqu'au rang k. On a

$$(1+p)^{p^k} = 1 + \lambda p^{k+1} \text{ avec } \lambda \in \mathbb{N}^* \text{ premier à } p.$$

On en déduit :

$$(1+p)^{p^{k+1}} = (1+\lambda p^{k+1})^p = 1 + \sum_{j=1}^{p-1} C_p^j \lambda^j p^{(k+1)j} + \lambda^p p^{(k+1)p}.$$

Pour $j = 1$ on a le terme λp^{k+2} puis pour $j \geq 2$ on peut mettre p^{k+3} en facteur. On a donc un entier u tel que

$$(1+p)^{p^{k+1}} = 1 + p^{k+2}(\lambda + up).$$

Ceci prouve le lemme par récurrence. □

On peut donc maintenant passer à la preuve du théorème dans le cas p impair : on a $(1+p)^{p^{r-1}} = 1 \bmod p^r$ et par ailleurs $(1+p)^{p^{r-2}} = 1 + \lambda p^{r-1}$ avec p ne divisant pas λ. Notamment $(1+p)^{p^{r-2}} \neq 1 \bmod p^r$ et par conséquent on en déduit que $1+p$ est d'ordre p^{r-1} dans $(\mathbb{Z}/p^r\mathbb{Z})^\times$. Soit alors φ le morphisme surjectif suivant

$$\varphi \ : \ (\mathbb{Z}/p^r\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times, \quad x \bmod p^r \mapsto x \bmod p.$$

Soit $x_0 \in (\mathbb{Z}/p^r\mathbb{Z})^\times$ tel que $\varphi(x_0)$ engendre le groupe cyclique $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$. L'ordre de x_0 est un multiple de $p-1$ donc dans le groupe cyclique $< x_0 >$ engendré par x_0, il y a un élément y_0 d'ordre $p-1$. Or le groupe $(\mathbb{Z}/p^r\mathbb{Z})^\times$ est abélien donc l'élément $(1+p)y_0$ est d'ordre $p^{r-1}(p-1)$ dans $(\mathbb{Z}/p^r\mathbb{Z})^\times$ qui est donc cyclique. □

Passons maintenant à la preuve du théorème dans le cas $p = 2$. L'idée est assez similaire à la preuve du cas impair.

Lemme 3.6.5 *Soit $k \in \mathbb{N}^*$. On a $(5)^{2^k} = 1 + \lambda 2^{k+2}$ avec λ impair.*

Démonstration : La preuve se fait par récurrence sur $k \geq 1$. Pour $k = 1$ on développe

$$(5)^2 = (1+4)^2 = 1 + 3 \cdot 8.$$

Supposons le résultat vrai jusqu'au rang k. On a

$$(5)^{2^k} = 1 + \lambda 2^{k+2} \text{ avec } \lambda \text{ impair.}$$

On en déduit :

$$(5)^{2^{k+1}} = (1+\lambda 2^{k+2})^2 = 1 + \lambda 2^{k+3} + \lambda^2 2^{2k+4}.$$

Ceci prouve le lemme par récurrence. □

Soit alors $r \geq 3$ et φ le morphisme surjectif suivant

$$\varphi \ : \ (\mathbb{Z}/2^r\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times, \quad x \bmod 2^r \mapsto x \bmod 4.$$

Posons $N = \ker \varphi$. Par factorisation canonique le cardinal de N est 2^{r-2} et par le lemme précédent 5 d'ordre 2^{r-2} et est dans N qui est donc cyclique. On vérifie alors que $N \times \{-1, 1\}$ est isomorphe à $(\mathbb{Z}/2^r\mathbb{Z})^\times$ en appliquant le lemme 2.3.14. □

Théorème 3.6.6 *Soit $n \geq 1$ un entier. On a*

$$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times .$$

Démonstration : Cf. TD. □

Corollaire 3.6.7 *Le groupe des automorphismes de groupes de $\mathbb{Z}/n\mathbb{Z}$ est abélien de cardinal $\varphi(n)$.*

Démonstration : Immédiat. □

Chapitre 4

Groupes abéliens de type fini

4.1 Sommes directes, familles libres, familles génératrices

Définition 4.1.1 Soit I un ensemble non vide et $(A_i)_{i\in I}$ une famille de groupes abéliens. On note $\bigoplus_{i\in I} A_i$ et on appelle *somme directe (externe) des* A_i le sous-ensemble du produit $\prod_{i\in I} A_i$ constitué des familles $(x_i)_{i\in I}$ telles que tous les $x_i \in A_i$ sont nuls sauf un nombre fini (on dit dans ce cas que *les* x_i *sont presque tous nuls*).

Proposition 4.1.2 *Muni de l'addition terme à terme le produit* $\prod_{i\in I} A_i$ *est un groupe abélien et la somme directe* $\bigoplus_{i\in I} A_i$ *en est un sous-groupe.*

Démonstration : Immédiat. □

Définition 4.1.3 Soit A un groupe abélien et S un sous-ensemble (non-vide) de A. On appelle *groupe engendré par* S et on note $< S >$ le plus petit sous-groupe de A contenant S. Concretement on a

$$< S >= \left\{ x \in A \mid \exists n \in \mathbb{N},\ \exists s_1, \ldots, s_n \in S,\ \exists \lambda_1, \ldots, \lambda_n \in \mathbb{Z},\quad x = \sum_{i=1}^{n} \lambda_i s_i \right\}.$$

Attention : les coefficients λ_i sont dans $\mathbb{Z}$ et n'ont aucun rapport avec le groupe A.

Exemple 4.1.4 Le groupe $\mathbb{Z}$ est engendré par $\{1\}$. Il est également engendré par $\{-1\}$. Remarquons qu'il est également engendré par l'ensemble $\{5{,}27\}$. (Pourquoi ?)

Pour i_0 fixé, on identifie le groupe A_{i_0} au sous-groupe de $\bigoplus_{i\in I} A_i$ constitué des familles $(x_i)_{i\in I}$ telles que $\forall i \in I,\ i \neq i_0 \Rightarrow x_i = 0$. Avec cette identification le groupe $\bigoplus_{i\in I} A_i$ est visiblement engendré par la réunion $\bigcup_{i\in I} A_i$ et si $x = (x_i)_{i\in I} \in \bigoplus_{i\in I} A_i$ alors $x = \sum_{i\in I} x_i$ avec les $x_i \in A_i$ presque tous nuls.

Définition 4.1.5 Soit A un groupe abélien et soit $(A_i)_{i\in I}$ une famille de sous-groupes de A. On pose

$$\varphi : \bigoplus_{i\in I} A_i \to A,\ (x_i)_{i\in I} \mapsto \sum_{i\in I} x_i$$

le morphisme correspondant aux inclusions $A_i \subset A$.

1. On dit que *les* A_i *sont en somme directe (interne) dans* A si le morphisme φ est injectif.

2. On dit que A *est la somme directe (interne) des* A_i si le morphisme φ est bijectif. On écrit alors, par abus de notations, $A = \bigoplus_{i\in I} A_i$.

Attention à ne pas confondre les sommes directes externes et internes. Par exemple si on pose $A_1 = A_2 = \mathbb{Z}$ on peut former la somme directe (externe) $\mathbb{Z}\oplus\mathbb{Z}$. Par contre si on travaille dans le groupe abélien $A = \mathbb{Z}$ et que l'on considère les sous-groupes $A_1 = A_2 = \mathbb{Z}$ alors A_1 et A_2 ne sont pas en somme directe (interne) dans A ! Par contre, en toute généralité, la somme directe externe $A := \bigoplus_{i\in I} A_i$ d'une famille de groupes abéliens $(A_i)_{i\in I}$ est la somme directe interne des sous-groupes A_i vus dans A.

Remarque 4.1.6 Si l'ensemble I est fini, ce qui sera en pratique le plus souvent le cas pour nous, on voit sur les définitions que $\bigoplus_{i\in I} A_i = \prod_{i\in I} A_i$.

Notation 4.1.7 Si I est quelconque et que les groupes A_i sont tous égaux à un même groupe A, on notera $A^{(I)}$ plutôt que $\bigoplus_{i\in I} A$, et A^I plutôt que $\prod_{i\in I} A$.

Comme pour la situation bien connue en algèbre linéaire sur les K-ev sur un corps K, pour se donner un morphisme de groupes abéliens dont le départ est une somme directe de groupes abéliens il (faut et il) suffit de se donner des morphismes dont le départ sont les différents facteurs de la somme :

Lemme 4.1.8 *Soit $(A_i)_{i\in I}$ une famille de groupes abéliens et B un groupe abélien. Soit pour tout $i \in I$ des morphismes $\varphi_i : A_i \to B$. Il existe un unique morphisme $\varphi : \bigoplus_{i\in I} A_i \to B$ tel que pour tout $i \in I$ on a $\varphi_{|A_i} = \varphi_i$.*

Démonstration : Si φ et ψ coincident sur tous les A_i alors ils coincident sur la somme car les A_i engendrent $\bigoplus_{i\in I} A_i$. Ceci prouve l'unicité. Pour l'existence, il suffit de poser pour $x = (x_i)_{i\in I} \in \bigoplus_{i\in I} A_i$, la formule $\varphi(x) := \sum_{i\in I} \varphi_i(x_i)$, la somme étant bien définie car les x_i (donc les $\varphi_i(x_i)$) sont presque nuls. □

4.2 Familles libres, familles génératrices

Dans tout ce paragraphe, on notera A un groupe abélien. Comme pour les espaces vectoriels sur un corps K, on peut définir sur A la notion de familles libres et de familles génératrices, le corps des scalaires étant dans ce cadre remplacé par l'anneau $\mathbb{Z}$. Il faut toutefois faire attention aux analogies et à l'intuition que nous donne l'algèbre linéaire dans ce cadre, certains résultats classiques sur les espaces vectoriels devenant faux dans le cadre des groupes abéliens, comme nous allons le voir dans le paragraphe suivant.

Définition 4.2.1 Soit I un ensemble non-vide et $(x_i)_{i\in I}$ une famille d'éléments de A. On dit que la famille $(x_i)_{i\in I}$ est *libre* dans A si pour toute famille presque nulle $(\lambda_i)_{i\in I}$ d'éléments de $\mathbb{Z}$, on a

$$\sum_{i\in I} \lambda_i x_i = 0 \;\Rightarrow\; \forall i \in I,\ \lambda_i = 0.$$

Définition 4.2.2 Soit I un ensemble non-vide et $(x_i)_{i\in I}$ une famille d'éléments de A. On dit que la famille $(x_i)_{i\in I}$ est *génératrice* dans A si tout élément de A s'écrit comme combinaison linéaire finie à coefficients entiers des x_i :

$$\forall a \in A,\ \exists n \in \mathbb{N},\ \exists (i_1, \ldots, i_n) \in I^n,\ \exists \lambda_1, \ldots, \lambda_n \in \mathbb{Z},\quad a = \sum_{k=1}^{n} \lambda_k x_{i_k}.$$

Donnons deux exemples pour illustrer ces notions (on laisse en exercice les vérifications) :

1. Si $A = \mathbb{Z}$, la famille à un seul élément $\{n\}$ est libre pour tout entier non-nul n. La famille $\{n\}$ est génératrice si et seulement si $n = \pm 1$.
2. Si $n \geq 2$ est un entier et $A = \mathbb{Z}/n\mathbb{Z}$ alors la famille $\{1 \bmod n\}$ est génératrice mais n'est pas libre (car $n \cdot 1 \bmod n = 0$ dans $\mathbb{Z}/n\mathbb{Z}$, mais $n \neq 0$ DANS $\mathbb{Z}$!).

Définition 4.2.3 Un groupe abélien A qui est engendré par une famille finie est dit *de type fini.*

Proposition 4.2.4 *Si A est un groupe abélien de type fini engendré par n éléments, C un groupe abélien et $\varphi : A \to C$ un morphisme surjectif de groupes. Alors C est de type fini et on peut choisir un système de générateurs de cardinal $s \leq n$.*

Démonstration : Notons $\{e_1, \ldots, e_n\}$ une famille génératrice de A. On vérifie immédiatement que la famille $\{\varphi(e_1), \ldots, \varphi(e_n)\}$ engendre C. □

Proposition 4.2.5 *Soit $\varphi : A \to B$ un morphisme entre deux groupes abéliens tel que* $\ker(\varphi)$ *et* $\mathrm{Im}(\varphi)$ *sont de type finis. Alors le groupe de départ, A est de type fini.*

Démonstration : Soit $y_1 = \varphi(x_1), \ldots, y_r = \varphi(x_r)$ un système de générateurs pour l'image de φ. Soit x dans A. Il existe des entiers $n_1, \ldots, n_r \in \mathbb{Z}$ tels que $\varphi(x) = \sum_{i=1}^r n_i y_i = \varphi(\sum_{i=1}^r n_i x_i)$. On en déduit que l'élément $x - \sum_{i=1}^r n_i x_i$ est dans le noyau $\ker(\varphi)$. Si $z_1, \ldots, z_k$ est un ensemble de générateurs du noyau, on voit donc qu il existe des entiers $m_i \in \mathbb{Z}$ tels que

$$x = \sum_{i=1}^{r} n_i x_i + \sum_{j=1}^{k} m_i z_i.$$

Finalement ceci prouve que A engendré par les $x_1, \ldots, x_r, z_1, \ldots, z_k$. □

Théorème 4.2.6 *Soit A un groupe abélien de type fini et soit B un sous-groupe de A. Alors B est de type fini.*

Démonstration : On fait une récurrence sur le nombre de générateurs n de A. Si $n = 0$, (respectivement $n = 1$) le resultat est trivial (respectivement connu, les sous-groupes de $\mathbb{Z}$ étant les $d\mathbb{Z}$, pour d parcourant les entiers). Supposons que A est engendré par n éléments $(e_1, \ldots, e_n)$ et soit B un sous-groupe de A. Notons $\pi : \mathbb{Z}^n \to A$ le morphisme surjectif défini par $\pi((x_1, \ldots, x_n)) := \sum_{i=1}^n x_i e_i$. Notons K le sous groupe $\pi(\mathbb{Z}^{n-1} \times \{0\})$. Il est de type fini, engendré par au plus $n-1$ éléments par la proposition 4.2.4. Notons $p : A \to A/K$ la projection canonique. Le groupe $p(B)$ est monogène car c'est un sous-groupe de A/K et ce dernier est engendré par $p(\pi((0, \ldots, 0, 1)))$ (exercice !). Par ailleurs, $\ker(p_{|B}) = B \cap K \subset K$ est de type fini par hypothèse de récurrence. Ainsi le morphisme

$$p_{|B} : B \to A/K$$

a son image et son noyau de type fini. Donc le groupe de départ, B est de type fini par la proposition précédente 4.2.5. □

4.3 Groupes abéliens libres, bases

Définition 4.3.1 Soit A un groupe abélien. On dit qu'une famille $(e_i)_{i\in I}$ d'éléments de A est *une base de A* si cette famille est libre et génératrice, autrement dit si tout élément x de A s'écrit de manière unique

$$x = \sum_{i\in I} \lambda_i e_i \quad \text{avec les } \lambda_i \in \mathbb{Z} \text{ presque tous nuls.}$$

Un groupe abélien qui possède une base est dit *libre*.

Notons que dire que A est libre de base $(e_i)_{i\in I}$ équivaut à dire que les e_i sont tous d'ordre infinis et que A est la somme directe de ses sous-groupes $\mathbb{Z}e_i$, $i \in I$.

Exemple 4.3.2 Donnons tout de suite quelques exemples et contre-exemples :

1. "De toute famille génératrice on peut extraire une base" : Faux ! Considérer $\{2, 3\}$ dans $\mathbb{Z}$.
2. "Une famille génératrice minimale est une base" : Faux ! Considérer $\{2, 3\}$ dans $\mathbb{Z}$.
3. "Toute famille libre peut se compléter en une base" : Faux ! Considérer $\{2\}$ dans $\mathbb{Z}$.
4. "Toute famille libre maximale est une base" : Faux ! Considérer $\{2\}$ dans $\mathbb{Z}$
5. " Si A est libre et de type fini alors A admet une base finie"' : Vrai mais pas évident a priori ! Cf. un peu plus loin une preuve.
6. Les groupes $\mathbb{Z}^n$ sont libres pour tout entier $n \geq 1$
7. Par convention on dit que $\{0\}$ est libre de base l'ensemble vide.
8. Un groupe abélien fini A non réduit à $\{0\}$, de cardinal $n \geq 1$ n'est jamais libre (si $x \in A$ alors $nx = 0$ donc aucun élément x ne peut faire partie d'une famille libre, ie il n'y a pas de famille libre dans A, a fortiori pas de base).

Définition 4.3.3 Soit A un groupe abélien. On dit que A *est sans torsion* si pour tout $x \in A$ et pour tout $\lambda \in \mathbb{Z}$ on a

$$\lambda x = 0 \Rightarrow (\lambda = 0 \text{ ou } x = 0)\,.$$

Si A est un groupe abélien, on note A_{tor} le *sous-groupe de torsion de A* constitué des éléments x de A tels qu'il existe un entier non nul $\lambda \in \mathbb{Z}$ tel que $\lambda x = 0$. On vérifie aisément que c'est bien un sous-groupe de A. Le groupe A est sans torsion si et seulement si $A_{\text{tor}} = \{0\}$.

Proposition 4.3.4 *Si A est un groupe abélien libre, alors A est sans torsion.*

Démonstration : On note $(e_i)_{i\in I}$ une base de A et on se donne $x \in A$ que l'on décompose dans cette base : $x = \sum_{i\in I} \lambda_i e_i$. Soit $n \geq 1$ un entier tel que $nx = 0$. On a alors $\sum_{i\in I} n\lambda_i e_i = 0$ et, la famille (e_i) étant libre, on en déduit que pour tout $i \in I$, on a $n\lambda_i = 0$. Comme n est non nul, dans l'anneau intègre $\mathbb{Z}$ ceci implique que tout les λ_i sont nuls, donc que $x = 0$. □

Exemple 4.3.5 Le groupe $(\mathbb{Q}, +)$ est sans torsion mais il n'est pas libre (exercice : supposer que $\mathbb{Q}$ est libre de base $(e_i)_{i\in I}$; fixer e l'un des vecteurs de la base et considérer l'élément $e/2 \in \mathbb{Q}$ puis conclure). On verra par contre plus tard qu'un groupe abélien de type fini sans torsion est libre.

Attention : si A est un groupe et e_1, e_2 deux éléments de A tels que $A = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2$. Ceci ne signifie pas que A est libre de base $\{e_1, e_2\}$, mais entraîne a priori seulement que A est

engendré par $\{e_1, e_2\}$. Il n'y a aucune raison pour que la famille $\{e_1, e_2\}$ soit libre ! Par exemple si $A = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ et $e_1 = (1 \bmod 2, 0 \bmod 3)$ et $e_2 = (0 \bmod 2, 1 \bmod 3)$. On a $2e_1 + 3e_2 = 0$ donc la famille n'est pas libre et pourtant $A = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2$.

Proposition 4.3.6 *Soit A un groupe abélien libre et soit $(e_i)_{i\in I}$ une base de A. Soit B un groupe abélien et $(y_i)_{i\in I}$ une famille d'éléments de B. Il existe un unique morphisme de groupes $\varphi : A \to B$ tel que pour tout $i \in I$, on a $\varphi(e_i) = y_i$.*

Démonstration : Les e_i engendrent A, l'unicité en découle. Pour l'existence, on décompose un élément quelconque $x = \sum_{i\in I} n_i e_i$ de A dans la base des (e_i) et on pose

$$\varphi(x) := \sum_{i\in I} n_i y_i.$$

On vérifie alors immédiatement que ceci définit bien un morphisme de groupes. □

Théorème 4.3.7 *Soit A un groupe abélien libre de type fini. Alors A admet une base finie. De plus toutes les bases de A ont même cardinal, appelé* ***le rang de*** *A.*

Démonstration : Montrons tous d'abord que A admet une base finie. Nous montrerons ensuite qu'elles ont toutes même cardinal. Soit donc $(x_i)_{i\in I}$ une base de A (non nécessairement finie) et soit $(y_1, \ldots, y_n)$ une famille de générateurs de A. Pour tout $j \in \{1, \ldots, n\}$ il existe un sous ensemble fini d'indice I_j de I et des entiers relatifs $(r_i) \in \mathbb{Z}^{I_j}$ tels que

$$y_j = \sum_{i\in I_j} r_i x_i.$$

Posons $J := \bigcup_{j=1}^{n} I_j$. On voit que la famille des $(x_i)_{i\in J}$ est libre (comme sous-famille des $(x_i)_{i\in I}$) et génératrice car elle permet d'obtenir tous les $y_1, \ldots, y_n$ qui sont générateurs. C'est donc une base finie de A.

Considérons une base $(e_1, \ldots, e_{n_1})$ et une famille libre $(f_1, \ldots, f_{n_2})$ de A. On va montrer que $n_2 \leq n_1$ ce qui entraînera notamment que toute les bases sont finies : le groupe A est isomorphe à $\mathbb{Z}^{n_1}$ via l'isomorphisme : $\varphi : \sum_{i=1}^{n_1} \lambda_i e_i \mapsto (\lambda_1, \ldots, \lambda_{n_1})$. Dans $\mathbb{Z}^{n_1}$ l'image par φ de la famille $(f_1, \ldots, f_{n_2})$ est encore libre (sur $\mathbb{Z}$) car un isomorphisme conserve la liberté (exercice facile). Or on peut voir $\mathbb{Z}^{n_1}$ comme étant inclus dans $\mathbb{Q}^{n_1}$ et on constate alors que dans le $\mathbb{Q}$-espace vectoriel $\mathbb{Q}^{n_1}$ l'image par φ de la famille $(f_1, \ldots, f_{n_2})$ est encore libre (sur $\mathbb{Q}$) (libre sur $\mathbb{Z}$ implique libre sur $\mathbb{Q}$: exercice facile). Ceci implique $n_2 \leq n_1$. Ainsi si $(f_i)_{i\in I}$ est une base elle est en particulier libre donc de cardinal majoré par n_1. En échangeant les roles de (e_i) et (f_j) on voit alors que $n_1 = n_2$. □

Remarque 4.3.8 Pour la preuve du théorème précédent, nous avons utilisé des résultats liés à la théorie de la dimension sur les $\mathbb{Q}$-espaces vectoriels. Il est possible de s'en passer et par exemple d'utiliser plutôt le Lemme Matriciel Fondamental 4.3.11 qui suit.

Théorème 4.3.9 ***(de la Base Adaptée)*** *Soit G un groupe abélien libre de rang fini r et soit B un sous-groupe de G. Alors B est libre de rang $s \leq r$. De plus il existe une base $(e_1, \ldots, e_r)$ de G et il existe des entiers (uniquement déterminés) $d_1 | \cdots | d_s$ qui se divisent et tels que $d_1 \geq 1$ tels que : la famille $(d_1 e_1, \ldots, d_s e_s)$ est une base de B.*

Démonstration : Nous démontrons ici l'existence et nous occuperons de l'unicité des d_i plus tard. Soit $(x_i)_{1\leq i\leq r}$ une base quelconque de G. On sait par le théorème 4.2.6 que B est un sous-groupe de type fini. Soit $(y_i)_{1\leq i\leq l}$ un ensemble de générateurs (quelconque) de B. On peut écrire les y_j dans la base des $(x_i)_i$:

$$\forall j,\quad \exists A_{1j},\dots,A_{rj}\in\mathbb{Z}\ \text{ tels que }\ y_j=\sum_{i=1}^{r}A_{ij}x_i.$$

Autrement dit, les colonnes de la matrice $A:=(A_{ij})$ sont les coordonnées des y_j écrits dans la base $(x_i)_i$ de G. Nous allons maintenant effectuer des opérations sur les lignes et les colonnes de A :

1. retrancher à une colonne j un multiple α d'une colonne $k\neq j$, ie remplacer le générateur y_j par $y_j-\alpha y_k$ pour $\alpha\in\mathbb{Z}$;
2. retrancher à une ligne j un multiple α d'une ligne $k\neq j$, ie écrire une nouvelle famille (x'_i) dans laquelle $x_i=x'_i$ pour $i\neq j$ et $x_k=x'_k-\alpha x'_j$ pour $\alpha\in\mathbb{Z}$;
3. changer le signe d'une ligne (respectivement d'une colonne), ce qui revient à remplacer x_i (respectivement y_i) par $-x_i$ (respectivement $-y_i$) ;
4. permuter des lignes (respectivement des colonnes), ce qui revient à permuter les x_i (respectivement les y_i).

Toutes ces opérations ne changent visiblement pas la nature des (x_i) : il forment toujours une base ; et ne changent pas non plus la nature des (y_i) : ils forment toujours une famille génératrice. Montrons qu'en effectuant ces opérations il est possible d'aboutir à une matrice A' de la forme

$$A'=\begin{pmatrix} d_1 & & & & & \\ & \ddots & & & & \\ & & d_s & & & \\ & & & 0 & & \\ & & & & \ddots & \end{pmatrix},$$

où les $(d_i)_{1\leq i\leq s}$ avec $s\leq\min\{r,l\}$ sont des entiers positifs tels que $d_1|\cdots|d_s$ et $d_1\geq 1$. La base cherchée est alors celle dans laquelle la matrice A' est écrite.

Montrons comment, partant de la matrice A, on peut aboutir à la matrice A' en effectuant les opérations précédentes. C'est un procédé purement algorithmique qui est une variante du Pivot de Gauss sur $\mathbb{Z}$. Si $A=0$ il n'y a rien à faire. Sinon

1. On pose :
$$a:=\min\{|a_{ij}|\mid\forall i,j\text{ tels que }a_{ij}\neq 0\}.$$
Quitte à permuter lignes et colonnes on peut supposer que $a=|a_{11}|$ puis quitte à changer le signe de la première ligne on peut supposer que $a=a_{11}$. Pour $i\in\{2,\dots,r\}$ on effectue la division euclidienne de a_{i1} par a :
$$a_{i1}=q_ia+\delta_i\ \text{ avec }\ q_i\in\mathbb{Z}\ \text{ et }\ 0\leq\delta_i<a.$$
De même pour $j\in\{2,\dots,l\}$ on effectue la division euclidienne de a_{1j} par a :
$$a_{1j}=q'_ja+\delta'_j\ \text{ avec }\ q'_j\in\mathbb{Z}\ \text{ et }\ 0\leq\delta'_j<a.$$
On retranche ensuite q_i fois la première ligne à la ligne i et de même q'_j fois la première colonne à la colonne j. On obtient alors de nouveaux coefficients $a_{i1}=\delta_i$ et $a_{1j}=\delta'_j$.

(a) Si pour tout i et j on a $\delta_i = \delta'_j = 0$ alors on passe à l'étape 2 ci-dessous.

(b) Sinon on choisit un a_{1j} ou un a_{i1} non nul que l'on replace en position $(1,1)$ par échange de lignes/colonnes et on réitère le procédé précédent. À chaque itération la valeur a_{11} obtenue diminue strictement donc le procdé termine.

2. À la fin de l'étape précédente on obtient une matrice de la forme

$$\begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & A_1 & \\ 0 & & & \end{pmatrix}.$$

(a) Si a_{11} divise tous les éléments de A_1 on pose $d_1 := a$ et on itère le procédé avec la sous-matrice A_1 (en jouant donc uniquement sur les lignes $L_2, \ldots$ et $C_2, \ldots$ de A). Par itération on conclut.

(b) Si a ne divise pas tous les éléments A_1 : notons $a_{i_0 j_0}$ un élément qui n'est pas divisé par a, on ajoute la ligne i_0 à la ligne 1 (ce qui ne modifie pas a_{11} et on reprend tout le processus à l'étape 1 en faisant la division euclidienne de $a_{i_0 j_0}$ par a_{11} puis en itérant l'étape 1. On obtient finalement une matrice

$$\begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & A_1 & \\ 0 & & & \end{pmatrix}$$

comme avant mais avec un nouveau coefficient a_{11} strictement plus petit (car on a fait au moins une division euclidienne). Le procédé termine donc par itération et on arrive finalement à une telle matrice avec a_{11} qui divise tous les coefficients de A_1. □

Remarque 4.3.10 Attention, une base adaptée (e_i) comme dans le théorème précédent n'est pas unique en général.

Notons que dans le cadre de la preuve précédente nous avons en particulier prouvé l'existence dans le lemme matriciel suivant (sur $\mathbb{Z}$) qui permet de déduire les résultats essentiels concernant les groupes abéliens de type fini (GATF) et les groupes abéliens libres de type fini (GALTF).

Lemme 4.3.11 ***(Lemme Matriciel Fondamental)*** *Soit $r, n \geq 1$ deux entiers et soit $A \in M_{r,n}(\mathbb{Z})$ une matrice rectangulaire (r,n) à coefficients dans $\mathbb{Z}$. Il existe $P \in \mathrm{GL}_r(\mathbb{Z})$ et il existe $Q \in \mathrm{GL}_n(\mathbb{Z})$ telle que*

$$PAQ^{-1} = \begin{pmatrix} d_1 & & & & \\ & \ddots & & & \\ & & d_s & & \\ & & & 0 & \\ & & & & \ddots \end{pmatrix},$$

où les $(d_i)_{1 \leq i \leq s}$ avec $s \leq \min\{r,n\}$ sont des entiers positifs tels que $d_1 | \cdots | d_s$ et $d_1 \geq 1$, appelés ***facteurs invariants de*** *A. Ils sont de plus entièrement déterminés par la matrice A.*

Admettons pour l'instant l'unicité que sur laquelle nous reviendrons plus tard.

Revenons au théorème de la base adaptée et voyons concretement comment faire sur un exemple. Partant d'une base $\mathcal{B}$ de G, on écrit un ensemble de générateurs du sous-groupe B dans cette base et ceci nous fournit une matrice A. Le procédé algorithmique de la preuve nous fournit alors une base $\mathcal{E}$ de G telle que, en notant $P_{\mathcal{E}\to\mathcal{B}}$ la matrice de passage de $\mathcal{E}$ à $\mathcal{B}$ et en notant Q la matrice inversible correspondant aux changements dans les générateurs du sous-groupe B, alors la matrice

$$P_{\mathcal{E}\to\mathcal{B}}AQ$$

est de la forme diagonale annoncée dans le théorème. La matrice $P_{\mathcal{E}\to\mathcal{B}}$ qui indique les opérations faites sur les lignes de A est celle qui nous intéresse, ou plus exactement son inverse : $P_{\mathcal{B}\to\mathcal{E}}$ qui exprime la nouvelle base $\mathcal{E}$ dans l'ancienne base $\mathcal{B}$. concretement :

Exemple 4.3.12 : Soit $G = \mathbb{Z}^4$ pour lequel on choisit comme base, la base canonique, $\mathcal{B} = \{e_1, \ldots, e_4\}$ et soit B le sous-groupe de G engendré par les vecteurs $y_1 = (1, 2, 0, 0)$, $y_2 = (0, 2, 8, 0)$, $y_3 = (1, 2, 8, 0)$. On cherche le rang de B et une base adaptée $\mathcal{E}$. La matrice A associée est la suivante :

$$A = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 2 & 2 & 2 & 0 \\ 0 & 8 & 8 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Plutot que de suivre naivement l'algorithme on va tacher de minimiser le nombre d'opération afin que la matrice $P := P_{\mathcal{E}\to\mathcal{B}}$ à inverser soit la plus simple possible. Notons x, y, z, t les ligne de la matrice P. En soustrayant la colonne 1 à la colonne 3, on note que A est équivalente à

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & 2 & 0 & 0 \\ 0 & 8 & 8 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Ceci ne change pas la matrice P (qui n'est autre que l'identité à l'initialisation de l'algorithme). On effectue ensuite l'opération $L_2 \leftarrow L_2 - 2L_1$ dans A pour obtenir

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 8 & 8 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

En écrivant les lignes, la matrice P est changée de la facon suivante en : $x, y - 2x, z, t$. On effectue ensuite l'opération $C_2 \leftarrow C_2 - C_3$ dans A pour obtenir

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 8 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

La matrice P est inchangée par cette opération. Finalement on en déduit que le rang de B est 3, ses invariants étant $d_1 = 1, d_2 = 2, d_3 = 8$. De plus la matrice P à inverser est la suivante :

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Son inverse est

$$P^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

et on en déduit donc qu'une base adaptée $\mathcal{E}$ de $\mathbb{Z}^4$ est donnée par les vecteurs

$$v_1 = (1, 2, 0, 0),\ v_2 = e_2,\ v_3 = e_3, v_4 = e_4.$$

Avant de conclure ce paragraphe, disons quelques mots sur l'unicité des invariants (d_i) dans le lemme matriciel fondamental (et donc dans le théorème de la base adaptée) : nous donnerons une preuve de cette unicité plus loin comme conséquence de l'unicité obtenue pour les groupes abéliens de type fini (cf. paragraphe suivant). Il existe cependant une preuve directe que nous esquissons ici, pour les lecteurs connaissant la notion de mineurs d'ordre k d'une matrice :

1. Notons déjà que d_1 est le pgcd des coefficients de A (car le pgcd des coefficients de A et de PAQ^{-1} sont les mêmes, ou dit autrement le sous-groupe de $\mathbb{Z}$ engendré par les coefficients de la matrice ne change pas par les opérations sur les lignes et colonnes que l'on fait). Ainsi d_1 est uniquement déterminé.
2. Notons $m_k(A)$ le pgcd des mineurs d'ordre k de A. On a l'assertion suivante :

   $$m_k(PAQ^{-1}) = m_k(A).$$

   Si ceci est vrai alors $m_k(A) = d_1 \dots d_k$ et les d_i sont donc uniquement déterminés. Il reste à prouver l'assertion. On va en fait montrer (esquisser) que si P est une matrice (quelconque) à coefficients entiers, alors

   $$m_k(A) | m_k(PA).$$

   En utilisant ceci avec une matrice P inversible on aura alors

   $$m_k(A) | m_k(PA) | m_k(P^{-1}PA) = m_k(A)$$

   d'où $m_k(A) = m_k(PA)$ et en transposant on obtient de même que $m_k(AQ) = m_k(A)$ ce qui prouve l'assertion. Reste à prouver la relation de divisibilité : ceci se fait directement en exprimant les mineurs de PA comme combinaisons linéaires à coefficients entiers des mineurs de A ce qui provient in fine du fait que les lignes de PA sont des combinaisons linéaires des lignes de A à coefficients dans $\mathbb{Z}$ (puisqu'on multiplie A à gauche par une matrice inversible dans $\mathbb{Z}$). □

4.4 Groupes abéliens de type fini

Lemme 4.4.1 *Soit M un groupe abélien et $(M_i)_{i\in I}$ des sous-groupes de M tels que $M = \bigoplus_{i\in I} M_i$. Soit par ailleurs pour tout $i \in I$, des sous-groupes N_i de M_i et posons $N := \bigoplus_{i\in I} N_i$. On a l'isomorphisme suivant :*

$$M/N \simeq \bigoplus_{i\in I} M_i/N_i.$$

Démonstration : Soit $x \in M$ et soit $x = \sum_{i\in I} x_i$ sa décomposition selon les M_i. Considérons le morphisme de groupe φ définit par :

$$\varphi : M \to \bigoplus_{i\in I} M_i/N_i, \quad x \mapsto (x_i \bmod N_i)_{i\in I}.$$

Le morphisme φ est surjectif par construction. Il suffit de montrer que son noyau est N pour conclure par factorisation canonique. Soit donc x dans le noyau de φ. On voit que $x_i = 0 \bmod N_i$ pour tout $i \in I$ donc $x_i \in N_i$ pour tout $i \in I$. Or N est la somme des N_i, donc x est dans N. Réciproquement si x est dans N il est clair que $\varphi(x) = 0$ ce qui conclut. □

L'énoncé principal de ce paragraphe est le suivant.

Théorème 4.4.2 ***(de structure des GATF)*** *Soit A un groupe abélien de type fini. Il existe des entiers $r, s \geq 0$ et il existe des entiers $d_1|\cdots|d_s$ qui se divisent et tels que $d_1 \geq 2$ tels que*

$$A \simeq \mathbb{Z}^r \oplus \bigoplus_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}.$$

De plus les entiers, r et s ainsi que les (d_i) sont uniquement déterminés par A.

Comme pour le théorème de la base adaptée nous allons tout d'abord donner une preuve de l'existence puis nous prouverons l'unicité dans le paragraphe suivant.

Démonstration : C'est une conséquence assez directe du théorème de la base adaptée : soit $f : \mathbb{Z}^n \to A$ un morphisme surjectif. Notons N son noyau et prenons une base de $\mathbb{Z}^n$ adaptée à N : $v_1, \ldots, v_n$. Il existe alors un entier s et des entiers $d_1|\cdots|d_s$ tels que $d_1 \geq 1$ et tels que

$$\mathbb{Z}^n = \bigoplus_{i=1}^{n} \mathbb{Z}v_i \quad \text{et} \quad N = \bigoplus_{i=1}^{s} d_i\mathbb{Z}v_i.$$

En quotientant et en utilisant le lemme précédent, on obtient que

$$M \simeq \mathbb{Z}^n/N \simeq \mathbb{Z}^{n-s} \times \prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}.$$

On conclut en éliminant de cette dernière formule les facteurs triviaux (avec $d_i = 1$). □

Remarque 4.4.3 On voit aisément sur l'écriture précédente que le sous groupe de A des éléments d'ordre fini, que l'on note A_{tor} s'identifie au groupe $\prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}$.

Corollaire 4.4.4 *Un groupe abélien de type fini est libre si et seulement si il est sans torsion.*

Remarque 4.4.5 Comme on l'a vu avec l'exemple de $\mathbb{Q}$ cet énoncé est faux en général si on ne suppose pas le groupe de type fini.

4.5 Quelques exemples d'applications

4.5.1 Groupes abélien donné par une présentation

Définition 4.5.1 Soit $A \in \mathcal{M}_{r,n}(\mathbb{Z})$ une matrice et G un groupe abélien. On dit que G *est donnée par la présentation* $(g_1, \dots, g_n)$ *avec les relations* $A \begin{pmatrix} g_1 \\ \vdots \\ g_n \end{pmatrix} = 0$ si le morphisme

$$\theta : \mathbb{Z}^n \to G, \quad (x_1, \dots, x_n) \mapsto \sum_{i=1}^{n} x_i g_i$$

est surjectif et de noyau engendré par les lignes de A.

On souhaite connaitre la structure de G, ie ses invariants $d_1 | \dots | d_s$.

Le noyau $\ker\theta$ est un sous-groupe de $\mathbb{Z}^n$, donc est libre et il est engendré par les colonnes de la matrice ${}^tA \in \mathcal{M}_{n,r}(\mathbb{Z})$. On peut donc calculer ses invariants par l'algorithme donné pour le théorème de la base adaptée : il existe $P \in \mathrm{GL}_n(\mathbb{Z})$ et $Q \in \mathrm{GL}_r(\mathbb{Z})$ tel que

$P^tAQ = D$ avec D diagonale ayant sur la diagonale les invariants $d_1 | \dots | d_s$ et $s \leq \min(r, n)$.

On obtient ainsi une base adaptée $(e_1, \dots, e_n)$ de $\mathbb{Z}^n$ telles que $(d_1 e_1, \dots, d_s e_s)$ est une base de $\ker\theta$. En écrivant le quotient de $\mathbb{Z}^n$ par $\ker\theta$ dans la base $(e_1, \dots, e_n)$ et en appliquant la factorisation canonique au morphisme θ, on a donc

$$G \simeq \mathbb{Z}^n / \ker\theta \simeq \mathbb{Z}^{n-s} \times \prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}.$$

Quitte à enlever les facteurs triviaux correspondants aux $d_i = 1$ on obtient ainis les invariants de G comme désiré.

4.5.2 Résolution d'un système d'équations linéaires dans $\mathbb{Z}$

Soit comme dans le paragraphe précédent $A \in \mathcal{M}_{r,n}(\mathbb{Z})$. On veut cette fois résoudre le système

$$AX = 0$$

où $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ est l'inconnue à valeurs dans $\mathbb{Z}^n$.

Notons $\mathcal{S}$ l'ensemble des solutions. C'est un sous-groupe de $\mathbb{Z}^n$. Il est donc libre. De plus on peut appliquer le lemme de réduction matricielle sur $\mathbb{Z}$ à la matrice A : il existe $P \in \mathrm{GL}_r(\mathbb{Z})$ et $Q \in \mathrm{GL}_n(\mathbb{Z})$ telles que

$PAQ = D$ avec D diagonale ayant sur la diagonale les invariants $d_1 | \dots | d_s$ et $s \leq \min(r, n)$.

Notons que s n'est autre que le rang de A. Le système à résoudre s'écrit donc $P^{-1}DQ^{-1}X = 0$. En posant

$$Y = Q^{-1}X, \quad \text{le système se réécrit} \quad DY = 0.$$

La matrice D étant diagonale ce système se résoud immédiatement : notons $e_1, \dots, e_n$ les vecteurs colonne de la base canonique de $\mathbb{Z}^n$, on voit que une base des solutions de $DY = 0$ est donnée par $e_{s+1}, \dots, e_n$. Ainsi les vecteurs $X_i := Qe_i$ pour i variant entre $s+1$ et n forment une base de $\mathcal{S}$ ensemble des solutions de $AX = 0$. Cet ensemble est donc un sous-groupe libre de rang $n - s$ où s est le rang de A. On a

$$\mathcal{S} := \{ \sum_{j=s+1}^{n} \lambda_i X_i \in \mathbb{Z}^n \mid \lambda_{s+1}, \dots, \lambda_n \in \mathbb{Z} \}.$$

Notons que $\mathcal{S}$ est le noyau du morphisme $\varphi : \mathbb{Z}^n \to \mathbb{Z}^r$ donné par $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto AX$. On peut donc aussi se poser la question des invariants du quotient $\mathbb{Z}^n/\mathcal{S}$: si s est le rang de A on a vu que $\mathcal{S}$ est libre de rang $n - s$. Notons $d_1 | \dots | d_{n-s}$ ses invariants et $e_1, \dots, e_n$ une base de $\mathbb{Z}^n$ adaptée à $\mathcal{S}$. on a donc

$$\mathbb{Z}^n/\mathcal{S} \simeq \prod_{i=1}^{n-s} \mathbb{Z}/d_i\mathbb{Z} \times \mathbb{Z}^s.$$

Or $\mathbb{Z}^n/\mathcal{S}$ est isomorphe à l'image de φ qui est un sous-groupe libre de $\mathbb{Z}^r$ donc $\mathbb{Z}^n/\mathcal{S}$ est sans torsion donc tous les d_i valent nécéssairement 1 et on conclut que la quotient $\mathbb{Z}^n/\mathcal{S}$ est isomorphe à Z^s où s est le rang de A.

4.5.3 Tout endomorphisme de $\mathbb{Z}^n$ surjectif est un isomorphisme

On veut ici prouver l'énoncé donné dans le titre du paragraphe : soit $n \geq 1$ un entier et soit $\varphi : \mathbb{Z}^n \to \mathbb{Z}^n$ un morphisme de groupes surjectif. Montrons que φ est injectif. Pour cela on introduit K le noyau de φ. C'est un sous-groupe de $\mathbb{Z}^n$ donc il est libre de rang fini. Prenons une base adaptée $(e_1, \dots, e_n)$ à K et notons $d_1 | \dots | d_s$ ses invariants. On voit que, φ étant surjectif, on a

$$\mathbb{Z}^n = \mathrm{Im}(\varphi) \simeq \mathbb{Z}^n/K \simeq \prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z} \times \mathbb{Z}^{n-s}.$$

Par unicité dans le théorème de structure, on doit donc avoir : $n - s = n$ ie $s = 0$ donc K est le groupe trivial (de base vide), autrement dit φ est un isomorphisme.

4.6 Unicité dans le théorème de structure et dans le théorème de la base adaptée

4.6.1 Unicité dans le théorème de structure

Nous allons commencer ce paragraphe par introduire la notion d'exposant d'un groupe et prouver le lemme de Cauchy abélien, puis nous passerons aux questions d'unicité.

Définition 4.6.1 Soit G un groupe fini. On appelle *exposant de G* et on note $e(G)$ le max des ordres de x quand x parcourt G.

Lemme 4.6.2 *L'exposant de G divise le cardinal de G. De plus si on suppose G abélien alors pour tout $x \in G$ l'ordre de x divise l'exposant de G.*

Démonstration : Par définition il existe dans G un élément x_0 tel que $ord(x_0) = e(G)$. Donc par le théorème de Lagrange on voit que $e(G)$ divise le cardinal de G. Si de plus G est abélien, soit x un élément quelconque d'ordre d. Supposons par l'absurde que d ne divise pas $e(G)$. Alors en décomposant d et $e(G)$ en facteurs premiers, on a

$$e(G) = p^\alpha e_1,\ d = p^\beta d_1 \quad \text{et} \quad p \wedge e_1 = p \wedge d_1 = 1, \quad \text{et} \quad \beta > \alpha \geq 0.$$

Notamment on en déduit que l'élément $a := x_0^{p^\alpha}$ est d'ordre e_1 et $b := x^{d_1}$ est d'ordre p^β, donc que ab est d'ordre $e_1 p^\beta$ qui est strictement plus grand que $e(G)$. Ceci est une contradiction.□

Remarque 4.6.3 Attention la seconde partie de l'énoncé est fausse en général si le groupe n'est pas abélien. Par exemple dans le groupe symétrique S_3 on voit que l'exposant est 3 et une transposition est d'ordre 2 qui ne divise pas 3 (cf. le chapitre suivant pour ces notions).

Théorème 4.6.4 ***(Lemme de Cauchy abélien)*** *Soit G un groupe abélien fini. Si p est un facteur premier du cardinal de G alors il existe $x \in G$ d'ordre p.*

Démonstration : Soit $x_1, \ldots, x_n$ un ensemble de générateurs de G (cela existe car G est fini), d'ordre respectifs $d_1, \ldots, d_n$. Posons

$$\varphi :< x_1 > \times \cdots \times < x_n > \to G,\ (y_1, \ldots, y_n) \mapsto \prod_{i=1}^{n} y_i.$$

Comme G est abélien c'est un morphisme et par construction il est surjectif. Donc

$$G \simeq \prod_{i=1}^{n} < x_i > / \ker(\varphi).$$

En particulier, on voit que le cardinal de G divise $d_1 \ldots d_n$ qui à son tour divise $e(G)^n$. Ainsi si p est un facteur premier du cardinal de G alors p divise $e(G)$. Donc il existe e_1 tel que $e(G) = pe_1$. Si x_0 est d'ordre $e(G)$ on conclut en remarquant que $x_0^{e_1}$ est d'ordre p. □

Remarque 4.6.5 le même énoncé est vrai dans le cas non abélien : c'est par exemple une conséquence que l'on a prouvée des théorèmes de Sylow.

Nous pouvons maintenant passer aux questions d'unicité. Commençons par l'unicité dans le théorème de structure. Soit A un groupe abélien de type fini. Tout d'abord via la remarque 4.4, on a que A/A_{tor} est isomorphe à $\mathbb{Z}^r$ donc cet entier r est bien défini de manière unique. Ainsi quitte à remplacer A par A_{tor} on peut supposer (et on le fait) que $A = A_{\text{tor}}$ ie que A est un groupe abélien fini.

Fixons un nombre premier p. Nous allons intéresser à la réduction modulo p dans A (définie via le morphisme de multiplication par $p : A \to A$, $x \mapsto px$). L'image de ce morphisme est pA et le quotient est A/pA. De plus on munit naturellement (exercice : le vérifier !) A/pA d'une structure d'espace vectoriel sur le corps $\mathbb{Z}/p\mathbb{Z}$ par la multiplication externe suivante qui est bien définie :

$$\mathbb{Z}/p\mathbb{Z} \times A/pA \to A/pA, \quad (\lambda, x) \mapsto \lambda x.$$

Lemme 4.6.6 *Soit A un groupe abélien fini et soit p un nombre premier. Les conditions suivantes sont équivalentes :*

1. *La multiplication par $p : A \to A$ n'est pas injective.*
2. *La multiplication par $p : A \to A$ n'est pas surjective.*
3. *$A/pA \neq \{0\}$.*
4. *p divise le cardinal de A.*

Démonstration : L'unique chose non triviale est de vérifier que si p divise le cardinal de A alors il existe dans A des éléments non nuls d'ordre p : c'est le lemme de Cauchy abélien précédemment prouvé. Le reste est laissé en exercice. □

Proposition 4.6.7 *Soit $m_1, \ldots, m_n \in \mathbb{N} - \{0,1\}$ quelconques et soit $A = \prod_{i=1}^n \mathbb{Z}/m_i\mathbb{Z}$. Soit p un nombre premier. La dimension du $\mathbb{Z}/p\mathbb{Z}$-ev A/pA est :*

$$\dim_{\mathbb{Z}/p\mathbb{Z}}(A/pA) = \mathrm{Card}\left(\{j \in \{1, \ldots, n\} \mid p | m_j\}\right).$$

Démonstration : Pour tout entier i entre 1 et n, notons $C_i = \mathbb{Z}/m_i\mathbb{Z}$. On a

$$A/pA \simeq \prod_{i=1}^n C_i/pC_i.$$

Cet isomorphisme est a priori seulement un isomorphisme de groupes mais on vérifie facilement que c'est en fait un isomorphisme d'espace vectoriels. De plus $C_i/pC_i \neq 0$ si et seulement si p divise m_i, le cardinal de C_i. Dans ce cas C_i est cyclique donc le quotient C_i/pC_i également, donc ce dernier est un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel de dimension 1. Ceci permet de conclure. □

Nous pouvons maintenant passer à la preuve de l'unicité dans le théorème de structure dans le cas fini : soit A un groupe abélien fini et $d_1 | \cdots | d_s$ tels que $d_1 \geq 2$ et $A \simeq \prod_{i=1}^s \mathbb{Z}/d_i\mathbb{Z}$. Par la proposition 4.6.7 précédente on voit que pour tout nombre premier p, on a $\dim_{\mathbb{Z}/p\mathbb{Z}}(A/pA) \leq s$ avec égalité si et seulement si p divise d_1. Ainsi l'entier s est unique et donné par la formule

$$s = \sup_p \dim_{\mathbb{Z}/p\mathbb{Z}}(A/pA).$$

On prouve ensuite l'unicité des (d_i) par récurrence sur le cardinal de A. Si A est de cardinal 1 ou un nombre premier, l'assertion est triviale. Sinon, soit p un nombre premier divisant d_1. Un tel nombre premier ne dépend pas de la décomposition (d_i) par ce qui précède. On a alors

$$pA \simeq \prod_{i=1}^s p\mathbb{Z}/d_i\mathbb{Z} \simeq \prod_{i=1}^s \mathbb{Z}/d_i'\mathbb{Z},$$

où $d_i' = \frac{d_i}{p}$ pour tout i entre 1 et s. Cette dernière écriture est une décomposition pour le groupe pA qui est de cardinal strictement plus petit que celui de A. Il faut juste faire attention que certains d_i' peuvent valoir 1 (ceux tels que $d_i = p$) : les s' premiers. Ainsi les $d_{s'+1}', \ldots, d_s'$ sont uniquement déterminés, donc il en est de même des $d_{s'+1}, \ldots, d_s$. De plus on a $d_1 = \ldots = d_{s'} = p$ et $s - s'$ est le nombre de termes dans la décomposition de pA, donc s' est uniquement déterminé également. Ceci prouve que la décomposition est bien unique par récurrence. □

4.6.2 Unicité dans le théorème de la base adaptée

Passons maintenant à l'unicité dans le théorème 4.3.11 ou ce qui revient au même dans le théorème 4.3.9. On rappelle que l'on part d'un groupe G abélien de rang fini r muni d'une base et d'un sous-groupe B muni d'un système de générateurs (ou ce qui revient au même d'une matrice A représentant en colonnes les générateurs de B dans la base de G fixée). Notons t le plus grand entier j tel que $d_j = 1$. On a donc $1 = d_1 = \cdots = d_t < d_{t+1}| \cdots |d_s$. On a de plus

$$G/B \simeq \mathbb{Z}^{r-s} \oplus \bigoplus_{j=t+1}^{s} \mathbb{Z}/d_j\mathbb{Z}.$$

On en déduit que $(G/B)_{\mathrm{tor}} \simeq \bigoplus_{j=t+1}^{s} \mathbb{Z}/d_j\mathbb{Z}$. Or $d_{t+1} > 1$ donc ceci est la décomposition (unique) donnée par le théorème de structure (pour les groupes abéliens finis) donc les $d_{t+1}, \ldots, d_s$ sont uniques et l'entier $s - t$ est également uniquement déterminé. Or $s = \mathrm{rg}(B)$ est aussi uniquement déterminé donc il en est de même de t, donc tous les $d_1, \ldots, d_s$ sont uniques. □

Chapitre 5

Groupe Symétrique

5.1 Le groupe symétrique $\mathcal{S}_X$

Définition 5.1.1 Soit X un ensemble. On appelle *groupe symétrique* de X et on note $\mathcal{S}_X$ l'ensemble des bijections de X sur lui même. Une telle bijection s'appelle une *permutation* de X. Si n est un entier non nul et $X = \{1, \ldots, n\}$, on note S_n en lieu et place de S_X et on note t_{ij} ou (ij) la permutation qui envoie i sur j et j sur i (pour $1 \leq i \neq j \leq n$) et fixe les autres éléments. Une telle permutation s'appelle une *transposition*. Plus généralement avec X quelconque de cardinal au moins k, on appelle *k-cycle* (ou *cycle de longueur k*) toute permutation de la forme $c_k := (a_1, \ldots, a_k)$ (les a_i étant deux à deux distincts) définie de la façon suivante :

$$c_k(a_i) = a_{i+1} \text{ pour } 1 \leq i \leq k-1, \quad c_k(a_k) = a_1, \quad \text{et} \quad c_k(x) = x \text{ pour tout } x \notin \{a_1, \ldots, a_k\}.$$

Proposition 5.1.2 *Si X est un ensemble non vide, l'ensemble $\mathcal{S}_X$ muni de la composition est un groupe, de neutre Id_X. L'inverse d'une permutation σ est sa bijection réciproque σ^{-1}. Par ailleurs Le groupe $\mathcal{S}_n$ est de cardinal $n!$*

Démonstration : Immédiat. □

Nous tacherons dans la suite de travailler avec $\mathcal{S}_X$, plutôt qu'avec $\mathcal{S}_n$ y compris quand X est fini, néanmoins le résultat suivant dont la preuve est évidente indique un moyen de se ramener à $\mathcal{S}_n$ quand X est fini.

Proposition 5.1.3 *Si E et F sont deux ensembles et $f : E \to F$ est une bijection, alors $\mathcal{S}_E$ et $\mathcal{S}_F$ sont isomorphes et l'application*

$$\varphi : \mathcal{S}_E \to \mathcal{S}_F, \quad \sigma \mapsto f \circ \sigma \circ f^{-1}$$

est un isomorphisme de groupes.

Nous travaillerons dans la suite de ce chapitre, avec un ensemble X fini et non vide.

Définition 5.1.4 Soit $\sigma \in \mathcal{S}_X$ et soit $x \in X$. L'ensemble

$$\omega(x) := \{\sigma^j(x) \mid j \in \mathbb{Z}\}$$

et appelé *l'orbite de* x (pour σ).

Remarque 5.1.5 Le groupe cyclique $< \sigma >$ opère sur X via $(\sigma^j, x) \mapsto \sigma^j(x)$. On constate que $\omega(x)$ est l'orbite de x pour cette action. En particulier les orbites forment une partition de X.

Remarque 5.1.6 La permutation $\sigma \in S_X$ est un cycle si et seulement si elle admet une unique orbite ω de cardinal strictement supérieur à 1. Ce cardinal est la longueur du cycle.

Définition 5.1.7 Soit $\sigma \in \mathcal{S}_X$. On appelle *support de* σ le sous-ensemble de X, noté X_σ et défini par $X_\sigma := \{x \in X \mid \sigma(x) \neq x\}$.

Proposition 5.1.8 *Soient $s, t \in \mathcal{S}_X$ deux permutations à supports disjoints (ie $X_s \cap X_t = \emptyset$). Alors $st = ts$.*

Démonstration : Soit $a \in X_t$. Par hypothèse, $a \notin X_s$ donc $s(a) = a$ donc $st(a) = s(t(a))$ et $ts(a) = t(s(a)) = t(a)$. De plus $t(a)$ est dans X_t (sinon on aurait $t(t(a)) = t(a)$ d'où, en composant par t^1, t(a)=a ce qui est impossible). Donc l'hypothèse implique que $t(a) \notin X_s$, donc $s(t(a)) = t(a)$. Si a est dans X_s un argument symétrique montre que $st(a) = ts(a) = s(a)$. Si a n'est ni dans X_s ni dans X_t alors $st(a) = a = ts(a)$. □

Théorème 5.1.9 *Toute permutation $\sigma \in \mathcal{S}_X - \{\mathrm{Id}_X\}$ se décompose en produit de cycles à supports deux à deux disjoints. De plus cette décomposition est unique à l'ordre des facteurs près.*

Démonstration : Pour l'existence, il suffit de se souvenir que X est la réunion disjointes des orbites $\omega(x)$ et que sur une telle orbite, σ agit de façon cyclique. Notons $\omega(x_1), \ldots, \omega(x_m)$ les différentes orbites. On a

$$\forall j \leq m, \quad \sigma_{|\omega(x_j)} = (x_j, \sigma(x_j), \ldots, \sigma^{r_j}(x_j)) =: c_j.$$

Les c_j sont des cycles de support $\omega(x_j)$ deux à deux disjoints et visiblement on a $\sigma = \prod_{j=1}^m c_j$. Par ailleurs, les supports des cycles intervenant dans une décomposition d'une permutation $\sigma \neq \mathrm{Id}_X$ sont nécessairement les orbites (pour σ) non triviales et ceci prouve l'unicité. □

Théorème 5.1.10 *Si X est de cardinal fini au moins égal à deux, alors les transpositions engendrent le groupe $\mathcal{S}_X$.*

Démonstration : Nous allons donner deux preuves différentes :

1. En utilisant le théorème précédent, on voit qu'il suffit de prouver que tout cycle est un produit de transpositions. Or
$$(x_1, \ldots, x_k) = (x_1 x_2)(x_2 x_3) \ldots (x_{k-1} x_k).$$
2. Le seconde preuve se fait par récurrence sur le cardinal n de $X := \{x_1, \ldots, x_n\}$: le résultat est immédiat si $n = 2$. Si la propriété est vraie au rang $n-1$: soit $s \in \mathcal{S}_X$. Soit $s(x_n) = x_n$ et dans ce cas $s_{|\{x_1,\ldots,x_{n-1}\}}$ est une permutation de l'ensemble $X - \{x_n\}$ qui est de cardinal $n-1$. Donc s peut s'écrire comme un produit de transpositions. Le même produit donne la décomposition de s. Soit $s(x_n) = x_k \neq x_n$ et dans ce cas $s' := (x_n x_k)s$ est encore une permutation de $X - \{x_n\}$ que l'on peut donc décomposer en produit de transpositions $t_1 \ldots t_r$. On voit que $s = (x_n x_k) t_1 \ldots t_r$. □

Lemme 5.1.11 *Soit c un k-cycle. Son ordre est k.*

Démonstration : En considérant les indices modulo k, on a voit que $c^j(x_r) = x_{r+j}$ pour tout j et pour tout r : il s'agit d'une récurrence immédiate sur j. Notamment $c^k = Id$ donc k est un multiple de l'ordre de c. De plus si $j < k$ on a $c^j(x_1) = x_{j+1} \neq x_1$ donc c n'est pas d'ordre j. Donc l'ordre de c est k. □

Proposition 5.1.12 *Soit $s = \prod_{i=1}^{r} c_i$ un produit de cycles à supports deux à deux disjoints. Alors l'ordre de s est le ppcm des ordres des c_i.*

Démonstration : Comme les c_i commutent deux à deux, on voit immédiatement que le ppcm est un multiple de l'ordre de s. Si l'ordre d était strictement plus petit, alors l'un au moins des c_i ne serait pas annulé. En prenant un x dans le support de ce c_i tel que $c_i^d(x) \neq x$, on aurait donc

$$x = \mathrm{Id}_X(x) = s^d(x) = c_i^d(x) \neq x.$$

Ceci est une contradiction. □

Proposition 5.1.13 *Si $n \geq 3$ le centre de S_n est trivial : $Z(S_n) = \{1\}$.*

Démonstration : Soit $s \in S_n$ différent de 1. Il existe donc i tel que $s(i) = j \neq i$. Soit $k \neq i, j$ et $t = (kj)$. On a

$$st(i) = s(i) = j \quad \text{et} \quad ts(i) = t(j) = k.$$

Donc $st \neq ts$ donc $s \notin Z(S_n)$. □

Remarque 5.1.14 Le groupe S_2 est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ donc égal à son centre qui est donc non-trivial.

5.2 Le groupe alterné $\mathcal{A}_X$ et le morphisme signature

Proposition 5.2.1 *Si $n \geq 2$ et k est un entier alors les k-cycles sont conjugués dans S_n.*

Démonstration : Soit $n \geq 2$ et soient $c_a := (a_1, \ldots, a_k)$ et $c_b := (b_1, \ldots, b_k)$ deux k-cycles. On vérifie aisément, avec des notations évidentes, la formule

$$\forall \sigma \in \mathcal{S}_X,\ \sigma \circ c_a \circ \sigma^{-1} = c_{\sigma(a)}.$$

Soient donc $s = (a_1 \ldots a_k)$ et $t = (b_1 \ldots b_k)$ deux k-cycles. On construit une permutation $\sigma \in S_n$ de la façon suivante : on pose $\sigma(a_i) = b_i$ et on complète par une bijection de $\{1, \ldots, n\} - \{a_1, \ldots, a_k\}$ sur $\{1, \ldots, n\} - \{b_1, \ldots, b_k\}$ (existe car ces deux ensembles ont même cardinal). On vérifie immédiatement que $\sigma s \sigma^{-1} = t$. □

Théorème 5.2.2 *Soit X un ensemble fini de cardinal $n \geq 2$. Il existe un unique morphisme surjectif $\varepsilon : \mathcal{S}_X \to \{\pm 1\}$. Ce morphisme vaut -1 sur les transpositions.*

Démonstration : Existence : Notons $f : S_X \to S_n$ un isomorphisme. On va construire un morphisme $\varepsilon_n : S_n \to \{\pm 1\}$ surjectif puis on posera $\varepsilon := \varepsilon_n \circ f$. Soit Δ la fonction de n variables $x_1, \ldots, x_n$ de $\mathbb{Z}^n$ dans $\mathbb{Z}$ définie par :

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

Soit par ailleurs $1 \leq r < s \leq n$ deux entiers, notons τ la transposition (r,s) qui échange r et s. On introduit la fonction

$$\tau\Delta(x_1, \ldots, x_n) := \prod_{1 \leq i < j \leq n} (x_{\tau(j)} - x_{\tau(i)}).$$

Plus généralement, on a une action de S_n sur l'ensemble des fonctions de $\mathbb{Z}^n$ dans $\mathbb{Z}$ donnée par

$$\sigma \cdot f(x_1, \ldots, x_n) := f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

On vérifie immédiatement que l'on a

$$\sigma \cdot (\tau f) = (\sigma\tau) \cdot f.$$

Par ailleurs, on voit que entre Δ et $\tau\Delta$, pour $j = s$, $i = r$, le facteur $(x_s - x_r)$ est changé en $-(x_s - x_r)$. Les autres facteurs peuvent se voir par paire de la forme suivante :

$(x_k - x_s)(x_k - x_r)$ pour $k > s$, $(x_s - x_k)(x_k - x_r)$ pour $r < k < s$, $(x_s - x_k)(x_r - x_k)$ pour $k < r$.

Tous ces facteurs restent inchangés globalement quand on applique τ à Δ. Donc on voit que

$$\tau\Delta = -\Delta.$$

On sait que S_n est engendré par les transpositions donc on peut noter $\varepsilon_n(\sigma)$ le signe de $\sigma\Delta$ pour toute permutation $\sigma \in S_n$. Comme $\sigma \cdot (\tau\Delta) = (\sigma\tau) \cdot \Delta$ on en déduit que ε_n est un morphisme (surjectif car $\varepsilon_n(\tau) = -1$).

Montrons que $\varepsilon(t) = -1$ si t est une transposition : on sait par le lemme précédent que les transpositions sont conjuguées donc s'il existe τ une transposition telle que $\varepsilon(\tau) = -1$ alors $\varepsilon(t) = \varepsilon(\sigma\tau\sigma^{-1}) = \varepsilon(\tau) = -1$ pour toute transposition t. Supposons donc par l'absurde que pour toute transposition t on a $\varepsilon(t) = 1$. Dans ce cas pour tout produit σ de transposition on a encore $\varepsilon(\sigma) = 1$. Mais on sait que $\mathcal{S}_X$ est engendré par les transpositions, donc ε envoie $\mathcal{S}_X$ sur $\{1\}$: impossible.

Il reste à prouver l'unicité : soit ε et ε' deux morphismes non triviaux de $\mathcal{S}_X$ dans $\{\pm 1\}$. Soit $\sigma \in \mathcal{S}_X$. Il existe $t_1, \ldots, t_r$ des transpositions telles que $\sigma = t_1 \ldots t_r$. Donc $\varepsilon(\sigma) = \prod_{i=1}^r \varepsilon(t_i) = (-1)^r = \prod_{i=1}^r \varepsilon'(t_i) = \varepsilon'(\sigma)$. □

Définition 5.2.3 On appelle morphisme *signature* le morphisme donné par le théorème précédent.

Proposition 5.2.4 *Si c est un k-cycle on a $\varepsilon(c) = (-1)^{k+1}$.*

Démonstration : On a $c = (x_1, \ldots, x_k) = (x_1 x_2) \ldots (x_{k-1} x_k)$. Donc $\varepsilon(c) = \prod_{i=1}^{k-1} \varepsilon(x_i x_{i+1}) = (-1)^{k+1}$. □

Définition 5.2.5 On pose $\mathcal{A}_X := \mathrm{Ker}(\varepsilon)$. On appelle ce sous-groupe distingué de $\mathcal{S}_X$ le *groupe alterné*.

Proposition 5.2.6 *Soit H un sous-groupe d'indice de 2 dans $\mathcal{S}_X$ (ie le cardinal du quotient $\mathcal{S}_X/H$ est 2). Alors $H = \mathcal{A}_X$.*

Démonstration : Comme l'indice est 2 on sait que H est distingué dans $\mathcal{S}_X$, donc l'ensemble quotient est naturellement muni d'une structure de groupe. Ce groupe étant de cardinal 2, il est isomorphe à $\{\pm 1\}$. Notons i cet isomorphisme. De plus la projection canonique $\pi : \mathcal{S}_X \to \mathcal{S}_X/H$ est sujective de noyau H. En composant à l'arrivée par le morphisme i, on obtient un nouveau morphisme : $\varphi = i \circ \pi \ : \ \mathcal{S}_X \to \{\pm 1\}$ qui est toujours surjectif de noyau H. Mais étant surjectif, φ est en fait égal au morphisme signature par unicité de ce dernier. Donc $H = \mathrm{Ker}(\varphi) = \mathrm{Ker}(\varepsilon) = \mathcal{A}_X$. □

Proposition 5.2.7 *Si $n \geq 3$ les produits pairs de transpositions engendrent A_n. De même les 3-cycles engendrent A_n.*

Démonstration : On sait que S_n est engendré par les transpositions. Si $s \in A_n$ alors s peut donc se décomposer comme un produit de transposition. De plus $\varepsilon(s) = 1$ donc le produit doit contenir un nombre pair de transpositions. Pour ce qui est des 3-cycles. On a, si a, b, c, d sont deux à deux distincts,

$$(ab)(bc) = (abc) \ ; \ (ab)(ac) = (acb), \quad \text{et} \quad (ab)(cd) = (ab)(ac)(ac)(cd) = (acb)(acd).$$

Ceci prouve que tout produit pair de transposition peut s'écrire comme un produit de 3-cycles donc que les 3-cycles engendrent A_n. □

Proposition 5.2.8 *i $n \geq 5$, les 3-cycles sont conjugués dans A_n.*

Démonstration : la preuve est la même que celle prouvant que les cycles sont conjugués dans S_n : soit (abc) et (xyz) deux 3-cycles. Si la permutation σ construite dans S_n telle que $(xyz) = \sigma(abc)\sigma^{-1}$ est dans A_n alors on a fini. Sinon on se donne deux lettres supplémentaires u et v différentes de x, y, z (possible car $n \geq 5$) et on pose $\sigma' := (uv) \circ \sigma$. Par construction cette nouvelle permutation est de signature 1 (car σ était de signature -1) et on a :

$$\sigma'(abc)\sigma^{-1} = (uv)\sigma(abc)\sigma^{-1}(uv) = (uv)(xyz)(uv) = (xyz).$$

Ceci permet de conclure. □

Proposition 5.2.9 *Les doubles transpositions sont conjuguées dans A_n pour $n \geq 4$.*

Démonstration : Soit $(ab)(cd)$ et $(xy)(zt)$ deux doubles transpositions dans A_n. On pose $s(a) = x$, $s(b) = y$, $s(c) = z$ et $s(d) = t$ et on complète come d'habitude en une bijection de $\{1, \ldots, n\}$ sur lui même. Si s est dans A_n on a fini, sinon on pose $s' := (zt)s$. On a alors

$$(zt)s(ab)(cd)s^{-1}(zt) = (zt)(xy)(zt)(zt) = (zt)(xy) = (xy)(zt),$$

la dernière {egalité provenant de ce que (zt) et (xt) sont à support disjoint. □

5.3 Déterminant

Soit A un anneau commutatif et $n \geq 1$. On note $\mathcal{M}_n(A)$ l'anneau des matrices carrées de taille n à coefficients dans A.

Définition 5.3.1 Soit $M = (m_{ij})$ une matrice de $\mathcal{M}_n(A)$. On définit le *déterminant de M* par la formule

$$\det(M) := \sum_{\sigma \in \mathcal{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)}.$$

Remarque 5.3.2 Si $n = 2$ on retrouve la formule classique $\det(M) = ad - bc$. Pour $n = 3$ on retrouve la "règle de Sarrus".

Lemme 5.3.3 *On a* $\det({}^tM) = \det(M)$.

Démonstration : Il suffit de réciter la définition du déterminant de la transposée et de faire un changement d'indice dans la somme ($\tau = \sigma^{-1}$) puis dans le produit ($j = \tau^{-1}(i)$). □

Remarque 5.3.4 On veut pouvoir parler du *polynôme caractéristique* d'une matrice carrée M de taille n, à coefficients dans un corps K. Ce polynôme sera défini par $\det(XI_n - M)$. Il faut donc pour cela interpréter $XI_n - M$ comme une matrice à coefficients dans un certain anneau commutatif A. La bonne manière de voir est de constater que $XI_n - M$ est un élément de $\mathcal{M}_n(K[X])$.

5.4 Simplicité de A_n et groupe dérivé

5.4.1 Groupe dérivé

Définition 5.4.1 Soit G un groupe. On appelle *groupe dérivé* $D(G)$ le sous-groupe engendré par les commutateurs de G, ie les éléments de la forme $xyx^{-1}y^{-1}$ avec $x, y \in G$.

Remarque 5.4.2 Le groupe dérivé est distingué dans G et mieux : si φ est un automorphisme de G alors

$$\varphi(xyx^{-1}y^{-1}) = \varphi(x)\varphi(y)\varphi(x)^{-1}\varphi(y)^{-1}$$

donc $D(G)$ est stable par tout automorphisme de G. On dit que c'est un sous-groupe *caractéristique*.

Proposition 5.4.3 *Le groupe $G/D(G)$ es abélien ; c'est le plus petit sous-groupe distingué de G vérifiant ceci : si N est distingué dans G alors, G/N est abélien si et seulement si $D(G)$ est un sous-groupe de N.*

Démonstration : Le fait que $G/D(G)$ est abélien vient du fait que si $x, y \in G$ alors $xyx^{-1}y^{-1}$ est dans $D(G)$ donc, dans le quotient on a $\bar{x}\bar{y} = \bar{y}\bar{x}$. Soit par ailleurs N un sous-groupe de G distingué et tel que le quotient G/N est abélien. Alors pour tout $x, y \in G$ on a $xyx^{-1}y^{-1} = 1 \bmod N$, donc $xyx^{-1}y^{-1} \in N$, donc le groupe $D(G)$ est inclus dans N. Réciproquement si $D(G) \subset N$ et si $x, y \in G$ alors $xyx^{-1}y^{-1} \in D(G) \subset N$ donc $xy = yx \bmod N$. □

Remarque 5.4.4 Si N contient $D(G)$ alors on vérifie que N est automatiquement distingué dans G : soit $x \in G$ et $y \in N$ alors $n = xyx^{-1}y^{-1} \in D(G) \subset N$, donc $xyx^{-1} = ny \in N$.

Définition 5.4.5 Soit $G \neq \{1\}$ un groupe. On dit qu'il est *simple* si ses seuls sous-groupes distingués sont G et $\{1\}$.

Proposition 5.4.6 *Si G est un groupe abélien simple alors G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ pour un certain nombre premier p.*

Démonstration : Comme G est abélien tout ses sous-groupes sont distingués. On veut donc montrer que si G n'admet pas de sous-groupe autre que $\{1\}$ et G alors G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Soit $x \in G$ différent de 1. Si x est d'ordre infini alors $< x >$ est isomorphe à $\mathbb{Z}$ donc G admet une infinité de sous-groupes stricts (puisque c'est le cas pour $\mathbb{Z}$) donc G n'est pas simple. Si x est d'ordre fini $d \geq 2$ alors $< x >= G$ (sinon G aurait un sous-groupe strict non trivial) et de plus ce groupe ne peut pas avoir de sous-groupes strict. Or $< x > \simeq \mathbb{Z}/d\mathbb{Z}$ donc pour tout diviseur de d il admet un (et un seul) sous-groupe. Il faut donc que d soit premier. Enfin pour tout p on vérifie que $\mathbb{Z}/p\mathbb{Z}$ est simple. □

5.4.2 Simplicité de A_n

Commençons par noter que $A_2 = \{1\}$ et $A_3 \simeq \mathbb{Z}/3\mathbb{Z}$ donc est simple. Le cas de A_4 est un peu différent, c'est le groupe de cardinal 12 suivant :

$$A_4 = \{1, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\}.$$

On note traditionnellement V_4 le sous-groupe suivant de A_4 :

$$V_4 = \{1, (12)(34), (13)(24), (14)(23)\}.$$

Il est facile de voir que V_4 est stable par conjugaison $\sigma(12)(34)\sigma^{-1} = (\sigma(1)\sigma(2))(\sigma(3)\sigma(4)))$ donc V_4 est distingué dans A_4 et donc A_4 N'est PAS simple. Ce cas est exceptionnel comme l'indique le théorème suivant :

Théorème 5.4.7 *Si $n \geq 5$ alors A_5 est simple.*

Démonstration : On donne d'abord une preuve pour le cas $n = 5$ puis nous utiliserons ceci pour nous ramener du cas général au cas $n = 5$.

1. Le cas $n = 5$: Le groupe A_5 est de cardinal 60. Si on classe ses éléments selon leur ordre, on a : Id (d'ordre 1), les produits de deux transpositions disjointes (d'ordre 2 : il y en a 15), les 3-cycles (d'ordre 3 il y en a 20) et les 5-cycles (d'ordre 5 : il y en a 24). Soit H un groupe différent de $\{1\}$ distingué dans A_5. Montrons que $H = A_5$.
   (a) Si H contient un élément d'ordre 3 alors par conjugaison dans A_5 il les contient tous.
   (b) Si H contient un élément d'ordre 2, les doubles transpositions étant conjugués dans A_5 on en déduit que H contient au moins 21+15=36 éléments donc par cardinalité $H = A_5$.
   (c) Si H contient un élément d'ordre 5 alors il contient le 5-Sylow (de cardinal 5) engendré par cet élément. Donc H contient tous les 5-Sylow puisqu'ils sont conjugués, donc H contient tous les éléments d'ordre 5.
   (d) Le groupe H ne peut contenir, en plus de l'identité, que des éléments d'ordre 2 (ou 3 ou respectivement 5) sinon il serait de cardinal 16 (ou 21 ou respectivement 25) qui ne divise pas 60. Donc H contient au moins deux types d'éléments (en plus de l'identité) donc son cardinal vaut au moins $1 + 15 + 20 = 36$. Donc par cardinalité $H = A_5$.

2. Le cas $n \geq 6$: soit $E = \{1, \ldots, n\}$, soit H distingué dans A_n et soit $\sigma \in H - \{1\}$. Il existe donc $a \in E$ tel que $b := \sigma(a) \neq a$. Soit $c \in E$ différent de $a, b, \sigma(b)$ et soit $t = (acb)$ de sorte que $t^{-1} = (abc)$ et enfin posons $\rho = t\sigma t^{-1}\sigma^{-1} = (acb)(\sigma(a)\sigma(b)\sigma(c))$. Cette permutation ρ a un support inclus dans $F := \{a, b, c, \sigma(a), \sigma(b), \sigma(c)\}$. Or $b = \sigma(a)$ donc F est de cardinal au plus 5. Quitte à ajouter des éléments (qui ne jouerons aucun rôle) on peut supposer que F est de cardinal 5. On va donc se ramener via ceci au cas précédemment étudié de A_5. Notons que sur F la permutation $\rho \neq 1$ car $\rho(b) = t\sigma(b)$ et ceci est différent de b car $\sigma(b) \neq t^{-1}(b) = c$. On travaille désormais sur $A_F \simeq A_5$. Notons que l'on peut injecter A_F dans A_n via

$$u \mapsto \bar{u} \text{ avec } \bar{u}_{|F} = u \text{ et } \bar{u}_{|E-F} = \mathrm{Id}_{E-F}.$$

On pose $H_F := \{u \in A_F \mid \bar{u} \in H\} = H \cap A_F$. On voit immédiatement que H_F est distingué dans A_F et de plus $\rho_{|F}$ est dans H_F et non triviale. Par simplicité de A_5 on en déduit que $H_F = A_F$. Notamment si s est un 3-cycle de A_F il est dans H_F, donc $\bar{s}$ est un 3-cycle de H. Or les 3-cycles engendrent A_n, donc $H = A_n$. □

Corollaire 5.4.8 *Si $n \geq 5$ alors $D(A_n) = A_n$ et si $n \geq 2$ alors $D(S_n) = A_n$.*

Démonstration : On va plutôt donner une preuve directe (et je vous laisse justifier pourquoi c'est aussi un corollaire du théorème précédent, pour $n \geq 5$). Si $n \geq 2$ on a : $D(A_n) \subset D(S_n) \subset A_n$: la première inclusion est triviale et la seconde découle du fait que S_n/A_n est de cardinal 2 donc abélien et de la proposition 5.4.3. Par ailleurs les 3-cycles engendrent A_n pour $n \geq 3$, il suffit donc de prouver que si $\sigma = (abc)$ est un 3-cycle alors $\sigma \in D(A_n)$. On a $\sigma^2 = (acb)$ est également un 3-cycle or les 3 cycles sont conjugués dans A_n si $n \geq 5$ donc : si$n \geq 5$ il existe $t\tau \in A_n$ tel que $\tau\sigma\tau^{-1} = \sigma^2$ ie tel que $\sigma = \tau\sigma\tau^{-1}\sigma^{-1} \in D(A_n)$. Il nous reste donc juste à vérifier que $D(S_n) = A_n$ pour $n \in \{2, 3, 4\}$. Pour $n = 2$ c'est trivial. Pour $n \in \{3, 4\}$ il suffit de voir que les 3-cycles sont dans $D(S_n)$ or les 3-cycles sont conjugués dans S_n pour $n \geq 3$ donc le même argument que précédemment fonctionne. □

Corollaire 5.4.9 *Pour $n \geq 5$ les sous-groupes distingués de S_n sont $\{1\}$, A_n et S_n.*

Démonstration : Soit H distingué dans S_n. On a $H \cap A_n$ est distingué dans A_n donc par simplicité de A_n on en déduit que $H \cap A_n = \{1\}$ ou $H \cap A_n = A_n$.

1. Si $H \cap A_n = A_n$ alors $H = A_n$ ou $H = S_n$.
2. Si $H \cap A_n = \{1\}$ alors par restriction à H, la signature ε induit un isomorphisme de H sur $\varepsilon(H)$. Donc H est de cardinal au plus 2. Si $H = \{1, \sigma\}$ est de cardinal 2 alors on voit que pour tout $t \in S_n$ on a $t\sigma t^{-1} \in H - \{1\}$ donc $t\sigma t^{-1} = \sigma$, donc σ est dans le centre de S_n qui est trivial (car $n \geq 3$). Ceci est impossible donc H est de cardinal 1 ce qui conclut. □

Corollaire 5.4.10 *Soit H un sous-groupe d'indice n de S_n alors H est isomorphe à S_{n-1}*

Démonstration : Pour $n \leq 3$ le résultat est trivial. Pour $n = 4$, le groupe H est de cardinal 6. Il a été vu en TD (feuille IV exercice C) que dans ce cas soit H est isomorphe à S_3 soit H est commutatif. Mais dans ce dernier cas le théorème de structure des groupes abéliens finis implique que H est isomorphe à $\mathbb{Z}/6\mathbb{Z}$. Or S_4 ne contient pas d'éléments d'ordre 6 donc H doit être isomorphe à S_3.

Passons maintenant au cas $n \geq 5$. Posons $G = S_n$. Le groupe G opère par translation sur $X := G/H$. On en déduit donc un morphisme $\varphi : G \to S(X)$. Or

$$\mathrm{Stab}(\bar{1}) = \{g \in G \mid gH = H\} = \{g \in G \mid g \in H\} = H.$$

Notons f une bijection de X sur $\{1, \ldots, n\}$ telle que $f(\bar{1}) = 1$. Cette bijection induit un isomorphisme ψ entre $S(X)$ et S_n et en composant avec φ nous obtenons ainsi un morphisme $\psi \circ \varphi : G \to S_n$. Admettons un instant que φ soit injectif. Dans ce cas par cardinalité on en déduit que φ est un isomorphisme. Ainsi $\varphi(H)$ s'envoie par ψ sur l'ensemble

$$S(1) = \{s \in S_n \mid s(1) = 1\},$$

ie $\psi \circ \varphi(H)$ est le stabilisateur d'un point dans S_n c'est donc un groupe isomorphe à S_{n-1}. Il nous reste pour conclure à prouver que φ est injectif : on a

$$\ker(\varphi) = \{x \in G \mid \forall g \in G \;\; xgH = gH\} = \bigcap_{g \in G} gHg^{-1}.$$

Donc $\ker(\varphi)$ est inclus dans H donc de cardinal au plus $(n-1)! < \frac{n!}{2}$ et par ailleurs $\ker(\varphi)$ est distingué dans S_n donc par le corollaire précédent $\ker(\varphi)$ ne peut qu'être égal à $\{1\}$. □

5.5 Isomorphismes entre groupes de petit cardinaux du type $\mathrm{PGL}_2(k)$

5.5.1 Groupes linéaires et centres

Définition 5.5.1 Soit k un corps et E un k-ev de dimension finie $n \geq 1$. On note $\mathrm{GL}(E)$ (et $\mathrm{GL}_n(k)$ la version matricielle) le *groupe linéaire* des endomorphismes bijectifs de E dans E. On note $\mathrm{SL}(E)$ (et $\mathrm{SL}_n(k)$ la version matricielle) le *groupe spécial linéaire* des éléments de $\mathrm{GL}(E)$ de déterminant 1. On note $\mathrm{PGL}(E)$ (et $\mathrm{PGL}_n(k)$ la version matricielle) le *groupe projectif linéaire* défini comme étant le quotient de $\mathrm{GL}(E)$ par son centre . Enfin on note $\mathrm{PSL}(E)$ (et $\mathrm{PSL}_n(k)$ la version matricielle) le *groupe projectif spécial linéaire* donné par le quotient de $\mathrm{SL}(E)$ par son centre.

Lemme 5.5.2 *Soit $u \in \mathrm{GL}(E)$ telle que u laisse stable toutes les droites vectorielles de E. Alors u est une homothétie.*

Démonstration : On veut démontrer une inversion de quantificateurs :

$$\text{Si} \quad (\forall x \in E \; \exists \lambda \in k^*, \; u(x) = \lambda x) \quad \text{Alors} \quad (\exists \lambda \in k^* \; \forall x \in E, \; u(x) = \lambda x)\,.$$

En dimension 1 il n'y a rien à prouver. Sinon si x, y sont non colinéaires alors $u(x) = \lambda_x x$ et $u(y) = \lambda_y y$ donc

$$u(x+y) = \lambda_{x+y}(x+y) = \lambda_{x+y}x + \lambda_{x+y}y = u(x) + u(y) = \lambda_x x + \lambda_y y.$$

Donc finalement $\lambda_x = \lambda_{x+y} = \lambda_y$. Si x et y sont colinéaires c'est évident. □

Proposition 5.5.3 *Le centre Z de $\mathrm{GL}(E)$ est l'ensemble des homothéties, isomorphe à k^*.*

Démonstration : Soit $f \in \mathrm{GL}(E)$ qui n'est pas une homothétie. Par le lemme précédent, il existe $x \in E$ tel que $(x, f(x))$ est une famille libre (ie tel que la droite vectorielle de vecteur directeur x n'est pas invariante par f). On peut compléter ceci en une base $(x, f(x), e_3, \ldots, e_n)$ de E. Soit maintenant $g : E \to E$ linéaire donnée par

$$g(e_i) = e_i \text{ pour } i \geq 3, \text{ et } \quad g(x) = x, \quad \text{et } \quad g(f(x)) = x + f(x).$$

g envoie une base sur une base donc est dans $\mathrm{GL}(E)$ et par ailleurs

$$fg(x) = f(x) \quad \text{et } \quad gf(x) = x + f(x).$$

Comme x est non nul ceci entraîne que f n'est pas dans le centre de $\mathrm{GL}(E)$. □

Corollaire 5.5.4 *En notant $n = \dim E$, on a*

$$Z(\mathrm{SL}(E)) = Z \cap \mathrm{SL}(E) \simeq \mu_n(k) = \{\lambda \in k \mid \lambda^n = 1\}.$$

Démonstration : La seconde égalité est immédiate. Prouvons la première. Il est clair que $Z \cap \mathrm{SL}(E) \subset Z(\mathrm{SL}(E))$. Pour l'inclusion réciproque on reprend la preuve de la proposition précédente : si $f \in SL(E)$ n'est pas une homothétie alors l'application g précédente ne commute pas à f. Or, avec les notations de la preuve précédente, en écrivant la matrice de g dans la base $(x, f(x), e_3, \ldots, e_n)$ on voit immédiatement que g est de déterminant 1. Ainsi f n'est pas dans le centre de $\mathrm{SL}(E)$. □

5.5.2 Cardinaux des groupes linéaires

Soit p un nombre premier et $\alpha \geq 1$. Dans ce qui suit on fixe $\mathbb{F}_q$ un corps fini de cardinal $q = p^\alpha$ (vous verrez en M1 que le cardinal d'un corps fini est nécessairement de cette forme et que pour chacun de ces q on peut construire un corps fini de cardinal q. Par ailleurs vous verrez et nous l'utiliserons dans la preuve du point 3. du théorème 5.5.9 qu'un tel corps est naturellement muni d'une structure de $\mathbb{Z}/p\mathbb{Z}$-ev)). Nous appliquerons ensuite nos résultats pour exhiber des isomorphismes entre groupes de type linéaire et groupes symétriques, en prenant $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$ et $\mathbb{F}_4 = \mathbb{Z}/5\mathbb{Z}$.

Lemme 5.5.5 *L'ensemble $\mu_n(\mathbb{F}_q)$ des racines n-ieme de l'unité sur $\mathbb{F}_q$ est de cardinal $d := \mathrm{pgcd}(n, q-1)$.*

Démonstration : Par Bézout on sait qu'il existe $u, v \in \mathbb{Z}$ tels que $d = un + v(q-1)$. Soit $x \in \mathbb{F}_q^*$. On a $x^{q-1} = 1$ donc si x est de plus une racine n-ieme de l'unité alors $x^d = x^{un+v(q-1)} = (x^n)^u (x^{q-1})^v = 1$. Réciproquement si $x^d = 1$ alors a fortiori $x^n = 1$ donc $\mu_n(\mathbb{F}_q) = \mu_d(\mathbb{F}_q)$. Or le polynôme $X^{q-1} - 1$ admet tous les éléments non nuls de $\mathbb{F}_q$ comme racines distinctes, donc $q-1$ racines donc est scindé. De plus le polynôme $X^d - 1$ divise $X^{q-1} - 1$ (exercice !!). Donc $X^d - 1$ est scindé sur $\mathbb{F}_q$ ie le cardinal de $\mu_d(\mathbb{F}_q)$ est d. □

Théorème 5.5.6 *Sur $\mathbb{F}_q$ et avec $n \geq 1$ les cardinaux des groupes linéaires introduits précédemment sont :*

1. $|\mathrm{GL}_n(\mathbb{F}_q)| = \prod_{i=0}^{n-1}(q^n - q^i)$.
2. $|\mathrm{SL}_n(\mathbb{F}_q)| = q^{n-1} \prod_{i=0}^{n-2}(q^n - q^i)$.

3. $|\mathrm{PGL}_n(\mathbb{F}_q)| = |\mathrm{SL}_n(\mathbb{F}_q)|$.
4. $|\mathrm{PSL}_n(\mathbb{F}_q)| = \frac{|\mathrm{SL}_n(\mathbb{F}_q)|}{\mathrm{pgcd}(n,q-1)}$.

Démonstration : Se donner une matrice A de $\mathrm{GL}_n(\mathbb{F}_q)$ revient à se donner l'image de la base canonique $(e_1,\dots,e_n)$ de $\mathbb{F}_q^n$ (la matrice A écrivant cette image en colonnes) de sorte que cette image soit une base (pour que A soit inversible). Ainsi $\mathrm{GL}_n(\mathbb{F}_q)$ est en bijection avec l'ensemble des bases de $\mathbb{F}_q^n$. Pour choisir une telle base $(f_1,\dots,f_n)$ on peut prendre

1. f_1 quelconque non nul.
2. f_2 quelconque sauf dans la droite engendrée par f_1 (qui est $\mathbb{F}_q f_1$ donc de cardinal q).
3. f_3 quelconque sauf dans le plan engendré par (f_1,f_2) (qui est de dimension 2 sur $\mathbb{F}_q$ donc de cardinal q^2).
4. De même jusqu'à f_n quelconque sauf dans l'hyperplan $(f_1,\dots,f_{n-1})$ (de cardinal q^{n-1}).

Ainsi le cardinal de l'ensemble des bases est : $(q^n-1)\dots(q^n-q^{n-1})$ qui est ce que l'on annonçait pour $\mathrm{GL}_n(\mathbb{F}_q)$.

Les points 2. et 3. du théorème découle de la description du centre de $\mathrm{GL}_n(\mathbb{F}_q)$ et du fait que $\mathbb{F}_q^*$ est de cardinal $q-1$. Enfin le dernier point découle de la description du centre de $\mathrm{SL}_n(\mathbb{F}_q)$ et du lemme précédent. □

5.5.3 Action du groupe linéaire sur l'espace projectif

Définition 5.5.7 Soit E un k-ev de dimension finie $n \geq 2$. On appelle *espace projectif* et on note $\mathbb{P}(E)$ l'ensemble des droites vectorielles de E (rappelons que, même si on n'utilisera pas cette description, cet espace peut se voir comme le quotient de $E-\{0\}$ par k^*).

On a une action naturelle de $\mathrm{GL}(E)$ sur $\mathbb{P}(E)$ donnée par

$$\mathrm{GL}(E)\times\mathbb{P}(E)\to\mathbb{P}(E),\quad (P,\Delta_e)\mapsto\Delta_{P(e)},$$

où pour $x\in E$, Δ_x est la droite vectorielle de vecteur directeur x.

On voit que via cette action les homothéties agissent trivialement : si $P=\lambda\mathrm{Id}_E$ avec $\lambda\in k^*$ et si Δ_e est une droite, alors $\Delta_{P(e)}=\Delta_{\lambda e}=\Delta_e$. Ceci entraîne que l'action donnée par $\mathrm{GL}(E)$ passe au quotient et fournit une action bien définie de $\mathrm{PGL}(E)$ sur $\mathbb{P}(E)$:

$$\mathrm{PGL}(E)\times\mathbb{P}(E)\to\mathbb{P}(E),\quad (\bar{P},\Delta_e)\mapsto\Delta_{P(e)}.$$

Proposition 5.5.8 *Cette action de* $\mathrm{PGL}(E)$ *sur* $\mathbb{P}(E)$ *est fidèle.*

Démonstration : Soit $\bar{P}\in\mathrm{PGL}(E)$ tel que pour tout $x\in E$ on a $\Delta_{P(x)}=\Delta_x$. Autrement dit P laisse stable toutes les droites vectorielles de E. Par le lemme 5.5.2 ceci implique que P est une homothétie donc que $\bar{P}$ est trivial dans $\mathrm{PGL}(E)$. □

On travaillera désormais sur $E=\mathbb{F}_q^2$ avec q une puissance d'un nombre premier. L'espace projectif $\mathbb{P}(E)$ (qui se note dans ce cas aussi $\mathcal{P}^1(\mathbb{F}_q)$, on parle de *la droite projective* sur $\mathbb{F}_q$) est composé de $q+1$ éléments : les droites de vecteur directeur $(\bar{1},\bar{k})\in(\mathbb{F}_q)^2$ pour $k\in\{0,\dots,q_1\}$ et la droite de vecteur directeur $(\bar{0},\bar{1})$. On obtient finalement un morphisme injectif

$$\varphi:\mathrm{PGL}_2(\mathbb{F}_q)\to\mathcal{S}_{q+1}.$$

Nous allons utiliser ceci pour prouver le théorème suivant identifiant certains groupes symétriques de petits cardinaux et certains groupes linéaires.

Théorème 5.5.9 *On a les isomorphismes suivants :*

1. $\mathrm{GL}_2(\mathbb{F}_2) = \mathrm{SL}_2(\mathbb{F}_2) = \mathrm{PSL}_2(\mathbb{F}_2) \simeq S_3$.
2. $\mathrm{PGL}_2(\mathbb{F}_3) \simeq S_4$ *et* $\mathrm{PSL}_2(\mathbb{F}_3) \simeq A_4$.
3. $\mathrm{PGL}_2(\mathbb{F}_4) = \mathrm{PSL}_2(\mathbb{F}_4) \simeq A_5$.
4. $\mathrm{PGL}_2(\mathbb{F}_5) \simeq S_5$ *et* $\mathrm{PSL}_2(\mathbb{F}_5) = A_5$.

Démonstration : Commençons par le point 1. : $\mathbb{F}_2^*$ est de cardinal 1, donc par le théorème 5.5.6 on voit que les groupes $\mathrm{GL}_2(\mathbb{F}_2)$, $\mathrm{SL}_2(\mathbb{F}_2)$, $\mathrm{PGL}_2(\mathbb{F}_2)$ et $\mathrm{PSL}_2(\mathbb{F}_2)$ sont égaux de cardinal 6. Par le morphisme φ ils s'injectent dans S_3 qui est également de cardinal 6, donc lui sont isomorphes.

Pour le second point : $\mathrm{PGL}_2(\mathbb{F}_3)$ est de cardinal 24 (par le th. 5.5.6) donc par le même raisonnement on en déduit qu'il est isomorphe à S_4. Comme $\mathrm{PSL}_2(\mathbb{F}_3)$ en est un sous-groupe d'indice 2, on déduit de la proposition 5.2.6 que ce groupe est isomorphe à A_4.

Pour le point 3. : Le corps $\mathbb{F}_4$ est un $\mathbb{Z}/2\mathbb{Z}$-ev donc est de caractéristique 2, donc $-\mathrm{Id} = \mathrm{Id}$ donc

$$\mathrm{SL}_2(\mathbb{F}_4) = \mathrm{PSL}_2(\mathbb{F}_4) = \mathrm{PGL}_2(\mathbb{F}_4).$$

Le morphisme $\varphi : \mathrm{PSL}_2(\mathbb{F}_4) \to S_5$ est injectif et $\mathrm{PSL}_2(\mathbb{F}_4)$ est de cardinal 60, ie d'image d'indice 2 dans S_5 donc est isomorphe à A_5.

Pour le dernier point : on considère encore le morphisme injectif $\varphi : \mathrm{PGL}_2(\mathbb{F}_5) \to S_6$. Cette fois $\mathrm{PGL}_2(\mathbb{F}_5)$ est de cardinal 120 donc d'indice 6 dans S_6. On utilise donc le corollaire 5.4.10 pour conclure. □

5.6 Digression : les suites exactes

Nous faisons ici un très bref paragraphe pour introduire une notion fort utile en algèbre.

Définition 5.6.1 Soit F, G, H trois groupes et soit $f : F \to G$ et $g : G \to H$ deux morphismes de groupes. On dit que la suite

$$F \xrightarrow{f} G \xrightarrow{g} H$$

est *une suite exacte* si

$$\ker(g) = \mathrm{Im}(f).$$

Définition 5.6.2 Plus généralement soit $(G_i)_{i\in X}$ une famille de groupes indexés par un ensemble X qui sera soit $\{0, \dots, n\}$ pour un certain entier $n \geq 3$ soit l'ensemble $\mathbb{N}$ entier. Soit également, pour tout $i \in X$, des morphismes de groupes $f_i : G_i \to G_{i+1}$. On dit que la suite

$$\cdots \to G_{i-1} \xrightarrow{f_{i-1}} G_i \xrightarrow{f_i} G_{i+1} \xrightarrow{f_{i+1}} \cdots$$

est, un entier i_0 étant fixé *une suite exacte en* G_{i_0} si $\ker(f_{i_0}) = \mathrm{Im}(f_{i_0-1})$. La suite est dite *exacte* si elle est exacte en G_i pour tout $i \in X$ (en excluant la valeur $i = 0$; et également $i = n$ si $X = \{0, \dots, n\}$).

Exemple 5.6.3 Il y a un cas particulier très courant de suite exacte, que l'on appelle *suite exacte courte* : soit F, G, H trois groupes munis de morphismes $f : F \to G$ et $g : G \to H$

comme précédemment. On considère de plus les deux morphismes triviaux : $\{1\} \to F$ et $H \to \{1\}$. Si la suite

$$\{1\} \to F \xrightarrow{f} G \xrightarrow{g} H \to \{1\}$$

est exacte, on dit que c'est une suite exacte courte. Ceci se traduit très concretement de la façon suivante ; il faut et il suffit que les trois conditions suivantes soient simultanément remplies :

1. f est injective (c'est l'exactitude en F),
2. $\mathrm{Im}(f) = \ker(g)$ (c'est l'exactitude en G),
3. g est surjective (c'est l'exactitude en H).

Définition 5.6.4 Si $f : G \to H$ est un morphisme de groupes. On dit que $s : H \to G$ est *une section de* f si $f \circ s = \mathrm{Id}_H$.

Exemple 5.6.5 : Si K est un corps et $n \geq 1$, la suite $\{1\} \to \mathrm{SL}_n(K) \to \mathrm{GL}_n(K) \xrightarrow{\det} K^* \to \{1\}$ est exacte et l'application $s : K^* \to \mathrm{GL}_n(K)$ donnée par $x \mapsto \begin{pmatrix} x & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$ est une section du déterminant.

Exemple 5.6.6 Si G est un groupe et H un sous-groupe distingué, on a la suite exacte courte naturelle suivante (avec comme morphismes l'inclusion et la projection canonique) :

$$\{1\} \to H \to G \to G/H \to \{1\}.$$

Partant d'un groupe G, si N est un sous-groupe distingué on obtient le groupe quotient G/N. Une question naturelle est de chercher, les groupes N et G/N étant donnés, à reconstruire G. Plus généralement étant donnés deux groupes N et H on cherche les groupes G tels que l'on a une suite exacte courte

$$\{1\} \to N \to G \to H \to \{1\}.$$

Dans ce cas H s'identifiera par factorisation canonique au quotient G/N.

Définition 5.6.7 Un groupe G obtenu commme ci-dessus s'appelle *une extension de H par N*.

L'étude des extensions est un problème difficile. Nous allons juste illustrer ceci sur deux exemples très simples :

1. Tout d'abord, partant de $N = \mathbb{Z}/2\mathbb{Z}$ et $H = \mathbb{Z}/2\mathbb{Z}$, on peut trouver au moins deux extensions non isomorphes :
   (a) Le groupe $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ convient (exercice immédiat).
   (b) Le groupe $G = \mathbb{Z}/4\mathbb{Z}$ convient également (on prend comme inclusion de $\mathbb{Z}/2\mathbb{Z}$ dans $\mathbb{Z}/4\mathbb{Z}$ le morphisme qui envoie $x \bmod 2$ sur $2x \bmod 4$ et comme surjection de $\mathbb{Z}/4\mathbb{Z}$ dans $\mathbb{Z}/2\mathbb{Z}$ le morphisme qui envoie $x \bmod 4$ sur $x \bmod 2$).
   (c) On sait que ces deux groupes ne sont pas isomorphes.
2. De même avec $N = \mathbb{Z}/3\mathbb{Z}$ et $H = \mathbb{Z}/2\mathbb{Z}$:

(a) Le groupe $G = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ convient.

(b) Le groupe S_3 convient également (en prenant l'inclusion définie en envoyant $1 \bmod 3$ sur (123) et le morphisme de projection sur H donné par le morphisme signature composé avec l'unique isomorphisme de $\{\pm 1\}$ sur $\mathbb{Z}/2\mathbb{Z}$).

(c) Le premier groupe est commutatif, le second non ; ils ne peuvent donc pas être isomorphes.

5.7 Automorphismes de S_n

Définition 5.7.1 Soit G un groupe. On appelle *automorphisme intérieur*, tout morphisme bijectif $\varphi : G \to G$ tel qu'il existe $g \in G$ tel que

$$\forall x \in G, \quad \varphi(x) = gxg^{-1} =: i_g(x)$$

. On note $\mathrm{Int}(G)$ l'ensemble des automorphismes intérieurs.

Proposition 5.7.2 *Les automorphismes intérieurs forment un sous-groupe de* $\mathrm{Aut}(G)$. *On a de plus la suite exacte suivante :*

$$\{1\} \to Z(G) \to \underset{g}{G} \underset{\mapsto}{\to} \underset{i_g}{\mathrm{Int}}(G) \to \{1\}.$$

Démonstration : La preuve est évidente. □

Théorème 5.7.3 *Si* $n \neq 6$ *on a* $\mathrm{Aut}(S_n) = \mathrm{Int}S_n$.

Corollaire 5.7.4 *Si* $n \geq 3$ *et* $n \neq 6$ *alors* $\mathrm{Aut}(S_n) \simeq S_n$.

Démonstration : On utilise la suite exacte prcédente et le théorème avec le fait que dans notre situation le centre est trivial. □

Avant de passer à la preuve du théorème 5.7.3 voyons la situation exceptionnelle $n = 6$.

Théorème 5.7.5 *On a :* $\mathrm{Int}(S_6) \neq \mathrm{Aut}(S_6)$.

Une fois que l'on sait que ces deux groupes sont différents on peut facilement voir qu'ils ne sont pas trop différents.

Proposition 5.7.6 *Le groupe* $\mathrm{Int}(S_6)$ *est d'indice 2 dans* $\mathrm{Aut}(S_6)$.

Démonstration : Exercice : on pourra pour cela considérer deux automorphismes non intérieurs φ et ψ et déterminer comment se transforme par φ (et ψ) la classe de conjugaison des transpositions de S_6 puis en déduire que $\varphi \circ \psi$ conserve les transpositions et enfin que $\varphi \circ \psi$ est intérieur. □

Passons maintenant à la preuve des deux théorèmes 5.7.3 et 5.7.5.

5.7.1 Preuve du théorème 5.7.3

Proposition 5.7.7 *Soit $n \geq 2$ et soit $\varphi \in \mathrm{Aut}(S_n)$. Si φ transforme les transpositions en transpositions alors φ est intérieur.*

Démonstration : Il a été vu en TD (ou on peut prouver en exercice) que S_n est engendré par les transpositions $t_i := (1i)$ pour $i \geq 2$. Pour tout i on a donc que $\varphi(t_i)$ est une transposition. Or t_i et t_j ne commutent pas, donc $\varphi(t_i)$ et $\varphi(t_j)$ ne sont pas à support disjoint. Posons $\varphi(t_2) = (a_1a_2)$ et $\varphi(t_3) = (a_1a_3)$. Si pour $i \geq 4$ on avait $\varphi(t_i) = (a_2a_3)$ alors on a $(a_1a_2)(a_1a_3)(a_2a_3) = (a_1a_3)$ donc en composant pas φ^{-1} on en déduirait que $(12)(13)(1i) = (13)$ ce qui est faux ! Donc pour tout $i \geq 2$ on a $\varphi(t_i) = (a_1a_i)$ avec $a_1, \ldots, a_n$ deux à deux distincts (par injectivité de φ). Ainsi l'application

$$a : \{1, \ldots, n\} \to \{1, \ldots, n\}, \quad i \mapsto a_i$$

est une permutation de S_n et $at_ia^{-1} = (a_1a_i) = \varphi(t_i)$. Donc φ est intérieur et on a $\varphi = i_a$. □

On voudrait utiliser ceci pour prouver que tous les automorphismes sont intérieurs. Notons déjà que si τ est une transposition alors τ est d'ordre 2. Si $n \geq 4$ il y a bien sur d'autres éléments d'ordre 2 : par exemple $(12)(34)$. Soit donc φ un automorphisme de S_n et soit τ une transposition. Alors la permutation $\sigma := \varphi(\tau)$ une permutation d'ordre 2. On la décompose en produit de cycles à support disjoint. L'ordre de σ est donc le ppcm des ordres des différents cycles intervenant dans sa décomposition. Pour que ce ppcm soit 2 il faut donc (et il suffit) que σ se décompose comme un produit de $k \geq 1$ transpositions deux à deux disjointes. Notons $c(\sigma)$ le centralisateur de σ (ie l'ensemble des permutations de S_n qui commutent à σ). On voit immédiatement que

$$c(\varphi(\tau)) = \varphi(c(\tau)).$$

En particulier le cardinal de $c(\varphi(\tau))$ est égal à celui de $c(\tau)$. On va donc étudier le cardinal du centralisateur d'un élément :

Lemme 5.7.8 *Soit $s \in S_n$ tel que s se décompose en k_1 cycle d'ordre 1, ..., k_n cycles d'ordre n, tous à supports deux à deux disjoints. Ainsi $n = k_1 + \ldots + nk_n$. Si $c(s)$ est le centralisateur de s, on a*

$$\mathrm{Card}(c(s)) = \prod_{i=1}^{n} k_i! i^{k_i}.$$

Démonstration : Exercice ! □

En utilisant le lemme on peut conclure très facilement :

$$\mathrm{Card}(c(\tau)) = 2(n-2)! = \mathrm{Card}(c(\varphi(\tau))) = 2^k k!(n-2k)!$$

On voit que ceci implique $k = 1$ sauf si $n = 6$ (et dans ce cas $k = 3$ est autorisé). Donc si $n \neq 6$ on conclut avec la proposition précédente que φ est intérieur. □

5.7.2 Preuve du théorème 5.7.5

Rappelons une chose que l'on a déjà utilisé (pour prouver qu'un sous-groupe d'indice n de S_n est isomorphe à S_{n-1}) : soit E et F deux ensembles de cardinal n et soit $f : E \to F$ une bijection ensembliste. On en déduit un isomorphisme

$$\varphi \ : \ S_E \to S_F, \quad \sigma \mapsto f\sigma f^{-1}.$$

De plus φ transforme le stabilisateur d'un élément $e \in E$ en le stabilisateur de $f(e)$. Notons

$$S(i) := \{\sigma \in S_n \mid \sigma(i) = i\}$$

le stabilisateur de i dans S_n. C'est un sous-groupe d'indice n de S_n visiblement isomorphe à S_{n-1}.

Lemme 5.7.9 *Les $S(i)$ sont conjugués dans S_n.*

Démonstration : En effet, si i et j sont dans $\{1, \ldots, n\}$ et $\tau \in S_n$ telle que $\tau(i) = j$ alors on voit que $S(j) = \tau S(i)\tau^{-1}$. □

Proposition 5.7.10 *Soit $n \neq 4$. Si $\mathrm{Aut}(S_n) = \mathrm{Int}(S_n)$ alors les sous-groupes d'indice n de S_n sont tous conjugués (donc sont les $S(i)$).*

Démonstration : On fait une preuve par la contraposée : soit H un sous-groupe de S_n d'indice n non-conjugué au $S(i)$. On a déjà prouvé qu'en faisant opérer S_n par translation sur S_n/H on obtient ainsi un isomorphisme et que $\varphi(H)$ est le stabilisateur de la classe de $H = \bar{1}$. Notons f une bijection de $X = S_n/H$ sur $\{1, \ldots, n\}$ telle que $f(\bar{1}) = 1$. Cette bijection induit un isomorphisme ψ entre $S(X)$ et S_n et en composant avec φ nous obtenons ainsi un automorphisme $\psi \circ \varphi$ de S_n tel que $\psi \circ \varphi(H) = S(1)$. Or H et $S(1)$ ne sont pas conjugués, donc $\psi \circ \varphi$ n'est pas intérieur. □

Remarque 5.7.11 En fait la réciproque de la proposition précédente est vraie : exercice ! Nous n'en aurons pas besoin.

Lemme 5.7.12 *Le groupe S_5 contient 6 sous-groupes de Sylow de cardinal 5.*

Démonstration : Notons n_5 le nombre de 5-Sylow de S_5. Il est congru à 1 modulo 5 et divise 24, donc $n_5 = 1$ ou $n_5 = 6$ Si $n_5 = 1$ alors l'unique 5-Sylow est distingué. Or on sait que dans S_5 les seuls sous-groupes distingués sont $\{1\}$, A_5 et S_5. Par cardinalité un 5-Sylow est différent de ces groupes donc $n_5 = 1$. □

Nous pouvons maintenant conclure la preuve du théorème 5.7.5 : notons X l'ensemble de cardinal 6 des 5-Sylow de S_5. Le groupe S_5 agit sur X par conjugaison, transitivement (car tous les 5-Sylow sont conjugués) et fidèlement (sinon en notant $\varphi : S_5 \to S_6$ le morphisme correspondant, il aurait un noyau non trivial qui serait donc A_5 ou S_5 puisque distingué et donc l'image serait de cardinal au plus 2 ce qui contredit la transitivité). Ainsi le groupe $\varphi(S_5)$ est un sous-groupe de S_6 isomorphe à S_5, donc d'indice 6 dans S_6 et différent des stabilisateurs $S(i)$ (car S_5 agit transitivement sur X). On conclut avec la proposition 5.7.10 précédente. □