Algèbre 5

Cours donné en L3 au premier semestre 2024-25

Charles De Clercq

Université Paris 13
LAGA, CNRS (UMR 7539)
F-93430 Villetaneuse
France

Ces notes constituent la partie théorique du cours et on été rédigées à partir des notes précédentes de Jörg Wildeshaus. Il est essentiel de travailler le matériel *chez soi*. On fera usage de quelques notions de base et résultats traités pendant le cours "Groupes et symétries" (L2, deuxième semestre) : on en rappelera cependant au moins l'existence, avec des références précises au polycopié [G]. Exemple : [G, Déf. 2.13] fait référence à la Définition 2.13 de *loc.cit.* (il s'agit donc de la définition des morphismes de groupes).

Contents

1 Groupes : définitions et exemples **2**

2 Ordre d'un élément **7**

3 Sous-groupes **9**

4 Groupes engendrés, relations **11**

5 Morphismes **14**

6 Classes modulo un sous-groupe **17**

7 Groupes quotients **20**

8 Théorèmes d'isomorphismes **25**

9 Produit direct, lemme Chinois **31**

10 Groupes abéliens **33**

11 Produits semi-directs **35**

12 Anneaux : propriétés de base **40**

13 Homomorphismes, idéaux et anneaux quotient **46**

14 Anneaux principaux, anneaux Euclidiens, anneaux factoriels **57**

15 Le corps des fractions **66**

1 Groupes : définitions et exemples

On commence par quelques rappels sur des notions vues en L2.

Définition 1.1. Soit G un ensemble, et

$$\cdot : G \times G \longrightarrow G$$

une loi de composition interne. On dit que la paire $(G, \cdot)$ est un *groupe* si les axiomes suivants sont satisfaits :

(1) *associativité* : on a

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c, \ \forall \ a, b, c \in G$$

(2) *élément neutre* : il existe un élément $e_G \in G$ tel que

(2a) pour tout $a \in G$ on a

$$e_G \cdot a = a \cdot e_G = a;$$

(2b) *inverses* : $\forall a \in G,\ \exists\, b \in G,$

$$b \cdot a = a \cdot b = e_G$$

Remarque 1.2. 1. L'inverse d'un élément a (axiome $(2b)$) est unique, on le notera donc généralement a^{-1}.

2. Lorsque la loi est claire dans le contexte, on écrira simplement G pour le groupe $(G, \cdot)$ et le produit $a \cdot b$ sera noté ab.

3. Si G est fini en tant qu'ensemble, on dira que $(G, \cdot)$ est un groupe fini.

Détails. *1. Si on a $ba = ab = e$ et $ca = ac = e$, alors on a simplement $b = be = b(ac) = (ba)c = ec = c$.*

Définition 1.3. Un groupe $(G, \cdot)$ est dit abélien (ou commutatif) si pour tous $a \cdot b = b \cdot a$, pour tout a et tout b dans G.

Une des spécificités de la théorie des groupe est qu'elle propose beaucoup d'exemples simples, et très exotiques. Il est déterminant pour l'assimiler ou résoudre des exercices de garder en tête et maîtriser des exemples concrets. Tout au long de ce cours, chaque nouvelle notion sera illustrée d'exemples qui nous suivront poru éclairer la théorie : ne les négligez pas.

Exemples 1.4. 1. Les ensembles munis des lois $(\mathbb{Z}, +)$, $(\mathbb{Q}^*, \times)$, $(\mathbb{R}[X], +)$, $(\mathbb{Z}/n\mathbb{Z}, +)$, $(\mathfrak{S}_n, \circ)$, $(\{\text{rotations vectorielles du plan}\}, \circ)$, $(GL_n(\mathbb{Q}), \times)$ sont des groupes.

2. Si $(G, \cdot)$ et $(G', *)$ sont deux groupes, leur produit cartésien $G \times G'$ est muni naturellement d'une structure de groupe qu'on appelle le *produit direct* de G et G'.

3. Pour chaque axiome de la Définition , on exhibe un couple $(G, \cdot)$ qui fait défaut.

Détails. *1. (a) Rappel : sur $\mathbb{Z}$ pour $n \in \mathbb{N}$ on pose la relation d'équivalence $x \simeq y$ si n divise $x - y$. On note $\overline{x}$ la classe d'équivalence de x.*
Cette relation est compatible avec l'additions dans $\mathbb{Z}$: $\overline{x} + \overline{x'} = \overline{x + x'}$ est bien défini.

(b) (groupe symétrique) Si $\mathfrak{X}$ est un ensemble, on note $Perm(\mathfrak{X})$ l'ensemble des bijection (permutations) de $\mathfrak{X}$ dans $\mathfrak{X}$.
$(Perm(\mathfrak{X}), \circ)$ est un groupe, où $\circ$ est la composition des applications. Lorsque $\mathfrak{X} = \{1, ..., n\}$ est un ensemble à n éléments, on note ce groupe (fini) $\mathfrak{S}_n$.

2. *loi produit, neutre et inverse.*

3. *(a)* $(GL_n(\mathbb{R}), +)$ *ce n'est pas une loi de composition interne.*

   (b) On pose $* : \mathbb{C} \times \mathbb{C} \longrightarrow \mathbb{C}$, $(z, z') \mapsto \overline{zz'}$. *Ce n'est pas associatif et pas de neutre.*

   (c) $(\mathbb{Q}, \times)$ *pas d'inverse.*

Thèmes 1.5. 1. (Rappels sur le groupe symétrique $\mathfrak{S}_n$). On a pour habitude de représenter un élément $\sigma \in \mathfrak{S}_n$ par le tableau

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & ... & n-1 & n \\ \sigma(1) & \sigma(2) & \sigma(3) & ... & \sigma(n-1) & \sigma(n) \end{pmatrix}.$$

ou encore par la suite d'associations

$$\begin{array}{l} 1 \to \sigma(1) \\ 2 \to \sigma(2) \\ \quad \vdots \\ n-1 \to \sigma(n-1) \\ n \to \sigma(n) \end{array}$$

Le groupe $\mathfrak{S}_n$ est de cardinal $n!$.

(k-cycles) Soit $2 \leq k \leq n$ un entier et $(i_1, ..., i_k) \in \{1, ..., n\}^k$ distincts. On note $(i_1, ..., i_k)$ la permutation de $\mathfrak{S}_n$ déterminée par

$$i_1 \to i_2 \quad , \quad i_2 \to i_3 \quad , \quad \cdots \quad , \quad i_{k-1} \to i_k \quad , \quad i_k \to i_1$$

et qui laisse fixe les éléments hors de $\{i_1, ..., i_k\}$.

Un 2-cycle est appelé une transposition.

2. (Table d'un groupe) Une façon parfois commode de représenter un groupe G est d'écrire sa table, c'est à dire d'écrire dans un tableau tous les produits possibles des éléments de G (on place à l'intersection de la "ligne g" et la "colonne g'" le produit gg'. Établissons-la pour $\mathfrak{S}_3$. D'une part, ses éléments sont donnés par

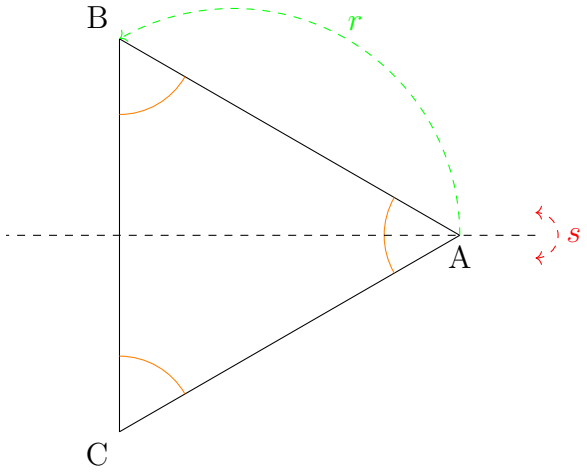
$$\mathfrak{S}_3 = \{id, (12), (13), (23), (123), (132)\}$$

et sa table est donnée par

	id	(12)	(13)	(23)	(123)	(132)
id						
(12)						
(13)						
(23)						
(123)						
(132)						

La table d'un groupe permet d'en observer quelques propriétés (par exemple, elle est symétrique si et seulement si G est abélien, chaque élément apparaît une et une seule fois sur chaque lignes/colonnes...).

3. (Isométries qui préservent un triangle régulier) On considère le triangle formé (par exemple) par les racines troisièmes de l'unité dans $\mathbb{C}$.



Les isométries qui préservent le triangle ABC, munies de la composition des applications, forment un groupe qu'on appelle diédral.
On le note D_3.

Deux des éléments de ce groupe diédral sont essentiels :

- la rotation r d'angle $\frac{2\pi}{3}$ qui envoit A sur B, B sur C et C sur A;
- la symétrie s d'axe ici horizontal. Elle échange B et C, tout en laissant A invariant.

Avec un peu de géométrie, on montre que D_3 est un groupe de cardinal 6. On verra bientôt dans ce cours et en TD qu'essentiellement, c'est le même groupe que $\mathfrak{S}_3$. La construction et les thèmes successifs que nous verrons autour de D_3 se généralisent pour le polynôme régulier à n-cotés, donnant lieu au groupe diédral D_n.

Thème 1.6. (Autour de l'associativité). L'associativité est un axiome tout sauf anodin : sans lui on ne peut pas même parler de la puissance n-ième d'un élément. On a cependant très rarement à la démontrer.

(Exemple vu en TD) Soit $\mathfrak{X} = \{x \in \mathbb{R},\ x > 0 \text{ et } x \neq 1\}$. La formule $x * y = x^{ln(y)}$ définit une loi de composition interne sur $\mathfrak{X}$ qui est associative.

On l'a vu précédemment, il est très facile de construire des opérations non-associatives (par exemple $(z, z') \mapsto \overline{zz'}$ sur $\mathbb{C}$).

Soit $(G, \cdot)$ un groupe et $a \in G$ et $k \in \mathbb{Z}$. Si $k = 0$ on pose $a^0 = e_G$ et si k est strictement positif on note $a^k := a \cdot ... \cdot a$ (produit de k termes). Enfin on pose $a^{-k} := (a^{-1})^k$. Dans ce cadre on retrouve toutes les identités habituelles des puissances, par exemple de nombres réels non-nuls.

Détails. *Soit $(G, \cdot)$ un groupe, $a \in G$.*
(a) $a^i \cdot a^j = a^{i+j}\ \forall\ i, j \in \mathbb{Z}$.
(b) $(a^i)^j = a^{ij} = (a^j)^i\ \forall\ i, j \in \mathbb{Z}$.

Remarque 1.7. Par convention, on note souvent pour les groupes abéliens la loi $+$, et on écrit alors ka plutôt que a^k. Aussi, on parle de *l'opposé* d'un élément a plutôt que de son inverse, et on écrit $-a$ plutôt que a^{-1}.

1.1 Premières propriétés

On peut légèrement affiner les axiomes de la Définition 1.1 en affaiblissant les axiomes (2a) et (2b) comme suit.

Lemme 1.8. *Les axiomes (2a) et (2b) de la définition 1.1 peuvent être remplacés par les deux suivants :*

(2') élément neutre à gauche *: il existe un élément $e_G \in G$ tel que*

(2'a) pour tout $a \in G$ on a

$$e_G \cdot a = a;$$

(2'b) inverses à gauche *: $\forall a \in G,\ \exists\, b \in G,$*

$$b \cdot a = e_G$$

Proof. Soit $a \in G$. Par hypothèse il existe $b \in G$ tel que $b \cdot a = e_G$, et il existe un inverse à gauche de b, qu'on note c.

On a $c \cdot e_G = c \cdot (b \cdot a) = (c \cdot b) \cdot a = e_G \cdot a = a$ et donc

$$a \cdot e_G = (c \cdot e_G) \cdot e_G = c \cdot (e_G \cdot e_G) = c \cdot e_G = a$$

et ainsi (2a) découle de (2'a) et (2'b).

Comme e_G est neutre a gauche, on a maintenant obtenu que $c = a$, d'où

$$a \cdot b = c \cdot b = e_G$$

et (2b) en découle aussi. **C.Q.F.D.**

Remarque 1.9.

- On a vu précédemment l'unicité de l'inverse dans le cadre des groupes. On voit de plus que si a, b sont deux éléments de G, alors $(a^{-1})^{-1} = a$, et $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.
- L'élément neutre e_G est nécessairement unique.

Détails. *On le montre rapidement.*

Proposition 1.10. *Soit $(G, \cdot)$ un groupe, et $a \in G$.*
L'application de "translation à gauche par a", définie par

$$\begin{array}{rccc} \tau_a : & G & \longrightarrow & G \\ & x & \longmapsto & a \cdot x \end{array}$$

est une bijection. Il en va de même avec la translation à droite.

Démonstration. L'application est injective : si $ax = ax'$, alors en multipliant à gauche par a^{-1}, on obtient $x = x'$. Elle est aussi clairement surjective : si $x \in G$, alors $\tau(a^{-1} \cdot x) = x$.

Le même raisonnement en multipliant à droite par a^{-1} le montre pour la translation à droite.
Preuve alternative : donner la bijection réciproque. **C.Q.F.D.**

Corollaire 1.11. *Soit $(G, \cdot)$ un groupe et a, b deux éléments de G. Alors il existe un et un seul élément $x \in G$ tel que*

$$a \cdot x = b$$

2 Ordre d'un élément

Désormais pour alléger les notations, on va se permettre de supprimer le symbole $\cdot$ quand il n'y a pas d'ambiguïté quant à la loi de composition :

$$ab \quad \text{au lieu de} \quad a \cdot b$$

Définition 2.1. Soient G un groupe, et $g \in G$. On considère l'ensemble

$$N_g := \{n \in \mathbb{N} \,|\, n \geq 1 \ , \ g^n = e\} \subset \mathbb{N}^*$$

Si $N_g \neq \emptyset$, on pose $o(g) := min(N_g)$, et on dit que g est *d'ordre fini*. Sinon, on pose $o(g) := \infty$, et on dit que g est *d'ordre infini*. L'entier positif $o(g)$ est appelé *l'ordre de g* et bien entendu, le seul élément d'ordre 1 est l'élément neutre e_G.

Proposition 2.2. *Soient G un groupe g un élément d'ordre fini de G. Si $m \in \mathbb{Z}$ est tel que $g^m = e_G$, alors, $o(g)$ divise m.*

Démonstration. Posons $n := o(g)$.
(a) Division Euclidienne de n par m : $m = nr + s$, $r, s \in \mathbb{Z}$, $0 \leq s < n$. Alors,

$$e_G = g^m = g^{nr+s} = (g^n)^r g^s$$

Donc, $e_G = e_G^r g^s = g^s$. Or, $s < n$, donc $s \notin N_g$. Puisque $s \geq 0$, on en conclut que $s = 0$, c'est-à-dire, que n divise m.

C.Q.F.D.

Exemples 2.3. 1. Ordre des éléments dans $(\mathbb{Z}, +)$, dans $(\mathbb{R}^*, \times)$.

2. Ordre des éléments dans $(\mathbb{Z}/n\mathbb{Z}, +)$;

3. Ordre d'un k-cycle dans $\mathfrak{S}_n$.

Détails. *1. Dans $\mathbb{Z}$ les éléments sont d'ordre 1 ou ∞, dans $(\mathbb{R}^*, \times)$ on voit que les seuls éléments tels que $x^n = 1$ dans $\mathbb{R}$ c'est -1 et 1, ordre 2 seulement.*

2. $o(\overline{k}) = \frac{n}{pgcd(k,n)}$, Cf. TD

3. si on prend un k-cycle et x_i dans son support on a $x_i = \sigma^{i-1}(x_1)$ donc pour tout i on a $\sigma^k(x_i) = \sigma^k(\sigma^{i-1}(x_1)) = \sigma^{i-1}\sigma^k(x_1) = \sigma^{i-1}(x_1) = x_i$ et c'est le plus petit vérifiant cette propriété en évaluant en x_1 par exemple.

Thème 2.4 (Groupes finis et ordre d'un produit)**.**

1. Déterminer l'ordre d'un élément permet de déterminer toutes les puissances qui l'annulent. On peut montrer simplement que dans un groupe fini G de cardinal n, l'ordre des éléments de G est majoré par n. La théorème de Lagrange que nous verrons très vite fournit des restrictions supplémentaires sur l'ordre des éléments dans un groupe fini.

2. Si g et g' sont deux éléments de G, d'ordres respectifs n et m, il est difficile de prédire l'ordre du produit gg'.

Détails. *1. On considére les puissances g, g^2, g^3, ... , g^{n+1} d'un élément g. Comme G a n éléments on a $g^k = g^l$ pour $0 < k < l$, et donc $g^{l-k} = e_G$ et g est d'ordre plus petit que n.*

2. Si g et g' sont inverses l'un de l'autre, l'ordre est 1. Si G est commutatif, on voit que l'ordre est majoré par le ppcm. On peut aussi dire des choses si n et m sont premiers entre eux (TD). Mais si le groupe n'est pas commutatif, gg' peut même être d'ordre infini.

Thème 2.5 (Le groupe symétrique, II)**.** Vous l'avez vu l'année dernière, tout élément du groupe symétrique $\mathfrak{S}_n$ se décompose de manière unique en un produit de cycles à support disjoints (donc qui commutent entre eux). La preuve de ce résultat est de plus algorithmique, et permet de déterminer aisément l'ordre de tout élement de $\mathfrak{S}_n$.

Détails. *Exemple :*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 3 & 9 & 7 & 2 & 5 & 8 & 1 & 6 \end{pmatrix}.$$

on a $\sigma = (1478)(23965)$ on a vu que (1478) est d'ordre 4 et (23965) d'ordre 5 donc σ d'ordre 20 (attention pour ça on utilise à nouveau l'unicité de la décomposition en cycles).

3 Sous-groupes

Définition 3.1. Soient G un groupe et $H \subset G$ un sous-ensemble non-vide. H est appelé *sous-groupe* de G si les axiomes suivants sont satisfaits :

(1) $h_1 h_2 \in H,\ \forall\, h_1, h_2 \in H$.

(2) $h^{-1} \in H,\ \forall\, h \in H$.

Exemples 3.2. 1. Sous-groupes de $(\mathbb{Z}, +)$.

2. Sous-groupe engendré par 1 élément.

Détails. *1. Description rapide, preuve TD.*

2. si $g \in G$ alors $H = \{g^k, k \in \mathbb{Z}\}$ est un sous groupe de G. C'est le plus petit sous-groupe qui contient g et son ordre/cardinal est égal à l'ordre de g. On dit dans ce cas si H est fini que c'est un groupe cyclique.

Proposition 3.3. *Soient G un groupe, et H un sous-groupe de G. Alors, l'élément neutre e de G appartient à H.*

Démonstration. En tant que sous-groupe de G, l'ensemble H est non-vide. Choisissons $h \in H$. Grâce à 3.1 (2), son inverse h^{-1} appartient à H. Grâce à 3.1 (1), le produit de h et de h^{-1} appartient à H donc l'élément neutre appartient à H. **C.Q.F.D.**

En particulier, l'axiome "H non-vide" de la Définition 3.1 peut être remplacé par "H contient l'élément neutre".

Corollaire 3.4. *Soient G un groupe, et H un sous-groupe de G. Alors H, muni de la loi interne induite par celle de G, est lui-même un groupe. L'élément neutre de H coïncide avec celui de G. Pour $h \in H$, l'inverse de h dans H coïncide avec l'inverse de h dans G.*

Démonstration. La loi est associative d'associativité dans H car elle l'est déjà dans G. L'élément neutre de G appartient à H d'après 3.3 ; l'unique inverse dans G d'un élément de H appartient à H grâce à 3.1 (2).
C.Q.F.D.

Dans ce cours, on va utiliser la notation

$$H \leq G \text{ ou même parfois } H < G$$

pour dire que "H est un sous-groupe de G". Attention, cette notation n'est pas utilisée dans tous les livres !

Proposition 3.5. *Soit G un groupe.*
(a) Soient H_i, $i \in I$ des sous-groupes de G. Alors, leur intersection

$$\bigcap_{i \in I} H_i \subset G$$

est un sous-groupe de G.

(b) Soient H_1, H_2 des sous-groupes de G. Alors, leur union

$$H_1 \cup H_2 \subset G$$

est un sous-groupe de G si et seulement si $H_1 \subset H_2$ ou $H_2 \subset H_1$.

Démonstration. (a) $\forall\ i \in I$, $e_G \in H_i$, donc $e_G \in \cap_i H_i$, et $\cap_i H_i \neq \emptyset$. Soient $h_1, h_2 \in \cap_i H_i$. Par hypothèse le produit $h_1 h_2$, et l'inverse h_1^{-1} appartient à H_i, pour tout $i \in I$. L'intersection $\cap_{i\in I} H_i$ est donc bien un sous-groupe de G.

(b) Supposons d'abord $H_1 \subset H_2$. Alors, $H_1 \cup H_2 = H_2 \leq G$. Pareil si $H_2 \subset H_1$. Supposons maintenant $H_1 \cup H_2 \leq G$, et $H_1 \not\subset H_2$. Donc : $\exists\ h_1 \in H_1 - H_2$. Soit $h_2 \in H_2$. Puisque $h_1, h_2 \in H_1 \cup H_2$, et $H_1 \cup H_2$ est un groupe, $h_1 h_2 \in H_1 \cup H_2$. Cet élément ne peut appartenir à H_2 ; sinon,

$$h_1 = h_1(h_2 h_2^{-1}) = (h_1 h_2) h_2^{-1} \in H_2$$

Donc, $h_1 h_2 \in H_1$, et

$$h_2 = (h_1^{-1} h_1) h_2 = h_1^{-1}(h_1 h_2) \in H_1$$

C.Q.F.D.

Corollaire 3.6. *Soit M un sous-ensemble d'un groupe G. Il existe un plus petit sous-groupe de G qui contient M. On l'appelle le sous-groupe engendré par M, noté $< M >$.*

Définition 3.7. Soient G un groupe, $A, B \subset G$ deux sous-ensembles. On pose

$$AB := \{ab \,|\, a \in A\ ,\ b \in B\} \subset G$$

En général, AB n'est pas un sous-groupe de G, même si A et B le sont .

Proposition 3.8. *Soient G un groupe, $H, K \leq G$ deux sous-groupes. Alors, $HK \leq G$ si et seulement si $HK = KH$.*

Démonstration. Supposons d'abord que $HK \leq G$. Alors,

$$HK = \{hk \,|\, h \in H\ ,\ k \in K\} = \{(hk)^{-1} \,|\, h \in H\ ,\ k \in K\}$$

On rappelle que $(hk)^{-1} = k^{-1}h^{-1}$. Donc :

$$HK = \{k^{-1}h^{-1} \,|\, h \in H\ ,\ k \in K\} = \{kh \,|\, h \in H\ ,\ k \in K\}$$

ce qui est égal à KH car le passage à l'inverse est bijectif.

Maintenant, supposons que $HK = KH$. L'ensemble HK contient l'élément

$$e_G = e_G e_G$$

(puisque H et K sont des sous-groupes), donc il n'est pas vide. Soient $h_1k_1, h_2k_2 \in HK$, avec $h_i \in H$ et $k_i \in K$. $k_1h_2 \in KH = HK$, donc $\exists\, h \in H, k \in K$ tel que $k_1h_2 = hk$. Alors,

$$(h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2 = h_1(hk)k_2 = (h_1h)(kk_2)$$

ce qui fait partie de HK. Quant aux inverses,

$$(h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH = HK$$

Donc, $HK \leq G$. **C.Q.F.D.**

4 Groupes engendrés, relations

On a précédemment élucidé le plus petit sous-groupe d'un groupe G qui contient un élément g. Explicitons cela pour des sous-ensembles plus complexes.

Notation 4.1. Etant donnés plusieurs sous-ensembles $M_1, M_2, M_3, \ldots$ d'un groupe G, on écrit $< M_1, M_2, M_3, \ldots >$ au lieu de $< M_1 \cup M_2 \cup M_3 \cup \ldots >$. On écrit aussi simplement $< a, b, c, \ldots >$ au lieu de $< \{a, b, c, \ldots\} >$. Un cas particulier, mais très important concerne les sous-groupes de la forme $< a >$, c'est-à-dire ceux engendrés par un seul élément.

Proposition 4.2. *[G, Rem. 3.48] Soit G un groupe, et $M \subset G$. On pose*

$$M^{-1} := \{m^{-1} \,|\, m \in M\}$$

Soit $g \in < M >$, $g \neq e_G$. Alors

$$\exists\, n \geq 1\ ,\ m_1, m_2, \ldots, m_n \in M \cup M^{-1}\ ,\ g = m_1m_2 \cdots m_n$$

Démonstration. Posons

$$H := \{e_G, m_1m_2 \cdots m_n \,|\, n \geq 1\ ,\ m_1, m_2, \ldots m_n \in M \cup M^{-1}\}$$

H est un sous-groupe de G ; l'observation essentielle étant que l'inverse de $m_1m_2 \cdots m_n$ est $m_n^{-1} \cdots m_2^{-1}m_1^{-1}$, ce qui est un produit d'éléments de $M \cup M^{-1}$ si tous les m_k sont dans $M \cup M^{-1}$. $M \subset H$, donc H est un sous-groupe de G contenant M. Donc : $< M > \leq H$. Soit $g = m_1m_2 \cdots m_n \in H$. $\forall\, k, m_k \in M \cup M^{-1} \subset < M >$. Puisque $< M >$ est un groupe, $g \in < M >$. Donc : $H \leq < M >$. **C.Q.F.D.**

Les éléments du sous-groupe engendré par une partie M de G sont donc les mots formés d'éléments de M ou de leurs inverses, en ajoutant s'il le fautl'élément neutre e_G, vu comme le "mot de longueur zéro".

Corollaire 4.3. *Soit G un groupe, et $M \subset G$. Supposons que*

$$ab = ba\ \forall\ a, b \in M$$

Alors, le sous-groupe $< M >$ de G est Abélien.

Démonstration. Il s'agit de montrer que

$$gh = hg \; \forall \; g, h \in < M >$$

Ecrivons

$$g = a_1 a_2 \cdots a_k \quad \text{et} \quad h = b_1 b_2 \cdots b_n$$

avec $a_i, b_j \in M \cup M^{-1}$; ceci est possible grâce à 4.2. Pour prouver que

$$(a_1 a_2 \cdots a_k)(b_1 b_2 \cdots b_n) = (b_1 b_2 \cdots b_n)(a_1 a_2 \cdots a_k)$$

on applique une récurrence par $k + n$. Si $k + n = 0$, alors $g = h = e_G$ donc c'est clair dans cette situation.

Supposons le résultat démontré en longueur $k + n - 1$ et écrivons

$$gh = a_1 a_2 \cdots a_k b_1 b_2 \cdots b_n.$$

Si $k = 0$, g est neutre et il n'y a rien à montrer. Pour invoquer l'hypothèse de récurrence et démontrer le résultat, il suffit donc de montrer que

$$gh = a_1 a_2 \cdots a_{k-1} b_1 b_2 \cdots b_n a_k,$$

c'est à dire que a_k commute avec les éléments de $M \cup M^{-1}$. On traite tous les cas séparément :

(1) $a_k, b_j \in M$. Ceci est notre hypothèse.

(2) $a_k \in M, b_j \in M^{-1}$. Donc $b_j^{-1} \in M$, et

$$a_k b_j^{-1} = b_j^{-1} a_k$$

On multiplie alors cette égalition par b_j à gauche, et puis par b_j à droite, pour obtenir $b_j a_k = a_k b_j$.

(3) $a_k \in M^{-1}, b_j \in M$. Pareil.

(4) $a_k, b_j \in M^{-1}$. Donc $a_k^{-1}, b_j^{-1} \in M$, et

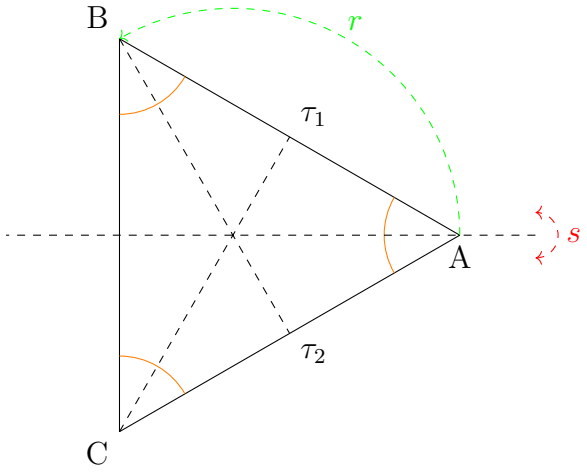
$$a_k^{-1} b_j^{-1} = b_j^{-1} a_k^{-1}$$

Inverser cette équation, pour obtenir $b_j a_k = a_k b_j$. **C.Q.F.D.**

Thème 4.4. 1. Générateurs et unicité.

2. (Le groupe $\mathfrak{S}_n$, III) On a vu précédemment que les cycles engendrent $\mathfrak{S}_n$. On peut trouver d'autres générateurs que les cycles : par exemple, les transpositions engendrent $\mathfrak{S}_n$. Suivant les situations certains générateurs peuvent être plus ou moins utiles ou adaptés.

3. (le groupe D_3, II) On considère toujours le groupe des isométries qui préservent le triangle (régulier) ABC.



Avec un peu de géométrie, on peut montrer que le éléments de D_3 sont id, r, r^2, s, ainsi que les deux symétries axiales τ_1 et τ_2 qui passent par les deux (autres) médianes de ABC. On remarque que $\tau_1 = r \circ s$ et que $\tau_2 = s \circ r$.

On a donc

$$D_3 = \{id, r, r^2, s, rs, sr\};$$

la rotation r et la symétrie s engendrent D_3 entier. N'importe quel produit d'éléments $s^{\alpha_1} r^{\alpha_2} s^{\alpha_3} ... r^{\alpha_{n-1}} s^{\alpha_n}$ peut se simplifier en un des éléments de D_3 ci-dessus grâce à la relation $srs = r^2$. Trouver l'écriture la plus simple possible d'un élément dans un groupe, comme on vient de la faire avec D_3, en fonction d'éléments remarquables et des règles qui les lient, est une tâche utile et difficile. C'est ce qu'on appelle une description par "générateurs et relations".

4. (le groupe $\mathbb{H}_8$ des quaternions) On considère l'ensemble

$$\mathbb{H}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$$

pour lequel on définit une multiplication par les règles suivantes :

   (a) 1 est l'élément neutre;
   (b) -1 commute avec tous les éléments de $\mathbb{H}_8$ et $(-1) \cdot (-1) = 1$;
   (c) $ij = -ji = k$;
   (d) $i^2 = j^2 = k^2 = -1$.

   On construit ainsi bien un groupe, dont la table est donnée par

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	$-j$	j	$-i$	i	-1	1
$-k$	$-k$	k	j	$-j$	i	$-i$	1	-1

Le groupe $\mathbb{H}_8$ n'est pas abélien, -1 y est d'ordre 2, tandis que tous les autres éléments non-neutres sont d'ordre 4.

Détails. *1. On peut choisir des générateurs différents pour un groupe, par exemple $\mathbb{Z}/6\mathbb{Z}$: $\overline{1}$ est générateur, $\overline{2}$ n'est pas générateur, mais $\overline{5}$ l'est. On a déjà vu en réalité avec l'ordre qu'être générateur dans $\mathbb{Z}/n\mathbb{Z}$ c'est être la classe d'un entier premier à n, indicatrice d'Euler.*

2. Tout cycle $(i_1...i_k)$ se décompose en le produit de transpositions $(i_1 i_2)...(i_{k-1} i_k)$ donc la décomposition en cycles à support disjoints induit que les transpositions engendrent $\mathfrak{S}_n$. Ca sera utile par exemple pour calculer la signature.

3. Un exemple de réécriture d'un élément dans D_3.

5 Morphismes

Comme il est d'usage en algèbre, après avoir considéré des structures algébriques, on s'intéresse aux applications qui les respectent.

Définition 5.1. [G, Déf. 2.13] Soient $(G, \cdot)$, $(H, *)$ deux groupes. Une application

$$\alpha : G \longrightarrow H$$

est appelée *homomorphisme (de groupes)* ou *morphisme (de groupes)* si

$$\forall\, g_1, g_2 \in G\ , \quad \alpha(g_1 \cdot g_2) = \alpha(g_1) * \alpha(g_2)$$

L'ensemble des homomorphismes de $(G, \cdot)$ vers $(H, *)$ est noté

$$\mathrm{Hom}((G, \cdot), (H, *))$$

Si $(H, *) = (G, \cdot)$, et $\alpha \in \mathrm{Hom}((G, \cdot), (G, \cdot))$, on dit que α est un *endomorphisme (du groupe G).*

On va à nouveau se permettre de supprimer les symboles $\cdot$ et $*$ quand il n'y a pas d'ambiguïté quant aux lois de composition:

$$\mathrm{Hom}(G, H) \quad \text{au lieu de} \quad \mathrm{Hom}((G, \cdot), (H, *))$$

Définition 5.2. Soient G, H deux groupes, et $\alpha \in \mathrm{Hom}(G, H)$.
(a) α est un *épimorphisme (de groupes)* si α est surjectif. On écrit

$$\alpha : G \twoheadrightarrow H$$

α est un *monomorphisme (de groupes)* si α est injectif. On écrit

$$\alpha : G \hookrightarrow H$$

α est un *isomorphisme (de groupes)* si α est bijectif. On écrit

$$\alpha : G \xrightarrow{\sim} H$$

Si $H = G$, et $\alpha : G \xrightarrow{\sim} G$, on dit que α est un *automorphisme de* G.

(b) On dit que G *est isomorphe à* H, et on écrit $G \cong H$ s'il existe un isomorphisme de G vers H.

(c) On définit *l'image de* α comme

$$\operatorname{im}\alpha := \{\alpha(g) \,|\, g \in G\} \subset H$$

On définit le *noyau de* α comme

$$\ker\alpha := \{g \in G \,|\, \alpha(g) = e_H\} \subset G$$

Exemples 5.3. (a) L'application déterminant définit un morphisme de groupes $GL_n(\mathbb{R}) \longrightarrow (\mathbb{R}^*, \times)$. Son noyau est le groupe spécial linéaire.

(b) Soit $\alpha : G \to H$ un homomorphisme de groupes. D'après la Proposition 5.5 (c) (voir ci-dessous), $\operatorname{im}\alpha$ est un sous-groupe de H. Alors, α induit un homomorphisme

$$G \longrightarrow \operatorname{im}\alpha \quad , \quad g \longmapsto \alpha(g)$$

Notons-le α'. (α' n'est pas égal à α car les deux applications n'ont pas la même cible!) Par construction, α' est surjectif, c'est-à-dire, c'est un épimorphisme. En plus, si α est un monomorphisme, alors α' est un isomorphisme :

$$\alpha' : G \xrightarrow{\sim} \operatorname{im}\alpha$$

Thème 5.4. (Automorphismes intérieurs)
Soit G un groupe, et $x \in G$. On définit une application

$$int(x) : G \longrightarrow G \,, \quad g \longmapsto xgx^{-1}$$

Soient $g_1, g_2 \in G$. Alors,

$$int(x)(g_1g_2) = xg_1g_2x^{-1} = xg_1x^{-1}xg_2x^{-1} = (int(x)(g_1))(int(x)(g_2))$$

Donc, $int(x)$ est un endomorphisme de G. En fait, c'est un automorphisme : son inverse est égal à $int(x^{-1})$. L'application $int(x)$ est appelée la *conjugaison par* x et pour tout sous-ensemble H de G, on note

$$xHx^{-1} := int(x)(H) = \{xhx^{-1} \,|\, h \in H\}$$

L'ensemble $\operatorname{Aut}(G)$ des automorphismes d'un groupe G est lui-même un groupe, pour la compositions des applications. On observe même que l'application

$$\begin{array}{rccc} int: & (G,\cdot) & \longrightarrow & (\operatorname{Aut}(G),\circ) \\ & x & \longmapsto & int(x) \end{array}$$

est un morphisme de groupes.

Proposition 5.5. *Soient G, H deux groupes, et $\alpha \in \mathrm{Hom}(G,H)$.*
(a) α envoie l'élément neutre de G vers l'élément neutre de H.
(b) $\forall\, g \in G$, $\alpha(g^{-1}) = \alpha(g)^{-1}$.
(c) $\mathrm{im}\,\alpha$ est un sous-groupe de H. Plus généralement,

$$\alpha(G') := \{\alpha(g') \,|\, g' \in G'\} \subset H$$

est un sous-groupe de H pour tout $G' \leq G$.
(d) l'image réciproque d'un sous-groupe de H est un sous-groupe de G. En particulier, $\ker\alpha$ est un sous-groupe de G.
(e) α est un monomorphisme si et seulement si $\ker\alpha = \{e\}$.
(f) α est un isomorphisme si et seulement si $\exists\, \beta \in \mathrm{Hom}(H,G)$,

$$\beta \circ \alpha = \mathrm{id}_G : G \longrightarrow G \qquad et \qquad \alpha \circ \beta = \mathrm{id}_H : H \longrightarrow H$$

Ici on note $\cdot$ la composition des applications.

Démonstration. (a) Si $g \in G$, on a $\alpha(g) = \alpha(e_G \cdot g) = \alpha(e_G) * \alpha(g)$ donc en multipliant par l'inverse de $\alpha(g)$ on a $\alpha(e_G) = e_H$.

(b) Pour tout $g \in G$, $\alpha(g) * \alpha(g^{-1}) = \alpha(g \cdot g^{-1}) = \alpha(e_G) = e_H$.

(c) $\alpha(G')$ est clairement non-vide car G' l'est, stable par produit car $\alpha(g) * \alpha(g') = \alpha(g \cdot g')$ et $gg' \in G'$, et stable par inverse par (b).

(d) Soit $K \leq H$. On a e_G appartient à $\alpha^{-1}(K)$ par (a) et car e_H est un élément de K. Si g et g' sont deux éléments de $\alpha^{-1}(K)$, alors $\alpha(gg') = \alpha(g)\alpha(g')$ est un élément de K. De même par $b)$ si g appartient à $\alpha^{-1}(K)$, $\alpha(g^{-1}) = \alpha(g)^{-1}$ est un élément de K.

(e) Supposons que α soit un monomorphisme : si x est un élément de $\ker\alpha$ alors $\alpha(x) = \alpha(e_G)$ donc $x = e_G$. Réciproquement si $\alpha(x) = \alpha(y)$, alors $\alpha(xy^{-1}) = e_H$ donc $xy^{-1} = e_G$ et $x = y$.

(f) Il s'agit de montrer que si un morphisme de groupes α est une bijection, alors sa bijection réciproque est aussi un morphisme. Si $(h, h') \in H^2$, alors $h * h' = \alpha(\alpha^{-1}(h)) * \alpha(\alpha^{-1}(h'))$ et donc $\alpha^{-1}(h * h') = \alpha^{-1}(h) * \alpha^{-1}(h')$.
C.Q.F.D.

Corollaire 5.6. *Soient G un groupe, et $H \leq G$. Alors,*

$$\forall\, g \in G\ ,\ gHg^{-1} \leq G$$

Démonstration. D'après le Thème 5.4,

$$int(g) : G \longrightarrow G\ , \quad x \longmapsto gxg^{-1}$$

est un endomorphisme de G. D'après la Proposition 5.5 (c), l'image sous $int(g)$ du sous-groupe H est un sous-groupe de G. **C.Q.F.D.**

Remarque 5.7 (Morphismes et ordre)**.** Si $\alpha : G \longrightarrow H$ est un morphisme de groupes et $g \in G$, alors $o(\alpha(g))|o(g)$. Cette remarque impose de sévères restrictions sur les morphismes entre deux groupes.

Thème 5.8. 1. Étant donné un entier n positif, on peut considérer

$$\begin{array}{rccc} \pi : & \mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ & k & \longmapsto & \overline{k} \end{array} .$$

Cette application est un morphisme de groupes car elle est compatible avec l'addition dans $\mathbb{Z}$, et en outre on a $\ker \pi = n\mathbb{Z}$. Le morphisme π est appelé la projection canonique de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$. On construira dans la suite une vaste généralisation de ces propriétés, dans le cadre des groupes quotients.

2. (Morphismes et générateurs) Tout morphisme $\alpha : (\mathbb{Z}, +) \longrightarrow (G, *)$ est uniquement déterminé par l'image de 1, puisque pour tout $k \in \mathbb{Z}$, on a nécessairement $\alpha(k) = \alpha(1) * ... * \alpha(1) = \alpha(1)^{*k}$. De même, tout morphisme $\beta : \mathbb{Z}/n\mathbb{Z} \longrightarrow (G, *)$ est déterminé par l'image de $\overline{1}$. Exemple : déterminer tous les morphismes $\mathbb{Z}/n\mathbb{Z} \longrightarrow (\mathbb{R}^*, \times)$.

   Plus généralement, si $\{g_1, ..., g_k\}$ est un système de générateurs d'un groupe G, alors tout morphisme γ dont l'ensemble de départ est G est uniquement déterminé par les images $\gamma(g_1), ..., \gamma(g_k)$ de ces éléments.

3. (le groupe $\mathfrak{S}_n$, IV) Vous avez montré en L2 (preuve qui n'est pas facile) qu'il existe un et un seul morphisme sgn : $\mathfrak{S}_n \longrightarrow \{\pm 1\}$. On peut le définir en décrétant que pour toute transposition τ, on a $\text{sgn}(\tau) = -1$. Ce morphisme est appelé la signature et son noyau, noté $\mathfrak{A}_n$, est un groupe dit alterné.

6 Classes modulo un sous-groupe

Définition 6.1. [G, Lemme 3.30, Term. 3.31] Soient G un groupe, H un sous-groupe de G, et $g \in G$. On pose

$$gH := \{gh \,|\, h \in H\} \subset G$$

et

$$Hg := \{hg \,|\, h \in H\} \subset G$$

gH est appelé la *classe à gauche de g modulo H*, et Hg la *classe à droite de g modulo H*.

Exercice 6.2. Soient G un groupe et $x \in G$ et H un sous-groupe de G. On définit une application

$$m'_x : H \longrightarrow xH \ , \ h \longmapsto xh$$

Alors, m'_x est une bijection. En particulier H et xH ont même cardinal.

Proposition 6.3. *Soient G un groupe, et H un sous-groupe de G.*
(a)

$$G = \bigcup_{g \in G} gH\,, \quad et \quad G = \bigcup_{g \in G} Hg$$

(b) Soient $g_1, g_2 \in G$. Alors,

$$g_1H \cap g_2H = \begin{cases} g_1H = g_2H & si\ g_1^{-1}g_2 \in H \\ \emptyset & sinon \end{cases}$$

En particulier,

$$g_2 \in g_1H \Longrightarrow g_1H = g_2H$$

(puisque $g_2 = g_2e_G \in g_2H$).
(c) Soient $g_1, g_2 \in G$. Alors,

$$Hg_1 \cap Hg_2 = \begin{cases} Hg_1 = Hg_2 & si\ g_2g_1^{-1} \in H \\ \emptyset & sinon \end{cases}$$

En particulier,

$$g_2 \in Hg_1 \Longrightarrow Hg_1 = Hg_2$$

Démonstration. On montre uniquement les énoncés pour les classes à gauche.

(a) Evidemment, $\bigcup_{g \in G} gH \subset G$. Soit $g \in G$. Alors,

$$g = ge_G \in gH$$

Donc, $G \subset \bigcup_{g \in G} gH$.

(b) D'une part $g_1H \cap g_2H$ n'est pas vide alors on a $g_1h_1 = g_2h_2$ pour certains h_1, h_2 dans H. Dès lors si $g_1h \in g_1H$, alors

$$g_1h = g_1h_1h_1^{-1}h = g_2h_2h_1^{-1}h$$

et donc $g_1H \subset g_2H$. Le même raisonnement en remplaçant g_1 par g_2 montre donc que soit $g_1H \cap g_2H$ est vide, soit $g_1H = g_2H$. Cette dernière condition est alors clairement équivalente au fait que $g_1^{-1}g_2$ est un élément de H, puisque dans ce cas $g_1H \cap g_2H \neq \emptyset$. **C.Q.F.D.**

Deux classes à gauche modulo H (ou à droite) sont donc soit identiques, soit disjointes.

Corollaire 6.4. *[G, Cor. 3.35] Soient G un groupe, et H un sous-groupe de G. Supposons donné un système de représentants pour les classes à gauche modulo H, c'est à dire un sous-ensemble $L \subset G$ tel que*

$$\forall\, g \in G\,,\ |\, L \cap gH\,| = 1$$

(Autrement dit, on choisit un élément dans chaque classe modulo H.)

Alors on a la réunion disjointe

$$G = \coprod_{g \in L} gH$$

On construit donc ainsi une partition de G en classes à gauche modulo H.

Cette partition est appelée la *décomposition de G en classes à gauche modulo H*. L'ensemble L est appelé un *système de représentants* pour les classes à gauche modulo H.

Définition 6.5. [G, Term. 3.43] Soient G un groupe, et H un sous-groupe de G. On dit que H est *d'indice fini dans G* si l'ensemble des classes à gauche modulo H est fini. On définit alors *l'indice de H dans G*, noté $[G : H]$, comme étant le cardinal de cet ensemble de classes. Si H n'est pas d'indice fini dans G, on pose

$$[G : H] = \infty$$

Donc, $[G : H]$ est égal au cardinal de tout système de représentants pour les classes à gauche modulo H.

Exemples 6.6.

1. Classes à gauche modulo un sous-groupe de $(\mathbb{Z}, +)$.
2. (le groupe $\mathfrak{S}_n$, V) Le sous-groupe $\mathfrak{A}_n$ de $\mathfrak{S}_n$ ($n > 1$) est d'indice 2, puisqu'étant donnée une transposition τ, on a $\mathfrak{S}_n = \mathfrak{A}_n \sqcup \tau\mathfrak{A}_n$.
3. (le groupe D_3, III) On a vu précédemment que le groupe D_3 des isométries laissant invariant un triangle régulier ABC d'écrit
$$D_3 = \{id, r, r^2, s, rs, sr\},$$
On note $H =< r >$ le sous-groupe engendré par la rotation r précédente et $K =< s >$ celui engendré par la symétrie s. Identifier les classes à gauche modulo H et K et exhiber dans les deux cas un système de représentants pour les classes à gauche.

Détails.

1. *Un système de représentants.*
2. *Si $\sigma \in \mathfrak{S}_n$ est de signature -1, alors si τ est une transposition, $\tau \circ \sigma$ est de signature 1 donc dans $\mathfrak{A}_n$. N'importe quel choix de transposition donne un système de représentants. On a en particulier $|\mathfrak{A}_n| = \frac{n!}{2}$.*
3. *On a deux classes à gauche modulo H : $id \cdot H = H = \{id, r, r^2\}$ et $sH = \{s, sr, sr^2\}$. On sait que $srs = r^2$ donc $sr^2 = s^2rs = rs$ et on a bien $D_3 = H \sqcup sH$. Pour K : on a $K = \{id, s\}$, $rK = \{r, rs\}$ et $r^2K = \{r^2, r^2s = srs^2 = sr\}$. On pouvait savoir à l'avance le nombre d'éléments dans un système de représentants en regardant les cardinaux.*

Remarque 6.7. Si G est un groupe fini, alors tout sous-groupe de G est d'indice fini. En revanche si G est infini, on ne peut prédire la finitude des indices des sous-groupes de G

Détails. *Les sous-groupes de $\mathbb{Z}$ sont tous d'indice fini, sauf le sous-groupe trivial.*

Théorème 6.8 (Lagrange)**.** (J.L. Lagrange, 1736–1813) *Soient G un groupe fini, et H un sous-groupe de G. Alors,*

$$|\,G\,| \;=\; |\,H\,| \cdot [G : H]$$

En particulier, les nombres entiers $|\,H\,|$ et $[G : H]$ divisent $|\,G\,|$.

Démonstration. On fixe un système de représentants L pour les classes à gauche modulo H. D'après 6.4,

$$G = \coprod_{g \in L} gH$$

est une partition. Donc:

$$|\,G\,| = \sum_{g \in L} |\,gH\,|$$

D'après l'Exercice 6.2

$$|\,G\,| = \sum_{g \in L} |\,H\,| \;=\; |\,H\,| \cdot |\,L\,| \;=\; |\,H\,| \cdot [G : H]$$

C.Q.F.D.

Corollaire 6.9. *Si $|\,G\,|$ est un groupe d'ordre un nombre premier, alors G est cyclique (donc abélien) et n'admet que deux sous-groupes : $\{e\}$ et G.*

Démonstration. L'ordre de g est égal à l'ordre du sous-groupe $< g >$ qu'il engendre, et ce dernier divise $|\,G\,|$ par le théorème de Lagrange.

Si $|\,G\,|$ est premier, alors tous les éléments de $G \smallsetminus \{e_G\}$ sont d'ordre p et engendrent G. Autrement dit si un sous-groupe de G contient un élément $g \neq e_G$, il contient $< g >= G$. **C.Q.F.D.**

7 Groupes quotients

Soit $(G, \cdot)$ un groupe et H un de ses sous-groupes, disons d'indice fini. On fixe un système de représentants $\{g_1, ..., g_n\}$ pour les classes à gauche modulo H. On aimerait munir l'ensemble de classes à gauche $\{g_1H, ..., g_nH\}$ d'une structure de groupe compatible avec celle de G, mais pour cela quelques restrictions sont nécessaires.

Définition 7.1. Soient G un groupe, et $H \leq G$. On dit que H est un *sous-groupe distingué* de G, et on écrit

$$H \trianglelefteq G \text{ ou même } H \triangleleft G$$

si pour tout $g \in G$, on a $gHg^{-1} = H$.

Lemme 7.2. *Soit $\alpha : G \longrightarrow H$ un morphisme de groupes. L'image réciproque de tout sous groupe distingué $K \subset H$ est un sous-groupe distingué de G. En particulier, le noyau d'un morphisme de groupes est distingué.*

Démonstration. Soit $x \in \alpha^{-1}(K)$ et $g \in G$. L'élément

$$\alpha(gxg^{-1}) = \alpha(g)\alpha(x)\alpha(g)^{-1}$$

appartient bien à K, donc le sous-groupe $\alpha^{-1}(K)$ est distingué. **C.Q.F.D.**

Remarque 7.3.

1. L'image d'un sous-groupe distingué n'est en revanche pas toujours distinguée.
2. Prouver qu'un sous-groupe est le noyau d'un morphisme est souvent très pratique pour montrer qu'il est distingué. On obtient par exemple immédiatement que $\mathfrak{A}_n$ est distingué dans $\mathfrak{S}_n$, $SL_n(\mathbb{C})$ est distingué dans $GL_n(\mathbb{C})$... On verra très vite la réciproque : tout sous-groupe distingué est le noyau d'un certain morphisme.

Détails. *1. Un exemple (par exemple on envoit $\mathbb{Z}/2\mathbb{Z}$ sur une transposition dans $\mathfrak{S}_n$...)*

2. quelques noyaux.

Exemple 7.4. Tout sous-groupe d'un groupe Abélien G est distingué, puisque

$$ghg^{-1} = h \; \forall \; g, h \in G$$

Lemme 7.5. *Un sous-groupe H d'un groupe G est distingué si et seulement si pour tout $g \in G$, $gHg^{-1} \subset H$.*

Démonstration. Il s'agit de montrer que $g \in G$ on a $H \subset gHg^{-1}$. En effet si $h \in H$, alors $h = gg^{-1}hgg^{-1} \subset gHg^{-1}$ car $g^{-1}Hg \subset H$. **C.Q.F.D.**

Proposition 7.6. *Soient G un groupe, et $H \leq G$. Les énoncés suivants sont équivalents :*

(a) $H \trianglelefteq G$.

(b) $\forall \; g \in G$, $gH = Hg$, *c'est-à-dire la classe à gauche de g modulo H est égale à la classe à droite de g modulo H.*

(c) $\forall\ g_1, g_2 \in G$, *l'ensemble* $(g_1H)(g_2H)$ *est égal à la classe à gauche de* g_1g_2 *modulo* H.

Démonstration. (a) $\Rightarrow$ (b) : Si $g \in G$ et H est distingué, on a

$$gH = gH(g^{-1}g) = (gHg^{-1})g = Hg.$$

(b) $\Rightarrow$ (c) : Un élément de $(g_1H)(g_2H)$ s'écrit $g_1h_1g_2h_2$ pour deux éléments h_1, h_2 de H. Par hypothèse $g_2H = Hg_2$ donc on a un élément $\tilde{h} \in H$ tel que

$$g_1h_1g_2h_2 = g_1g_2\tilde{h}h_2$$

et $(g_1H)(g_2H) \subset g_1g_2H$. L'inclusion réciproque est claire.

(c) $\Rightarrow$ (a) : On a $(gH)(g^{-1}H) = e_GH = H$ par hypothèse, donc gHg^{-1} est bien entendu contenu dans H. Le Lemme 7.5 indique alors que H est distingué. **C.Q.F.D.**

Thème 7.7. (le groupe des quaternions $\mathbb{H}_8$, II) On peut observer une propriété du groupe $\mathbb{H}_8$: tous ses sous-groupes sont distingués. Un groupe qui vérifie cette propriété est appelé un groupe de Dedekind.

Détails. *Description rapide des groupes de Dedekind finis, groupe abélien ou produit de quaternions d'un groupe abélien d'exposant* 2 *et d'un groupe abélien d'ordre impair.*

Définition 7.8. [G, Not. 3.28, Lemme 3.30] Soient G un groupe, et $H \leq G$. On pose

$$G/H := \{\text{classes à gauche modulo } H\}$$

On a donc $|\,G/H\,| = [G : H]$.

Théorème 7.9. *Soient* G *un groupe, et* $H \trianglelefteq G$.

(a) La règle

$$(g_1H) \cdot (g_2H) := (g_1g_2)H$$

définit une loi de composition $\cdot$ *sur* G/H. $(G/H, \cdot)$ *est à nouveau un groupe. Son élément neutre est* $e_GH \in G/H$, *l'inverse de* $gH \in G/H$ *est* $g^{-1}H$. *On a* $|\,G/H\,| = [G : H]$.

(b) L'application

$$\pi : G \longrightarrow G/H\ ,\ g \longmapsto gH$$

est un épimorphisme de groupes. On a $\ker\pi = H$. *En particulier,* π *est un isomorphisme si et seulement si* $H = \{e_G\}$.

Définition 7.10. Dans la situation du Théorème 7.9, on appelle G/H le *groupe quotient de* G *par* H, et

$$\pi : G \twoheadrightarrow G/H$$

la surjection canonique (ou l'épimorphisme canonique) de G *vers* G/H.

Remarque 7.11. On sera souvent confrontés au problème suivant : soient E, F deux ensembles, et $\sim$ une relation d'équivalence sur E. Supposons qu'on essaie de construire une application

$$E/\sim \longrightarrow F$$

($E/\sim$:= le quotient de E par $\sim$, c'est-à-dire l'ensemble des classes d'équivalence). Cette construction se passe en deux étapes : (1) Définir une application $f : E \to F$. (2) Montrer que pour $x, y \in E$, la relation $x \sim y$ implique que $f(x) = f(y)$. On peut alors définir

$$E/\sim \longrightarrow F\ ,\ [x] \longmapsto f(x)$$

($[x]$:= la classe de x). Ceci est *bien défini* car $[x] = [y]$ implique $f(x) = f(y)$ (d'après (2)).

Démonstration du Théorème 7.9. (a) Il s'agit d'abord de prouver que l'application

$$G/H \times G/H \longrightarrow G/H\ ,\ (g_1H, g_2H) \longmapsto (g_1g_2)H$$

est bien définie. Autrement dit, que pour $g_1, g_1', g_2, g_2' \in G$ avec $g_1H = g_1'H$ et $g_2H = g_2'H$, on a

$$(g_1g_2)H = (g_1'g_2')H$$

D'après la Proposition 7.6 (c), on a

$$(g_1g_2)H = g_1Hg_2H = g_1'Hg_2'H = (g_1'g_2')H$$

donc c'est effectivement le cas et on obtient une loi de composition sur G/H.

La vérification des axiomes de groupes pour cette loi découle directement du fait que G lui-même est un groupe, grâce à la relation

$$(g_1g_2)H = (g_1H)(g_2H).$$

En effet par exemple pour l'associativité (3 (1)), on a

$$aH((bH)(cH)) = aH((bc)H) = (abc)H = ((ab)H)(cH) = ((aH)(bH))cH$$

(b) Prouvons d'abord que π est un homomorphisme. Ceci est encore la Proposition 7.6 (c). En effet, dire que π est un homomorphisme est équivalent à

$$\forall\ g_1, g_2 \in G\ ,\quad (g_1g_2)H = (g_1H)(g_2H)$$

La surjectivité de π est évidente. Pour déterminer son noyau, soit $g \in G$. Alors,

$$g \in \ker\pi \Longleftrightarrow gH = eH \overset{6.3\ (b)}{\Longleftrightarrow} g \in H$$

C.Q.F.D.

Théorème 7.12 (Propriété universelle du groupe quotient)**.**
Soient G_1 un groupe, et $H \trianglelefteq G_1$. Notons π la surjection canonique de G_1 vers G_1/H. Soit G_2 un groupe.
(a) Soit $\alpha \in \mathrm{Hom}(G_1, G_2)$, et supposons que

$$H \subset \ker \alpha$$

c'est-à-dire $\forall\, h \in H$, $\alpha(h) = e_{G_2}$. Alors, il existe une unique application

$$\tilde{\alpha} : G_1/H \longrightarrow G_2$$

telle que $\alpha = \tilde{\alpha} \circ \pi$. L'application $\tilde{\alpha}$ est un homomorphisme de groupes.
(b) La règle $\alpha \mapsto \tilde{\alpha}$ induit une application

$$\{\alpha \in \mathrm{Hom}(G_1, G_2) \,|\, H \subset \ker \alpha\} \longrightarrow \mathrm{Hom}(G_1/H, G_2)$$

Cette application est bijective. Autrement dit : se donner un homomorphisme $G_1/H \to G_2$ revient à la même chose que se donner un homomorphisme $G_1 \to G_2$ qui est trivial sur H.

Démonstration. (a) Vu la surjectivité de π, il est clair qu'il existe au plus une application $\tilde{\alpha}$ telle que $\alpha = \tilde{\alpha} \circ \pi$. On souhaiterait poser

$$\tilde{\alpha}(gH) := \alpha(g)$$

Mais il faut montrer que ceci est bien défini : soient $g, g' \in G_1$, $gH = g'H$. Il s'agit de vérifier que $\alpha(g) = \alpha(g')$. D'après la Proposition 6.3 (b), $(g')^{-1}g \in H$, ce qui est contenu dans $\ker \alpha$ d'après notre hypothèse. Donc,

$$e_{G_2} = \alpha((g')^{-1}g) = \alpha(g')^{-1}\alpha(g)$$

et $\alpha(g) = \alpha(g')$. Pour montrer que $\tilde{\alpha}$ est un homomorphisme, on fait comme dans la preuve du Théorème 7.9.
(b) Il s'agit de montrer que

$$\{\alpha \in \mathrm{Hom}(G_1, G_2) \,|\, H \subset \ker \alpha\} \longrightarrow \mathrm{Hom}(G_1/H, G_2)\ ,\ \alpha \longmapsto \tilde{\alpha}$$

est bijectif. La surjectivité est évidente : pour $\beta \in \mathrm{Hom}(G_1/H, G_2)$, posons

$$\alpha := \beta \circ \pi : G_1 \longrightarrow G_2$$

On a alors $\tilde{\alpha} = \beta$ grâce à l'unicité dans (a). Quant à l'injectivité, prenons $\alpha_1, \alpha_2 \in \mathrm{Hom}(G_1, G_2)$, avec restrictions triviales à H. Si $\tilde{\alpha_1} = \tilde{\alpha_2}$, alors

$$\alpha_1 = \tilde{\alpha_1} \circ \pi = \tilde{\alpha_2} \circ \pi = \alpha_2$$

C.Q.F.D.

7.1 Sous-groupes d'un quotient

On fixe désormais H un sous-groupe distingué d'un groupe G et on note

$$\pi : G \twoheadrightarrow G/H$$

est la surjection canonique associé.

Proposition 7.13. *La surjection canonique π induit une bijection entre les sous-groupes de G/H et les sous-groupes de G qui contiennent H. Cette bijection préserve de plus les sous-groupes distingués.*

Démonstration. Soit $\tilde{H}$ un sous-groupe de G/H. On a

$$\tilde{H} = \pi(\pi^{-1}\tilde{H})$$

car π est surjectif. On en déduit que l'application $\tilde{H} \mapsto \pi^{-1}(\tilde{H})$ est injective, à valeurs dans les sous groupes qui contiennent H car $\pi^{-1}(\tilde{H})$ contient évidemment $\pi^{-1}(e_{G/H}) = H$.

Il reste à montrer que si K est un sous-groupe de G qui contient H, on a $K = \pi^{-1}(\pi(K))$: l'inclusion $\subset$ est triviale. Pour l'autre si $x \in \pi^{-1}(\pi(K))$, alors $\pi(x) = \pi(k)$, pour un $k \in K$. Dès lors xk^{-1} appartient au noyau H de π, donc à K et x lui-même est dans K.

C.Q.F.D.

8 Théorèmes d'isomorphismes

Théorème 8.1 (Théorème d'homomorphie)**.** *Soient G_1 et G_2 deux groupes, et $\alpha \in \mathrm{Hom}(G_1, G_2)$. Notons π la surjection canonique de G_1 vers $G_1/\ker\alpha$.*

(a) Il existe une unique application

$$\beta : G_1/\ker\alpha \longrightarrow G_2$$

telle que $\alpha = \beta \circ \pi$. De plus β est un homomorphisme de groupes.

(b) β est injectif, et donc, un monomorphisme de groupes $G_1/\ker\alpha \hookrightarrow G_2$.

(c) (premier théorème d'isomorphisme) β induit un isomorphisme

$$G_1/\ker\alpha \xrightarrow{\sim} \mathrm{im}\,\alpha$$

Définition 8.2. Dans la situation du Théorème 8.1, on appelle

$$G_1/\ker\alpha \xrightarrow{\sim} \mathrm{im}\,\alpha$$

l'isomorphisme canonique entre $G_1/\ker\alpha$ et $\mathrm{im}\,\alpha$.

Rappelons que l'énoncé "$G_1/\ker\alpha \cong \mathrm{im}\,\alpha$" est également vrai en théorie d'espaces vectoriels...

Démonstration du Théorème 8.1. (a) Ceci résulte de la propriété universelle 7.12 (a), appliquée à $H := \ker\alpha$. On a donc

$$\forall\ g \in G_1\ ,\ \beta(g\ker\alpha) = \alpha(g)$$

(b) Prouvons que $\ker \beta$ est trivial : soit $g \in G_1$ tel que $\beta(g \ker \alpha) = e$. D'après (a), ceci veut dire que $\alpha(g) = e$, et donc, que $g \in \ker \alpha$. Autrement dit,

$$g \ker \alpha = e \ker \alpha$$

est l'élément neutre de $G_1/\ker \alpha$.

(c) Appliquer l'Exemple 5.3 (b) à la situation dans (b). **C.Q.F.D.**

Complément 8.3. *Soit $K \leq H \leq G$. On suppose $K \trianglelefteq G$. Alors, le noyau du morphisme*

$$\pi_H : H \longrightarrow G/K \ , \ h \longmapsto \pi(h)$$

est égal à K. D'après le Théorème 8.1, π_H induit un monomorphisme

$$H/K \hookrightarrow G/K$$

Son image est $\pi(H)$. Il induit donc un isomorphisme

$$H/K \xrightarrow{\sim} \pi(H)$$

Démonstration. Notons d'abord que $K \trianglelefteq H$ car $K \trianglelefteq G$. On utilise 7.9 (b) et 5.3 (b) pour le premier et le dernier énoncé. Par construction, l'image de $H/K \to G/K$ est $\pi(H)$. **C.Q.F.D.**

Exemples 8.4. 1. Soit G un groupe, $g \in G$ et

$$\gamma_g : \mathbb{Z} \longrightarrow G \ , \ i \longmapsto g^i$$

le morphisme $\mathbb{Z} \longrightarrow G$ donné par $\gamma_g(1) = g$. Déterminons l'image et le noyau de γ_g.

Par définition, on a

$$\operatorname{im} \gamma_g = \{g^i \in G \,|\, i \in \mathbb{Z}\} \subset G$$

et $\operatorname{im} \gamma_g = < g >$ est le sous-groupe de G engendré par g. En outre,

$$\ker \gamma_g = \{i \in \mathbb{Z} \,|\, g^i = e\} \subset \mathbb{Z}$$

qui est un sous-groupe de $\mathbb{Z}$ et s'écrit donc $n\mathbb{Z}$, pour un certain $n \in \mathbb{Z}$. L'entier n détermine l'ordre de G :

- si $n = 0$, alors g est d'ordre infini;
- sinon $o(g) = n$.

Autrement dit, γ_g est injectif si et seulement si g est d'ordre infini. Le premier théorème d'isomorphisme indique donc que γ_g induit un isomorphisme

$$\mathbb{Z}/\ker \gamma_g \xrightarrow{\sim} < g >$$

2. On a donc obtenu l'alternative suivante, pour un groupe G engendré par un élément g :

- si g est d'ordre infini, alors $\gamma_g \in \mathrm{Hom}(\mathbb{Z}, G)$ est un isomorphisme;
- si g est d'ordre fini, $\gamma_g \in \mathrm{Hom}(\mathbb{Z}, G)$ induit un isomorphisme entre G et $\mathbb{Z}/o(g)\mathbb{Z}$; G est donc cyclique.

3. On fixe $n \in \mathbb{N}^*$. Considérons le nombre complexe

$$\zeta := \exp(2\pi i/n) \in \mathbb{C}^*$$

Posons

$$\gamma_\zeta : \mathbb{Z} \longrightarrow \mathbb{C}^* \ , \ k \longmapsto \zeta^k$$

comme dans (a). L'image de γ_ζ est donc le sous-groupe (multiplicatif) de $\mathbb{C}^*$ engendré par ζ :

$$\mathrm{im}\, \gamma_\zeta = < \zeta > = \{\zeta^k \in \mathbb{C}^* \,|\, k \in \mathbb{Z}\} \leq \mathbb{C}^*$$

Quel est le noyau de γ_ζ ?

$$\ker \gamma_\zeta = \{k \in \mathbb{Z} \,|\, \zeta^k = 1\} \subset \mathbb{Z}$$

Donc, pour $k \in \mathbb{Z}$,

$$k \in \ker \gamma_\zeta \Longleftrightarrow 1 = \exp(2\pi i/n)^k = \exp(2\pi i k/n) \Longleftrightarrow k/n \in \mathbb{Z}$$

(On rappelle que $\exp(z) = 1$ si et seulement si z est un multiple entier de $2\pi i$.) Donc, le noyau de γ_ζ consiste en les multiples entiers de n. Autrement dit,

$$\ker \gamma_\zeta = n\mathbb{Z}$$

On a donc

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \{\zeta^k \in \mathbb{C}^* \,|\, k \in \mathbb{Z}\}$$

via γ_ζ. On peut appeler ceci la *représentation sous forme circulaire* du groupe $\mathbb{Z}/n\mathbb{Z}$.

4. On fixe $n \in \mathbb{N}^*$, et on considère le groupe symétrique $\mathfrak{S}_n$. On a $\mathfrak{A}_n := \ker(\mathrm{sgn})$, donc

$$\mathfrak{A}_n = \{\sigma \in \mathfrak{S}_n \,|\, \mathrm{sgn}(\sigma) = 1\}$$

Si $n \geq 2$, alors sgn est un épimorphisme et par le Théorème d'homomorphie, sgn induit

$$\mathfrak{S}_n/\mathfrak{A}_n \xrightarrow{\sim} \{\pm 1\} \quad \text{pour } n \geq 2$$

On particulier, on retrouve $|\,\mathfrak{S}_n : \mathfrak{A}_n\,| = 2$ et $|\mathfrak{A}_n| = \frac{n!}{2}$.

Thème 8.5. 1. On fixe $n \in \mathbb{N}^*$. On se propose de définir le groupe $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$: en tant qu'ensemble,

$$(\mathbb{Z}/n\mathbb{Z})^\times := \{\overline{x} \in \mathbb{Z}/n\mathbb{Z} \,|\, \exists\, \overline{y} \in \mathbb{Z}/n\mathbb{Z},\ \overline{xy} = \overline{1}\} \subset \mathbb{Z}/n\mathbb{Z}$$

Avec un peu d'arithmétique, on a vu en TD que

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{x} \in \mathbb{Z}/n\mathbb{Z} \mid \ pgcd(x,n) = 1\} \subset \mathbb{Z}/n\mathbb{Z}$$

On montre par exemple avec l'identité de Bezout que $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$ est un groupe, où $\cdot$ est la multiplication

$$\begin{array}{rccc} \cdot : & (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^\times \\ & (\overline{x}, \overline{y}) & \longmapsto & \overline{xy} \end{array}$$

On a donc défini ainsi un groupe fini contenu dans $\mathbb{Z}/n\mathbb{Z}$, sans pour autant être un sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$.

2. Prenons $n = 5$. Alors,

$$(\mathbb{Z}/5\mathbb{Z})^\times = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$$

On considère l'élément $\overline{2}$ de $(\mathbb{Z}/5\mathbb{Z})^\times$. On a

$$\overline{2}^2 = \overline{4}\ ,\ \overline{2}^3 = \overline{8} = \overline{3}\ ,\ \overline{2}^4 = \overline{16} = \overline{1}$$

Donc, $o(\overline{2}) = 4$, et $\overline{2}$ est un générateur de $(\mathbb{Z}/5\mathbb{Z})^*$. On a donc

$$\mathbb{Z}/4\mathbb{Z} \cong (\mathbb{Z}/5\mathbb{Z})^*$$

3. D'après la théorie des corps (l'an prochain...), $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique pour tout nombre *premier* p. Ce n'est pas le cas pour tout entier : regardons pour $n = 8$. On a

$$(\mathbb{Z}/8\mathbb{Z})^\times = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$$

On a

$$\overline{3}^2 = \overline{9} = \overline{1}\ ,\ \overline{5}^2 = \overline{25} = \overline{1}\ ,\ \overline{7}^2 = \overline{49} = \overline{1}$$

Donc, aucun élément de $(\mathbb{Z}/8\mathbb{Z})^\times$ n'est d'ordre $|\,(\mathbb{Z}/8\mathbb{Z})^\times\,| = 4$. On peut en conclure que le groupe $(\mathbb{Z}/8\mathbb{Z})^\times$ n'est pas cyclique et qu'il est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

4. (indicatrice d'Euler et petit théorème de Fermat)

Définition 8.6. *L'indicatrice d'Euler* (L. Euler, 1707–1783) est l'application

$$\begin{array}{rccc} \varphi : & \mathbb{N}^* & \longrightarrow & \mathbb{N} \\ & n & \longmapsto & |\,(\mathbb{Z}/n\mathbb{Z})^\times\,| \end{array}$$

On a vu que, $\varphi(p) = p - 1$ pour tout nombre premier p.

Proposition 8.7. *Soit $n \in \mathbb{N}^*$, $x \in \mathbb{Z}$ tel que $pgcd(x,n) = 1$.*
Alors, $x^{\varphi(n)}$ est congru à 1 modulo n.

Démonstration. Il faut montrer que $o(\overline{x})$, l'ordre de $\overline{x}$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$, divise $\varphi(n)$, une conséquence directe du théorème de Lagrange. **C.Q.F.D.**

Corollaire 8.8 (Petit Théorème de Fermat)**.** (P. de Fermat, 1601–1665) *Soit p un nombre premier. Alors x^p est congru à x modulo p pour tout $x \in \mathbb{Z}$.*

Démonstration. Si p ne divise pas x, on sait d'après la Proposition 8.7 que $\overline{x}^{p-1} = \overline{1}$ et ainsi $\overline{x}^p = \overline{x}$. Si p divise x, $\overline{x}$ et $\overline{x}^p$ sont tous les deux nuls modulo p. **C.Q.F.D.**

Remarque 8.9. Le Petit Théorème de Fermat est employé dans les tests de primalité : pour savoir si un (grand) nombre entier n peut être premier, on voit si

$$\forall\ 1 \leq x \leq n\ ,\ n \,|\, x^n - x$$

Exemple : $n = 6$ et $x = 2$. En fait, $2^6 - 2 = 64 - 2 = 62$ n'est pas divisible par 6. Donc, 6 n'est pas premier.

Théorème 8.10 (Théorème de Wilson)**.** *Un entier $n > 1$ est premier si et seulement si $(n-1)! \equiv -1[n]$.*

Proof. Si n n'est pas premier, alors en notant d un diviseur non trivial on a que d divise $(n-1)!$, donc d ne divise pas $(n-1)! + 1$ (les deux sont premiers entre eux) et n ne le divise pas non plus.

Réciproquement toutes les classes non-nulles de $\mathbb{Z}/p\mathbb{Z}$ sont inversibles. Les seules classes qui sont leur propre inverse étant -1 et 1 (solutions du polynôme $X^2 - 1 = 0$) on obtient en regroupant par paquets d'inverses mutuels que dans le produit $(p-1)!$ modulo p, il ne reste que -1. **C.Q.F.D.**

Théorème 8.11 (Deuxième théorème d'isomorphisme)**.** *Soient G un groupe, $K \trianglelefteq G$, $H \leq G$. Alors*

(a) $HK = KH \leq G$, et $K \trianglelefteq HK$.

(b) $H \cap K \trianglelefteq H$.

(c) $H/(H \cap K) \cong HK/K$.

Démonstration. (a) Pour tout $h \in H$, on a $hK = Kh$ d'après la Proposition 7.6 (b). L'équation $HK = KH$ en résulte. Pour voir que $HK \leq G$, on applique la Proposition 3.8. $K \trianglelefteq G$ et $K \leq HK$, donc $K \trianglelefteq HK$.

(b) Soient $k \in K$ et $h \in H$. Alors, $hkh^{-1} \in K$ car $K \trianglelefteq G$. Si en plus $k \in H \cap K$, alors $hkh^{-1} \in H$.

(c) On considère la composition

$$\alpha : H \hookrightarrow HK \twoheadrightarrow HK/K$$

de l'inclusion du sous-groupe H dans HK, et de l'épimorphisme canonique de HK vers HK/K. Concrètement, ce morphisme envoie h vers la classe de h modulo K. Clairement α est surjectif : tout élément de la cible est de la forme hkK, pour $h \in H$ et $k \in K$. Mais

$$\alpha(h) = hK = hkK$$

(Proposition 6.3 (b)). Déterminons $\ker \alpha$: soit $h \in H$. Alors

$$h \in \ker \alpha \iff hK = eK \in HK/K \iff h \in K$$

Ainsi $\ker \alpha = H \cap K$, et on applique le Théorème d'homomorphie.

C.Q.F.D.

Remarque 8.12. en considérant dans le deuxième théorème d'isomorphisme le cas où H et K sont tous les deux finis, on obtient alors

$$|\, HK \,| = \frac{|\, H \,| \cdot |\, K \,|}{|\, H \cap K \,|}$$

(on peut aussi le montrer de manière élémentaire)

Théorème 8.13 (Troisième théorème d'isomorphisme)**.** *Soient G un groupe, $K \leq H$ deux sous-groupes distingués de G. (D'après ce qui précède, on peut considérer H/K comme un sous-groupe distingué de G/K.) Alors*

$$(G/K)/(H/K) \cong G/H$$

Démonstration. Le noyau de l'épimorphisme canonique $G \to G/H$ est égal à H, et contient donc K. On applique la propriété universelle pour obtenir

$$\alpha : G/K \longrightarrow G/H$$

Concrètement, ce morphisme envoie la classe de g modulo K vers la classe de g modulo H. On voit donc que α est surjectif. Déterminons $\ker \alpha$. Soit $\pi : G \to G/K$ l'épimorphisme canonique. Pour $g \in G$,

$$gK \in \ker \alpha \iff gH = eH \in G/H \iff g \in H$$

Ceci montre que $\ker \alpha = \pi(H) \overset{8.3}{=} H/K$. α est donc un épimorphisme

$$G/K \to G/H,$$

de noyau H/K. On applique le Théorème d'homomorphie. **C.Q.F.D.**

9 Produit direct, lemme Chinois

On a vu précédemment la notion suivante.

Définition 9.1. Soient G et H deux groupes. Leur *produit direct* est défini comme étant le produit cartésien $G \times H$, muni de la loi de composition

$$(G \times H) \times (G \times H) \longrightarrow G \times H \quad , \quad ((g_1, h_1), (g_2, h_2)) \longmapsto (g_1 g_2, h_1 h_2)$$

Soit $(G_\alpha)_\alpha$ une famille de groupes. On définit le produit direct $\prod_\alpha G_\alpha$ en imitant la Définition 9.1. L'ordre dans lequel cette itération est effectuée n'importe pas. Exemple : on écrit $\mathbb{Z}^r$ pour le produit direct de r facteurs $\mathbb{Z}$. Donc,

$$\mathbb{Z}^r = \{(z_1, \ldots, z_r) \,|\, z_i \in \mathbb{Z}, i = 1, \ldots, r\}$$

Exemples 9.2. (a) Le produit direct $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est un groupe Abélien d'ordre 4. Il n'est pas cyclique car

$$\forall\, (x, y) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\ ,\ 2(x, y) = (x, y) + (x, y) = (2x, 2y) = (0, 0)$$

Donc, il n'y pas d'élément d'ordre 4 dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(b) Le produit direct $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ est un groupe Abélien d'ordre 6. Il est cyclique : en fait, $z_0 := (\overline{1}, \overline{1}) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ est d'ordre 6 car

$$2z_0 = (\overline{0}, \overline{2})\ ,\ 3z_0 = (\overline{1}, \overline{0})\ ,\ 4z_0 = (\overline{0}, \overline{1})\ ,\ 5z_0 = (\overline{1}, \overline{2})\ ,\ 6z_0 = (\overline{0}, \overline{0})$$

Théorème 9.3 (Lemme Chinois)**.** *Soient $m, n \in \mathbb{N}_{\geq 1}$, $pgcd(m, n) = 1$. Alors,*

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

Le groupe $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est donc cyclique dans cette situation.

Démonstration.

Preuve 1: On a en général que si G, G' sont deux groupes et g, g' sont d'ordre fini dans G et G', respectivement, alors l'élément (g, g') du groupe produit $G \times G'$ est d'ordre $n = ppcm(o(g), o(g'))$. En effet on a clairement $(g, g')^n = (e_G, e_{G'})$, et si k est un entier non nul tel que

$$(g, g')^k = (g^k, g'^k) = (e_G, e_{G'}),$$

alors $o(g)$ et $o(g')$ divisent tous deux l'ordre de (g, g'). L'élément $(\overline{1}, \overline{1})$ est donc d'ordre mn et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est cyclique.

Preuve 1' : On considère le morphisme

$$\gamma_{z_0} : \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

associé à $z_0 := (\overline{1}, \overline{1}) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ (Exemple 8.4, 1.). Donc,

$$\forall\, i \in \mathbb{Z}\ ,\ \gamma_{z_0}(i) = (\bar{i}, \bar{i})$$

Déterminons le noyau de γ_{z_0} : soit $i \in \mathbb{Z}$.

$$i \in \ker \gamma_{z_0} \Longleftrightarrow (\bar{i}, \bar{i}) = (\overline{0}, \overline{0}) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \Longleftrightarrow m \,|\, i \text{ et } n \,|\, i$$

Cette dernière condition équivaut à $mn \,|\, i$ car $pgcd(m, n) = 1$. Donc, $\ker \gamma_{z_0} = mn\mathbb{Z}$. Le Théorème d'homomorphie dit alors que

$$\mathbb{Z}/mn\mathbb{Z} \cong \operatorname{im} \gamma_{z_0}$$

En particulier, $\operatorname{im} \gamma_{z_0}$ a le même ordre que $\mathbb{Z}/mn\mathbb{Z}$, à savoir mn. Mais $\operatorname{im} \gamma_{z_0} \leq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, et l'ordre de ce dernier groupe est égal à mn. On en conclut que $\operatorname{im} \gamma_{z_0} = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. **C.Q.F.D.**

Comme le montre l'Exemple 9.2 (b) précédent, l'hypothèse sur $pgcd(m, n)$ est indispensable.

Corollaire 9.4. *Soient $a, b, m, n \in \mathbb{Z}$, $m, n \geq 1$, $pgcd(m, n) = 1$. Alors, il existe $x \in \mathbb{Z}$ tel que*

$$x \equiv a \mod m\ ,\ x \equiv b \mod n$$

Démonstration. Le morphisme

$$\gamma_{z_0} : \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

de 9.3 est surjectif. **C.Q.F.D.**

Corollaire 9.5. *Soit $n \in \mathbb{N}_{\geq 1}$, $n = \prod_{p \,|\, n} p^{\alpha_p}$ sa factorisation en puissances de nombres premiers différents ($\alpha_p > 0$). Alors,*

$$\mathbb{Z}/n\mathbb{Z} \cong \prod_{p \,|\, n} \mathbb{Z}/p^{\alpha_p}\mathbb{Z}$$

Démonstration. Récurrence sur le nombre de p, en appliquant le Lemme Chinois. **C.Q.F.D.**

Théorème 9.6. *Soient $m, n \in \mathbb{N}_{\geq 1}$, $pgcd(m, n) = 1$. Alors,*

$$(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$$

En particulier, $\varphi(mn) = \varphi(m)\varphi(n)$ si $pgcd(m, n) = 1$.

Démonstration. On considère la bijection

$$\gamma : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}\ ,\ \bar{i} \longmapsto (\bar{i}, \bar{i})$$

du Lemme Chinois. Les sous-ensembles $(\ \bullet\ )^\times$ de $\mathbb{Z}/mn\mathbb{Z}$, $\mathbb{Z}/m\mathbb{Z}$, et $\mathbb{Z}/n\mathbb{Z}$ sont caractérisés par les conditions $pgcd(x, mn) = 1$, $pgcd(x, m) = 1$, et $pgcd(x, n) = 1$, respectivement. Ceci montre que pour tout $\bar{i} \in \mathbb{Z}/mn\mathbb{Z}$,

$$\bar{i} \in (\mathbb{Z}/mn\mathbb{Z})^\times \Longleftrightarrow \gamma(\bar{i}) \in (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$$

Donc, γ induit une bijection

$$\gamma : (\mathbb{Z}/mn\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$$

Elle respecte les lois de multiplication puisqu'elle envoie $\overline{i}$ vers $(\overline{i}, \overline{i})$. Donc, c'est un isomorphisme. **C.Q.F.D.**

Corollaire 9.7. *Soit $n \in \mathbb{N}_{\geq 1}$, $n = \prod_{p\,|\,n} p^{\alpha_p}$ sa factorisation en puissances de nombres premiers différents. Alors,*

$$\varphi(n) = \prod_{p\,|\,n} (p-1)p^{\alpha_p - 1} = n \prod_{p\,|\,n} \frac{p-1}{p}$$

Démonstration. Il suffit de montrer l'énoncé pour $n = p^\alpha$, pour un nombre premier p et $\alpha > 0$ (le Théorème 9.6 permet alors de raisonner par récurrence sur le nombre de p). On a

$$\mathbb{Z}/p^\alpha\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{p^\alpha - 1}\}$$

La condition $pgcd(x, p^\alpha) = 1$ équivaut à $p \not| x$, ce qui exclut $1/p$ des éléments de $\mathbb{Z}/p^\alpha\mathbb{Z}$. **C.Q.F.D.**

10 Groupes abéliens

Soient à nouveau G et H deux groupes, avec éléments neutres e_G et e_H. On définit des morphismes de groupes

$$i_G : G \longrightarrow G \times H \ , \ g \longmapsto (g, e_H)$$

$$i_H : H \longrightarrow G \times H \ , \ h \longmapsto (e_G, h)$$

$$p_G : G \times H \longrightarrow G \ , \ (g, h) \longmapsto g$$

$$p_H : G \times H \longrightarrow H \ , \ (g, h) \longmapsto h$$

Visiblement, i_G et i_H sont des monomorphismes, et p_G et p_H des épimorphismes. Via i_G et i_H, on peut identifier G et H à des sous-groupes de $G \times H$. Ce sont des sous-groupes distingués car $i_G(G) = \ker p_H$ et $i_H(H) = \ker p_G$. L'intersection de ces sous-groupes dans $G \times H$ est triviale ; leur produit $i_G(G)i_H(H)$ est égal à $G \times H$. Réciproquement :

Proposition 10.1. *Soit G un groupe, H et K deux sous-groupes distingués tels que $H \cap K = \{e\}$ et $G = HK$. Alors, l'application*

$$H \times K \longrightarrow G \ , \ (h, k) \longmapsto hk$$

est un isomorphisme de groupes.

Démonstration. Montrons d'abord que

$$\forall\, h \in H, k \in K\ ,\ hk = kh \in G$$

Comme H est distingué dans G, on a $khk^{-1} \in H$, donc $khk^{-1}h^{-1}$ est un élément de H. De même K est distingué donc $hk^{-1}h^{-1}$ est dans K et $khk^{-1}h^{-1} \in H \cap K$ est trivial, i.e. $hk = kh$.

Appelons α l'application de l'énoncé. On a pour tous couples (h_1, k_1), (h_2, k_2) de $H \times K$:

$$\alpha(h_1, k_1)\alpha(h_2, k_2) = h_1k_1h_2k_2 = h_1h_2k_1k_2 = \alpha(h_1h_2, k_1k_2),$$

et α est un morphisme, clairement surjectif car d'image $HK = G$. On a

$$(h, k) \in \ker\alpha \iff hk = e \iff h = k^{-1} \in H \cap K = \{e_G\},$$

Donc, α est injectif. **C.Q.F.D.**

Théorème 10.2. *Soit G un groupe Abélien, engendré par un nombre fini d'éléments. (On dit alors que G est un groupe Abélien* de type fini.*) Alors, G est isomorphe à un produit direct fini de groupes cycliques (finis ou infinis). Plus précisément :*

(a) Il existe $r \geq 0$, des nombres premiers p_i (non nécessairement différents), et des $\alpha_i \geq 1$ tels que

$$G \cong \mathbb{Z}^r \times \prod_i \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$$

r et les p_i et α_i sont uniquement déterminés par G.

(b) Si G est fini (donc, de type fini), alors $r = 0$ dans (a), c'est-à-dire il existe des nombres premiers p_i (non nécessairement différents), et des $\alpha_i \geq 1$ tels que

$$G \cong \prod_i \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$$

Ceci est appelé la *Classification des groupes Abéliens de type fini*. Pour la démonstration, il faut attendre l'an prochain. On observe que le Lemme Chinois permet de simplifier éventuellement les facteurs $\prod_i \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$.

Exemple 10.3. Soit G un groupe Abélien d'ordre p^2, où p est un nombre premier. D'après le Théorème 10.2, il n'y a que deux cas possibles : soit G est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$, soit il est isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. On en conclut notamment que si en plus G n'est pas cyclique, alors $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Prenons $G = (\mathbb{Z}/8\mathbb{Z})^*$, étudié à l'exemple 8.5. C'est un groupe abélien d'ordre est d'ordre 4, qui n'est pas cyclique. Il est donc isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Vous verrez en TD qu'en réalité, tous les groupes d'ordre p^2 sont abéliens (ce n'est plus le cas dès p^3).

Exercice 10.4. Construire un isomorphisme

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \xrightarrow{\sim} (\mathbb{Z}/8\mathbb{Z})^*$$

11 Produits semi-directs

Définition 11.1. [G, Déf. 3.1] Soit $(G, \cdot)$ un groupe, E un ensemble. Une *action* ou *opération (à gauche) de* $(G, \cdot)$ *sur* E est la donnée d'une application

$$\cdot : G \times E \longrightarrow E$$

tel que les axiomes suivants sont satisfaits :

(1) On a

$$g \cdot (h \cdot x) = (gh) \cdot x \ ; \ \forall \ g, h \in G, x \in E$$

(2) Si e est l'élément neutre de $(G, \cdot)$, alors

$$e \cdot x = x \ ; \ \forall \ x \in E$$

Définition 11.2. Soient G, $(H, *)$ deux groupes,

$$\cdot : G \times H \longrightarrow H$$

une action de G sur l'ensemble H. $\cdot$ est appelée une *action par des automorphismes de groupes* sur H si de plus

$$g \cdot (h_1 * h_2) = (g \cdot h_1) * (g \cdot h_2) \ \forall \ g \in G, h_1, h_2 \in H$$

Autrement dit, une action par des automorphismes de groupes sur H est une action, qui respecte la loi de composition interne de H. En fait :

Proposition 11.3. *Soit $\cdot : G \times H \to H$ une action de G par des automorphismes de groupes sur H.*
(a) Si e_H est l'élément neutre de H, alors

$$g \cdot e_H = e_H \ ; \ \forall \ g \in G$$

(b) Soit $h \in H$. Alors,

$$g \cdot h^{-1} = (g \cdot h)^{-1} \ ; \ \forall \ g \in G$$

Démonstration. (a) D'après la définition,

$$g \cdot e_H = (g \cdot e_H) * (g \cdot e_H)$$

Donc, $g \cdot e_H = e_H$.

(b) D'après la définition,

$$(g \cdot h) * (g \cdot h^{-1}) = (g \cdot e_H) \overset{(a)}{=} e_H$$

Donc, $g \cdot h^{-1} = (g \cdot h)^{-1}$. **C.Q.F.D.**

Exemples 11.4. (a) Soit G un groupe non-trivial. Alors, l'action par multiplication à gauche [G, Déf. 3.17] de G sur lui-même n'est pas une action de G par des automorphismes de groupes, car elle ne respecte pas l'élément neutre.

(b) Soit G un groupe. Alors, l'action par conjugaison [G, Ex. 3.15] de G sur lui-même est une action de G par des automorphismes de groupes : en effet,

$$g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) \ \forall \ g, x, y \in G$$

(c) Plus généralement, soient K un groupe, G et H deux sous-groupes. On suppose que $H \trianglelefteq K$. Alors, G agit sur H par conjugaison :

$$\cdot : G \times H \longrightarrow H \ , \ (g, h) \longmapsto ghg^{-1}$$

C'est une action de G par des automorphismes de groupes.

(d) Pour tous groupes (G, H), il y a l'action *triviale* de G sur H :

$$g \cdot h := h \ ; \ \forall \ g \in G, h \in H$$

C'est une action de G par des automorphismes de groupes.

Définition 11.5. Soient G, H deux groupes,

$$\cdot : G \times H \longrightarrow H$$

une action par des automorphismes de groupes sur H. On définit le *produit semi-direct externe par rapport à l'action* $\cdot$ comme étant le produit cartésien $H \times G$, muni de la loi de composition

$$(H \times G) \times (H \times G) \longrightarrow H \times G \ , \ ((h_1, g_1), (h_2, g_2)) \longmapsto (h_1(g_1 \cdot h_2), g_1 g_2)$$

On note $H \rtimes_{\cdot} G$ le produit semi-direct par rapport à $\cdot$.

Quand il n'y a pas d'ambiguïté quant à l'action $\cdot$, on écrit parfois $H \rtimes G$ au lieu de $H \rtimes_{\cdot} G$. Certaines sources vont alors (par abus de langage) jusqu'à appeler cet objet *le* produit semi-direct.

Exemple 11.6. Si $\cdot$ est l'action triviale (Exemple 11.4 (d))

$$g \cdot h = h \ ; \ \forall \ g \in G, h \in H$$

alors $H \rtimes_{\cdot} G = H \times G$, le produit direct étudié dans le chapitre 9.

Proposition 11.7. *Soient G, H deux groupes, avec éléments neutres e_G et e_H,*

$$\cdot : G \times H \longrightarrow H$$

une action par des automorphismes de groupes.

(a) Le produit semi-direct $H \rtimes_\cdot G$ est un groupe. Son élément neutre est (e_H, e_G). L'inverse de $(h, g) \in H \rtimes_\cdot G$ est donné par $(g^{-1} \cdot h^{-1}, g^{-1})$.

(b) L'application

$$i_G : G \longrightarrow H \rtimes_\cdot G \ , \ g \longmapsto (e_H, g)$$

est un monomorphisme.

(c) L'application

$$i_H : H \longrightarrow H \rtimes_\cdot G \ , \ h \longmapsto (h, e_G)$$

est un monomorphisme. Son image $i_H(H)$ est un sous-groupe distingué de $H \rtimes_\cdot G$.

(d) L'intersection de $i_H(H)$ et de $i_G(G)$ dans $H \rtimes_\cdot G$ est triviale ; leur produit $i_H(H)i_G(G)$ est égal à $H \rtimes_\cdot G$.

(e) L'application

$$p_G : H \rtimes_\cdot G \longrightarrow G \ , \ (h, g) \longmapsto g$$

est un épimorphisme. Son noyau est égal à $i_H(H)$.

Démonstration. (a) Soient $h_1, h_2, h_3 \in H$ et $g_1, g_2, g_3 \in G$. Alors, $((h_1, g_1)(h_2, g_2))(h_3, g_3)$ est égal à

$$(h_1(g_1 \cdot h_2), g_1 g_2)(h_3, g_3) = (h_1(g_1 \cdot h_2)(g_1 g_2 \cdot h_3), g_1 g_2 g_3)$$

alors que $(h_1, g_1)((h_2, g_2)(h_3, g_3))$ est égal à

$$(h_1, g_1)(h_2(g_2 \cdot h_3), g_2 g_3) = (h_1(g_1 \cdot (h_2(g_2 \cdot h_3))), g_1 g_2 g_3)$$

Mais

$$(g_1 \cdot h_2)(g_1 g_2 \cdot h_3) = g_1 \cdot (h_2(g_2 \cdot h_3))$$

car $\cdot$ est une action par des automorphismes de groupes. Ceci montre la loi d'associativité.

On voit facilement que (e_H, e_G) est l'élément neutre de $H \rtimes_\cdot G$.

Soit $(h, g) \in H \rtimes_\cdot G$. Alors,

$$(g^{-1} \cdot h^{-1}, g^{-1})(h, g) = ((g^{-1} \cdot h^{-1})(g^{-1} \cdot h), e_G)$$

Mais

$$(g^{-1} \cdot h^{-1})(g^{-1} \cdot h) = g^{-1} \cdot (h^{-1} h) = g^{-1} \cdot e_H = e_H$$

car $\cdot$ est une action par des automorphismes de groupes, et grâce à la Proposition 11.3 (a).

(b) On a

$$\forall\, g_1, g_2 \in G\ ,\ (e_H, g_1)(e_H, g_2) = (e_H(g_1 \cdot e_H), g_1 g_2)$$

ce qui est égal à $(e_H, g_1 g_2)$ d'après la Proposition 11.3 (a). i_G est donc un homomorphisme de groupes, clairement injectif.

(c) On a

$$\forall\, h_1, h_2 \in H\ ,\ (h_1, e_G)(h_2, e_G) = (h_1(e_G \cdot h_2), e_G)$$

ce qui est égal à $(h_1 h_2, e_G)$ car $\cdot$ est une action. i_H est donc un homomorphisme de groupes. Il est injectif. D'après (e), $i_H(H)$ est le noyau d'un homomorphisme. Il est donc distingué dans $H \rtimes_\cdot G$.

(e) On a

$$\forall\, h_1, h_2 \in H, g_1, g_2 \in G\ ,\ (h_1, g_1)(h_2, g_2) = (h_1(g_1 \cdot h_2), g_1 g_2)$$

par définition. Donc, p_G est un homomorphisme de groupes $H \rtimes_\cdot G \to G$. Il est surjectif. Son noyau est égal à

$$\{(h, g) \,|\, g = e_G\} = \mathrm{im}(i_H)$$

(d) La composition $p_G \circ i_G$ étant l'identité de G, on voit que l'image de i_G a une intersection triviale avec $\ker(p_G) = i_H(H)$ (d'après (e)). Soit $(h, g) \in H \rtimes_\cdot G$. Alors,

$$(h, g) = (h, e_G)(e_H, g)$$

donc $(h, g) \in i_H(H) i_G(G)$. **C.Q.F.D.**

On a vu plus haut comment construire le produit semi-direct externe de deux groupes G et H (relativement à une action). On montre désormais un cas particulier important : montrer qu'un groupe G est le produit semi-direct de deux de ses sous-groupes H et K, relativement à une action par conjugaison. On dit dans ce cas que G est le produit semi-direct interne de H et K.

Voici un cas particulier de 11.7; ceci est une généralisation de la Proposition 10.1 :

Proposition 11.8. *Soit G un groupe, H et K deux sous-groupes tels que $H \cap K = \{e\}$ et $G = HK$. On suppose que $H \trianglelefteq G$. On considère l'action*

$$\cdot : K \times H \longrightarrow H\ ,\ (k, h) \longmapsto khk^{-1}$$

de l'Exemple 11.4 (c). Alors, l'application

$$H \rtimes_\cdot K \longrightarrow G\ ,\ (h, k) \longmapsto hk$$

est un isomorphisme de groupes.

Démonstration. Appelons α l'application de l'énoncé. On a pour tout $(h_1, k_1), (h_2, k_2) \in H \rtimes. K$:

$$\alpha(h_1, k_1)\alpha(h_2, k_2) = h_1k_1h_2k_2 = h_1(k_1h_2k_1^{-1})k_1k_2 = h_1(k_1 \cdot h_2)k_1k_2$$

Donc, $\alpha(h_1, k_1)\alpha(h_2, k_2)$ est égal à

$$\alpha(h_1(k_1 \cdot h_2), k_1k_2) = \alpha((h_1, k_1)(h_2, k_2))$$

On a montré que α est un homomorphisme. Il est surjectif car son image est $HK = G$. On a

$$(h, k) \in \ker \alpha \iff hk = e \iff k = h^{-1} \in H \cap G = \{e\}$$

Donc, α est injectif. **C.Q.F.D.**

Soit G un groupe Abélien. On a l'action φ de $\mathbb{Z}/2\mathbb{Z}$ par des automorphismes de groupes sur G qui envoie $\overline{1}$ vers $x \mapsto -x$. (On note que $x \mapsto -x$ est un endomorphisme de G puisque G est Abélien !) On l'appelle *l'action par inversion* de $\mathbb{Z}/2\mathbb{Z}$.

Thème 11.9. 1. (le groupe $\mathfrak{S}_n$, VI) La proposition 11.8 s'applique sans peine au groupe symétrique : considérons le sous-groupe (distingué) $\mathfrak{A}_n$ de $\mathfrak{S}_n$ et $K = \{id, \tau\}$ le sous-groupe engendré par une transposition. Bien entendu $\mathfrak{A}_n \cap K = \{id\}$. En outre

$$|\,\mathfrak{A}_nK\,| = |\,\mathfrak{A}_n\,| \cdot |\,K\,| = n!,$$

et groupe $\mathfrak{S}_n$ s'écrit comme un produit semi-direct interne $\mathfrak{A}_n \rtimes \mathbb{Z}/2\mathbb{Z}$.

2. (le groupe diédral, V) On a vu que les groupes $\mathfrak{S}_3$ et D_3 sont isomorphes. La situation est différente pour D_n, $n \geq 4$ notamment car $\mathfrak{A}_n$ n'est plus cyclique dans ces cas.

   Comme vu en TD, la description que nous avons faite de D_3 avec les générateurs r (rotation) et s (symétrie) se généralise pour les polygones réguliers à n côtés. Notre groupe D_n est le groupe des isométries qui préservent un tel polygone, de cardinal $2n$ et engendré par r (d'ordre n) et s (d'ordre 2) avec la relation $srs = r^{-1}$. Ses éléments sont les suivants

   $$D_n = \{id, r, r^2, ..., r^{n-1}, \sigma, \sigma r^2, ..., \sigma r^{n-1}\}$$

   On a que $H =< r >$ est un sous groupe distingué de D_n. En posant $K = \{id, \sigma\}$ le sous-groupe engendré par la symétrie σ, on a évidemment $H \cap K = \{id\}$. En outre

   $$|\,HK\,| = |\,H\,| \cdot |\,K\,| = 2n,$$

   et D_n est isomorphe à un produit semi-direct interne $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

3. (groupes de petit cardinal) On a désormais en main les outils qui permettent de déterminer (à isomorphisme près) tous les groupes finis de petit cardinal.

Détails. *(groupes de petit cardinal. Cardinal premier* 1*,* 2*,* 3*,* 5*,* 7*,* 11*,* 13 *un seul groupe. Cardinal* p^2 *c'est commutatif il y a* $\mathbb{Z}/p2$ *et* $\mathbb{Z}/p \times \mathbb{Z}/p$ *pour* 4*,* 9*.*

Cardinal 6 *: abélien = cyclique et une seule autre possibilité (=*$D_3 = \mathfrak{S}_3$*).*

Cardinal 8 *: on a* D_4 *et les quaternions* $\mathbb{H}_8$*, qui sont non-isomorphes (par ex groupes distingués différents) et sont les seuls non abéliens.*

Cardinal 10 *: commutatif = cyclique et sinon uniquement* D_5*.*

Cardinal 12 *: abélien on a* $\mathbb{Z}/12$*,* $\mathbb{Z}/6 \times \mathbb{Z}/2$*,* $\mathbb{Z}/3 \times \mathbb{Z}/2 \times \mathbb{Z}/2$*. En non commutatif on a* D_6*,* $\mathfrak{A}_4$*, et un produit semi-direct* $\mathbb{Z}/3 \rtimes \mathbb{Z}/4$*.*

12 Anneaux : propriétés de base

Définition 12.1. Soit A un ensemble,

$$+ : A \times A \longrightarrow A$$

et

$$\cdot : A \times A \longrightarrow A$$

deux lois de composition internes. On dit que le triplet $(A, +, \cdot)$ est un *anneau (unitaire)* si les axiomes suivants sont satisfaits :

(1) La paire $(A, +)$ est un groupe Abélien.

(2) La paire $(A, \cdot)$ satisfait la loi d'associativité :

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \; \forall \; a, b, c \in A$$

(3) Il existe un élément $1 \in A$ tel qu'on ait

$$1 \cdot a = a = a \cdot 1 \; \forall \; a \in A$$

(4) On a

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

et

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \; \forall \; a, b, c \in A$$

L'axiome 12.1 (4) s'appelle la *loi de distributivité*. Un élément 1 comme dans l'axiome 12.1 (3) est appelé *élément neutre pour la multiplication*. On note 0 l'élément neutre pour l'addition $+$. Pour alléger la notation, on va se permettre de supprimer le symbole $\cdot$ quand il n'y a pas d'ambiguïté :

$$ab \quad \text{au lieu de} \quad a \cdot b$$

Aussi, on parlera simplement de "l'anneau A" au lieu de "l'anneau $(A, +, \cdot)$".

Exemples 12.2. (a) Rappelons qu'on note $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ les ensembles des nombres entiers, rationnels, et réels, respectivement. Munis des lois d'addition et de multiplication que tout le monde connaît, ces objets sont des anneaux.
(b) Rappelons qu'on note $\mathbb{N}$ l'ensemble des nombres naturels. On peut le munir des lois d'addition et de multiplication que tout le monde connaît. Mais $(\mathbb{N}, +, \cdot)$ n'est pas un anneau puisque $(\mathbb{N}, +)$ n'est pas un groupe.

Définition 12.3. Soit A un anneau. On dit que A est *commutatif*, si

$$ab = ba \; \forall \; a, b \in A$$

Donc, tous les anneaux qu'on a considérés dans l'Exemple 12.2 (a) sont commutatifs. Mais il existe des anneaux qui ne sont pas commutatifs.

Exemple 12.4. L'anneau $(M_2(\mathbb{R}), +, \cdot)$.
On rappelle que

$$M_2(\mathbb{R}) := \Big\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \Big\}$$

admet deux lois internes de composition, l'addition et la multiplication des matrices. $(M_2(\mathbb{R}), +)$ est un groupe Abélien, $(M_2(\mathbb{R}), \cdot)$ satisfait la loi d'associativité, et l'élément neutre pour la multiplication est donné par la matrice

$$I := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

En plus, la loi de distributivité est également satisfaite. Donc, $(M_2(\mathbb{R}), +, \cdot)$ est un anneau. Il n'est pas commutatif (exemple ?). On définit trois matrices

$$A := \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \; , \; X := \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \; ,$$

et $Y := I$. Alors,

$$AX = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = A = AY$$

On voit donc : $AX = AY$, mais $X \neq Y$. L'analogue de la Proposition **??** pour les anneaux est donc faux en général. (Voir la Proposition 12.8...)

Proposition 12.5. *Soit $(A, +, \cdot)$ un anneau.*
(a) Il n'y a qu'un seul élément neutre pour la multiplication.
(b) Soient $a, b \in A$. Alors,

$$a \cdot 0 = 0 = 0 \cdot a \; , \; a(-b) = -ab = (-a)b$$

En particulier, $a(-1) = -a = (-1)a$.

Démonstration. (a) Supposons que $e \in A$, et que

$$ea = a = ae \; \forall \; a \in A$$

On a alors $e = 1 \cdot e = 1$.

(b) $a0 + a = a0 + a1 = a(0 + 1) = a$ grâce à la loi de distributivité, donc $a0 = 0$ d'après la Proposition **??** ($(A, +)$ est un groupe !). Pareil pour $0a$. $a(-b) + ab = a(-b + b) = a0 = 0$ toujours grâce à la loi de distributivité, donc $a(-b) = -ab$. Pareil pour $(-a)b$. **C.Q.F.D.**

Définition 12.6. Soit A un anneau.

(a) On dit que A est *intègre* si $1 \neq 0$, et si

$$ab \neq 0 \; \forall \; a, b \in A - \{0\}$$

(b) On dit que A est un *corps* si $1 \neq 0$, et si

$$\forall \; a \in A - \{0\} \; \exists \; b \in A \; , \; ab = 1$$

Dans la situation de 12.6 (b), si $ab = 1$, alors $ba = 1$: en fait, $b \neq 0$ car $a0 = 0 \neq 1$. Puisque A est un corps, on trouve alors $c \in A$ avec $bc = 1$. Alors,

$$c = 1c = (ab)c = a(bc) = a1 = a$$

Donc : dans un corps A, il n'y a pas de différence entre inverse à gauche et inverse à droite. On parle donc simplement de l'inverse d'un élément ; l'inverse de $a \in A - \{0\}$ est noté a^{-1}.

Proposition 12.7. *Tout corps est intègre.*

Démonstration. Soit A un corps, $a, b \in A$ tels que $ab = 0$. Si $b \neq 0$,

$$0 = 0b^{-1} = abb^{-1} = a1 = a$$

Si $a \neq 0$,

$$0 = a^{-1}0 = a^{-1}ab = 1b = b$$

C.Q.F.D.

Proposition 12.8. *Soit A un anneau intègre, $a, x, y \in A$, $a \neq 0$.*

(a) La relation $ax = ay$ implique $x = y$.

(b) La relation $xa = ya$ implique $x = y$.

Démonstration. $ax = ay$ implique $a(x - y) = 0$. Puisque A est intègre, et $a \neq 0$, on conclut que $x - y = 0$. Pareil pour $xa = ya$. **C.Q.F.D.**

Donc : l'analogue de la Proposition **??** est vrai pour les anneaux intègres.

Exemples 12.9. (a) $\mathbb{Z}$, $\mathbb{Q}$, et $\mathbb{R}$ sont des anneaux (commutatifs) intègres. $\mathbb{Q}$ et $\mathbb{R}$ sont même des corps (commutatifs).

(b) $M_2(\mathbb{R})$ n'est pas intègre car d'après l'Exemple 12.4, la conclusion de la Proposition 12.8 ne vaut pas dans $M_2(\mathbb{R})$.

Corollaire 12.10. *Soit A un anneau avec $1 \neq 0$.*

(a) Les énoncés suivants sont équivalents :

(1) A est intègre.

(2) Pour tout $a \in A - \{0\}$, l'application

$$m_a : A \longrightarrow A \ , \ x \longrightarrow ax$$

est injective.

(b) Les énoncés suivants sont équivalents :

(1) A est un corps.

(2) Pour tout $a \in A - \{0\}$, l'application

$$m_a : A \longrightarrow A \ , \ x \longrightarrow ax$$

est surjective.

(3) Pour tout $a \in A - \{0\}$, l'application

$$m_a : A \longrightarrow A \ , \ x \longrightarrow ax$$

est bijective.

Démonstration. (a) (2) $\Rightarrow$ (1) : $a \in A - \{0\}$. m_a étant injectif, 0 est le seul antécédent de 0 sous m_a. Donc, $b \neq 0$ implique $ab \neq 0$. A est donc intègre.

(1) $\Rightarrow$ (2) : Supposons A intègre. Soient $a \in A - \{0\}$, $x, y \in A$ tel que

$$ax = m_a(x) = m_a(y) = ay$$

D'après la Proposition 12.8 (a), $x = y$. m_a est donc injectif.

(b) (2) $\Rightarrow$ (1) : $a \in A - \{0\}$. m_a étant surjectif, 1 admet un antécédent b sous m_a. Donc, $1 = m_a(b) = ab$.

(3) $\Rightarrow$ (2) : C'est évident.

(1) $\Rightarrow$ (3) : $a \in A - \{0\}$. D'après la Proposition 12.7, A est intègre. Donc, m_a est injectif d'après (a). Soit $b \in A$. Alors, $c := a^{-1}b$ satisfait

$$m_a(c) = ac = aa^{-1}b = b$$

C.Q.F.D.

Théorème 12.11. *Soit A un anneau intègre, $\#A < \infty$. Alors, A est un corps.*

Démonstration. Soit $a \in A - \{0\}$. D'après le Corollaire 12.10 (a),

$$m_a : A \longrightarrow A \ , \ x \longmapsto ax$$

est injectif. A étant un ensemble fini, m_a est donc bijectif. D'après le Corollaire 12.10 (b), A est un corps. **C.Q.F.D.**

Définition 12.12. Soit A un anneau.
(a) Un élément $a \in A$ est appelé *inversible* s'il existe $b \in A$ avec $ab = 1 = ba$.
(b) L'ensemble des éléments inversibles de A est noté A^*.

Exemple 12.13. Pour $A = \mathbb{Z}$, quels sont les éléments inversibles ? On en voit tout de suite deux : 1 et -1 (qui sont en plus leurs propres inverses). Soit $n \in \mathbb{Z}$, et supposons qu'il existe $m \in \mathbb{Z}$ tel que $mn = 1$. Alors, $n \neq 0$ et $m \neq 0$. Si $|\, n \,| > 1$, alors

$$|\, mn \,| \;=\; |\, m \,|\, |\, n \,| > 1$$

contrairement à notre hypothèse. Donc, $|\, n \,| = 1$. On en conclut que $\mathbb{Z}^* = \{1, -1\}$.

Proposition 12.14. *Soit A un anneau. Alors, $(A^*, \cdot)$ est un groupe.*

Démonstration. Clairement $1 \in A^*$. Soient $a, a' \in A^*$. On trouve donc $b, b' \in A$ avec

$$ab = ba = a'b' = b'a' = 1$$

Alors

$$(aa')(b'b) = a(a'b')b = ab = 1 = b'a' = b'(ba)a' = (b'b)(aa')$$

Donc, aa' admet $b'b$ comme inverse, et appartient donc à A^*. En plus, $b \in A^*$ car $ba = 1 = ab$. La loi d'associativité est satisfaite dans A^* puisqu'elle l'est dans A. **C.Q.F.D.**

Exemple 12.15. Pour $A = M_2(\mathbb{R})$, on trouve $A^* = GL_2(\mathbb{R})$.

Proposition 12.16. *Soit A un anneau. Les énoncés suivants sont équivalents :*

(1) A est un corps.

(2) $A^* = A - \{0\}$.

Démonstration. Notons d'abord que les deux hypothèses (1) et (2) impliquent que $1 \neq 0$. On applique alors la définition d'un corps. **C.Q.F.D.**

Définition 12.17. Soient A un anneau, X une indéterminée. On définit

$$A[X] := \{\sum_{n=0}^{N} a_n X^n \,|\, N \in \mathbb{N}\ ,\ a_n \in A\}$$

On définit l'addition et la multiplication

$$+ : A[X] \times A[X] \longrightarrow A[X]$$

et

$$\cdot : A[X] \times A[X] \longrightarrow A[X]$$

par les règles

$$\sum_n a_n X^n + \sum_n b_n X^n := \sum_n (a_n + b_n) X^n$$

et

$$\big(\sum_n a_n X^n\big) \cdot \big(\sum_n b_n X^n\big) := \sum_n c_n X^n$$

avec $c_n := \sum_{k+l=n} a_k b_l$. Le triplet $(A[X], +, \cdot)$ est appelé *l'anneau des polynômes en une variable* sur A.

Proposition 12.18. *Soient A un anneau, X une indéterminée. Alors, $(A[X], +, \cdot)$ est un anneau.*

Démonstration. Puisque l'addition des polynômes se fait "composante par composante", on voit facilement que $(A[X], +)$ est un groupe Abélien. Le polynôme constant $1 = 1X^0$ est l'élément neutre pour la multiplication.

Il reste à vérifier la loi d'associativité pour la multiplication, et les lois de distributivité.

Soient alors $\sum_n a_n X^n$, $\sum_n b_n X^n$ et $\sum_n c_n X^n \in A[X]$. On a

$$\big(\sum_n a_n X^n\big)\big(\sum_n b_n X^n\big) = \sum_n \big(\sum_{k+l=n} a_k b_l\big) X^n$$

et donc,

$$\big(\big(\sum_n a_n X^n\big)\big(\sum_n b_n X^n\big)\big)\big(\sum_n c_n X^n\big) = \sum_n \big(\sum_{k+l+m=n} a_k b_l c_m\big) X^n$$

Le même calcul montre que cette expression est égale à

$$\big(\sum_n a_n X^n\big)\big(\big(\sum_n b_n X^n\big)\big(\sum_n c_n X^n\big)\big)$$

On a également

$$\big(\sum_n a_n X^n\big)\big(\sum_n b_n X^n + \sum_n c_n X^n\big) = \sum_n \big(\sum_{k+l=n} a_k (b_l + c_l)\big) X^n$$

Grâce à la distributivité dans A, cette dernière expression est égale à

$$\sum_n \big(\sum_{k+l=n} a_k b_l\big) X^n + \sum_n \big(\sum_{k+l=n} a_k c_l\big) X^n$$

et donc, à

$$\big(\sum_n a_n X^n\big)\big(\sum_n b_n X^n\big) + \big(\sum_n a_n X^n\big)\big(\sum_n c_n X^n\big)$$

Pareil pour montrer que

$$\big(\sum_n a_n X^n + \sum_n b_n X^n\big)\big(\sum_n c_n X^n\big)$$

est égal à

$$\big(\sum_n a_n X^n\big)\big(\sum_n c_n X^n\big) + \big(\sum_n b_n X^n\big)\big(\sum_n c_n X^n\big)$$

C.Q.F.D.

Remarque 12.19. Par récurrence, on voit donc que pour tout anneau A et tout $n \geq 1$,

$$A[X_1, X_2, \ldots, X_n] := A[X_1][X_2]\ldots[X_n]$$

est un anneau. Il est facile de voir que $A[X_1, X_2, \ldots, X_n]$ est l'ensemble des polynômes en n variables, muni des lois d'addition et de multiplication habituelles.

13 Homomorphismes, idéaux et anneaux quotient

Ce chapitre ressemblera fortement au chapitre **??** : la notion d'idéal correspond à celle de sous-groupe distingué, et les anneaux quotient sont les analogues des groupes quotient.

Définition 13.1. Soient A, B deux anneaux, avec éléments neutres pour les multiplications 1_A et 1_B. Une application

$$\alpha : A \longrightarrow B$$

est appelée *homomorphisme (d'anneaux)* si

$$\forall\, a_1, a_2 \in A\ , \quad \alpha(a_1 + a_2) = \alpha(a_1) + \alpha(a_2) \quad \text{et} \quad \alpha(a_1 a_2) = \alpha(a_1)\alpha(a_2)$$

et si $\alpha(1_A) = 1_B$. L'ensemble des homomorphismes de A vers B est noté

$$\mathrm{Hom}(A, B)$$

Si $A = B$, et $\alpha \in \mathrm{Hom}(A, A)$, on dit que α est un *endomorphisme (de l'anneau A).*

Définition 13.2. Soient A, B deux anneaux, et $\alpha \in \mathrm{Hom}(A, B)$.
(a) α est un *épimorphisme (d'anneaux)* si α est surjectif. On écrit

$$\alpha : A \twoheadrightarrow B$$

α est un *monomorphisme (d'anneaux)* si α est injectif. On écrit

$$\alpha : A \hookrightarrow B$$

α est un *isomorphisme (d'anneaux)* si α est bijectif. On écrit

$$\alpha : A \xrightarrow{\sim} B$$

Si $A = B$, et $\alpha : A \xrightarrow{\sim} A$, on dit que α est un *automorphisme (de l'anneau A)*.
(b) On dit que A *est isomorphe à* B, et on écrit $A \cong B$ s'il existe un isomorphisme de A vers B.
(c) On définit *l'image de* α comme

$$\operatorname{im}\alpha := \{\alpha(a) \,|\, a \in A\} \subset B$$

On définit le *noyau de* α comme

$$\ker\alpha := \{a \in A \,|\, \alpha(a) = 0\,(\in B)\} \subset A$$

Définition 13.3. Soient A un anneau avec élément neutre pour la multiplication 1_A, et $B \subset A$ un sous-ensemble. B est appelé *sous-anneau* de A si les axiomes suivants sont satisfaits :

(1) $(B, +)$ est un sous-groupe de $(A, +)$.

(2) $b_1 b_2 \in B \;\forall\; b_1, b_2 \in B$.

(3) $1_A \in B$.

Tout sous-anneau B d'un anneau A, muni des mêmes lois internes de composition $+$ et $\cdot$, est donc un anneau. En plus, l'inclusion $B \hookrightarrow A$ est un monomorphisme d'anneaux.

Exemples 13.4. (a) Soit $n \in \mathbb{Z}$. La multiplication par n

$$\pi_n : \mathbb{Z} \longrightarrow \mathbb{Z}\,, \quad z \longmapsto nz$$

est alors un endomorphisme du groupe $(\mathbb{Z}, +)$ (voir l'Exemple 5.3 (a)). Par contre, le seul n tel que π_n soit un endomorphisme de l'anneau $(\mathbb{Z}, +, \cdot)$, est $n = 1$: π_n doit envoyer 1 vers 1, ce qui est le cas si et seulement si $n = 1$. π_n est alors égal à l'identité $\mathrm{id}_{\mathbb{Z}}$.
(b) L'application

$$\det : M_2(\mathbb{R}) \longrightarrow \mathbb{R}$$

respecte la multiplication :

$$\forall\; A_1, A_2 \in M_2(\mathbb{R})\,, \quad \det(A_1 A_2) = \det(A_1)\det(A_2)$$

Mais det n'est pas un homomorphisme d'anneaux car

$$\forall\; A \in M_2(\mathbb{R})\,, \quad \det(-A) = \det(-I_2)\det(A) = \det(A)$$

donc, si $\det(A) \neq 0$, on a $\det(-A) \neq -\det(A)$. On voit ainsi que det n'est pas un homomorphisme de groupes $(M_2(\mathbb{R}), +) \to (\mathbb{R}, +)$.

(c) Soit A un anneau, avec élément neutre pour la multiplication 1_A. On rappelle l'application

$$\gamma_{1_A} : \mathbb{Z} \longrightarrow A$$

de l'Exemple 8.4 (a). Celle-ci envoie $i \in \mathbb{Z}$ vers $i1_A$ (Définition **??**, et la remarque qui lui suit — on l'applique au groupe $(A, +)$, qui a l'addition comme loi de composition). Si $i \geq 1$, $i1_A$ est donc égal à $1_A + 1_A + \ldots 1_A$ (i fois), si $i \leq -1$,

$$i1_A = -((-i)1_A)$$

et si $i = 0$, alors $i1_A = 0$. Ceci montre en particulier que

$$\forall\, i, j \in \mathbb{Z}\,, \quad \gamma_{1_A}(i+j) = \gamma_{1_A}(i) + \gamma_{1_A}(j) \quad \text{et} \quad \gamma_{1_A}(ij) = \gamma_{1_A}(i)\gamma_{1_A}(j)$$

Par définition, on a $\gamma_{1_A}(1) = 1_A$. L'application γ_{1_A} est donc un homomorphisme d'anneaux.
(d) Soit A un anneau, $x \in A$ tel que $\forall\, a \in A$, $ax = xa$. On définit une application

$$\tau_x : A[X] \longrightarrow A\,,\ \sum_n a_n X^n \longmapsto \sum_n a_n x^n$$

(avec $\tau_x(1) = \tau_x(X^0) = x^0 = 1$). Alors, τ_x est un homomorphisme d'anneaux : soient $\sum_n a_n X^n, \sum_n b_n X^n \in A[X]$. Alors,

$$\tau_x\big(\sum_n a_n X^n + \sum_n b_n X^n\big) = \tau_x\big(\sum_n (a_n + b_n) X^n\big) = \sum_n (a_n + b_n) x^n$$

Grâce à la distributivité dans A, cette expression est égale à

$$\sum_n a_n x^n + \sum_n b_n x^n = \tau_n\big(\sum_n a_n X^n\big) + \tau_n\big(\sum_n b_n X^n\big)$$

D'une part,

$$\tau_x\big(\big(\sum_n a_n X^n\big)\big(\sum_n b_n X^n\big)\big) = \tau_x\big(\sum_n c_n X^n\big) = \sum_n c_n x^n$$

avec $c_n = \sum_{k+l=n} a_k b_l$. D'autre part,

$$\tau_x\big(\sum_n a_n X^n\big)\tau_x\big(\sum_n b_n X^n\big) = \big(\sum_n a_n x^n\big)\big(\sum_n b_n x^n\big) = \sum_n \big(\sum_{k+l=n} a_k x^k b_l x^l\big)$$

Cette dernière expression est égale à

$$\sum_n \big(\sum_{k+l=n} a_k b_l x^k x^l\big) = \sum_n c_n x^n$$

car x commute avec tout élément de A. Finalement,

$$\tau_x(1) = \tau_x(X^0) = x^0 = 1$$

(e) Soit $\alpha : A \to B$ un homomorphisme d'anneaux. D'après la Proposition 13.5 (c) (voir ci-dessous), $\operatorname{im}\alpha$ est un sous-anneau de B. Alors, α induit un homomorphisme

$$A \longrightarrow \operatorname{im}\alpha \quad , \quad a \longmapsto \alpha(a)$$

Notons-le α'. Par construction, α' est surjectif, c'est-à-dire un épimorphisme. En plus, si α est un monomorphisme, alors α' est un isomorphisme :

$$\alpha' : A \xrightarrow{\sim} \operatorname{im}\alpha$$

Proposition 13.5. *Soient A, B deux anneaux, et $\alpha \in \operatorname{Hom}(A, B)$.*
(a) α envoie l'élément neutre 0_A de $(A, +)$ vers l'élément neutre 0_B de $(B, +)$.
(b) $\forall\, a \in A$, $\alpha(-a) = -\alpha(a)$.
(c) $\operatorname{im}\alpha$ est un sous-anneau de B. Plus généralement,

$$\alpha(A') := \{\alpha(a') \,|\, a' \in A'\} \subset B$$

est un sous-anneau de B pour tout sous-anneau A' de A.
(d) $\ker\alpha$ est un sous-groupe de $(A, +)$, et

$$\forall\, a, b \in A\ ,\ x \in \ker\alpha\ ,\ axb \in \ker\alpha$$

(e) α est un monomorphisme ssi $\ker\alpha = \{0_A\}$.
(f) α est un isomorphisme ssi $\exists\, \beta \in \operatorname{Hom}(B, A)$,

$$\beta \cdot \alpha = \mathrm{id}_A : A \longrightarrow A \qquad et \qquad \alpha \cdot \beta = \mathrm{id}_B : B \longrightarrow B\ .$$

Démonstration. (a) et (b) résultent de la Proposition 5.5 (a), (b).

(c) $(\alpha(A'), +) \leq (B, +)$ d'après la Proposition 5.5 (c). Soient $a'_1, a'_2 \in A'$. Alors, $\alpha(a'_1)\alpha(a'_2) = \alpha(a'_1 a'_2) \in \alpha(A')$. Finalement, $1_B = \alpha(1_A) \in \alpha(A')$.

(d) $\ker\alpha \leq (A, +)$ d'après la Proposition 5.5 (d). Soient $a, b \in A$. Pour tout $x \in \ker\alpha$,

$$\alpha(axb) = \alpha(a)\alpha(x)\alpha(b) = \alpha(a)0_B\alpha(b) = 0_B$$

c'est-à-dire $axb \in \ker\alpha$.

(e) Ceci résulte de la Proposition 5.5 (e).

(f) Supposons que α est bijectif. Soit $\beta : B \to A$ l'application inverse. On a donc

$$\beta \cdot \alpha = \mathrm{id}_A : A \longrightarrow A \qquad \text{et} \qquad \alpha \cdot \beta = \mathrm{id}_B : B \longrightarrow B\ .$$

D'après la Proposition 5.5 (f), β est un homomorphisme de groupes $(B, +) \to (A, +)$. En plus, $\beta(1_B) = 1_A$ car $\alpha(1_A) = 1_B$. Il reste donc à montrer que

$$\forall\, b_1, b_2 \in B\ ,\quad \beta(b_1 b_2) = \beta(b_1)\beta(b_2)$$

α étant injectif, cette égalité résulterait de

$$\forall\, b_1, b_2 \in B\ ,\quad \alpha(\beta(b_1 b_2)) = \alpha(\beta(b_1)\beta(b_2))$$

Calculons le coté gauche : $\alpha(\beta(b_1 b_2)) = b_1 b_2$ puisque $\alpha \cdot \beta = \mathrm{id}_B$. Quant au coté droite,

$$\alpha(\beta(b_1)\beta(b_2)) = \alpha(\beta(b_1))\alpha(\beta(b_2)) = b_1 b_2$$

car $\alpha \in \mathrm{Hom}(A, B)$, et car $\alpha \cdot \beta = \mathrm{id}_B$. **C.Q.F.D.**

Définition 13.6. Soient A un anneau, et $I \subset A$. On dit que I est un *idéal* de A, si I est un sous-groupe de $(A, +)$, et si pour tout $a, b \in A$ et $x \in I$, on a $axb \in I$.

Corollaire 13.7. *Soient A, B deux anneaux, et $\alpha \in \mathrm{Hom}(A, B)$. Alors,* $\ker \alpha$ *est un idéal de A.*

Démonstration. D'après la Proposition 13.5 (d), $\ker \alpha$ a la propriété caractérisant les idéaux de A. **C.Q.F.D.**

Exemples 13.8. (a) Soit A un anneau. Alors, $\{0\}$ et A sont des idéaux de A. Si $\{0\}$ et A sont les seuls idéaux, et si $A \neq \{0\}$, on appelle A un anneau *simple*.

(b) Soit A un anneau. Alors, le seul idéal I contenant 1 est égal à A : en effet, soit $a \in A$. Alors, $a = a1 \in I$.

(c) Soit K un corps. Alors, K est un anneau simple : soit $I \subset K$ un idéal non-nul. On choisit $0 \neq x \in I$. Puisque K est un corps, x admet un inverse x^{-1}. Donc, $1 \in I$, et on applique (b).

(d) Considérons l'anneau $\mathbb{Z}$, et fixons $n \in \mathbb{Z}$. Le sous-groupe $n\mathbb{Z}$ de $(\mathbb{Z}, +)$ est alors un idéal : si $x \in \mathbb{Z}$ est un multiple de n, alors ax est un multiple de n pour tout $a \in \mathbb{Z}$. Puisque l'on sait que tout sous-groupe de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$, on a montré en particulier : tout sous-groupe de $\mathbb{Z}$ est un idéal.

Proposition 13.9. *Soit A un anneau.*

(a) Soient I_j des idéaux de A. Alors, leur intersection

$$\bigcap_j I_j \subset A$$

est un idéal de A.

(b) Soient I_1, I_2 des idéaux de A. Alors, leur union

$$I_1 \cup I_2 \subset A$$

est un idéal de A si et seulement si $I_1 \subset I_2$ ou $I_2 \subset I_1$.

Démonstration. (a) D'après la Proposition 3.5 (a), $\cap_j I_j$ est un sous-groupe de A. Soient $a, b \in A$ et $x \in \cap_j I_j$. Alors, $\forall j$, $axb \in I_j$, donc $axb \in \cap_j I_j$.

(b) Supposons d'abord $I_1 \subset I_2$. Alors, $I_1 \cup I_2 = I_2$, ce qui est un idéal de A. Pareil si $I_2 \subset I_1$. Supposons maintenant que $I_1 \cup I_2$ est un idéal de A. C'est donc en particulier un sous-groupe. D'après la Proposition 3.5 (b), on a donc $I_1 \subset I_2$ ou $I_2 \subset I_1$. **C.Q.F.D.**

Définition 13.10. Soient A un anneau, et $M \subset A$ un sous-ensemble. On pose

$$(M)_A := \bigcap_{M \subset I \text{ idéal de } A} I$$

D'apres la Proposition 13.9 (a), $(M)_A$ est un idéal de A. C'est le plus petit idéal de A contenant l'ensemble M. Il est appelé *l'idéal de A engendré par M*.

Quand il n'y a pas d'ambiguïté quant à l'anneau A, on écrit (M) au lieu de $(M)_A$. Etant donné plusieurs sous-ensembles $M_1, M_2, M_3, \ldots$ de A, on écrit $(M_1, M_2, M_3, \ldots)$ au lieu de $(M_1 \cup M_2 \cup M_3 \cup \ldots)$. On écrit $(a, b, c, \ldots)$ au lieu de $(\{a, b, c, \ldots\})$. Comme ceci a été le cas pour les groupes, un cas particulier, mais très important concerne les idéaux de la forme (a), c'est-à-dire ceux engendrés par un seul élément :

Définition 13.11. Soient A un anneau, et $I \subset A$ un idéal. I est appelé *idéal principal* s'il est de la forme $I = (a)$, avec un élément a de A.

Exemple 13.12. Attention ! En général, le sous-groupe $< a >$ de $(A, +)$ engendré par a est strictement plus petit que l'idéal (a) engendré par a. Prenons $A = \mathbb{Q}$ et $a = 1$. Alors, $< 1 >$ est égal à $\mathbb{Z} \subset \mathbb{Q}$. Mais $(1)_{\mathbb{Q}} = \mathbb{Q}$ d'après l'Exemple 13.8 (c).

Définition 13.13. Soient A un anneau, et $I, J \subset A$ deux idéaux.
(a) La *somme* de I et J est définie comme

$$I + J := \{x + y \in A \,|\, x \in I \ , \ y \in J\}$$

(b) Le *produit* de I et J est défini comme

$$IJ := (xy \in A \,|\, x \in I \ , \ y \in J)_A$$

Proposition 13.14. *Soient A un anneau, et $I, J \subset A$ deux idéaux.*
(a) $I + J$ et IJ sont des idéaux de A. $I + J$ est l'idéal engendré par I et J.
(b) On a les inclusions

$$IJ \subset I \cap J \quad et \quad I, J \subset I + J$$

Démonstration. (a) Le produit est défini comme l'idéal engendré par un certain ensemble ; c'est donc un idéal. Quant à la somme $I + J$, elle contient $0 + 0 = 0$, et n'est donc pas vide. Soient $x, x' \in I$ et $y, y' \in J$, et considérons $x + y, x' + y' \in I + J$. $(I, +)$ et $(J, +)$ étant des sous-groupes, $x+x', -x \in I$ et $y+y', -y \in J$. Donc, la somme $x+y+x'+y' = x+x'+y+y'$ (on rappelle que $(A, +)$ est Abélien !) et $-(x + y) = -x - y$ appartiennent à $I + J$. $I + J$ est donc un sous-groupe de $(A, +)$. Soient en plus $a, b \in A$. I et J étant des idéaux, $axb \in I$ et $ayb \in J$. Donc, $a(x+y)b = axb+ayb \in I+J$. Soit enfin K l'idéal engendré par I et J. Il contient I et J, donc également

tout élément de la forme $x + y$, avec $x \in I$ et $y \in J$. Donc, $I + J \subset K$. Réciproquement, $I + J$ est un idéal contenant I et J, donc également l'idéal engendré par I et J.

(b) Soient $x \in I$ et $y \in J$. Alors, $x \in A$, et puisque J est un idéal, $xy \in J$. Pour la même raison, $xy \in I$. Donc, $I \cap J$ contient tous les xy, avec $x \in I$ et $y \in J$. Puisque $I \cap J$ est un idéal (Proposition 13.9 (a)), il contient donc l'idéal IJ engendré par les xy, avec $x \in I$ et $y \in J$.

$I \subset I + J$ car $0 \in J$, et $x = x + 0$, $\forall\, x \in I$. Pareil pour $J \subset I + J$.

C.Q.F.D.

Exemples 13.15. (a) On considère l'anneau $\mathbb{Z}$, et deux idéaux $n\mathbb{Z}$ et $m\mathbb{Z}$ (voir l'Exemple 13.8 (c)). Alors,

$$n\mathbb{Z} \cap m\mathbb{Z} = ppcm(n, m)\mathbb{Z}$$

$$(n\mathbb{Z})(m\mathbb{Z}) = nm\mathbb{Z}$$

et

$$n\mathbb{Z} + m\mathbb{Z} = pgcd(n, m)\mathbb{Z}$$

En fait, $x \in \mathbb{Z}$ appartient à $n\mathbb{Z} \cap m\mathbb{Z}$ si et seulement si x est divisible à la fois par n et par m, ce qui est le cas si et seulement si $ppcm(n, m)$ divise x. La formule pour le produit $(n\mathbb{Z})(m\mathbb{Z})$ est évidente. Pour la somme, remarquons d'abord que $pgcd(n, m)$ divise n et m. Donc, $pgcd(n, m)\mathbb{Z}$ contient n et m, et donc, l'idéal engendré par n et m. Réciproquement, $n\mathbb{Z} + m\mathbb{Z} \supset pgcd(n, m)\mathbb{Z}$: d'après l'algorithme d'Euclide, on trouve $a, b \in \mathbb{Z}$ tels que $an + bm = pgcd(n, m)$. Donc, $pgcd(n, m)$ appartient à l'idéal engendré par n et m.

(b) Dans la situation de (a), supposons que $pgcd(n, m) = 1$. Alors,

$$n\mathbb{Z} \cap m\mathbb{Z} = (n\mathbb{Z})(m\mathbb{Z}) = nm\mathbb{Z}$$

et

$$n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$$

Puisque pour tout anneau A, le groupe $(A, +)$ est Abélien, tout idéal I de A est un sous-groupe distingué de $(A, +)$. On peut donc former le quotient A/I, qui est à nouveau un groupe par rapport à l'addition (Théorème 7.9).

Théorème 13.16. *Soit $(A, +, \cdot)$ un anneau, et $I \subset A$ un idéal.*

(a) La règle

$$(a_1 + I) \cdot (a_2 + I) := (a_1 \cdot a_2) + I$$

définit une loi de composition $\cdot$ sur A/I. $(A/I, +, \cdot)$ est à nouveau un anneau. Son élément neutre pour la multiplication est $1 + I \in A/I$.

(b) L'application

$$\pi : A \longrightarrow A/I\ ,\ a \longmapsto a + I$$

est un épimorphisme d'anneaux. On a $\ker \pi = I$.

Définition 13.17. Dans la situation du Théorème 13.16, on appelle A/I *l'anneau quotient de* A *par* I, et

$$\pi : A \twoheadrightarrow A/I$$

l'épimorphisme canonique de A *vers* A/I.

Démonstration du Théorème 13.16. (a) Il s'agit d'abord (et surtout...) de prouver que l'application

$$A/I \times A/I \longrightarrow A/I \ , \ (a_1 + I, a_2 + I) \longmapsto (a_1 a_2) + I$$

est bien définie. Autrement dit, que pour $a_1, a_1', a_2, a_2' \in A$ avec $a_1 + I = a_1' + I$ et $a_2 + I = a_2' + I$, on a

$$(a_1 a_2) + I = (a_1' a_2') + I$$

On a $a_1 - a_1', a_2 - a_2' \in I$. Donc,

$$a_1 a_2 - a_1' a_2' = a_1(a_2 - a_2') + (a_1 - a_1')a_2' \in I$$

car I est un idéal, et donc, $(a_1 a_2) + I = (a_1' a_2') + I$. Donc,

$$A/I \times A/I \longrightarrow A/I$$

est effectivement bien définie, et donc une deuxième loi de composition sur A/I.

L'axiome 12.1 (1) est satisfait puisqu'il ne concerne que l'addition ; on applique le Théorème 7.9 (a). Les axiomes 12.1 (2)–(4) pour $(A/I, +, \cdot)$ résultent de ceux pour $(A, +, \cdot)$.

(b) D'après le Théorème 7.9 (b), π est un épimorphisme de groupes, de noyau I. D'après (a), il respecte les éléments neutres pour la multiplication. Par définition de la multiplication dans A/I,

$$\forall\ a_1, a_2 \in A \ , \quad (a_1 a_2) + I = (a_1 + I)(a_2 + I)$$

C.Q.F.D.

Théorème 13.18 (Propriété universelle de l'anneau quotient)**.** *Soient* A_1 *un anneau, et* $I \subset A_1$ *un idéal. Notons* π *l'épimorphisme canonique de* A_1 *vers* A_1/I. *Soit* A_2 *un anneau.*

(a) Soit $\alpha \in \mathrm{Hom}(A_1, A_2)$*, et supposons que*

$$I \subset \ker \alpha$$

c'est-à-dire $\forall\ x \in I$, $\alpha(x) = 0$. *Alors, il existe une unique application*

$$\tilde{\alpha} : A_1/I \longrightarrow A_2$$

telle que $\alpha = \tilde{\alpha} \cdot \pi$ *(*$\cdot$ *= la composition des applications).* $\tilde{\alpha}$ *est un homomorphisme d'anneaux* $A_1/I \to A_2$.

(b) La règle $\alpha \mapsto \tilde{\alpha}$ induit une application

$$\{\alpha \in \mathrm{Hom}(A_1, A_2) \,|\, I \subset \ker \alpha\} \longrightarrow \mathrm{Hom}(A_1/I, A_2)$$

Cette application est bijective. Autrement dit : se donner un homomorphisme $A_1/I \to A_2$ revient à la même chose que se donner un homomorphisme $A_1 \to A_2$ qui est trivial sur I.

Démonstration. (a) La propriété universelle du groupe quotient montre l'existence et l'unicité de l'application $\tilde{\alpha}$. Elle montre aussi que $\tilde{\alpha}$ est un homomorphisme de groupes $(A_1/I, +) \to (A_2, +)$. On a

$$\forall\, a \in A_1\ , \quad \tilde{\alpha}(a + I) = \alpha(a)$$

Pour montrer que $\tilde{\alpha}$ est même un homomorphisme d'anneaux, on fait comme dans la preuve du Théorème 13.16.

(b) Imiter la preuve de 7.12 (b). **C.Q.F.D.**

Théorème 13.19 (Théorème d'homomorphie)**.** *Soient A_1 et A_2 deux anneaux, et $\alpha \in \mathrm{Hom}(A_1, A_2)$. (D'après le Corollaire 13.7,* $\ker \alpha$ *est un idéal de A_1.) Notons π l'épimorphisme canonique de A_1 vers $A_1/\ker \alpha$.*

(a) Il existe une unique application

$$\beta : A_1/\ker \alpha \longrightarrow A_2$$

telle que $\alpha = \beta \cdot \pi$. β est un homomorphisme d'anneaux.

(b) β est injectif, et donc, un monomorphisme d'anneaux $A_1/\ker \alpha \hookrightarrow A_2$.

(c) β induit un isomorphisme

$$A_1/\ker \alpha \xrightarrow{\sim} \mathrm{im}\, \alpha$$

Démonstration. (a) Ceci résulte de la propriété universelle 13.18 (a), appliquée à $I := \ker \alpha$. On a donc

$$\forall\, a \in A_1\ ,\ \beta(a + \ker \alpha) = \alpha(a)$$

(b) Prouvons que $\ker \beta$ est trivial : soit $a \in A_1$ tel que $\beta(a + \ker \alpha) = 0$. D'après (a), ceci veut dire que $\alpha(a) = 0$, et donc, que $a \in \ker \alpha$. Autrement dit,

$$a + \ker \alpha = 0 + \ker \alpha$$

est l'élément nul de $A_1/\ker \alpha$.

(c) Appliquer l'Exemple 13.4 (e) à la situation dans (b). **C.Q.F.D.**

Exemples 13.20. (a) Soit A un anneau,

$$\gamma_{1_A} : \mathbb{Z} \longrightarrow A$$

l'homomorphisme d'anneaux de l'Exemple 13.4 (c). Si γ_{1_A} est injectif, alors $\gamma_{1_A} : \mathbb{Z} \hookrightarrow A$ est un monomorphisme. Sinon, le noyau $\ker \gamma_{1_A}$ est strictement plus grand que $\{0\}$. D'après le Corollaire 13.7, $\ker \gamma_{1_A}$ est un idéal de $\mathbb{Z}$, donc

(voir Exemple 13.8 (d)) de la forme $n\mathbb{Z}$, avec $n \in \mathbb{N}_{\geq 1}$. D'après le Théorème d'homomorphie, γ_{1_A} induit donc un monomorphisme $\mathbb{Z}/n\mathbb{Z} \hookrightarrow A$ (qui envoie $\overline{1}$ vers 1_A).

(b) Mais qui est donc cet anneau quotient $\mathbb{Z}/n\mathbb{Z}$, pour $n \in \mathbb{N}_{\geq 1}$? On sait qu'en tant qu'ensemble,

$$\mathbb{Z}/n\mathbb{Z} = \{x + n\mathbb{Z} \,|\, x \in \mathbb{Z}\}$$

Cet ensemble a n éléments, que l'on peut représenter par les classes de $0, 1, \ldots, n-1$ modulo n (voir l'Exemple 8.4 (d)). La loi d'addition sur $\mathbb{Z}/n\mathbb{Z}$ est

$$(x + n\mathbb{Z}) + (y + n\mathbb{Z}) := (x + y) + n\mathbb{Z}$$

et la loi de multiplication est

$$(x + n\mathbb{Z})(y + n\mathbb{Z}) := (xy) + n\mathbb{Z}$$

L'élement neutre pour l'addition est $0 + n\mathbb{Z}$, l'élement neutre pour la multiplication est $1 + n\mathbb{Z}$.

(c) Quels sont les éléments inversibles dans l'anneau $\mathbb{Z}/n\mathbb{Z}$, pour $n \in \mathbb{N}_{\geq 1}$? Soit alors $x \in \mathbb{Z}$. D'après la Définition 12.12, sa classe $x + n\mathbb{Z}$ est inversible (en tant qu'élément de $\mathbb{Z}/n\mathbb{Z}$) si et seulement si

$$\exists\, y \in \mathbb{Z}\ ,\ xy + n\mathbb{Z} = (x + n\mathbb{Z})(y + n\mathbb{Z}) = 1 + n\mathbb{Z}$$

c'est-à-dire

$$\exists\, y \in \mathbb{Z}\ ,\ xy \equiv 1 \mod n$$

On se propose de montrer : ceci est le cas si et seulement si $pgcd(x, n) = 1$. En fait, si n divise $(xy - 1)$, aucun diviseur non-trivial de n ne peut diviser xy, donc $pgcd(x, n) = 1$. Réciproquement, supposons que $pgcd(x, n) = 1$. D'après l'algorithme d'Euclide, on trouve $y, m \in \mathbb{Z}$ tels que $xy + nm = 1$. Donc, $xy \equiv 1 \mod n$. On a donc montré : le groupe des éléments inversibles $(\mathbb{Z}/n\mathbb{Z})^*$ est égal à

$$\{x + n\mathbb{Z} \,|\, x \in \mathbb{Z}\ ,\ pgcd(x, n) = 1\} \subset \mathbb{Z}/n\mathbb{Z}$$

conformément à la notation introduite dans l'Exemple **??** (a).

Proposition 13.21. *Soient A un anneau, et $J \subset A$ un idéal. On note*

$$\pi : A \twoheadrightarrow A/J$$

l'épimorphisme canonique.

(a) Soit $\tilde{I}$ un idéal de A/J. Alors, sa pré-image

$$\pi^{-1}\tilde{I} := \{a \in A \,|\, \pi(a) \in \tilde{I}\}$$

est un idéal de A.

(b) La règle $\tilde{I} \mapsto \pi^{-1}\tilde{I}$ est une application

$$\pi^{-1} : \{\tilde{I} \,|\, \tilde{I} \text{ idéal de } A/J\} \longrightarrow \{I \,|\, I \text{ idéal de } A\}$$

π^{-1} est injectif, et un idéal $I \subset A$ est de la forme $\pi^{-1}\tilde{I}$ ssi I contient J. Donc : π^{-1} induit une bijection

$$\pi^{-1} : \{\tilde{I} \,|\, \tilde{I} \text{ idéal de } A/J\} \longrightarrow \{I \,|\, I \text{ idéal de } A \text{ contenant } J\}$$

La réciproque de cette bijection est donnée par

$$\pi(I) \longmapsto I$$

Démonstration. On imite fidèlement la démonstration de la Proposition 7.13. **C.Q.F.D.**

Exemple 13.22. La Proposition 13.21 permet notamment d'identifier les idéaux de l'anneau $\mathbb{Z}/n\mathbb{Z}$, pour $n \in \mathbb{N}_{\geq 1}$: ils sont en bijection avec les idéaux de $\mathbb{Z}$ contenant $n\mathbb{Z}$. On sait (voir l'Exemple 13.8 (d)) que tout idéal de $\mathbb{Z}$ est de la forme $m\mathbb{Z}$, pour $m \in \mathbb{N}$. On a

$$n\mathbb{Z} \subset m\mathbb{Z} \Longleftrightarrow n \in m\mathbb{Z} \Longleftrightarrow m \,|\, n$$

Donc, les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont parametrisés par les diviseurs de n ; tout idéal de $\mathbb{Z}/n\mathbb{Z}$ est de la forme $m\mathbb{Z}/n\mathbb{Z}$, pour $m \in \mathbb{N}$, avec $m \,|\, n$.

Théorème 13.23 (Lemme Chinois)**.** *Soient A un anneau, et $I, J \subset A$ deux idéaux tels que $I + J = A$. Alors,*

$$A/(I \cap J) \cong A/I \times A/J$$

Si en plus $IJ = JI$ (par exemple, si A est commutatif), alors $I \cap J = IJ$.

On retrouve comme cas particulier le Lemme Chinois pour l'anneau $A = \mathbb{Z}$ (Théorème 9.3) : soient $m, n \in \mathbb{N}_{\geq 1}$, et supposons que $pgcd(m, n) = 1$. D'après l'Exemple 13.15 (b), ces hypothèses impliquent

$$n\mathbb{Z} \cap m\mathbb{Z} = nm\mathbb{Z}$$

et

$$n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$$

Donc, d'après le Théorème 13.23,

$$\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

Démonstration du Théorème 13.23. On considère l'homomorphisme

$$\alpha : A \longrightarrow A/I \times A/J \ , \ a \longmapsto (a + I, a + J)$$

Déterminons le noyau de α : soit $a \in A$. Alors,

$$a \in \ker \alpha \Longleftrightarrow (a+I, a+J) = (0+I, 0+J) \in A/I \times A/J \Longleftrightarrow a \in I \text{ et } a \in J$$

ce qui équivaut à $a \in I \cap J$. Donc, $\ker \alpha = I \cap J$.

Le Théorème d'homomorphie dit alors que

$$A/(I \cap J) \cong \operatorname{im} \alpha$$

Soient $a, b \in A$. Puisque $I + J = A$, on peut trouver $x, x' \in I$ et $y, y' \in J$ tel que $a = x + y$ et $b = x' + y'$. Posons $c := x' + y \in A$. Alors,

$$\alpha(c) = (c+I, c+J) = (x'+y+I, x'+y+J) = (y+I, x'+J) = (a+I, b+J)$$

c'est-à-dire $(a + I, b + J) \in \operatorname{im}\alpha$. On en conclut que $\operatorname{im}\alpha = A/I \times A/J$.

Pour terminer, il reste à montrer que l'inclusion $IJ \subset I \cap J$ de la Proposition 13.14 (b) est en fait une égalité si $I + J = A$, et si $IJ = JI$: on a par distributivité

$$I \cap J = A(I \cap J) = (I + J)(I \cap J) = I(I \cap J) + J(I \cap J) \subset IJ + JI = IJ$$

C.Q.F.D.

14 Anneaux principaux, anneaux Euclidiens, anneaux factoriels

Définition 14.1. Soit A un anneau commutatif. A est dit *principal* si A est intègre, et si tout idéal de A est prinicipal (voir Définition 13.11).

Définition 14.2. Soit A un anneau commutatif. A est dit *Euclidien* si A est intègre, et s'il existe une application

$$\varphi : A - \{0\} \longrightarrow \mathbb{N}$$

tel que $\forall\, a, b \in A - \{0\}\ \exists\, q, r \in A$,

$$a = qb + r \quad \text{et} \quad (r = 0 \ \text{ ou } \ \varphi(r) < \varphi(b))$$

(*division Euclidienne* par rapport à φ).

Définition 14.3. Soient A un anneau commutatif, et $x \in A - \{0\}$. L'élément x est dit *irréductible* si x n'est pas inversible, et si la relation $x = uv$, avec $u, v \in A$ implique que u ou v est inversible.

Exemple 14.4. Dans $A = \mathbb{Z}$, les éléments irréductibles sont exactement ceux de la forme $\pm p$, avec un nombre premier p.

Définition 14.5. Soient A un anneau commutatif, et $a, b \in A$. On dit que a et b sont *associés* l'un à l'autre s'il existe $u \in A^*$ tel que $b = ua$. On écrit alors $a \sim b$.

La relation $\sim$ est clairement une relation d'équivalence sur A. Si $a \sim b$, alors a est irréductible si et seulement si b l'est.

Définition 14.6. Soit A un anneau commutatif.
(a) On dit que A *admet la factorisation* si tout élément non-inversible $a \in A - \{0\}$ peut se représenter comme produit d'éléments irréductibles :

$$a = x_1 \cdots x_r \ , \ \text{avec } x_1, \ldots, x_r \in A \text{ irréductibles}$$

(b) On dit que A *admet la factorisation unique* s'il admet la factorisation, et si toute identité

$$x_1 \cdots x_r = y_1 \cdots y_s$$

entre produits d'éléments irréductibles implique que $r = s$, et que $x_i \sim y_{\sigma(i)}$ pour une permutation $\sigma \in \mathfrak{S}_r$.
(c) On dit que A est un anneau *factoriel* si A est intègre, et s'il admet la factorisation unique.

Théorème 14.7. *Tout anneau Euclidien est principal.*

Théorème 14.8. *Tout anneau principal est factoriel.*

On verra les démonstrations plus tard.

Exemples 14.9. (a) L'anneau $\mathbb{Z}$ est Euclidien : on définit

$$\varphi : \mathbb{Z} - \{0\} \longrightarrow \mathbb{N}\ ,\ z \longmapsto\ |\, z\,|$$

Pour $a, b \in \mathbb{Z} - \{0\}$, on définit $q := \left[\frac{a}{b}\right]$, le plus grand nombre entier qui est inférieur ou égal à $\frac{a}{b}$. Alors, $r := a - qb \in \mathbb{Z}$ est contenu entre 0 et $b - 1$ si $b > 0$; r est contenu entre $b + 1$ et 0 si $b < 0$. D'après les Théorèmes 14.7 et 14.8, $\mathbb{Z}$ est principal, donc factoriel. En fait, on le savait déjà : tout idéal de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$ (Exemple 13.8 (d)), donc principal, et $\mathbb{Z}$ est factoriel parce que tout le monde le sait.
(b) Soit K un corps commutatif. L'anneau $K[X]$ est alors Euclidien, donc principal, donc factoriel : on définit

$$\varphi := \deg : K[X] - \{0\} \longrightarrow \mathbb{N}\ ,\ f \longmapsto \deg(f)$$

Ici, la division Euclidienne est la division classique des polynômes.

Définition 14.10. Soient A un anneau commutatif, et $a, b, x \in A$.
(a) On dit que x *divise* a, ou que a *est divisible par* x, et on écrit $x \,|\, a$ s'il existe $y \in A$ tel que $a = xy$.
(b) x est appelé un *diviseur commun* de a et de b si $x \,|\, a$ et $x \,|\, b$.
(c) x est appelé un *multiple commun* de a et de b si $a \,|\, x$ et $b \,|\, x$.
(d) x est appelé un *plus grand diviseur commun* de a et de b si x est un diviseur commun de a et de b, et si tout autre diviseur commun de a et de b divise x. On écrit alors $x = pgcd(a, b)$.
(e) x est appelé un *plus petit multiple commun* de a et de b si x est un multiple commun de a et de b, et si tout autre multiple commun de a et de b est divisible par x. On écrit alors $x = ppcm(a, b)$.

Attention ! En général, l'existence des *pgcd* et *ppcm* n'est pas assurée. Même s'ils existent, il peuvent en exister plusieurs. Exemple : $2 = pgcd(4, 6)$, et $-2 = pgcd(4, 6)$ dans $\mathbb{Z}$. L'équation x"="$pgcd(a, b)$ est donc un abus de notation en ce que $x = pgcd(a, b)$ et $y = pgcd(a, b)$ n'implique pas $x = y$.

Cependant, si A est intègre, $x = pgcd(a,b)$ et $y = pgcd(a,b)$ (pour $a, b \neq 0$) implique que $x \sim y$ (utiliser la Proposition 12.8). Dans un anneau intègre, "le" *pgcd* et "le" *ppcm* sont donc uniquement déterminés (s'ils existent) en tant qu'élements de $A/\sim$.

Dans un anneau factoriel A, on se sert de la factorisation unique de façon suivante : on fixe d'abord un système $\mathfrak{X} = (x_i \,|\, i \in I)$ de représentants des classes modulo $\sim$ d'éléments irréductibles. Autrement dit, pour tout élément irréductible y de A, il existe un unique indice i tel que $y \sim x_i$. Soit $a \in A - \{0\}$. En modifiant les facteurs d'une factorisation de a selon l'observation ci-dessus, on trouve : il existe des exposants $\alpha_i \in \mathbb{N}$, prèsque tous nuls, et $u \in A^*$ tel que

$$a = u \cdot \prod_i x_i^{\alpha_i}$$

La factorisation unique montre que les α_i et u sont uniquement déterminés par a. Ceci permet de montrer :

Proposition 14.11. *Soient A un anneau factoriel, $\mathfrak{X} = (x_i \,|\, i \in I)$ comme ci-dessus, et $a, b \in A - \{0\}$. Ecrivons*

$$a = u \cdot \prod_i x_i^{\alpha_i} \text{ et } b = v \cdot \prod_i x_i^{\beta_i}$$

avec $u, v \in A^*$ et $\alpha_i, \beta_i \in \mathbb{N}$.

(a) $a \,|\, b$ si et seulement si $\forall i$, $\alpha_i \leq \beta_i$.

(b) a et b admettent des plus grands diviseurs communs. Plus précisément,

$$\prod_i x_i^{\min(\alpha_i, \beta_i)} = pgcd(a,b)$$

(c) a et b admettent des plus petits multiples communs. Plus précisément,

$$\prod_i x_i^{\max(\alpha_i, \beta_i)} = ppcm(a,b)$$

Démonstration. Les parties (b) et (c) sont impliquées par la partie (a) (considérer la factorisation d'un diviseur ou d'un multiple commun...).

Clairement a divise b si $\forall\, i$, $\alpha_i \leq \beta_i$. Si a divise b, alors il existe $c \in A - \{0\}$ tel que $b = ac$. La factorisation de c est de la forme

$$c = w \cdot \prod_i x_i^{\gamma_i}$$

avec $w \in A^*$ et $\gamma_i \in \mathbb{N}$. Ceci donne

$$b = ac = uw \cdot \prod_i x_i^{\alpha_i + \gamma_i}$$

donc $\alpha_i + \gamma_i = \beta_i$ pour tout i car les β_i sont uniquement déterminés par b. **C.Q.F.D.**

Si l'anneau est même principal, on peut dire plus :

Proposition 14.12 (Identité de Bézout)**.** *Soient A un anneau principal, et $a, b \in A - \{0\}$.*
(a) L'idéal (a, b) est engendré par $pgcd(a, b)$.
(b) Il existe $u, v \in A$ tel que $au + bv = pgcd(a, b)$.

Démonstration. (a) implique (b) car tout élément de l'idéal engendré par a et b est de la forme $au + bv$, avec $u, v \in A$.

Quant à (a), soit $x \in A$ un plus grand diviseur commun de a et de b (ceci existe grâce au Théorème 14.8 et à la Proposition 14.11). Divisons a et b par x. On obtient deux éléments a', b' de A avec $pgcd(a', b') = 1$. Soit $c \in A$ un générateur de (a', b'). (A est principal !) Puisque $a', b' \in (c)$, c est diviseur commun de a' et de b'. Donc, c divise 1, c'est-à-dire $c \in A^*$. Mais l'idéal engendré par un élément inversible est tout l'anneau A. Donc, $(a', b') = A$. Multipliant cette équation par x, on obtient

$$(a, b) = (a'x, b'x) = (pgcd(a, b))$$

C.Q.F.D.

Il existe des anneaux factoriels dans lesquels l'identité de Bézout ne vaut pas !

Exemples 14.13. (a) On considère une racine carrée $\sqrt{-5}$ de -5 dans $\mathbb{C}$, et on pose

$$\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \,|\, a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

$\mathbb{Z}[\sqrt{-5}]$ est un sous-anneau de $\mathbb{C}$: on voit facilement que $(\mathbb{Z}[\sqrt{-5}], +)$ est un groupe. $1 = 1 + 0\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$. Soient $a, b, c, d \in \mathbb{Z}$. Alors,

$$(a + b\sqrt{-5})(c + d\sqrt{-5}) = ac + (b + d)\sqrt{-5} - 5bd = (ac - 5bd) + (b + d)\sqrt{-5}$$

appartient à $\mathbb{Z}[\sqrt{-5}]$. En tant que sous-anneau d'un corps commutatif, $\mathbb{Z}[\sqrt{-5}]$ est commutatif et intègre. On se propose de montrer que $\mathbb{Z}[\sqrt{-5}]$ n'est pas factoriel.

Posons

$$N : \mathbb{Z}[\sqrt{-5}] \longrightarrow \mathbb{N}\ ,\ a + b\sqrt{-5} \longmapsto |\, a + b\sqrt{-5} \,|^2 = a^2 + 5b^2$$

(1) L'application N est multiplicative : $\forall\, x, y \in \mathbb{Z}[\sqrt{-5}]$, $N(xy) = N(x)N(y)$.
(2) $(\mathbb{Z}[\sqrt{-5}])^* = \{1, -1\} (= \{x \in \mathbb{Z}[\sqrt{-5}] \,|\, N(x) = 1\})$: on a clairment "$\supset$". Soit alors $x \in (\mathbb{Z}[\sqrt{-5}])^*$. Il existe donc $y \in \mathbb{Z}[\sqrt{-5}]$ tel que $xy = 1$. Donc, par (1),

$$1 = N(1) = N(x)N(y)$$

c'est-à-dire $N(x) = N(y) = 1$ (car les deux appartiennent à $\mathbb{N}$).
(3) Les éléments 3, $2 + \sqrt{-5}$ et $2 - \sqrt{-5}$ sont irréductibles dans $\mathbb{Z}[\sqrt{-5}]$: on observe que ces éléments ont tous l'image 9 sous N. Si par exemple

$3 = xy$, avec $x, y \in \mathbb{Z}[\sqrt{-5}]$, alors $9 = N(x)N(y)$. Supposons que ni x ni y n'est inversible, c'est-à-dire (d'après (2)) que $N(x), N(y) \geq 2$. Leur produit étant 9, on aurait alors $N(x) = N(y) = 3$. Ecrivons $x = a + b\sqrt{-5}$. Donc, $3 = a^2 + 5b^2$. Mais il est impossible de représenter 3 sous cette forme, avec $a, b \in \mathbb{Z}$. On en conclut que x ou y est inversible et donc, que 3 est irréductible. Pareil pour $2 + \sqrt{-5}$ et $2 - \sqrt{-5}$.
(4) Dans l'anneau $\mathbb{Z}[\sqrt{-5}]$, on a les factorisations

$$9 = 3 \cdot 3 = (2 + \sqrt{-5}) \cdot (2 - \sqrt{-5})$$

de 9 en produit d'éléments irréductibles. Or, $(\mathbb{Z}[\sqrt{-5}])^* = \{1, -1\}$ (d'après (2)), donc 3 n'est associé ni à $2 + \sqrt{-5}$ ni à $2 - \sqrt{-5}$. $\mathbb{Z}[\sqrt{-5}]$ n'admet donc pas la factorisation unique, donc, il n'est pas factoriel.
(b) L'anneau des *entiers de Gauß* (C.F. Gauß, 1777–1855). On pose

$$\mathbb{Z}[i] := \{a + bi \,|\, a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

On montre comme dans (a) que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$. Il est donc commutatif et intègre. Posons

$$\varphi : \mathbb{Z}[i] \longrightarrow \mathbb{N}\ ,\ a + bi \longmapsto\ |\, a + bi \,|^{\,2} = a^2 + b^2$$

(1) L'application φ est multiplicative.
(2) $\mathbb{Z}[i]$ est Euclidien : soient $x, y \in \mathbb{Z}[i] - \{0\}$. Ecrivons $\frac{x}{y} = s + ti$, avec $s, t \in \mathbb{R}$, et choisissons $m, n \in \mathbb{Z}$ tels que

$$|\, s - m \,| \leq \frac{1}{2} \text{ et } |\, t - n \,| \leq \frac{1}{2}$$

On pose $q := m + ni \in \mathbb{Z}[i]$. Alors,

$$|\, \frac{x}{y} - q \,|^{\,2} = |\, (s - m) + (t - n)i \,|^{\,2} = (s - m)^2 + (t - n)^2 \leq \frac{1}{2}$$

donc avec $r := x - qy \in \mathbb{Z}[i]$

$$\varphi(r) = |\, \frac{x}{y} - q \,|^{\,2} \varphi(y) \leq \frac{1}{2}\varphi(y) < \varphi(y)$$

(3) D'après les Théorèmes 14.7 et 14.8, l'anneau $\mathbb{Z}[i]$ est principal et factoriel.
(4) $(\mathbb{Z}[i])^* = \{1, -1, i, -i\} (= \{x \in \mathbb{Z}[i] \,|\, \varphi(x) = 1\})$: comme dans (a).
(5) Soit $p \in \mathbb{Z}$ un nombre premier. Alors, soit p reste irréductible dans $\mathbb{Z}[i]$, soit

$$\exists\, a + bi \in \mathbb{Z}[i] \text{ irréductible }\ ,\ p = a^2 + b^2 = (a + bi)(a - bi) = \varphi(a + bi)$$

En effet, soit

$$p = x_1 \cdots x_r$$

une factorisation de p en produit d'éléments irréductibles de $\mathbb{Z}[i]$. D'après (4), p n'est pas inversible dans $\mathbb{Z}[i]$; le nombre r de facteurs est donc au moins

égal à 1. Si $r = 1$, alors p est irréductible. Sinon, p n'est pas irréductible, et

$$p^2 = \varphi(p) = \varphi(x_1) \cdots \varphi(x_r)$$

(d'après (1)), avec $\varphi(x_k) \in \mathbb{Z}$ pour tout k. L'unicité de la factorisation dans l'anneau $\mathbb{Z}$ montre que $r \leq 2$, et donc, que $r = 2$. p est donc le produit de deux éléments irréductibles $x_1 = a + bi$ et x_2 de $\mathbb{Z}[i]$. On a

$$p^2 = \varphi(p) = \varphi(x_1)\varphi(x_2)$$

avec $\varphi(x_i) \in \mathbb{N}$, $i = 1, 2$. Les x_i étant irréductibles, ils ne sont pas inversibles. Donc, d'après (4), $\varphi(x_i) \geq 2$, $i = 1, 2$. Leur produit est égal à p^2, donc (l'anneau $\mathbb{Z}$ est factoriel !) $\varphi(x_i) = p$, $i = 1, 2$. En particulier,

$$p = \varphi(x_1) = \varphi(a + bi) = a^2 + b^2$$

(6) On considère les possibles valeurs modulo 4 des nombres premiers. Evidemment, aucun nombre premier peut être congru à 0 mod 4. Par contre, il existe des nombre premiers congrus à 1 ou 3 mod 4. Le seul premier congru à 2 mod 4 est égal à 2.

(7) 2 n'est pas irréductible dans $\mathbb{Z}[i]$: $2 = (1 + i)(1 - i)$. D'après (5), $1 + i$ et $1 - i$ sont irréductibles. La même chose est vraie pour $-1 - i$ et $-1 + i$.

(8) Tout nombre premier p congru à 3 mod 4 est irréductible dans $\mathbb{Z}[i]$: sinon, d'après (5), on aurait une équation de la forme $p = a^2 + b^2$, avec $a, b \in \mathbb{Z}$. Mais les carrés dans $\mathbb{Z}$ sont congrus à 0 ou 1 mod 4, donc les sommes de deux carrés ne peuvent être congrues à 3 mod 4.

(9) On rappelle la formule de Wilson : pour tout nombre premier p,

$$(p - 1)! \equiv -1 \mod p$$

(TD !).

(10) Soit p un nombre premier congru à 1 mod 4. On montrera (voir ci-dessous) que p n'est pas irréductible dans $\mathbb{Z}[i]$.

(11) Les éléments irréductibles de $\mathbb{Z}[i]$ sont les suivants :

(α) $\pm 1 \pm i$.

(β) $\pm p$, $\pm pi$, pour les nombres premiers p congrus à 3 mod 4.

(γ) $a+bi$, $a, b \in \mathbb{Z}$ tels que $a^2+b^2 = p$, pour les nombres premiers p congrus à 1 mod 4.

(12) Il reste à démontrer l'énoncé (10) : un nombre premier p congru à 1 mod 4 n'est pas irréductible dans $\mathbb{Z}[i]$: d'après (9), on a modulo p :

$$-1 \equiv (p-1)! \equiv \left(1 \cdot 2 \cdots \frac{p-1}{2}\right) \left((p - \frac{p-1}{2}) \cdot (p - \frac{p-3}{2}) \cdots (p-1)\right)$$

ce qui est congru à

$$(-1)^{\frac{p-1}{2}} \left(1 \cdot 2 \cdots \frac{p-1}{2}\right)^2$$

modulo p. Le nombre p étant congru à 1 mod 4, $\frac{p-1}{2}$ est pair, donc $(-1)^{\frac{p-1}{2}} = 1$. Posant $m := (\frac{p-1}{2})!$, on trouve au total que

$$m^2 \equiv -1 \mod p$$

Donc : $p \,|\, (m^2+1) = (m+i)(m-i)$; ceci est une relation de divisibilité dans $\mathbb{Z}[i]$. Cet anneau étant principal, donc factoriel, on raisonne comme suit : si p était irréductible dans $\mathbb{Z}[i]$, alors p diviserait $m+i$ ou $m-i$. Donc, l'un des nombres $\frac{m}{p} \pm \frac{i}{p}$ appartiendrait à $\mathbb{Z}[i]$, ce qui est absurde.

D'après (5), il existe donc $a, b \in \mathbb{Z}$ tels que $p = a^2+b^2$, et que $\pm a \pm bi \in \mathbb{Z}[i]$ soient irréductibles. Donc : tout nombre premier congru à 1 mod 4 est la somme de deux carrés (entiers) !

Démonstration du Théorème 14.7. Soit A un anneau Euclidien, avec $\varphi : A - \{0\} \to \mathbb{N}$ comme dans la Définition 14.2. Soit I un idéal. S'il n'y a pas d'éléments non-nuls dans I, il s'agit de l'idéal engendré par 0, ce qui est principal. S'il y en a, l'ensemble

$$M := \{\varphi(x) \,|\, x \in I - \{0\}\} \subset \mathbb{N}$$

n'est pas vide. M admet un élément minimal, disons $\varphi(b)$, avec $b \in I - \{0\}$. On montrera que b engendre I : soit en effet $a \in I$. D'après la division Euclidienne par rapport à φ, on trouve $q, r \in A$ tels que $a = qb+r$, et tel que soit $r = 0$, soit $\varphi(r) < \varphi(b)$. Mais $r = a - qb$ appartient à I, donc d'après le choix de b, $\varphi(r)$ ne peut être strictement plus petit que $\varphi(b)$. On en conclut que $r = 0$, c'est-à-dire, b divise a. Donc, $I = (b)$. **C.Q.F.D.**

On prépare la démonstration du Thórème 14.8.

Définition 14.14. Soit A un anneau commutatif. A est dit *Noethérien* (E. Noether, 1882–1935) si toute chaîne d'inclusions d'idéaux de A

$$I_1 \subset I_2 \subset I_3 \subset \ldots$$

devient stationnaire :

$$\exists\, k_0 \ , \ \forall\, k \geq k_0 \ , \ I_k = I_{k_0}$$

Lemme 14.15. *Tout anneau Noethérien et intègre admet la factorisation.*

Démonstration. Soit A un anneau Noethérien. Considérons le sous-ensemble

$$M := \{a \in A - (A^* \cup \{0\}) \,|\, a \text{ n'est pas un produit d'éléments irréductibles}\}$$

de A. Il s'agit de montrer que $M = \emptyset$. Supposons que $M \neq \emptyset$: $x \in M$. Donc, x ne peut être irréductible. On trouve alors $x', x'' \in A$ non-inversibles, et tels que $x = x'x''$. On a $x' \in M$ ou $x'' \in M$, disons : $x' \in M$. Posons $x_0 := x$, $x_1 := x'$. On a

$$(x_0) \subset (x_1)$$

et cette inclusion est stricte — sinon, x'' serait inversible. On continue le raisonnement avec x_1 au lieu de x_0, pour obtenir une chaîne infinie d'inclusions strictes

$$(x_0) \subset (x_1) \subset (x_2) \subset \dots$$

ce qui est impossible dans un anneau Noethérien. **C.Q.F.D.**

Lemme 14.16. *Tout anneau principal est Noethérien.*

Démonstration. On suppose donnée une chaîne d'inclusions d'idéaux d'un anneau principal A

$$I_1 \subset I_2 \subset I_3 \subset \dots$$

Posons $I := \bigcup_k I_k$; on montre facilement que ceci est un idéal (voir la Proposition 13.9 (b)). Puisque A est principal, cet idéal est de la forme $I = (a)$, avec $a \in A$. Puisque $a \in \bigcup_k I_k$, on trouve un k_0 tel que $a \in I_{k_0}$. Donc,

$$(a) \subset I_{k_0} \subset I_{k_0+1} \subset \dots \subset I = (a)$$

et toutes ces inclusions sont des égalités. **C.Q.F.D.**

Donc, tout anneau principal admet la factorisation. Il reste à montrer qu'elle est unique. Pour cela, l'ingrédient central est le suivant :

Lemme 14.17 (Lemme d'Euclide)**.** *Soient A un anneau principal, $x \in A$ irréductible, et $u, v \in A$ tels que $x \,|\, uv$. Alors, $x \,|\, u$ ou $x \,|\, v$.*

Démonstration. On considère l'idéal (x), et l'anneau quotient $A/(x)$. Dire qu'un élément de A est divisible par x revient à dire qu'il appartient à (x), ou encore, que sa classe dans le quotient $A/(x)$ est nulle.

Il s'agit donc de montrer que $K := A/(x)$ est intègre. En fait, on montrera même : K est un corps. Pour cela, notons π l'épimorphisme canonique de A vers K. Soit $\tilde{I} \neq K$ un idéal de K. D'après la Proposition 13.21, sa préimage $I := \pi^{-1}\tilde{I}$ est un idéal de A différent de A, et contenant (x). Puisque A est principal, I est de la forme $I = (y)$. $y \in A$ n'est pas inversible (car $I \neq A$), et y divise x (car $x \in I$) : $x = zy$. x étant irréductible, z est inversible, c'est-à-dire $y \sim x$. Donc, $I = (y) = (x)$, et l'idéal de départ $\tilde{I}$ est égal à $\{0\}$.

Donc, $\{0\}$ est le seul idéal de K qui n'est pas égal à K. Soit $k \in K - \{0\}$. L'idéal (k) n'étant pas nul, il est donc égal à K. Donc, $1 \in (k)$, c'est-à-dire on trouve $k' \in K$ tel que $kk' = 1$. **C.Q.F.D.**

Démonstration du Théorème 14.8. Soit donc A un anneau principal. D'après les Lemmes 14.15 et 14.16, A admet la factorisation. Soit

$$x_1 \cdots x_r = y_1 \cdots y_s$$

une identité entre produits d'éléments irréductibles dans A. Il faut montrer que $r = s$, et que $x_i \sim y_{\sigma(i)}$ pour une permutation $\sigma \in \mathfrak{S}_r$. Supposons que

$r \leq s$. On fait une récurrence sur r. Si $r = 1$, alors $x_1 = y_1 \dots y_s$. Aucun des y_j étant inversible, on a forcément $s = 1$ et $x_1 = y_1$. Supposons alors $r \geq 2$. x_1 divise $x_1 \dots x_r = y_1 \dots y_s$, donc d'après le Lemme d'Euclide, il divise l'un des facteurs y_j : $\exists\, u \in A$, $y_j = ux_1$. y_j est irréductible, et x_1 n'est pas inversible, donc u est inversible, ce qui montre que $x_1 \sim y_j$, et également, que

$$x_2' \dots x_r = y_1 \dots y_{j-1} y_{j+1} y_s$$

avec $x_2' := u^{-1}x_2 \sim x_2$. On applique alors l'hypothèse de récurrence.

C.Q.F.D.

Exemple 14.18. L'anneau $\mathbb{Z}[X]$ n'est pas principal : sinon, on pourrait appliquer l'Identité de Bézout à l'idéal $(2, X)$ engendré par (le nombre entier) $2 = 2X^0 \in \mathbb{Z}[X]$ et la variable X. Soit $f \in \mathbb{Z}[X]$ un diviseur commun de 2 et de X. Le degré de f est alors égal à 0 (puisqu'il est inférieur ou égal à celui de 2), c'est-à-dire f est un polynôme constant $f = n \in \mathbb{Z} \subset \mathbb{Z}[X]$. n doit diviser X dans $\mathbb{Z}[X]$, donc $n = \pm 1$. Les seuls diviseurs communs de 2 et de X sont donc les polynômes constants 1 et -1. Donc, $1 = pgcd(2, X)$.

Si l'Identité de Bézout était valable dans $\mathbb{Z}[X]$, on trouverait donc $g, h \in \mathbb{Z}[X]$ tels que

$$2g + Xh = 1$$

Le polynôme Xh n'a pas de coéfficient constant. Donc, si $g = \sum_n a_n X^n$, avec $a_n \in \mathbb{Z}$, on aurait $2a_0 = 1$, ce qui est absurde puisque 2 n'est pas inversible dans $\mathbb{Z}$.

$\mathbb{Z}[X]$ n'est donc pas un anneau principal. Mais il est factoriel, grâce au résultat suivant :

Théorème 14.19. *Soit A un anneau factoriel. Alors, l'anneau $A[X]$ est factoriel.*

On admet ce résultat (attendre l'an prochain pour la démonstration). Par récurrence, on en déduit :

Corollaire 14.20. *Soit A un corps, ou un anneau principal, ou un anneau factoriel. Alors, pour tout entier $n \geq 1$, l'anneau $A[X_1, X_2, \dots, X_n]$ est factoriel.*

Exemples 14.21. (a) Soit A un anneau commutatif et intègre. On peut montrer que $A[X]$ est principal si et seulement si A est un corps (auquel cas $A[X]$ est donc même Euclidien). Ceci donne un autre exemple d'un anneau factoriel qui n'est pas principal : $K[X_1, X_2]$, pour tout corps commutatif K.
(b) Il existe des anneaux principaux qui ne sont pas Euclidiens. En fait, on peut les trouver parmi les anneaux "arithmétiques" (i.e., ceux qui sont des "extensions finies" de $\mathbb{Z}$ dans $\mathbb{C}$, comme $\mathbb{Z}[\sqrt{-5}]$ ou $\mathbb{Z}[i]$). Mais il n'est pas facile de montrer que (1) un anneau donné n'est pas Euclidien (s'il est

principal...), (2) un anneau donné est principal (s'il n'est pas Euclidien...). Pour donner un exemple, l'anneau

$$\mathbb{Z}[\frac{1+\sqrt{-19}}{2}] := \{a + b\frac{1+\sqrt{-19}}{2} \,|\, a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

est principal. Mais il n'est pas Euclidien. Voir l'an prochain (deuxième semestre).

15 Le corps des fractions

On fixe un anneau commutatif et intègre A. Rappelons la Proposition 12.8 : pour $a, x, y \in A$, avec $a \neq 0$, la relation $xa = ya$ implique $x = y$. Cette observation sera utilisée par la suite.

On considère le produit cartésien

$$A \times (A - \{0\})$$

ainsi que la relation

$$(a, b) \sim (c, d) :\Longleftrightarrow ad = cb$$

Lemme 15.1. *$\sim$ est une relation d'équivalence sur $A \times (A - \{0\})$.*

Démonstration. $(a, b) \sim (a, b)$ car $ab = ab$. Si $(a, b) \sim (c, d)$, alors $(c, d) \sim (a, b)$. Finalement, supposons que $(a, b) \sim (c, d)$, et que $(c, d) \sim (e, f)$. On a donc

$$ad = cb \quad \text{et} \quad cf = ed$$

On en conclut que

$$daf = adf = cbf = cfb = edb = deb$$

(car A est commutatif), donc $af = eb$, donc $(a, b) \sim (e, f)$. **C.Q.F.D.**

On définit l'ensemble $Frac(A)$ comme étant le quotient de $A \times (A - \{0\})$ par $\sim$. La classe de (a, b) est notée $\frac{a}{b}$.

Lemme 15.2. *(a) La loi interne de composition*

$$+ : Frac(A) \times Frac(A) \longrightarrow Frac(A) \ , \ \left(\frac{a}{b}, \frac{x}{y}\right) \longmapsto \frac{ay + xb}{by}$$

est bien définie.
(b) La loi interne de composition

$$\cdot : Frac(A) \times Frac(A) \longrightarrow Frac(A) \ , \ \left(\frac{a}{b}, \frac{x}{y}\right) \longmapsto \frac{ax}{by}$$

est bien définie.

Démonstration. (a) Supposons que $\frac{a}{b} = \frac{c}{d}$, et que $\frac{x}{y} = \frac{u}{v}$, c'est-à-dire que $ad = cb$, et que $xv = uy$. Il faut montrer que

$$\frac{ay + xb}{by} = \frac{cv + ud}{dv}$$

c'est-à-dire que $(ay + xb)dv = (cv + ud)by$:

$$(ay + xb)dv = adyv + xvbd = cbyv + uybd = (cv + ud)by$$

(b) Pareil, mais plus simple. **C.Q.F.D.**

Proposition 15.3. *Le triplet $(FracA, +, \cdot)$ est un corps commutatif.*

Démonstration. Les lois d'associativité, de distributivité et de commutativité sont vérifiées parce qu'elles valent dans A. Exemple :

$$\frac{a}{b}\left(\frac{c}{d}\frac{e}{f}\right) = \frac{a}{b}\frac{ce}{df} = \frac{ace}{bdf} = \frac{ac}{bd}\frac{e}{f} = \left(\frac{a}{b}\frac{c}{d}\right)\frac{e}{f}$$

Le neutre pour $+$ est $\frac{0}{1}$. L'opposé de $\frac{a}{b}$ est $\frac{-a}{b}$ car

$$\frac{a}{b} + \frac{-a}{b} = \frac{0}{b^2} = \frac{0}{1}$$

Le neutre pour $\cdot$ est $\frac{1}{1}$. Le triplet $(FracA, +, \cdot)$ est donc un anneau commutatif.

En fait, c'est un corps : $\frac{1}{1} \neq \frac{0}{1}$ car $1 \neq 0$ (A est intègre !), et tout $\frac{a}{b} \neq \frac{0}{1}$ admet un inverse : car $a \neq 0$, et

$$\frac{a}{b}\frac{b}{a} = \frac{ab}{ab} = \frac{1}{1}$$

C.Q.F.D.

Définition 15.4. $Frac(A) := (FracA, +, \cdot)$ est appelé le *corps des fractions* de l'anneau commutatif et intègre A.

Exemple 15.5. $Frac(\mathbb{Z}) = \mathbb{Q}$.

Il y a une application $\iota : A \to Frac(A)$ qui envoie a vers $\frac{a}{1}$. On voit facilement que c'est un homomorphisme d'anneaux. Puisqu'il est injectif, c'est un monomorphisme :

$$\iota : A \hookrightarrow Frac(A)$$

Via ι, on identifie A à un sous-anneau de $Frac(A)$. Donc : tout anneau commutatif et intègre est contenu dans un corps commutatif. En plus, $Frac(A)$ est le plus petit corps contenant A :

Théorème 15.6 (Propriété universelle du corps des fractions)**.**
Soient K un corps (non nécessairement commutatif), et

$$\alpha : A \hookrightarrow K$$

un monomorphisme d'anneaux. Alors, il existe une unique application

$$\beta : Frac(A) \longrightarrow K$$

telle que $\alpha = \beta \cdot \iota$, et qui soit multiplicative :

$$\forall\, x, y \in Frac(A)\ ,\ \beta(xy) = \beta(x)\beta(y)$$

β est même un monomorphisme d'anneaux.

Démonstration. Il existe au plus une extension multiplicative β de α à $Frac(A)$: pour $\frac{a}{b} \in Frac(A)$, on a

$$\frac{a}{b} = \frac{a}{1}\frac{1}{b} = \iota(a)\iota(b)^{-1}$$

donc

$$\frac{a}{b}\iota(b) = \iota(a)$$

β doit respecter cette relation :

$$\beta(\frac{a}{b})\beta(\iota(b)) = \beta(\iota(a))$$

En plus, $\beta \cdot \iota = \alpha$, et donc,

$$\beta(\frac{a}{b})\alpha(b) = \alpha(a)$$

autrement dit,

$$\beta(\frac{a}{b}) = \alpha(a)\alpha(b)^{-1}$$

Pour voir que β existe, il faut montrer que cette dernière formule donne une application

$$Frac(A) \longrightarrow K$$

qui est bien définie. En fait, si $\frac{a}{b} = \frac{c}{d}$, alors $ad = cb$, donc $\alpha(ad) = \alpha(cb)$. Donc,

$$\alpha(bd)\alpha(a)\alpha(b)^{-1} = \alpha(bda)\alpha(b)^{-1} = \alpha(adb)\alpha(b)^{-1}$$

(car A est commutatif) est égal à

$$\alpha(ad)\alpha(b)\alpha(b)^{-1} = \alpha(ad) = \alpha(cb) = \alpha(cbd)\alpha(d)^{-1} = \alpha(bd)\alpha(c)\alpha(d)^{-1}$$

Au total,

$$\alpha(bd)\alpha(a)\alpha(b)^{-1} = \alpha(bd)\alpha(c)\alpha(d)^{-1}$$

et donc, $\alpha(a)\alpha(b)^{-1} = \alpha(c)\alpha(d)^{-1}$.

Des calculs similaires montrent que β est multiplicatif, et additif.

$\beta : Frac(A) \to K$ envoie $1 = \frac{1}{1}$ vers 1. Donc, c'est un homomorphisme d'anneaux entre deux corps. Mais un tel homomorphisme est toujours injectif : son noyau est un idéal de la source, donc soit $\{0\}$, soit tout le corps (Exemple 13.8 (c)). Mais il envoie 1 vers $1 \neq 0$, donc 1 n'appartient pas au noyau. **C.Q.F.D.**

Corollaire 15.7. *Soit A un corps commutatif. Alors,*

$$Frac(A) \cong A$$

Démonstration. D'après la propriété universelle de $Frac(A)$, l'identité $A \to A$ se prolonge vers un monomorphisme $Frac(A) \hookrightarrow A$. **C.Q.F.D.**

References

[G] G. Ginot, *Groupes et symétries*, polycopié du cours "Groupes et symétries" (L2, deuxième semestre 2020-21, Université Paris Nord).