AR3 - Algèbre et Arithmétique

11 janvier 2017

Avant-propos

Ce texte est le fruit d'un cours d'arithmétique que j'ai donné à des étudiants de deuxième et troisième année de Licence de Mathématiques à l'université de Rennes 1 en 2015-2016. Selim BENSLAMA, qui suivait ce cours, a prit l'initiative de rédiger ses notes sous LaTeX, et souhaitait en faire profiter ses successeurs. Après quelques retouches de ma part, c'est le texte que vous avez entre les mains. Nous remercions Bernard LE STUM de nous avoir fait connaître le modèle Legrand Orange Book, ainsi que David Bourqui et Christophe Mourougane, à qui j'ai emprunté quelques exercices.

Les prérequis pour ce cours sont une connaissance de base de théorie des ensembles, ainsi que des propriétés de divisibilité dans $\mathbb{Z}$.

L'objectif du cours est un introduction à la structure de groupe - essentiellement abéliens, bien qu'un chapitre soit dédié au groupe symétrique et en particulier à la construction du morphisme de signature -, et celle d'anneaux (commutatifs unitaires), avec en vue l'étude des anneaux $\mathbb{Z}/n\mathbb{Z}$ et la théorie de la divisibilité dans les anneaux principaux, qui permettra de traiter l'anneau $\mathbb{Z}[i]$ des entiers de Gauß. Un des points les plus difficiles est sans doute la notion de structure quotient, mais qui en vaut la peine : on verra la construction "à la main" de quelques corps finis.

Le lecteur averti notera quelques omissions notables : en particulier la cyclicité des groupes finis d'inversibles dans les corps, ainsi que la théorie générale des corps finis, qui ne demandent pourtant plus beaucoup d'efforts supplémentaires. Mais les cours de L2-L3, tout comme les journées, ne font que 24h... Aussi, toutes les preuves ne sont pas rédigées, ou pas comme elles le devraient.

Enfin, un mot sur la licence que nous avons choisie : taper un polycopié sur ces sujets revient trop souvent à réinventer la poudre d'Euclide, Fermat, Gauß, Galois,... C'est pourquoi nous invitons ceux qui le souhaitent à modifier à leur sauce le texte même et à le réutiliser librement.

François MAUCOURANT

Réalisé en LaTeXà partir du modèle Legrand Orange Book (sous la même licence)

Table des matières

1. Notion de Groupe

1.1 Définition et premières propriétés

Définition 1.1.1 Soit E un ensemble. Une **loi de composition interne** (LCI) est une application

$$* : E \times E \to E.$$

Pour $x, y \in E$, on note $x * y$ l'élément de E obtenu par application de $*$ au couple (x, y).

Définition 1.1.2 Un **groupe** est un couple $(G, *)$ où G est un ensemble non vide et

$$* : G \times G \to G,$$

une loi de composition interne, qui vérifie :

1. $*$ est associative : $\forall (a, b, c) \in G^3$, $(a * b) * c = a * (b * c)$,
2. Il existe un élément neutre : $\exists e \in G$ tel que $\forall a \in G$, $a * e = e * a = a$,
3. Tout élément a un inverse : $\forall a \in G$, $\exists b \in G$ tel que $a * b = b * a = e$.

Proposition 1.1.1

- Tout groupe a un unique élément neutre.
- Tout élément a d'un groupe a un unique inverse.

Preuve.

- Si e et e' sont des éléments neutres, alors :

$$\begin{aligned} e * e' &= e \text{ comme } e' \text{ est un neutre} \\ &= e' \text{ comme } e \text{ est un neutre} \end{aligned}$$

  D'où $e = e'$.
- Si b et b' sont des inverses de a, alors :

$$\begin{aligned} b * (a * b') &= b * e = b \\ (b * a) * b' &= e * b' = b' \end{aligned}$$

D'où $b = b'$.

■

⚠La définition d'un groupe contient un "axiome caché" qui est trop souvent oublié lorsqu'on vérifie les axiomes sur un exemple : l'internalité de la loi de composition *interne*. Par exemple, l'ensemble des nombres impairs auquel on ajoute 0 n'est pas un groupe additif.

▪ **Exemples**

- Le groupe trivial $G = \{e\}$ avec la loi $e.e = e$.
- $(\mathbb{C}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Z}, +)$ sont des groupes.
- De même, tout espace vectoriel $(E, +, .)$ est, lorsqu'on regarde la structure additive $(E, +)$, un groupe.
- $(\mathbb{C}^*, \times)$ est un groupe.
- $(\mathbb{N}, +)$ n'est pas un groupe.
- $(\mathbb{Z}^*, \times)$ n'est pas un groupe.
- $\mathbf{GL}(n, \mathbb{R})$ est un groupe.

1.2 Groupe symétrique d'un ensemble E

Soit E un ensemble non vide. On considère l'ensemble :

$$\mathscr{S}_E = \{\text{bijections } f : E \to E\},$$

l'ensemble des bijections de E dans lui-même. On munit $\mathscr{S}_E$ de l'opération $\circ$ de composition des applications.

Proposition 1.2.1 Le couple $(\mathscr{S}_E, \circ)$ est un groupe, appelé **groupe symétrique de** E.

Démonstration. La composition de deux applications injectives étant injective, et le composition de deux applications surjectives étant surjective (exercice !), la loi $\circ$ est bien une loi interne.
La composition des applications est bien une opération associative.
Pour tout $f \in \mathscr{S}_E$, on a $f \circ Id_E = Id_E \circ f = f$, d'où existence d'un neutre, à savoir Id_E.
Soit $f \in \mathscr{S}_E$, comme f est bijective, elle a un inverse g qui satisfait

$$f \circ g = g \circ f = Id_E.$$

D'où le résultat. ■

Les éléments du groupe symétrique $\mathscr{S}_E$ sont appelés **permutations** (de E). En pratique, lorsque E est fini, on représente souvent une telle permutation σ par un tableau dont la première ligne est les éléments de E, et la deuxième leur image par σ. Par exemple, si $E = \{1, 2, 3, 4, 5\}$,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) & \sigma(5) \end{pmatrix}.$$

On a alors :

$$e = Id_E = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix},$$

Si on pose

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}, \sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix},$$

on calcule ainsi le produit (à compléter ! !)

$$\sigma \circ \sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ & & & & \end{pmatrix}.$$

⚠Les applications que l'on applique en premier sont celles les plus à droite !

L'inverse se calcule aussi aisément sous cette forme en intervertissant les deux lignes et en réordonnant les colonnes :

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ & & & & \end{pmatrix},$$

$$(\sigma')^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ & & & & \end{pmatrix}.$$

On s'aperçoit qu'en un certain sens, les groupes symétriques ne dépendent essentiellement que du cardinal de l'ensemble E - il est en effet loisible de remplacer 1 par a, 2 par b,.., 5 par e, sans changer la nature des calculs ci-dessus. Pour fixer les idées, on est donc amené à définir :

Définition 1.2.1 Soit $n \geq 1$ un entier, on note $\mathscr{S}_n$ le groupe symétrique sur l'ensemble $\{1, ..., n\}$. Ce groupe est de cardinal $n!$.

Démonstration. Une permutation $\sigma \in \mathscr{S}_n$ est uniquement déterminée par un tableau comme ci-dessus. La deuxième ligne doit contenir une et une seule fois chaque entier entre 1 et n, il s'agit donc d'un *arrangement* au sens de la combinatoire. On rappelle que puisque l'on a n choix pour $\sigma(1)$, $n-1$ choix pour $\sigma(2)$, etc, on a donc

$$n \times (n-1) \times (n-2) \times ... \times 1 = n!,$$

arrangements possibles de $\{1, ..., n\}$. ■

1.3 Notations et Définitions

Définition 1.3.1 Un groupe $(G, *)$ est dit **commutatif** (ou **abélien**) si $\forall (a, b) \in G^2$, $a * b = b * a$.

Notations :

- Pour des groupes non commutatifs :
  - on note e l'élément neutre,
  - on omet, ou on note $\cdot$ la LCI ($ab = a \cdot b = a * b$),
  - on note a^{-1} l'inverse de a,
  - on définit par récurrence le produit de n termes :

$$x_1 x_2 ... x_n = (x_1 x_2 ... x_{n-1}) x_n.$$

- Pour des groupes commutatifs :
  - on note $+$ la LCI,
  - on note 0 l'élément neutre,
  - on note $-a$ l'inverse de a.

1.4 Itération d'un élément dans un groupe

Soient $(G, *)$ un groupe, $g \in G$ et $n \in \mathbb{N}^*$. On définit par récurrence :

- $g^1 = g$,
- $g^{n+1} = g^n * g$ pour $n \geq 1$.

On pose aussi :

- $g^0 = e$,
- Si $n \in \mathbb{Z}^-$, par définition, on note $g^n = (g^{-n})^{-1}$.

Théorème 1.4.1 $\forall (m,n) \in \mathbb{Z}^2, \forall g \in G, g^m * g^n = g^{m+n}$ et $(g^m)^n = g^{mn}$.

Preuve en exercice. En particulier, il faut noter que l'inverse de l'inverse est l'élément lui-même ; $(a^{-1})^{-1} = a$, et la preuve en est la symétrie entre a et $b = a^{-1}$ dans l'expression $ab = ba = e$.

Remarque :

- Si G n'est pas abélien, $(ab)^n$ a toute les chances de ne pas être égal à $a^n b^n$. De par la définition, on a par exemple
$$(ab)^3 = ababab.$$
- Lorsque le groupe est abélien et noté additivement, on note nx l'itération n fois de x.

1.5 Règle de Calcul dans les groupes

Proposition 1.5.1

- **(Règles de simplification à gauche et à droite)**
$$(ax = ay) \Rightarrow (x = y)$$
et
$$(xa = ya) \Rightarrow (x = y).$$
- $(xy = e) \Rightarrow (x = y^{-1})$.
- $(xy)^{-1} = y^{-1}x^{-1}$.

Preuve.

- Si $ax = ay$ alors $a^{-1}ax = a^{-1}ay$ donc $ex = ey$ d'où $x = y$.
Si $xa = ya$ alors $xaa^{-1} = yaa^{-1}$ donc $xe = ye$ d'où $x = y$.
- Si $xy = e$ alors $xyy^{-1} = ey^{-1}$ donc $xe = y^{-1}$ d'où $x = y^{-1}$.
- $(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xex^{-1} = xx^{-1} = e$
donc $y^{-1}x^{-1} = (xy)^{-1}$.

■

Définition 1.5.1 Soit $f : E \to E$. Si $f \circ f = Id_E$, on dit que f est une **involution** de E.

Proposition 1.5.2 On considère les applications suivantes :

- $i : G \to G$
$g \mapsto g^{-1}$
est une involution de G.

- Pour $a \in G$, $m_a : G \to G$
$g \mapsto ga$
${}_am : G \to G$
$g \mapsto ag$
sont des bijections de G dans lui-même.

Preuve.

- $(g^{-1})^{-1} = g$, donc $i(i(g)) = g$

- Soit $a \in G$, $g \in G$.
  $m_{a^{-1}} \circ m_a(g) = m_{a^{-1}}(ga) = gaa^{-1} = ge = g$
  $m_a \circ m_{a^{-1}}(g) = m_a(ga^{-1}) = ga^{-1}a = ge = g$

■

1.6 Sous-Groupes

Définition 1.6.1 Soit $(G, *)$ un groupe et H une partie de G. On dit que H est un **sous-groupe de** G si :

1. $H \neq \varnothing$
2. $\forall (a,b) \in H^2$, $ab \in H$
3. $\forall a \in H$, $a^{-1} \in H$

Lemme 1.6.1 Un sous-groupe contient toujours l'élément neutre.

Démonstration. Soit H un sous-groupe. Comme $H \neq \emptyset$, il existe $a \in H$. Donc $a^{-1} \in H$. Donc $aa^{-1} \in H$, c'est à dire $e \in H$. ■

Proposition 1.6.2 H est un sous-groupe de G si et seulement si :

1. $H \neq \varnothing$
2. $\forall (a,b) \in H$, $ab^{-1} \in H$

Preuve.
($\Rightarrow$) :

- $i) \Rightarrow i)$
- Soit $(x,y) \in H^2$. $y^{-1} \in H$ par $iii)$
  Donc $xy^{-1} \in H$ par $ii)$
  Ce qui montre $ii)$.

($\Leftarrow$) :

- $i) \Rightarrow i)$
- Comme $H \neq \varnothing$, $\exists x \in H$. Donc, par $ii)$, $xx^{-1} = e \in H$
- Avec $(e,y) \in H^2$, par $ii)$, $ey^{-1} = y^{-1} \in H$
  Ce qui montre $iii)$
- Avec $(x, y^{-1}) \in H^2$, par $ii)$, $x(y^{-1})^{-1} = xy \in H$
  Ce qui montre $ii)$.

■

En pratique, pour montrer qu'un couple $(G, \star)$ est un groupe, on utilisera dans la majorité des cas le résultat suivant :

Proposition 1.6.3 Un sous-groupe H de G muni de la loi de composition interne restreinte à H est un groupe.

Preuve. $*_{|H\times H} : H \times H \to H$ est bien interne puisque H est un sous-groupe.

- $*_{|H\times H}$ est associative comme $*$.
- $e \in H$, donc H a bien un neutre
- Comme H est un sous-groupe, l'inverse de $a \in H$ est dans H.

■

Proposition 1.6.4 Une intersection quelconque de sous-groupes est un sous-groupe.

Preuve. Soient $(H_i)_{i\in I}$ une famille de sous-groupes de G, alors :
- $\forall i \in I, e \in H_i$. Donc $e \in \cap_{i\in I} H_i$.
- $\forall (a,b) \in \cap_{i\in I} H_i, \forall i \in I, ab^{-1} \in H_i$. Donc $ab^{-1} \in \cap_{i\in I} H_i$.

■

Théorème 1.6.5 Les sous-groupes de $(\mathbb{Z},+)$ sont les ensembles

$$n\mathbb{Z} = \{nx \,|\, x \in \mathbb{Z}\},$$

où $n \in \mathbb{N}$.

Preuve. ***$n\mathbb{Z}$* est un sous-groupe :**
- $0 = n0 \in n\mathbb{Z}$
- Soient $(x,y) \in (n\mathbb{Z})^2$, $x - y = nq - nq' = n(q-q') \in nZ$

Tous les sous-groupes sont de la forme *$n\mathbb{Z}$*.
Soit H est sous-groupe de $\mathbb{Z}$. Soit $H = \{0\} = 0\mathbb{Z}$ (et la preuve est terminée), soit H n'est pas réduit à $\{0\}$. Il contient donc un élément non nul, et quitte à considérer son opposé (qui est aussi dans H), il existe ainsi un élément non nul et positif dans H. Posons

$$n = \min(\{y | y \in H \cap \mathbb{N}^*\}),$$

qui est alors bien défini. Vérifions que $H = n\mathbb{Z}$, en procédant par double inclusion :
- $\subset$: $\forall q \in \mathbb{Z}$, $nq = qn \in H$, donc $n\mathbb{Z} \subset H$
- $\supset$: Soit $x \in H$, faisons la division euclidienne de x par n : $x = nq + r$ avec $0 \leq r < n$. Donc, $r = x - qn \in H$, donc $r = 0$ par définition de n. D'où $n|x$, et ainsi $H \subset nZ$.

■

1.7 Sous-Groupe engendré par une partie

Définition 1.7.1 Soient G un groupe, $X \subset G$ une partie. On appelle **sous-groupe engendré par** X l'ensemble $\langle X \rangle = \{g_1 g_2 ... g_n$ où $n \in \mathbb{N}$, $g_i \in X$ ou $g_i \in X^{-1}\}$.

Preuve. **(Il s'agit bien d'un sous-groupe)**
- Le produit vide (que l'on inclus dans la définition) donne e, donc $e \in \langle X \rangle$
- $\forall (x,y) \in (\langle X \rangle)^2$, on a : $x = g_1 g_2 ... g_n$ et $y = h_1 h_2 ... h_m$.
  Ainsi, $xy^{-1} = g_1 g_2 ... g_n (h_1 h_2 ... h_m)^{-1} = g_1 g_2 ... g_n h_m^{-1} h_{m-1}^{-1} ... h_1^{-1} \in \langle X \rangle$.

■

Lemme 1.7.1 $\langle X \rangle$ est le plus petit sous-groupe de G contenant X, autrement dit

$$\langle X \rangle = \bigcap_{H \text{ sous-groupe de } G} H.$$

1.8 Morphismes de Groupe

Définition 1.8.1 Soient $(G_1, \times)$ et $(G_2, *)$ deux groupes. Un **morphisme de groupes de G_1 dans** G_2 est une application $f : G_1 \to G_2$ qui vérifie :

$$\forall (x,y) \in G_1^2, f(x \times y) = f(x) * f(y)$$

■ **Exemple 1.1**

- $f \left| \begin{array}{ccc} G_1 & \longrightarrow & G_2 \\ x & \longmapsto & e_{g_2} \end{array} \right.$,
- $exp \left| \begin{array}{ccc} (\mathbb{R},+) & \longrightarrow & (\mathbb{R}_+^*,\times) \\ x & \longmapsto & e^x \end{array} \right.$,
- $ln \left| \begin{array}{ccc} (\mathbb{R}_+^*,\times) & \longrightarrow & (\mathbb{R},+) \\ x & \longmapsto & \ln(x) \end{array} \right.$,
- $|\cdot| \left| \begin{array}{ccc} (\mathbb{C}^*,\times) & \longrightarrow & (\mathbb{R}^*,\times) \\ z & \longmapsto & |z| \end{array} \right.$,
- $det \left| \begin{array}{ccc} (GL_n(\mathbb{R}),\cdot) & \longrightarrow & (\mathbb{R}^*,\times) \\ A & \longmapsto & det(A) \end{array} \right.$.

■

Proposition 1.8.1 Soit $f : (G_1,\times) \to (G_2,*)$ un morphisme de groupe. Alors
1. $f(e_{G_1}) = e_{G_2}$,
2. $\forall x \in G_1,\ f(x^{-1}) = f(x)^{-1}$,
3. $\forall n \in \mathbb{Z},\ \forall x \in G_1,\ f(x^n) = f(x)^n$,
4. $\forall (x_1,x_2,...,x_n) \in G_1^n,\ f(x_1 \times x_2 \times ... \times x_n) = f(x_1) * f(x_2) * ... * f(x_n)$.

Preuve.
1. $f(e_{G_1}) = f(e_{G_1} \times e_{G_1}) = f(e_{G_1}) * f(e_{G_1})$,
   donc $e_{G_2} = f(e_{G_1})$ en multipliant par $f(e_{G_1})^{-1}$ à droite ou à gauche.
2. $f(x \times x^{-1}) = f(x) * f(x^{-1}) = f(e_{G_1}) = e_{G_2}$,
   donc $f(x^{-1}) = f(x)^{-1}$ en multipliant par $f(x)^{-1}$ à gauche.
3. Par récurrence.
4. Par récurrence.

■

Proposition 1.8.2 Soit $f : G_1 \to G_2$ un morphisme de groupe. Alors
1. L'image directe d'un sous-groupe de G_1 est un sous-groupe de G_2.
2. L'image réciproque d'un sous-groupe de G_2 est un sous-groupe de G_1.
3. Soient
$$Im(f) = \{f(x) | x \in G_1\},$$
et
$$Ker(f) = \{x \in G_1 | f(x) = e_{G_2}\},$$
que l'on appelle respectivement l'image et le noyau de f. Alors :
f est injective si et seulement si $Ker(f) = \{e_{G_1}\}$.

Preuve.
1. Soit H un sous-groupe de G_1.
   - $e_{G_2} = f(e_{G_1}) \in f(H)$, donc $f(H) \neq \emptyset$.
   - Soit $x, y \in f(H)$, alors il existe $x', y' \in H$ tels que $f(x') = x$ et $f(y') = y$.
     $xy^{-1} = f(x') * f(y')^{-1} = f(x') * f(y'^{-1}) = f(x \times y'^{-1}) \in f(H)$.
2. Soit H un sous-groupe de G_2.
   - $f(e_{G_1}) = e_{G_2} \in H$, donc $f^{-1}(H) \neq \emptyset$.
   - Soit $x, y \in f^{-1}(H)$, donc $f(x) \in H$ et $f(y) \in H$.
     $f(x \times y^{-1}) = f(x) * f(y^{-1}) = f(x) * f(y)^{-1} \in H$
     Donc $x \times y^{-1} \in f^{-1}(H)$.
3. $\boxed{\Rightarrow}$ On sait que $f(e_{G_1}) = e_{G_2}$.
   Soit $x \in Ker(f)$, $f(x) = e_{G_2} = f(e_{G_1})$. Comme f est injective, $x = e_{G_1}$. D'où $Ker(f) = \{e_{G_1}\}$

$\boxed{\Leftarrow}$ Soit $(x,y) \in G_1^2$ tq $f(x) = f(y)$
Alors, $f(x) * f(y)^{-1} = e_{G_2} = f(x) * f(y^{-1}) = f(x \times y^{-1})$
Donc $x \times y^{-1} = e_{G_1}$, ou encore $x = y$

■

Définition 1.8.2 Un morphisme bijectif est appelé un **isomorphisme**.

Lemme 1.8.3 L'application réciproque d'un morphisme de groupe bijectif $(G_1, \star)$ dans $(G_2, *)$ est elle-même un morphisme de groupe de $(G_2, *)$ dans $(G_1, \star)$.

La preuve est laissée en exercice.

1.9 Exercices

Exercice 1.1 Parmi les couples suivants, déterminez lesquels sont des groupes. $(\mathbb{N}, +)$, $(\mathbb{Q}^*, \times)$, un espace vectoriel euclidien muni du produit scalaire, matrices $\{M :^t MM = I_n\}$ muni du produit matriciel, $(M_n(\mathbb{R}), +)$, $(M_n(\mathbb{R}), \times)$, fonctions de $\mathbb{R}$ dans $\mathbb{R}$ muni de la composition, fonctions de $[0,1]$ dans $\mathbb{R}$ muni de l'addition de fonctions, bijections croissantes de $[0,1]$ dans $[0,1]$ muni de la composition, l'ensemble des homothéties d'un espace vectoriel muni de la composition.

Exercice 1.2 Montrez que si G_1, G_2, G_3 sont des groupes et si $f : G_1 \to G_2$ et $g : G_2 \to G_3$ sont des morphismes de groupe, alors $g \circ f$ est un morphisme de groupe.

Exercice 1.3 Soit $(G, .)$ un groupe tel que pour tout $x \in G$, on ait $x^2 = e$. Montrez que G est commutatif. *Indication :* Pour x, y dans G, déterminez l'inverse de x, puis calculez $(xy)^2$.

Exercice 1.4 1) Soit $(G, *)$ un groupe, et $f : G \to G$ définie par $f(x) = x^{-1}$. Montrez que f est un morphisme si et seulement si G est commutatif.
2) Soit $(G, *)$ un groupe qui vérifie $\forall x \in G, x^2 = e$. Montrez que G est commutatif.

Exercice 1.5 Soit H, K deux sous-groupes d'un groupe G. Montrez que $H \cup K$ est un sous-groupe de G si et seulement si $H \subset K$ ou bien $K \subset H$.

Exercice 1.6 Démontrer le Lemme 1.8.3.

2. Relations d'équivalence

2.1 Relations d'équivalence

Définition 2.1.1 Une relation binaire R sur un ensemble X est dite *relation d'équivalence* si elle est :

- **réflexive :** $\forall x \in X,\ xRx$.
- **symétrique :** $\forall (x,y) \in X^2,\ xRy \Rightarrow yRx$.
- **transitive :** $\forall (x,y,z) \in X^3,\ (xRy \text{ et } yRz) \Rightarrow xRz$.

Définition 2.1.2 La classe d'équivalence d'un élément x de X est l'ensemble

$$\overline{x} = \{y \in X \text{ tels que } xRy\}.$$

■ **Exemple 2.1**

- relation d'égalité : $\overline{x} = \{x\}$.
- Étant donné une fonction $f : X \to Y$, on définit sur X la relation

$$xRy \Leftrightarrow f(x) = f(y).$$

Vérifions que c'est bien une relation d'équivalence.

- **réflexivité :** $f(x) = f(x)$ donc xRx
- **symétrique :** si yRx alors $f(y) = f(x)$ donc $f(x) = f(y)$ donc xRy.
- **transitivité :** si xRy et yRz, on a $f(x) = f(y)$ et $f(y) = f(z)$, et donc $f(x) = f(z)$, ce qui entraîne xRz.

Dans ce cas, il est facile de voir que les classes s'expriment de la façon suivante :

$$\overline{x} = f^{-1}(f(x)).$$

Cet exemple est important dans le sens où toute relation d'équivalence peut être construite de cette manière.

- Soit G un groupe et H un sous-groupe de G. On défini la *relation à gauche modulo H* sur G par $xRy \Leftrightarrow x^{-1}y \in H$.
  - **réflexivité :** $xRx \Leftrightarrow x \times x^{-1} = e_G \in H$
  - **symétrique :** $yRx \Leftrightarrow y^{-1}x \in H \Leftrightarrow (y^{-1} \times x)^{-1} = x^{-1} \times y \in H \Leftrightarrow xRy$
  - **transitivité :** xRy et $yRz \Rightarrow x^{-1} \times y \in H$ et $y^{-1} \times z \in H \Rightarrow (x^{-1} \times y) \times (y^{-1} \times z) = x^{-1} \times z \in H \Rightarrow xRz$

  Montrons que dans ce cas les classes sont

$$\overline{x} = xH = \{x \times h | h \in H\}.$$

  Procédons par double inclusion.
  - $\boxed{\supset}$ Posons $y = x \times h$, $xRy \Leftrightarrow x^{-1} \times y = x^{-1} \times x \times h = h \in H$
  - $\boxed{\subset}$ Soit $y \in \overline{x}$, donc $x^{-1} \times y \in H$.
    Donc, $\exists h \in H$ tq $x^{-1} \times y = h \Leftrightarrow y = x \times h$
- Soit E un ensemble de *groupes*. Montrez que si G, G' sont deux groupes (dans E), la relation $\sim$ définie par $G \sim G'$ si et seulement si il existe un isomorphisme de groupe de G dans G', est une relation d'équivalence sur E.

■

Définition 2.1.3 Une **partition** d'un ensemble X est une famille $(F_i)_{i \in I}$ de sous-ensembles de X, indexés par un ensemble I, avec
- $X = \bigcup_{i \in I} F_i$.
- $i \neq j \Rightarrow F_i \cap F_j = \emptyset$.

Considérons l'ensembles des classes $\{\overline{x} : x \in X\} \subset \mathscr{P}(X)$ associées à une relation R sur X. On peut le voir comme une famille d'ensembles (indexés, par exemple, par eux-mêmes, pour éviter les répétitions).

Théorème 2.1.1 Les classes pour une relation d'équivalence forment une partition. Réciproquement, étant donné une partition de $X = \bigcup_{i \in I} F_i$, la relation

$$xRy \Leftrightarrow \exists i \in I \text{ tel que } \{x, y\} \subset F_i,$$

est une relation d'équivalence dont les classes sont les éléments de la partition.

Preuve.
- $\forall (x, y) \in X^2$, $\overline{x} = \overline{y}$ ou $\overline{x} \cap \overline{y} = \emptyset$,
- $\bigcup_{x \in X} \overline{x} = X$.

■

2.2 Relation d'équivalence et quotient

Définition 2.2.1 Soit R une relation d'équivalence sur X. On note X/R l'ensemble des classes d'équivalence (qui est un sous-ensemble de $\mathscr{P}(X)$). L'application $\pi \left| \begin{array}{ccc} X & \longrightarrow & X/R \\ x & \longmapsto & \overline{x} \end{array} \right.$ est appelé **surjection canonique**.
Tout antécédent d'une classe est appelé **représentant** de la classe. Si G est un groupe, H un sous-groupe de G, et que l'on considère la relation d'équivalence à gauche modulo H, on note alors G/H (au lieu de G/R) l'ensemble des classes $\{xH : x \in G\}$.

Théorème 2.2.1 **(Critère de passage au quotient)** Soit R une relation d'équivalence sur X, et $f : X \to Y$ une fonction. Notons π la surjection canonique $\pi : X \to X/\mathscr{R}$. On a équivalence entre les deux points suivants.

- Pour tout $(x, x') \in X^2$, $xRx' \Rightarrow f(x) = f(x')$.
- Il existe une fonction $\overline{f} : X/R \to Y$ telle que $f = \overline{f} \circ \pi$.

Preuve.

- $\boxed{ii) \Rightarrow i)}$ Supposons qu'il existe une fonction $\overline{f} : X/R \to Y$ avec $f = \overline{f} \circ \pi$.
  Soient $(x, y) \in X^2$ avec xRy, donc $\overline{x} = \overline{y}$. Donc :

$$\begin{aligned} f(x) &= \overline{f}(\pi(x)), \\ &= \overline{f}(\overline{x}), \\ &= \overline{f}(\overline{y}), \\ &= \overline{f}(\pi(y)), \\ &= f(y) \end{aligned}$$

- $\boxed{i) \Rightarrow ii)}$ Définissons $\overline{f} \left| \begin{array}{ccc} X/R & \longrightarrow & Y \\ \overline{x} & \longmapsto & f(x) \end{array} \right.$
  Par hypothèse, si $\overline{x} = \overline{y}$, $\overline{f}(\overline{x}) = \overline{f}(\overline{y})$. Donc $\overline{f}$ est bien définie. Elle satisfait l'égalité annoncée.

■

2.3 Groupe quotient (cas abélien)

Proposition 2.3.1 Si G est un groupe commutatif et H un sous-ensemble de G, l'ensemble G/H peut-être muni d'une unique loi de groupe tq $\pi : G \to G/H$ soit un morphisme de groupes.

Preuve. Pour que π soit un morphisme, il faut et il suffit que $\forall (x, y) \in G^2$, $\overline{x \times y} = \overline{x} * \overline{y}$ où $*$ est la loi sur G/H.
Pour $\overline{x}, \overline{y} \in G/H$, on pose $\overline{x} * \overline{y} = \overline{x \times y}$. Il faut vérifier que

$$\left.\begin{array}{l} x'Rx \\ y'Ry \end{array}\right\} \Rightarrow (x' \times y')R(x \times y)$$

- $x'Rx \Leftrightarrow x'^{-1} \times x \in H$
  $y'Ry \Leftrightarrow y'^{-1} \times y \in H$
- On a donc :

$$\begin{aligned} (x' \times y')^{-1} \times (x \times y) &= y'^{-1} \times x'^{-1} \times x \times y \\ &= (y'^{-1} \times y) \times (x'^{-1} \times x) \text{ comme G commutatif} \\ &\in H \end{aligned}$$

- On a donc bien $(x' \times y')R(x \times y)$, ce qui montre que la loi de composition interne $*$ est bien définie.

■

■ **Exemple 2.2**
- Le groupe $\mathbb{R}/2\pi\mathbb{Z}$: on identifie deux nombres x, y si $x - y \in 2\pi\mathbb{Z}$ càd $x = y + 2k\pi$, où k est un entier relatif. On obtient ainsi le groupe des angles, angles que l'on peut librement additionner et soustraire entre eux.
- Le groupe $\mathbb{Z}/n\mathbb{Z}$: deux entiers sont dans la même classe modulo n si leur différence est multiple de n. On peut ainsi additionner et soustraire les égalités de congruence.

■

2.4 Passage au quotient d'un morphisme

Théorème 2.4.1 Soit G_1 et G_2 deux groupes, H un sous-groupe de G_1 et $f : G_1 \to G_2$ un morphisme. On suppose G_1 abélien, alors il y a équivalence entre :
1. Il existe $\overline{f} : G_1/H \to G_2$ un morphisme tq $f = \overline{f} \circ \pi$, où π est la surjection canonique de G_1 dans G_1/H.
2. $H \subset Ker(f)$

De plus, si c'est le cas, $\overline{f}$ est unique et $\begin{cases} Im(\overline{f}) = Im(f) \\ Ker(\overline{f}) = \pi(Ker(f)) \end{cases}$

Corollaire 2.4.2 Dans le cas particulier où $H = Ker(f)$, on a que $\overline{f} : G_1/Ker(f) \to Im(f)$ est un isomorphisme.

■ **Exemple 2.3** $(\mathbb{Z}^2, +)$ est un groupe abélien. Soit $f \left| \begin{array}{ccc} \mathbb{Z}^2 & \longrightarrow & \mathbb{Z} \\ (x,y) & \longmapsto & x \end{array} \right.$
- f est un morphisme : $f(x,y) + f(x',y') = x + x' = f(x + x', y + y')$
- $Ker(f) = \{(0,y) | y \in \mathbb{Z}\}$.
  Donc $\overline{f} : \mathbb{Z}^2/Ker(f) \to \mathbb{Z}$ est un isomorphisme avec $\mathbb{Z}$.

■

2.5 Ordre d'un groupe, indice d'un sous-groupe

Définition 2.5.1
- Soit G un groupe, on appelle **ordre de** G son cardinal.
- Soit H un sous-groupe de G, on appelle **indice de** H **dans** G, que l'on note $[G : H]$, le cardinal de l'ensemble quotient G/H : $[G : H] = |G/H|$

Théorème 2.5.1 **(Lagrange)** Si H est un sous-goupe de G, alors $|G| = |H| \cdot |G/H| = |H| \cdot [G : H]$
En particulier, si G est fini, l'ordre d'un sous-groupe divise l'ordre du groupe.

Preuve. Rappelons que sur G, on a une relation à gauche modulo H : $xRy \Leftrightarrow x^{-1}y \in H$ dont les classes sont $\{xH | x \in G\}$.
Or, la multiplication à gauche par x est bijective, donc $|xH| = |H|$
Cette relation partitionne donc G en $[G : H]$ morceaux de cardinal $|H|$.
Donc $|G| = |H| \cdot [G : H] = |H| \cdot |G/H|$ ■

Définition 2.5.2 Soient G un groupe et $g \in G$. **L'ordre de** g est le plus petit entier $n \geq 1$ tq $g^n = e$. S'il n'existe pas de tel n, on convient de dire que g est d'ordre infini.

■ **Exemple 2.4**
- Dans $\mathbb{Z}$, 2 est d'ordre infini
- g est d'ordre $1 \Leftrightarrow g = g^1 = e$

- Dans $\mathscr{S}_3$, $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ est d'ordre 1
  $\tau_{12} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ est d'ordre 2, comme τ_{13} et τ_{23}
  $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ est d'ordre 3.

■

Lemme 2.5.2 Si g est d'ordre fini n, alors le morphisme $\varphi_g \left| \begin{array}{ccc} \mathbb{Z} & \longrightarrow & G \\ m & \longmapsto & g^m \end{array} \right.$ a pour noyau $n\mathbb{Z}$ et le sous-groupe engendré par g est d'ordre n, et on a :

$$\langle g \rangle = \{e, g, g^2, ..., g^{n-1}\}.$$

Preuve.

- $\boxed{\supset}$: Soit $k \in n\mathbb{Z}$, alors $\exists a \in \mathbb{Z}$ tq $k = an$
  Donc $g^k = g^{an} = (g^n)^a = e^a = e$
- $\boxed{\subset}$: Soit $k \in \mathbb{Z}$ tq $g^k = e$. Notons q, r le quotient et le reste de la division euclidienne de k par n, donc $k = qn + r$ avec $0 \leq r < n$.
  Alors, $g^k = g^{qn+r} = g^{qn} g^r = g^r$. Comme $0 \leq r < n$, $r = 0$
  Donc $n|k$ et $k \in n\mathbb{Z}$.

■

⚠L'équation $g^k = e$ n'assure pas que g soit d'ordre k. Ce que signifie cette équation est très précisément :

Corollaire 2.5.3 Soit $k \in \mathbb{Z} - \{0\}$. On a l' équivalence :

$$g^k = e \Leftrightarrow \text{l'ordre de } g \text{ divise } k.$$

Un corollaire très important du théorème de Lagrange est le résultat suivant :

Théorème 2.5.4 L'ordre d'un élément d'un groupe divise l'ordre du groupe.

■ **Exemple 2.5** Dans $(\mathbb{Z}/15\mathbb{Z}, +)$,

- L'ordre de $\overline{1}$ est 15.
- L'ordre de $\overline{3}$ est 5 : $\langle \overline{3} \rangle = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}\}$.
- L'ordre de $\overline{5}$ est 3 : $\langle \overline{3} \rangle = \{\overline{0}, \overline{5}, \overline{10}\}$.

■

2.6 Exercices

Exercice 2.1 Faire la liste des éléments de $(\mathscr{S}_3, \circ)$, et précisez pour chaque élément, le sous-groupe engendré ainsi que leur ordre. Même question avec $(\mathbb{Z}/6\mathbb{Z}, +)$ et $(\mathbb{Z}/12\mathbb{Z}, +)$.

Exercice 2.2 Montrez que $2\pi\mathbb{Z}$ est un sous-groupe de $(\mathbb{R}, +)$. Montrez que le groupe $(\{z \in \mathbb{C} : |z| = 1\}, \times)$ est isomorphe à $(\mathbb{R}, 2\pi\mathbb{Z}, +)$.

Exercice 2.3 1) Soit p un nombre premier, et $(G, \star)$ un groupe d'ordre p.
Montrer que G est cyclique, c'est à dire qu'il existe $g \in G$ tel que $G = \langle g \rangle$. *Indication :* Soit g un élément de G différent de l'élément neutre. Que peut-on dire de l'ordre du sous-groupe de G engendré par g ?

2) Soit $(G,+)$ un groupe commutatif de neutre 0, a,b deux éléments d'ordres respectifs p,q. Montrez que l'ordre de $a+b$ divise pq.
3) Montrez que si p et q sont premiers entre eux, $\langle a\rangle \cap \langle b\rangle = \{0\}$.
4) Toujours en supposant $pgcd(p,q) = 1$, montrez que $a+b$ est d'ordre pq.
5) Pouvez vous exhiber un exemple de cette situation où p et q ne sont pas premiers entre eux, et où l'ordre de $a+b$ est strictement plus petit que pq ?

Exercice 2.4 Soit $(G,\cdot)$ un groupe fini qui vérifie que pour tout $x \in G$, $x^2 = e$. On a vu que G était commutatif. Montrez que le cardinal de G est une puissance de 2. *Indication : procéder par récurrence sur le cardinal de G, et faire un quotient.*.

Exercice 2.5 Montrez que $(\mathbb{Z},+)$ est un sous-groupe de $(\mathbb{Q},+)$. Soit G le groupe quotient $\mathbb{Q}/\mathbb{Z}$. Quel est l'ordre de la classe de la fraction p/q où p,q entiers premiers entre eux ? Ce groupe G contient-il des éléments d'ordre infini ? Est-il fini ?

Exercice 2.6 Déterminez la liste des sous-groupes de $(\mathbb{Z}/n\mathbb{Z},+)$.

Exercice 2.7 Soient (n,m) deux entiers ≥ 1. Montrez qu'il existe un morphisme surjectif de groupes additifs $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ si et seulement si m divise n.

Exercice 2.8 Par *somme alternée des chiffres* d'un nombre, on entend la somme des chiffres avec un coefficient -1 tous les deux chiffres. Par exemple, la somme alternée des chiffres de 15628 est $1-5+6-2+8 = 7$, celle de 25 est $2-5 = -3$. Montrez qu'un nombre entier est divisible par 11 si et seulement si la somme alternée de ses chiffres en base 10 l'est.

3. Introduction aux groupes symétriques

3.1 Rappels

Soit $n \in \mathbb{N}^*$. On rappelle que $\mathcal{S}_n$ est l'ensemble des bijections de $\{1,...,n\}$ dans lui-même. Un élément σ de $\mathcal{S}_n$ est appelé permutation, que l'on note sous la forme $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$. et $|\mathcal{S}_n| = n!$. $(\mathcal{S}_n, \circ)$ est un groupe où $\circ$ est la composition des applications, dont le neutre est $id_{\{1,...,n\}} = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$.

À part dans les cas $n = 1$ ou 2, ce groupe n'est pas commutatif.

Proposition 3.1.1 $\mathcal{S}_n$ n'est pas commutatif si $n \geq 3$

Démonstration. Pour $n = 1$ et $n = 2$, on peut vérifier directement que le groupe est commutatif. Pour $n \geq 3$, on peut prendre $\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 1 & 3 & \cdots & n \end{pmatrix}$, et $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 1 & 3 & 2 & 4 & \cdots & n \end{pmatrix}$, puis vérifier que

$$\tau\sigma \neq \sigma\tau.$$

■

3.2 Support d'une permutation

Définition 3.2.1 Soit $\sigma \in \mathcal{S}_n$. On appelle le *support* de la permutation σ le sous-ensemble de $\{1,...,n\}$ défini par $supp(\sigma) = \{i \in \{1,..,n\} \text{ tel que } \sigma(i) \neq i\}$

▪ Exemple 3.1

- $supp(\sigma) = \{1,2\}$,
- $supp(\tau) = \{2,3\}$,
- $supp(id) = \varnothing$.

▪

Proposition 3.2.1 On a :
1. Pour tout $\sigma \in \mathcal{S}_n$, on a $\sigma(supp(\sigma)) = supp(\sigma)$.
2. Soient σ, σ' deux éléments de $\mathcal{S}_n$ de supports disjoints, alors σ et σ' commutent.

Démonstration. 1. Montrons que $\sigma(supp(\sigma)) \subset supp(\sigma)$:
Soit $i \in supp(\sigma)$. Si $\sigma(i) \notin supp(\sigma)$, on aura $\sigma(\sigma(i)) = \sigma(i)$. Comme σ est injectif, $\sigma(i) = i$, ce qui est absurde.

Comme σ est injectif, on a égalité entre les cardinaux $|\sigma(supp(\sigma))| = |supp(\sigma)|$. Comme l'un est inclu dans l'autre et de même cardinal (fini), on a bien l'égalité.

2. Soit $i \in \{1, ..., n\}$,
   - Si $i \in supp(\sigma)$, $i \notin supp(\sigma')$ et $\sigma'(i) = i$. Donc $\sigma(\sigma'(i)) = \sigma(i)$.
     De plus, puisque $\sigma(i) \in supp(\sigma)$, $\sigma(i) \notin supp(\sigma')$. Ainsi, $\sigma'(\sigma(i)) = \sigma(i)$.
   - On peut faire le même raisonnement pour $i \in supp(\sigma')$.
   - Si $i \notin supp(\sigma)$ et $i \notin supp(\sigma')$, on aura $\sigma(\sigma'(i)) = \sigma'(\sigma(i)) = i$

■

Définition 3.2.2 Un **cycle** de longueur l avec $l \in \mathbb{N}$ et $l \geq 2$ est une permutation σ de S_n tel qu'il existe un sous-ensemble ordonné $\{j_0, j_1, ..., j_{l-1}\}$ de $\{1, ..., n\}$ tel que
1. Le support de σ est $supp(\sigma) = \{j_0, ..., j_{l-1}\}$,
2. Pour tout $i \in \{0, ..., l-2\}$, $\sigma(j_i) = j_{i+1}$ et $\sigma(j_{l-1}) = j_0$.

On note ce cycle $(j_0, ..., j_{l-1})$ que l'on nomme parfois un *l-cycle*

■ **Exemple 3.2** $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} = (1,2,3) = (2,1,3) = (3,1,2)$. On remarque l'écriture d'un cycle n'est pas unique, et que le support ne suffit pas à caractériser un cycle : $(1,2,3) \neq (3,2,1)$ ■

Définition 3.2.3 Un cycle de longueur 2 est appelé une **transposition**.

■ **Exemple 3.3** Dans $\mathcal{S}_4$, les seules transpositions sont $(1,2)$, $(1,3)$, $(1,4)$, $(2,3)$, $(2,4)$ et $(3,4)$. Exercice : De façon générale, donner une formule pour le nombre de transpositions dans le groupe $\mathcal{S}_n$. ■

Théorème 3.2.2 Le groupe $\mathcal{S}_n$ est engendré par les transpositions : toutes permutations peuvent s'écrire comme le produit d'au plus $n-1$ transpositions.

Démonstration. Par récurrence sur n avec l'hypothèse H_n = "tout élément de S_n est produit d'au plus $n-1$ transpositions" ■

R La décomposition en produit de transposition n'est pas unique.

Proposition 3.2.3 Soit $l \geq 2$. Un l-cycle est d'ordre l.

Démonstration. Soit $\sigma = (j_0, ..., j_{l-1})$ et $k \in \mathbb{N}$ tel que $\sigma^k(j_i) = j_i$.
Comme $\sigma^k(j_i) = j_{i+k \mod l}$, $k = 0 \mod l$. Le plus petit k non nul et positif qui marche est donc $k = l$. ■

3.3 σ-orbites : décomposition canonique en produit de cycle

On simplifie les notations en notant $\sigma x = \sigma(x)$. Ce n'est bien sûr pas un produit ni l'application d'une loi interne !

Définition 3.3.1 Soit $x \in \{1,...,n\}$ et $\sigma \in \mathcal{S}_n$. On appelle σ-orbite de x le sous-ensemble

$$O_\sigma(x) = \{\sigma^k x \text{ avec } k \in \mathbb{Z}\}.$$

Pour la relation d'équivalence R_σ définie par $xR_\sigma y \Leftrightarrow y \in O_\sigma(x)$, $O_\sigma(x)$ est la classe de x.

Démonstration. Montrons que R_σ est bien une relation d'équivalence :

- *R_σ est symétrique :* Soient $x, y \in \{1,...,n\}$,

$$\begin{aligned} xR_\sigma y &\Leftrightarrow y \in O_\sigma(x), \\ &\Leftrightarrow \exists k \in \mathbb{Z} \text{ tel que } \sigma^k x = y, \\ &\Leftrightarrow \exists k \in \mathbb{Z} \text{ tel que } \sigma^{-k} y = x, \\ &\Leftrightarrow x \in O_\sigma(y), \\ &\Leftrightarrow yR_\sigma x. \end{aligned}$$

- *reflexivité :* Soit $x \in \{1,...,n\}$, on a $x = \sigma^0 x$ d'où $x \in O_\sigma(x)$ donc $xR_\sigma x$.
- *R_σ est transitive :* Soient $x, y, z \in \{1,...,n\}$
  Supposons $xR_\sigma y$ et $yR_\sigma z$. Alors $y \in O_\sigma(x)$ et $z \in O_\sigma(y)$. Donc $\exists k, l \in \mathbb{Z}$ tels que $\sigma^k x = y$ et $\sigma^l y = z$. Donc $\sigma^{k+l} x = z$, d'où $z \in O_\sigma(x)$. C'est à dire $xR_\sigma z$.

Regardons maintenant la classe de x :

$$\begin{aligned} \overline{x} &= \{y \text{ tel que } xR_\sigma y\} \\ &= \{y \text{ tel que } \exists k \in \mathbb{Z} \text{ tel que } \sigma^k x = y\} \\ &= \{\sigma^k x \text{ avec } k \in \mathbb{Z}\} \\ &= O_\sigma(x) \end{aligned}$$

■

Définition 3.3.2 On dit que x est un **point fixe de** σ si $\sigma(x) = x$, ce qui est équivalent à $x \notin supp(\sigma)$ ou encore à $O_\sigma(x) = \{x\}$

Théorème 3.3.1 — Décomposition canonique en produit de cycles à supports disjoints. Soit $\sigma \in \mathcal{S}_n - \{e\}$. Il existe $k \geq 1$, des entiers $l_1,..,l_k \geq 1$ et $c_1,...,c_k$ des cycles de longueurs respectives $l_1,...,l_k$ à supports deux-à-deux disjoints tel que $\sigma = c_1...c_k$. Cette décomposition est unique à l'ordre des facteurs près. L'entier k est le nombre d'*orbites non ponctuelles*.

Proposition 3.3.2 L'ordre d'une permutation est égal au ppcm de la longueur des cycles de sa décomposition canonique.

Démonstration. Exercice. ■

3.4 Signature d'une permutation

Définition 3.4.1 On appelle **signature** d'une permutation σ de $\mathcal{S}_n$ le nombre $\varepsilon(\sigma) = (-1)^{n-m}$ où m est le nombre de σ-orbite (orbites ponctuelles comprises).

Théorème 3.4.1 Soit σ une permutation et τ une transposition. Alors, $\varepsilon(\sigma\tau) = -\varepsilon(\sigma)$.

Démonstration. ■

Corollaire 3.4.2
1. Soit $\sigma \in \mathcal{S}_n$, $\sigma = \tau_1 ... \tau_k$ une décomposition en produit de transpositions, alors $\varepsilon(\sigma) = (-1)^k$.
2. $\varepsilon : \mathcal{S}_n \to (\{-1,1\}, \times)$ est un morphisme de groupes.

Calcul de la signature :
- A partir du nombre m de σ-orbites : $\varepsilon(\sigma) = (-1)^{n-m}$. On prendra soin de ne pas oublier les orbites ponctuelles (qui sont négligées dans la décomposition en produit de cycles !
- A partir d'une décomposition en transpositions : $\varepsilon(\tau_1 ... \tau_k) = (-1)^k$.
- Sous forme d'un produit de cycle : $\varepsilon(c_1 ... c_k) = \prod_{i=1}^{k} \varepsilon(c_i)$.
- Avec la formule (essentiellement inutilisable) $\varepsilon(\sigma) = \prod_{i<j} \frac{\sigma(j)-\sigma(i)}{j-i}$.
- Avec l'algèbre linéaire et la formule

$$det(M) = \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} m_{i,\sigma(i)}$$

où $M = (m_{ij}) \in M_n(K)$. On trouve alors que si σ est une permutation de $\mathcal{S}_n$ et M_n la matrice associée, $\varepsilon(\sigma) = det(M_\sigma)$.

3.5 Exercices

Exercice 3.1 Démontrez la proposition 3.3.2.

Exercice 3.2 Soit les deux permutations de $\mathcal{S}_7$, $\alpha = (2,4,6)(1,5,7)$ et $\beta = (2,4)(5,6)$.
1) Quels sont les ordres de α et β ?
2) En déduire que le sous-groupe engendré par α et β a un ordre multiple de 6.

Exercice 3.3 Soit σ la permutation de $\mathcal{S}_{10}$ définie par

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 7 & 9 & 1 & 8 & 3 & 2 & 10 & 6 & 5 \end{pmatrix}$$

1) Donner les décompositions de σ en produit de cycles disjoints et en déduire une décomposition de σ en un produit de transpositions.
2) En déduire de deux facons différentes la signature de σ.
3) Calculez σ^{2000}.

Exercice 3.4 Soient les deux éléments du groupe symétrique $\mathcal{S}_6$,

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 5 & 1 & 3 & 2 \end{pmatrix},$$

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

1) Donnez la décomposition en produit de cycles à support disjoints, l'ordre ainsi que la signature de τ et σ respectivement.
2) Déterminer les composées $\sigma^2\tau$ et $\tau\sigma$.

Exercice 3.5 Soit $\sigma \in \mathscr{S}_{10}$ une permutation d'ordre 14. Montrez que σ est impaire, c'est à dire de signature -1.

Exercice 3.6 On mélange un jeu de 32 cartes "à l'américaine", de façon précise. Numérotons les cartes de 1 à 36 selon leur place dans le paquet. On commence par découper le tas de 32 cartes en deux tas (les cartes de 1 à 16 et celles de 17 à 32), puis on les intercale une à une en commançant par le bas et le premier tas, càd la dernière carte du nouveau paquet est la dernière du premier tas (la numéro 16), puis l'avant dernière est la dernière du deuxième tas (la numéro 32), l'avant-avant dernière est la numéro 15, etc...
1) Écrire la permutation de $\mathscr{S}_{32}$ correspondante.
2) En supposant que l'on puisse faire cette opération de façon parfaite, finit-on par retrouver la configuration initiale en itérant ce procédé ? Si oui, au bout de combien de fois ?

4. Généralités sur les anneaux

4.1 Anneaux

Définition 4.1.1 Un triplet $(A,+,\times)$ où A est un ensemble non vide muni de deux LCI $+$ et $\times$ est appelé *anneau commutatif unitaire* (ACU) si :

1. $(A,+)$ est un groupe abélien dont le neutre est noté 0_A
2. $\times$ est associative : $\forall (x,y,z)\in A^3,\ (x\times y)\times z = x\times(y\times z)$
3. $\times$ est commutatif : $\forall (x,y)\in A^2,\ a\times b = b\times a$
4. $\times$ a un neutre noté 1_A : $\forall x\in A,\ x\times 1_A = 1_A\times x = x$
5. $\times$ est distributive par rapport à $+$: $\forall (x,y,z)\in A^3,\ a\times(b+c) = a\times b + a\times c$

▪ **Exemple 4.1** $(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{C},+,\times)$ ou encore $(\mathbb{C}[X],+,\times)$. Les nombres décimaux $\mathbb{D}$ est un autre exemple. ▪

▪ **Exemple 4.2** *(L'anneau nul).* Les axiomes ne supposent pas que $0_A \neq 1_A$. Si on a cette égalité $0_A = 1_A$, alors A ne contient qu'un seul élément (exercice !) $\{0_A\}$. Cet anneau est appelé l'anneau nul. ▪

4.2 Règles de calcul dans un anneau

Notations :

On note, pour $k\geq 1$ et $x\in A$,

$$x^k = x\times ..\times x \ (k \text{ fois}).$$

Par convention, on pose $x^0 = 1_A$. Notons que x n'étant pas nécessairement inversible pour la loi $\times$, x^k n'a pas à priori de sens pour les exposants $k\geq 0$.

Bien souvent, on se contentera de noter xy pour le produit $x\times y$.

⚠ Rappelons que dans le groupe additif $(A,+)$, pour n un entier naturel, l'élément $n.x$ désigne $x+..+x$ (n fois) Il faut bien comprendre que $n.x$ ne désigne pas le produit de deux éléments de A ; $n.x$ et yx désignent donc les résultats de deux opérations à priori très différentes. Cependant, la distributivité implique que

$$n.x = (1_A+..+1_A)\times x = (n.1_A)\times x,$$

qui est bien le produit de deux éléments de A. On verra plus loin l'interprétation de cette égalité.

Proposition 4.2.1 Soit $(A,+,\times)$ un anneau, alors :

1. $\forall a \in A,\ a \times 0_A = 0_A$.
2. $\forall (a,b) \in A^2,\ (-a)\times b = a \times (-b) = -(a\times b)$.
3. Soient I et J des ensembles finis, alors $\forall (a_i)_{i\in I} \in A^I$ et $\forall (b_j)_{j\in J} \in A^J$,
$$(\sum_{i\in I} a_i)(\sum_{j\in J} b_j) = \sum_{(i,j)\in I\times J} a_i \times b_j.$$
4. $\forall (m,n) \in \mathbb{N}^2,\ x^{m+n} = x^m \times x^n$ et $(x^m)^n = x^{mn}$.
5. **(Formule du binôme de Newton)** $\forall (x,y) \in A^2,\ \forall n \in \mathbb{N}^*$,
$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k}.(x^k \times y^{n-k}).$$

4.3 Eléments inversibles

Définition 4.3.1 On appelle **groupe des inversibles** de l'anneau commutatif unitaire A l'ensemble
$$A^\times = \left\{x \in A \text{ tel que } \exists y \in A, \text{ avec } x\times y = y\times x = 1_A\right\}.$$
Ce groupe est parfois noté U_A.

⚠ Certains auteurs notent A^* ce groupe des inversibles. Cette notation est ambigüe car elle peut aussi désigner $A-\{0\}$, qui n'est pas forcément le même ensemble (par exemple, pour $A=\mathbb{Z}$). Dans la suite, on désignera toujours par A^* l'ensemble $A-\{0_A\}$.

■ **Exemple 4.3**

- $\mathbb{R}^\times = \mathbb{R}-\{0\} = \mathbb{R}^*$.
- $\mathbb{Z}^\times = \{-1,1\}$.
- $\mathbb{C}[X]^\times = \mathbb{C}^*$.

■

Définition 4.3.2 Un **corps** K est un anneau commutatif unitaire non nul dont tout élément non nul est inversible, c'est-à-dire $K^\times = K^* = K-\{0_K\}$.

■ **Exemple 4.4** $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$ ou encore $(\mathbb{Q},+,\times)$.
$(\mathbb{D},+,\times)$ n'en est pas un : $3^{-1} = \frac{1}{3} \notin \mathbb{D}$. L'anneau nul n'est pas un corps. ■

4.4 Morphismes d'anneaux

Définition 4.4.1 Soient A et B deux anneaux commutatifs unitaires, et $f : A \to B$ une application. On dit que f est un **morphisme d'anneaux** si :

1. $\forall (x,y) \in A^2,\ f(x)+f(y) = f(x+y)$
2. $\forall (x,y) \in A^2,\ f(x)\times f(y) = f(x\times y)$
3. $f(1_A) = 1_B$

Cette définition est bien plus contraignante que celle de morphisme de groupe. En particulier, on verra en TD qu'il peut ne pas exister de morphisme d'anneaux entre deux anneaux particuliers, alors qu'il existe toujours au moins un morphisme de groupe entre deux groupes.

■ **Exemple 4.5**

- $\varphi : \mathbb{Z} \to \mathbb{C}$ l'injection canonique
- $id : \mathbb{Z} \to \mathbb{Z}$ est l'unique morphisme d'anneau de $\mathbb{Z}$ dans $\mathbb{Z}$.

■

Théorème 4.4.1 Soit A un anneau, alors il existe un unique morphisme d'anneau

$$\varphi \left| \begin{array}{ccc} \mathbb{Z} & \longrightarrow & A \\ n & \longmapsto & n \cdot 1_A \end{array} \right. ,$$

appelé morphisme canonique.

Définition 4.4.2 On dit que deux anneaux commutatifs unitaires A et B sont isomorphes si il existe $f : A \to B$ un morphisme unitaire d'anneaux bijectif. Un tel morphisme est appelé **isomorphisme d'anneaux**.

Théorème 4.4.2 La fonction réciproque d'un isomorphisme d'anneaux est un isomorphisme d'anneaux.

Démonstration. Puisque f est bijectif, $f^{-1} : Im(f) \to A$ est bien définie et est bijectives. De plus, $\forall (x, y) \in Im(f)^2$, on a :

- $f(1_A) = 1_B \Leftrightarrow f^{-1}(1_B) = 1_A$
- $f(f^{-1}(x+y)) = x + y = f(f^{-1}(x) + f(f^{-1}(y))$. Comme f est bijective, $f^{-1}(x+y) = f^{-1}(x) + f^{-1}(y)$
- $f(f^{-1}(x \times y)) = x \times y = f(f^{-1}(x) \times f(f^{-1}(y))$. Comme f est bijective, $f^{-1}(x \times y) = f^{-1}(x) \times f^{-1}(y)$

■

Conséquence :

Etre isomorphe est une relation d'équivalence sur l' "ensemble des anneaux" puisque la composée de 2 morphismes est un morphisme.

4.5 Anneaux produits

A partir d'une famille d'anneaux, on peut en construire de nouveaux. Un façon de faire est de définir leur produit.

Définition 4.5.1 Soient I un ensemble non vide d'indices et $\forall i \in I$, $(A_i, +_i, \times_i)$ un anneau. On munit $\prod_{i \in I} A_i$ des lois + et × définie par : $\begin{cases} (a_i)_{i \in I} + (b_i)_{i \in I} = (a_i +_i b_i)_{i \in I} \\ (a_i)_{i \in I} \times (b_i)_{i \in I} = (a_i \times_i b_i)_{i \in I} \end{cases}$

Proposition 4.5.1

1. $(\prod_{i \in I} A_i, +, \times)$ est un anneau commutatif unitaire.
2. Les projections canoniques $p_j \left| \begin{array}{ccc} \prod_{i \in I} A_i & \longrightarrow & A_j \\ (a_i)_{i \in I} & \longmapsto & a_j \end{array} \right.$ sont des morphismes d'anneaux.

Démonstration.

1. $\forall i \in I$, $(A_i, +_i, \times_i)$ est un anneau. Donc toutes les démonstrations sur $\prod_{i \in I} A_i$ seront vérifiées pour $\forall i \in I$, d'où $(\prod_{i \in I} A_i, +, \times)$ est un ACU.

2. $p_j((a_i)_{i\in I}+(b_i)_{i\in I}) = p_j((a_i +_i b_i)_{i\in I}) = a_j +_j b_j = p_j((a_i)_{i\in I}) + p_j((b_i)_{i\in I})$
   $p_j((a_i)_{i\in I}\times(b_i)_{i\in I}) = p_j((a_i \times_i b_i)_{i\in I}) = a_j \times_j b_j = p_j((a_i)_{i\in I}) \times p_j((b_i)_{i\in I})$

■

Un exemple crucial est donné par les anneaux de fonctions. Si X est un ensemble quelconque, et A un anneau, rappelons que l'ensemble $\mathscr{F}(X,A)$ des fonctions de X dans A s'interprète naturellement comme un produit :

$$\mathscr{F}(X,A) \simeq A^X,$$

$$(f : X \to A) \mapsto (f(x))_{x\in X}.$$

Par exemple, l'ensemble des fonctions de $[0,1]$ dans $\mathbb{C}$ est naturellement muni d'une structure d'anneaux. Exercice : expliciter cette structure.

4.6 Sous-Anneaux

Définition 4.6.1 Soit A un anneau commutatif unitaire $B \subset A$ est appelé un **sous-anneau de** A si :

1. $(B,+)$ est un sous-groupe de $(A,+)$
2. $\forall (x,y) \in B^2,\ xy \in B$
3. $1_A \in B$

■ **Exemple 4.6** $A = \mathbb{R}^2$ et $B = \mathbb{R}\times\{0\}$
$(B,+,\times)$ est isomorphe à $\mathbb{R}$ en tant qu'anneau avec $1_B = (1,0)$
Cependant, $1_A = (1,1) \neq (1,0) = 1_B$. Donc B n'est pas un sous-anneau de A.

Il est souvent plus simple de montrer qu'un objet est un sous-anneau d'un anneau déjà connu que de vérifier qu'il s'agit bien d'un anneau. ■

■ **Exemple 4.7** $\mathbb{Z}[i] = \{a+bi \text{ où } a,b\in\mathbb{Z}\} \subset \mathbb{C}$ est un sous-anneau, appelé *Anneau des entiers de Gauß*.

1. $(a_1+ib_1)+(a_2+ib_2) = (a_1+a_2)+i(b_1+b_2) \in \mathbb{Z}[i]$
2. $(a_1+ib_1)(a_2+ib_2) = (a_1a_2-b_1b_2)+i(a_1b_2+a_2b_1)$
3. $1_{\mathbb{C}} = 1 = 1+0i \in \mathbb{Z}[i]$

■

4.7 Diviseurs de zéro, anneaux intègres

Définition 4.7.1

1. Soit A un anneau commutatif unitaire. Un élément $a \in A-\{0\}$ est appelé **diviseur de zéro** si $\exists b \in A-\{0\}$ tel que $ab = 0$.
2. On dit que A est **intègre** si A n'est pas l'anneau nul et qu'il ne contient aucun diviseur de zéro.

Lemme 4.7.1

1. Soit $x \in A^\times$ (x inversible), alors x n'est pas diviseur de zéro.
2. Un corps est un anneau intègre.

Démonstration.

1. Par l'absurde : $\exists b \in A^*$ tq $ab = 0 \Leftrightarrow a^{-1}ab = 0 \Leftrightarrow b = 0$
2. Si A est un corps, $A = A^\times \cup \{0\}$ qui ne contient aucun diviseur de zéro.

■

Lemme 4.7.2 Un sous-anneau d'un anneau intègre est intègre.

4.8 Exercices

Exercice 4.1 1. Soit $\mathscr{F}(\mathbb{R},\mathbb{R})$ l'ensemble de toutes les fonctions de $\mathbb{R}$ dans $\mathbb{R}$. Rappelez pourquoi c'est un anneau, et quelles sont ses lois de compositions ainsi que son neutre.
2. Soit $C^0(\mathbb{R},\mathbb{R})$ l'ensemble des fonctions continues de $\mathbb{R}$ dans $\mathbb{R}$, muni de l'addition et de la multiplication ponctuelle. Montrez que c'est un anneau.
3. Pour $k \geq 0$, soit $C^k(\mathbb{R},\mathbb{R})$ l'ensemble des fonctions k fois dérivables dont la dérivée k-ième est continue, muni de l'addition et de la multiplication ponctuelle. Montrez que c'est un anneau.

Exercice 4.2 Montrez que l'ensemble

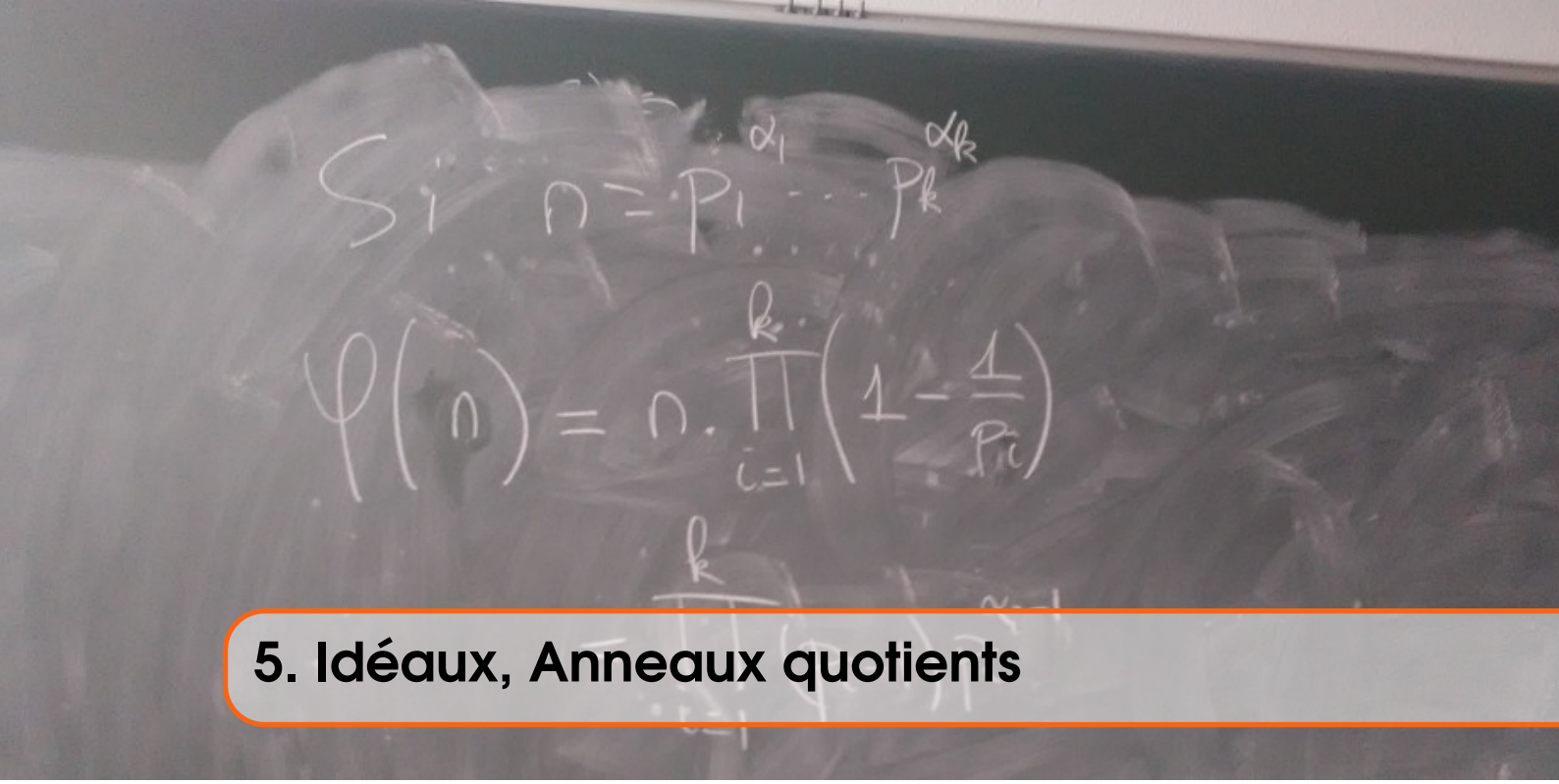
$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \,:\, (a,b) \in \mathbb{Z}^2\},$$

est un sous-anneau de $\mathbb{R}$, et qu'il est intègre.

Exercice 4.3 1. Quels sont les morphismes unitaires d'anneaux de $\mathbb{Z}$ dans $\mathbb{Z}$?
2. Quels sont les morphismes unitaires d'anneaux de $\mathbb{Z}$ dans $\mathbb{Q}$?
3. Quels sont les morphismes unitaires d'anneaux de $\mathbb{Q}$ dans $\mathbb{Z}$?
4. Quels sont les morphismes unitaires d'anneaux de $\mathbb{Q}$ dans $\mathbb{Q}$?
5. Quels sont les morphismes unitaires d'anneaux de $\mathbb{Z}[i]$ dans $\mathbb{Z}[i]$?
6. (plus dur) Quels sont les morphismes unitaires d'anneaux de $\mathbb{R}$ dans $\mathbb{R}$? *Indication* On pourra essayer de montrer qu'un tel morphisme doit être croissant en considérant les carrés de nombres réels.

Exercice 4.4 Déterminez le groupe des inversibles de $\mathbb{Z}[i]$.

Exercice 4.5 Montrer que l'anneau produit $\mathbb{Z} \times \mathbb{Z}$ n'est pas isomorphe à l'anneau $\mathbb{Z}[i]$. *Typiquement, pour ce genre de question qui demande de différencier deux objets, on trouve un propriété que possède l'un mais pas l'autre des objets.*



5. Idéaux, Anneaux quotients

5.1 Exemple : $\mathbb{F}_4$

Un des objectifs de ce chapitre est de pouvoir construire de nouvelles structures d'anneaux. Un exemple est le corps à quatre éléments $\mathbb{F}_4$, dont les éléments sont notés $0, 1, \alpha, \alpha+1$, avec les lois suivantes :

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	α	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	α

et

$\times$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

On voit tout de suite qu'il serait au mieux pénible de vérifier à la main que les lois $+, \times$ définies par ces tableaux sont associatives, distributives, etc. La bonne approche est plus conceptuelle et va nous permettre de construire $\mathbb{F}_4$ à partir d'anneaux existants, en étendant la notion de quotient.

5.2 Idéaux

Une notion centrale de la théorie des anneaux est celle d'idéal. Historiquement, les idéaux ont été introduits au XIXème siècle pour palier à certains défauts de la factorisation en premiers dans des anneaux ; de même que l'on introduit des nombres "imaginaires" pour obtenir une résolution formelle de l'équation $x^2+1=0$, Ernst Kummer introduisait des nombres "idéaux" pour obtenir une décomposition unique en facteurs premiers dans les anneaux de corps de nombre. Pour nous, l'intérêt des idéaux sera double : premièrement, ils sont indispensables pour définir les structures quotients. D'autre part, ils nous permettront d'identifier les anneaux dit *principaux*, où justement les "nombres idéaux" de Kummer s'identifient aux nombres "classiques" - car paradoxalement, pour pouvoir discuter d'objets caractérisés par "l'absence de", il faut commencer par parler de ce qui n'est pas (trop) là...

Définition 5.2.1 Soit A un anneau commutatif unitaire, $I \subset A$ est appelé un **idéal de** A si :
1. $(I,+)$ est un sous-groupe de $(A,+)$
2. I est absorbant : $\forall x \in I, \forall a \in I, ax \in I$

Lemme 5.2.1 **(Critère)** I est un idéal de A ssi :
- $I \neq \varnothing$
- $\forall \lambda \in A, \forall (x,y) \in I^2, \lambda x + y \in I$

Démonstration.
- $\boxed{\Rightarrow}$ $0 \in I \Rightarrow I \neq \varnothing$
  Par absorption, $\lambda x \in I$, donc $\lambda x + y \in I$
- $\boxed{\Leftarrow}$ $x - y = x + (-1)y \in I \Rightarrow I$ est un sous-groupe
  $\lambda x = \lambda x + 0 \in I \Rightarrow I$ absorbant.

■

▪ **Exemple 5.1**
- A, $\{0\}$ le sont
- $n\mathbb{Z}$ l'est dans $\mathbb{Z}$
- $\mathbb{R} \times \{0\}$ l'est dans $\mathbb{R}^2$

▪

Proposition 5.2.2
1. Soit $\varphi : A \to B$ un morphisme d'anneau, alors $Ker(\varphi)$ est un idéal de A
2. Soit J un idéal de B, alors $\varphi^{-1}(J)$ est un idéal de A
3. Si $\varphi : A \to B$ est surjectif et $I \subset A$ un idéal, $\varphi(I)$ est un idéal de B

Démonstration.
1. $ii) \Rightarrow i)$ en prenant $J = \{0\}$
2. Soit J un idéal de B, alors :
   - $0 \in J \Rightarrow 0 \in \varphi^{-1}(J) \Rightarrow \varphi^{-1}(J) \neq \varnothing$
   - Soit $(\lambda, x, y) \in A \times \varphi^{-1}(J) \times \varphi^{-1}(J)$,
     $\varphi(\lambda x + y) = \varphi(\lambda)\varphi(x) + \varepsilon(y) \in J$, donc $\lambda x + y \in \varphi^{-1}(J)$
3. Soit $\lambda \in B$, $x, y \in \varphi(I)$. $\exists a, b, c \in A$ tq $\begin{cases} \varphi(a) = \lambda \\ \varphi(b) = x \\ \varphi(c) = y \end{cases}$, alors :

$$\lambda x + y = \varphi(a)\varphi(b) + \varphi(c) = \varphi(ab + c) \in \varphi(I)$$

■

Proposition 5.2.3 Soit A un anneau commutatif unitaire et $x \in A$, alors Ax est un idéal, dit **idéal principal engendré par** x.

Démonstration. Comme $0 = 0x$, $0 \in Ax$ et Ax est non vide.
Soient $\lambda \in A$ et $u, v \in Ax$. $\exists a, b \in A$ tel que

$$\begin{cases} u = ax, \\ v = bx \end{cases}$$

Donc $\lambda u + v = x(\lambda a + b) \in xA$. ■

Cet idéal Ax est souvent noté (x), à ne pas confondre avec le sous-groupe additif engendré - qui lui n'est pas toujours un idéal.

Définition 5.2.2 Un anneau est dit **principal** si il est intègre et tous ses idéaux sont principaux (càd pour tout idéal I de A, il existe $x \in A$ tel que $I = (x) = Ax$).

▪ **Exemple 5.2** L'anneau des entiers relatifs $\mathbb{Z}$ est principal. En effet, soit I un idéal de $\mathbb{Z}$. C'est en particulier un sous-groupe, donc un ensemble de la forme $n\mathbb{Z}$, qui est un idéal principal. De plus $\mathbb{Z}$ est intègre, ce qui conclut. ▪

Proposition 5.2.4 Un anneau unitaire $A \neq \{0\}$ a pour seuls idéaux $\{0\}$ et A ssi c'est un corps.

Démonstration. $\boxed{\Rightarrow}$ Soit A un anneau dont les seuls idéaux sont $\{0\}$ et A.
Soit $x \in A - \{0\}$, $x = x1 \in Ax$ donc $Ax \neq \{0\}$.
Donc $Ax = A$, donc $1 \in Ax$, d'où il existe $y \in A$ tel que $xy = 1$, ainsi $x \in A^\times$.
$\boxed{\Leftarrow}$ Supposons que A soit un corps. Soit I un idéal de A.

- Soit $I = \{0\}$
- Sinon, $\exists x \in I - \{0\}$. Donc $\exists y \in A$ tq $xy = 1 \in I$
  Donc $\forall x \in A$, $x = 1x \in I$, donc $A = I$

■

5.3 Anneaux quotients

Soit I un idéal de A. On rappelle que , comme I est un sous-groupe additif de A, la relation modulo I par donnée par $x \sim y$ si $y - x \in I$. On sait qu'il existe une unique structure sur A/I tq $\pi \left| \begin{array}{ccc} A & \longrightarrow & A/I \\ x & \longmapsto & \overline{x} \end{array} \right.$ soit un morphisme de groupes additifs.

Théorème 5.3.1 Il existe une unique loi de composition interne $\times$ sur le quotient A/I telle que A/I soit un anneau commutatif unitaire et π soit un morphisme unitaire d'anneaux.

Démonstration.
On sait déjà qu'il existe une seule structure de groupe additif sur A/I telle que la projection canonique soit un morphisme de groupe. Il nous faut simplement prouver qu'il existe une seule loi multiplicative pour laquelle cette même projection est un morphisme d'anneaux.

* **Unicité :** Supposons qu'il existe cette loi $\times$, alors nécéssairement :

$$\overline{x} \times \overline{y} = \pi(x) \times \pi(y) = \pi(xy) = \overline{xy},$$

ce qui impose la loi $\times$ (sans prouver qu'elle soit bien définie).

* **Existence :** Il faut vérifier que $\forall \overline{x}, \overline{y}, \overline{a}, \overline{b} \in A/I$ tels que

$$\begin{cases} \overline{x} = \overline{a} \\ \overline{y} = \overline{b} \end{cases}, \overline{xy} = \overline{ab},$$

alors $\overline{xy} = \overline{ab}$. En effet,

$$\begin{aligned} xy - ab &= xy + xb - xb + ab \\ &= x(y-b) + b(x-a) \\ &\in I \text{ par absorption.} \end{aligned}$$

Il faut ensuite vérifier que $(A/I, +, \times)$ est bien un anneau :

- $(\overline{x}\times\overline{y})\times\overline{z}=\overline{xy}\times\overline{z}=\overline{xyz}=\overline{x}\times\overline{yz}=\overline{x}\times(\overline{y}\times\overline{z})$
- $\overline{x}\times(\overline{y}+\overline{z})=\overline{x(y+z)}=\overline{xy+xz}=\overline{xy}+\overline{xz}=\overline{xy}+\overline{xz}$
- $\overline{x}=\overline{1}\times\overline{x}=\overline{1x}=\overline{x1}=\overline{x}\times\overline{1}$
- $\times$ est commutatif (clair)
- $\pi : A\to A/I$ est un morphisme (facile).

■

En particulier, $\mathbb{Z}/n\mathbb{Z}$ a naturellement une strucure d'anneau.

Théorème 5.3.2 Soit $n\geq 2$, on a équivalence entre
1. $\mathbb{Z}/n\mathbb{Z}$ est un corps
2. $\mathbb{Z}/n\mathbb{Z}$ est intègre
3. n est premier

Démonstration.
- $\boxed{1)\Rightarrow 2)}$ Trivial.
- $\boxed{2)\Rightarrow 3)}$ Par contraposée. Soit $n=ab$, avec $1<a<n, 1<b<n$ donc $\overline{0}=\overline{ab}$, mais $\overline{a}\neq\overline{0}$ et $\overline{b}\neq\overline{0}$. Donc $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre.
- $\boxed{3)\Rightarrow 1)}$ Soit $\overline{x}\in(\mathbb{Z}/n\mathbb{Z})-\{\overline{0}\}$, montrons que $\overline{x}$ est inversible.
Par le théorème de Bézout : $\exists a,b\in\mathbb{Z}$ tq $ax+bn=1$. Appliquons la projection canonique , on obtient $\overline{ax}=\overline{1}$ Donc, $\overline{a}$ est l'inverse de $\overline{x}$.

■

5.4 Factorisation des morphismes

Théorème 5.4.1 Soient A et B deux anneaux et I un idéal de A. On pose $\pi : A\to A/I$ la projection canonique et $f : A\to B$ un morphisme d'anneaux. Alors il y a équivalence entre :
1. $I\subset Ker(f)$
2. $\forall x\in I, f(x)=0$
3. $\exists\overline{f} : A/I\to B$ un morphisme d'anneau tel que $f=\overline{f}\circ\pi$

Si ces conditions sont vérifiées, $\overline{f}$ est unique et $\begin{cases} Im(\overline{f})=Im(f) \\ Ker(\overline{f})=\ker(f)/I \end{cases}$

Démonstration. Si on applique le théorème au morphisme de groupe f, on en déduit les équivalences recherchées. Il suffit donc de montrer qu'en plus d'être un morphisme de groupe, $\overline{f}$ est aussi un morphisme d'anneaux.
- Soit $(\overline{x},\overline{y})\in(A/I)^2$, $\overline{f}(\overline{xy})=f(xy)=f(x)f(y)=\overline{f}(\overline{x})\overline{f}(\overline{y})$
- $\overline{f}(\overline{1_A})=f(1_A)=1_B$

■

■ **Exemple 5.3** On pose $A=\mathbb{Z}[j]=\{a+bj\,;\,a,b\in\mathbb{Z}\}$, où $j=e^{2i\pi/3}$. On peut remarquer les choses suivantes : $j^3=1$ donc $0=j^3-1=(j-1)(j^2+j+1)$, d'où $0=j^2+j+1$ ou encore $j^2=-j-1$.

Montrons que A est un sous-anneau de $\mathbb{C}$:
On pose $z_1=a_1+jb_1$ et $z_2=a_2+jb_2$, deux éléments quelconques de A
- $A\neq\varnothing$
- $(A,+)$ sous-groupe : $z_1-z_2=(a_1-a_2)+j(b_1-b_2)\in A$

- stabilité par $*$:

$$\begin{aligned} z_1 * z_2 &= (a_1 + jb_1)(a_2 + jb_2) \\ &= a_1a_2 + j^2 b_1 b_2 + j(a_1 b_2 + a_2 b_1) \\ &= (a_1a_2 - b_1 b_2) + j(a_1 b_2 + a_2 b_1 - b_1 b_2) \\ &\in A. \end{aligned}$$

- $1 = 1 + 0j \in A$.

Prenons $I = 2\mathbb{Z}[j] = \{a + bj \,;\, a, b \text{ pairs}\}$. C'est l'idéal principal engendré par 2. Les quatres classes de A/I sont

$$A/I = \{\overline{0}, \overline{1}, \overline{j}, \overline{j+1}\},$$

et en tant que groupe additif,

$$(A/I, +) \sim (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +).$$

On peut facilement calculer les lois + et × sur le quotient A/I :

$+$	$\overline{0}$	$\overline{1}$	$\overline{j}$	$\overline{j+1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{j}$	$\overline{j+1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{j+1}$	$\overline{j}$
$\overline{j}$	$\overline{j}$	$\overline{j+1}$	$\overline{0}$	$\overline{1}$
$\overline{j+1}$	$\overline{j+1}$	$\overline{j}$	$\overline{1}$	$\overline{0}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{j}$	$\overline{j+1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{j}$	$\overline{j+1}$
$\overline{j}$	$\overline{0}$	$\overline{j}$	$\overline{j+1}$	$\overline{1}$
$\overline{j+1}$	$\overline{0}$	$\overline{j+1}$	$\overline{1}$	$\overline{j}$

En d'autre termes, $\mathbb{Z}[j]/2\mathbb{Z}[j]$ est un corps à 4 éléments. ∎

5.5 Exercices

Exercice 5.1 Pour les anneaux $A = \mathbb{Z}/n\mathbb{Z}$, on considère les cas $n \in \{3, 6, 7, 12\}$.
1) Faites la liste des éléments inversibles et des diviseurs de zéro.
2) Quels sont les idéaux de A ? Faites la liste.

Exercice 5.2 Quels sont les morphismes d'anneaux de $\mathbb{Z}/n\mathbb{Z}$ ($n \geq 2$), vers $\mathbb{C}$?

Exercice 5.3 Soient n, m deux entiers $\geq n$. Déterminez une condition nécéssaire et suffisante à l'existence d'un morphisme d'anneaux de $\mathbb{Z}/n\mathbb{Z}$ vers $\mathbb{Z}/m\mathbb{Z}$.

Exercice 5.4 Soit k un corps, $x \in k$.
1) Montrez que

$$I_x = \{P \in k[X] \,:\, P(x) = 0\},$$

est un idéal de $k[X]$.
2) Tout idéal de $k[X]$ est-il de cette forme ?
3) Déterminez $k[X]^\times$.

Exercice 5.5 Soit A un anneau commutatif unitaire. Soit $a \in A - \{0\}$, on considère l'application

$$m_a : A \to A, x \mapsto ax.$$

1) Est-ce que m_a est un morphisme de groupes ? d'anneaux ?
2) Montrez que m_a est injective si et seulement si a n'est pas diviseur de zéro.

3) Montrez que m_a est surjective si et seulement si a est inversible.
4) En déduire qu'un anneau intègre et fini est un corps.

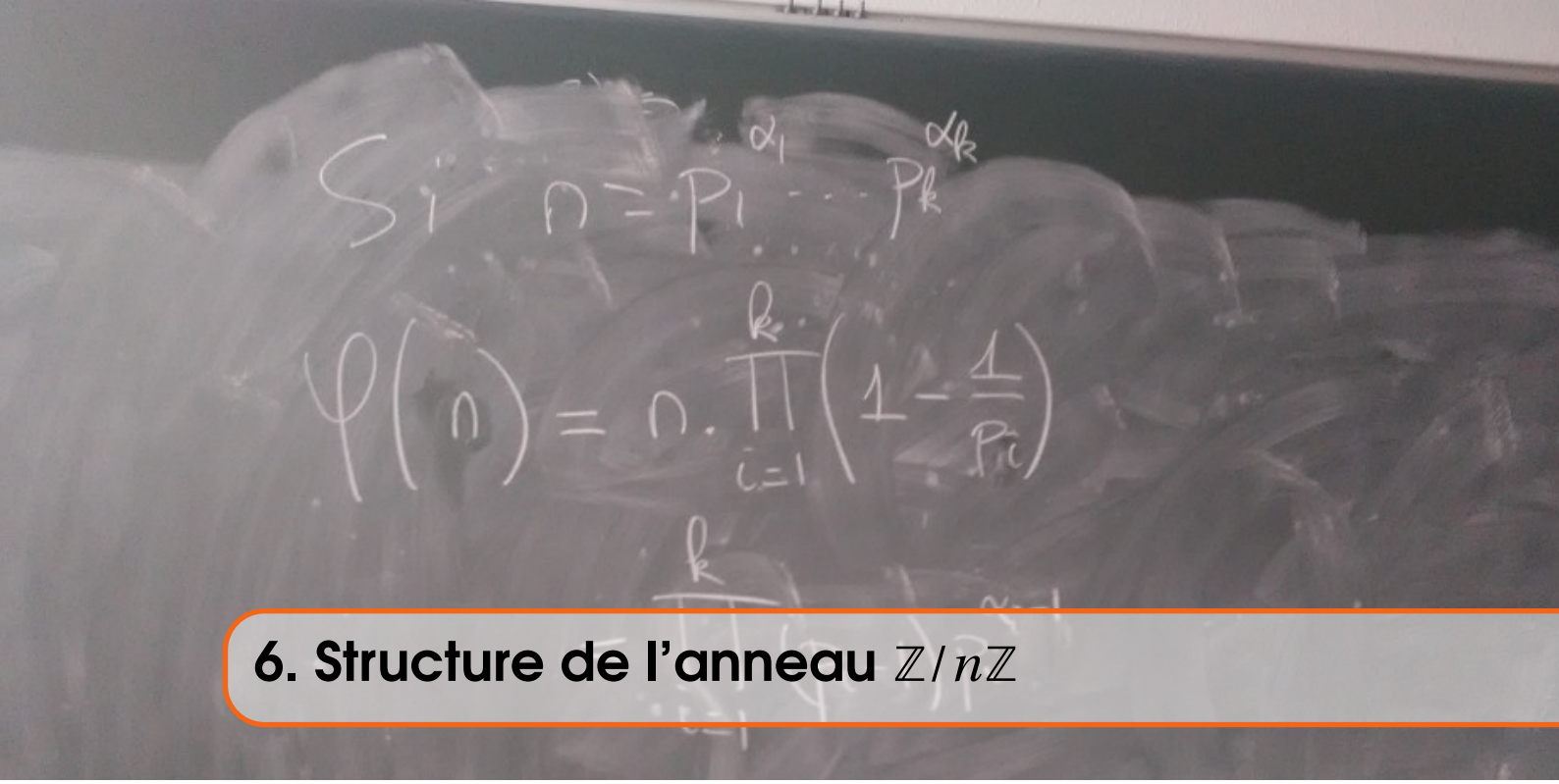
Exercice 5.6 Montrez qu'un morphisme d'anneaux d'un corps k vers un anneau non nul A est nécéssairement injectif.

Exercice 5.7 Résoudre l'équation d'inconnue X :

$$X^3 = 2$$

dans les anneaux suivants :
a) $\mathbb{Z}/5\mathbb{Z}$,
b) $\mathbb{Z}/25\mathbb{Z}$,
c) $\mathbb{Z}/125\mathbb{Z}$.
Indication : on pourra, dans les cas b) et c), essayer de se ramener partiellement au cas précédent pour éviter des calculs trop longs...

Exercice 5.8 Soit $p \neq 2$ un nombre premier impair.
1) Montrez que $\psi : (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$, $\psi(x) = x^2$, est un morphisme de groupe. Quel est son noyau ?
2) Montrez qu'un élément de $(\mathbb{Z}/p\mathbb{Z})^\times$ est un carré si et seulement si $x^{(p-1)/2} = 1$.
3) Combien y-a-t-il de carrés dans $(\mathbb{Z}/p\mathbb{Z})$?



6. Structure de l'anneau $\mathbb{Z}/n\mathbb{Z}$

6.1 Groupes cycliques

Définition 6.1.1

- Un groupe est dit **monogène** si il est engendré par un seul élément : $\exists x \in G$ tel que $\langle x \rangle = G$.
- Un groupe est dit **cyclique** si il est monogène et fini.
- Un **générateur** du groupe (monogène) G est un élément $g \in G$ tel que $G = \langle g \rangle$.

Théorème 6.1.1 Soit $G = \langle g \rangle$ un groupe monogène, alors :

1. Si G est infini, G est isomorphe à $\mathbb{Z}$
2. Si G est fini, on note $n = |G|$ et G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$

Démonstration. Soit $\varphi_g \left| \begin{array}{ccc} \mathbb{Z} & \longrightarrow & G \\ n & \longmapsto & g^n \end{array} \right.$ l'application d'itération. On a vu que c'est un morphisme de groupe. Comme g génère G, φ_g est surjectif. $Ker(\varphi_g)$ est un sous-groupe de $\mathbb{Z}$, donc égal à $n\mathbb{Z}$ pour un certain $n \in \mathbb{N}$. D'après le théorème de factorisation des morphismes, il existe un unique morphisme $\overline{\varphi_g} : \mathbb{Z}/n\mathbb{Z} \to G$ tel que $\varphi_g = \overline{\varphi_g} \circ \pi$ avec $\begin{cases} Im(\overline{\varphi_g}) = Im(\varphi_g) = G \\ Ker(\overline{\varphi_g}) = Ker(\varphi_g)/n\mathbb{Z} = \{\overline{0}\} \end{cases}$

Donc, $\overline{\varphi_g}$ est injectif et surjectif, c'est un isomorphisme.

1. Si $n = 0$, φ_g est injectif, donc $G \sim \mathbb{Z}$
2. Si $n \geq 1$, φ_g est un isomorphisme, donc $|\mathbb{Z}/n\mathbb{Z}| = |G| = n$

■

6.2 Générateur d'un groupe cyclique

Théorème 6.2.1 **(de Bézout)** Soit $(a, b) \in \mathbb{Z}^2$, alors $a \wedge b = 1 \Leftrightarrow \exists (u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$

Théorème 6.2.2 Soit $G = \langle x \rangle$ un groupe monogène, alors :
1. Si G est infini, les seuls générateurs de G sont x et x^{-1}.
2. Si G est cyclique, les générateurs de G sont $\{x^k\ ;\ k \in \mathbb{Z} \text{ et } k \wedge |G| = 1\}$.

Démonstration. Il suffit de démontrer les énoncés analogues dans $\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$.
1. Si $n \in \mathbb{Z}$, $\langle n \rangle = n\mathbb{Z}$ qui est égal à $\mathbb{Z}$ ssi $n = \pm 1$
2. $\boxed{\subset}$ Supposons $G = (\mathbb{Z}/n\mathbb{Z}, +)$, soit $x \in G$ tel que $\langle x \rangle = G = \mathbb{Z}x$
   En particulier, $\mathbb{Z}x \ni \overline{1}$, donc $\exists k \in \mathbb{Z}$ tel que $k\overline{x} = 1$, c'est-à-dire $\exists p \in \mathbb{Z}$ tel que $kx = 1 + pn$, ou encore $kx - pn = 1$.
   Par le théorème de Bézout, $x \wedge n = 1$.
   $\boxed{\supset}$ Si $x \wedge n = 1$, $\exists (u, v) \in \mathbb{Z}^2$ tel que $xu + vn = 1$, donc $u\overline{x} = \overline{1}$.
   Donc, $G = \langle \overline{1} \rangle \subset \langle \overline{x} \rangle$, donc $\overline{x}$ est générateur de G.

■

Corollaire 6.2.3 Soit $n \geq 2$, alors

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{x} : x \wedge n = 1\} = \{\text{générateurs de } (\mathbb{Z}/n\mathbb{Z}, +)\}.$$

6.3 Fonction indicatrice d'Euler

Définition 6.3.1 Pour $n \geq 2$, on définit **l'indicatrice d'Euler**

$$\varphi(n) = card\left\{x \in \{1, ..., n-1\} \text{ tels que } x \wedge n = 1\right\} = |(\mathbb{Z}/n\mathbb{Z})^\times|.$$

.

■ **Exemple 6.1**
- $\varphi(1) = 1$ par convention
- $\varphi(2) = 1$
- $\varphi(3) = 2$
- $\varphi(4) = 2$
- ...

■

Lemme 6.3.1 Soit $n \in \mathbb{N}^*$ et $d|n$, alors il n'y a qu'un seul sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d, qui est cyclique et engendré par $\left(\overline{\frac{n}{d}}\right)$.

Démonstration. La démonstration est vu en TD, exercice 2 de la Feuille 2. ■

Théorème 6.3.2 Pour tout $n \in \mathbb{N}^*$, on a

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

Démonstration. Regardons l'application $\left|\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \{\text{sous-groupe de } \mathbb{Z}/n\mathbb{Z}\} \\ \overline{x} & \longmapsto & \langle \overline{x} \rangle \end{array}\right.$. Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont $\{H_d\}_{d|n}$, et $|H_d| = d$ d'après le lemme précédent.
Chaque H_d a exactement $\varphi(d)$ générateurs. Si on fait le compte, $n = \sum_{d|n} \varphi(d)$ ■

■ **Exemple 6.2** Si on regarde les premières valeurs de n , on obtient les relations :
- $\varphi(1) = 1$,

- $\varphi(1)+\varphi(2)=2$,
- $\varphi(1)+\varphi(3)=3$,
- $\varphi(1)+\varphi(2)+\varphi(4)=4$,
- $\varphi(1)+\varphi(5)=5$,
- $\varphi(1)+\varphi(2)+\varphi(3)+\varphi(6)=6$,
- ...

On voit que l'on obtient un système linéaire *triangulaire*, facile à inverser. Il est cependant possible d'obtenir une formule close pour $\varphi(n)$, c'est l'objet de la section suivante. ∎

6.4 Convolution de Dirichlet et Inversion de Möbius

Nous pourrions donner la formule finale pour φ et la démontrer par une simple récurrence, ce qui serait très rapide. Ce n'est pas la voie que l'on a choisie ici : nous allons tout d'abord regarder un exemple (assez original) d'anneau commutatif unitaire, à savoir l'anneau de convolution de Dirichlet.

Soit $\mathbb{C}^{\mathbb{N}^*}=\{(u_n)_{n\in\mathbb{N}^*}\}$ l'ensemble des suites à valeurs dans $\mathbb{C}$. On définit les lois de composition internes suivantes :

$$+\left|\begin{array}{ccc}\mathbb{C}^{\mathbb{N}^*}\times\mathbb{C}^{\mathbb{N}^*} & \longrightarrow & \mathbb{C}^{\mathbb{N}^*}\\ ((u_n)_{n\geq 1},(v_n)_{n\geq 1}) & \longmapsto & (u+v)_n=u_n+v_n\end{array}\right.,$$

et

$$*\left|\begin{array}{ccc}\mathbb{C}^{\mathbb{N}^*}\times\mathbb{C}^{\mathbb{N}^*} & \longrightarrow & \mathbb{C}^{\mathbb{N}^*}\\ ((u_n)_{n\geq 1},(v_n)_{n\geq 1}) & \longmapsto & (u*v)_n=\sum\limits_{n=pq}u_pv_q\end{array}\right..$$

Ce produit est appelé *produit de convolution*. Enfin, on définit l'élément $\delta=(\delta_n)_{n\geq 1}$ par

$$\delta_n=\begin{cases}1 \text{ si } n=1\\ 0 \text{ si } n\geq 2\end{cases}$$

Théorème 6.4.1 $(\mathbb{C}^{\mathbb{N}^*},+,*)$ est un anneau commutatif unitaire, appelé *Anneau de convolution de Dirichlet.*

Démonstration.

- $(\mathbb{C}^{\mathbb{N}^*},+)$ est simplement le groupe produit $\mathbb{C}^{\mathbb{N}^*}$.
- Vérifions que $*$ est associative : Soit $(u,v,w)\in\left(\mathbb{C}^{\mathbb{N}^*}\right)^3$

$$\begin{aligned}[u*(v*w)]_n&=\sum_{n=pq}u_p(v*w)_q\\ &=\sum_{n=pq}\left(u_p\sum_{q=rs}v_rw_s\right)\\ &=\sum_{n=pq}\left(\sum_{q=rs}u_pv_rw_s\right)\\ &=\sum_{n=prs}u_pv_rw_s\end{aligned}$$

Grâce à ce résultat, on réorganiser p, r, et s à notre guise, donc

$$[u*(v*w)]_n=[(u*v)*w]_n.$$

- $*$ est commutatif : Soit $(u,v,w) \in \left(\mathbb{C}^{\mathbb{N}^*}\right)^2$,

$$(u*v)_n = \sum_{n=pq} u_p v_q = \sum_{n=qp} v_q u_p = (v*u)_n.$$

- $*$ est distributive : $(u,v,w) \in \left(\mathbb{C}^{\mathbb{N}^*}\right)^3$

$$\begin{aligned}
[u*(v+w)]_n &= \sum_{n=pq} u_p (v+w)_q \\
&= \sum_{n=pq} u_p (v_q + w_q) \\
&= \sum_{n=pq} u_p v_q + u_p w_q \\
&= \sum_{n=pq} u_p v_q + \sum_{n=pq} u_p w_q \\
&= (u*v)_n + (u*w)_n.
\end{aligned}$$

- Neutre : $(u*\delta)_n = \sum_{n=pq} u_p \delta_q = u_n \delta_1 = u_n$.

■

Définition 6.4.1 La **fonction de Möbius** est définie comme suit :

$$\mu \left| \begin{array}{ccc} \mathbb{N}^* & \longrightarrow & \{-1,0,1\} \\ n & \longmapsto & \begin{cases} 0 & \text{si un carré } (\neq 1) \text{ divise } n \\ (-1)^k & \text{si } n = p_1 \dots p_k,\ p_i \text{ premiers distincts} \end{cases} \end{array} \right.$$

Exemples :

- $\mu(1) = 1$
- $\mu(2) = -1$
- $\mu(3) = -1$
- $\mu(4) = 0$
- $\mu(5) = -1$
- $\mu(6) = 1$
- ...

Enfin, on note $\mathbb{1}$ la suite constante égale à 1. Notez bien que ce n'est pas l'unité de l'anneau de convolution !

Lemme 6.4.2 La fonction de Möbius est l'inverse de la constante $\mathbb{1}$ pour le produit de convolution.

Démonstration. Calculons simplement la suite $\mathbb{1} * \mu$.

- Pour le premier terme, $(\mathbb{1} * \mu)_1 = 1 * \mu(1) = 1$.

- Soit $n \geq 2$, $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ sa décomposition en nombre premier.

$$\begin{aligned}
(\mathbb{1} * \mu)_n &= \sum_{\substack{n=ab \\ b=p_1^{\beta_1}\dots p_k^{\beta_k} \\ 0\leq\beta_i\leq\alpha_i}} \mathbb{1}(a)\mu(b) \\
&= \sum_{0\leq\beta_i\leq 1} \mu(p_1^{\beta_1}\dots p_k^{\beta_k}) \\
&= \sum_{0\leq\beta_1\leq 1} (-1)^{\sum\beta_i} \\
&\quad \vdots \\
&\quad 0\leq\beta_k\leq 1 \\
&= \sum_{n=0}^{k} \binom{k}{n} (-1)^n \\
&= (1-1)^k = 0.
\end{aligned}$$

■

Corollaire 6.4.3 (Formule d'inversion de Möbius) Soient $(u_n)_n$ et $(v_n)_n$ deux suites tel que

$$v_n = \sum_{d|n} u_d,$$

alors

$$v_n = \sum_{d_1 d_2 = n} \mu(d_1) u_{d_2}.$$

Démonstration. En effet, $u = v * \mathbb{1}$, donc $u * \mu = v * \mathbb{1} * \mu = v * \delta = v$. ■

Théorème 6.4.4 *(Formule pour l'indicatrice d'Euler)*
Si $n = \prod_{i=1}^{k} p_i^{a_i}$ est la décomposition de n en facteurs premiers, alors

$$\varphi(n) = \prod_{i=1}^{k} (p_i - 1) p_i^{a_i - 1}.$$

Autrement dit,

$$\frac{\varphi(n)}{n} = \prod_{i=1}^{k} (1 - \frac{1}{p_i}).$$

Démonstration. On applique la formule d'inversion de Möbius : $\varphi(n) = \sum_{n=d_1 d_2} \mu(d_1) d_2$. Ecrivons $d_1 = \prod_{i=1}^{k} p_i^{b_i}$ où $0 \leq b_i \leq a_i$.

Comme $\varphi(d_1) = 0$ si un des $b_i \geq 2$,

$$\begin{aligned}\varphi(n) &= \sum_{0\leq b_i\leq 1} \mu\left(\prod_{i=1}^{k} p_i^{b_i}\right) \prod_{i=1}^{k} p_i^{a_i-b_i} \\ &= \sum_{0\leq b_i\leq 1} (-1)^{\sum b_i} \prod_{i=1}^{k} p_i^{a_i-b_i} \\ \frac{\varphi(n)}{n} &= \sum_{0\leq b_i\leq 1} \prod_{i=1}^{k} \left(\frac{-1}{p_i}\right)^{b_i} \\ &= \left(1-\frac{1}{p_1}\right)\ldots\left(1-\frac{1}{p_n}\right)\end{aligned}$$

En multipliant ce résultat par n, on obtient la formule cherchée.

■

▪ **Exemple 6.3**

- $\#(\mathbb{Z}/24\mathbb{Z})^\times = \varphi(24) = \varphi(2^3 * 3) = 8$.
- $\#(\mathbb{Z}/210\mathbb{Z})^\times = \varphi(2*3*5*7) = (2-1)*(3-1)*(5-1)*(7-1) = 48$.

▪

Définition 6.4.2 (suites multiplicatives) Une suite $(u_n)_{n\geq 1}$ est dite *multiplicative* si $\forall (n,m) \in (\mathbb{N}^*)^2$ tels que $n \wedge m = 1$, alors $u_{nm} = u_n u_m$.

▪ **Exemple 6.4** $(Id)_n$, $(\mu(n))_n$ et $(\mathbb{1})_n$ sont multiplicatives. ▪

Proposition 6.4.5 Le produit de convolution de deux suites multiplicatives est multiplicative.

Application : $\varphi = Id * \mu$ est multiplicative.

6.5 Applications arithmétiques

Théorème 6.5.1 Soit $n \geq 2$ et $\overline{x} \in (\mathbb{Z}/n\mathbb{Z})^\times$, c'est à dire que $\overline{x}$ est la classe d'un entier x premier à n. Alors,

$$\overline{x}^{\varphi(n)} = \overline{1},$$

égalité ayant lieu dans $\mathbb{Z}/n\mathbb{Z}$, autrement dit

$$x^{\varphi(n)} \equiv 1 \text{ (mod n)}.$$

Démonstration. D'après le théorème de Lagrange, l'ordre de $\overline{x}$ dans le groupe multiplicatif $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ divise $\varphi(n)$. D'où le résultat. ■

Corollaire 6.5.2 (petit théorème de Fermat) Si p est un nombre premier, alors $\forall x \in \mathbb{Z}$,

$$x^p \equiv x \text{ (mod p)}.$$

Démonstration. On a $\varphi(p) = p-1$.

- **1er cas :** $p|n$, alors $x^p \equiv 0 \equiv x$ (mod p).
- **2eme cas :** $p \nmid n$, donc $p \wedge n = 1$. Alors, $x^p \equiv x \times (x^{p-1}) \equiv x$ (mod p).

■

La réciproque est fausse.

Définition 6.5.1 Un entier n est dit *de Carmichael* si il n'est pas premier et que pour tout $x \in \mathbb{Z}$, on a $x^n \equiv x \pmod{p}$.

Un exemple de tel nombre est 561, qui est le plus petit. Si ils sont relativement rares, il y en a "plus" que de puissances quatrièmes.

Théorème 6.5.3 — (Alfred, Granville, Pomerance - 1994). Il existe une infinité de nombre de Carmichael, et pour n assez grand, il y en a au moins $n^{2/7}$ dans l'intervalle $[1, n]$.

6.6 Test de primalité

On se donne un entier n et on aimerait prouver que n est composite (composé) sans avoir à exhiber de diviseur. En supposant que n est impair, on calcule par exemple $2^n \bmod n$. Si $2^n \neq 2 \pmod{n}$, alors n n'est pas premier. Sinon, le test n'est pas concluant.

▪ **Exemple 6.5** $n = 27 = 16 + 8 + 2 + 1 = 2^4 + 2^3 + 2^1 + 2^0$

$$2^0 = 1_{[27]}$$
$$2^1 = 2_{[27]}$$
$$2^2 = 4_{[27]}$$
$$2^4 = 4^2 = 16_{[27]}$$
$$2^8 = 16^2 = 13_{[27]}$$
$$2^{16} = 13^2 = 7_{[27]}$$

Donc, $2^{27} = 2^{16+8+2+1} = 2^{16} \times 2^8 \times 2^2 \times 2^1 = 7 \times 13 \times 4 \times 2 = 26_{[27]}$ et 27 n'est pas premier. ▪

6.7 Théorème des nombres chinois

Théorème 6.7.1 Soient $n, m \geq 2$ tel que $n \wedge m = 1$, alors on a un isomorphisme entre $\mathbb{Z}/nm\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

R Une conséquence est la multiplicité de φ. On a en effet

$$(n \wedge m = 1) \Rightarrow \varphi(nm) = \varphi(n)\varphi(m).$$

6.8 Exercices

Exercice 6.1 A l'aide de l'algorithme d'Euclide, déterminez l'inverse de :
1) 11 modulo 100,
2) 10 modulo 13,
3) 101 modulo 1000,
4) 110 modulo 1000 (piège ?)

Exercice 6.2 1) Déterminez la liste des éléments de $(\mathbb{Z}/20\mathbb{Z})^\times$.
2) Déterminez la liste des éléments de $(\mathbb{Z}/25\mathbb{Z})^\times$.
3) Quels sont les diviseurs de zéro dans $(\mathbb{Z}/25\mathbb{Z})^\times$?
4) Montrez que 2 est d'ordre 20 dans $((\mathbb{Z}/25\mathbb{Z})^\times, \times)$.
5) Le groupe $((\mathbb{Z}/25\mathbb{Z}), +)$ est-il cyclique ? Si oui, déduire des questions précédentes la liste de ses générateurs.

6) Le groupe $((\mathbb{Z}/25\mathbb{Z})^\times, \times)$ est-il cyclique ? Si oui, déduire des questions précédentes la liste de ses générateurs.
7) Montrez que l'on peut définir un *logarithme discret*, plus précisémment une application *notée* $\log_2$:

$$\log_2 : (\mathbb{Z}/25\mathbb{Z})^\times \to \{k \in \mathbb{N} : 0 \leq k \leq 19\},$$

telle que $2^{\log_2(\overline{x})} = \overline{x} \bmod 25$, et donnez quelques une de ses valeurs.
8) Y-a-t-il une relation, et si oui, laquelle, entre $\log_2(x)$ et $\log_2(x^{-1})$? En déduire une valeur de $\log_2$ que vous n'aviez pas précédemment.

Exercice 6.3 1) Déterminez l'ordre du groupe $((\mathbb{Z}/100\mathbb{Z})^\times, \times)$ (On ne demande pas de les compter individuellement !).
2) Dans un groupe cyclique d'ordre 40, combien y-a-t-il d'éléments d'ordre 2 ?
3) Calculez les ordres de 49 et 99 dans $((\mathbb{Z}/100\mathbb{Z})^\times, \times)$. Le groupe $((\mathbb{Z}/100\mathbb{Z})^\times, \times)$ est-il cyclique ?

Exercice 6.4 Soit p un nombre premier, tel qu'il existe un entier $k \geq 1$ tel que $p = 2^k + 1$. Un tel nombre premier est dit *de Fermat*, et les seuls connus sont $p = 3, 5, 17, 257, 65537$. Le but de l'exercice est de démontrer que pour un tel nombre premier de Fermat, k est nécessairement une puissance de 2, c'est à dire qu'en fait $p = 2^{2^n} + 1$ pour un certain $n \geq 0$.

Nos hypothèses sont donc : Soit $k \geq 1$ un nombre entier, tel que $p = 2^k + 1$ est premier.
1) Montrez que l'ordre de $\overline{2}$ dans le groupe multiplicatif $G = (\mathbb{Z}/p\mathbb{Z})^\times$ est nécessairement $> k$.
2) Montrez que l'ordre de $\overline{2}$ divise $2k$.
3) Déduisez-en que $\overline{2}$ est d'ordre $2k$.
4) Quel est le cardinal de G ? Déduisez-en que k est une puissance de 2.

7. Polynômes à une variable

Le lecteur est sans doute familier avec les polynômes réels $\mathbb{R}[x]$ ou complexes $\mathbb{C}[X]$. Nous redéfinissons ici la notion de polynôme, pour pouvoir considérer des polynômes à coeffcients dans un anneau commutatif unitaire arbitraire, par exemple $\mathbb{Z}/4\mathbb{Z}[X]$.

7.1 Construction

Soit A un anneau commutatif unitaire, $A^{(\mathbb{N})}$ désigne l'ensemble des suites de A presques nulles : $A^{(\mathbb{N})} = \{(a_n)_{n\geq 0} \text{ tq } \exists N \in \mathbb{N}, \forall n \geq N, a_n = 0\}$.

On munit cet ensemble des deux LCI suivantes :

$$+ \left| \begin{array}{ccc} A^{(\mathbb{N})} \times A^{(\mathbb{N})} & \longrightarrow & A^{(\mathbb{N})} \\ (a_n)_n, (b_n)_n & \longmapsto & (a_n)_n + (b_n)_n = (a_n + b_n)_n \end{array} \right. ,$$

et

$$\times \left| \begin{array}{ccc} A^{(\mathbb{N})} \times A^{(\mathbb{N})} & \longrightarrow & A^{(\mathbb{N})} \\ (a_n)_n, (b_n)_n & \longmapsto & (a_n)_n (b_n)_n = \left(\sum_{i=0}^{n} a_i b_{n-i} \right)_n \end{array} \right. ,$$

On note $0 = (0, 0, ...)$, $1 = (1, 0, 0, ...)$, et enfin $X = (0, 1, 0, 0, ...)$.

On note $A[X]$ la structure $(A^{(\mathbb{N})}, +, \times)$.

Lemme 7.1.1 Tout polynôme p de $A[X]$ a une écriture unique $(a_n)_n = \sum_{n\in\mathbb{N}} a_n X^n$.

En particulier, deux polynômes sont égaux si et seulement leurs coefficients sont égaux.

Théorème 7.1.2 $A[X]$ est un anneau commutatif unitaire.

Proposition 7.1.3 L'application $\left| \begin{array}{ccc} A & \longrightarrow & A[X] \\ a & \longmapsto & (a, 0, 0, ...) \end{array} \right.$ est un morphisme d'anneau injectif qui permet d'identifier A à un sous-anneau de $A[X]$.

R Les polynômes *ne sont pas* des fonctions. Illustrons par un exemple : L'ensemble des fonctions de $\mathbb{Z}/3\mathbb{Z}$ dans lui-même est $\mathscr{F}(\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}) = (\mathbb{Z}/3\mathbb{Z})^{(\mathbb{Z}/3\mathbb{Z})}$, qui a pour cardinal 27. L'ensemble des polynômes $\mathbb{Z}/3\mathbb{Z}[X]$ est quand à lui infini (il contient par exemple les polynômes distincts $1, X, X^2, X^3, ..$).
On sait que $\forall x \in \mathbb{Z}/3\mathbb{Z}$, $x^3 = x$. Donc la fonction polynômiale X^3 coïncide avec la fonction polynômiale X, et pourtant il s'agit de deux polynômes différents.

7.2 Propriété universelle

La manipulation de base que l'on peut faire avec un polynôme est de remplacer la variable X par une valeur : on peut *évaluer* un polynôme en un point. En termes théoriques, ceci donne lieu à un morphisme d'anneaux. Le théorème suivant dit même qu'en un certain sens, c'est la seule opération possible.

Théorème 7.2.1 Soit A et B deux anneaux commutatifs unitaires et $\phi : A \to B$ un morphisme d'anneau. Soit $\beta \in B$. Il existe un unique morphisme d'anneaux $e^{\phi}_{\beta} : A[X] \to B$ tel que

$$\begin{cases} e^{\phi}_{\beta}|_A = \phi \\ e^{\phi}_{\beta}(X) = \beta \end{cases}$$

Le morphisme e^{ϕ}_{β} est appelé **morphisme d'évaluation** en β selon ϕ. Réciproquement, tout morphisme d'anneaux de $A[X]$ dans B est un morphisme d'évaluation pour un certain β et un certain ϕ.

Dans beaucoup de cas, on a $A = B$ et $\phi = id_A$, mais ce n'est pas le seul cas intéressant. Quelques exemples en vrac :

■ **Exemple 7.1**

- $\bar{\cdot} : \mathbb{C} \to \mathbb{C}$, $e^{\bar{\cdot}}_X : \mathbb{C}[X] \to \mathbb{C}[X]$
- $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $e^{\pi}_X : \mathbb{Z}[X] \to \mathbb{Z}/n\mathbb{Z}[X]$
- $e^{id}_{X+1} \left| \begin{array}{ccc} \mathbb{R}[X] & \longrightarrow & \mathbb{R}[X] \\ P & \longmapsto & P(X+1) \end{array} \right.$
- $e^{id}_{i} \left| \begin{array}{ccc} \mathbb{R}[X] & \longrightarrow & \mathbb{C} \\ P & \longmapsto & P(i) \end{array} \right.$

■

Démonstration.

UNICITE : Soit Φ un tel morphisme, soit $P \in A[X]$ où $P(X) = \sum_{n\in\mathbb{N}} a_n X^n$. $\Phi(P) = \sum_{n\in\mathbb{N}} \Phi(a_n)\Phi(X)^n = \sum_{n\in\mathbb{N}} \phi(a_n)\beta^n$ ne dépend pas de Φ.

EXISTENCE : Soit $P = \sum_{n\in\mathbb{N}} a_n X^n \in A[X]$, posons $e^{\phi}_{\beta}(P) = \sum_n \phi(a_n)\beta^n$. Vérifions qu'il s'agisse d'un morphisme d'anneau :

- $e^{\phi}_{\beta}(1_{A[X]}) = \varphi(1_A)\beta^0 = 1_B$
- Stabilité par somme :

$$\begin{aligned} e^{\phi}_{\beta}(P) &= \sum_{n\in\mathbb{N}} \phi(a_n + b_n)\beta^n \\ &= \sum_{n\in\mathbb{N}} \phi(a_n)\beta^n + \sum_{n\in\mathbb{N}} \phi(b_n)\beta^n \\ &= e^{\phi}_{\beta}(P) + e^{\phi}_{\beta}(Q). \end{aligned}$$

- Stabilité par produit :

$$\begin{aligned} e_\beta^\phi(PQ) &= e_\beta^\phi\left(\sum_{n\in\mathbb{N}}\sum_{k=0}^{n} a_k b_{n-k} X_n\right) \\ &= \sum_{n\in\mathbb{N}}\left(\sum_{k=0}^{n}\phi(a_k)\phi(b_{n-k})\right)\beta^n \\ &= \left(\sum_{n\in\mathbb{N}}\phi(a_n)\beta^n\right)\left(\sum_{n\in\mathbb{N}}\phi(b_n)\beta^n\right) \\ &= e_\beta^\phi(P)e_\beta^\phi(Q). \end{aligned}$$

■

7.3 Degré

Définition 7.3.1 Si $P=\sum_n a_n X^n \in A[X]$, on définit $deg(P)\in\mathbb{N}\cup\{-\infty\}$ par

$$deg(P)=\sup\{n\,:\,a_n\neq 0\},$$

où $deg(0)=-\infty$ par convention.

Le **coefficient dominant** de $P\neq 0$ est $a_{deg(P)}$ où $(a_n)_n$ sont les coefficients de P.

Proposition 7.3.1 Soient $P,Q\in A[X]$, alors

1. $deg(P+Q)\leq max(deg(P),deg(Q))$ avec égalité si $deg(P)\neq deg(Q)$.
2. Si A est intègre, $deg(PQ)=deg(P)+deg(Q)$. Dans tous les cas, $deg(PQ)\leq deg(P)+deg(Q)$.

Démonstration. Soient P,Q deux polynômes. Si P ou Q est nul, ces propriétés sont faciles. On suppose donc $P\neq 0$, $Q\neq 0$.Notons $P=\sum_{k=0}^{d} a_k X^k$ où $a_d\neq 0$ et $Q=\sum_{k=0}^{d'} b_k X^k$ où $a_{d'}\neq 0$.

1. On a $P+Q=\sum_{n\in\mathbb{N}}(a_n+b_n)X^n$ où $a_n+b_n=0$ si $n>max(d,d')$. D'où $deg(P+Q)\leq max(deg(P),deg(Q))$.
   Pour le cas d'égalité, si $d>d'$, $a_d+b_d=a_d\neq 0$, donc $deg(P+Q)=d$. De même si $d<d'$.
2. Montrons d'abord l'inégalité générale. On a
$$PQ=\sum_{n\in\mathbb{N}}\left(\sum_{k=0}^{n} a_k b_{n-k}\right)X^n.$$
   Soit $n>deg(P)+deg(Q)$, et soit $k\in[0,n]$, on a $n=k+(n-k)$. Nécessairement, $k>deg(P)$ ou $n-k>deg(Q)$. Donc $a_k b_{n-k}=0$. Donc $deg(PQ)\leq deg(P)+deg(Q)$.
   Si A est intègre, calculons le coefficient de degré $d+d'$ de PQ :
$$\begin{aligned} \sum_{k=0}^{d+d'} a_k b_{n-k} &= \sum_{k=0}^{d-1} a_k b_{n-k} + a_d b_{d'} + \sum_{k=d+1}^{d+d'} a_k b_{n-k} \\ &= \sum_{k=0}^{d-1} a_k 0 + a_d b_{d'} + \sum_{k=d+1}^{d+d'} 0 b_{n-k} \\ &= a_d b_{d'}. \end{aligned}$$
   Comme A est intègre et $a_d\neq 0$ et $b_{d'}\neq 0$, $a_d b_{d'}\neq 0$.
   Donc $deg(PQ)=deg(P)+deg(Q)$.

■

Corollaire 7.3.2 $A[X]$ est intègre si et seulement si A est intègre.

Démonstration.

- $\boxed{\Rightarrow}$ Si $A[X]$ est intègre, A est un sous-anneau de $A[X]$, donc A est intègre.
- $\boxed{\Leftarrow}$ Si A est intègre, soient $P, Q \in A[X]$ tel que $PQ = 0$. Or

$$\begin{aligned} deg(PQ) = -\infty &\Leftrightarrow deg(P) + deg(Q) = -\infty \\ &\Leftrightarrow deg(P) = -\infty \text{ ou } deg(Q) = -\infty \\ &\Leftrightarrow P = 0 \text{ ou } Q = 0 \end{aligned}$$

■

7.4 Division de polynômes

Théorème 7.4.1 Soient A un anneau commutatif unitaire, $P \in A[X]$ et $Q \in A[X] - \{0\}$. On suppose le coefficient dominant de Q inversible dans A. Alors, il existe $(D, R) \in A[X]^2$ tels que

$$A = DQ + R,$$

et $deg(R) < deg(Q)$. De plus, si A est intègre, D et R sont uniques.

Démonstration.

EXISTENCE :

- **1^{er} cas : $deg(Q) = 0$.** Dans ce cas, Q est une constante inversible. Alors, $\exists\, Q' \in A[X]$ tel que $QQ' = 1$.
  En prenant $D = PQ'$ et $R = 0$, on a bien $P = PQ'Q + R = P \times 1 + 0$ et $deg(R) < deg(Q)$.
- **2^{eme} cas : $deg(Q) \geq 1$.** Dans ce cas, on procède par récurrence sur le degré de P.
  - *Initialisation :* $deg(P) < deg(Q)$
    On prend $D = 0$ et $R = P$. On a bien $P = DQ + R = 0 \times Q + P$ avec $deg(R) < deg(Q)$.
  - *Hérédité :* Supposons qu'on sache diviser euclidiennement par Q tout polynôme de degré $\leq n$. Soit P de degré $n+1$ tel que $deg(P) \geq deg(Q) = d$. Notons

$$P = \sum_{i=0}^{n+1} a_i X^i \text{ avec } a_{n+1} \neq 0,\ Q = \sum_{i=0}^{d} b_i X^i \text{ avec } b_d \neq 0.$$

    Soit α l'inverse de b_d, $P - a_{n+1}\alpha Q X^{n+1-d} = \sum_{i=0}^{n+1} a_i X^i - \sum_{i=0}^{d} a_{n+1}\alpha b_i X^{n+1-d+i}$
    Le coefficient de degré $n+1$ de ce polynôme est $a_{n+1} - b_d a_{n+1}\alpha = 0$. Donc, $deg(P - a_{n+1}\alpha Q X^{n+1-d}) \leq n$.
    Comme on sait diviser ce polynôme par Q par hypothèse de récurrence, il existe $D, R \in A[X]$ tel que $deg(R) < deg(Q)$ et

$$P - a_{n+1}\alpha Q X^{n+1-d} = DQ + R,$$

    D'où

$$P = (D + a_{n+1}\alpha X^{n+1-d})Q + R.$$

UNICITE : On suppose que A est intègre. Soient (D, R) et (D', R') deux couples de polynômes tel que

$$\begin{cases} DQ + R = P = D'Q + R' \\ deg(R) < deg(Q) \\ deg(R') < deg(Q) \end{cases}$$

Alors :

- $(D-D')Q+(R-R')=0$ donc $(D-D')Q=R'-R$.

$$\begin{aligned} deg[(D-D')Q] &= deg(R'-R) \\ deg(D-D')+deg(Q) &= deg(R'-R) < deg(Q) \\ deg(D-D') &< 0 \\ D-D' &= 0 \\ D &= D'. \end{aligned}$$

- Par conséquent, $(D-D')Q+(R-R')=R-R'=0$ d'où $R=R'$.

■

7.5 Anneaux euclidiens

Définition 7.5.1 Un anneau est dit **euclidien** si A est un anneau intègre et qu'il existe une application $\nu : A-\{0\} \to \mathbb{N}$ appelé **stathme** tel que pour tout $(a,b) \in A^2$ avec $b \neq 0$, il existe $(q,r) \in A^2$ tels que $a=qb+r$ où $r=0$ ou $\nu(r)<\nu(b)$.

Exemple 7.2

- $(\mathbb{Z}, |\cdot|)$.
- Si K est un corps, $(K[X], deg)$ est euclidien.
- Avec $N \left| \begin{array}{ccc} \mathbb{Z}[i] & \longrightarrow & \mathbb{N} \\ z=a+ib & \longmapsto & N(z)=|z|^2=a^2+b^2 \end{array} \right.$, $(\mathbb{Z}[i], N)$ est euclidien.

■

Lemme 7.5.1 $(\mathbb{Z}[i], N=|\cdot|^2)$ est euclidien.

Démonstration. Soient $(z,z') \in Z[i]^2$ tel que $z' \neq 0$. Alors

$$\begin{cases} \exists a \in \mathbb{Z} \text{ tel que } \left|a - Re\left(\frac{z}{z'}\right)\right| \leq \frac{1}{2} \\ \exists b \in \mathbb{Z} \text{ tel que } \left|b - Im\left(\frac{z}{z'}\right)\right| \leq \frac{1}{2} \end{cases}$$

On pose $q=a+ib$ et $r=z-qz'$.

$$\begin{aligned} |r|^2 &= |z-qz'|^2 \\ &= |z'|^2 \left|\frac{z}{z'} - (a+ib)\right|^2 \\ &= |z'|^2 \left(\left|a - Re\left(\frac{z}{z'}\right)\right|^2 + \left|b - Im\left(\frac{z}{z'}\right)\right|^2\right) \\ &\leq \frac{|z'|^2}{2} < |z'|^2 \end{aligned}$$

Donc $|r|^2 < |z'|^2$. ■

Théorème 7.5.2 Les anneaux euclidiens sont principaux.

Démonstration. Soient A un anneau euclidien de stathme $\nu : A-\{0\} \to \mathbb{N}$ et I un idéal de A.

- **1^{er} cas :** $I=\{0\}$. Alors I est engendré par 0, I est bien un idéal principal.
- **2^{eme} cas :** $I \neq \{0\}$. L'ensemble non vide $\nu(I-\{0\}) \subset \mathbb{N}$ est minoré. Notons n son plus petit élément, et choisissons $x \in I_{\{0\}}$ tel que $\nu(x)=n$. Montrons que $(x\rangle = I$.

– $\boxed{\subset}$ On a $x \in I$, donc $(x) \subset I$.
– $\boxed{\supset}$ Soit $y \in I$, par division euclidienne, il existe $(d, r) \in A^2$ tel que $y = dx + r$ et de plus $v(r) < v(x)$ si $r \neq 0$.
Or $r = y - dx \in I$. Si $r \neq 0$, $r \in I$ avec $v(r) < v(x)$, ce qui est impossible puisque $v(x) = \min_{a \in I - \{0\}} v(a)$. Donc $r = 0$ et $y \in (x)$.

■

7.6 Exercices

Exercice 7.1 Montrez que si A est un anneau commutatif, et $a \in A$, alors $A[X]/(X-a)$ est isomorphe à A.

Exercice 7.2 Montrez que $\mathbb{Z}[X]/(2, X)$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

Exercice 7.3 Montrez que $\mathbb{C}[X]/(X^2-2)$ n'est pas intègre, en explicitant un diviseur de zéro.

Exercice 7.4 Soit $n \geq 1$.
1) Décomposer le polynôme $X^n - 1$ en produit de facteurs irréductibles dans $\mathbb{C}[X]$.
2) On pose

$$\Phi_n(X) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} \left(X - \exp\left(\frac{2i\pi k}{n}\right)\right) \in \mathbb{C}[X],$$

appelé *n-ième polynôme cyclotomique*. Quel est le degré de Φ_n ? Montrez que

$$\prod_{d|n} \Phi_d(X) = X^n - 1.$$

3) Explicitez Φ_n pour $n \leq 7$.
4) Montrez par récurrence que Φ_n est en fait un polynôme à coefficients entiers (indication : division euclidienne).

Exercice 7.5 1) Montrez que

$$\mathbb{Z}[i\sqrt{2}] = \{x + yi\sqrt{2} : (x, y) \in \mathbb{Z}^2\},$$

est un anneau, et qu'il est intègre.
2) Montrez que $\mathbb{Z}[i\sqrt{2}]$ est isomorphe à $\mathbb{Z}[X]/(X^2+2)$.
3) Montrez que l'anneau $\mathbb{Z}[i\sqrt{2}]$ est euclidien pour le stathme $N(z) = |z|^2$.

Exercice 7.6 Soit $d > 1$ un entier sans facteurs carrés. On pose

$$\mathbb{Z}[\sqrt{d}] = \{x + y\sqrt{d} : x, y \in \mathbb{Z}^2\}.$$

1) Montrez que $\mathbb{Z}[\sqrt{d}]$ est un anneau commutatif unitaire, et qu'il est intègre.
2) Montrez que l'écriture $x + y\sqrt{d}$ est unique.
3) Montrez que l'application $\sigma : x + y\sqrt{d} \mapsto x - y\sqrt{d}$ est un automorphisme d'anneau.

4) Montrez que l'ensemble des inversibles est l'ensemble des α tels que

$$|\sigma(\alpha)\alpha| = 1.$$

Donnez un exemple d'inversible d'ordre infini pour $d = 2$.
5) Montrez que si $d \neq d'$, tous deux des nombres entiers sans facteurs carrés, il n'existe pas de morphisme d'anneau de $\mathbb{Z}[\sqrt{d}]$ dans $\mathbb{Z}[\sqrt{d'}]$. (Indication : considérer l'image de $\sqrt{d}$ et l'équation polynomiale qu'elle vérifie).

Exercice 7.7 *Polynômes à coefficients entiers.* Si $P \in \mathbb{Z}[X] - \{0\}$ est un polynôme à coefficients entiers, $P = \sum_{k=0}^{d} a_k X^k$, on pose

$$c(P) = pgcd(a_0, ..., a_d),$$

le pgcd de ses coefficients (que l'on choisit > 0). L'entier $c(P)$ est appelé *contenu* de P. On dit que P est *primitif* si $P \neq 0$ et $c(P) = 1$.
1) Montrez que pour tout $P \neq 0$, il existe un polynôme P_0 primitif, tel que

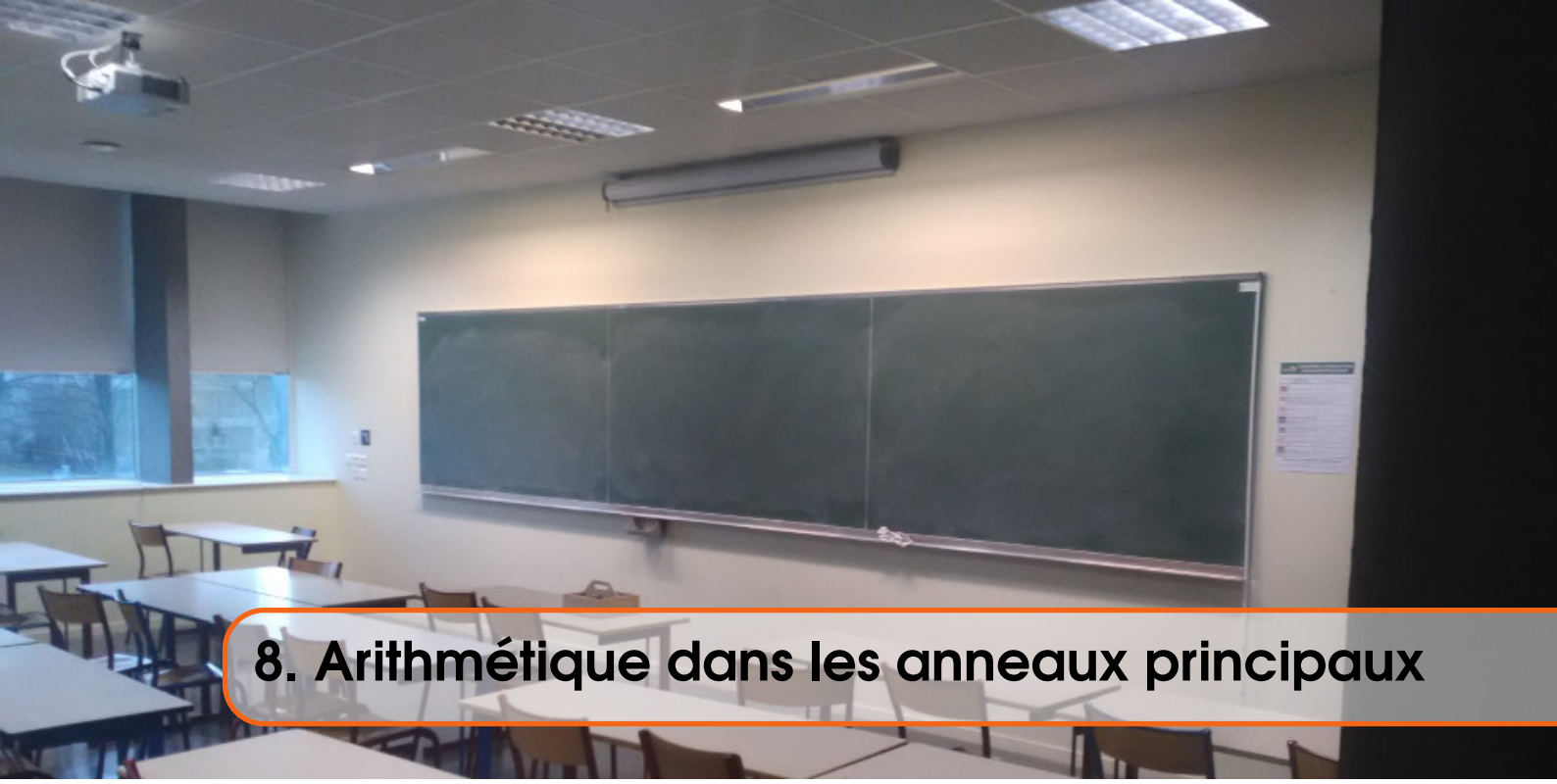
$$P = c(P)P_0.$$

2) Réciproquement, montrez que si $P = dQ$ pour $d \in \mathbb{Z} - \{0\}$ et $P, Q \in \mathbb{Z}[X] - \{0\}$ et Q primitif, alors $c(P) = d$.
3) Soient P_0,Q_0 deux polynômes primitifs. Soit p est un nombre premier,

$$\varphi_p : \mathbb{Z}[X] \to (\mathbb{Z}/p\mathbb{Z})[X],$$

le morphisme de réduction des coefficients modulo p qui envoie X sur X, montrez que $\varphi_p(P_0) \neq 0$ et $\varphi_p(Q_0) \neq 0$.
4) Toujours sous les mêmes hypothèses, montrez que p ne divise pas $c(P_0Q_0)$.
5) En déduire que $c(P_0Q_0) = 1$, c'est à dire que le produit de deux polynômes primitifs est primitif.
6) Déduire de ce qui précède le résultat suivant (dû à Gauß) : si P, Q sont deux polynômes à coefficients entiers, alors

$$c(PQ) = c(P)c(Q).$$



8. Arithmétique dans les anneaux principaux

8.1 Divisibilité, éléments associés

Définition 8.1.1 Dans un anneau intègre A, on dit que a **divise** b, noté $a|b$ si $\exists c$ tel que $b = ac$.
De façon équivalente, $a|b \Leftrightarrow (b) \subset (a)$.

Lemme 8.1.1 $a|b$ et $b|c \Rightarrow a|c$.

Démonstration.
On a $a|b$ donc il existe $a' \in A$ tel que $b = aa'$,et de même il existe $b' \in A$ tel que $c = bb'$. Donc, $c = aa'b'$. ■

Définition 8.1.2 Dans un anneau intègre A, On dit que a et b sont deux éléments sont **associés** (sous-entendu, modulo $A^\times$) si l'une des conditions équivalentes suivantes est vérifiée :

1. $a|b$ et $b|a$,
2. $(a) = (b)$,
3. Il existe $u \in A^\times$ tel que $a = bu$.

Démonstration. (que les conditions sont équivalentes)

- $\boxed{1) \Leftrightarrow 2)}$ On a $(a|b$ et $b|a) \Leftrightarrow ((b) \subset (a)$ et $(a) \subset (b)) \Leftrightarrow (a) = (b)$.
- $\boxed{2) \Rightarrow 3)}$ $a \in (b)$ et $b \in (a)$, donc il existe $(c,d) \in A^2$ tel que $a = bc$ et $b = da$. Donc $a = adc$ d'où $a(1-dc) = 0$.
  - Si $a = 0$, $b = 0$ et $u = 1$ fonctionne.
  - Si $a \neq 0$, alors par intégrité $(1-dc) = 0$, donc $1 = dc$. d et c sont alors inversibles, et $a = bu$ avec $u = c$.
- $\boxed{2) \Leftarrow 3)}$ Alors, $a \in (b)$, donc $(a) \subset (b)$
  Comme u inversible, notons u' son inverse et $au' = b$. Donc $b \in (a)$ et $(b) \subset (a)$.
  D'où l'égalité $(a) = (b)$.

■

Corollaire 8.1.2 La relation "a est associé à b", que l'on note $a \sim b$ si a et b sont associés, est une relation d'équivalence.

8.2 Idéaux premiers

Définition 8.2.1 Un idéal I d'un anneau A est dit **premier** si c'est un idéal **propre** ($I \neq A$) et que $\forall (x,y) \in A^2$,

$$xy \in I \Rightarrow (x \in I \text{ ou } y \in I).$$

Cette propriété d'un idéal se traduit comme une propriété du quotient.

Proposition 8.2.1 On a équivalence entre
1. I est un idéal premier,
2. L'anneau quotient A/I est intègre.

Démonstration. La propriété $\forall (x,y) \in A^2$, $xy \in I \Rightarrow x \in I$ *ou* $y \in I$ se traduit par $\forall (\overline{x},\overline{y}) \in (A/I)^2$, $\overline{xy} = \overline{0} \Rightarrow \overline{x} = \overline{0}$ ou $\overline{y} = \overline{0}$. Comme A/I n'est pas l'anneau nul si est seulement si I est propre, c'est bien équivalent au fait que A/I soit intègre. ■

▪ **Exemple 8.1**
- Dans un anneau intègre, $\{0\}$ est un idéal premier.
- $p\mathbb{Z}$ où p est premier est un idéal premier de l'anneau $\mathbb{Z}$.
- Si K est un corps, $\forall a \in K$, $(X-a)$ est un idéal premier dans $K[X]$.

▪

Lemme 8.2.2 Soit K un corps et $a \in K$. Alors, pour tout $P \in K[X]$,

$$P(a) = 0 \Leftrightarrow P \in (X-a) \Leftrightarrow (X-a) | P.$$

Démonstration.
- $\boxed{\Rightarrow}$ En divisant P par $X-a$, on obtient $P = D(X-a) + R$ où $deg(R) < deg(X-a) = 1$, R est donc une constante que l'on va chercher.
  En évaluant P en a, on obtient $Q(a)(a-a) + R(a) = R(a) = 0$. Donc $R = 0$ et $P = D(X-a)$.
- $\boxed{\Leftarrow}$ Si $(X-a)|P$, $P = D(X-a)$ et $P(a) = Q(a)(a-a) = 0$.

■

8.3 Idéaux maximaux

Définition 8.3.1 Un idéal I d'un anneau A est dit **maximal** si il est propre et si pour tout idéal J de A tel que $I \subset J \subset A$, alors $J = I$ ou $J = A$.

Lemme 8.3.1 Soit I et J deux idéaux d'un anneau A, alors l'ensemble $I + J$ *défini* par

$$I + J = \{i + j \ : i \in I, j \in J\},$$

est un idéal de A.

De même que la notion d'idéal premier, cette notion peut se traduire par une propriété de l'anneau quotient.

Proposition 8.3.2 On a équivalence entre
1. I est un idéal maximal,
2. A/I est un corps.

Démonstration.

- $\boxed{\Rightarrow}$ Supposons que I soit un idéal maximal. Soit $\overline{x} \in (A/I)^*$ (l'ensemble des éléments non nuls), et x un représentant de $\overline{x}$. On cherche à montrer que $\overline{x}$ est inversible. Posons $J = (x) + I$, qui est un idéal tel que $I \subset J \subset A$. Comme $\overline{x} \in (A/I)^*$, $x \notin I$ donc $J \neq I$. Par maximalité, $J = A$.
  Donc $1 \in J$, c'est à dire $1 = ax + b$ où $b \in I$, $a \in A$. Donc $\overline{1} = \overline{ax}$, $\overline{x}$ est ainsi inversible.
  De plus, comme I est propre, $I \neq A$ et donc A/I n'est pas l'anneau nul.
- $\boxed{\Leftarrow}$ Supposons que A/I est un corps. Comme un corps n'est pas l'anneau nul, $I \neq A$ et donc I est propre.
  Soit J un idéal tel que $I \subset J \subset A$.

  - **1^{er} cas :** $I = J$.
  - **2^{eme} cas :** $I \neq J$, donc $\exists x \in J/I$, c'est-à-dire $\overline{x} \neq \overline{0}$ dans A/I.
    Comme A est un corps, $\exists \overline{y} \in A/I$ tel que $\overline{1} = \overline{xy}$, ce qui revient à $1 = xy + b$, donc à $1 \in J$. Par conséquent, $J = A$.

■

▪ **Exemple 8.2**

- $p\mathbb{Z}$ avec p premier est maximal.
- Soit K un corps et $a \in K$. $(X - a)$ est maximal dans $K[X]$.

▪

Corollaire 8.3.3 Les idéaux maximaux sont premiers.

Démonstration. Si I est maximal, A/I est un corps, donc A/I est intègre. I est donc premier. ■

La réciproque peut être fausse : l'idéal $(X) \subset \mathbb{Z}[X]$ est premier, mais pas maximal. Cependant, dans les anneaux principaux, elle est vraie.

Théorème 8.3.4 Soit A un anneau principal, alors un idéal $I \neq \{0\}$ est premier si et seulement si il est maximal.

Démonstration.

- $\boxed{\Leftarrow}$ C'est le corollaire précédent.
- $\boxed{\Rightarrow}$ Soit $\mathfrak{P} \subset A$ un idéal premier de l'anneau principal A. Comme A est principal, $\exists p \in A$ tel que $(p) = \mathfrak{P}$. On veut montrer que $\mathfrak{P}$ est maximal.

  Soit I un idéal tel que $\mathfrak{P} \subset I \subset A$. Toujours par principalité de A, il existe $\exists i \in I$ tel que $(i) = I$.
  Comme $p \in I$, il existe $a \in A$ tel que $p = ia$. Puisque $\mathfrak{P}$ est premier, $i \in \mathfrak{P}$ ou $a \in \mathfrak{P}$. Considérons ces deux cas.

  - $\boxed{\text{Si } i \in \mathfrak{P}}$, alors $(i) \subset \mathfrak{P}$, donc $I = \mathfrak{P}$ par double inclusion.
  - $\boxed{\text{Si } a \in \mathfrak{P}}$, alors il existe $b \in A$ tel que $a = bp$. Donc $p = ia = ibp$, soit $p(1 - ib) = 0$. Comme $p \neq 0$ car $\mathfrak{P} \neq \{0\}$, $1 - ib = 0$ et $ib = 1$. Donc i est inversible, et $I = A$.

■

8.4 Plus petit commun multiple

Définition 8.4.1 Soit A est un anneau, $(a_1,...,a_n) \in (A^*)^n$. On dit que m est **un plus petit commun multiple (ppcm)** de $a_1,...,a_n$ si :

1. $m \neq 0$
2. $\forall i \in \{1,...,n\}$, $a_i | m$
3. Si x est un autre multiple commun de $a_1,...,a_n$, alors $m|x$

On note $m \sim a_1 \bigvee ... \bigvee a_n$.

R Il s'agit bien d'"un" ppcm, il n'est pas forcément unique. A priori, il pourrait ne pas en exister.

Proposition 8.4.1 Soit A un anneau principal et $(a_1,...,a_n) \in (A^*)^n$. Définissons $m \in A$ par

$$(m) = (a_1) \cap ... \cap (a_n).$$

Alors m est un ppcm de $a_1,...,a_n$, et tous les ppcm sont de cette forme.
Les ppcm de $a_1,...,a_n$ forment une classe pour la relation d'association.

Démonstration.

- Vérifions qu'un tel m est un ppcm de $a_1,...,a_n$
  1. $\prod_{i=1}^{n} a_i \in (m)$, donc $m \neq 0$ puisque $\prod_{i=1}^{n} a_i \neq 0$, A étant intègre.
  2. $\forall i \in \{1,...,n\}$, $(m) \subset (a_i)$, donc $a_i | m$.
  3. Soit x un multiple commun de $a_1,...,a_n$, alors $x \in (m)$ d'où $m|x$.
- Soit m' un autre ppcm, on veut montrer que $m \sim m'$. Comme $\forall i \in \{1,...,n\}$, $a_i | m'$, $m|m'$. De même, $m'|m$.

■

Corollaire 8.4.2 Dans un anneau principal, les ppcm sont associatifs : $a_1 \bigvee (a_2 \bigvee a_3) = (a_1 \bigvee a_2) \bigvee a_3$.

8.5 Plus grand commun diviseur

Définition 8.5.1 Soit $(a_1,...,a_n) \in (A^*)^n$. On dit que d est un plus grand diviseur commun (pgcd) de $a_1,...,a_n$ si :

- $\forall i \in \{1,...,n\}$, $d|a_i$,
- Si d' est un diviseur commun à $a_1,...,a_n$, alors $d'|d$.

On note dans ce cas $d \sim a_1 \bigwedge ... \bigwedge a_n$.

R Là aussi, le pgcd n'est pas toujours unique. Et il n'existe pas toujours, à priori.

Proposition 8.5.1 Soit A un anneau principal, et $(a_1,...,a_n) \in (A^*)^n$. Soit $d \in A$ tel que

$$(d) = (a_1) + ... + (a_n).$$

Alors d est un pgcd de $a_1,...,a_n$. De plus, tous les pgcd sont associés.

Démonstration. On procède de la même manière qu'avec les ppcm.

1. $\forall i \in \{1,...,n\}$, $a_i \in (d)$, donc $d|a_i$
2. Soit d' un diviseur commun, alors $d' \in (a_i)$ $\forall i \in \{1,...,n\}$. Donc $(d) \subset (d')$ et $d'|d$

De plus, les pgcd sont de cette forme et sont associés (modulo $A^\times$). ■

▪ **Exemple 8.3** Dans $\mathbb{Z}/3\mathbb{Z}[X]$, $X+\overline{2} \wedge X = \overline{2}$ et $X+\overline{2} \wedge X = \overline{1}$

$$\begin{cases} X+\overline{2} = \overline{2}(\overline{2}X+\overline{1}) \\ X = \overline{2}(\overline{2}X) \end{cases}$$

et

$$\begin{cases} X+\overline{2} = \overline{1}(X+\overline{2}) \\ X = \overline{1}(X) \end{cases}$$

▪

8.6 Algorithme d'Euclide

Dans un anneau euclidien A de stathme ν, on peut calculer un pgcd de 2 élément par divisions successives, "le" pgcd étant le dernier reste non nul.

Tout repose sur le lemme suivant :

Lemme 8.6.1 Dans l'anneau euclidien A, si $a = qb + c$, alors $a \wedge b \sim b \wedge c$.

Pour trouver un pgcd de a et b, on pose donc $a_0 = a$, $a_1 = b$, puis par récurrence, on divise a_i par a_{i+1} :

$$a_i = q_i a_{i+1} + a_{i+2}.$$

avec $\nu(a_{i+2}) < \nu(a_{i+1})$, ou bien $a_{i+2} = 0$. Comme $\nu(a_i)$ est une suite strictement d'entiers décroissante, on tombe sur un reste nul après un nombre fini d'étapes. D'après le lemme précédent, on a $a_i \wedge a_{i+1} \sim a_{i+1} \wedge a_{i+2}$. Lors de la dernière division, le reste est nul et donc a_{i+1} divise a_i, et donc

$$a_i \wedge a_{i+1} \sim a_{i+1}.$$

8.7 Éléments premier entre eux

Définition 8.7.1 Dans un anneau principal, on dit que deux éléments a et b sont **premiers entre eux** si $a \wedge b \sim 1$.

Théorème 8.7.1 (de Bézout) Soit A un anneau principal. Alors $a \wedge b \sim 1$ si et seulement si il existe $(u, v) \in A^2$ tels que

$$au + bv = 1.$$

Démonstration.

- $\boxed{\Rightarrow}$ On a $(a \wedge b) = (a) + (b)$, donc $1 \in (a) + (b)$, donc il existe $(u, v) \in A^2$ tels que $1 = au + bv$.
- $\boxed{\Leftarrow}$ Si $au + bv = 1$, $1 \in (a \wedge b($ et $a \wedge b|1$. Mais, évidemment, $1|(a \wedge b)$, donc $1 = a \wedge b$.

■

Théorème 8.7.2 (Lemme de Gauss) Soit A un anneau principal, $(a, b, c) \in A^3$.
(1) Si $(a \wedge b \sim 1)$ et $(a|bc)$ alors $a|c$.
(2) Si $(a \wedge b \sim 1)$ et $(a|c)$ et $(b|c)$ alors $ab|c$.

Démonstration.

1. Par Bézout, il existe $(u,v) \in A^2$ tels que $au+bv=1$. Comme $a|bc$, il existe $d \in A$ tel que $bc=ad$.

$$\begin{aligned} c(au+bv) &= c,\\ cau+cbv &= c,\\ acu+adv &= c,\\ a(cu+dv) &= c, \end{aligned}$$

et donc $a|c$.

2. Comme $a \wedge b \sim 1$, il existe $(u,v) \in A^2$ tels que $au+bv=1$. Comme $a|c$ et $b|c$, il existe $(d,e) \in A^2$ tel que $c=da=eb$.

$$\begin{aligned} c(au+bv) &= c,\\ acu+bcv &= c,\\ aebu+bdav &= c,\\ ab(eu+dv) &= c, \end{aligned}$$

et donc $ab|c$.

■

Proposition 8.7.3 Soit A un anneau principal. Si $(a \wedge b \sim 1)$ et $(a \wedge c \sim 1)$ alors $a \wedge bc \sim 1$.

Démonstration. Par le théorème de Bézout, il existe $(u,v) \in A^2$ tels que $au+bv=1$ et il existe $(u',v') \in A^2$ tel que $au'+cv'=1$.

$$\begin{aligned} (au+bv)(au'+cv') &= 1,\\ a^2uu'+aucv'+bvau'+bcvv' &= 1,\\ a(auu'+ucv'+bau)+bc(vv') &= 1, \end{aligned}$$

et donc $a \wedge bc \sim 1$. ■

8.8 Éléments irréductibles

Définition 8.8.1 Dans l'anneau intègre A, soit $x \in A-(A^\times \cup \{0\})$. L'élément x est dit **irréductible** si $\forall (y,z) \in A^2$,

$$(x=yz) \Rightarrow (x \sim y \text{ ou } x \sim z).$$

De manière équivalente,

$$(x=yz) \Rightarrow (y \in A^\times \text{ ou } z \in A^\times).$$

Définition 8.8.2 Soit $x \in A-(A^\times \cup \{0\})$. L'élément x est dit **premier** si $\forall (y,z) \in A^2$,

$$(x|yz) \Rightarrow (x|y \text{ ou } x|z).$$

Proposition 8.8.1 Dans un anneau, les éléments premiers sont irréductibles.

Démonstration. Soit x premier. Soient y,z tels que $x=yz$. On a donc $x|yz$ donc $x|y$ ou $x|z$. Si x divise y, on peut écrire $y=xt$, d'où $x=xtz$. Donc $x(1-tz)=0$. x étant différent de 0, $tz=1$ et ainsi $z \in A^\times$.
On traite de même le cas où $x|z$. ■

Proposition 8.8.2 L'élément non nul x est premier si et seulement si (x) est un idéal premier, non réduit à $\{0\}$.

Théorème 8.8.3 Soit A est un anneau principal, et $x \in A$, alors x est irréductible dans A si et seulement si il est premier dans A.

Démonstration. ■

8.9 Décomposition en facteurs premiers

Lemme 8.9.1 **(Noethérianité des anneaux principaux)** Soit A un anneau principal. Alors, pour toutes suites d'idéaux $(I_n)_{n\in\mathbb{N}}$ de A croissante au sens de l'inclusion $(I_k \subset I_{k+1})$, elle est ultimement stationnaire (càd constante à partir d'un certain rang).

Démonstration. ■

Théorème 8.9.2 **(Factorialité des anneaux principaux)** Soit A un anneau principal. Tout élément a non nul et non inversible admet une unique décomposition en facteur irréductible : il existe $k \in \mathbb{N}$ et $(\pi_1, ..., \pi_k)$ des irréductibles, tels que

$$a = \pi_1 ... \pi_k.$$

Si $a = \pi'_1 ... \pi'_{k'}$ est une autre écriture en produit d'irréductibles, alors $k = k'$ et il existe $\sigma \in \mathcal{S}_k$ une permutation telle que pour tout $i \in \{1, .., k\}$,

$$\pi_i \sim \pi'_{\sigma(i)}.$$

Démonstration. ■

8.10 Valuations

Définition 8.10.1 Soit A un anneau intègre. S'il vérifie l'existence et l'unicité de la décomposition en produit d'irréductibles, on dit qu'il est **factoriel**.
On appelle dans ce cas **système de premiers** tout sous-ensemble P de A tel que

- $\forall p \in P$, p est premier,
- Si x est irréductible, il existe un unique $p \in P$ tel que $x \sim p$.

■ **Exemple 8.4**

- Dans $\mathbb{Z}$, l'ensemble des nombres premiers positifs.
  Ou bien l'ensemble $\{2, -3, 5, -7, ...\}$.
- Dans $K[X]$ où K est un corps, on peut choisir l'ensemble des polynômes irréductibles unitaires de $K[X]$.
- Dans $\mathbb{Z}[i]$, l'ensemble des éléments irréductibles dont la partie réelle est strictement positive et la partie imaginaire positive ou nulle.

■

Proposition 8.10.1 Soient A un anneau factoriel et P un système de premiers. Alors, pour tout $x \in A^*$, il existe un unique $u \in A^\times$ et une unique famille presque nulle $(v_p(x))_{p\in P}$ de $\mathbb{N}$ telle que

$$x = u \prod_{p\in P} p^{v_p(x)}.$$

Le nombre $v_p(x)$ est appelé **valuation p-adique** de x.

■ **Exemple 8.5** $60 = 2^2 \times 3 \times 5$
- $v_2(60) = 1$
- $v_3(60) = 2$
- $v_5(60) = 1$
- $v_p(60) = 0$ si $p \notin \{2,3,5\}$

■

Théorème 8.10.2 Soient A un anneau principal et P un système de premiers, alors pour toutcouple $(a,b) \in (A^*)^2$,
1. $a|b \Leftrightarrow \forall p \in P,\ v_p(a) \leq v_p(b)$
2. $a \wedge b \sim \prod_{p\in P} p^{min(v_p(a),v_p(b))}$
   $a \vee b \sim \prod_{p\in P} p^{max(v_p(a),v_p(b))}$
3. $(a \wedge b)(a \vee b) \sim ab$.

Démonstration.
1. $\boxed{\Rightarrow}$ Soit $a|b$, écrivons $a = u_1 \prod_{p\in P} p^{v_p(a)}$ et $b = u_2 \prod_{p\in P} p^{v_p(b)}$.
   Comme $a|b$, $\exists c \in A$ tel que $b = ac$. Écrivons $c = u_3 \prod_{p\in P} p^{v_p(c)}$
   Donc, $b = ac = u_1u_3 \prod_{p\in P} p^{v_p(a)+v_p(c)}$. Par unicité de la décomposition, $v_p(b) = v_p(a)+v_p(c)$.
   Ainsi, puisque $v_p(c) \geq 0$, $v_p(a) \leq v_p(b)$

   $\boxed{\Leftarrow}$ Écrivons de la même manière $a = u_1 \prod_{p\in P} p^{v_p(a)}$ et $b = u_2 \prod_{p\in P} p^{v_p(b)}$. Notons $c = u_2u_1^{-1} \prod_{p\in P} p^{v_p(b)-v_p(a)}$.
   Comme $v_p(b) \geq v_p(a)$, $v_p(c) = v_p(b) - v_p(a) \geq 0$ qui est bien une écriture de $c \in A^*$. De plus,

$$\begin{aligned} ac &= u_1 \prod_{p\in P} p^{v_p(a)} u_2u_1^{-1} \prod_{p\in P} p^{v_p(c)} \\ &= u_2 \prod_{p\in P} p^{v_p(a)+v_p(b)-v_p(a)} \\ &= u_2 \prod_{p\in P} p^{v_p(b)} \\ &= b \end{aligned}$$

   Donc $a|b$.
2. Montrons que $x = \prod_{p\in P} p^{min(v_p(a),v_p(b))}$ est un pgcd de a et de b
   - $\forall p \in P,\ v_p(x) = min(v_p(a),v_p(b)) \leq v_p(a)$, donc $x|a$
     $\forall p \in P,\ v_p(x) = min(v_p(a),v_p(b)) \leq v_p(b)$, donc $x|b$
   - Soit y un diviseur commun de a et de b, alors $\forall p \in P,\ v_p(y) \leq v_p(a)$ et $v_p(y) \leq v_p(x)$.
     Donc $v_p(y) \leq min(v_p(a),v_p(b)) = v_p(x)$. Ainsi, $y|x$

   On peut procéder de manière analogue pour le ppcm.

■

■ **Exemple 8.6** Dans $\mathbb{R}[X]$, $P = (X-1)^2(X+1)(X-2)$ et $Q = 3(X+1)^2(X-2)^2$. Donc

$$P \wedge Q \sim (X+1)(X+2)$$

et

$$P \vee Q \sim (X-1)^2(X+1)(X-2)^2.$$

■

8.11 Théorème chinois

Théorème 8.11.1 Soient A un anneau principal et $(a,b) \in A^2$ premiers entre eux. Alors, il existe un isomorphisme canonique d'anneau

$$\overline{\varphi} \left| \begin{array}{ccc} A/(ab) & \longrightarrow & A/(a) \times A/(b) \\ x \mod ab & \longmapsto & (x \mod a, x \mod b) \end{array} \right.$$

d'inverse

$$\overline{\varphi}^{-1} \left| \begin{array}{ccc} A/(a) \times A/(b) & \longrightarrow & \dfrac{A/(ab)}{xbv+yau} \\ (x,y) & \longmapsto & \end{array} \right.$$

, où (u,v) sont des solutions de l'équation de Bézout $au+bv=1$.

Démonstration. Vérifions d'abord que $\overline{\varphi}$ est bien défini. On pose $\varphi \left| \begin{array}{ccc} A & \longrightarrow & A/(a) \times A/(b) \\ x & \longmapsto & (x \mod a, x \mod b) \end{array} \right.$.

- $\varphi(1) = (1 \mod a, 1 \mod b) = 1_{A/(a)\times A/(b)}$,
- $\varphi(x+y) = \varphi(x) + \varphi(y)$,
- $\varphi(xy) = \varphi(x)\varphi(y)$.

Donc φ est un morphisme d'anneaux, vérifions que $Ker(\varphi) = (ab)$.

- $\boxed{\supset}$ $\varphi(ab) = (ab \mod a, ab \mod b) = (0,0)$.
  Donc $ab \in Ker(\varphi)$ et $(ab) \subset Ker(\varphi)$
- $\boxed{\subset}$ Si $x \in Ker(\varphi)$, $a|x$ et $b|x$. Comme $a \wedge b \sim 1$, $ab|x$, d'où $x \in < ab >$ et $Ker(\varphi) \subset (ab)$.

Ainsi, $Ker(\varphi) = (ab)$. D'après le théorème de factorisation des morphismes, $\overline{\varphi}$ existe bien. De plus, il est injectif car $Ker(\overline{\varphi}) = Ker(\varphi)/(ab) = 0$.
Vérifions maintenant qu'il est surjectif et que la formule proposée donne bien son inverse.
Soient $(x \mod a, y \mod b) \in A/(a) \times A/(b)$, alors

$$\begin{aligned} \varphi(xbv+yau) &= (xbv+yau \mod a, xbv+yau \mod b), \\ &= (xbv \mod a, yau \mod b), \\ &= (x \mod a, y \mod b). \end{aligned}$$

Ainsi, $xbv+yau$ est bien l'inverse de (x,y) ■

■ **Exemple 8.7** $\mathbb{R}[X]/(X^2-1) \approx \mathbb{R}[X]/(X-1) \times \mathbb{R}[X]/(X+1)$. En particulier, $\mathbb{R}[X]/(X^2-1)$ n'est pas intègre. ■

Théorème 8.11.2 Soient A un anneau principal et $(a_1,...,a_n) \in A^n$ deux-à-deux premiers entre eux. Alors, le morphisme canonique $\pi : A/(\prod_{i\in\{1,...,n\}} a_i) \to \prod_{i\in\{1,...,n\}} A/(a_i)$ est un isomorphisme d'anneau.

Démonstration. La preuve se fait par récurrence. ■

8.12 Exercices

Exercice 8.1 1) Montrez que 11 est premier dans $\mathbb{Z}[i]$, mais que 13 ne l'est pas.
2) Soit π un élément irréductible dans $\mathbb{Z}[i]$. Montrez que son conjugué complexe est aussi irréductible, et qu'ils sont associés si et seulement si $\pi \in \{\pm 1 \pm i\}$ ou $\pi \in \mathbb{Z} \cup i\mathbb{Z}$.

Exercice 8.2 1) Déterminez les 6 polynômes unitaires irréductibles de degré ≤ 2 de $\mathbb{Z}/3\mathbb{Z}[X]$.
2) Donnez la liste des polynômes irréductibles de degré ≤ 4 de $\mathbb{Z}/2\mathbb{Z}[X]$.

Exercice 8.3 1) Déterminez le groupe des inversibles de l'anneau $\mathbb{Z}[i]$.
2) Calculez un pgcd et un ppcm dans $\mathbb{Z}[i]$ de $3+i$ et $3+4i$.
3) Montrez que si a, b sont deux entiers, un pgcd de a, b dans $\mathbb{Z}$ est également un pgcd a, b dans $\mathbb{Z}[i]$.
4) Montrez que $\pi_0 = 1+i$ est irréductible dans $\mathbb{Z}[i]$, et qu'il est associé à son conjugué complexe.

Exercice 8.4 Soit $A = \mathbb{Z}[i\sqrt{5}] = \{a + i\sqrt{5}b,\ a, b \in \mathbb{Z}\}$. 1) Montrez que A est un anneau intègre.
2) On pose $N(x) = x\overline{x}$. Montrez que si $x \in A$, $N(x)$ est entier.
3) Montrez que $x \in U_A$ si et seulement si $N(x) = 1$.
4) Décrire le groupe des inversibles $A^\times$.
5) Montrez, en utilisant la norme, que 3 est irréductible.
6) Montrez, en considérant $2 + i\sqrt{5}$, que l'idéal (3) n'est pas premier.

Exercice 8.5 On note $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$. On considère l'équation d'inconnues (x, y, z)

$$(E) : 2x^4 + 2y^4 = z^4.$$

1) Quelles sont les puissances quatrièmes dans $\mathbb{F}_5$? Montrez que la seule solution dans $\mathbb{F}_5$ de (E) est $(0,0,0)$.
2) Montrez, en utilisant 1), que dans $\mathbb{Z}$, la seule solution est $(x, y, z) = (0,0,0)$.
3) On rappelle que $\mathbb{Z}[i]$ est isomorphe à $\mathbb{Z}[X]/(X^2+1)$. Construire un morphisme d'anneaux Ψ de $\mathbb{Z}[i]$ dans $\mathbb{F}_5$.
4) Montrez qu'un tel Ψ est nécessairement surjectif. Montrez que $Ker(\Psi)$ est un idéal principal engendré par un irréductible $d \in \mathbb{Z}[i]$.
5) Montrez que (E) a une unique solution dans $\mathbb{Z}[i]$, à savoir $(0,0,0)$.

Exercice 8.6 1) Soit p un nombre premier, différent de 2. Supposons que -1 est un carré modulo p, c'est à dire qu'il existe $\overline{x} \in \mathbb{Z}/p\mathbb{Z}$ avec $\overline{x}^2 = -1$. Quel est l'ordre (multiplicatif) de $\overline{x}$? Montrez qu'alors p est congru à 1 modulo 4.
2) Soit p un nombre premier congru à 1 modulo 4, $p = 4k+1$. Soit

$$P = X(X^{2k} - 1).$$

Montrez qu'il existe $\overline{y} \in \mathbb{Z}/p\mathbb{Z}$ qui n'est pas racine de P.
3) Même hypothèses que la question précédente. Que vaut $\overline{y}^{4k}$? Déterminez l'ordre (multiplicatif) de $\overline{y}^{2k}$.
4) Montrez que si p est congru à 1 modulo 4, ou si $p = 2$, alors -1 est un carré modulo p.
5) Résumez sous forme de théorème le résultat obtenu dans cet exercice.

Exercice 8.7 Soit p un nombre premier (positif, de $\mathbb{Z}$) congru à 3 modulo 4.
1) Montrez que p n'est pas la somme de deux carrés d'entiers naturels.
2) Soit $\pi \in \mathbb{Z}[i]$ un facteur premier de p dans $\mathbb{Z}[i]$, montrez que $\pi\overline{\pi} = p$ ou p^2, puis montrez que nécessairement $\pi\overline{\pi} = p^2$.
3) En déduire que si p est congru à 3 modulo 4, il reste premier dans $\mathbb{Z}[i]$.

Exercice 8.8 Soit p un nombre premier (positif, de $\mathbb{Z}$) congru à 1 modulo 4.
1) Montrez que p divise $x^2 + 1$ pour un entier x.
2) Supposons par l'absurde que p soit premier dans $\mathbb{Z}[i]$, montrez que p divise $x - i$ ou $x + i$, et en déduire une contradiction.
3) Soit π un facteur premier de p dans $\mathbb{Z}[i]$, montrez que $\pi\overline{\pi} = p$.
4) En déduire que p est somme de deux carrés, et se décompose comme le produit de deux nombres premiers conjugués de $\mathbb{Z}[i]$.

Exercice 8.9 Résumez sous forme de théorème les résultats des trois exercices précédents.

9. Polynômes, Corps finis

9.1 Zéros de polynômes

Théorème 9.1.1 Soient A un anneau intègre et $P \in A[X]^*$ de degré n. Alors P a au plus n zéros.

Démonstration. On procède par récurrence sur le degré n.

- Si $n = 0$, P est une constante non nulle. Donc P n'a aucun zéros (ou 0 zéro).
- On suppose que tous polynôme de degré au plus n, prenons P un polynôme de degré au plus $n+1$ et notons $Z(P)$ l'ensemble des zéros de P.
  - Si $Z(P) = \varnothing$, $0 < n+1$, donc c'est vérifié.
  - Sinon, on peut choisir un $a \in Z(P)$. Comme $X - a$ est unitaire, on peut réaliser la division euclidienne de P par $X - a$. Donc : $P = Q(X-a) + R$ avec $deg(R) < 1$. Donc, R est une constante.
    Or, $P(a) = 0$ par hypothèse, donc $Q(a)(a-a) + R(a) = R(a) = 0$. Ainsi, $R = 0$ et $P = Q(X-a)$. Et, comme $deg(P) = n+1$, $deg(Q) = deg(P) - deg(X-a) = n$.

    Les racines de P sont alors les racines de Q et a. Comme Q a au plus n racines, P a au plus $n+1$ racines.

■

9.2 Anneaux quotients de $K[X]$

Soit K un corps.

Proposition 9.2.1 Soit $P \in K[X]$ de degré $d \geq 1$. Alors, $E = K[X]/(P)$ est un K-espace vectoriel de dimension d dont une base est $(X^i)_{i \in \{0,\dots,d-1\}}$.
Ainsi, tout élément de E a un unique représentant de degré au plus $d-1$

Démonstration.

- $(E, +)$ est un groupe additif.

- Le produit externe $\left|\begin{array}{ccc} K\times E & \longrightarrow & E \\ (k,Q) & \longmapsto & kQ \end{array}\right.$ est bien distributif par rapport à l'addition.
- $1\times Q = Q$

E est bien un K-espace vectoriel. Vérifions que $(X^i)_{i\in\{0,\dots,d-1\}}$ est bien une base de E

- Famille Génératrice : Soit $\overline{Q}\in E$ et Q un de ses représentants. En réalisant la division euclidienne de Q par P : $Q = DP+R$ avec $deg(R) < deg(P)$. Ainsi, $\overline{Q} = \overline{DP+R} = \overline{R}$.
  Donc, pour toute classe $\overline{Q}$ de E, on peut l'écrire sous la forme $\overline{Q} = \sum_{i=0}^{d-1} a_i X^i$
- Famille Libre : Soit $(a_0,\dots,a_{d-1})\in K^d$ tel que $\sum_{i=0}^{d-1} a_i X^i = 0$.
  Donc, le polynôme $Q = \sum_{i=0}^{d-1} a_i X^i$ représente la classe $\overline{0}$, d'où $P|Q$. mais, comme $deg(Q) < deg(P)$, $Q = 0$ et $a_0 = \dots = a_{d-1} = 0$

■

▪ Exemple 9.1

- $\mathbb{C} = \mathbb{R}[X]/(X^2+1)$ est un $\mathbb{R}$-espace vectoriel de dimension 2 où $i = \overline{X}$
- En notant $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ lorsque p est premier, $E = \mathbb{F}_7[X]/(X^2+1)$ est un $\mathbb{F}_7$-espace vectoriel de dimension 2. Donc $|E| = |\mathbb{F}_7|^2 = 49$

▪

Théorème 9.2.2 Soient $P\in K[X]$ de degré au moins 1 et $E = K[X]/(P)$. Alors, on a équivalence entre :

1. P est irréductible dans $K[X]$.
2. E est intègre.
3. E est un corps.

Démonstration. $\boxed{1)\Rightarrow 3)}$ Si P est irréductible, comme $K[X]$ est principal, P est premier et (P) est un idéal premier. Comme les idéaux premiers sont maximaux dans un anneau principal, $K[X]/(P)$ est un corps.
$\boxed{3)\Rightarrow 2)}$ Les corps sont des anneaux intègres.
$\boxed{2)\Rightarrow 1)}$ Si $K[X]/(P)$ est intègre, alors l'idéal (P) est premier, donc P est premier, donc irréductible. ■

9.3 Critère d'irréductibilité

Proposition 9.3.1 Soit K un corps.

1. Les polynômes de degré 1 dans $K[X]$ sont irréductibles.
2. Un polynôme de degré 2 ou 3 est irréductible si et seulement s'il n'a pas de racine dans K.

Démonstration.

1. Si P est de degré 1, en écrivant $P = UV$, soit U est de degré 0 soit V est de degré 0. Dans les deux cas, U ou V est une constante non nulle, donc inversible.
2. $\boxed{\Leftarrow}$ Si P est de degré 2 ou 3 avec $P = UV$ et sans racine, soit U ou V est une constante, donc inversible, soit U ou V est un polynôme de degré 1. En écrivant $U = aX+b$, U a une racine qui est $\frac{-b}{a}$. Donc P a une racine, ce qui est absurde.

   $\boxed{\Rightarrow}$ Par contra-posée : Si P a une racine, il n'est pas irréductible.
   Si P a une racine, noté α, $X-\alpha|P$ et $P = (X-\alpha)Q$ avec $deg(Q) = deg(P)-1\geq 1$. Donc Q n'est pas inversible, comme $X-\alpha$, P n'est pas inversible.

■

R Attention ! C'est totalement faux pour les polynômes de degré supérieur ou égal à 4 : X^4+1 est sans racine mais réductible dans $\mathbb{R}[X]$.

Définition 9.3.1 Soit $P \in \mathbb{Z}[X]$. On dit que P est **primitif** si $P \neq 0$ et $P = \sum_{i=0}^{d} a_i X^i$ avec $a_d \neq 0$ et $pgcd(a_0, ..., a_d) = 1$.

■ **Exemple 9.2** $6X^2+4X+9$ est primitif alors que $6X^2+4X+8$ ne l'est pas. ■

Lemme 9.3.2 $P \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Z}[X]$ si et seulement si il est irréductible dans $\mathbb{Q}[X]$ et primitif.

Théorème 9.3.3 — Critère de réduction. Soit $P \in \mathbb{Z}[X]$ non nul et p un nombre premier. Supposons
1. P est primitif
2. Avec $\pi : \mathbb{Z}[X] \to \mathbb{Z}/p\mathbb{Z}[X]$ la projection canonique, $\pi(P)$ est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$
3. $deg(\pi(P)) = deg(P)$

Alors P est irréductible.

Démonstration. ■

Théorème 9.3.4 — Critère d'Eisenstein, admis. Soit $p \geq 2$ premier et P un polynôme non nul de $\mathbb{Z}[X]$ s'écrivant $P = \sum_{i=0}^{d} a_i X^i$ où $a_d \neq 0$, en supposant
1. P primitif
2. $\forall i \in \{0, ..., d-1\}$, $p | a_i$
3. $p \nmid a_d$
4. $p^2 \nmid a_0$

Alors P est irréductible dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$

■ **Exemple 9.3** $2X^5+5X^2+25X+10$ est irréductible dans $\mathbb{Q}[X]$ ■

9.4 Corps algébriquement clos

Définition 9.4.1 On dit qu'un corps K est *algébriquement clos* s'il satisfait l'une des propriétés équivalentes suivantes :
1. Tout polynôme de $K[X]$ a une racine dans K.
2. Les irréductibles de $K[X]$ sont de degré 1.
3. Tout polynôme non nul de $K[X]$ admet une écriture $\alpha \prod_{i=1}^{deg(P)} (X - x_i)$ où $\alpha \in K^*$ et $x_i \in K$.
   (Un tel polynôme est dit **scindé** sur K).

Démonstration. ■

Théorème 9.4.1 — d'Alembert-Gauss, admis. Le coprs $\mathbb{C}$ des nombres complexes est algébriquement clos.

Corollaire 9.4.2 Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 ayant un déterminant négatif (ayant des racines non réelles).

Démonstration. Soit $P \in \mathbb{R}[X]$ irréductible. Décomposons-le dans $\mathbb{C}$: $P = \alpha \prod_{i=1}^{deg(P)} (X - x_i)$ avec α non nul. Comme α est le coefficient dominant de P, $\alpha \in \mathbb{R}$.

On peut remarquer que $\overline{P} = \overline{\alpha} \prod_{i=0}^{deg(P)} (X - \overline{x}_i)$ et que $\overline{P} = P$ puisque $P \in \mathbb{R}[X]$. Donc les racines de P sont stables par conjugaison.

- $x_1 \in \mathbb{R}$, donc $X - x_1 | P$. Par irréductibilité, $P \sim X - x_1$, donc $deg(P) = 1$
- $x_i \notin \mathbb{R}$, donc $(X-x_1)(X-\overline{x}_1) | P$. On sait que $(X-x_1)(X-\overline{x}_1) \in \mathbb{R}[X]$, donc, par irréductibilité, $P \sim (X - x_1)(X - \overline{x}_1)$ où $(X - x_1)(X - \overline{x}_1)$ a un discriminant négatif.

■

9.5 Exercices

Exercice 9.1 (Application des critères d'irréductibilité)
1) Montrez que le polynôme $X^3 - 7X^2 + 14X + 10$ est irréductible dans $\mathbb{Q}[X]$ (Indication : $p = 7$).
2) Montrez que le polynôme $X^7 - 14X^6 + 4X^5 + 64X + 6$ est irréductible dans $\mathbb{Q}[X]$.

Exercice 9.2 Montrez que $\mathbb{Z}/3\mathbb{Z}[X]/(X^4 + X + 2)$ est un corps fini, et qu'il a 81 éléments.

Exercice 9.3 Soient $k_1 = (\mathbb{Z}/5\mathbb{Z}[X])/(X^2 + X + 2)$ et $k_2 = (\mathbb{Z}/5\mathbb{Z}[X])/(X^2 + 2)$.
1) Montrez que k_1 et k_2 sont des corps.
2)On note α la classe de X dans k_1 et β la classe de X dans k_2. Posons $f_1(a) = a$ et $f_2(a) = a$ si $a \in \mathbf{Z}/5\mathbf{Z}$, et $f_1(\alpha) = \beta^6$, $f_2(\alpha) = 2\beta + 2$, f_1, f_2 se prolongent-ils en morphismes de corps de k_1 dans k_2 ? Sont-ce des isomorphismes ?

Exercice 9.4 Soit Q un polynôme de degré ≥ 1 à coefficients entiers relatifs.
1) On suppose que $Q(0) = 1$. Montrez par l'absurde qu'il existe une infinité de nombres premiers intervenants dans la décomposition en facteurs premiers des nombres de $Q(\mathbb{Z})$.
2) On ne suppose plus que $Q(0) = 1$. Montrez que le résultat persiste en se ramenant au cas précédent.

Exercice 9.5 *Progression arithmétique faible.* On rappelle que Φ_n est le n-ième polynôme cyclotomique.
1) Soit $P_n = \prod_{d<n} \Phi_d$. Montrez que P_n et Φ_n sont premiers dans $\mathbb{C}[X]$, puis dans $\mathbb{Q}[X]$.
2) Montrez qu'il existe A, B dans $\mathbb{Z}[X]$ et $m \in \mathbb{Z} - \{0\}$ avec

$$m = AP_n + B\Phi_n.$$

3) Soit x un entier, et p un diviseur premier de $\Phi_n(x)$ qui ne divise pas m (on suppose qu'il en existe). Montrez que p ne divise pas $P_n(x)$.
4) Rappelez que vaut $P_n\Phi_n$. Montrez, en utilisant cette équation, que x est d'ordre n dans $(\mathbb{Z}/p\mathbb{Z})^\times$.

5) Montrez que p est congru à 1 modulo n.
6) Conclure, en utilisant l'exercice précédent, qu'il existe une infinité de nombres premiers congrus à 1 modulo n.