Institut Galilée

Licence 3ème année

Algèbre 5

Semestre 5, 2025–2026

Table des matières

I. Théorie des groupes **3**

1. Groupes : définitions et premiers exemples . . . 3
2. Premières propriétés et table d'un groupe . . . 4
3. Groupes symétriques et diédraux . . . 5
4. Ordre d'un élément . . . 5
5. Sous-groupes . . . 6
6. Groupes engendrés, relations . . . 7
7. Morphismes de groupes . . . 9
8. Classes modulo un sous-groupe . . . 11
9. Groupes quotients . . . 13
10. Propriété universelle du groupe quotient . . . 15
11. Premier théorème d'isomorphisme . . . 15
12. Lemme chinois et un peu d'arithmétique . . . 16
13. Autres théorèmes d'isomorphisme . . . 19
14. Groupes abéliens . . . 20
15. Produits semi-directs . . . 20

II. Anneaux commutatifs **25**

1. Définition et premiers exemples . . . 25
2. Sous-anneaux, éléments inversibles . . . 26
3. Anneaux intègres, corps . . . 27
4. Morphismes et idéaux . . . 28
5. Idéaux engendrés, opérations sur les idéaux . . . 29
6. Anneaux quotients, théorèmes d'isomorphismes . . . 30
7. Produits direct, lemme Chinois . . . 31
8. Idéaux premiers, idéaux maximaux . . . 32
9. Divisibilité, anneaux euclidiens . . . 33
10. Anneaux principaux . . . 34
11. Éléments irréductibles et premiers . . . 35
12. PGCD et théorème de Bezout . . . 37
13. Arithmétique des anneaux euclidiens . . . 38
14. Anneaux factoriels . . . 38
15. Arithmétique des anneaux factoriels . . . 40

I. Théorie des groupes

1. Groupes : définitions et premiers exemples

Définition 1.1. Soit G un ensemble, et

$$\cdot : G \times G \longmapsto G$$

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 pour tout a, b, c dans G,

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

(2) *élément neutre* : il existe un élément e_G de G tel que

(2a) pour tout a dans G on a

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

(2b) *inverses* : pour tout a dans G, il existe un élément b de G tel que

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

Remarque 1.2.

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

ii. 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.

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

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.

Remarque 1.4. 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}.

Exemples 1.5.

i. Muni de l'addition, l'ensemble $\mathbb{Z}$ est un groupe (infini, abélien) d'élément neutre 0.

ii. Pour tout $n \geq 1$, le groupe $\mathbb{Z}/n\mathbb{Z}$ est fini, abélien.

iii. Pour tout ensemble X, l'ensemble $\mathfrak{S}(X)$ des bijections de X dans X, muni de la composition $\circ$ des applications, est un groupe. On dit que $\mathfrak{S}(X)$ est le *groupe symétrique* de X.

iv. Pour tout entier $n \geq 1$, l'ensemble $\mathrm{GL}_n(\mathbb{R})$ des matrices inversibles de taille n est un groupe, pour la multiplication matricielle.

Une des spécificités de la théorie des groupe est qu'elle propose de nombreux exemples très concrets, et parfois très exotiques. Pour l'assimiler et résoudre des exercices, il est essentiel de garder en tête et maîtriser quelques exemples. Tout au long de ce cours, nous illustrerons chaque nouvelle notion par des exemples pour éclairer la théorie : ne les négligez pas.

Exercice 1.6. Pour chaque axiome de la Définition 1.1, exhiber un contre-exemple.

Lemme 1.7. *Si $(G, \cdot)$ et $(G', *)$ sont deux groupes, le produit cartésien $G \times G'$ est muni naturellement d'une structure de groupe en accolant les lois respectives de G et G'. On parle alors du* produit direct *de G et G'.*

Démonstration. On pose $((x, y), (x', y')) \mapsto (x \cdot x', y * y')$, qui est bien une loi de composition interne associative, naturellement d'élément neutre $(e_G, e_{G'})$ et telle que $(x, y)^{-1} = (x^{-1}, y^{-1})$. □

Remarque 1.8. Plus tard, nous construirons à partir des lois de G et G' d'autres lois plus sophistiquées sur le produit cartésien $G \times G'$.

2. Premières propriétés et table d'un groupe

L'axiome d'associativité semble évident, mais nous avons vu précédemment qu'il n'est pas toujours garanti. Il est en réalité tout sauf anodin : sans lui, on ne peut pas même définir sereinement la puissance n-ième d'un élément.

Exercice 2.1. (À faire chez soi). On considère l'ensemble

$$\mathfrak{X} = \{x \in \mathbb{R},\ x > 0 \text{ et } x \neq 1\}.$$

Montrer que la formule $x * y = x^{ln(y)}$ définit une loi de composition interne sur $\mathfrak{X}$ qui est associative. Montrer que $(\mathfrak{X}, *)$ est un groupe.

Définition 2.2. Soit $(G, \cdot)$ un groupe, $a \in G$ 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 $a^{-k} := (a^{-1})^k$.

Remarque 2.3. En définissant ainsi les puissances (éventuellement négatives) d'un élément $g \in G$, on retrouve les identités habituelles des puissances.

Lemme 2.4. *L'élément neutre e_G d'un groupe G est unique (on rappelle que l'inverse d'un élément de G l'est aussi). Si a et b sont deux éléments de G, l'inverse de ab est $b^{-1}a^{-1}$.*

Démonstration. Si e et e' sont deux neutres, on a

$$e = ee' = e'.$$

On voit de plus aisément que $(ab)^{-1} = b^{-1}a^{-1}$. □

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

Exercice 2.5. 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* : $\forall a \in G,\ \exists\, b \in G,$

$$b \cdot a = e_G$$

Une façon parfois commode de représenter un groupe G fini est d'écrire sa table, c'est à dire d'élaborer un tableau qui représente totalement sa loi. Pour se faire, on choisit d'une part une expression de chaque élément du groupe (choix important, nous y reviendrons) et on place tous les produits possibles de ces éléments suivant la règle : à l'intersection de la "ligne g" et la "colonne g'", on trouve le produit gg'. Établissons-la pour le groupe $\mathbb{Z}/6\mathbb{Z}$. D'une part, on choisit le système de représentants classique donné par les restes de la division par 6, si bien que

$$\mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$$

et sa table est donnée par

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$						
$\bar{1}$						
$\bar{2}$						
$\bar{3}$						
$\bar{4}$						
$\bar{5}$						

La table d'un groupe permet d'en observer quelques propriétés (par exemple, on remarque qu'elle est ici symétrique par rapport à la diagonale car G est abélien). On remarque aussi que chaque élément apparaît une et une seule fois sur chaque lignes/colonnes.

3. Groupes symétriques et diédraux

Les groupes symétriques et diédraux sont deux exemples fondamentaux, qui nous suivront tout au long du cours.

Thème 3.1. (Rappels sur le groupe symétrique $\mathfrak{S}_n$).

Si X est un ensemble fini de cardinal n, on note généralement $\mathfrak{S}_n$ le groupe $\mathfrak{S}(X)$ de ses permutations. En notant $1, ..., n$ les éléments de X, on a pour habitude de représenter un élément $\sigma \in \mathfrak{S}_n$ par le tableau

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

où $\sigma(i)$ est l'image de i par σ, ou encore par la suite d'associations

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

Exercice 3.2. Montrer que le groupe $\mathfrak{S}_n$ est un groupe fini et déterminer son cardinal.

Définition 3.3. (k-cycles) Soit $2 \leq k \leq n$ un entier et $(i_1, ..., i_k) \in \{1, ..., n\}^k$ des entiers distincts.
On note $(i_1, ..., i_k)$ la permutation de $\mathfrak{S}_n$ déterminée par

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

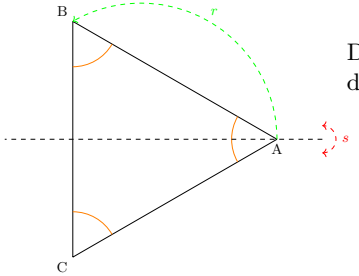
et qui laisse fixe les éléments hors de $\{i_1, ..., i_k\}$. Les éléments de cette forme sont les *k-cycles* de $\mathfrak{S}_n$. Les 2-cycles sont généralement appelés les *transpositions*.

Exercice 3.4. Déterminer la table de $\mathfrak{S}_3$.

Thème 3.5. (Isométries qui préservent un triangle régulier)
Soit $n \geq 2$ un entier et $\mathbb{U}_n = \{e^{\frac{2ik\pi}{n}}, k = 0, ..., n-1\}$ les racines n-ièmes de l'unité dans $\mathbb{C}$. On considère le groupe D_n des isométries affines de $\mathbb{C}$ (vu comme plan affinne sur $\mathbb{R}$) qui laissent $\mathbb{U}_n$ stable. En réalité, ces isométries laissent stable l'origine 0, donc on peut supposer ces isométries vectorielles. On pose donc

$$D_n := \{f \in \mathrm{O}(\mathbb{R}^2), f(\mathbb{U}_n) \subset \mathbb{U}_n\}.$$

Nous étudierons en détails D_n, mais commençons déjà par le cas $n = 3$: on considère le triangle régulier formé par les racines troisièmes de l'unité dans $\mathbb{C}$.



Deux des éléments de ce groupe diédral sont essentiels :

i. la rotation r d'angle $\frac{2\pi}{3}$;
ii. la symétrie s d'axe horizontal.

On montrera par la suite que D_3 possède 6 éléments, qui sont tous réalisés comme des compositions de puissances r et s. Déterminer sa table, qu'en conclure ?

4. Ordre d'un élément

Définition 4.1. Soient G un groupe, et $g \in G$. On considère le sous-ensemble de $\mathbb{N}^*$

$$N_g := \{n \in \mathbb{N}^*, g^n = e_G\}.$$

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*.

Proposition 4.2. *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 $n = o(g)$ et écrivons la division Euclidienne de n par m : $m = nq + r$, $q, r \in \mathbb{Z}$, $0 \leq r < n$. Alors,

$$e_G = g^m = g^{nq+r} = (g^n)^q g^r$$

et donc $e_G = g^r$, mais comme $0 \leq r < n$, on a $r \notin N_g$. Puisque r est positif on en conclut que $r = 0$ et n divise m. □

Exemples 4.3. i. Ordre des éléments dans $(\mathbb{Z}, +)$, dans $(\mathbb{R}^*, \times)$.

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

Exercice 4.4. Soit G un groupe.

i. Montrer que si $g \in G$, alors $o(g) = o(g^{-1})$.

ii. Montrer que si G est fini de cardinal n, alors l'ordre de tout élément de G est plus petit que n.

iii. Soit g et g' sont deux éléments de G qui commutent, d'ordres finis respectifs n et m premiers entre eux. Montrer que $o(gg') = ppcm(o(g), o(g'))$. Et si n et m sont quelconques ?

Thème 4.5 (Le groupe symétrique, II)**.**

Exercice 4.6. Déterminer l'ordre d'un k-cycle dans $\mathfrak{S}_n$.

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 $\mathfrak{S}_n$.

Exercice 4.7. Déterminer la décomposition en cycles à supports disjoints et l'ordre de la permutation σ suivante

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

5. Sous-groupes

Définition 5.1. Soit 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) $h_1 h_2 \in H$, pour tout h_1, h_2 dans H.

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

Exemples 5.2. i. Sous-groupes de $(\mathbb{Z}, +)$.

ii. Sous-groupe engendré par 1 élément.

Proposition 5.3. *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 5.1 (2), son inverse h^{-1} appartient à H. Grâce à 5.1 (1), le produit de h et de h^{-1} appartient à H donc l'élément neutre appartient à H. □

En particulier, l'axiome "H non-vide" de la Définition 5.1 peut être remplacé par "H contient l'élément neutre".

Corollaire 5.4. *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 bien définie et associative dans H car elle l'est déjà dans G. L'élément neutre de G appartient à H d'après 5.3 ; l'unique inverse dans G d'un élément de H appartient à H grâce à 5.1 (2). □

Dans ce cours, on va utiliser la notation $H \leq G$ (ou parfois $H < G$) pour dire que "H est un sous-groupe de G".

Proposition 5.5. *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 $H_1 \not\subset H_2$, on a donc un $h_1 \in H_1 \setminus H_2$. 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

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

□

Corollaire 5.6. *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 $<M>$.*

Démonstration. On considère $<M>=\bigcap_{M\subset H, H\leq G} H$. Ce sous-ensemble de G est non-vide, car l'intersection est non vide (prendre $H = G$) et car $M \subset <M>$. C'est en outre un sous-groupe de G par la Proposition précédente, naturellement le plus petit contenant M. □

On s'attèle maintenant à donner une définition "effective" du sous-groupe engendré par une partie d'un groupe G

Définition 5.7. Soient G un groupe, $A, B \subset G$ deux sous-ensembles. On pose

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

Proposition 5.8. *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 $k_i \in K$. $k_1 h_2 \in KH = HK$, donc $\exists\ h \in H, k \in K$ tel que $k_1 h_2 = hk$. 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 est bien un sous-groupe de G. □

6. Groupes engendrés, relations

On a précédemment élucidé le plus petit sous-groupe d'un groupe G qui contient un élément g. Généralisons cette description pour des (familles de) sous-ensembles arbitraires.

Notation 6.1. Etant donnés plusieurs sous-ensembles $M_1, M_2, M_3, \ldots$ d'un groupe G, on écrit généralement $<M_1, M_2, M_3, \ldots>$ en lieu et place $<M_1 \cup M_2 \cup M_3 \cup \ldots>$. On écrit aussi simplement $<a, b, c, \ldots>$ au lieu de $<\{a, b, c, \ldots\}>$.

Proposition 6.2. *Soit G un groupe, et $M \subset G$ un sous-ensemble de G. On pose*

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

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

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

Démonstration. Posons

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

H est un sous-groupe de G ; l'observation essentielle étant que l'inverse de $m_1 m_2 \cdots m_n$ 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 et donc $< M > \leq H$.

Soit $g = m_1 m_2 \cdots m_n \in H$. $\forall\ k, m_k \in M \cup M^{-1} \subset < M >$. Puisque $< M >$ est un groupe, $g \in < M >$. Donc : $H \leq < M >$. □

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. On considère l'élément neutre e_G, comme le "mot de longueur zéro".

Corollaire 6.3. *Soit G un groupe, et $M \subset G$. Supposons que tous les éléments de M commutent entre eux. Alors, le sous-groupe $< M >$ de G est abélien.*

Démonstration. Il s'agit de montrer que pour tout g et h dans $< M >$, $gh = hg$. Écrivons

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

avec $a_i, b_j \in M \cup M^{-1}$; ceci est possible grâce à 6.2. 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

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

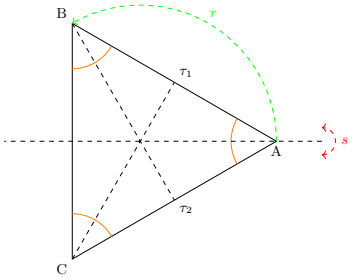
Inverser cette équation, pour obtenir $b_j a_k = a_k b_j$. □

Définition 6.4. Soit G un groupe et M un sous ensemble de G. si $< M >= G$, on dit que M engendre le groupe G. Si G est engendré par un seul élément g, on dit que G est monogène. Si g est deplus d'ordre fini, on dit que G est cyclique.

Exercice 6.5. Déterminer les générateurs de $\mathbb{Z}/n\mathbb{Z}$.

Thème 6.6. i. (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, montrer que les transpositions engendrent $\mathfrak{S}_n$. Suivant le problème considéré, certains générateurs sont être plus ou moins adaptés.

ii. (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. Montrer que l'on a

$$\tau_1 = r \circ s \text{ et que } \tau_2 = s \circ r.$$

On obtient donc

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

la rotation r et la symétrie s engendrent D_3 entier.

Remarquez que 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 élé-

ments 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".

iii. (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.

7. Morphismes de groupes

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

Définition 7.1. Soient $(G,\cdot)$, $(H,*)$ deux groupes. Une application

$$\alpha : G \longrightarrow H$$

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

$$\text{pour tous } g_1,\ g_2 \text{ dans } G, \quad \alpha(g_1 \cdot g_2) = \alpha(g_1) * \alpha(g_2)$$

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

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

Un morphisme d'un groupe G dans lui-même est un *endomorphisme*.

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 :

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

Remarque 7.2. On dit que G et G' sont deux groupes isomorphes (noté $G \simeq G$) s'il existe un isomorphisme de groupes $G \to G'$ (c'est à dire un morphisme de groupes bijectif).

Définition 7.3. On définit *l'image de* α comme

$$\mathrm{Im}\,\alpha := \{\alpha(g), g \in G\} \subset H$$

On définit le *noyau de* α comme

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

Exemples 7.4.
i. L'application déterminant définit un morphisme de groupes $GL_n(\mathbb{R}) \longrightarrow (\mathbb{R}^*,\times)$. Son noyau est le groupe $SL_n(\mathbb{R})$.
ii. Les deux projections $\pi_1 : G \times G' \longrightarrow G$ et $\pi_2 : G \times G' \longrightarrow G'$ sont des morphismes de groupes surjectifs, de noyaux respectifs isomorphes à G' et G.

Proposition 7.5. *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) Pour tout $g \in G$, $\alpha(g^{-1}) = \alpha(g)^{-1}$.

(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 $\ker\alpha = \{e\}$.

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 $x = y$.

□

Exercice 7.6 (Morphismes et ordre). Si $\alpha : G \longrightarrow H$ est un morphisme de groupes et $g \in G$, alors $o(\alpha(g))|o(g)$. Cela impose de sévères restrictions sur les morphismes entre deux groupes.

Exercice 7.7. Montrer qu'un morphisme $\alpha : G \longrightarrow G'$ est un isomorphisme si et seulement si α est bijective.

Thème 7.8. (Automorphismes intérieurs)
Soit G un groupe, et $x \in G$. On définit l'application

$$\begin{array}{rccc} int_x : & G & \longrightarrow & G \\ & g & \longmapsto & xgx^{-1} \end{array}$$

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

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

est un morphisme de groupes. Quel est son noyau ?

Remarque 7.9. Soient G un groupe, et $H \leq G$. Alors,

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

Thème 7.10. i. Étant donné un entier n strictement positif, on peut considérer la surjection

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

Cette application est un morphisme de groupes car elle est compatible avec l'addition dans $\mathbb{Z}$, et 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.

ii. (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 $\bar{1}$.

Exemple 7.11. Déterminer tous les morphismes de groupes $\alpha : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ et $\beta : \mathbb{Z}/n\mathbb{Z} \to (\mathbb{R}^*, \times)$.

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.

iii. (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

$$\varepsilon : \mathfrak{S}_n \longrightarrow \{\pm 1\}.$$

défini en décrétant que pour toute transposition τ, on a $\varepsilon(\tau) = -1$. Ce morphisme est appelé la signature et son noyau, noté $\mathfrak{A}_n$, est un groupe dit alterné.

8. Classes modulo un sous-groupe

Définition 8.1. Soient G un groupe, H un sous-groupe de G, et $g \in G$. On pose $gH := \{gh, h \in H\} \subset G$ et $Hg := \{hg, h \in H\} \subset G$. Le sous-ensemble gH est appelé la *classe à gauche de g modulo H*, et Hg est la *classe à droite de g modulo H*.

Exercice 8.2. Soient G un groupe, $x \in G$ et H un sous-groupe de G. On définit une application

$$\begin{array}{rccc} m_x : & H & \longrightarrow & xH \\ & h & \longmapsto & xh \end{array}$$

Alors, m_x est une bijection. En particulier H et xH ont même cardinal.

Proposition 8.3. *Soient G un groupe, et H un sous-groupe de G.*
(a)

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

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

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

En particulier $g_2 \in g_1H \Longrightarrow g_1H = g_2H$.
(c) Soient $g_1, g_2 \in G$. Alors,

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

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 $g_1H \cap g_2H \neq \emptyset$.

On voit donc bien que si $g_2 \in g_1H$, c'est à dire qu'on a $g_2 = g_1h$ pour un élément $h \in H$, alors bien entendu $g_2H \subset g_1H$, et réciproquement si $g_1h' \in g_1H$, alors $g_1h' = g_1hh^{-1}h' = g_2h^{-1}h' \in g_2H$. □

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

Corollaire 8.4. *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 $R \subset G$ tel que pour tout $g \in G$, $\mathrm{Card}(L \cap gH) = 1$ (on choisit un élément dans chaque classe modulo H). Alors on a la réunion disjointe*

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

Les classes à à gauche modulo H forment donc une partition de G.

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

Définition 8.5. 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 8.6.

i. Classes à gauche modulo un sous-groupe de $(\mathbb{Z}, +)$.

ii. (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 $\mathfrak{S}_n = \mathfrak{A}_n \sqcup \tau\mathfrak{A}_n$.

iii. (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. Comparer les cardinaux de G, des sous-groupes et des classes à gauches.

Remarque 8.7. 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

Théorème 8.8 (Lagrange)**.** *Soient G un groupe fini, et H un sous-groupe de G. Alors*

$$\mathrm{Card}(G) = \mathrm{Card}(H) \cdot [G : H]$$

En particulier, les nombres entiers $\mathrm{Card}(H)$ *et* $[G : H]$ *divisent* $\mathrm{Card}(G)$.

Démonstration. On fixe un système de représentants R pour les classes à gauche modulo H. D'après 8.4,

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

est une partition. Donc :

$$\mathrm{Card}(G) = \sum_{g \in R} \mathrm{Card}(gH),$$

D'après l'Exercice 8.2

$$\mathrm{Card}(G) = \sum_{g \in R} \mathrm{Card}(H) = \mathrm{Card}(H) \cdot \mathrm{Card}(L) = \mathrm{Card}(H) \cdot [G : H]$$

□

Corollaire 8.9. *Si G est un groupe fini, l'ordre de tout élément de G divise* $\mathrm{Card}(G)$.

Démonstration. L'ordre de $g \in G$ est égal au cardinal du sous-groupe $<g>$ engendré par g ; un diviseur de $\mathrm{Card}(G)$. □

Corollaire 8.10. *Si G est un groupe d'ordre un nombre premier, alors il est cyclique (donc abélien) et ses sous-groupes sont $\{e\}$ 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 $G \setminus \{e_G\}$ sont d'ordre p et engendrent G. Autrement dit si un sous-groupe de G contient un élément $g \neq e_G$, il contient $<g>= G$. □

9. 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. Il s'agit de munir l'ensemble des classes à gauche $\{g_1H, ..., g_nH\}$ modulo H d'une structure de groupe compatible avec celle de G, mais pour cela quelques restrictions sont nécessaires.

Définition 9.1. Soient G un groupe, et H un sous-groupe de G. On dit que H est un *sous-groupe distingué* de G (et on écrit $H \triangleleft G$) si pour tout élément g de G, on a $gHg^{-1} = H$.

Lemme 9.2. *Soit $\alpha : G \longrightarrow H$ un morphisme de groupes. L'image réciproque de tout sous groupe distingué $K \triangleleft H$ 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. □

Remarque 9.3.
i. L'image d'un sous-groupe distingué n'est en revanche pas toujours distinguée.
ii. 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.

Remarque 9.4. Bien entendu, si G est abélien alors tous ses sous-groupes sont distingués

Lemme 9.5. *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 $g^{-1}Hg \subset H$. □

Proposition 9.6. *Soient G un groupe, et H un sous-groupe de G. Les énoncés suivants sont équivalents :*

(a) H est distingué dans G.
(b) Pour tout $g \in G$, $gH = Hg$.
(c) Pour tout $(g_1, g_2) \in G^2$, $(g_1H)(g_2H) = (g_1g_2)H$.

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

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

(b) ⇒ (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) ⇒ (a) : On a $(gH)(g^{-1}H) = e_GH = H$ par hypothèse, donc gHg^{-1} est bien entendu contenu dans H. Le Lemme 9.5 indique alors que H est distingué. □

Thème 9.7. (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. Avez-vous d'autres exemples de groupes de Dedekind ?

Définition 9.8. Soient G un groupe, et H un sous-groupe de G. On pose $G/H := \{\text{classes à gauche modulo } H\}$, et donc $\mathrm{Card}(G/H) = [G : H]$.

Théorème 9.9. *Soient G un groupe, et H un sous-groupe de G.*

(a) La règle

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

définit une loi de composition $\cdot$ sur G/H qui le munit d'une structure de groupe. Son élément neutre est $e_GH \in G/H$, l'inverse de $gH \in G/H$ est $g^{-1}H$. On a de plus $\mathrm{Card}(G/H) = [G : H]$.

(b) L'application

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

est un morphisme de groupes surjectif, de noyau $\ker\pi = H$. *En particulier, π est un isomorphisme si et seulement si $H = \{e_G\}$.*

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

$$\begin{array}{ccc} G/H \times G/H & \longrightarrow & G/H \\ (g_1H, g_2H) & \longmapsto & (g_1g_2)H \end{array}$$

est bien définie. Autrement dit, il faut 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 9.6 (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 on a

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

(b) Prouvons d'abord que π est un morphisme. Ceci est encore la Proposition 9.6 (c). En effet, dire que π est un morphisme est équivalent à

$$\text{pour tous } g_1, g_2 \text{ dans } G, \quad (g_1g_2)H = (g_1H)(g_2H)$$

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

$$g \in \ker\pi \iff gH = eH \overset{8.3\ (b)}{\iff} g \in H$$

□

Définition 9.10. Dans la situation du Théorème 9.9, on appelle G/H le *groupe quotient de G par H*, et $\pi : G \longrightarrow G/H$ est la *surjection canonique (ou projection canonique) de G vers G/H.*

On fixe désormais H un sous-groupe distingué d'un groupe G et on note $\pi : G \longrightarrow G/H$ la surjection canonique associée. La Proposition suivante décrit tous les sous groupes de G/H à partir de ceux de G.

Proposition 9.11. *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.

□

10. Propriété universelle du groupe quotient

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

$$E/\sim \longrightarrow F$$

où $E/\sim$ est 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

$$\begin{array}{ccc} E/\sim & \longrightarrow & F \\ [x] & \longmapsto & f(x) \end{array}$$

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

Théorème 10.1 (Propriété universelle du groupe quotient)**.**
Soient G_1 un groupe, et H un sous-groupe distingué de G_1. On note π la surjection canonique de G_1 vers G_1/H. Soit G_2 un groupe.

(a) Soit $\alpha \in \mathrm{Hom}(G_1, G_2)$. Si $H \subset \ker\alpha$, 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 morphisme 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 morphisme $G_1/H \to G_2$ revient à la même chose que se donner un morphisme $G_1 \to G_2$ 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 8.3 (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 morphisme, on fait comme dans la preuve du Théorème 9.9.

(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

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

□

11. Premier théorème d'isomorphisme

Les groupes quotients sont fondamentaux et le résultat suivant, dont l'intérêt dépasse la théorie des groupes, est extrêmement utile pour les identifier.

Théorème 11.1. *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 $\alpha = \beta \circ \pi$. L'application β est un morphisme de groupes.

(b) β est injectif.

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

$$G_1/\ker\alpha \simeq \mathrm{Im}\,\alpha$$

Démonstration. (a) Ceci résulte de la propriété universelle 10.1 (a), appliquée à $H := \ker\alpha$. On a donc

$$\text{pour tout } g \text{ dans } G_1,\ \beta(g\ker\alpha) = \alpha(g)$$

(b) Prouvons que $\ker\beta$ est trivial : soit g un élément de 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) Par définition $\mathrm{Im}(\alpha) = \mathrm{Im}(\beta)$ donc $\beta : G_1/\ker\alpha \longrightarrow \mathrm{Im}(\alpha)$ est surjective. □

Définition 11.2. Dans la situation du Théorème 11.1, on appelle $G_1/\ker\alpha \simeq \mathrm{Im}\,\alpha$ *l'isomorphisme canonique entre* $G_1/\ker\alpha$ *et* $\mathrm{Im}\,\alpha$.

Lemme 11.3. *Soit $K \leq H \leq G$. Si K est distingué dans G, le noyau de la surjection canonique $\pi_H : H \longrightarrow G/K$ est égal à K. D'après le Théorème 11.1, π_H induit un morphisme injectif*

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

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

Démonstration. Notons d'abord que $K \triangleleft H$ car $K \triangleleft G$. On utilise 9.9 (b) et 7.4 (b) pour le premier et le dernier énoncé. Par construction, l'image de $H/K \to G/K$ est $\pi(H)$. □

Exemples 11.4. i. Soit G un groupe, $g \in G$ et

$$\begin{array}{rccc} \gamma_g : & \mathbb{Z} & \longrightarrow & G \\ & i & \longmapsto & g^i \end{array}$$

le morphisme $\mathbb{Z} \longrightarrow G$ donné par $\gamma_g(1) = g$. Par définition, on a

$$\mathrm{Im}\,\gamma_g = \{g^i \in G, i \in \mathbb{Z}\} \subset G$$

donc $\mathrm{Im}\,\gamma_g = < g >$ 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 est donc de la forme $n\mathbb{Z}$, 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

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

On retrouve donc l'alternative précédente : 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 et $< g > \simeq \mathbb{Z}$;
— 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.

12. Lemme chinois et un peu d'arithmétique

Les deux exemples suivants montrent que les produits directs de groupes cycliques peuvent être de différente nature.

Exemples 12.1. (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 toutefois pas cyclique, puisque tous ses éléments sont d'orde 2 :

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

Il n'y a donc pas d'élément d'ordre 4 dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(b) Le produit direct $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ (abélien d'ordre 6) est lui cyclique : en effet l'élément $z_0 := (\bar{1}, \bar{1}) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ est d'ordre 6 car

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

Le lemme Chinois suivant explicite ce phénomène.

Théorème 12.2 (Lemme chinois)**.** *Soient m, n deux entiers strictement positifs et premiers entre eux. On a un isomorphisme*

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

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 abéliens 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 $(\bar{1}, \bar{1})$ est donc d'ordre mn et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est cyclique.

Preuve 1' : En notant $z_0 = (\bar{1}, \bar{1})$, on considère le morphisme associé

$$\begin{array}{rccc} \gamma_{z_0} : & \mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ & k & \longmapsto & (\bar{k}, \bar{k}) \end{array}$$

Déterminons le noyau de γ_{z_0} : si $k \in \mathbb{Z}$,

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

En particulier mn divise i car m et n sont premiers entre eux. Donc, $\ker \gamma_{z_0} = mn\mathbb{Z}$ et le Théorème d'homomorphie implique que

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

Notons que $\operatorname{Im} \gamma_{z_0}$ a le même ordre que $\mathbb{Z}/mn\mathbb{Z}$, à savoir mn. Mais $\operatorname{Im} \gamma_{z_0} < \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, ce dernier groupe étant aussi d'ordre mn. On en conclut que $\operatorname{Im} \gamma_{z_0} = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ et l'isomorphisme escompté. □

Corollaire 12.3. *Soient $a, b, m, n \in \mathbb{Z}$, $m, n \geq 1$, $\operatorname{pgcd}(m, n) = 1$. 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 12.2 est surjectif. □

Corollaire 12.4. *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. □

Thème 12.5 (Groupe des inversibles, indicatrice d'Euler)**.**

i. Soit n un entier strictement positif. On considère le groupe $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$: en tant qu'ensemble,

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

Nous avons vu précédemment que

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{x} \in \mathbb{Z}/n\mathbb{Z}, \ \operatorname{pgcd}(x, n) = 1\}.$$

L'ensemble $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$ est un groupe dont l'élément neutre est $\bar{1}$ pour la multiplication

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

On obtient ainsi un groupe fini contenu dans $\mathbb{Z}/n\mathbb{Z}$, mais qui n'est pas un un sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$.

ii. Prenons $n = 5$. Alors,

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

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

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

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

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

iii. D'après la théorie des corps (que vous verrez peut-être 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

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

On a

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

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

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

Définition 12.6. *L'indicatrice d'Euler* est l'application

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

Exemple 12.7. On voit bien que, $\varphi(p) = p - 1$ si et seulement si p est premier (ou égal à 1).

Proposition 12.8. *Soit $n \in \mathbb{N}^*$, $x \in \mathbb{Z}$ tel que* $\mathrm{pgcd}(x, n) = 1$. *Alors $x^{\varphi(n)}$ est congru à 1 modulo n.*

Démonstration. Il faut montrer que $o(\bar{x})$, l'ordre de $\bar{x}$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$, divise $\varphi(n)$, ce qui est immédiat par le théorème de Lagrange. □

Corollaire 12.9 (Petit Théorème de Fermat)**.** *Soit p un nombre premier. Alors pour tout $x \in \mathbb{Z}$ on a $x^p \equiv x[p]$.*

Démonstration. Si p ne divise pas x, on sait d'après la Proposition 12.8 que $\bar{x}^{p-1} = \bar{1}$ et ainsi $\bar{x}^p = \bar{x}$. Si p divise x, $\bar{x}$ et $\bar{x}^p$ sont tous les deux nuls modulo p. □

Remarque 12.10. 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 12.11 (Théorème de Wilson)**.** *Un entier $n > 1$ est premier si et seulement si $(n-1)! \equiv -1[n]$.*

Démonstration. 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. □

Théorème 12.12. *Si m et n sont des entiers strictement positifs premiers entre eux, 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 $\mathrm{pgcd}(m, n) = 1$.

Démonstration. On considère la bijection

$$\begin{array}{rccc} \gamma : & \mathbb{Z}/mn\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ & \bar{k} & \longmapsto & (\bar{k}, \bar{k}) \end{array}$$

du Lemme chinois. Les inversibles respectifs de $\mathbb{Z}/mn\mathbb{Z}$, $\mathbb{Z}/m\mathbb{Z}$, et $\mathbb{Z}/n\mathbb{Z}$ sont caractérisés par les conditions $\mathrm{pgcd}(x, mn) = 1$, $\mathrm{pgcd}(x, m) = 1$, et $\mathrm{pgcd}(x, n) = 1$. Comme les m et n sont premiers entre eux on obtient

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

L'application γ induit ainsi 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 $\bar{k}$ vers $(\bar{k}, \bar{k})$. Donc, c'est un isomorphisme. □

Corollaire 12.13. *Soit $n \in \mathbb{N}_{\geq 1}$, $n = \prod_{p,n} p^{\alpha_p}$ sa factorisation en puissances de nombres premiers distincts. 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 12.12 permet alors de raisonner par récurrence sur le nombre de premiers dans la décomposition de n). On a

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

La condition $\text{pgcd}(x, p^\alpha) = 1$ équivaut au fait que p ne divise pas x, ce qui exclut $1/p$ des éléments de $\mathbb{Z}/p^\alpha\mathbb{Z}$. □

13. Autres théorèmes d'isomorphisme

Les deux autres théorèmes d'isomorphismes suivants sont des applications directes du Théorème 11.1.

Théorème 13.1 (Deuxième théorème d'isomorphisme)**.** *Soient G un groupe, $K \triangleleft G$ un sous-groupe distingué et $H \leq G$. Alors*

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

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

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

Démonstration. (a) Pour tout $h \in H$, on a $hK = Kh$ d'après la Proposition 9.6 (b), donc $HK = KH$ et HK est un sous-groupe de G par la Proposition 5.8. En outre comme K est distingué dans G et $K \leq HK$, on K est distingué dans HK.

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

(c) On considère la composition

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

de l'inclusion du sous-groupe H dans HK, et de la surjection 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 $k \in K$ et $\alpha(h) = hK = hkK$. 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 il reste à appliquer le premier Théorème d'isomorphisme. □

Remarque 13.2. En considérant le deuxième théorème d'isomorphisme dans le cas où H et K sont tous les deux finis, on obtient

$$\frac{\text{Card}(H)}{\text{Card}(H \cap K)} = \frac{\text{Card}(HK)}{\text{Card}(K)},$$

d'où $\text{Card}(HK) = \frac{\text{Card}(H)\text{Card}(K)}{\text{Card}(H \cap K)}$ (on peut aussi le montrer de manière élémentaire).

Théorème 13.3 (Troisième théorème d'isomorphisme)**.** *Soit G un groupe et H, K deux sous-groupes distingués de G tel que $K \leq H$. Alors*

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

Démonstration. Le noyau de la surjection 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, et on voit bien que α est surjectif. Déterminons son noyau $\ker\alpha$: soit $\pi : G \to G/K$ la surjection canonique. Pour $g \in G$,

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

Ceci montre que $\ker\alpha = \pi(H) \overset{11.3}{=} H/K$. Ainsi α est une surjection

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

de noyau H/K, et il reste à invoquer le premier Théorème d'isomorphisme. □

14. Groupes abéliens

On définit le produit direct $\prod_\alpha G_\alpha$ d'une famille arbitraire de groupes $(G_\alpha)_\alpha$ à la manière du Lemme 1.7.

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 morphismes injectifs, tandis que p_G et p_H sont surjectifs. Comme précédemment on remarque que via i_G et i_H, G et H s'identifient respectivement à des sous-groupes de $G \times H$, tous deux 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 et leur produit $i_G(G)i_H(H)$ est égal à $G \times H$. Le résultat suivant montre que réciproquement, on peut identifier avec ces propriétés un groupe comme produit direct de deux de ses sous-groupes.

Proposition 14.1. *Soit G un groupe, H et K deux sous-groupes distingués tels que $H \cap K = \{e\}$ et $G = HK$. Alors, l'application*

$$\begin{array}{rccc} \alpha : & H \times K & \longrightarrow & G \\ & (h, k) & \longmapsto & hk \end{array}$$

est un isomorphisme de groupes.

Démonstration. Montrons d'abord que sous nos hypothèses, les éléments de h et k commutent. 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. $hk = kh$.

Ainsi 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 enfin

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

Donc, α est un isomorphisme de groupes. □

Ce théorème est une première petite étape vers la *Classification des groupes Abéliens de type fini* (vous la démontrerez l'an prochain).

Théorème 14.2. *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, alors il existe des nombres premiers p_i (non nécessairement différents), et des entiers $\alpha_i \geq 1$ tels que

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

Exemple 14.3. Soit G un groupe abélien d'ordre p^2, où p est un nombre premier. D'après le Théorème 14.2, il n'y a que deux cas possibles :

i. soit G est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$,
ii. soit il est isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

On peut en réalité montrer que tous les groupes d'ordre p^2 sont abéliens ; on obtient ainsi tous les groupes d'ordre p^2 (ce n'est plus le cas dès p^3).

15. Produits semi-directs

Définition 15.1. 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) Pour tout $(g, h) \in G^2$ et $x \in E$,

$$g \cdot (h \cdot x) = (gh) \cdot x$$

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

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

Définition 15.2. Soient G, $(H, *)$ deux groupes,

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

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

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

Une action par des automorphismes de groupes sur H est une action, qui respecte la loi de composition interne de H.

Proposition 15.3. *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 pour tout $g \in G$,

$$g \cdot e_H = e_H$$

(b) Soit $h \in H$. Alors pour tout $g \in G$,

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

Démonstration. (a) D'après la définition $g \cdot e_H = (g \cdot e_H) * (g \cdot e_H)$, d'où $g \cdot e_H = e_H$.

(b) D'après la définition $(g \cdot h) * (g \cdot h^{-1}) = (g \cdot e_H) \overset{(a)}{=} e_H$, et ainsi $g \cdot h^{-1} = (g \cdot h)^{-1}$. □

Exemples 15.4. (a) L'action *triviale* de G sur H est donnée par $g \cdot h := h$, pour tout $(g, h) \in G \times H$. C'est une action de G par des automorphismes de groupes.

(b) Soit G un groupe non-trivial. Alors, l'action par multiplication à gauche de G sur lui-même $(g \cdot g' = gg')$ n'est pas une action de G par des automorphismes de groupes, car elle ne respecte pas l'élément neutre.

(c) Soit G un groupe. Alors, l'action par conjugaison $(g \cdot g' = gg'g^{-1})$ de G sur lui-même est une action de G par des automorphismes de groupes : en effet pour tout $(g, x, y) \in G^3$

$$g(xy)g^{-1} = (gxg^{-1})(gyg^{-1})$$

(d) Plus généralement, soient G un groupe et H un sous groupe distigué de G. Alors, G agit sur H par conjugaison :

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

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

Définition 15.5. Soient G, H deux groupes et

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

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

$$\begin{array}{ccc} (H \times G) \times (H \times G) & \longrightarrow & H \times G \\ ((h_1, g_1), (h_2, g_2)) & \longmapsto & (h_1(g_1 \cdot h_2), g_1 g_2) \end{array}$$

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 $H \rtimes_\cdot G$.

Exemple 15.6. Si $\cdot$ est l'action triviale (Exemple 15.4 (a)), on remarque que le produit semi-direct $H \rtimes_\cdot G$ n'est autre que le produit direct $H \times G$.

Proposition 15.7. *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

$$\begin{array}{rccc} i_G : & G & \longrightarrow & H \rtimes_\cdot G \\ & g & \longmapsto & (e_H, g) \end{array}$$

est un morphisme de groupes injectif.

(c) L'application

$$\begin{array}{rccc} i_H : & H & \longrightarrow & H \rtimes_\cdot G \\ & h & \longmapsto & (h, e_G) \end{array}$$

est un morphisme de groupes injectif. 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

$$\begin{array}{rccc} p_G : & H \rtimes_\cdot G & \longrightarrow & G \\ & (h, g) & \longmapsto & g \end{array}$$

est un morphisme de groupes surjectif de noyau est égal à $i_H(H)$.

Démonstration. Exercice. □

On a vu plus haut comment construire le produit semi-direct externe de deux groupes (relativement à une action). Tout comme on l'a fait précédemment pour le produit direct, il est possible d'exhiber des conditions suffisantes pour qu'un groupe G soit isomorphe au produit semi-direct de deux de ses sous-groupes H et K, où K agit sur H par conjugaison. On dit dans ce cas que G est le produit semi-direct interne de H et K (comparer avec la Proposition 14.1).

Proposition 15.8. *Soit G un groupe, H et K deux sous-groupes tels que $H \cap K = \{e\}$ et $G = HK$. On suppose de plus que H est distingué dans G. Considérons l'action par conjugaison*

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

Alors, l'application

$$\begin{array}{rccc} \alpha : & H \rtimes_\cdot K & \longrightarrow & G \\ & (h, k) & \longmapsto & hk \end{array}$$

est un isomorphisme de groupes.

Démonstration. On a pour tout $(h_1, k_1), (h_2, k_2) \in H \rtimes_\cdot K$:

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

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

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

et α est un morphisme, surjectif car d'image $HK = G$. De plus α est injectif car

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

□

Thème 15.9. i. (le groupe $\mathfrak{S}_n$, VI) La proposition 15.8 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

$$\mathrm{Card}(\mathfrak{A}_nK) = \mathrm{Card}(\mathfrak{A}_n) \cdot \mathrm{Card}(K) = n!.$$

par la Remarque 13.2. Le groupe $\mathfrak{S}_n$ s'écrit ainsi bien comme le produit semi-direct interne $\mathfrak{A}_n \rtimes \mathbb{Z}/2\mathbb{Z}$.

ii. (le groupe diédral, V) 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

$$\mathrm{Card}(HK) = \mathrm{Card}(H) \cdot \mathrm{Card}(K) = 2n,$$

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

iii. (Groupes de petit cardinal) On a désormais en main les outils qui permettent de déterminer (à isomorphisme près) tous les groupes finis de cardinal plus petit que 12.

II. Anneaux commutatifs

1. Définition et premiers exemples

Définition 1.1. Soit A un ensemble muni de deux lois de composition internes $+$ et $\cdot$. On dit que le triplet $(A, +, \cdot)$ est un *anneau (unitaire)* si les axiomes suivants sont satisfaits :

(1) $(A, +)$ est un groupe abélien.

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

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \text{ pout tous } a, b, c \in A$$

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

$$1 \cdot a = a = a \cdot 1 \text{ pour tout } a \in A$$

(4) On a

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

et

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \text{ pour tout } a, b, c \in A$$

L'axiome 1.1 (4) s'appelle la *loi de distributivité*. Un élément 1 comme dans l'axiome 1.1 (3) est appelé *élément neutre pour la multiplication*. On note 0 l'élément neutre pour l'addition $+$. Pour alléger la notation, on notera souvent ab au lieu de $a \cdot b$. Aussi, on parlera simplement de "l'anneau A" au lieu de "l'anneau $(A, +, \cdot)$".

Exemples 1.2. (a) Munis des additions et multiplications habituelles, les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ sont des anneaux.

(b) Un exemple pathologique : l'anneau nul $\{0\}$ formé. Il est caractérisé par le fait que $1 = 0$ et on l'excluera généralement dans la suite.

(c) Si I est un intervalle de $\mathbb{R}$, l'ensemble $\mathcal{F}(I, \mathbb{R})$ des fonctions de I dans $\mathbb{R}$ est un anneau, pour lequel l'élément neutre pour l'addition est la fonction identiquement nulle, et l'élément neutre multiplicatif est l'application constante égale à 1.

(d) Pour n un entier strictement positif, l'ensemble $M_n(\mathbb{R})$ des matrices carrées de taille n à coefficients dans $\mathbb{R}$, muni de l'adddition et de la multiplication des matrices, est un anneau. Les axiomes d'associativité et distributivité proviennent de ces mêmes propriétés, dans $\mathbb{R}$. L'élément neutre additif est la matrice nulle, tandis que l'élément neutre multiplicatif est la matrice identité.

Définition 1.3. Soit A un anneau. On dit que A est *commutatif* si $ab = ba$, pour tous a, b dans A.

Remarque 1.4. Les anneaux (a), (b) et (c) de la série d'exemples 1.2 sont commutatifs, contrairement à l'anneau (d) des matrices qui ne l'est pas. Dans ce cours, sauf mention du contraire, les anneaux seront toujours supposés commutatifs et non réduits à $\{0\}$: beaucoup de résultats pour les anneaux commutatifs ne subsistent pas dans le cadre non-commutatif.

Proposition 1.5. *Soit $(A, +, \cdot)$ un anneau.*

(a) L'élément neutre pour la multiplication est unique.

(b) Si a, b sont deux éléments de A, alors

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

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

Démonstration. (a) Si e et e' sont deux éléments neutres multiplicatifs, on a $e = e \cdot e' = e'$.

(b) On a $0 \cdot a + a = 0 \cdot a + 1 \cdot a = (0 + 1) \cdot a = a$ par distributivité, donc $0 \cdot a = 0$. La preuve est similaire pour $0 \cdot a$. On a ainsi

$$a \cdot (-b) + a \cdot b = a \cdot (-b + b) = a \cdot 0 = 0$$

et donc $a \cdot (-b) = -a \cdot b$ (même chose pour $(-a) \cdot b$). □

Thème 1.6 (Anneaux $\mathbb{Z}/n\mathbb{Z}$ et de polynômes)**.**

i. Soit $n \geq 1$ un entier. Comme vu précédemment l'ensemble $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, ..., \overline{n-1}\}$ est muni d'une structure de groupe via l'addition $\bar{x} + \bar{y} = \overline{x+y}$. On définit de même une multiplication par la formule

$$\bar{x} \cdot \bar{y} = \overline{xy}, \text{ pour tous } x, y \text{ dans } \mathbb{Z}$$

Cette multiplication est bien définie et munit $\mathbb{Z}/n\mathbb{Z}$ d'une structure d'anneau commutatif, dont le neutre additif est $\bar{0}$ et le neutre multiplicatif est $\bar{1}$. Notons que dans l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ les structures additives et multiplicatives sont étroitement liées.

ii. Soit A un anneau commutatif. On considère l'ensemble $A[X]$ des polynômes en une indéterminée à coefficients dans A, c'est à dire le polynôme nul, et l'ensemble des éléments de la forme $P = a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X + a_0$, avec $a_0, ..., a_n$ dans A avec $a_n \neq 0$ (formellement, on considère les suites à support fini de coefficients dans A). Munis des lois habituelles des polynômes (pour l'addition et la multiplication dans A), $(A[X], +\cdot)$ est un anneau commutatif, d'élément neutre additif le polynôme nul et d'élément neutre multiplicatif le polynôme constant 1_A.

Remarque 1.7. On peut en outre définir de manière similaire le degré $deg(P)$ d'un pôlynôme P en une variable à coefficients dans A, et les inégalités
— $deg(P+Q) \leq \max\{deg(P), deg(Q)\}$;
— $deg(PQ) \leq deg(P) + deg(Q)$.
Tout comme pour les polynômes à coefficients réels ou complexes deux polynômes sont égaux si et seulement s'ils ont même degré et même coefficients.

2. Sous-anneaux, éléments inversibles

Tout comme en théorie des groupes, on peut définir la notion sous-anneau d'un anneau A. Nous verrons par la suite que celle-ci s'avère peu intéressante en pratique.

Définition 2.1. Soit $(A, +, \cdot)$ un anneau. Un sous-anneau de A est une partie non-vide $B \subset A$ telle que

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

ii. B est stable par la multiplication $\cdot$, c'est à dire

$$x \cdot y \in B, \text{ pour tous } x, y \text{ dans } B.$$

iii. le neutre multiplicatif 1_A appartient à B.

Remarque 2.2. Si B est un sous-anneau de $(A, +, \cdot)$, alors $(B, +, \cdot)$ est un anneau avec pour neutres additifs et multiplicatifs $0_B = 0_A$ et $1_B = 1_A$.

Thème 2.3 (Entiers de Gauss)**.** L'ensemble $\mathbb{Z}[i]$ des entiers de Gauss est celui des nombres complexes dont les parties réelles et imaginaires sont toutes deux entières, c'est à dire

$$\mathbb{Z}[i] := \{a + ib \in \mathbb{C},\ (a, b) \in \mathbb{Z}^2\}.$$

Il s'agit clairement d'un sous-anneau de $\mathbb{C}$.
L'application

$$\begin{array}{rccc} N : & \mathbb{Z}[i] & \longrightarrow & \mathbb{Z} \\ & a + ib & \longmapsto & a^2 + b^2 \end{array},$$

qu'on appelle la *norme* dans $\mathbb{Z}[i]$, s'avèrera extrêmement utile dans la suite. Cette application est multiplicative (c'est à dire $N(xy) = N(x)N(y)$). On peut montrer cette propriété à la main ou en tirant parti du fait $\mathbb{Z}[i]$ est contenu dans $\mathbb{C}$.

Définition 2.4. Un élément a d'un anneau A est dit inversible (ou une unité) s'il existe un élément $b \in A$ tel que $ab = 1_A$. On note $A^\times$ l'ensemble des éléments inversibles de A.

Remarque 2.5. (a) L'élément neutre 1 est toujours bien entendu inversible, et il en va de même pour -1 par la Proposition 1.5. Si l'élement 0 est inversible, alors on a $b \in A$ tel que $0 = 0b = 1$ et A est l'anneau trivial.

(b) L'inverse d'un élément est unique (même preuve que pour l'unicité de l'inverse dans un groupe).

Proposition 2.6. *Si $(A, +, \cdot)$ est un anneau, alors $(A^\times, \cdot)$ est un groupe abélien d'élément neutre 1_A.*

Démonstration. L'élément neutre multiplicatif 1_A est en effet inversible et si x, y sont deux inversibles, alors leur produit xy admet pour inverse $y^{-1}x^{-1}$ et la multiplication définit bien une loi de composition interne pour $A^\times$. Si x est inversible, son inverse x^{-1} l'est bien entendu aussi et l'associativité découle de celle dans A. Ainsi $(A^\times, \cdot)$ est un groupe abélien (on rappelle que par défaut, A est un anneau commutatif). □

Exemple 2.7. (a) $\mathbb{Z}^\times = \{1, -1\}$.
(b) On a déterminé précédemment les inversibles de $\mathbb{Z}/n\mathbb{Z}$.
(c) $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$

3. Anneaux intègres, corps

Définition 3.1. Un anneau A non-nul est intègre s'il vérifie la propriété suivante :

pour tous éléments a, b dans A, $ab = 0 \Leftrightarrow a = 0$ ou $b = 0$.

Remarque 3.2. On dit aussi qu'un élément (non-nul) a d'un anneau A est un diviseur de zéro s'il existe $b \in A^*$ tel que $ab = 0$. Un anneau intègre est donc un anneau non-nul et sans diviseur de 0.

Exemple 3.3. (a) l'anneau $\mathbb{Z}$ est intègre.
(b) Quels sont les diviseurs de 0 dans $\mathbb{Z}/5\mathbb{Z}$? dans $\mathbb{Z}/6\mathbb{Z}$?

Proposition 3.4. *Soit A un anneau.*

i. Si A est intègre et P, $Q \in A[X]$, alors $deg(PQ) = deg(P) + deg(Q)$.

ii. A est intègre si et seulement si $A[X]$ est intègre.

Démonstration. i. Si P ou Q est nul, avec la convention $deg(0) = -\infty$, le résultat est vrai. Si P et Q sont non nuls de coefficients dominants a_n et b_m, alors le coefficient dominant de PQ est $a_n b_m$, puisque par intégrité cet élément est non-nul.

ii. La multiplication dans $A[X]$ étend celle de A (sur les constantes) donc bien entendu si $A[X]$ est intègre, A l'est aussi. Réciproquement si P et Q dont tels que $PQ = 0$, le point i) indique que P et Q ne peuvent être tous deux de degré strictement positif, on est donc ramenés à l'intégrité de A.

□

Corollaire 3.5. *Si A est un anneau intègre, alors $A[X]^\times = A^\times$.*

Démonstration. Par intégrité à nouveau, si P est inversible, alors il est non-nul et son degré ne peut être que 0. C'est ainsi une constante et les polynômes inversibles sont bien les polynômes constants, à coefficient dominant inversible. □

Proposition 3.6. *Si x, y, a sont trois éléments d'un anneau intègre A, avec a non-nul, alors $ax = ay \Rightarrow x = y$.*

Démonstration. En effet $ax = ay$ donne $a(x - y) = 0$ et par intégrité $x = y$. □

Définition 3.7. On dit qu'un anneau A est un corps (commutatif) si tous les éléments non-nuls de A sont inversibles.

Exemples 3.8. (a) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des corps.
(b) Le sous-ensemble de $\mathbb{C}$

$$\mathbb{Q}(i) = \{a + ib \in \mathbb{C}, (a, b) \in \mathbb{Q}^2\}$$

est un corps.
(c) Si p est un nombre premier, alors $\mathbb{Z}/p\mathbb{Z}$ est un corps.

Proposition 3.9. *Tout corps est un anneau intègre.*

Démonstration. Si A est un corps et $a \in A$ un diviseur de 0, alors a est inversible. On a donc un élément b non-nul tel que $ab = 0$, mais alors $b = a^1 ab = 0$, contradiction (un inversible ne divise pas 0). □

Remarque 3.10. Un anneau de polynômes $A[X]$ n'est jamais un corps.

Proposition 3.11. *Soit $n \geq 2$. On a*

$$(\mathbb{Z}/n\mathbb{Z} \text{ est intègre}) \Leftrightarrow (n \text{ est premier}) \Leftrightarrow (\mathbb{Z}/n\mathbb{Z} \text{ est un corps})$$

Démonstration. On a déjà vu que si n est premier, $\mathbb{Z}/n\mathbb{Z}$ est un corps ; il reste donc à montrer que si $\mathbb{Z}/n\mathbb{Z}$ est intègre, alors n est premier. Par contraposée : si n n'est pas premier, on a une décomposition non-triviale $n = ab$, si bien que $\bar{a}$ et $\bar{b}$ sont des diviseurs de 0. □

Théorème 3.12. *Un anneau A* fini *est intègre si et seulement s'il est un corps.*

Démonstration. Il s'agit de montrer qu'un anneau fini et intègre est un corps. Soit donc $a \in A^*$. La multiplication par a

$$\begin{array}{rccc} m_a : & A & \longrightarrow & A \\ & b & \longmapsto & ab \end{array}$$

est injective par intégrité, puisque par la Proposition 3.6, $ab = ab'$ implique $b = b'$. L'application m_a est une injection d'un ensemble *fini* dans lui-même ; c'est donc une bijection et par surjectivité il existe un élément a^{-1} tel que $aa^{-1} = 1_A$. On a donc $A^* = A^\times$ et A est un corps. □

4. Morphismes et idéaux

Définition 4.1. Soient A et B deux anneaux. Un morphisme d'anneaux de A dans B est une application $f : A \longrightarrow B$ tel que

i. $f : (A, +) \longrightarrow (B, +)$ est un morphisme de groupes (abéliens) ;

ii. $f(xy) = f(x)f(y)$, pour tous x, y dans A ;

iii. $f(1_A) = 1_B$.

$\mathrm{Hom}(A, B)$ est l'ensemble des morphismes d'anneaux de A vers B.

Remarque 4.2. (a) Si A' est un sous anneau de A et $f : A \longrightarrow B$ est un morphisme d'anneaux, alors $f(A')$ est un sous-anneau de B. En particulier l'image de f est un sous anneau de B.

(b) L'image réciproque d'un sous anneau de B est aussi un sous-anneau de A. En revanche, le noyau d'un morphisme d'anneaux $f : A \longrightarrow B$ n'est pas un sous-anneau de A (a moins que A ne soit trivial).

(c) La composée de deux morphismes d'anneaux est un morphisme d'anneaux.

(d) Puisqu'un morphisme d'anneaux $f : A \longrightarrow B$ est en particulier un morphisme de groupes, f est injectif si et seulement si son noyau est réduit à $\{0\}$.

(e) Si $f : A \longrightarrow B$ est un morphisme d'anneaux bijectif, alors f est un isomorphisme (l'application réciproque est elle aussi un morphisme d'anneaux).

Exemples 4.3.

i. Pour tout entier n strictement positif, la surjection canonique $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ est un morphisme d'anneaux.

ii. Si α est un réel, l'application d'évaluation

$$\begin{array}{rccc} & \mathbb{R}[X] & \longrightarrow & \mathbb{R} \\ & P & \longmapsto & P(\alpha) \end{array}$$

est un morphisme d'anneaux.

iii. L'application

$$\begin{array}{rccc} & \mathbb{C} & \longrightarrow & M_2(\mathbb{C}) \\ & a + ib & \longmapsto & \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \end{array}$$

est un morphisme d'anneaux.

iv. Si $k \neq 1$ la multiplication par k, $m_k : \mathbb{Z} \longrightarrow \mathbb{Z}$, n'est pas un morphisme d'anneaux.

Comme vu, le noyau d'un morphisme d'anneaux $f : A \longrightarrow B$ n'est pas nécessairement un sous-anneau de A. La notion adéquate et beaucoup féconde que celle de sous-anneau est celle d'*idéal*.

Définition 4.4. Soient $(A, +, \cdot)$ un anneau, et $I \subset A$. On dit que I est un *idéal* de A s'il vérifie les proppriétés suivantes :

i. $(I, +)$ est un sous-groupe de $(A, +)$;

ii. I est absorbant, c'est à dire pour tout $(a, i) \in A \times I$, $ai \in I$.

Remarque 4.5. (a) Tout anneau A possède deux idéaux triviaux : l'idéal nul $\{0\}$ et l'idéal A.

(b) Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, $n \in \mathbb{N}$.

Lemme 4.6. *Soit $f : A \longrightarrow B$ un morphisme d'anneaux.*

i. Le noyau de f est un idéal de A ;

ii. Plus généralement si J est un idéal de B, alors $f^{-1}(J)$ est un idéal de A.

iii. Pour tout idéal I de A, $f(I)$ est un idéal de l'anneau $Im(f)$ (attention, pas de B !).

Démonstration. i. L'application f étant un morphisme de groupes, $\ker(f)$ est un sous-groupe de A. En outre si $a \in A$ et $x \in \ker(f)$, alors $f(ax) = f(a)f(x) = 0$ et $\ker(f)$ est un idéal.

ii. L'image réciproque d'un sous-groupe est un sous-groupe. De plus si x appartient à $f^{-1}(J)$, alors pour tout $a \in A$,

$$f(ax) = f(a)f(x) \in J.$$

iii. D'une part $f(I)$ est un sous-groupe de $Im(f)$. De plus $f(I)$ est absorbant car si $b = f(i) \in f(I)$ et $b' = f(a) \in Im(f)$, alors on a $b'b = f(ia) \in f(I)$.

□

5. Idéaux engendrés, opérations sur les idéaux

De la même manière que pour les groupes, on introduit la notion d'idéal *engendré* par une partie d'un anneau A.

Proposition 5.1. *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. Similaires au cas des groupes. □

Définition 5.2. Si B est un sous-ensemble d'un anneau A, on note $< B >$ le plus petit idéal de A qui le contient ; on l'appelle l'idéal engendré par B. Concrètement, il s'agit de l'intersection de tous les idéaux de A qui contiennent B.

Remarque 5.3. À la manière des groupes on notera $< a >$, $< a, b >$... L'idéal engendré par un nombre fini d'éléments de A. Notez que la notation est la même pour le groupe engendré et l'idéal engendré dans ce cours ; il faudra donc prendre garde au contexte.

Exemples 5.4. (a) On obtient facilement la description de l'idéal engendré par un élément : si $x \in A$, alors

$$< x >= xA = \{xa, a \in A\}.$$

(b) On a $< x >= A$ si et seulement si x est inversible.

Définition 5.5. Soient A un anneau, et I, J deux idéaux de A.

(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

$$IJ = < \{xy \in A,\ x \in I,\ y \in J\} >$$

Proposition 5.6. *Soient I, J deux idéaux d'un anneau A.*

(a) L'idéal engendré par I et J est $I + J$; IJ est aussi un idéal de A.

(b) On a $IJ \subset I \cap J$.

Démonstration. (a) Le produit est clairement un idéal.

La somme $I + J$ est un idéal : d'une part elle contient $0 + 0 = 0$, et n'est donc pas vide. Si $x + y$ et $x' + y'$ deux éléments de $I + J$, leur somme $x + x' + y + y'$ est dans $I + J$ car I et J sont des sous-groupes et de même $-x - y \in I + J$, qui est donc un sous-groupe de A. De plus $I + J$ est clairement absorbant : si $a \in A$, alors $a(x + y) = ax + ay \in I + J$. Il s'agit donc bien d'un idéal, le plus petit qui contient I et J (tout tel idéal contient au moins les sommes d'éléments de I et J).

(b) En effet pour tous $(x, y) \in I \times J$, $xy \in I \cap J$ car I et J sont absorbant. □

Exemples 5.7. (a) On considère l'anneau $\mathbb{Z}$, et deux idéaux $n\mathbb{Z}$ et $m\mathbb{Z}$. Alors

$$n\mathbb{Z} \cap m\mathbb{Z} = \text{ppcm}(n, m)\mathbb{Z}$$

puisque $x \in n\mathbb{Z} \cap m\mathbb{Z}$ si et seulement si x est divisible à la fois par n et par m, c'est à dire si et seulement si $\text{ppcm}(m, n)$ divise x.

On a de plus

$$n\mathbb{Z} + m\mathbb{Z} = \text{pgcd}(n, m)\mathbb{Z}.$$

en effet $\subset$ car $\text{pgcd}(m, n)$ divise m et n, et $\supset$ découle de l'identité de Bezout. Enfin on a clairement $(n\mathbb{Z})(m\mathbb{Z}) = nm\mathbb{Z}$.

Proposition 5.8. *Soit A un anneau et I un idéal de A.*

i. $I = A \Leftrightarrow 1_A \in I$.

ii. A est un corps si et seulement si $\{0\}$ et A sont ses seuls idéaux.

Démonstration. i. Puisque I est absorbant, si $1_A \in I$, alors pour tout $a \in A$, $a = a \cdot 1_A \in I$.

ii. Si A est un corps et $J \subset A$ est un idéal non-nul, ce dernier contient un élément $a \in A$ non-nul, donc inversible. Comme J est absorbant il contient alors l'élément $1_A = a^{-1}a$ et donc $J = A$ par i.

□

Définition 5.9. On dit qu'un idéal I d'un anneau A est principal s'il est engendré par un élément, c'est à dire qu'il existe un élément $a \in A$ tel que $I = <a>$.

6. Anneaux quotients, théorèmes d'isomorphismes

Soit A un anneau et I un idéal de A. Puisque le groupe $(A, +)$ est abélien, le quotient A/I est naturellement lui-même un groupe abélien.

Théorème 6.1. *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 et $(A/I, +, \cdot)$ est un anneau. Son élément neutre pour la multiplication est $1 + I \in A/I$.

(b) La surjection canonique $\pi : A \longrightarrow A/I$ est un morphisme d'anneaux ; de plus $\ker \pi = I$.

Démonstration. Théorème 6.1 (a) Il s'agit avant tout de prouver que l'application

$$\begin{array}{ccc} A/I \times A/I & \longrightarrow & A/I \\ (a_1 + I, a_2 + I) & \longmapsto & (a_1 a_2) + I \end{array} ,$$

ce qui justifie l'introduction de la notion d'idéal. Si $a_1 + I = a_1' + I$ et $a_2 + I = a_2' + I$, alors $a_1 - a_1' \in I$ et $a_2 - a_2' \in I$. On a 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, $(a_1 a_2) + I = (a_1' a_2') + I$ et la multiplication est bien définie sur le quotient A/I.

Ainsi A/I est un groupe abélien, tandis que l'associativité, la distributivité et l'unité $1_A + I$ découlent directement des propriétés de A.

(b) On sait déjà que π est surjective, de noyau I d'après le cas des groupes. Il reste à observer que $\pi(1_A) = 1_A + I = 1_{A/I}$ et que d'après (a) on a bien pour tous a_1, a_2 dans A

$$\pi(a_1 a_2) = a_1 a_2 + I = (a_1 + I) \cdot (a_2 + I) = \pi(a_1) \cdot \pi(a_2).$$

□

La propriété universelle et le théorème d'isomorphisme se transmettent sans peine de la théorie des groupes à celle des anneaux, les idéaux jouant toujours le rôle des sous-groupes distingués.

Théorème 6.2 (Propriété universelle de l'anneau quotient)**.** *Soit A et B deux anneaux, et I un idéal de A. On note $\pi : A \longrightarrow A/I$ la surjection canonique.*

(a) Si $\alpha : A \longrightarrow B$ est un morphisme d'anneaux dont le noyau contient I, alors il existe une unique morphisme d'anneaux

$$\tilde{\alpha} : A/I \longrightarrow B$$

tel que $\alpha = \tilde{\alpha} \circ \pi$.

(b) L'assignation $\alpha \mapsto \tilde{\alpha}$ induit une bijection

$$\{\alpha \in \text{Hom}(A, B), I \subset \ker \alpha\} \xrightarrow{\sim} \text{Hom}(A/I, B).$$

Autrement dit : se donner un morphisme $A_1/I \to A_2$ revient à la même chose que se donner un morphisme $A_1 \to A_2$ qui est trivial sur I.

Démonstration. (a) La propriété universelle du groupe quotient montre l'existence et l'unicité de l'application $\tilde{\alpha}$, qui est définie par

$$\tilde{\alpha}(a+I) = \alpha(a).$$

Il est ainsi clair que $\tilde{\alpha}$ est un morphisme d'anneaux.

(b) Même preuve que pour les groupes. □

Théorème 6.3. *Soit $\alpha : A \longrightarrow B$ un morphisme d'anneaux et soit $\pi : A \longrightarrow A/ker(\alpha)$ la surjection canonique.*

(a) L'unique morphisme d'anneaux

$$\beta : A/\ker\alpha \longrightarrow B$$

telle que $\alpha = \beta \circ \pi$ est injectif.

(b) β induit un isomorphisme d'anneaux

$$A/\ker\alpha \simeq \operatorname{Im}\alpha$$

Démonstration. (a) Si $a \in A$ est tel que $\beta(a + \ker\alpha) = 0$, alors par définition de β on a $a \in ker(\alpha)$ donc sa classe est nulle dans $A/ker(\alpha)$.

(b) Même chose que pour les groupes. □

Thème 6.4 (Caractéristique d'un anneau)**.** Si A est un anneau, on peut toujours considérer l'application

$$\begin{array}{rccc} \varphi : & \mathbb{Z} & \longrightarrow & A \\ & k & \longmapsto & \underbrace{1_A + ... + 1_A}_{k \text{ fois}} . \end{array}$$

qui est un morphisme d'anneaux. Si φ est injectif, alors A contient un sous-anneau isomorphe à $\mathbb{Z}$. Sinon, $\ker\varphi$ est un idéal de $\mathbb{Z}$, donc de la forme $\mathbb{Z}/n\mathbb{Z}$ et d'après le premier théorème d'isomorphisme, φ induit donc une injection $\mathbb{Z}/n\mathbb{Z} \to A$. L'entier n est le plus petit k strictement positif tel que $k1_A = 0$. On l'appelle la caractéristique de l'anneau A.

Proposition 6.5. *Soient A un anneau, I un idéal de A et $\pi : A \longrightarrow A/I$ la surjection canonique. Un idéal de l'anneau quotient A/I est de la forme $\pi(J) = J/I$, pour un unique idéal J de A qui contient I.*

Démonstration. Déjà vu pour les groupes, il reste à observer que l'image réciproque (pour la projection canonique) d'un idéal de A/I est en effet un idéal de A. □

7. Produits direct, lemme Chinois

Tout comme pour les groupes, on peut définir le produit direct $A \times B$ de deux anneaux A et B, via $(a,b)\cdot(a',b') := (a \cdot_A a', b \cdot_B b')$.

Remarque 7.1. L'égalité $(1_A, 0_B)\cdot(0_A, 1_B) = (0_A, 0_B)$ implique que si A et B ne sont pas triviaux, le produit direct $A \times B$ n'est jamais intègre.

Théorème 7.2 (Lemme Chinois)**.** *Soit A un anneau et I, J deux idéaux de A tels que $I + J = A$. Alors,*

i. $IJ = I \cap J$;

ii. On a un isomorphisme d'anneaux

$$A/(I \cap J) \cong A/I \times A/J.$$

Démonstration.

i. On a toujours $IJ \subset I \cap J$. Réciproquement soit $x \in I \cap J$. Par hypothède on a deux éléments $i \in I$ et $j \in J$ tels que $i + j = 1$. En particulier $x = xi + xj$ est dans IJ puisque x est à la fois dans I et J.

ii. On applique le premier théorème d'isomorphisme à

$$\begin{array}{rccc} \alpha : & A & \longrightarrow & A/I \times A/J \\ & a & \longmapsto & (a+I, a+J) \end{array}$$

Déterminons le noyau de α : soit $a \in A$. Alors,

$$a \in \ker\alpha \Longleftrightarrow (a+I, a+J) = (0+I, 0+J) \in A/I \times A/J \Longleftrightarrow a \in I \cap J,$$

et donc $\ker\alpha = I \cap J$. Reste à monter que α est surjective, ce qui découle du fait que $I + J = A$. En effet si on fixe un couple $(a+I, b+J)$ de $A/I \times B/J$, on écrit $a = x + y$, $b = x' + y'$ avec $(x, x') \in I^2$ et $(y, y') \in J^2$. On voit alors que

$$\alpha(x' + y) = (x' + y + I, x' + y + J) = (y + I, x' + J) = (a + I, b + J)$$

et α est surjective.

□

On retrouve comme cas particulier le Lemme Chinois pour l'anneau $A = \mathbb{Z}$: comme vu précédemment, une condition équivalente au fait que $n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$ est que les entiers $m$et n soient premiers entre eux. Le Théorème correspond dans cette situation à l'isomorphisme d'anneaux

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

8. Idéaux premiers, idéaux maximaux

Définition 8.1. On dit qu'un idéal I d'un anneau A est propre, s'il n'est pas égal A.

Définition 8.2. Soit A un anneau et I un idéal de A.

i. On dit qu'un idéal I de A est premier si I et propre, et si pour tous éléments x, y dans A, $xy \in I \Rightarrow x \in I$ ou $y \in I$.

ii. On dit qu'un idéal I de A est maximal si I est propre, et s'il est maximal pour l'inclusion, c'est à dire

si $J \subset A$ est un idéal qui contient strictement I, alors $J = A$.

Remarque 8.3. Par définition, l'idéal $\{0\} \subset A$ est premier si et seulement si A est intègre, et maximal si et seulement si A est un corps.

Proposition 8.4. *Soit $f : A \longrightarrow B$ un morphisme d'anneaux. L'image réciproque $f^{-1}(J)$ d'un idéal premier de B est un idéal premier de A.*

Démonstration. On a vu précédemment que $f^{-1}(J)$ est un idéal, et puisque J est propre, on a $1_B \notin J$, donc $1_A \notin f^{-1}(J)$ car $f(1_A) = 1_B$, et ainsi $f^{-1}(J)$ est lui-aussi propre. Soient x, y dans A tels que $xy \in f^{-1}(J)$. Comme on a $f(xy) = f(x)f(y) \in J$, $f(x) \in J$ ou $f(y) \in J$ puisque J est premier. On a donc $x \in f^{-1}(J)$ ou $y \in f^{-1}(J)$. □

Remarque 8.5. (a) Le résultat de la proposition précédente ne vaut pas pour l'image directe (considérer par exemple la projection canonique $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$).

(b) La proposition précédente ne vaut pas pour les idéaux maximaux (considérer par exemple l'injection $\mathbb{Z} \longrightarrow \mathbb{Q}$).

Théorème 8.6. *Soit A un anneau et I un idéal de A.*

i. I est premier si et seulement si l'anneau quotient A/I est intègre ;

ii. I est maximal si et seulement si l'anneau quotient A/I est un corps ;

En particulier, tout idéal maximal est premier.

Démonstration. i. D'une part I étant propre, l'anneau A/I n'est pas trivial. On a de plus le fait qu'une classe $\bar{a}$ est nulle si et seulement si $a \in I$ donne

$$\begin{aligned} A/I \text{ intègre} &\iff \overline{xy} = 0 \Rightarrow \bar{x} = \bar{0} \text{ ou } \bar{y} = \bar{0}, \text{ pour tous } x, y \in A. \\ &\iff xy \in I \Rightarrow x \in I \text{ ou } y \in I, \text{ pour tous } x, y \in A. \\ &\iff I \text{ premier.} \end{aligned}$$

ii. On rappelle que comme vu précédemment, les idéaux de A/I sont les J/I, ou J est un idéal de A contenant I. On obtient alors

$$\begin{aligned} A/I \text{ est un corps} &\iff \text{les seuls idéaux de } A/I \text{ sont les idéaux triviaux.} \\ &\iff \text{les seuls idéaux de } A \text{ qui contiennent } I \text{ sont } I \text{ et } A. \\ &\iff I \text{ est maximal.} \end{aligned}$$

Comme nous l'avons vu précédemment, les corps sont des anneaux intègres, donc les idéaux maximaux sont premiers. □

Exemple 8.7. (a) Dans l'anneau $\mathbb{Z}$, $n\mathbb{Z}$ est premier si $n = 0$, ne l'est pas si $n = 1$ et si $n \geq 2$, alors

$$n\mathbb{Z} \text{ est premier} \iff n \text{ est premier} \iff n\mathbb{Z} \text{ est maximal.}$$

(b) Dans l'anneau $\mathbb{Z}[X]$, l'idéal engendré par le polynôme X est premier, sans être maximal.

Thème 8.8 (Théorème de Krull)**.** Nous allons maintenant avoir besoin du lemme de Zorn, un résultat important (et controversé !) des mathématiques qui vous sera très utile plus tard dans divers domaines des mathématiques. On le formule ici uniquement pour la relation d'ordre de l'inclusion (de sous-ensembles

dans un ensemble fixé).

Lemme 8.9 (Lemme de Zorn)**.** *Soit $\mathcal{X}$ un ensemble et soit $U = (\mathcal{U}_i)_{i\in\mathcal{I}}$ une famille non-vide de parties de $\mathcal{X}$. On suppose que toute chaine*

$$\mathcal{U}_{i_1} \subset \mathcal{U}_{i_2} \subset \mathcal{U}_{i_3} \subset ...$$

finie ou infinie d'éléments de U inclus les uns dans les autres admet un majorant (c'est à dire qu'il existe un élément $\mathcal{U}_{i_0} \in U$ qui les contient tous).
Alors U possède au moins un élément maximal (c'est à dire qui n'est contenu strictement dans aucun autre élément de U).

Théorème 8.10 (Théorème de Krull)**.** *Tout anneau A possède un idéal maximal.*

Démonstration. On rappelle qu'on a exclu le cas où A est l'anneau trivial. On applique le lemme de Zorn à l'ensemble

$$\mathcal{X}_A = \{\text{idéaux propres de } A\}$$

D'une part $\mathcal{X}_A$ est non-vide, car $\{0\}$ y figure. Étant donnée une chaîne

$$I_1 \subset I_2 \subset I_3 \subset ...$$

d'éléments de $\mathcal{X}_A$, on montre que $\mathcal{I} = \bigcup_{k\geq 1} I_k$ en est un majorant. Bien entendu, $\mathcal{I}$ contient tous les I_k, il s'agit donc de montrer que $\mathcal{I}$ est un élément de $\mathcal{X}_A$.

i. C'est un idéal de A : le neutre additif appartient à $\mathcal{I}$ et si x, y sont deux éléments de $\mathcal{I}$, alors il existe k_x, k_y des entiers tels que $x \in I_{k_x}$ et $y \in I_{k_y}$. La chaîne étant croissante, les deux appartiennent à $I_{\max(k_x,k_y)}$ et leur somme et inverse y figurent aussi. De même si $\mathcal{I}$ est clairement absorbant, puisque tout élément $x \in \mathcal{I}$ appartient à un idéal I_{k_x}.

ii. Il reste à montrer que $\mathcal{I}$ est propre : supposons maintenant par l'absurde que $\mathcal{I} = A$. On a alors $1_A \in \bigcup_{k\geq 1} I_k$, donc un entier $n \in \mathbb{N}^*$ tel que $1_A \in I_n$, mais cela contredirait que I_n est un idéal propre. L'idéal $\mathcal{I}$ est donc bien un élément de $\mathcal{X}_A$ et majore la chaîne de l'hypothèse.

En vertu du Lemme de Zorn, l'anneau A possède donc un idéal maximal. □

Corollaire 8.11. *i. Tout idéal propre I d'un anneau A est contenu dans un idéal maximal.*

ii. Tout élément a non-inversible d'un anneau A est contenu dans un idéal maximal.

Démonstration. i. On applique le théorème de Krull à l'anneau quotient A/I.

ii. Si a n'est pas inversible, alors l'idéal qu'il engendre est propre, et donc contenu dans un idéal maximal d'après *i.*

□

9. Divisibilité, anneaux euclidiens

Nous allons désormais introduire ds familles d'anneaux dont les propriétés approchent les propriétés arithmétiques des entiers. Vous connaissez les trois propriétés suivantes de l'anneau $\mathbb{Z}$:

i. l'anneau $\mathbb{Z}$ est muni de la *division euclidienne*

ii. la *relation de Bezout* lie deux entiers et leur pgcd.

iii. tout élément de $\mathbb{Z}$ s'écrit (au signe près) de manière unique comme un produit de nombres premiers.

Pour généraliser ces propriétés, nous allons donc introduire rigoureusement toutes les notions qui entrent en jeu dans un anneau quelconque : divisibilité, éléments "premiers", pgcd, division euclidienne, etc. Vous avez l'habitude d'utiliser indifféremment l'une ou l'autre de ces propriétés des entiers suivant le problème rencontré, mais nous verrons dans la suite que leurs trois analogues (anneaux euclidiens, anneaux principaux et anneaux factoriels) ne sont pas des notions équivalentes.

Définition 9.1. Soit A un anneau et x, y, deux éléments de A. On dit que x divise y (noté $x|y$) s'il existe un élément $a \in A$ tel que $y = ax$.

Proposition 9.2. *Pour tous éléments x, y d'un anneau A, on a*

$$x|y \iff <y> \subset <x>$$

Démonstration. On a $x|y$ si et seulement s'il existe $a \in A$ tel que $y = ax$, si et seulement si $y \in xA = <x>$, si et seulement si $<y> \subset <x>$. □

Thème 9.3 (Deux "divisions euclidiennes")**.** Vous avez rencontré précédemment deux exemples de divisions euclidiennes, dans l'anneau $\mathbb{Z}$ des entiers et l'anneau $K[X]$ des polynômes à coefficients dans un corps K.

Exemples 9.4. i. Soient a et b deux entiers, avec b non-nul. Alors il existe $q \in \mathbb{Z}$ et $r \in \mathbb{N}$ uniques tel que

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

ii. Soit K un corps et P_1, P_2 deux polynômes de $K[X]$, avec P_2 non-nul. Alors il existe $Q \in K[X]$ et $R \in K[X]$ uniques tel que

$$P_1 = QP_2 + R \text{ et } deg(R) < deg(P_2)$$

On le voit bien, ces résultats sont assez analogues : dans le cadre des polynômes, le degré joue le même rôle que la valeur absolue dans $\mathbb{Z}$. Notez que pour effectuer cette division euclidienne de P_1 par P_2, il suffit que le coefficient dominant de P_2 soit inversible. L'hypothèse "K est un corps" assure donc de pouvoir obtenir la division euclidienne par *tous* les polynômes non-nuls de $K[X]$.

Définition 9.5. Un anneau A est euclidien s'il vérifie les propriétés suivantes :

i. A est intègre.

ii. Il existe une application $\varphi : A^* \longrightarrow \mathbb{N}$ telle que

a) pour tous a, b dans A^*, $a|b \Rightarrow \varphi(a) \leq \varphi(b)$;

b) pour tous $a \in A$, $b \in A^*$, il existe $(q, r) \in A^2$ tel que

$$a = bq + r \text{ et } (r = 0 \text{ ou } \varphi(r) < \varphi(b)).$$

L'application φ est alors appelée un stathme euclidien et on dit que q et r sont le quotient et le reste de la division euclidienne de a par b dans A.

Exemples 9.6. (a) La valeur absolue et le degré sont des stasthmes euclidiens, respectivement pour l'anneau $\mathbb{Z}$ des entiers et $K[X]$ des polynômes à coefficients dans un corps. Nous construirons d'autres exemples de stathmes par la suite.

(b) La définition que nous avons choisie d'anneau euclidien n'impose pas l'unicité des quotients et restes.

10. Anneaux principaux

Définition 10.1. Un anneau A est dit principal s'il vérifie les propriétés suivantes :

i. A est intègre.

ii. Tout idéal de A est monogène.

Théorème 10.2. *Un anneau euclidien est principal.*

Démonstration. Notons φ le stathme associé à A. Comme A est intègre, il s'agit de montrer que tout idéal de A est engendré par un élément. Soit donc $I \subset A$ un idéal. Si $I = \{0\}$, il est bien monogène. Sinon notons

$$\mathbb{N}_I = \{\varphi(a),\ i \in I \setminus \{0\}\}.$$

il s'agit d'une partie non-vide de $\mathbb{N}$, on peut donc fixer un élément $x \in I$ non-nul dont l'image par φ est minimale dans $\mathbb{N}_I$. Sachant qu'on a bien sûr $< x > \subset I$, montrons qu'en réalité c'est une égalité : si $a \in I$, la division euclidienne de a par x est donnée par

$$a = qx + r \text{ avec } r = 0 \text{ ou } \varphi(r) < \varphi(x).$$

Puisque $r = a - qx$ est un élément de I, on ne peut pas avoir $\varphi(r) < \varphi(x)$ (l'image de x est minimale). On a donc $r = 0$ et x divise a, c'est à dire $I \subset <x>$ et I est monogène. □

On retrouve que les idéaux de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$ pour un entier n (notez que la preuve ci-dessus est plus ou moins similaire à la preuve vue dans le cadre des groupes). L'analogie vue précédemment entre l'anneau des entiers $\mathbb{Z}$ et celui des polynômes à coefficients dans un corps se traduit donc même au niveau des idéaux.

Corollaire 10.3. *Soit $K[X]$ l'anneau des polynômes à coefficients dans un corps K. Si I idéal est un idéal de $K[X]$, alors il existe un polynôme $P_I \in K[X]$ tel que*

$$I = P_I K[X] = \{P_I Q, Q \in K[X]\}.$$

Remarque 10.4. Le générateur P_I du corollaire précédent n'est bien sûr pas unique, tout comme on peut choisir n ou $-n$ comme générateur de $n\mathbb{Z}$. Nous verrons très vite comment caractériser ces générateurs.

Proposition 10.5. *Dans un anneau principal A tout idéal premier non-nul est maximal.*

Démonstration. Soit $I \subset A$ un idéal premier, engendré par un élément a (A est principal). Si $J =< b >$ est un idéal qui contient strictement I, alors on a $a \in < b >$, donc il existe un $x \in A$ tel que $a = xb$. Notons que comme I est premier, on a alors $xb \in I$ et ainsi $x \in I$ (car $J \neq I$). On écrit donc $x = ay$ pour un $y \in A$ et

$$a = xb = ayb,$$

d'où $a(1 - yb) = 0$ et par intégrité b est inversible puisque $I \neq \{0\}$. On a donc $J = A$ et l'idéal I est maximal. □

Thème 10.6 (Euclidien vs principal)**.** Un anneau euclidien est principal, mais la réciproque est fausse : il existe des exemples d'anneaux principaux, sans être euclidiens. Un exemple est donné par le sous anneau de $\mathbb{C}$

$$\mathbb{Z}[\omega] := \{a + \omega b,\ (a, b) \in \mathbb{Z}^2\} \text{ où } \omega = \tfrac{1+i\sqrt{19}}{2}.$$

La preuve de ce fait est accessible mais un peu longue et technique, nous ne la traiterons pas en cours.

Exercice 10.7. Soit $\mathbb{Z}[X]$ l'anneau des polynômes à coefficients dans $\mathbb{Z}$. On note I l'idéal engendré par les polynômes 2 et X.

i. Montrer que les polynômes constants 1 et -1 n'appartiennent à I.

Supposons maintenant par l'absurde que I est engendré par $P \in \mathbb{Z}[X]$.

ii. En utilisant que $2 \in I$, montrer que P est un polynôme constant.

iii. Montrer que $P \pm 1$. En déduire que $\mathbb{Z}[X]$ n'est pas principal.

Thème 10.8 (Anneaux de polynômes principaux/euclidiens)**.** On a vu précédemment que si K est un corps, l'anneau $K[X]$ est euclidien, et que l'anneau $\mathbb{Z}[X]$ n'est quant à lui même pas principal. Le résultat suivant montre qu'il n'existe en réalité pas de situation intermédiaire.

Théorème 10.9. *Soit A un anneau. Les conditions suivantes sont équivalentes.*

i. A est un corps.

ii. $A[X]$ est euclidien.

iii. $A[X]$ est principal.

11. Éléments irréductibles et premiers

Définition 11.1. Soit A un anneau intègre. On dit que deux éléments x, y de A sont associés si à la fois $x|y$ et $y|x$. On le notera $x \sim y$.

Proposition 11.2. *Pour deux éléments x, y d'un anneau intègre A, les conditions suivante sont équivalentes.*

i. x et y sont associés ;

ii. $< x >=< y >$;

iii. il existe un inversible $u \in A^\times$ tel que $x = uy$.

Démonstration. On a vu précédemment que $a|b$ si se seulement si b st un élément de $< a >$, l'équivalence $i. \Leftrightarrow ii.$ est donc évidente.

Si $x = uy$ pour un $u \in A^\times$, on a $x \in < y >$ et bien sûr $y \in < x >$ aussi puisque $y = u^{-1}x$, donc $ii.$ Réciproquement supposons que $< x >=< y >$. Si $x = 0$ le résultat est clair. Sinon on a deux éléments a, b de A tels que $x = ay$ et $y = bx$, donc $x = abx$. On obtient à nouveau $x(1 - ab) = 0$ et donc par intégrite que a et b sont inversibles, d'où $iii.$ □

Exemples 11.3. (a) Les inversibles de $\mathbb{Z}$ étant 1 et -1, deux entiers m et n sont associées si et seulement si $m = \pm n$.

(b) Si A est intègre, deux polynômes P et Q de $A[X]$ sont associés si et seulement s'il existe $a \in A^\times$ tel que $P = aQ$.

Remarque 11.4. Deux éléments associés ont les mêmes diviseurs.

Définition 11.5. Soit A un anneau intègre et x un élément de A.

i. On dit que x est irréductible s'il n'est pas inversible, et s'il vérifie :

si $x = ab$ dans A, alors a est inversible ou b est inversible.

ii. On dit que x est premier s'il n'est ni inversible, ni nul, et s'il vérifie :

si x divise ab dans A, alors x divise a ou x divise b.

Remarque 11.6. (a) Par définition, 0 n'est pas irréductible car $0 = 0 \cdot 0$.

(b) Un élément peut être irréductible dans un anneau A, mais ne plus l'être quand on étend l'anneau A. Par exemple tout nombre premier p est irréductible dans $\mathbb{Z}$, mais dans l'anneau des nombres rationneles $\mathbb{Q}$, p est inversible et donc pas irréductible.

Proposition 11.7. *Soit x un élément d'un anneau A intègre. On a :*

i. x est irréductible dans A si et seulement si $<x>$ est maximal parmi les idéaux monogènes de A ;

ii. x est premier dans A si et seulement si $<x>$ est un idéal premier de A, non-réduit à $\{0\}$.

Démonstration.

i. On sait que $<x> \subset <y> \Leftrightarrow y|x$. Si x est irréductible il n'est pas inversible donc $<x>$ est un idéal propre. D'autre part si $<x> \subset <y>$, alors il existe $a \in A$ tel que $x = ay$. Par irréductibilité, a est inversible ou y l'est. Dans le premier cas on a donc x et y associés, c'est à dire $<x> = <y>$ et dans le second $<y>$. L'idéal $<x>$ est donc maximal parmi les idéaux monogènes. La réciproque est similaire : si $<x>$ est maximal, x n'est pas inversible. De plus si on a $x = ab$, alors $x \in <a>$ donc par maximalité $<a> = A$ (et a est inversible) ou $<a> = <x>$, auquel cas a et x sont associés, c'est à dire b est inversible.

ii. D'une part si x est premier il n'est pas inversible ni nul donc $<x>$ ni propre ni nul, et réciproquement si $<x>$ est propre ou nul, x n'est pas inversible ni nul. De plus bien sûr

$$(ab \in <x> \Rightarrow a \in <x> \text{ ou } b \in <x>) \Longleftrightarrow (x|ab \Rightarrow x|a \text{ ou } x|b).$$

□

Corollaire 11.8. *Soit A est un anneau intègre.*

i. Tout élément associé à un élément irréductible est irréductible.

ii. Tout élément associé à un élément premier est premier.

Proposition 11.9. *Soit A un anneau intègre. Tout élément premier dans A est irréductible*

Démonstration. D'une part si x est premier il n'est pas inversible. De plus si $x = ab$, alors comme x est premier il divise, disons, a. On a donc

$$x = xa'b \text{ pour un élément } a' \in A$$

et ainsi $x(1 - a'b) = 0$. Par intégrité on obtient $a'b = 1$ et b est inversible. □

Thème 11.10 (Premier vs irréductible)**.** On a vu qu'un élément premier est irréductible, mais la réciproque est fausse.

Exercice 11.11. On considère

$$\mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5} \in \mathbb{C}, (a, b) \in \mathbb{Z}^2\}$$

et $N : \mathbb{Z}[i\sqrt{5}] \longrightarrow \mathbb{N}$ la norme donnée par $N(a+ib\sqrt{5}) = a^2+5b^2$.

i. Montrer que $\mathbb{Z}[i\sqrt{5}]$ est un anneau intègre.

ii. Montrer que $x \in \mathbb{Z}[i\sqrt{5}]$ est si et seulement s'il est de norme 1. En déduire que 3 n'est pas inversible dans $\mathbb{Z}[i\sqrt{5}]$.

iii. En observant que 3 divise $9 = (2+i\sqrt{5})(2-i\sqrt{5})$, montrer que 3 n'est pas premier.

On montre désormais que 3 n'est pas irréductible dans $\mathbb{Z}[i\sqrt{5}]$.

v. Soient x, y des éléments de $\mathbb{Z}[i\sqrt{5}]$ tels que $3 = xy$. Quelles sont les valeurs possibles de $N(x)$ et $N(y)$?

vi. Montrer que $\mathbb{Z}[i\sqrt{5}]$ ne possède pas d'élément de norme 3. En déduire que 3 est irréductible.

Proposition 11.12. *Dans un anneau principal, tous les éléments irréductibles sont premiers.*

Démonstration. Si x est irréductible, il n'est pas inversible et comme nous l'avons vu précédement il n'est pas nul non plus. D'après la Proposition 11.7 l'idéal $<x>$ est maximal parmi les idéaux monogènes, mais comme par hypothhèse A est principal il est ici simplement maximal. En particulier d'après le Théorème 8.6 $<x>$ est un idéal premier et x est premier par la Proposition 11.7. □

12. PGCD et théorème de Bezout

Définition 12.1. Soit A un anneau intègre et x, y deux éléments de A. On dit que x et y admettent un plus grand diviseur commun s'il existe un élément $d \in A$ tel que

d divise x, d divise y, si $a \in A$ qui divise x et y, alors a divise d.

On dit alors que d un pgcd de a et b.

Lemme 12.2. *Soit A un anneau intègre et x, y deux éléments de A admettant un* pgcd *noté d. Un élément $d' \in A$ est un* pgcd *de x et y si et seulement si d et d' sont associés.*

Démonstration. Si d et d' sont deux pgcd de x et y, alors par définition d' divise d (puisque $d'|x$ et $d'|y$)) et d divise d' (puisque $d|x$ et $d|y$)). Réciproquement si d' est associé à d, alors il divise x et y (puisque d les divise) et si d'' est un diviseur de x et y il divise d, donc d'. □

Remarque 12.3. (a) On dit que x et y sont premiers entre eux s'ils admettent 1_A comme pgcd. Le lemme précédent indique qu'alors l'ensemble des pgcd de x et y est $A^\times$.

(b) Puisque tout élément de A divise 0 on a $\text{pgcd}(x, 0) \sim x$. L'ensemble des pgcd de 0 et x correspond à l'ensemble des éléments associés à x.

(c) La définition du pgcd se généralise à un nombre fini d'éléments de A.

Proposition 12.4. *Soit A un anneau intègre et x, y deux éléments de A non-nuls qui admettent un* pgcd *d. Alors il existe x', y' deux éléments de A premiers entre eux tels que $x = dx'$ et $y = dy'$.*

Démonstration. On écrit $x = dx'$ et $y = dy'$ par définition du pgcd ; reste à montrer que x' et y' sont premiers entre eux. Si a est un diviseur de x' et y', alors da divise à la fois x et y, donc d. On obtient alors un élément $b \in A$ tel que $d = dab$, et $d(1 - ab) = 0$. Comme x et y ne sont pas nuls on a $d \neq 0$ et a est inversible, x' et y' sont premiers entre eux. □

Théorème 12.5. *Soit A un anneau principal. Tout couple (a, b) d'éléments de A admet un* pgcd. *Plus précisément, tout générateur de l'idéal $<a> + <b>$ est un pgcd de a et b, et réciproquement. Autrement dit,*

$$(d \text{ est un pgcd de } a \text{ et } b) \iff <a> + <b> = <d>.$$

Démonstration. Si a, b sont des éléments de A, alors $<a> + <b>$ est monogène, engendré par un élément d ; montrons qu'il s'agit d'un pgcd de a et b. D'une part $a \in <d>$ et $b \in <d>$ donc d divise à la fois a et b. D'autre part si d' divise a et b, alors $<a> \subset <d'>$, $<b> \subset <d'>$ donc

$$<d> = <a> + <b> \subset <d'>$$

et d' divise d. Réciproquement si d'' est un pgcd de a et b on a vu que d et d'' sont associés donc engendrent le même idéal. □

Théorème 12.6 (Théorème de Bezout)**.** *Soit A un anneau principal et a, b deux éléments de A.*

$$a \text{ et } b \text{ sont premiers entre eux} \iff \exists\ (u, v) \in A^2 \text{ tel que } au + bv = 1.$$

Démonstration. Comme vu précédemment a et b sont premiers entre eux si et seulement s'ils admettent 1 pour pgcd, c'est à dire si

$$<a> + <b> = A,$$

une condition équivalente à celle de l'énoncé. □

Corollaire 12.7 (Lemme de Gauss)**.** *Soit A un anneau principal. Si a, b et c sont des éléments de A, alors :*

$$a \text{ divise } bc \text{ et } a \text{ et } b \text{ premiers entre eux} \implies a \text{ divise } c$$

Démonstration. Si a et b sont premiers entre eux on a u, v dans A tels que $au + bv = 1$, d'où $au + bvc = c$. Comme a divise bc on a disons $ax = bc$, si bien que

$$c = au + bvc = au + avx = a(u + vx)$$

et a divise c. □

On définit un plus petit commun multiple de deux éléments x, y dans un anneau intègre A de façon très similaire aux pgcd. Un ppcm de x et y est un élément de A divisible par x, y, et qui divise tout autre élément vérifiant cette propriété.

Proposition 12.8. *Soit A un anneau principal et $(x, y) \in A^2$.*

i. Les éléments x et y admettent un ppcm*. Leurs* ppcm *sont éléments m de A tels que*
$$< x > \cap < y > = < m > .$$

ii. Si d et m sont des pgcd *et* ppcm *de x et y, alors xy et md sont associés.*

iii. Si x et y sont premiers entre eux, alors xy est un ppcm *de x et y.*

Démonstration. Exercice. □

13. Arithmétique des anneaux euclidiens

On a vu précédemment que l'existence des pgcd est assurée dans un anneau principal. Toutefois celle-ci n'est pas effective : il s'agit de trouver un générateur d'un certain idéal, un problème difficile. La situation est plus confortable pour les anneaux euclidiens, où l'on généralise sans peine l'algorithme d'Euclide de $\mathbb{Z}$.

Lemme 13.1. *Soit A un anneau euclidien de stathme $\varphi : A^* \longrightarrow \mathbb{N}$. Si a, b sont deux éléments de A avec b non-nul, et si $a = bq+r$ est la division euclidienne de a par b, alors* pgcd(a, b) *et* pgcd(b, r) *sont associés.*

Démonstration. Comme on a $a = bq + r$ on a $< a > \subset < b > + < r >$. Puisque bien entendu on a $< b > \subset < b > + < r >$ on obtient

$$< a > + < b > \subset < b > + < r > .$$

Le même raisonnement en partant de $r = a - bq$ montre que

$$< b > + < r > \subset < a > + < b >,$$

ainsi deux générateurs de ces idéaux (les pgcd qui nous intéressent) sont associés. □

Théorème 13.2 (Algorithme d'Euclide)**.** *Soit A un anneau euclidien de stasthme $\varphi : A^* \longrightarrow \mathbb{N}$. En effectuant les divisions euclidiennes successives*

$$\begin{aligned} a &= bq_1 + r_1 \text{ de } a \text{ par } b \\ b &= r_1 q_2 + r_2 \text{ de } b \text{ par } r_1 \\ r_1 &= r_2 q_3 + r_3 \text{ de } r_1 \text{ par } r_2 \\ &\dots \\ r_k &= r_{k+1} q_{k+2} + r_{k+2} \text{ de } r_k \text{ par } r_{k+1} \\ &\dots \end{aligned}$$

le dernier reste non-nul de ce processus est un pgcd *de a et b.*

Esquisse de la preuve. La suite des images des restes $\varphi(r_1)$, $\varphi(r_2)$, ... est strictement décroissante dans $\mathbb{N}$, jusqu'à stationner, disons au rang n (à partir de ce moment, on a nécessairement un reste nul, par définition du stasthme). En vertu du Lemme 13.1 on a

$$\text{pgcd}(a, b) \sim \text{pgcd}(b, r_1) \sim \text{pgcd}(r_1, r_2) \sim \cdots \sim \text{pgcd}(r_{n-1}, r_n) = r_{n-1}.$$

□

Exercice 13.3. Déterminer dans $\mathbb{Q}[X]$ un pgcd des polynômes

$$P = X^2 - X - 2 \text{ et } Q = X^5 - X^4 - 10X^3 + 10X^2 + 9X - 9.$$

14. Anneaux factoriels

Définition 14.1. On dit qu'un anneau A est factoriel s'il est intègre, et si tout élément $a \in A$ non-nul, non-inversible se décompose en un produit fini d'éléments irréductibles de A de façon unique, à l'ordre et au produit par un élément inversible près.
Concrètement, A est donc intègre et vérifie les deux axiomes suivants :

(A1) si $a \in A$ est non-nul, non-inversible, alors il existe $x_1, ..., x_n$ des éléments irréductibles de A tels que $a = x_1 \cdot ... \cdot x_n$.

(A2) si $a = y_1 \cdot ... \cdot y_m$ est une autre décomposition de a en un produit d'irréductibles de A, alors $m = n$ et il existe une permutation $\sigma \in \mathfrak{S}_n$ telle que pour tout $1 \leq i \leq n$, x_i et $y_{\sigma(i)}$ sont associés.

Ainsi de la même manière qu'on a "le" pgcd de deux éléments dans un anneau intègre, on parlera de "la" décomposition d'un élément dans un anneau factoriel, bien qu'elle ne soit définie qu'à multiplication par un inversible près.

Exercice 14.2. Observer la situation dans l'anneau $\mathbb{Z}$: quels sont les décompositions possibles d'un élément ?

Proposition 14.3 (Définition équivalente de la factorialité)**.** *Un anneau intègre A est factoriel si et seulement s'il vérifie l'axiome* (A1) *de la Définition 14.1 et l'axiome suivant*

(A2′) *Tout élément irréductible de A est premier.*

Démonstration. Supposons que A soit intègre, vérifie (A1), (A2) et soit $x \in A$ un élément irréductible. On a x non-nul, non-inversible. Supposons que $x|ab$ dans A, c'est à dire qu'il existe $y \in A$ tel que $xy = ab$.

— si a est inversible (resp. b est inversible), alors x divise b (resp. a), ce qu'il fallait démontrer.

— si a et b ne sont pas inversibles, on obtient avec leurs décompositions

$$a_1...a_n b_1...b_m = xy.$$

pour certains irréducibles $a_1, .., a_n, b_1, ...b_m$ de A. Par unicité (A2) de la décomposition de l'élément (non-inversible) xy, on obtient par exemple $x \sim a_i$ pour un entier $1 \leq i \leq n$ (resp. $x \sim b_j$ pour $1 \leq j \leq m$), auquel cas x divise a (resp. b).

Supposons maintenant que A intègre vérifie (A1) et (A2′). On fixe deux décompositions

$$x_1...x_n = x = y_1...y_m$$

d'un élément non-nul, non-inversible x de A, avec $n \leq m$. L'élément x_1 est irréductible, donc premier par hypothèse et il divise $y_1...y_m$: il existe $1 \leq j \leq m$ tel que $x_1|y_j$, c'est à dire $y_j = ax_1$ pour un certain $a \in A$. L'élément y_j étant irréductible et x_1 non-inversible, on a $a \in A^\times$ et ainsi

$$x_1...x_n = y_1...y_j...y_m = y_1...y_{j-1}ax_1y_{j+1}...y_m$$

donc $x_1(x_2...x_n - ay_1...y_{j-1}y_{j+1}...y_m) = 0$ et par intégrité

$$x_2...x_n \sim y_1...y_{j-1}y_{j+1}...y_m$$

On effectue le même processus, pour $x_2, x_3...x_n$ pour épuiser le membre de gauche, et puisqu'un produit d'irréductibles n'est pas inversible, on a alors $m = n$, et tout élément x_i est associé à un des y_j. □

Remarque 14.4. On a précédemment construit dans $\mathbb{Z}[i\sqrt{5}]$ un élément premier non-irréductible : il est donc intègre, mais pas factoriel.

Théorème 14.5. *Un anneau principal est factoriel.*

Démonstration. Si A est principal, il est intègre et on a vu précédemment (Proposition 11.12) qu'il vérifie l'axiome (A2′). Supposons par l'absurde que A ne vérifie pas l'axiome (A1), c'est à dire que l'ensemble

$$X = \{a \in A,\ a \neq 0,\ a \notin A^\times,\ a \text{ n'est pas un produit d'irréductibles}\}$$

est non-vide. On note $\mathcal{I}$ l'ensemble des idéaux engendrés par les éléments de X, et on applique le lemme de Zorn à l'ensemble $\mathcal{I}$: si

$$I_1 \subset I_2 \subset ...$$

est une chaîne d'élément de $\mathcal{I}$, on voit que l'union croissante $\bigcup_{j\geq 1} I_j$ est un idéal non-nul de A (même preuve que précédemment) et comme A est principal, il existe un élément $a \in A$ qui l'engendre et puisque a appartient à $\bigcup_{j\geq 1} I_j$, il existe un $k \geq 1$ tel que $a \in I_k =< a_k >$ pour un certain $a_k \in A$, et $a_k|x$. On a alors

$$\bigcup_{j\geq 1} I_j =< a >= I_k$$

et la chaine $I_1 \subset I_2 \subset ...$ admet bien un majorant dans $\mathcal{I}$. Le lemme de Zorn assure donc que $\mathcal{I}$ possède un élément $< x >$ maximal pour l'inclusion dans $\mathcal{I}$.

L'élément $x \in A$ est non-nul, non-inversible et n'est pas non plus irréductible (puisqu'il n'admet pas de décomposition). On a donc $x = zy$ avec y, z non-inversibles, mais alors on a

$$< x > \subsetneq < y > \text{ et } < x > \subsetneq < z >,$$

or y ou z se doit d'appartenir à X (sinon x admettrait une décomposition !) ; ceci contredit la maximalité de $< x >$ dans X. □

Thème 14.6. On a vu précédemment les implications

$$A \text{ euclidien} \Rightarrow A \text{ principal} \Rightarrow A \text{ factoriel}$$

et que la première implication est stricte. Pour montrer que la seconde l'est aussi, on peut utiliser le résultat suivant qu'il faut savoir, mais dont ne développerons pas la preuve (elle n'est pas très difficile mais un peu longue).

Théorème 14.7. *Un anneau A est factoriel si et seulement si $A[X]$ est factoriel.*

Les exemples précédents comme $\mathbb{Z}[X]$ nous permettent ainsi de construire des anneaux qui sont bien factoriels, sans pour autant être des anneaux principaux.

15. Arithmétique des anneaux factoriels

On rappelle que dans un anneau factoriel, tout élément non-nul, non-inversible s'écrit de manière unique comme un produit d'élément irréductibles, ceux-ci étant définis à association près.

Exemple 15.1. Donner une décomposition complète ans l'anneau $\mathbb{R}[X]$, puis dans $\mathbb{C}[X]$, du polynôme $P = X^4 - X^3 + X^2 - X$. Quels sont les irréductibles de $\mathbb{C}[X]$?

Lemme 15.2 (Diviseurs dans un anneau factoriel)**.** *Soit A un anneau factoriel et $a \in A$ non-nul, non-inversible. On écrit une décomposition*

$$a = x_1^{\alpha_1} ... x_n^{\alpha_n}$$

de a en un produit d'irréductibles $x_1, ..., x_n$ (avec les α_i strictement positifs). Les diviseurs de a sont les élément de la forme

$$u x_1^{\beta_1} ... x_n^{\beta_n}$$

avec u inversible et $0 \leq \beta_i \leq \alpha_i$ pour tout $1 \leq i \leq n$.

Démonstration. Si b est un diviseur de a inversible, il n'y a rien à montrer. Si b n'est pas inversible, on note x un de ses facteurs irréductibles, si bien que $x|a$. Par factorialité x est associé à un des x_i, on peut donc l'écrire $b_i x_i$ avec b_i inversible. Le même raisonnement pour tous les irréductibles qui entrent dans la décomposition de x assorti au fait que le produit des b_i est inversible assure que x est de la forme voulue (le fait que $\beta_i \leq \alpha_i$ est clair par unicité de la décomposition en produit d'irréductibles). □

Proposition 15.3 (pgcd et ppcm dans un anneau factoriel)**.** *Deux éléments a, b d'un anneau factoriel A admettent un* pgcd *et un* ppcm*. Plus précisément si on écrit les décompositions en produits d'irréductibles*

$$a = x_1^{\alpha_1} ... x_n^{\alpha_n} \text{ et } b = x_1^{\beta_1} ... x_n^{\beta_n},$$

(avec éventuellement les α_i ou β_i nuls), alors en posant $\gamma_i = \min(\alpha_i, \beta_i)$ et $\delta_i = \max(\alpha_i, \beta_i)$ pour tout $1 \leq i \leq n$ on a

$$\text{pgcd}(a, b) \sim x_1^{\gamma_1} ... x_n^{\gamma_n} \text{ et } \text{ppcm}(a, b) \sim x_1^{\delta_1} ... x_n^{\delta_n}$$

Démonstration. Cela découle directment de la description des diviseurs du Lemme 15.2. □

Théorème 15.4 (Lemme de Gauss)**.** *Soit a, b, c trois éléments d'un anneau factoriel. Si a divise bc et a est premier avec b, alors a divise c.*

Démonstration. On contemple les décompositions de a, b, c et bc. Si a divise bc, c'est que son support (c'est à dire les éléments irréductibles qui entrent dans sa décomposition) est contenu dans celui de bc (à association près). Comme a et b sont premiers entre eux, leurs supports sont disjoints et ainsi le support de a est contenu dans celui de c. Comme b ne contribue pas dans le produit bc pour les irréductibles du support de a, il est clair que a divise c. □