Algèbre générale

Sommaire

Remarque 0.1:

- Prérequis :
  - En principe, pour le début, il n'y a pas de prérequis à part de la théorie des ensembles et du dénombrement de base (et de l'expérience en mathématiques). On suppose que les ensembles usuels sont construits, et encore il n'y a pas besoin de $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ avant un bon bout de temps.
  - Pour la Partie 2.6, il faut quelques notions de géométrie, mais cette partie est une parenthèse et ne sert jamais dans la suite.
  - Pour la Partie 4, il faut quelques notions d'algèbre linéaire.
  - Pour la Partie 5, il faut des notions d'algorithmique, et parfois quelques notions d'analyse et de probabilités.

  Cependant, les exemples et exercices utilisent parfois d'autres notions.
- J'ai écrit ceci à des moments très espacés dans le temps donc il y a sûrement des incohérences et des points manquants. Le niveau de rigueur n'est pas homogène, mais il est toujours relativement élevé. Par ailleurs je n'ai pas relu le document de façon systématique.

- Pour les exercices, les $\star$ symbolisent la difficulté de l'exercice (de $\star$ à $\star\star\star$) et ♥ signifie que j'aime bien l'exercice.

1. Anneaux et corps

1.1. Structures algébriques

Définition 1.1.1 : Soit E un ensemble. On appelle loi de composition interne (ou loi) sur E toute fonction de E^2 dans E.

On note généralement les lois de composition interne de manière infixe : si la loi est $\star$, on notera $x \star y$ au lieu de $\star\ (x, y)$.

Exemple 1.1.1 : Les lois $+$ et $\times$ sont des lois de composition interne sur l'ensemble $\mathbb{Z}$ (ou sur $\mathbb{N}$, ou sur toute autre partie de $\mathbb{Z}$).

Définition 1.1.2 : Soient E un ensemble et $\star$ une loi de composition interne sur E. On dit que $\star$ est associative si et seulement si $\forall x, y, z \in E, (x \star y) \star z = x \star (y \star z)$.

Exemple 1.1.2 : Les lois $+$ et $\times$ sur l'ensemble $\mathbb{Z}$ (ou sur $\mathbb{N}$) sont associatives.

Remarque 1.1.1 : Si E est un ensemble muni d'une loi de composition interne associative $\star$, on peut noter sans ambiguïté $x \star y \star z$ au lieu de $x \star (y \star z)$ ou $(x \star y) \star z$. De même pour un produit d'un nombre quelconque d'éléments.

Définition 1.1.3 : Soient E un ensemble et $\star$ une loi de composition interne sur E. On dit que $\star$ est commutative si et seulement si $\forall x, y \in E, x \star y = y \star x$.

Exemple 1.1.3 : Les lois $+$ et $\times$ sur l'ensemble $\mathbb{Z}$ (ou sur $\mathbb{N}$) sont commutatives.

Définition 1.1.4 : Soient E un ensemble, $e \in E$ et $\star$ une loi de composition interne sur E. On dit que e est un élément neutre pour la loi $\star$ si et seulement si $\forall x \in E, x \star e = e \star x = x$.

Exemple 1.1.4 : 0 est un élément neutre pour la loi $+$ et 1 est un élément neutre pour la loi $\times$ sur $\mathbb{Z}$ (ou sur $\mathbb{N}$).

Lemme 1.1.1 : Soient E un ensemble et $\star$ une loi de composition interne sur E. Alors il existe au plus un élément neutre sur E pour la loi $\star$.

Preuve : Supposons que E admette deux éléments neutres e et e'. Alors $e \star e' = e = e'$. ■

Définition 1.1.5 : Soient E un ensemble, $a \in E$ et $\star$ une loi de composition interne sur E. On dit que a est un élément absorbant pour la loi $\star$ si et seulement si $\forall x \in E, x \star a = a \star x = a$.

Définition 1.1.6 : Soient E un ensemble muni d'une loi de composition interne associative $\star$ et d'un élément neutre e, $a \in \mathbb{N}$ et $(x_n)_{n \in [\![a, \infty[\![} \in E^{[\![a, \infty[\![}$. On pose pour tout $b < a$,

$$\prod_{i=a}^{b} x_i = e$$

puis pour tout $b \geqslant a - 1$,

$$\prod_{i=a}^{b+1} x_i = \left(\prod_{i=a}^{b} x_i \right) \star x_{b+1}$$

Remarque 1.1.2 : Si la loi est notée $+$, on utilise le symbole $\sum$ au lieu de $\prod$.
La lettre i est dite muette : on peut la remplacer par n'importe quelle autre lettre qui n'est pas déjà utilisée.

Définition 1.1.7 : Soient E un ensemble, $x \in E$ et $\star$ une loi de composition interne sur E qui admet un élément neutre e (qui est donc unique). On dit que x est inversible pour la loi $\star$ si et seulement si $\exists y \in E, x \star y = y \star x = e$. Un tel y s'appelle inverse de x pour la loi $\star$.

Exemple 1.1.5 : Pour tout $x \in \mathbb{Z}$, $-x$ est un inverse de x pour la loi $+$.

Lemme 1.1.2 : Soient E un ensemble, $\star$ une loi de composition interne associative sur E et $x \in E$. Alors il existe au plus un inverse de x pour la loi $\star$, qu'on note alors x^{-1} (ou $-x$ si la loi est notée $+$).

Preuve : Notons e l'élément neutre de E. Supposons que x admette deux éléments neutres y et z. Alors $y = y \star e = y \star (x \star z) = (y \star x) \star z = e \star z = z$. ■

Lemme 1.1.3 : Soient E un ensemble, $\star$ une loi de composition interne associative sur E et x, y des éléments inversibles de E. Alors $x \star y$ est inversible d'inverse $y^{-1} \star x^{-1}$.

Preuve : Notons e l'élément neutre de E. On a $(x \star y) \star (y^{-1} \star x^{-1}) = x \star (y \star y^{-1}) \star x^{-1} = x \star x^{-1} = e$ et de même, $(y^{-1} \star x^{-1}) \star (x \star y) = e$. ■

Définition 1.1.8 : Soient E un ensemble et $\star$ et $\perp$ deux lois de composition interne sur E. On dit que $\star$ est distributive sur $\perp$ si et seulement si $\forall x, y, z \in E, x \star (y \perp z) = (x \star y) \perp (x \star z)$.

Exemple 1.1.6 : Dans $\mathbb{Z}$, la loi $\times$ est distributive sur la loi $+$.

Définition 1.1.9 : Soient E un ensemble, $F \subseteq E$ et $\star$ une loi de composition interne sur E. On dit que F est stable par $\star$ si et seulement si $\forall x, y \in F, x \star y \in F$. Dans ce cas, on pose $\star_F : F^2 \to F$ la loi de composition interne définie par $\forall x, y \in F, x \star_F y = x \star y$. La loi $\star_F$ est dite loi induite par $\star$ sur F. On la notera souvent encore $\star$ par abus.

Exemple 1.1.7: Dans $\mathbb{Z}$, $\mathbb{N}$ est une partie stable pour les lois $+$ et $\times$.

Définition 1.1.10: Soient E un ensemble, $\sim$ une relation d'équivalence sur E et $\star$ une loi de composition interne sur E. La relation R est dite compatible avec la loi $\star$ si et seulement si $\forall x, x', y, y' \in E, (x \sim x') \wedge (y \sim y') \implies (x \star y \sim x' \star y')$.

Dans ce cas, on définit une loi de composition interne sur $E/\sim$ en posant pour tous $\overline{x}, \overline{y} \in E/\sim$, $\overline{x} \mathbin{\overline{\star}} \overline{y} = \overline{x \star y}$. La loi $\overline{\star}$ est dite loi quotient.

Remarque 1.1.3: Cette loi est bien définie. En effet, soient $x, x' \in E$ tels que $\overline{x} = \overline{x'}$ et $y, y' \in E$ tels que $\overline{y} = \overline{y'}$. On a $x \sim x'$ et $y \sim y'$ donc par compatibilité, $(x \star y) \sim (x' \star y')$ c'est-à-dire $\overline{x \star y} = \overline{x' \star y'}$.

Théorème 1.1.1: On conserve les mêmes notations.

1) Si $\star$ est associative alors $\overline{\star}$ l'est aussi.
2) Si $\star$ est commutative alors $\overline{\star}$ l'est aussi.
3) Si $e \in E$ est neutre pour $\star$ alors $\overline{e}$ est neutre pour $\overline{\star}$.
4) Si $x \in E$ est inversible pour $\star$ alors $\overline{x}$ est inversible pour $\overline{\star}$ d'inverse $\overline{x^{-1}}$.

Preuve:
1) Supposons que $\star$ est associative. Soient $\overline{x}, \overline{y}, \overline{z} \in E/\sim$, alors $(\overline{x} \mathbin{\overline{\star}} \overline{y}) \mathbin{\overline{\star}} \overline{z} = \overline{x \star y} \mathbin{\overline{\star}} \overline{z} = \overline{x \star y \star z} = \overline{x} \mathbin{\overline{\star}} \overline{y \star z} = \overline{x} \mathbin{\overline{\star}} (\overline{y} \mathbin{\overline{\star}} \overline{z})$. Ainsi $\overline{\star}$ est associative.

Les autres points sont tout aussi simples. ■

Exercice 1.1.1 (⋆ ⋆ ⋆ ♥): Soit E un ensemble fini non vide, muni d'une loi de composition interne associative $\star$. Montrer qu'il existe $s \in E$ tel que $s \star s = s$.

Solution: Soit $x \in E$ puis $f : \mathbb{N} \to E$ l'application définie par $f(i) = x^{2^i}$ (f est bien définie car la loi est associative). Puisque $\mathbb{N}$ est infini et E est fini, f n'est pas injective, donc il existe $i < j$ tels que $f(i) = f(j)$ i.e. $x^{2^i} = x^{2^j}$. Si $i + 1 = j$ alors $s = x^{2^i}$ fonctionne. Sinon, on a $2^j - 2^i + 1 \in \mathbb{N}^*$ et on peut donc multiplier par $x^{2^j - 2^{i+1}}$: on obtient $x^{2^j - 2^i} = x^{2^{j+1} - 2^{i+1}} = \left(x^{2^j - 2^i}\right)^2$ donc $s = x^{2^j - 2^i}$ convient.

Définition 1.1.11: Soient E un ensemble et $\star$ une loi de composition interne sur E. On dite que $(E, \star)$ est un monoïde si et seulement si $\star$ est associative et admet un élément neutre.

Exemple 1.1.8:
- $(\mathbb{N}, +)$ est $(\mathbb{Z}, +)$ sont des monoïdes.
- Si E est un ensemble alors l'ensemble des suites finies à valeurs dans E, muni de la concaténation, est un monoïde, dit monoïde libre sur E. L'élément neutre est la suite vide, c'est-à-dire l'unique application de $\emptyset$ dans E.

Remarque 1.1.4: Sauf mention contraire, on notera e l'élément neutre d'un monoïde.

Définition 1.1.12: Soient $(E, \star)$ un monoïde et $x \in E$. On pose $x^0 = 1$ puis $\forall n \in \mathbb{N}, x^{n+1} = x^n \star x$.

Théorème 1.1.2: Soient $(E, \star)$ un monoïde, $x \in A$ et $p, q \in \mathbb{N}$. Alors

1) $x^p \star x^q = x^{p+q}$
2) $(x^p)^q = x^{pq}$

Preuve:

1) Soit $p \in \mathbb{N}$. Notons $P(q)$ la relation $x^p \star x^q = x^{p+q}$. $P(0)$ est vraie. Soit $q \in \mathbb{N}$, supposons $P(q)$. Alors $x^p \star x^{q+1} = x^p \star x^q \star x = x^{p+q} \star x = x^{p+q+1}$ d'après ce qui précède. Ainsi $P(q+1)$ est vraie et par principe de récurrence, on en déduit le résultat.
2) Soit $p \in \mathbb{N}$. Notons $P(q)$ la relation $(x^p)^q = x^{pq}$. $P(0)$ est vraie. Soit $q \in \mathbb{N}$, supposons $P(q)$. alors $(x^p)^{q+1} = (x^p)^q \star x^p = x^{pq} \star x^p = x^{pq+p} = x^{p(q+1)}$. Ainsi $P(q+1)$ est vraie et par principe de récurrence, on en déduit le résultat.

■

Définition 1.1.13: Morphisme de monoïdes Soient $(E, \star)$ et $(F, \cdot)$ deux monoïdes, d'éléments neutres respectifs e et e'. On appelle morphisme de monoïdes toute fonction $\varphi : E \to F$ telle que $\varphi(e) = e'$ et $\forall x, y \in E, \varphi(x \star y) = \varphi(x) \cdot \varphi(y)$.

Théorème 1.1.3: Soient $(E, \star)$ et $(F, \cdot)$ deux monoïdes, d'éléments neutres respectifs e et e', et $\varphi : E \to F$ un morphisme de monoïdes. Alors $\forall x \in E, \forall n \in \mathbb{N}, \varphi(x^n) = \varphi(x)^n$.

Preuve: Soit $x \in E$. Notons $P(n)$ la relation $\varphi(x^n) = \varphi(x)^n$.
On a $\varphi(x^0) = \varphi(e) = f = \varphi(x)^0$ donc $P(0)$ est vraie.
Soit $n \in \mathbb{N}$, supposons $P(n)$. Alors $\varphi(x^{n+1}) = \varphi(x^n \star x) = \varphi(x^n) \cdot \varphi(x) = \varphi(x)^n \cdot \varphi(x) = \varphi(x)^{n+1}$ donc $P(n+1)$ est vraie.
Par principe de récurrence, on en déduit le résultat. ■

1.2. Généralités sur les groupes

Définition 1.2.1 : On appelle groupe tout couple $(G, \star)$ où G est un ensemble et $\star$ est une loi de composition interne telle que :
- $\star$ est associative ;
- il existe un élément neutre pour $\star$;
- tout élément possède un inverse par $\star$.

Si de plus $\star$ est commutative, on dit que le groupe $(G, \star)$ est abélien.

Remarque 1.2.1 : Sauf mention contraire, on notera la loi d'un groupe quelconque multiplicativement (l'élément neutre sera noté e ou 1) et la loi d'un groupe abélien additivement. On dira aussi abusivement qu'un ensemble G est un groupe sans préciser la loi de composition interne.

Désormais, sauf mention contraire, G désigne un groupe.

Exercice 1.2.1 ($\star\star\star$) : Soit G un ensemble muni d'une loi de composition interne associative $\star$ et d'un élément $e \in G$ tel que $\forall x \in G, e \star x = x$ et $\forall x \in G, \exists y \in G, y \star x = e$. Montrer que $(G, \star)$ est un groupe.

Solution :
- Soit $x \in G$, soit donc $y \in G$ tel que $y \star x = e$. Montrons que $x \star y = e$. Soit $z \in G$ tel que $z \star (x \star y) = e$, alors $x \star y = e \star x \star y = z \star x \star y \star x \star y = z \star x \star e \star y = z \star x \star y = e$.
- Soit $x \in G$, montrons que $x \star e = x$. Soit $y \in G$ tel que $y \star x = e$. D'après ce qui précède, on a aussi $x \star y = e$, donc $x \star e = x \star y \star x = e \star x = x$.

Remarque 1.2.2 : Dans un groupe :
- l'élément neutre est unique ;
- l'inverse d'un élément est unique ;
- un inverse à droite (resp. à gauche) d'un élément est l'inverse de cet élément.

Définition 1.2.2 : Soient G et H deux groupes. On dit qu'une application $\varphi : G \to H$ est un morphisme de groupes ssi $\forall x, y \in G, \varphi(xy) = \varphi(x)\varphi(y)$.

Lemme 1.2.1 : Si φ est un morphisme de groupes alors $\forall n \in \mathbb{Z}, \varphi(x^n) = \varphi(x)^n$.

Définition 1.2.3 : Si G et H sont deux groupes, on définit une loi de groupe sur $G \times H$ en posant $(x, y)(x', y') = (xx', yy')$.

Remarque 1.2.3 :
- $G \times H$ muni de cette loi est bien un groupe.
- Plus généralement, on définit naturellement le produit d'un nombre quelconque de groupes.

Définition 1.2.4 : Soit $H \subseteq G$. On dit que H est un sous-groupe de G ssi c'est un groupe pour la loi induite par celle de G.

Lemme 1.2.2 : H est un sous-groupe de G ssi $H \neq \emptyset$ et $\forall x, y \in H, xy^{-1} \in H$.

Exemple 1.2.1 :

- Pour tout $X \subseteq G$, l'ensemble $C_G(X) := \{g \in G; \forall x \in X, xg = gx\}$ est un sous-groupe de G, dit centralisateur de X dans G.
- En particulier, l'ensemble $Z(G) := C_G(G) = \{g \in G; \forall x \in G, xg = gx\}$ est un sous-groupe de G, dit centre de G.
- Pour tout $X \subseteq G$, l'ensemble $N_G(X) := \{g \in G; gXg^{-1} = X\}$ est un sous-groupe de G, dit normalisateur de X dans G.

Exercice 1.2.2 (⋆ ⋆) :

1) Montrer que les sous-groupes de $(\mathbb{R}, +)$ sont soit de la forme $a\mathbb{Z}$ avec $a \in \mathbb{R}_+$, soit denses dans $\mathbb{R}$.
2) a) Soit $f : \mathbb{R} \to \mathbb{R}$. Montrer que l'ensemble des périodes de f (c'est-à-dire $\{p \in \mathbb{R}; \forall x \in \mathbb{R}, f(x + p) = f(x)\}$) est un sous-groupe de $(\mathbb{R}, +)$.
   b) Si f admet 1 et $\sqrt{2}$ comme périodes, montrer que son groupe des périodes est dense dans $\mathbb{R}$.
   c) Si de plus f est continue, montrer que f est constante.
   d) Trouver une fonction f dont le groupe des périodes est dense dans $\mathbb{R}$, mais qui n'est pas constante.

Solution :

1) Soit G un sous-groupe de $(\mathbb{R}, +)$. Supposons que G n'est pas de la forme $a\mathbb{Z}$ avec $a \in \mathbb{R}_+$. On a $G \neq \{0\} = 0\mathbb{Z}$, soit donc $x_0 \in G \setminus \{0\}$. Quitte à remplacer x_0 par $-x_0 \in G$, on suppose $x_0 > 0$.

   On a $G \neq x_0\mathbb{Z}$ et $x_0\mathbb{Z} \subseteq G$, soit donc $y \in G \setminus x_0\mathbb{Z}$. y est non nul vu $0 \in x_0\mathbb{Z}$. Quitte à remplacer y par $-y$, on suppose $y > 0$. Posons $y' = y - nx_0$ où $n = \left\lfloor \frac{y}{x_0} - 1 \right\rfloor$, alors $y' \in G$ et on a $\frac{y}{x_0} - 1 < n < \frac{y}{x_0}$ (la première inégalité est stricte car sinon, on aurait $y = (n+1)x_0 \in x_0\mathbb{Z}$ ce qui absurde). On en déduit $-y \leftarrow nx_0 < x_0 - y$ puis $0 < y' < x_0$. Posons

$$x_1 = \begin{cases} y' & \text{si } \ y' \leqslant \frac{x_0}{2} \\ x_0 - y' & \text{sinon} \end{cases}$$

   alors $x_1 \in G$ et $0 < x_1 \leqslant \frac{x_0}{2}$. En itérant le processus, on obtient une suite $(x_n)_{n\in\mathbb{N}} \in G^{\mathbb{N}}$ telle que $x_0 > 0$ et $\forall n \in \mathbb{N}, 0 < x_{n+1} \leqslant \frac{x_n}{2}$ donc $x_n \underset{n}{\longrightarrow} 0$.

   Soit $a \in \mathbb{R}$, alors $\left(\left\lfloor \frac{a}{x_n} \right\rfloor x_n\right)_{n\in\mathbb{N}}$ est une suite d'éléments de G qui tend vers a. G est donc dense dans $\mathbb{R}$.
2) a) 0 est une période de f. Si p et q sont des périodes de f alors pour tout $x \in \mathbb{R}$, $f(x + (p - q)) = f((x + p - q) + q) = f(x + p) = f(x)$ donc $p - q$ est une période de f. L'ensemble des périodes de f est donc un sous-groupe de $(\mathbb{R}, +)$.

b) Supposons que f admette 1 et $\sqrt{2}$ comme périodes. Alors le groupe des périodes de f contient $\langle 1, \sqrt{2}\rangle = \left\{a + b\sqrt{2}; a, b \in \mathbb{Z}\right\}$. Or $\langle 1, \sqrt{2}\rangle$ est un sous-groupe de $(\mathbb{R}, +)$ et n'est pas de la forme $a\mathbb{Z}$: sinon, on aurait $\sqrt{2} = an$ avec $a \in \mathbb{R}_+$ et $n \in \mathbb{Z}$, et $1 = am$ avec $m \in \mathbb{Z} \setminus \{0\}$, donc $\sqrt{2} = \frac{\sqrt{2}}{1} = \frac{n}{m} \in \mathbb{Q}$, ce qui est absurde.

c) Supposons de plus que f est continue. Soient $x \in \mathbb{R}$ puis (x_n) une suite d'éléments de $\langle 1, \sqrt{2}\rangle$ qui converge vers x. Pour tout $n \in \mathbb{N}$, x_n est une période de f donc $f(x_n) = f(0)$. Puisque f est continue, on en déduit en passant à la limite que $f(x) = f(0)$. f est donc constante.

d) L'indicatrice de $\mathbb{Q}$ fonctionne, car son groupe des périodes contient $\mathbb{Q}$ donc est dense dans $\mathbb{R}$.

Lemme 1.2.3 : Une intersection de sous-groupes est un sous-groupe.

Exercice 1.2.3 (⋆) : Soient G un groupe et H_1, H_2 deux sous-groupes de G tels que $H_1 \cup H_2$ est un sous-groupe de G, montrer que $H_1 \subseteq H_2$ ou $H_2 \subseteq H_1$.

Solution : Supposons par l'absurde que $H_1 \not\subseteq H_2$ et $H_2 \not\subseteq H_1$. Soient donc $x \in H_2 \setminus H_1$ et $y \in H_1 \setminus H_2$. Comme $H_1 \cup H_2$ est un groupe, on a $xy \in H_1 \cap H_2$. Si $xy \in H_1$, alors $x \in H_1$, ce qui est absurde, et idem si $xy \in H_2$.

Lemme 1.2.4 : L'image directe et réciproque d'un sous-groupe par un morphisme est un sous-groupe.

Définition 1.2.5 : Soit $A \subseteq G$. On appelle sous-groupe engendré par A et on note $\langle A\rangle$ l'intersection des sous-groupes contenant A.

Si $x \in G$, on note $\langle x\rangle = \langle\{x\}\rangle$ le sous-groupe engendré par x.

Remarque 1.2.4 : $\langle A\rangle$ est le plus petit sous-groupe de G contenant A (au sens de l'inclusion).

*Exercice 1.2.4 (*théorème de Cayley $\star\star$*)* : Soit G un groupe. Montrer que G est isomorphe à un sous-groupe du groupe des permutations $S(G)$.

Solution :

- *Première méthode :* On pose

$$\tilde{\psi} : \begin{cases} G \to S(G) \\ x \mapsto \sigma_x : \begin{cases} G \to G \\ z \mapsto xz \end{cases} \end{cases}$$

Montrons que $\tilde{\psi}$ est bien définie, c'est-à-dire que pour tout $x \in G$, on a bien $\sigma_x \in S(G)$. Soient $x \in G$ et $y, z \in G$, alors $\sigma_x(z) = y \iff xz = y \iff z = x^{-1}y$. Ainsi y possède un unique antécédent par σ_x, d'où le résultat.

On pose maintenant $\psi : \begin{cases} G \to \tilde{\psi}(G) \\ x \mapsto \tilde{\psi}(x) \end{cases}$. ψ est surjective par définition. Soient $x, y \in G$ tels que $\psi(x) = \psi(y)$. Soit $z \in G$, alors $xz = yz$ donc $x = y$. ψ est donc bijective.

Soient $x, y \in G$ et $z \in G$. On a $\psi(xy)(z) = xyz = \psi(x)(yz) = \psi(x)(\psi(y)(z))$. Ainsi $\psi(xy) = \psi(x) \circ \psi(y)$: ψ est un morphisme de groupes. On a montré que ψ est un isomorphisme, donc G est isomorphe à $\mathrm{Im}(\psi)$ qui est un sous-groupe de $S(G)$.

- *Deuxième méthode :* G agit sur lui-même (par l'action $(g, x) \mapsto gx$), on dispose donc d'un morphisme $\varphi : \begin{cases} G \to S(G) \\ x \mapsto \begin{cases} G \to G \\ z \mapsto xz \end{cases} \end{cases}$. Il n'y a plus qu'à vérifier qu'il est injectif.

Remarque : en particulier, si G est un groupe fini d'ordre n alors il est isomorphe à un sous-groupe de S_n.

Définition 1.2.6 : Un sous groupe $H \subseteq G$ est dit normal ssi $\forall x \in G, xH = Hx$. Dans ce cas, on note $H \trianglelefteq G$.

On notera $H \leq G$ si H est un sous-groupe de G, non nécessairement normal.

Un groupe est dit simple ssi il ne possède pas de sous-groupe normal autre que $\{e\}$ et lui-même.

Exemple 1.2.2:
- Tout sous-groupe d'un groupe abélien est normal.
- Tout sous-groupe du centre est normal.

Lemme 1.2.5 : $H \trianglelefteq G \iff \forall x \in G, xHx^{-1} \subseteq H$

Lemme 1.2.6 : Si $H \trianglelefteq G$ et $\varphi : G \to G'$ est un morphisme alors $\varphi(H)$ est un sous-groupe normal de $\varphi(G)$. Si $H' \trianglelefteq G'$ alors $\varphi^{-1}(H')$ est un sous-groupe normal de G.

Lemme 1.2.7 : Soit H un sous-groupe de G. Alors le normalisateur $N_G(H)$ est le plus grand sous-groupe de G dans lequel H est normal. En particulier, $H \trianglelefteq G \iff H = N_G(H)$.

Définition 1.2.7 : Relation d'équivalence compatible : $xRy \wedge x'Ry' \implies xx'Ryy'$

Définition 1.2.8 : Si H est un sous-groupe de G, on définit les relations R_H^G et R_H^D par $xR_H^G y \iff x^{-1}y \in H$ et $xR_H^D y \iff xy^{-1} \in H$. Ce sont des relations d'équivalence. Les classes d'équivalences de x pour R_H^G et R_H^D sont respectivement xH et Hx, elles sont dites classes à gauche suivant H et classes à droite suivant H.

Théorème 1.2.1 (de Lagrange) : Si G est fini et H est un sous-groupe de G alors :
- $|G/R_H^G| = |G/R_H^D|$, on note ce nombre $[G : H]$
- $|G| = |H| \times [G : H]$.

Preuve :
- $A \mapsto A^{-1}$ est une bijection entre G/R_H^G et G/R_H^D
- $|G| = \sum_{xH \in G/R_H^G} |xH| = |G/H| \times |H|$

■

Définition 1.2.9 :
- On appelle ordre d'un groupe son cardinal.
- On appelle ordre d'un élément $x \in G$ l'ordre du sous-groupe $\langle x \rangle$.

Remarque 1.2.5 : D'après le théorème de Lagrange, si G est fini alors l'ordre d'un sous-groupe (ou d'un élément) de G divise l'ordre de G.

Exercice 1.2.5 (⋆) : Soient G un groupe et H_1, H_2 deux sous-groupes de G d'ordres finis et premiers entre eux. Que dire de $H_1 \cap H_2$?

Solution : Soit $x \in H_1 \cap H_2$. Par le théorème de Lagrange, l'ordre de x divise les ordres de H_1 et H_2, qui sont premiers entre eux, donc l'ordre de x vaut 1, et donc $H_1 \cap H_2 = \{1\}$.

Exercice 1.2.6 (⋆ ⋆ ⋆ ♥) : Soit G un groupe fini non commutatif. Démonter que la probabilité que deux éléments de G pris au hasard commutent est inférieure ou égale à $\frac{5}{8}$.

Solution : Soient $n = |G|$ et $N = |\{(x, y) \in G^2; xy = yx\}|$. Il suffit de montrer que $N \leqslant \frac{5}{8}n^2$.

Notons $Z = \{x \in G |\ \forall y \in G, xy = yx\}$ et pour tout $x \in G$, $C_x = \{y \in G; xy = yx\}$. On vérifie aisément que ces ensembles sont des sous-groupes de G. De plus $N = \sum_{x \in G} |C_x| = \sum_{x \in Z} |C_x| + \sum_{x \in G \setminus Z} |C_x|$. Si $x \in Z$ alors $|C_x| = n$. Si $x \in G \setminus Z$ alors C_x est un sous-groupe strict de G donc par le théorème de Lagrange, $|C_x|$ divise n d'où $|C_x| \leqslant \frac{n}{2}$. Soit $a \in G \setminus Z$ (a existe vu G non commutatif). Alors Z est un sous-groupe strict de C_a (strict car $a \in C_a \setminus Z$) donc par le même argument, $|Z| \leqslant \frac{|C_a|}{2} \leqslant \frac{n}{4}$. Ainsi $N \leqslant n|Z| + \frac{1}{2}n(n - |Z|) = \frac{n^2}{2} + \frac{n|Z|}{2} \leqslant \frac{5}{8}n^2$.

Lemme 1.2.8 : $H \trianglelefteq G$ ssi les relations R_H^G et R_H^D sont les mêmes. Dans ce cas, on les note R_H.

Théorème 1.2.2 : R est compatible ssi $R = R_H$ où $H \trianglelefteq G$.

Preuve : Si R est compatible, on montre d'abord que $H := \overline{1}$ est un sous-groupe de G, puis que $xRy \iff xR_H^G y \iff xR_H^D y$. Réciproquement, OK. ■

Théorème 1.2.3 (de correspondance) : Soient G un groupe et $H \trianglelefteq G$. Alors :
- $f : K \mapsto K/H$ définit une bijection de l'ensemble des sous-groupes de G contenant H sur l'ensemble des sous-groupes de G/H ;
- $H \leq K \leq L \leq G$ ssi $K/H \leq L/H$;
- $H \leq K \trianglelefteq L \leq G$ ssi $K/H \trianglelefteq L/H$.

Preuve :
- On vérifie facilement que f est bien définie. On note $\pi : G \to G/H$ la surjection canonique.

  Montrons que f est injective. Soient K, K' des sous-groupes de G contenant H tels que $K/H = K'/H$. Soit $k \in K$, alors $\pi(k) \in K'/H$ donc il existe $k' \in K'$ tel que $\pi(k) = \pi(k')$. Soit donc $h \in H$ tel que $k = k'h$. Comme $H \subseteq K'$, on a $k \in K'$. Ainsi $K \subseteq K'$, puis $K = K'$ par symétrie.

  Montrons que f est surjective. Soit L un sous-groupe de G/H. Alors $\pi^{-1}(L)$ est un sous-groupe de G contenant H, et on a $\pi^{-1}(L)/H = L$.
- Facile.
- Facile.

■

Théorème 1.2.4 (Premier théorème d'isomorphisme) : Si $\varphi : G \to G'$ est un morphisme de groupes alors il induit un isomorphisme $G/\ker\varphi \xrightarrow{\sim} \operatorname{im}\varphi$.

Preuve : L'isomorphisme est $x \ker\varphi \mapsto \varphi(x)$. ■

Exercice 1.2.7 (⋆ ⋆) : Soit G un groupe fini d'ordre pair $2n$ (où $n \in \mathbb{N}^*$).

1) Soit H un sous-groupe de G d'ordre n. Montrer que $H \trianglelefteq G$.
2) On suppose que G admet deux sous-groupes H_1 et H_2 d'ordre n tels que $H_1 \cap H_2 = \{1\}$. Montrer que $n = 1$ ou $n = 2$.
3) On suppose que G admet deux sous-groupes H_1 et H_2 d'ordre n distincts. Montrer que n est pair.

Solution :

1) Soit $x \in G$, montrons que $xH = Hx$.

- Si $x \in H$, c'est clair.
- On suppose maintenant $x \in G \setminus H$. Soit $xh \in xH$, alors $xh \in G \setminus H$ (sinon $x \in H$). Ainsi $xH \subseteq G \setminus H$ puis $xH = G \setminus H$ par égalité des cardinaux de ces deux ensembles. De même, $Hx = G \setminus H$ donc $xH = Hx$.

1) D'après la question précédente, on peut considérer les groupes G/H_1 et G/H_2. Soit $\varphi : \begin{cases} G \to G/H_1 \times G/H_2 \\ x \mapsto (\pi_1(x), \pi_2(x)) \end{cases}$ où π_1 et π_2 sont les surjections canoniques sur G/H_1 et G/H_2 respectivement. Alors φ est un morphisme de groupes, et il est injectif car $\ker\varphi = H_1 \cap H_2 = \{e\}$. On a donc $|G| \leqslant |G/H_1 \times G/H_2| = 4$ donc $n \leqslant 2$.

2) On considère le même morphisme φ (qui n'est plus injectif). On a $|G| = |\operatorname{im}\varphi| \times |\ker\varphi|$. Or $|\operatorname{im}\varphi| = 4$. En effet, on dispose de $x \in H_1 \setminus H_2$, $y \in H_2 \setminus H_1$ et $z \in G \setminus (H_1 \cup H_2)$. En identifiant G/H_1 et G/H_2 à $\mathbb{Z}/2\mathbb{Z}$, on a $\varphi(e) = (0,0)$, $\varphi(x) = (1,0)$, $\varphi(y) = (0,1)$ et $\varphi(z) = (1,1)$. Ainsi $|G|$ est un multiple de 4 donc n est pair.

Lemme 1.2.9: Soient $H_1, H_2 \leq G$. On pose $H_1H_2 := \{h_1h_2; (h_1,h_2) \in H_1 \times H_2\}$. Alors H_1H_2 est un sous-groupe de G ssi $H_2H_1 \subseteq H_1H_2$, ssi $H_2H_1 = H_1H_2$.

Preuve:

- Supposons que H_1H_2 soit un sous-groupe de G. Soit $z \in H_2H_1$. On écrit $z = yx$ avec $y \in H_2$ et $x \in H_1$. Alors $z = yx = \left(x^{-1}y^{-1}\right)^{-1}$. Or $x^{-1}y^{-1} \in H_1H_2$, et comme H_1H_2 est stable par passage à l'inverse, $z \in H_1H_2$. Ainsi $H_2H_1 \subseteq H_1H_2$.
- Réciproquement, supposons que $H_2H_1 \subseteq H_1H_2$. Clairement, $e \in H_1H_2$. Soient $z, z' \in H_1H_2$. On écrit $z = xy$ et $z' = x'y'$ avec $x, x' \in H_1$ et $y, y' \in H_2$. Alors $zz'^{-1} = xyy'^{-1}x'^{-1}$. Alors $yy'^{-1}x'^{-1} \in H_2H_1 \subseteq H_1H_2$, on peut donc écrire $yy'^{-1}x'^{-1} = x''y''$ avec $x'' \in H_1$ et $y'' \in H_2$. On a alors $zz'^{-1} = xx''y'' \in H_1H_2$. Ceci montre que H_1H_2 est un sous-groupe de G.
- À ce stade, on sait que H_1H_2 est un sous-groupe ssi $H_2H_1 \subseteq H_1H_2$. Montrons que dans ce cas, on a en fait $H_2H_1 = H_1H_2$. Soit $z \in H_1H_2$, alors $z^{-1} \in H_1H_2$: soient donc $x \in H_1$ et $y \in H_2$ tels que $z^{-1} = xy$. Alors $z = y^{-1}x^{-1} \in H_2H_1$.

■

Théorème 1.2.5 (Deuxième théorème d'isomorphisme): Soient $N \trianglelefteq G$ et $H \leq G$. Alors $H \cap N \trianglelefteq H$, $N \trianglelefteq HN$ et

$$H/(H \cap N) \simeq HN/N$$

Preuve: On considère la composée de l'injection canonique $H \hookrightarrow G$ et de la surjection canonique $G \twoheadrightarrow N$. Cette composée est un morphisme de noyau $H \cap N$ et d'image HN/N, d'où le résultat par le premier théorème d'isomorphisme. ■

Théorème 1.2.6 (Troisième théorème d'isomorphisme): Soient $M \trianglelefteq G$ et $N \trianglelefteq G$ tels que $M \leq N$. Alors $N/M \trianglelefteq G/M$ et

$$(G/M)/(N/M) \simeq G/N$$

Preuve: Appliquer le premier théorème d'isomorphisme à

$$\begin{aligned} G/M &\to G/N \\ xM &\mapsto \quad xN \end{aligned}$$

■

1.3. Généralités sur les anneaux

Définition 1.3.1:
- Soit A un ensemble muni de deux lois de composition interne $+$ et $\times$. On dit que $(A, +, \times)$ est un anneau ssi $(A, +)$ est un groupe abélien et la loi $\times$ est associative et distributive par rapport à l'addition. Dans ce cas :
- on dit que $(A, +, \times)$ est unitaire ssi la loi $\times$ admet un élément neutre ;
- on dit que $(A, +, \times)$ est commutatif ssi la loi $\times$ est commutative ;
- on dit que $(A, +, \times)$ est intègre ssi $\forall a, b \in A, ab = 0 \Longrightarrow a = 0 \vee b = 0$;
- on dit que $(A, +, \times)$ est nul ssi A ne possède qu'un seul élément (à savoir 0) ;
- si $(A, +, \times)$ est unitaire, un élément $x \in A$ est dit inversible ssi il possède un inverse pour la loi $\times$;
- on dit que $(A, +, \times)$ est un corps si c'est un anneau commutatif, unitaire, non nul et tel que tout élément non nul est inversible.

Remarque 1.3.1: Si $(A, +, \times)$ est un anneau alors $\forall x \in A, 0 \times x = x \times 0 = 0$. En particulier, si A est unitaire et non nul alors 0 n'est pas inversible.

Exemple 1.3.1: $(\mathbb{Z}, +, \times)$ est un anneau unitaire commutatif intègre dont les éléments inversibles sont -1 et 1.

Exercice 1.3.1 ($\star$): Soit A un anneau tel que tout élément de A est idempotent, i.e. $\forall x \in A, x^2 = x$.
1) Montrer que $\forall x \in A, 2x = 0$.
2) Montrer que A est commutatif.
3) Montrer que $\forall x, y \in A, xy(x + y) = 0$. Que dire si A est intègre ?

Solution:
1) Soit $x \in A$, alors $2x = (2x)^2 = 4x^2 = 4x$ donc $2x = 0$.
2) Soient $x, y \in A$, alors $x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + y + xy + yx$, donc $xy + yx = 0$. D'après la question précédente, $xy = xy + 2yx = yx$. Ainsi A est commutatif.
3) Soient $x, y \in A$. Comme A est commutatif, $xy(x + y) = x^2y + xy^2 = xy + xy = 2xy = 0$. Si A est intègre alors pour tous $x, y \in A \setminus \{0\}$, $x + y = 0$ donc pour tous $x, z \in A \setminus \{0\}$, en prenant $y = -z$ on obtient $x = z$. Ainsi A possède au plus deux éléments.

Exercice 1.3.2 ($\star\star$): Soient A un anneau unitaire et $a, b \in A$ tels que $1 - ab$ est inversible. Montrer que $1 - ba$ est inversible.

Solution: Calcul formel pour avoir l'idée du résultat : $(1 - ba)^{-1} = \sum_{n=0}^{\infty} (ba)^n = 1 + \sum_{n=0}^{\infty} (ba)^{n+1} = 1 + b\Big(\sum_{n=0}^{\infty} (ab)^n\Big)a = 1 + b(1 - ab)^{-1}a$.

Notons $c = (1 - ab)^{-1}$ et montrons que $1 - ba$ est inversible d'inverse $1 + bca$. On a
$(1 - ba)(1 + bca) = 1 - ba + bca - babca = 1 + b(-1 + c - bc)a$
$= 1 + b(-1 + (1 - b)c) = 1 + b(-1 + 1) = 1$ et de même,

$$(1+bca)(1-ba) = 1 - ba + bca - bcaba = 1 + b(-1 + c - cab)a = 1 + b(-1 + c(1-ab))$$
$$= 1 + b(-1+1) = 1$$

d'où le résultat.

Désormais, $(A, +, \times)$ est un anneau. On note 0 l'élément neutre pour la loi $+$ et 1 l'élément neutre pour la loi $\times$, à condition qu'il existe.

Théorème 1.3.1 (formule du binôme de Newton) : On suppose que A est unitaire. Soient $a, b \in A$ tels que $ab = ba$. Alors

$$\forall n \in \mathbb{N}, (a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Preuve : On montre le résultat par récurrence sur n. Pour $n = 0$ c'est clair. Soit $n \in \mathbb{N}$, supposons le résultat au rang n. Alors

$$\begin{aligned}
(a+b)^{n+1} &= \left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\right)(a+b) \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k} \\
&= \sum_{k=1}^{n+1} \binom{n}{k-1} a^k b^{n+1-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k} \\
&= b^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^k b^{n+1-k} + a^{n+1} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}
\end{aligned}$$

■

Lemme 1.3.1 : L'ensemble des éléments inversibles de A muni de la loi $\times$ est un groupe, dit groupe des inversibles de A et noté $A^\times$.

Définition 1.3.2 : Un élément $x \in A$ est dit nilpotent ssi $\exists n \in \mathbb{N}^*, x^n = 0$. Dans ce cas, on appelle indice de nilpotence de x l'entier $\min\{n \in \mathbb{N}^*, x^n = 0\}$.

L'anneau A est dit réduit ssi 0 est le seul élément nilpotent.

Exercice 1.3.3 (⋆) : Soient A un anneau unitaire et $x \in A$ un élément nilpotent.

1) Montrer que $1 - x$ est inversible.
2) Pour tout $n \in \mathbb{N}$, simplifier l'expression $U_n = \prod_{k=0}^{n} \left(1 + x^{2^k}\right)$.

Solution :

1) Soit n l'indice de nilpotence de A, alors $(1-x)(1 + x + ... + x^{n-1}) = 1 - x^n = 1 = (1 + x + ... + x^{n-1})(1-x)$ donc $1 - x$ est inversible.
2) On montre facilement par récurrence que pour tout $n \in \mathbb{N}$, $(1-x)U_n = 1 - x^{2^{n+1}}$ donc $U_n = (1-x)^{-1}\left(1 - x^{2^{n+1}}\right)$.

Définition 1.3.3 : Une partie $B \subseteq A$ est dite sous-anneau de $(A, +, \times)$ ssi $(B, +|_{B^2}, \times|_{B^2})$ est un anneau.

Lemme 1.3.2 : B est un sous-anneau de $(A, +, \times)$ ssi c'est un sous-groupe de $(A, +)$ et $\forall x, y \in B, xy \in B$.

Définition 1.3.4 : Produit d'anneaux

Définition 1.3.5 : Morphisme d'anneaux, noyau, image

Lemme 1.3.3 : L'image et l'image réciproque d'un sous-anneau par un morphisme est un sous-anneau.

Définition 1.3.6 : On suppose que A est unitaire.
- Si 1 est d'ordre fini $n \in \mathbb{N}$ en tant qu'élément du groupe $(A, +)$, on dit que A est de caractéristique n.
- Sinon, on dit que A est de caractéristique 0.

Remarque 1.3.2:
- Si A est de caractéristique $N \in \mathbb{N}^*$ alors $\forall a \in A, Na = 0$.
- Si A est intègre et $n \in \mathbb{N}$ et $a \in A \setminus \{0\}$ sont tels que $na = 0$, alors $(n1) \times a = 0$, donc $n1 = 0$. Du coup la caractéristique de A est non nulle et divise n.

Lemme 1.3.4 : Si A est unitaire et intègre alors sa caractéristique est 0 ou un nombre premier.

Preuve: Supposons que A est unitaire, intègre, et de caractéristique $c \neq 0$ et montrons que c est premier. On écrit $c = ab$ où $a, b \in \mathbb{N}^*$. Alors $0 = c1 = (a1)(b1)$, mais A est intègre donc $a1 = 0$ ou $b1 = 0$, et donc $a = c$ ou $b = c$. ■

Définition 1.3.7 : On suppose que A est unitaire. On dit qu'un ensemble M muni d'une loi de composition interne $+$ et d'une loi de composition externe $\cdot : A \times M \to M$ est un A-module ssi :
- $(M, +)$ est un groupe abélien ;
- $\forall x \in M, 1 \cdot x = x$;
- $\forall a, b \in A, \forall x \in M, (a + b) \cdot x = a \cdot x + b \cdot x$;
- $\forall a \in A, \forall x, y \in M, a \cdot (x + y) = a \cdot x + a \cdot y$;
- $\forall a, b \in A, \forall x \in M, (ab) \cdot x = a \cdot (b \cdot x)$.

Définition 1.3.8 : On suppose que A est commutatif et unitaire. Soit M un ensemble muni de deux lois de composition interne $+$ et $\times$ et d'une loi de composition externe $\cdot : A \times M \to M$. On dit que $(M, +, \times, \cdot)$ est une A-algèbre ssi :
- $(M, +, \times)$ est un anneau unitaire ;
- $(M, +, \cdot)$ est un A-module ;
- $\forall a \in A, \forall x, y \in M, a \cdot (x \times y) = (a \cdot x) \times y = x \times (a \cdot y)$.

Remarque 1.3.3 : Avec les mêmes notations, on a un morphisme d'anneaux

$$\begin{aligned} \varphi : A &\to M \\ a &\mapsto a \cdot 1 \end{aligned}$$

vérifiant $\forall a \in A, \forall x \in M, a \cdot x = \varphi(a)x$

Exemple 1.3.2 : Tout anneau est une $\mathbb{Z}$-algèbre pour la loi externe $(n, x) \mapsto nx$.

1.4. Idéaux

Définition 1.4.1 : Soit $I \subseteq A$. On dit que I est un idéal de $(A, +, \times)$ ssi $(I, +)$ est un sous-groupe de $(A, +)$ et $\forall (x, a) \in I \times A, xa \in I \wedge ax \in I$.

Remarque 1.4.1 :
- Un idéal est un sous-anneau.
- Si $(A, +, \times)$ est commutatif alors $xA := \{xa; a \in A\}$ est un idéal de A, dit idéal engendré par x. C'est le plus petit idéal de A contenant x.
- Si $(A, +, \times)$ est unitaire et I est un idéal contenant 1 alors $I = A$. Si I contient un élément inversible x alors $1 = x^{-1}x \in I$ et $I = A$.

Lemme 1.4.1 : Une intersection d'idéaux de A est un idéal de A. Une somme fini d'idéaux de A est un idéal de A.

Définition 1.4.2 :
- Si A est commutatif, on dit qu'un idéal I est principal ssi $\exists x \in A, I = xA$.
- A est dit principal ssi A est unitaire, commutatif, intègre et tous les idéaux de A sont principaux.

Remarque 1.4.2 : Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, qui sont principaux. Du coup, $\mathbb{Z}$ est un anneau principal.

Exercice 1.4.1 ($\star\star\star$) : Soit A un anneau commutatif unitaire. On dit que A est noethérien ssi tout idéal I de A est engendré par un nombre fini d'éléments, i.e est de la forme $I = x_1A + ... + x_kA$ où $x_1, ..., x_k \in I$. Montrer que A est noethérien ssi il n'existe pas de suite d'idéaux de A strictement croissante pour l'inclusion.

Solution :

- Supposons que A est noethérien. Supposons par l'absurde qu'il existe une suite $(I_n)_{n\in\mathbb{N}}$ d'idéaux strictement croissante pour l'inclusion. Alors on vérifie facilement que $I = \bigcup_{n\in\mathbb{N}} I_n$ est un idéal de A. Soient donc $x_1, ..., x_k \in I$ tels que $I = x_1A + ... + x_kA$. Pour tout $i \in [\![1, k]\!]$, il existe $n_i \in \mathbb{N}$ tel que $x_i \in I_{n_i}$. En notant $N = \max\{n_i; i \in [\![1, k]\!]\}$, on a $I = x_1A + ... + x_kA \in I_N$ donc $I = I_N$. Ainsi la suite $(I_n)_{n\in\mathbb{N}}$ est stationnaire, absurde.
- Réciproquement, raisonnons par contraposée et supposons que A n'est pas noethérien. Soit donc I un idéal qui n'est pas engendré par un nombre fini d'éléments. On va construire par récurrence une suite $(x_n)_{n\in\mathbb{N}} \in I^{\mathbb{N}}$ telle que $(x_0A + ... + x_nA)_{n\in\mathbb{N}}$ soit une suite d'idéaux strictement croissante pour l'inclusion.
  - On pose $I_0 = x_0A$ où $x_0 \in I$.
  - Soit $n \in \mathbb{N}$, supposons $x_0, ..., x_n$. Comme I n'est pas engendré par un nombre fini d'éléments, $x_0A + ... + x_nA$ est strictement inclus dans I. Soit donc $x_{n+1} \in I \setminus (x_0A + ... + x_nA)$. Alors $x_0A + ... + x_nA$ est strictement inclus dans $x_0A + ... + x_{n+1}A$, ce qui achève la construction.

Théorème 1.4.1 : Les relations d'équivalence sur A compatibles avec les lois $+$ et $\times$ sont exactement les relations $\sim$ de la forme $x \sim y \iff x - y \in I$ où I est un idéal de A. Dans ce cas, $A/\sim$ est un anneau, dit anneau quotient et noté A/I.

Preuve:
- Si $\sim$ est une relation d'équivalence compatible avec les lois $+$ et $\times$ alors $\sim$ est compatible avec la structure de groupe de A, donc de la forme $x \sim y \iff x - y \in I$ où I est un sous-groupe de A. Soient $x \in I$ et $a \in A$, alors $x \sim 0$ et $a \sim a$ donc $xa \sim ax \sim 0$ i.e. $xa \in I$ et $ax \in I$. Ainsi I est un idéal de A.
- Réciproquement, soit I un idéal de A. D'après les résultats sur les groupes quotients, la relation définie par $x \sim y \iff x - y \in I$ est une relation d'équivalence compatible avec la loi $+$. Soient $w, x, y, z \in I$ tels que $w \sim x$ et $y \sim z$, alors $w - x \in I$ et $y - z \in I$, donc $wy - xy \in I$ et $xy - xz \in I$, et donc $wy - xz \in I$ i.e. $wy \sim xz$. Ainsi $\sim$ est compatible avec la loi $\times$.

■

Théorème 1.4.2 : Soient A et A' deux anneaux, et $f : A \to A'$ un morphisme d'anneaux.
1) Si I' est un idéal de A' alors $f^{-1}(I')$ est un idéal de A. En particulier, $\ker f$ est un idéal de A.
2) Si I est un idéal de A alors $f(I)$ est un idéal de $\operatorname{im} f$.
3) $f(A)$ et $A/\ker f$ sont isomorphes en tant qu'anneaux.

Définition 1.4.3 :
- Un idéal R de A est dit radical ssi $\forall x \in A, \forall n \in \mathbb{N}, (x^n \in R \Rightarrow x \in R)$.
- Un idéal $P \neq A$ de A est dit premier ssi $\forall x, y \in A, xy \in P \Longrightarrow x \in P \vee y \in P$.
- Un idéal $M \neq A$ de A est dit maximal ssi les seuls idéaux de A contenant M sont M et A.

Exemple 1.4.1 :
- Les idéaux radicaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$ où n est sans facteur carré ou $n = 0$.
- Les idéaux premiers de $\mathbb{Z}$ sont les $p\mathbb{Z}$ où p est premier ou $p = 0$.
- Les idéaux maximaux de $\mathbb{Z}$ sont les $p\mathbb{Z}$ où p est premier.

Lemme 1.4.2 : Si A est un anneau principal alors tout idéal premier non trivial est maximal.

Preuve : Supposons que A est un anneau principal. Soient P un idéal premier non trivial, puis I un idéal contenant P. Comme A est principal, on dispose de $p \in P$ et $i \in I$ tels que $P = pA$ et $I = iA$. Comme $p \in I$, il existe $a \in A$ tel que $p = ia$. Comme P est premier, on a $i \in P$ ou $a \in P$. Si $i \in P$ alors $I = iA = P$. Sinon, il existe $a' \in A$ tel que $a = pa'$. Dans ce cas, $p = ia = ipa'$ donc $p(1 - ia') = 0$. Mais A est principal donc intègre et $p \neq 0$ car P est non trivial, donc $1 = ia' \in I$, et donc $I = A$. ■

Théorème 1.4.3 : On suppose que A est commutatif et unitaire.
1) Un idéal R est radical ssi l'anneau quotient A/R est réduit.
2) Un idéal $P \neq A$ est premier ssi l'anneau quotient A/P est intègre.
3) Un idéal $M \neq A$ est maximal ssi l'anneau quotient A/P est un corps.

Preuve :

1)
$$\begin{aligned} R \text{ est radical} &\iff \forall x \in A, \forall n \in \mathbb{N}, x^n \in R \Longrightarrow x \in R \\ &\iff \forall x \in A, \forall n \in \mathbb{N}, \overline{x}^n = 0 \Longrightarrow \overline{x} = 0 \\ &\iff A/R \text{ est réduit} \end{aligned}$$

2)
$$\begin{aligned} P \text{ est premier} &\iff \forall x, y \in A, xy \in P \Longrightarrow x \in P \vee y \in P \\ &\iff \forall x, y \in A, \overline{xy} = 0 \Longrightarrow \overline{x} = 0 \vee \overline{y} = 0 \\ &\iff A/P \text{ est intègre} \end{aligned}$$

3)
- Supposons que M est maximal. Soit $x \in A$ tel que $\overline{x} \neq 0$ (i.e. $x \notin M$). Alors $M + xA$ est un idéal qui contient strictement M, donc $M + xA = A$. Soient donc $a \in A$ et $m \in M$ tels que $1 = m + xa$, alors $\overline{1} = \overline{xa}$ donc $\overline{x}$ est inversible.
- Réciproquement, supposons que A/M est un corps. Soit I un idéal de A contenant M. Supposons $I \neq M$ et montrons $I = A$. Soit $x \in I \setminus M$. Comme $\overline{x} \neq 0$, on dispose de $y \in A$ tel que $\overline{xy} = \overline{1}$, i.e. $xy - 1 \in M$. On a alors $xy \in I$ et $xy - 1 \in I$ donc $1 \in I$, et donc $I = A$.

■

Remarque 1.4.3 : En particulier, tout idéal maximal est premier, et tout idéal premier est radical.

Exercice 1.4.2 (⋆) : Soient A un anneau commutatif unitaire et I un idéal de A. On appelle radical de I l'ensemble $\sqrt{I} = \{x \in A; \exists n \in \mathbb{N}^*, x^n \in I\}$.
1) Montrer que $\sqrt{I}$ est un idéal de A.

2) Déterminer les radicaux des idéaux de $\mathbb{Z}$.

Solution :

1) Montrons que $\sqrt{I}$ est un sous-groupe de $(A,+)$. Déjà, $0 \in \sqrt{I}$. Soient $x, y \in \sqrt{I}$, soient donc $i, j \in \mathbb{N}^*$ tels que $x^i \in I$ et $y^j \in I$. Alors $(-x)^i = (-1)^i x^i \in I$ donc $-x \in \sqrt{I}$. De plus $(x+y)^{i+j-1} = \sum_{k=0}^{i+j-1} \binom{i+j-1}{k} x^k y^{i+j-1-k}$. Mais $x^k \in I$ pour tout $k \geqslant i$ et $y^{i+j-1-k} \in I$ pour tout $k < i$, donc $(x+y)^{i+j-1} \in I$ et $x+y \in \sqrt{I}$.
2) Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$ où $n \in \mathbb{N}$. Soit $n \in \mathbb{N}$, notons $I = n\mathbb{Z}$. Si $n = 0$ alors $I = \{0\}$ et $\sqrt{I} = \{0\}$. Si $n = 1$ alors $I = \mathbb{Z}$ et $\sqrt{I} = \mathbb{Z}$. On suppose maintenant $n \geqslant 2$. Soit $x \in \sqrt{I}$, soit donc $i \in \mathbb{N}^*$ tel que $x^i \in I$. Alors $n | x^i$ donc pour tout facteur premier p de n, $p|x$. Ainsi, en notant $n = p_1^{\alpha_1} ... p_k^{\alpha_k}$ la décomposition en facteurs premiers de n (où $p_1, ..., p_k$ sont distincts), on a $\sqrt{I} \subseteq p_1 ... p_k \mathbb{Z}$ et montre facilement que l'inclusion réciproque est vérifiée.

Théorème 1.4.4 (de Krull) : Soient A un anneau commutatif unitaire, et I un idéal propre de A (i.e. un idéal différent de A tout entier). Alors il existe un idéal maximal de A contenant I.

Preuve : On utilise le résultat ensembliste suivant (conséquence du lemme de Zorn) :

Lemme 1.4.3 *(Principe maximal de Hausdorff)* : Soient A un ensemble et $\mathcal{F} \subseteq 2^A$. On suppose que $\mathcal{F} \neq \emptyset$ et que pour toute partie non vide $\mathcal{J}$ de $\mathcal{F}$ totalement ordonnée par l'inclusion, la réunion $\bigcup_{I \in \mathcal{J}} I$ soit contenue dans un élément de $\mathcal{F}$. Alors $\mathcal{F}$ possède un élément maximal pour l'inclusion.

Soit $\mathcal{F}$ l'ensemble des idéaux propres de A contenant I. Alors $\mathcal{F} \neq \emptyset$. Si $\mathcal{J}$ une partie non vide de $\mathcal{F}$ totalement ordonnée pour l'inclusion, on voit facilement que $\bigcup_{J \in \mathcal{J}} J$ est un idéal de A contenant I. C'est un idéal propre car il ne contient pas 1, et le principe maximal de Hausdorff permet de conclure. ■

Théorème 1.4.5 (chinois) : On suppose que A est unitaire. Soient $I_1, ..., I_k$ des idéaux de A tels que $\forall i \neq j, I_i + I_j = A$. Alors l'application

$$\begin{cases} A/(I_1 \cap ... \cap I_k) & \to (A/I_1) \times ... \times (A/I_k) \\ x \bmod I_1 \cap ... \cap I_k & \mapsto (x \bmod I_1, ..., x \bmod I_k) \end{cases}$$

est un isomorphisme d'anneaux.

Preuve :

Lemme 1.4.4 : $A = (I_1 \cap ... \cap I_{k-1}) + I_k$

Preuve : Il suffit de montrer le résultat pour $k = 3$, le reste suit par une récurrence facile. Comme $A = I_1 + I_3 = I_2 + I_3$, on dispose de $i_1 \in I_1$, $i_2 \in I_2$ et $i_3, i_3' \in I_3$ tels que $1 = i_1 + i_3 = i_2 + i_3'$. Du coup $1 = i_1(i_2 + i_3') + i_3 = i_1 i_2 + (i_1 i_3' + i_3) \in I_1 \cap I_2 + I_3$, donc $A = I_1 \cap I_2 + I_3$. ■

Soit maintenant φ le morphisme canonique de A dans $\prod_{i=1}^{k} A/I_k$. Alors $\ker\varphi = \bigcap_{i=1}^{k} I_k$. Montrons par récurrence sur k que φ est surjectif. Pour $k=1$ c'est trivial. Supposons le résultat au rang $k-1$ et prouvons-le au rang k. Soient $x_1, ..., x_k \in A$. Par hypothèse de récurrence, il existe $y \in A$ tel que $y - x_i \in I_i$ pour tout $i \in [\![1, k-1]\!]$. On a $y - x_k \in A = (I_1 \cap ... \cap I_{k-1}) + I_k$, soit donc $z \in I_1 \cap ... \cap I_{k-1}$ tel que $y - x_k - z \in I_k$. On pose $x = y - z$, alors $x - x_i \in I_i$ pour tout $i \in [\![1, k]\!]$.

Ainsi φ est surjectif, donc $\tilde{\varphi} : A/(I_1 \cap ... \cap I_k) \to (A/I_1) \times ... \times (A/I_k)$ est un isomorphisme d'anneaux.

1.5. Arithmétique

Ici, $(A, +, \times)$ est un anneau unitaire commutatif intègre.

Définition 1.5.1 : Soient $a, b \in A$. On dit que a divise b et on note $a|b$ ssi $\exists q \in A, b = aq$. On dit aussi que b est divisible par a et que b est un multiple de a.

Remarque 1.5.1 :
- $a|b \iff b \in aA \iff bA \subseteq aA$
- Comme A est intègre, un tel q est unique, et on pourra le noter $\frac{b}{a}$
- Un élément de A est inversible ssi il divise tous les éléments de A.
- La divisibilité est réflexive et transitive.
- On a $a|b$ et $b|a$ ssi il existe un inversible u tel que $a = ub$. Dans ce cas, on dit que a et b sont associés. L'association est une relation d'équivalence.

Définition 1.5.2 : $a \in A$ est dit irréductible ssi :
- a n'est pas inversible ;
- si $a = xy$ alors x est inversible ou y est inversible.

Exemple 1.5.1 : Les éléments irréductibles de $\mathbb{Z}$ sont les $\pm p$ où p est un nombre premier.

Définition 1.5.3 : Soit $(a_i)_{i\in I}$ une famille d'éléments de A.
- On dit que $d \in A$ est un plus grand commun diviseur (abrégé en PGCD) des $(a_i)_{i\in I}$ ssi c'est un diviseur commun des $(a_i)_{i\in I}$, et que tout diviseur commun des $(a_i)_{i\in I}$ divise d.
- On dit que $m \in A$ est un plus petit multiple commun (abrégé en PPCM) des $(a_i)_{i\in I}$ ssi c'est un multiple commun des $(a_i)_{i\in I}$ et tout multiple commun des $(a_i)_{i\in I}$ est un multiple de m.

Remarque 1.5.2 :
- Les $(a_i)_{i\in I}$ n'admettent pas toujours de PGCD ni de PPCM, y-compris s'il y a seulement deux éléments dans la famille.
- Les PGCD des $(a_i)_{i\in I}$, si il existent, forment une classe d'associés. De même pour les PPCM.
- Pour tout $a \in A$, a est un PGCD de 0 et a, et 0 est un PPCM de 0 et a.

Définition 1.5.4 : Soit $(a_i)_{i\in I}$ une famille d'éléments de A. On dit que les $(a_i)_{i\in I}$ sont premiers entre eux ssi 1 est un PGCD des $(a_i)_{i\in I}$.

Remarque 1.5.3 :
- Si les $(a_i)_{i\in I}$ sont deux à deux premiers entre eux alors ils sont premiers entre eux, mais la réciproque est fausse.
- Les $(a_i)_{i\in I}$ sont premiers entre eux ssi leurs seuls diviseurs communs sont les inversibles de A.

Lemme 1.5.1 : Si a est un élément irréductible de A alors tout élément $b \in A$ est premier avec a ou divisible par a.

Preuve : Supposons que b n'est pas divisible par a et montrons qu'il est premier avec a. Soit x un diviseur commun de a et b. On écrit $a = xy$ où $y \in A$. y n'est pas inversible, sinon a diviserait x, donc b. Comme a est irréductible, on en déduit que x est inversible. Ainsi a et b sont premiers entre eux. ■

Lemme 1.5.2 : Soit $a \in A \setminus \{0\}$ tel que l'idéal aA est premier. Alors a est irréductible.

Preuve :
- a n'est pas inversible, sinon on aurait $aA = A$ et aA ne serait pas premier.
- Soient $x, y \in A$ tels que $a = xy$. Alors $xy \in aA$ donc $x \in aA$ ou $y \in aA$. Supposons sans perte de généralité que $x \in aA$, soit donc $z \in A$ tel que $x = az$. On a alors $a = azy$ et comme A est intègre, $zy = 1$ et donc y est inversible.

■

Définition 1.5.5 : On dit que l'anneau $(A, +, \times)$ est factoriel ssi :
- tout élément non nul de A s'écrit sous la forme $up_1...p_r$ où u est inversible et $p_1, ..., p_r$ sont irréductibles.
- cette écriture est unique à permutation et multiplication par des inversibles près : si $up_1...p_r = vq_1...q_s$ avec u, v inversibles et $p_1, ..., p_r, q_1, ..., q_r$ irréductibles alors $r = s$ et il existe $\sigma \in S_r$ tels que p_i et $q_{\sigma(i)}$ soient associés pour tout i.

Remarque 1.5.4 :

- On suppose que l'anneau $(A, +, \times)$ est factoriel. Soit $\mathcal{P}$ un système de représentants irréductibles de A, i.e. une partie de A qui contient exactement un élément irréductible par classe d'associés contenant au moins un élément irréductible. Alors tout $a \in A$ s'écrit de manière unique sous la forme $a = u\prod_{p\in\mathcal{P}} p^{v_p(a)}$ où les $v_p(a)$ sont des entiers naturels presque tous nuls. $v_p(a)$ est dit valuation p-adique de a.
- On a $a|b \iff \forall p \in \mathcal{P}, v_p(a) \leqslant v_p(b)$.
- a et b sont premiers entre eux ssi $\forall p \in \mathcal{P}, v_p(a) = 0 \vee v_p(b) = 0$.
- Si $a, b \in A$ alors $\forall p \in \mathcal{P}, v_p(ab) = v_p(a) + v_p(b)$.

Lemme 1.5.3 : On suppose que l'anneau $(A, +, \times)$ est factoriel. Soient $a, b_1, ..., b_r \in A$.
1) Si a est premier avec chacun des b_i alors a est premier avec $b_1...b_r$.

2) Si les b_i sont premiers entre eux deux à deux et que a est un multiple de tous les b_i alors a est un multiple de $b_1 ... b_r$.

Preuve: Clair avec la remarque précédente. ■

Théorème 1.5.1: On suppose que l'anneau $(A, +, \times)$ est factoriel. Soit $(a_i)_{i\in I}$ une famille finie (non vide) d'éléments de A. Alors les $(a_i)_{i\in I}$ admettent un PGCD et un PPCM. Si de plus les $(a_i)_{i\in I}$ sont non nuls et $\mathcal{P}$ est un système de représentants irréductibles de A alors

$$\prod_{p\in\mathcal{P}} p^{\min\{v_p(a_i);i\in I\}} \text{ est un PGCD des } (a_i)_{i\in I}, \text{ et}$$
$$\prod_{p\in\mathcal{P}} p^{\max\{v_p(a_i);i\in I\}} \text{ est un PPCM des } (a_i)_{i\in I}.$$

Preuve: Si les $(a_i)_{i\in I}$ sont non nuls on vérifie facilement que les formules ci-dessus fonctionnent. Si les $(a_i)_{i\in I}$ sont tous nuls, ils admettent 0 comme PGCD et comme PPCM. Si certains des $(a_i)_{i\in I}$ sont nuls mais pas tous alors ils admettent 0 comme PPCM. De plus, on note $J = \{i \in I; a_i \neq 0\}$. D'après ce qui précède, les $(a_i)_{i\in J}$ admettent un PGCD, qui est aussi un PGCD des $(a_i)_{i\in I}$. ■

Lemme 1.5.4: On suppose que l'anneau $(A, +, \times)$ est factoriel. Soient $a, b \in A$, d un PGCD de a et b et m un PPCM de a et b. Alors ab et dm sont associés.

Preuve: Si a et b sont non nuls alors dm est associé à

$$\prod_{p\in\mathcal{P}} p^{\min\{v_p(a),v_p(b)\}} \prod_{p\in\mathcal{P}} p^{\max\{v_p(a),v_p(b)\}} = \prod_{p\in\mathcal{P}} p^{v_p(a)+v_p(b)} = \prod_{p\in\mathcal{P}} p^{v_p(ab)}$$

donc dm est associé à ab. Si $a = 0$ ou $b = 0$ c'est clair. ■

Lemme 1.5.5: On suppose que l'anneau $(A, +, \times)$ est factoriel. Soient $a, a_1, ..., a_n \in A$. Alors
- les PGCD de $aa_1, ..., aa_n$ sont exactement les ad où d est un PGCD de $a_1, ..., a_n$;
- les PPCM de $aa_1, ..., aa_n$ sont exactement les am où m est un PPCM de $a_1, ..., a_n$.

Preuve: Facile avec le théorème précédent. ■

Lemme 1.5.6: Soit A un anneau intègre vérifiant la propriété d'existence d'une décomposition en produit de facteurs irréductibles. Les propriétés suivantes sont équivalentes :
- A est factoriel ;
- pour tout élément irréductible p de A, l'idéal pA est premier ;
- (lemme de Gauss) si $a, b, c \in A$ sont tels que $a|bc$ et a est premier avec b, alors a divise c.

Preuve:
- Supposons le lemme de Gauss. Soit $p \in A$ irréductible. On a $pA \neq A$ car p n'est pas inversible. Soient $a, b \in A$ tels que $ab \in pA$, i.e. $p|\ ab$. Par un lemme précédent, soit $p|a$, soit p est premier avec a. Dans le premier cas $a \in pA$ et dans le second cas, $b \in pA$ par le lemme de Gauss. Ainsi pA est premier.
- Supposons que pour tout élément irréductible p de A, l'idéal pA est premier. On fixe $\mathcal{P}$ un système de représentants irréductibles de A. Soit $a \in A \setminus \{0\}$, on écrit $a = u\prod_{p\in\mathcal{P}} p^{v_p} = v\prod_{p\in\mathcal{P}} p^{w_p}$ où u et v sont inversibles et les familles $(v_p)_{p\in\mathcal{P}}$ et $(w_p)_{p\in\mathcal{P}}$ sont presque nulles. Supposons par l'absurde qu'il existe $p_0 \in \mathcal{P}$ tel que $v_{p_0} \neq w_{p_0}$, disons $w_{p_0} > v_{p_0}$.

Alors $p_0 \mid \prod_{p \neq p_0} p^{v_p}$. Mais l'idéal $p_0 A$ est premier, donc p_0 divise un $p \in \mathcal{P} \setminus \{p_0\}$. p et p_0 sont alors associés, ce qui contredit le choix de $\mathcal{P}$, absurde. Du coup pour tout $p \in \mathcal{P}$, $v_p = w_p$, puis $u = v$. Ainsi A est factoriel.

- Supposons que A est factoriel. On fixe $\mathcal{P}$ un système de représentants irréductibles de A.
  - Si $a = 0$ alors $bc = 0$, donc $b = 0$ ou $c = 0$, mais a est premier avec b donc $c = 0$ et $a|c$.
  - Sinon, on a, b et c sont non nuls et on a $v_p(a) \leqslant v_p(b) + v_p(c)$. Comme a est premier avec b, on a pour tout $p \in \mathcal{P}$, $v_p(a) = 0$ ou $v_p(b) = 0$. Dans les deux cas, $v_p(a) \leqslant v_p(c)$ i.e. $a|c$.

■

Remarque 1.5.5: Du coup, dans un anneau factoriel, pour tout $p \in A \setminus \{0\}$, l'idéal pA est premier ssi p est irréductible.

Théorème 1.5.2: Tout anneau principal est factoriel.

Preuve: Soit A un anneau principal.

- Montrons que A est noethérien, i.e. qu'il n'existe pas de suite d'idéaux de A strictement croissante. Supposons par l'absurde qu'il existe une suite $(I_n)_{n\in\mathbb{N}}$ d'idéaux strictement croissante. Soit $I = \bigcup_{n\in\mathbb{N}} I_n$. On vérifie facilement que I est un idéal de A. Mais A est principal, donc il existe $a \in A$ tel que $I = aA$. On a $a \in I$, soit donc $n \in \mathbb{N}$ tel que $a \in I_n$. On a alors $I = I_n$, ce qui contredit la stricte croissance de $(I_n)_{n\in\mathbb{N}}$.
- Déduisons-en l'existence de la décomposition en facteurs irréductibles. Supposons par l'absurde qu'il existe $a \in A$ ne pouvant pas s'écrire comme produit d'un inversible et d'éléments irréductibles. Alors a n'est pas irréductible, donc on peut écrire $a = a_1 b_1$ où a_1 et b_1 ne sont pas inversibles. Mais alors aA est inclus dans $a_1 A$ et dans $b_1 A$. De plus ces inclusions sont strictes : si $a_1 \in aA$ alors il existe $a' \in A$ tel que $a_1 = aa' = a_1 b_1 a'$ donc $b_1 a' = 1$ et b_1 est inversible, absurde. Du coup $a_1 \in a_1 A \setminus aA$ et de même, $b_1 \in b_1 A \setminus aA$. De plus a_1 et b_1 ne peuvent pas être tous les deux irréductibles puisque a ne s'écrit pas comme produit d'éléments irréductibles. On suppose sans perte de généralité que a_1 n'est pas irréductible, et on peut alors écrire $a_1 = a_2 b_2$ où a_2 et b_2 ne sont pas irréductibles. En itérant le processus, on obtient une suite $(a_n I)_{n\in\mathbb{N}^*}$ d'idéaux strictement croissante, absurde.
- D'après le lemme précédent, il suffit maintenant de montrer que si $p \in A$ est irréductible alors l'idéal pA est premier. Il suffit pour cela de montrer qu'il est maximal. Soit I un idéal de A contenant pA. Comme A est principal, on peut écrire $I = xA$, de sorte qu'il existe $y \in A$ tel que $p = xy$. Comme p est irréductible, x est inversible ou y est inversible, donc $I = A$ ou $I = pA$. Comme p n'est pas inversible, on a $pA \neq A$ donc l'idéal pA est maximal.

■

Théorème 1.5.3: On suppose que $(A, +, \times)$ est principal. Soit $(a_i)_{i\in I}$ une famille finie (non vide) d'éléments de A. Soient $d, m \in A$.

- d un générateur de l'idéal $\sum_{i\in I} a_i A$ ssi d est un PGCD des $(a_i)_{i\in I}$.
- m un générateur de l'idéal $\bigcap_{i\in I} a_i A$ ssi m est un PPCM des $(a_i)_{i\in I}$.

Preuve:

- Supposons que d est un générateur de $\sum_{i\in I} a_i A$. Pour tout $i \in I$, $a_i \in \sum_{i\in I} a_i A = dA$ donc $d|a_i$. De plus, soit b un diviseur des $(a_i)_{i\in I}$. Alors pour tout $i \in I$, $a_i A \subseteq bA$, donc $dA = \sum_{i\in I} a_i A \subseteq bA$ et $b|a$. Ainsi d est un PGCD des $(a_i)_{i\in I}$.
- Réciproquement, supposons que d est un PGCD des $(a_i)_{i\in I}$ et montrons que $\sum_{i\in I} a_i A = dA$. Soit $x = \sum_{i\in I} a_i x_i \in \sum_{i\in I} a_i A$, alors $d|x$ donc $x \in dA$. Réciproquement, soit x un générateur de l'idéal $\sum_{i\in I} a_i A$. Alors x divise tous les a_i, donc $x|d$ i.e. $dA \subseteq xA = \sum_{i\in I} a_i A$.
- Supposons que m est un générateur de $\bigcap_{i\in I} a_i A$. Alors m est un multiple de tous les a_i. De plus, soit b un multiple des $(a_i)_{i\in I}$. Alors pour tout $i \in I$, $bA \subseteq a_i A$, donc $bA \subseteq \bigcap_{i\in I} a_i A = ma$ et $m|b$. Ainsi m est un PPCM des $(a_i)_{i\in I}$.
- Réciproquement, supposons que m est un PPCM des $(a_i)_{i\in I}$ et montrons que $\bigcap_{i\in I} a_i A = mA$. Soit $x \in \bigcap_{i\in I} a_i A$, alors tous les a_i divisent x, donc $m|x$ et $x \in mA$. Réciproquement, $m \in \bigcap_{i\in I} a_i A$ donc $mA \subseteq \bigcap_{i\in I} a_i A$.

■

Théorème 1.5.4 (de Bézout) : On suppose que $(A, +, \times)$ est principal. Soit $(a_i)_{i\in I}$ une famille finie (non vide) d'éléments de A.
- Soit d un PGCD des $(a_i)_{i\in I}$. Alors il existe $(u_i)_{i\in I} \in A^I$ telle que $\sum_{i\in I} u_i a_i = d$.
- Alors les $(a_i)_{i\in I}$ sont premiers entre eux ssi il existe $(u_i)_{i\in I} \in A^I$ telle que $\sum_{i\in I} u_i a_i = 1$.

Preuve :
- D'après le théorème précédent, d est un générateur de l'idéal $\sum_{i\in I} a_i A$. En particulier, $d \in \sum_{i\in I} a_i A$, d'où le résultat.
- Le sens direct découle immédiatement du point précédent. Réciproquement, supposons qu'il existe $(u_i)_{i\in I} \in A^I$ telle que $\sum_{i\in I} u_i a_i = 1$. Soit d un PGCD des $(a_i)_{i\in I}$, alors $d|1$ donc d est inversible. Du coup 1 est un PGCD des $(a_i)_{i\in I}$, qui sont donc premiers entre eux.

■

Définition 1.5.6 : On dit que l'anneau $(A, +, \times)$ est euclidien ssi il est unitaire, intègre, commutatif et muni d'un stathme euclidien, i.e. il existe une fonction $\varphi : \mathbb{N} \setminus \{0\} \to \mathbb{N}$ telle que :
- pour tous $a, b \in A \setminus \{0\}$, $\varphi(ab) \geqslant \varphi(a)$;
- pour tous $a, b \in A$ avec $b \neq 0$, il existe $q, r \in A$ tels que $a = bq + r$ et $\varphi(r) < \varphi(b)$ si $r \neq 0$.

On dit que q est un quotient et r est un reste de la division euclidienne de a par b.

Théorème 1.5.5 : Tout anneau euclidien est principal.

Preuve : Soit A un anneau euclidien. Soit donc $\varphi : A \setminus \{0\} \to \mathbb{N}$ un stathme euclidien. Soit I un idéal de A. Si $I = \{0\}$ alors $I = 0A$. Sinon, on dispose de $x \in I \setminus \{0\}$ tel que $\varphi(x)$ soit minimal. Montrons que $I = xA$. Soit $a \in I$. On écrit $a = xq + r$ avec $\varphi(r) < \varphi(b)$ si $r \neq 0$. Comme $a \in I$ et $x \in I$, on a $r \in I$. Si $r \neq 0$ alors $\varphi(r) < \varphi(x)$, ce qui est impossible par

minimalité de $\varphi(x)$. Ainsi $r = 0$, donc $a = xq \in xA$. Finalement $I \subseteq xA$ et l'inclusion réciproque est claire. ■

Remarque 1.5.6: Dans un anneau euclidien, on dispose d'un moyen efficace pour trouver un PGCD de deux éléments non nuls a et b (il s'agit de l'algorithme d'Euclide). On écrit la division euclidienne de a par b : $a = bq + r$. Si $r = 0$ alors a est un PGCD de a et b. Sinon, tout PGCD de b et r est un PGCD de a et b. On répète le processus et comme $\varphi(r) < \varphi(b)$, il va finir par s'arrêter. On peut ensuite utiliser les calculs effectuer pour trouver $u, v \in A$ tels que $au + bv = d$ où d est le PGCD de a et b obtenu.

Exercice 1.5.1: Dans $\mathbb{Z}$, montrons que 111 et 47 sont premiers entre eux, et déterminons deux entiers u et v tels que $47u + 111v = 1$. On écrit :
- $111 = 2 \times 47 + 17$
- $47 = 2 \times 17 + 13$
- $17 = 1 \times 13 + 4$
- $13 = 3 \times 4 + 1$

donc 111 et 47 sont premiers entre eux. Ensuite, on remonte les calculs :

$$\begin{aligned} 1 &= 13 - 3 \times 4 \\ &= 13 - 3(17 - 1 \times 13) = 4 \times 13 - 3 \times 17 \\ &= 4(47 - 2 \times 17) - 3 \times 17 = 4 \times 47 - 11 \times 17 \\ &= 4 \times 47 - 11 \times (111 - 2 \times 47) = 26 \times 47 - 11 \times 111 \end{aligned}$$

donc $u = 26$ et $v = -11$ conviennent.

Lemme 1.5.7 : Soit A un anneau euclidien (non trivial) muni d'un stathme φ. Soit $\alpha = \min\{\varphi(a); a \in A \setminus \{0\}\}$. Alors les éléments de A inversibles sont exactement les $a \neq 0$ tels que $\varphi(a) = \alpha$.

Preuve:
- Soit a un élément de A inversible. Alors $a \neq 0$ et $\forall b \in A \setminus \{0\}, \varphi(b) = \varphi(b \times 1) \geqslant \varphi(1) = \varphi(aa^{-1}) \geqslant \varphi(a)$ donc $\varphi(a) = \alpha$.
- Réciproquement, soit $a \in A \setminus \{0\}$ tel que $\varphi(a) = \alpha$. On écrit la division euclidienne de 1 par a : $1 = aq + r$ avec $r = 0$ ou $\varphi(r) < \varphi(a)$. Par minimalité de $\varphi(a)$, on a nécessairement $r = 0$, donc $1 = aq$ et a est inversible.

■

Exercice 1.5.2 (⋆ ⋆): Soit $\mathbb{Z}[i] = \{x + iy; x, y \in \mathbb{Z}\}$ l'ensemble des entiers de Gauss.
1) Montrer que $\forall z \in \mathbb{C}, \exists z_0 \in \mathbb{Z}[i], |z - z_0| < 1$.
2) En déduire que $(\mathbb{Z}[i], +, \times)$ est un anneau euclidien.
3) Quels sont les éléments inversibles de $\mathbb{Z}[i]$?
4) Y a-t-il unicité du quotient et du reste de la division euclidienne ?

Solution:
1) Soient $z \in \mathbb{C}$, puis $a = \Re(z)$ et $b = \Im(z)$. Notons a_0 et b_0 les entiers les plus proches de a et b respectivement, de sorte que $|a - a_0| \leqslant \frac{1}{2}$ et $|b - b_0| \leqslant \frac{1}{2}$. Soit $z_0 = a_0 + ib_0 \in \mathbb{Z}[i]$, alors $|z - z_0|^2 = (a - a_0)^2 + (b - b_0)^2 \leqslant \frac{1}{2}$ donc $|z - z_0| \leqslant \frac{1}{\sqrt{2}} < 1$.

2) Déjà, $\mathbb{Z}[i]$ est clairement un sous-anneau de $\mathbb{C}$. C'est donc un anneau unitaire commutatif intègre. On va montrer qu'il s'agit d'un anneau euclidien pour le stathme $z \mapsto |z|^2$ (qui est bien à valeurs dans $\mathbb{N}$, contrairement à $z \mapsto |z|$).
   - Soient $z, z' \in \mathbb{Z}[i] \setminus \{0\}$, alors $\varphi(zz') = |zz'|^2 \geqslant |z| = \varphi(z)$ car $|z| \geqslant 1$.
   - Soient $a, b \in \mathbb{Z}[i]$ avec $b \neq 0$. D'après la question précédente, on dispose de $q \in \mathbb{Z}[i]$ tel que $|\frac{a}{b} - q| < 1$. On pose $r = a - bq$ et on a alors si $r \neq 0$, $|r|^2 = |b|^2 \ |\frac{a}{b} - q \ |^2 < |b|^2$.
3) Les éléments inversibles de $\mathbb{Z}[i]$ sont les éléments non nuls de stathme minimal. Il s'agit donc de $\{-1, 1, -i, i\}$.
4) Non, par exemple $1 + i = 2 \times 1 + (i - 1) = 2 \times i + (1 - i)$ avec $|i - 1|^2 = |1 - i|^2 < |2|^2$.

Lemme 1.5.8 : Soit A un anneau euclidien muni d'un stathme φ vérifiant de plus $\forall x, y \in A \setminus \{0\}, x \neq y \implies \varphi(x - y) \leqslant \max(\varphi(x), \varphi(y))$. Alors il y a unicité du quotient et du reste de la division euclidienne.

Preuve : Soient $a \in A$ et $b \in B \setminus \{0\}$. On suppose que l'on dispose de deux divisions euclidiennes $a = bq + r = bq' + r'$ avec $r = 0$ ou $\varphi(r) < \varphi(b)$ et $r' = 0$ ou $\varphi(r') < \varphi(b)$. On a $b(q - q') + (r - r') = 0$. On suppose par l'absurde que $q \neq q'$.
- Si r, r' et $r - r'$ sont non nuls alors $\varphi(r - r') \leqslant \max(\varphi(r), \varphi(r')) < \varphi(b) \leqslant \varphi(-b(q - q')) = \varphi(r - r')$, absurde.
- Si $r = 0$ et $r' \neq 0$ alors $\varphi(b) \leqslant \varphi(b(q - q')) = \varphi(r') < \varphi(b)$, absurde. Symétriquement, si $r' = 0$ et $r \neq 0$ on aboutit à une absurdité.

Du coup, on a $r = r'$ et donc $q = q'$ par intégrité de A. ■

1.6. Arithmétique dans $\mathbb{Z}$

Théorème 1.6.1 : L'anneau $(\mathbb{Z}, +, \times)$ est euclidien pour le stathme valeur absolue. De plus, y a unicité du quotient et du reste de la division euclidienne de $a \in \mathbb{Z}$ par $b \in \mathbb{Z} \setminus \{0\}$.

Preuve : Unicité : supposons qu'il existe $(q_1, r_1), (q_2, r_2) \in \mathbb{Z}^2$ tels que $a = bq_1 + r_1 = bq_2 + r_2$, $0 \leqslant r_1 < b$ et $0 \leqslant r_2 < b$. Alors $b(q_1 - q_2) = r_2 - r_1 \in [\![-b + 1, b - 1]\!]$, donc $|r_2 - r_1| = b|q_1 - q_2| < b$. On a nécessairement $|q_1 - q_2| = 0$, sinon $|q_1 - q_2| \geqslant 1$ et $b|q_1 - q_2| \geqslant b$. Ainsi $q_1 = q_2$, puis $r_1 = r_2$.
Existence : soit $S = \{a - bk; k \in \mathbb{Z} \wedge a - bk \geqslant 0\}$. Si $a \geqslant 0$ alors $a \in S$ et si $a < 0$ alors $a - ba \in S$. Ainsi S est une partie non vide de $\mathbb{N}$, et on peut considérer $r = \min(S)$. Soit $q \in \mathbb{Z}$ tel que $r = a - bq$. Si $r \geqslant b$ alors $a - b(q + 1) = r - b \geqslant 0$ donc $r - b \in S$ ce qui est absurde. Ainsi $0 \leqslant r < b$, d'où le résultat. ■

Remarque 1.6.1 : Dans $\mathbb{Z}$, les classes d'association sont les $\{-n, n\}$ où $n \in \mathbb{N}$. On choisit comme système de représentants irréductibles les nombres premiers, i.e. les nombres irréductibles positifs. On note $\mathbb{P}$ l'ensemble des nombres premiers. On appelle le PGCD (resp. PPCM) des $(a_i)_{i \in I}$ l'unique PGCD (resp. PPCM) des $(a_i)_{i \in I}$ qui est positif. On le note $\bigwedge_{i \in I} a_i$ (resp. $\bigvee_{i \in I} a_i$).

Lemme 1.6.1 : Soient $a, b \in \mathbb{Z}$ avec $b \neq 0$ et $a|b$. Alors $|a| \leqslant |b|$.

Preuve : Facile ■

Théorème 1.6.2 : Il existe une infinité de nombre premiers.

Preuve : Supposons par l'absurde qu'il n'existe qu'un nombre fini de nombres premiers $p_1, ..., p_n$. Soit $N = p_1...p_n + 1$. Comme $\mathbb{Z}$ est factoriel et que N n'est pas inversible, N admet un diviseur premier p_{i_0}. Mais alors $p_{i_0} \mid N - p_1...p_n = 1$, absurde. ■

Remarque 1.6.2 : Voir l'Exercice 1.6.7, l'Exercice 1.6.22 et l'Exercice 2.2.1 pour d'autres preuves du théorème.

Exercice 1.6.1 (⋆ ⋆) :
1) Montrer que l'ensemble des nombres premiers congrus à 3 modulo 4 est infini.
2) Montrer que l'ensemble des nombres premiers congrus à 5 modulo 6 est infini.

Remarque 1.6.3 : Ces résultats sont des cas particuliers du théorème de la progression arithmétique, démontré par Dirichlet en 1838 : si a et b sont premiers entre eux alors il existe une infinité de nombres premiers congrus à a modulo b. D'après Jacobi, sa démonstration « atteint les sommets de la perspicacité humaine ». Voir l'Exercice 3.3.3 pour un autre cas particulier du théorème de Dirichlet.

Solution :
1) Supposons que l'ensemble des nombres premiers congrus à 3 modulo 4 est fini, on le note $P_3 = \{p_1, ..., p_n\}$. Posons $N = 4p_1...p_n - 1$. Alors N possède un diviseur premier $p_i \in P_3$.

En effet, supposons que ce n'est pas le cas. Comme N est impair, tous ses diviseurs premiers seraient congrus à 1 modulo 4, donc N serait congru à 1 modulo 4, ce qui est absurde.

Or p_i divise $p_1...p_n$, donc divise $4p_1...p_n - N = 1$, ce qui est absurde.

1) Supposons que l'ensemble des nombres premiers congrus à 5 modulo 6 est fini, on le note $P_5 = \{p_1, ..., p_n\}$. Posons $N = 6p_1...p_n - 1$. Alors N possède un diviseur premier $p_i \in P_5$.

   En effet, supposons que ce n'est pas le cas. Comme N est impair et non divisible par 3, tous ses diviseurs premiers seraient congrus à 1 modulo 6, donc N serait congru à 1 modulo 6, ce qui est absurde.

   Or p_i divise $p_1...p_n$, donc divise $6p_1...p_n - N = 1$, ce qui est absurde.

Définition 1.6.1 : Soit $n \in \mathbb{N}$. Puisque $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$, on peut considérer l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$. Si $a \in \mathbb{Z}$, on note $a \bmod n$ (ou $\overline{a}$ lorsqu'il n'y a pas d'ambiguïté) la classe de a dans $\mathbb{Z}/n\mathbb{Z}$. Si $a, b \in \mathbb{Z}$, on dit que a et b sont congrus modulo n et on note $a \equiv b[n]$ ssi $a \bmod n = b \bmod n$.

Remarque 1.6.4 :
- $a \equiv b[n] \iff n|a - b$
- Si $a \equiv b[n]$ et $c \equiv d[n]$ alors $a + c \equiv b + d[n]$ et $ac \equiv bd[n]$.

Lemme 1.6.2 : Soit $n \in \mathbb{N}$.
- Si $n = 0$ alors $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}$.

- Si $n = 1$ alors $\mathbb{Z}/n\mathbb{Z}$ est l'anneau trivial.
- Si $n \geqslant 2$ alors $\mathbb{Z}/n\mathbb{Z}$ est de cardinal n et pour toute suite de n entiers consécutifs $k, k+1, ..., k+n-1$, on a $\mathbb{Z}/n\mathbb{Z} = \left\{\overline{k}, \overline{k+1}, ..., \overline{k+n-1}\right\}$.

Preuve: Laborieux mais facile. ■

Lemme 1.6.3: Soient $n \geqslant 2$ et $k \in \mathbb{Z}$. Alors $\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ ssi $k \wedge n = 1$.

Preuve: D'après le théorème de Bézout,

$$\begin{aligned} \overline{k} \text{ est inversible dans } \mathbb{Z}/n\mathbb{Z} &\iff \exists u \in \mathbb{Z}, \overline{k}\overline{u} = \overline{1} \\ &\iff \exists u, v \in \mathbb{Z}, ku + nv = 1 \\ &\iff k \wedge n = 1 \end{aligned}$$

■

Théorème 1.6.3 (chinois): Soient $n_1, ..., n_k$ des entiers deux à deux premiers entre eux. Alors l'application

$$\begin{cases} \mathbb{Z}/n_1...n_k\mathbb{Z} & \to \mathbb{Z}/n_1\mathbb{Z} \times ... \times \mathbb{Z}/n_k\mathbb{Z} \\ x \bmod n_1...n_k & \mapsto (x \bmod n_1, ..., x \bmod n_k) \end{cases}$$

est un isomorphisme d'anneaux.

Preuve: Comme les $n_1, ..., n_k$ sont deux à deux premiers entre eux, on a pour tous $i \neq j$, $n_i\mathbb{Z} + n_j\mathbb{Z} = \mathbb{Z}$ et $n_1...n_k\mathbb{Z} = n_1\mathbb{Z} \cap ... \cap n_k\mathbb{Z}$, donc le résultat découle immédiatement du théorème chinois général. ■

Définition 1.6.2: Soit $n \geqslant 2$. On pose $\varphi(n)$ le cardinal du groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$. La fonction φ ainsi définie s'appelle l'indicatrice d'Euler.

Remarque 1.6.5: D'après le lemme précédent, $\varphi(n) = |\{k \in [\![1, n]\!], k \wedge n = 1\}|$.

Lemme 1.6.4:
- Soient $p \in \mathbb{P}$ et $\alpha \in \mathbb{N}^*$. Alors $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.
- Soient $m, n \geqslant 2$ des entiers premiers entre eux. Alors $\varphi(mn) = \varphi(m)\varphi(n)$.
- Soit $n \geqslant 2$. On écrit $n = p_1^{\alpha_1}...p_k^{\alpha_k}$ sa décomposition en facteurs premiers. Alors $\varphi(n) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1)$

Preuve:
- L'ensemble des nombres de $[\![1, p^\alpha]\!]$ non premiers avec p est l'ensemble des multiples de k compris entre 1 et p^α. Il y en a $p^{\alpha-1}$: $p, 2p, ..., p^{\alpha-1}p$. Du coup $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.
- D'après le théorème chinois,

$$\varphi : \begin{cases} \mathbb{Z}/nm\mathbb{Z} & \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ x \bmod nm & \mapsto (x \bmod n, x \bmod m) \end{cases}$$

est un isomorphisme. De plus on voit que la restriction $\tilde{\varphi} : G_{nm} \to G_n \times G_m$, où G_k désigne le groupe des inversibles de $\mathbb{Z}/k\mathbb{Z}$, est toujours bijective. Du coup $\varphi(nm) = |G_{nm}| = |G_n| \times |G_m| = \varphi(n)\varphi(m)$.

- Trivial en utilisant les deux points précédents.

■

Exercice 1.6.2 (⋆): Soit $n \geqslant 2$.
1) Pour tout diviseur d de n, on pose $E_d = \{k \in [\![1, n]\!]; k \wedge n = d\}$. Déterminer $|E_d|$.
2) En déduire que $n = \sum_{d|n} \varphi(d)$ où φ est l'indicatrice d'Euler.

Solution:
1) On suppose $d > 0$ (sinon $|E_d| = 0$). Vu $d|n$, on écrit $n = dn'$ avec $n' \in \mathbb{N}$. Notons $F = \{k' \in [\![1, n']\!]; k' \wedge n' = 1\}$. Soit $\psi : E_d \to F$ définie par $\psi(k) = \frac{k}{d}$. ψ est bien définie car si $k \in E_d$ alors $k \wedge n = d$ donc $d|k$ et en posant $k' = \frac{k}{d}$, on a $(dk') \wedge (dn') = d$ donc par homogénéité, $k' \wedge n' = 1$ i.e. $k' \in F$. De plus ψ est clairement bijective. Ainsi $|E_d| = |F| = \varphi(n') = \varphi(\frac{n}{d})$.
2) On a $[\![1, n]\!] = \bigcup_{d|n} E_d$ et cette union est disjointe donc en passant au cardinal, $n = \sum_{d|n} \varphi(\frac{n}{d})$. Or en notant $D(n)$ l'ensemble des diviseurs positifs de n, l'application $f : D(n) \to D(n)$ définie par $d \mapsto \frac{n}{d}$ est bijective donc $n = \sum_{d|n} \varphi(d)$.

Lemme 1.6.5: Soient p un nombre premier et $k \in [\![1, p-1]\!]$. Alors $p|\binom{p}{k}$.

Preuve: Notons $a = p(p-1)...(p-k+1)$. On a $a = \binom{p}{k} k!$ donc a est divisible par $k!$ ainsi que par p. Or $p \wedge k! = 1$ car les facteurs premiers de $k!$ sont ceux de $1, 2, ..., k$ et ils sont donc $< p$. Ainsi $pk!|\ a$ donc $p|\binom{p}{k}$. ■

Exercice 1.6.3 (⋆):
1) Soient k et n deux entiers naturels non nuls premiers entre eux. Montrer que $n|\binom{n}{k}$.
2) Montrer que $\forall n \in \mathbb{N}^*, (n+1)|\ \binom{2n}{n}$.

Solution:
1) Si $n < k$ alors $n|\binom{n}{k} = 0$. Si $n = k$ alors $n = k = 1$ car $n \wedge k = 1$, donc $n|\binom{n}{k}$. Si $k < n$, on a $k\binom{n}{k} = n\binom{n-1}{k-1}$, or $n \wedge k = 1$ donc $n|\binom{n}{k}$.
2) On a $(n+1)\binom{2n}{n-1} = n\binom{2n}{n}$ donc $(n+1)|n\binom{2n}{n}$, mais $(n+1) \wedge n = 1$ donc $(n+1)|\binom{2n}{n}$.

Théorème 1.6.4 (morphisme de Frobenius): Soit A un anneau unitaire intègre commutatif de caractéristique $p \neq 0$. Alors $\varphi : \begin{cases} A \to A \\ x \mapsto x^p \end{cases}$ est un morphisme d'anneaux, dit morphisme de Frobenius.

Preuve: Comme A est commutatif, on a clairement $\forall x, y \in A, \varphi(xy) = \varphi(x)\varphi(y)$. Comme A est intègre, on sait que $p \in \mathbb{P}$. On en déduit que $\forall x, y \in A, \varphi(x+y) = \varphi(x) + \varphi(y)$ à l'aide du lemme précédent et de la formule du binôme de Newton. ■

Théorème 1.6.5 (petit théorème de Fermat) : Soient p un nombre premier et $a \in \mathbb{Z}$. Alors $a^p \equiv a[p]$. Si de plus p ne divise pas a alors $a^{p-1} \equiv 1[p]$.

Preuve : Le résultat est clair si $p|a$. On suppose que $p|a$ et on va montrer que $a^{p-1} \equiv 1[p]$, ce qui suffit pour conclure. Soit

$$\varphi : \begin{cases} (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times \\ \overline{k} \qquad\quad \mapsto \overline{ka} \end{cases}$$

Alors φ est bien définie et injective car $\overline{a}$ est inversible dans $\mathbb{Z}/p\mathbb{Z}$. Par égalité des cardinaux des ensembles de départ et d'arrivée de φ, φ est bijective, donc $\prod_{\overline{k}\in(\mathbb{Z}/p\mathbb{Z})^\times} \overline{k} = \prod_{\overline{k}\in(\mathbb{Z}/p\mathbb{Z})^\times} \varphi\left(\overline{k}\right)$, i.e. $(p-1)! \equiv a^{p-1}(p-1)![p]$, d'où le résultat puisque $(p-1)!$ est inversible modulo p. ■

Remarque 1.6.6 :

- On peut aussi montrer le petit théorème de Fermat par récurrence sur a en utilisant le fait que $p|\binom{p}{k}$ si $k \in [\![1, p-1]\!]$.
- Voir l'Exercice 2.1.2 pour une preuve du petit théorème de Fermat utilisant les actions de groupe.
- Le petit théorème de Fermat est aussi un cas particulier du théorème d'Euler (Théorème 2.2.2).

Exercice 1.6.4 (⋆ ⋆) : Soient $a \geqslant 2$ un entier et $p > 2$ un nombre premier ne divisant pas $a^2 - 1$. Soit $n = \frac{a^{2p}-1}{a^2-1}$. Montrer que n est pseudo-premier en base a, i.e. que n n'est pas premier mais que $a^{n-1} \equiv 1[n]$.

Solution :

- On a $n = \frac{a^p-1}{a-1} \times \frac{a^p+1}{a+1}$ avec $\frac{a^p-1}{a-1} = \sum_{k=0}^{p-1} a^k \in \mathbb{Z}$ et $\frac{a^p+1}{a+1} = \sum_{k=0}^{p-1} (-a)^k \in \mathbb{Z}$ car p est impair. De plus $\frac{a^p-1}{a-1} \geqslant 2$ et $\frac{a^p+1}{a+1} \geqslant 2$ donc n n'est pas premier.
- On a $a^{2p} = 1 + n(a^2-1) \equiv 1[n]$ donc il suffit de montrer que $2p \mid n-1$, i.e. $2|n-1$ et $p|n-1$.
  - On a $n - 1 = \sum_{k=1}^{p-1} a^{2k}$: il s'agit d'une somme d'un nombre pair de termes de même parité, donc $2|n-1$.
  - Par le petit théorème de Fermat, $a^{2p} \equiv a^2[p]$, donc $n(a^2-1) \equiv a^2 - 1[p]$. Ainsi $p|(n-1)(a^2-1)$, mais $p \wedge (a^2-1) = 1$ donc par le lemme de Gauss, $p|n-1$.

Exercice 1.6.5 (⋆ ⋆) :

1) Montrer que $\forall n \in \mathbb{N}, 5|(2^{3n+5} + 3^{n+1})$.
2) Montrer que $\forall n \in \mathbb{N}, 30|(n^5 - n)$.
3) Quel est le reste de la division euclidienne de $16^{2^{1000}}$ par 7 ?

Solution : (Pour chaque question, il y a énormément de façons de faire)

1) Soit $n \in \mathbb{N}$. Alors $2^{3n+5} = 8^n 2^5 \equiv 3^n \times 2[5]$, donc $2^{3n+5} + 3^{n+1} \equiv 3^n \times 2 + 3^n \times 3 \equiv 0[5]$.

2) Soit $n \in \mathbb{N}$. Alors $n^5 - n = n(n^4-1) = n(n^2-1)(n^2+1) = n(n-1)(n+1)(n^2+1)$. Parmi les entiers $n-1$, n et $n+1$, il y a toujours un multiple de 2 et un multiple de 3. De plus, $n^5 \equiv n[5]$ par le petit théorème de Fermat. Ainsi, $n^5 - n$ est divisible par 2, 3 et 5, donc par 30.
3) On a $2^{999} + 1 = 2^{999} - (-1)^{999} = (2-(-1))(1-2+...+2^{998})$ donc $2^{999} \equiv -1[3]$, puis $2^{1000} \equiv -2 \equiv 4[6]$. Soit donc $n \in \mathbb{N}$ tel que $2^{1000} = 6n+4$. Alors $16^{2^{1000}} = (16^n)^6 16^4 \equiv 1 \times 2^4 \equiv 2[7]$ par le petit théorème de Fermat.

Théorème 1.6.6 (de Wilson): Soit $p \geqslant 2$. Alors p est premier ssi $(p-1)! \equiv -1[p]$.

Preuve:
- Déjà, supposons $(p-1)! \equiv -1[p]$. Si p n'est pas premier, il admet un facteur premier $q \in [\![1, p-1]\!]$. On a $q|(p-1)!$ et $q|(p-1)!+1$, ce qui est absurde. Donc p est premier.
- Réciproquement, supposons que p est premier. Tous les entiers compris entre 1 et $p-1$ sont premiers avec p, donc sont inversibles modulo p. De plus, un entier $a \in [\![0, p-1]\!]$ est son propre inverse modulo p lorsque $a^2 \equiv 1[p] \iff p|a^2-1 = (a-1)(a+1) \iff p|(a-1) \vee p|(a+1) \iff a = 1 \vee a = p-1$. Ainsi, parmi les nombres $1, 2, ..., p-1$, il y en a 2 qui sont leur propre inverse (ils sont bien distincts car $p > 2$), et on peut regrouper tous les autres en des paires dont le produit vaut 1. Ainsi $(p-1)! \equiv 1 \times 1 \times ... \times 1 \times (p-1) \equiv -1[p]$.

■

*Exercice 1.6.6 (*formule de Legendre $\star\star$*)*:
1) Soient n un entier supérieur ou égal à 2 et p un nombre premier. Montrer que

$$v_p(n!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

(où $v_p(n!)$ est l'exposant de p dans la décomposition en facteurs premiers de $n!$).
2) Par combien de 0 se termine l'écriture en base 10 de 1000! ?

Solution:
1) Pour tout $j \in [\![1, n]\!]$, le nombre de multiples de j compris entre 1 et n vaut $\left\lfloor \frac{n}{j} \right\rfloor$. Du coup, pour tout $k \in \mathbb{N}^*$, le nombre de nombres compris entre 1 et n qui sont multiples de p^k mais pas de p^{k+1} vaut $\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor$, et chacun de ces nombres a une valuation p-adique de k. Du coup

$$v_p(n!) = \sum_{k=1}^{\infty} k\left(\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor \right) = \sum_{k=1}^{\infty} k \left\lfloor \frac{n}{p^k} \right\rfloor - \sum_{k=2}^{\infty} (k-1) \left\lfloor \frac{n}{p^k} \right\rfloor = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

2) Le nombre de 0 par lequel se termine l'écriture en base 10 de 1000! vaut $\min(v_2(1000!), v_5(1000!))$. D'après la formule de Legendre, ce nombre est égal à $v_5(1000!)$ car pour tout k, $\left\lfloor \frac{1000}{5^k} \right\rfloor \leqslant \left\lfloor \frac{1000}{2^k} \right\rfloor$. On a $v_5(1000!) = \left\lfloor \frac{1000}{5} \right\rfloor + \left\lfloor \frac{1000}{25} \right\rfloor + \left\lfloor \frac{1000}{125} \right\rfloor + \left\lfloor \frac{1000}{625} \right\rfloor = 200 + 40 + 8 + 1 = 249$. L'écriture en base 10 de 1000! se termine donc par 249 zéros.

*Exercice 1.6.7 (*nombres de Mersenne $\star\star$*)*:

1) Soient $a, n \geqslant 2$ deux entiers tels que $a^n - 1$ est premier. Montrer que $a = 2$ et que n est premier.
2) Pour tout nombre premier p, on note $M_p = 2^p - 1$ le nombre de Mersenne d'indice p. Soit p un nombre premier de la forme $4k + 3$ avec $k \in \mathbb{N}^*$.
   a) Montrer que $2^{\frac{p-1}{2}} \equiv (-1)^{k+1}[p]$. *Indication : trouver une expression de* $N := 2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!$ *modulo* p.
   b) Montrer que si $2p + 1$ est premier, alors M_p n'est pas premier.

Solution:

1) $a^n - 1$ est divisible par $a - 1$. Comme $a^n - 1$ est premier et $a^n - 1 \neq a - 1$, on en déduit $a - 1 = 1$ i.e. $a = 2$. Écrivons $n = pq$ où $p, q \in \mathbb{N}^*$. Alors $a^n - 1 = 2^n - 1 = (2^p)^q - 1$ est divisible par $2^p - 1$, donc $2^p - 1 = 1$ ou $2^p - 1 = 2^n - 1$ i.e. $p = 1$ ou $p = n$. n est donc premier.
2) a) On a $N = 2^{\frac{p-1}{2}}\left(1 \times 2 \times ... \times \frac{p-1}{2}\right) = 2 \times 4 \times ... \times (p-1) = 2 \times 4 \times ... \times (4k+2)$. Or $2k + 2 \equiv -2k - 1[p]; 2k + 4 \equiv -2k + 1[p]; ...; 4k + 2 \equiv -1[p]$. Donc $N \equiv (2 \times 4 \times ... \times 2k) \times ((-2k-1)(-2k+1)...(-1)) \equiv (-1)^{k+1}(2k+1)!$. Ainsi $2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! \equiv (-1)^{k+1}\left(\frac{p-1}{2}\right)![p]$. Comme $\left(\frac{p-1}{2}\right)!$ est premier avec p, on en déduit le résultat.
   b) Supposons que $2p + 1$ est premier. On a $2p + 1 = 2(4k + 3) + 1 = 4(2k + 1) + 1$. En appliquant le résultat de la question précédente à $2p + 1$ (qui est premier et de la forme $4k' + 1$), on obtient $2^p = 2^{\frac{2p+1-1}{1}} \equiv (-1)^{2k+2} \equiv 1[p]$, donc M_p est divisible par p et n'est donc pas premier.

Exercice 1.6.8 ($\star$): Trouver tous les entiers $a, b, c \in \mathbb{N}^*$ tels que

$$\begin{cases} a \vee b = 42 \\ a \wedge c = 3 \\ a + b + c = 29 \end{cases}$$

Solution: Soient $a, b, c \in \mathbb{N}^*$ vérifiant le système.

Déjà, a et c sont divisibles par 3, donc b ne l'est pas car sinon, on aurait $3|a + b + c = 29$. Puisque $a \vee b = 42 = 2 \times 3 \times 7$, les facteurs premiers possibles de b sont 2 et 7, et ils ont une valuation d'au plus 1, donc $b \in \{1, 2, 7, 14\}$. De plus a est divisible par 3, et ses autres facteurs premiers possibles sont 2 et 7, qui ont une valuation d'au plus 1, donc $a \in \{3, 6, 21\}$.

- Si $a = 3$ alors la condition $a \vee b = 42$ impose $b = 14$, et on obtient le triplet $(3, 14, 12)$ qui est bien solution.
- Si $a = 6$ alors $b \in \{7, 14\}$. Si $b = 7$ alors $c = 16$, mais alors on n'a pas $a \wedge c = 3$. Si $b = 14$ on obtient le triplet $(6, 14, 9)$ qui est bien solution.
- Si $a = 21$ alors $c \leqslant 8$, et c est un multiple de 3 donc $c \in \{3, 6\}$. Si $c = 3$ alors $b = 5$, mais alors on n'a pas $a \vee b = 42$. Si $c = 6$ on obtient le triplet $(21, 2, 6)$ qui est bien solution.

Finalement, le système admet trois solutions, à savoir $(a, b, c) \in \{(3, 14, 12), (6, 14, 9), (21, 2, 6)\}$.

Exercice 1.6.9 (⋆ ⋆): Montrer qu'il n'existe pas de polynôme $P \in \mathbb{Z}[X]$ non constant tel que $P(n)$ soit premier pour tout entier n supérieur à un certain rang N.

Solution: Supposons qu'il existe un $P \in \mathbb{Z}[X]$ non constant tel que $P(n)$ soit premier pour tout entier n supérieur à un certain rang N. Notons $p = P(N)$, qui est un nombre premier. Alors pour tous $j, k \in \mathbb{N}$, $(N + kp)^j \equiv N[p]$, donc $P(N + kp) \equiv P(N) \equiv 0[p]$. Puisque $P(N + kp)$ est premier, on a $P(N + kp) = p$ pour tout $k \in \mathbb{N}$. Le polynôme $P - p$ a une infinité de racines, ce qui est absurde car P n'est pas constant.

Exercice 1.6.10 (⋆): Soit $(F_n)_{n\in\mathbb{N}}$ la suite de Fibonacci, définie par $F_0 = 0$, $F_1 = 1$ et $\forall n \in \mathbb{N}^*, F_{n+2} = F_{n+1} + F_n$. Montrer que pour tout $n \in \mathbb{N}^*$, F_n et F_{n+1} sont premiers entre eux.

Solution:

- *Première méthode :* On montre le résultat par récurrence. $F_1 = F_2 = 1$ donc le résultat est vrai pour $n = 1$. Soit $n \in \mathbb{N}^*$. Supposons $F_n \wedge F_{n+1} = 1$. Par le théorème de Bézout, soient $a, b \in \mathbb{Z}$ tels que $aF_n + bF_{n+1} = 1$. Alors $a(F_{n+2} - F_{n+1}) + bF_{n+1} = 1$ i.e. $aF_{n+2} + (b - a)F_{n+1} = 1$ donc à nouveau par le théorème de Bézout, $F_{n+2} \wedge F_{n+1} = 1$.
- *Deuxième méthode* : Soit $n \in \mathbb{N}^*$ Si $d|F_n$ et $d|F_{n+1}$ alors $d|F_n + F_{n+1} = F_{n+2}$. Réciproquement, si $d|F_{n+1}$ et $d|F_{n+2}$ alors $d|F_{n+2} - F_{n+1} = F_n$. Ainsi F_n et F_{n+1} d'une part et F_{n+1} et F_{n+2} d'autre part ont les mêmes diviseurs communs. En particulier, $F_n \wedge F_{n+1} = F_{n+1} \wedge F_{n+2}$ puis on en déduit le résultat par une récurrence triviale.

Exercice 1.6.11 (⋆): Pour tout $n \in \mathbb{N}^*$, on pose $\left(1 + \sqrt{2}\right)^n = a_n + b_n\sqrt{2}$ où $a_n, b_n \in \mathbb{N}^*$. Montrer que $a_n \wedge b_n = 1$.

Solution: L'existence de (a_n) et (b_n) vient du binôme de Newton, et leur unicité vient de l'irrationalité de $\sqrt{2}$.

- *Première méthode :* soit $n \in \mathbb{N}^*$. Par la formule du binôme de Newton, on voit que $\left(1 - \sqrt{2}\right)^n = a_n - b_n\sqrt{2}$, donc $(-1)^n = \left(1 + \sqrt{2}\right)^n\left(1 - \sqrt{2}\right)^n = \left(a_n + b_n\sqrt{2}\right)\left(a_n - b_n\sqrt{2}\right) = a_n^2 - 2b_n^2$, donc $((-1)^n a_n)a_n + \left(2(-1)^{n+1}b_n\right)b_n = 1$. Par le théorème de Bézout, on en déduit que $a_n \wedge b_n = 1$.
- *Deuxième méthode :* Soit $n \in \mathbb{N}^*$, alors $a_{n+1} + b_{n+1}\sqrt{2} = \left(1 + \sqrt{2}\right)^{n+1} = \left(1 + \sqrt{2}\right)\left(a_n + b_n\sqrt{2}\right) = (a_n + 2b_n) + (a_n + b_n)\sqrt{2}$ donc $a_{n+1} = a_n + 2b_n$ et $b_{n+1} = a_n + b_n$.

  Montrons par récurrence que $a_n \wedge b_n = 1$. On a $a_1 = b_1 = 1$ donc le résultat est vrai pour $n = 1$. Soit $n \in \mathbb{N}^*$, supposons le résultat au rang n. Par le théorème de Bézout, soient $u, v \in \mathbb{Z}$ tels que $a_n u + b_n v = 1$. Alors $(v - u)a_{n+1} + (2u + v)b_{n+1} = 1$ donc à nouveau par le théorème de Bézout, $a_{n+1} \wedge b_{n+1} = 1$, ce qui achève la récurrence.

*Exercice 1.6.12 (*nombres de Fermat ⋆ ⋆ ♥*)*:

1) Soit $n \in \mathbb{N}^*$ tel que $2^n + 1$ est premier. Montrer que n est une puissance de 2.
2) Pour tout $n \in \mathbb{N}$, on pose $F_n = 2^{2^n} + 1$ le n-ième nombre de Fermat. Montrer que les nombres de Fermat sont deux à deux premiers entre eux.

3) En déduire une démonstration de l'existence d'une infinité de nombres premiers.

Remarque 1.6.7: Pierre de Fermat conjecture en 1640 que ces nombres sont tous premiers. Cette conjecture ce révéla fausse : F_5 est composé, de même que tous les suivants jusqu'à F_{32}. Pour certains d'entre eux, cela a été démontré grâce au test de Pépin. On ne sait pas à l'heure actuelle si les nombres à partir de F_{33} sont premiers. Les nombres de Fermat interviennent notamment dans le théorème de Gauss-Wantzel : un polynôme régulier à n côtés peut être construit à la règle et au compas si et seulement si n est le produit d'une puissance de 2 et de nombres de Fermat premiers distincts.

Solution:
1) On écrit $n = mk$ où $m = 2^{v_2(n)}$ et k est donc un entier impair. Alors $2^n + 1 = (2^m)^k - (-1)^k$, donc $2^n + 1$ est divisible par $2^m - (-1) = 2^m + 1$. Comme $2^n + 1$ est premier et que $2^m + 1 > 1$, on en déduit que $2^m + 1 = 2^n + 1$, donc $n = m = 2^{v_2(n)}$.
2) Soient $n \in \mathbb{N}$ et $k \in \mathbb{N}^*$, montrons que F_n et F_{n+k} sont premiers entre eux. On a $F_{n+k} - 1 = 2^{2^{n+k}} = (F_n - 1)^{2^k} \equiv (-1)^{2^k} = 1[F_n]$ donc $F_n | F_{n+k} - 2$. En particulier, en notant $d = F_n \wedge F_{n+k}$, on a $d | F_{n+k}$ et $d | F_{n+k} - 2$, donc $d | 2$. Comme les F_n sont impairs, on en déduit $d = 1$, c'est à dire $F_n \wedge F_{n+k} = 1$.
3) Pour tout $n \in \mathbb{N}$, notons p_n un facteur premier de F_n. Puisque les F_n sont deux à deux premiers entre eux, les p_n sont deux à deux distincts, et il y en a une infinité.

*Exercice 1.6.13 (*nombres parfaits $\star\star\star$ ♥*)*:
1) a) Pour tout $n \in \mathbb{N}^*$, on pose $\sigma(n)$ la somme des diviseurs positifs de n. Exprimer $\sigma(n)$ en fonction des termes intervenant dans la décomposition en produit de facteurs premiers de n.
   b) Montrer que σ est multiplicative, c'est-à-dire que pour tous $m, n \in \mathbb{N}^*$ premiers entre eux, $\sigma(mn) = \sigma(m)\sigma(n)$.
2) a) On dit que $n \in \mathbb{N}^*$ est parfait si et seulement si $\sigma(n) = 2n$. Si $2^p - 1$ est un nombre premier, montrer que $2^{p-1}(2^p - 1)$ est un nombre parfait.
   b) Réciproquement, montrer que tout nombre parfait pair est de la forme $2^{p-1}(2^p - 1)$ où $2^p - 1$ est premier.
3) a) Montrer que si n est un nombre parfait impair, alors il est de la forme $n = p^{1+4\alpha}Q^2$ où p est un nombre premier congru à 1 modulo 4, $\alpha \in \mathbb{N}$, $Q \in \mathbb{N}^*$ et $p \wedge Q = 1$ (théorème d'Euler). *Indication : à partir de la décomposition en produit de facteurs premiers* $n = \prod p_i^{\alpha_i}$, *étudier la valeur de* $\sigma\left(p_i^{\alpha_i}\right)$ *modulo* 4.
   b) Montrer qu'un nombre parfait impair a au moins trois facteurs premiers distincts.

Remarque :A l'heure actuelle, on ne sait pas s'il existe un nombre parfait impair. On sait que s'il en existe un alors il a au moins 1500 *chiffres décimaux et au moins* 10 *facteurs premiers distincts dont le plus grand est supérieur à* 10^8.

Solution:
1)
2) Soit $n \in \mathbb{N}^*$. On écrit $n = \prod_{i=1}^k p_i^{\alpha_i}$ où les p_i sont des nombres premiers distincts et $\alpha_i \in \mathbb{N}^*$. Les diviseurs positifs de n sont les nombres de la forme $\prod_{i=1}^k p_i^{\beta_i}$ où $0 \leqslant \beta_i \leqslant \alpha_i$ pour tout i. Du coup, $\sigma(n) = \sum_{\beta_1=0}^{\alpha_1} \dots \sum_{\beta_k=0}^{\alpha_k} \prod_{i=1}^k p_i^{\beta_i}$.

3) Soient $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ et $m = \prod_{j=1}^{l} q_j^{\beta_j}$ des entiers premiers entre eux. Pour tous i et j, on a donc $p_i \neq q_j$, donc la décomposition en facteurs premiers de mn est $\left(\prod_{i=1}^{k} p_i^{\alpha_i}\right)\left(\prod_{j=1}^{l} q_j^{\beta_j}\right)$. On a donc

$$\begin{aligned}\sigma(mn) &= \sum_{\gamma_1=0}^{\alpha_1} \dots \sum_{\gamma_k=0}^{\alpha_k} \sum_{\delta_1=0}^{\beta_k} \dots \sum_{\delta_l=0}^{\beta_l} \left(\prod_{i=1}^{k} p_i^{\gamma_i}\right)\left(\prod_{i=1}^{l} q_i^{\delta_i}\right) \\ &= \left(\sum_{\gamma_1=0}^{\alpha_1} \dots \sum_{\gamma_k=0}^{\alpha_k} \prod_{i=1}^{k} p_i^{\gamma_i}\right)\left(\sum_{\delta_1=0}^{\beta_1} \dots \sum_{\delta_l=0}^{\beta_l} \prod_{i=1}^{l} q_i^{\delta_i}\right) = \sigma(m)\sigma(n)\end{aligned}$$

4) a) Soit $2^p - 1$ un nombre premier (donc $p \geqslant 2$). Alors 2^{p-1} et $2^p - 1$ sont premiers entre eux car le seul diviseur premier de 2^{p-1} est 2, qui ne divise pas $2^p - 1$. De plus $\sigma(2^{p-1}) = 1 + 2 + \dots + 2^{p-1} = 2^p - 1$ et $\sigma(2^p - 1) = 1 + (2^p - 1) = 2^p$ car $2^p - 1$ est premier. D'après la question précédente, on en déduit $\sigma(2^{p-1}(2^p - 1)) = \sigma(2^{p-1})\sigma(2^p - 1) = (2^p - 1)2^p = 2 \times 2^{p-1}(2^p - 1)$ donc $2^{p-1}(2^p - 1)$ est parfait.

   b) Soit n un nombre parfait pair, on écrit $n = 2^{p-1}k$ où $p \geqslant 2$ et k est impair. D'une part, $\sigma(n) = 2n = 2^p k$. D'autre part, comme 2^{p-1} et k sont premiers entre eux, on a $\sigma(n) = \sigma(2^{p-1})\sigma(k) = (2^p - 1)\sigma(k)$. Ainsi $2^p k = (2^p - 1)\sigma(k)$. Comme 2^p et $2^p - 1$ sont premiers entre eux, on en déduit que $2^p - 1 | k$. Soit donc $j \in \mathbb{N}^*$ tel que $k = (2^p - 1)j$. Supposons par l'absurde que $j > 1$. Alors k admet au moins 3 diviseurs distincts, à savoir 1, j et k, donc $\sigma(k) \geqslant 1 + j + k$. Mais d'autre part, on a $2^p(2^p - 1)j = (2^p - 1)\sigma(k)$ donc $\sigma(k) = 2^p j = k + j$, ce qui est absurde. Ainsi $j = 1$, donc $k = 2^p - 1$ et $n = 2^{p-1}(2^p - 1)$. De plus, on a vu que $\sigma(k) = k + 1$ donc $k = 2^p - 1$ est premier.

5) a) Soit $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ un nombre parfait impair. On a $\sigma(n) = 2n = \prod_{i=1}^{k} \sigma(p_i^{\alpha_i})$. On vérifie aisément que pour tout i,

$$\sigma(p_i^{\alpha_i}) = \sum_{k=0}^{\alpha_i} p_i^k \equiv \begin{cases} \alpha_i + 1 \text{ si } p_i \equiv 1[4] \\ 0 \quad \text{si } p_i \equiv 3[4] \text{ et } \alpha_i \text{ est impair} \\ 1 \quad \text{si } p_i \equiv 3[4] \text{ et } \alpha_i \text{ est pair} \end{cases}$$

   (modulo 4). Mais puisque n est impair, on a $2n \equiv 2[4]$. Il existe donc nécessairement un i_0 tel que $\alpha_{i_0} + 1 \equiv 2[4]$, i.e. $\alpha_{i_0} = 1 + 4\alpha$ où $\alpha \in \mathbb{N}$, et p_{i_0} est alors congru à 1 modulo 4. Tous les autres termes du produit $\prod_{i=1}^{k} \sigma(p_i^{\alpha_i})$ sont alors congrus à 1 ou 3 modulo 4, donc tous les autres α_i sont pairs. On a donc $n = p^{1+4\alpha}Q^2$ où $p = p_{i_0}$ est un nombre premier congru à 1 modulo 4, $\alpha \in \mathbb{N}$, $Q \in \mathbb{N}^*$ et $\alpha \wedge Q = 1$.

   b) Soit $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ un nombre parfait impair. Alors

$$2 = \frac{\sigma(n)}{n} = \prod_{i=1}^{k} \frac{\sigma(p_i^{\alpha_i})}{p_i^{\alpha_i}} = \prod_{i=1}^{k} \left(1 + \frac{1}{p_i} + \dots + \frac{1}{p_i^{\alpha_i}}\right) \leqslant \prod_{i=1}^{k} \frac{1}{1 - \frac{1}{p_i}}$$

   Si $k = 1$ alors $2 \leqslant \frac{1}{1-\frac{1}{p_1}} \leqslant \frac{3}{2}$ ce qui est absurde. Si $k = 2$ alors $2 \leqslant \left(\frac{1}{1-\frac{1}{p_1}}\right)\left(\frac{1}{1-\frac{1}{p_2}}\right) \leqslant \frac{3}{2} \times \frac{5}{4} = \frac{15}{8}$ ce qui est absurde. Ainsi $k \geqslant 3$, c'est-à-dire que n a au moins trois facteurs premiers distincts.

Exercice 1.6.14 (⋆): Soient $a, b \in \mathbb{N}^*$ avec $b \geqslant 2$ et $a \wedge b = 1$. Montrer que

$$\exists!(u_0, v_0) \in \mathbb{N}^2, \begin{cases} u_0 a - v_0 b = 1 \\ u_0 < b \\ v_0 < a \end{cases}$$

et exprimer en fonction de u_0 et v_0 tous les couples $(a, b) \in \mathbb{Z}$ tels que $ua - vb = 1$.

Solution : Par le théorème de Bézout, il existe $u_1, v_1 \in \mathbb{Z}$ tels que $u_1 a - v_1 b = 1$. Soient q et u_0 le quotient le reste de la division euclidienne de u_1 par b. $(bq + u_0)a - v_1 b = 1$, donc $u_0 a - v_0 b = 1$ où $v_0 = v_1 - qa$. De plus on a $0 \leqslant u_0 < b$ et $-1 \leqslant v_0 b = u_0 a - 1 < u_0 a \leqslant ba$, d'où $0 \leqslant v_0 < a$.

Soient maintenant $u, v \in \mathbb{Z}$ tels que $ua - vb = 1$, alors $(u_0 - u)a - (v_0 - v)b = 0$. Comme $a \wedge b = 1$, on en déduit $a | v_0 - v$ et $b | u_0 - u$. Soient donc $k, k' \in \mathbb{Z}$ tels que $v = v_0 + ka$ et $u = u_0 + k'b$. On voit alors que $ab(k - k') = 0$, donc $k = k'$. Ainsi $\exists k \in \mathbb{Z}, \begin{cases} u = u_0 + kb \\ v = v_0 + kb \end{cases}$. Réciproquement, si $\begin{cases} u = u_0 + kb \\ v = v_0 + kb \end{cases}$ où $k \in \mathbb{Z}$ alors $au - bv = 1$.

*Exercice 1.6.15 (*théorème de Liouville $\star\star$*)*:
1) Soit $p > 5$ un entier impair. Montrer que $(p-1)^2 \mid (p-1)!$.
2) Montrer que l'équation $(p-1)! + 1 = p^m$ d'inconnues $p > 5$ et $m \in \mathbb{N}^*$ n'a pas de solution.

Solution :
1) Comme $p > 5$, on a $2 < \frac{p-1}{2} < p - 1$ et comme p est impair, $\frac{p-1}{n}$ est un entier. Du coup $(p-1)^2 = 2\frac{p-1}{2}(p-1) \mid (p-1)!$.
2) Supposons que $(p-1)! + 1 = p^m$ avec $p > 5$ et $m \in \mathbb{N}^*$. Alors $(p-1)!$ est pair donc p^m est impair, et donc p est impair. D'après la question précédente, $(p-1)^2 \mid (p-1) \neq p^m - 1 = (p-1)\sum_{k=0}^{m-1} p^k$ donc $p - 1 | \sum_{k=0}^{m-1} p^k$. Mais d'autre part $\sum_{k=0}^{m-1} p^k \equiv \sum_{k=0}^{m-1} 1 = m[p-1]$ donc $m \equiv 0[p-1]$.

   Comme $m \geqslant 1$, on a $m \geqslant p - 1$. Du coup $p^m = p^{p-1} > (p-1)! + 1 = p^m$, absurde. L'équation proposée n'a donc pas de solution.

Exercice 1.6.16 ($\star$): Montrer qu'un entier congru à 7 modulo 8 ne peut pas être la somme de trois carrés parfaits.

Solution : Après une vérification fastidieuse, on voit qu'un carré parfait est toujours congru à 0, 1 ou 4 modulo 8. La somme de trois carrés parfaits n'est donc jamais congrue à 7 modulo 8.

Exercice 1.6.17 ($\star\star$ ♥): On veut résoudre dans $\mathbb{Z}^3$ l'équation $x^2 + y^2 = z^2$. Soit (x, y, z) une solution de cette équation (on dit que (x, y, z) est un triplet pythagoricien).
1) Montrer que l'on peut se ramener au cas où x, y et z sont premiers entre eux, et que dans ce cas, x, y et z sont de plus premiers entre eux deux à deux.
2) On suppose maintenant que x, y et z sont deux à deux premiers entre eux. Montrer que z est impair et que x et y sont de parités différentes.

3) On suppose maintenant que x et z sont impairs et y est pair. On pose $y = 2y'$, $X = \frac{x+z}{2}$ et $Z = \frac{z-x}{2}$. Montrer que X et Z sont des carrés parfaits premiers entre eux.
4) En déduire que les solutions sont les triplets de la forme $(d(u^2 - v^2), 2duv, d(u^2 + v^2))$ où $d \in \mathbb{N}$ et $u, v \in \mathbb{Z}$, à une permutation près des deux premières composantes.

Solution :
1)

- Notons $d = \text{pgcd}(x, y, z)$ puis $(x', y', z') = \left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right)$, alors l'équation $x^2 + y^2 = z^2$ est équivalente à $x'^2 + y'^2 = z'^2$ x', y' et z' sont premiers entre eux. On peut donc se ramener au cas où x, y et z sont premiers entre eux.
- Dans ce cas, si p est un diviseur premier de x et y alors il divise $x^2 + y^2 = z^2$, donc il divise z, ce qui est absurde puisque x, y et z sont premiers entre eux. Ainsi $x \wedge y = 1$ et de même, $y \wedge z = 1$ et $x \wedge z = 1$.

1) Déjà, $\text{pgcd}(x, y) = 1$ donc x et y ne peuvent pas être tous les deux pairs. S'ils sont tous les deux impairs alors $z^2 = x^2 + y^2$ est pair, donc z est pair, donc $z^2 \equiv 0[4]$. Mais d'autre part, $x^2 + y^2 \equiv 1 + 1 = 2[4]$ ce qui est absurde. Ainsi x et y sont de parités différentes. z^2 est alors nécessairement impair, donc z aussi.
2) • Déjà, si d est un diviseur commun à X et Z alors il divise $X + Z = z$ et $Z - X = x$, donc $d = 1$ puisque $\text{pgcd}(x, z) = 1$. Ainsi X et Z sont premiers entre eux.
   • On a $y'^2 = \frac{y^2}{4} = \frac{z^2 - x^2}{4} = XZ$. Soit p diviseur premier de X, alors p ne divise pas Z donc $v_p(X) = v_p(y'^2) - v_p(Z) = 2v_p(y') \in 2\mathbb{N}$. Ainsi tous les facteurs premiers de X apparaissent à une puissance paire dans la décomposition en facteurs premiers de X, donc X est un carré parfait. De même, Z est un carré parfait.
3) On a vu que si $\text{pgcd}(x, y, z) = 1$ alors il existe $u, v \in \mathbb{Z}$ tels que $(x, y, z) = (u^2 - v^2, 2uv, u^2 + v^2)$ à une permutation près des deux premières composantes (avec $u^2 = X$ et $v^2 = Y$). Dans le cas général, il existe $d \in \mathbb{N}$ et $u, v \in \mathbb{Z}$ tels que $(x, y, z) = (u^2 - v^2, 2uv, u^2 + v^2)$ à une permutation près des deux premières composantes (avec $d = \text{pgcd}(x, y, z)$). Réciproquement, on vérifie aisément que ces triplets sont bien solutions.

Exercice 1.6.18 (⋆ ⋆ ♥) : Montrer que tout nombre impair non divisible par 5 admet un multiple qui ne s'écrit (en base 10) qu'avec des 1.

Solution : Notons $E = \{1, 11, 111, ...\}$ l'ensemble des nombres qui ne s'écrivent qu'avec des 1 en base 10. Soit n un nombre impair non divisible par 5. Par le principe des tiroirs, il existe $i, j \in E$ distincts qui ont le même reste modulo n (car l'ensemble des restes modulo n est fini et E est infini). On suppose sans perte de généralité $j > i$. Alors $j - i$ est de la forme $1...10...0$, donc il existe $k \in \mathbb{N}^*$ tel que $\frac{j-i}{10^k} \in E$ (k est le nombre de chiffres de i). Alors $j - i$ est divisible par n et par 10^k. Comme n n'est ni un multiple de 2, ni un multiple de 5, n et 10^k sont premiers entre eux, donc $j - i$ est divisible par $n10^k$, et donc $\frac{j-i}{10^k}$ est divisible par n et ne s'écrit qu'avec des 1.

Remarque : avec la même méthode, on peut montrer que tout entier naturel non nul admet un multiple qui ne s'écrit qu'avec des 0 *et des* 5.

Exercice 1.6.19 (⋆ ⋆) :

1) Soit $n \in \mathbb{N}^*$. Déterminer le nombre de chiffres de n en base 10.
2) Pour tout $n \in \mathbb{N}^*$, on pose $S(n)$ la somme des chiffres en base 10 de n. Montrer que la suite $\left(\frac{S(n+1)}{S(n)}\right)_{n\in\mathbb{N}^*}$ est bornée. Cette suite converge-t-elle ?
3) Montrer que $\forall n \in \mathbb{N}^*, 1 \leqslant S(n) \leqslant 9(1+\log_{10}(n))$.
4) Montrer que la suite $\left(\sqrt[n]{S(n)}\right)_{n\geqslant 1}$ converge et préciser sa limite.

Solution :

1) Si k est un entier tel que $10^k \leqslant n < 10^{k+1}$, alors n a $k+1$ chiffres. Or $10^k \leqslant n < 10^{k+1} \iff k \leqslant \log_{10}(n) < k+1 \iff k = \lfloor \log_{10}(n) \rfloor$. Le nombre de chiffres de n est donc $\lfloor \log_{10}(n) \rfloor + 1$.
2) Pour tout $n \in \mathbb{N}^*$, on a $S(n+1) = \begin{cases} S(n)+1 \text{ si } n \text{ ne se termine pas par un } 9 \\ S(n)-8 \text{ sinon} \end{cases}$ donc $\frac{S(n+1)}{S(n)} \leqslant 1 + \frac{1}{S(n)} \leqslant 2$ et $\frac{S(n+1)}{S(n)} \geqslant 1 - \frac{8}{S(n)} \geqslant -7$. La suite $\left(\frac{S(n+1)}{S(n)}\right)_{n\in\mathbb{N}^*}$ est donc bornée. On va montrer qu'elle diverge en exhibant deux sous-suites qui convergent vers des valeurs différentes.
   - En posant $\sigma(n) = 10^n$, on a $\frac{S(\sigma(n+1))}{S(\sigma(n))} = \frac{2}{1} = 2 \underset{n\to\infty}{\longrightarrow} 2$.
   - En posant $\tau(n) = 10^n - 1$, on a $\frac{S(\tau(n+1))}{S(\tau(n))} = \frac{1}{9n} \underset{n\to\infty}{\longrightarrow} 0$.
3) C'est évident d'après la question 1.
4) D'après la question 3, $1 \leqslant \sqrt[n]{S(n)} \leqslant \sqrt[n]{9(1+\log_{10}(n))} = \exp\left(\frac{1}{n}\ln(9(1+\log_{10}(n)))\right) \underset{n\to\infty}{\longrightarrow} 1$ donc la suite $\left(\sqrt[n]{S(n)}\right)_{n\geqslant 1}$ converge vers 1.

Exercice 1.6.20 (⋆ ⋆) :

1) Soit $n \in \mathbb{N}^*$. Montrer que la somme dess chiffres de n (en base 10) est congrue à n modulo 9.
2) Trouver la somme des chiffres de la somme des chiffres de la somme des chiffres de 4444^{4444} (en base 10).

Solution :

1) En écrivant $n = \sum a_k 10^k$, on a $n \equiv \sum a_k 1^k = S(n)[9]$.
2) Pour tout $n \in \mathbb{N}^*$, on note $c(n)$ le nombre de chiffres de n et $S(n)$ la somme des chiffres de n. On a $S(n) \leqslant 9c(n)$.

   En notant $A = 4444^{4444}$, on a $A < 10^{5\times 4444}$ donc $c(A) \leqslant 5 \times 4444$ et $S(A) \leqslant 9 \times 5 \times 4555 < 10^6$, puis $S(S(A)) \leqslant 9 \times 6 = 54$.

   Or $4444^{4444} \equiv 7^{4444} \equiv (-2)^{4444} \equiv \left((-2)^3\right)^{1481} \times (-2) \equiv -2 \equiv 7[9]$. Ainsi $S(S(A)) \equiv 7[9]$, donc $S(S(A)) \in \{7, 16, 25, 34, 43, 52\}$. Dans tous les cas, on en déduit $S(S(S(A))) = 7$.

Exercice 1.6.21 (⋆ ⋆ ♥) : On note $(p_n)_{n\in\mathbb{N}}$ la suite des nombres premiers (rangés dans l'ordre croissant). On souhaite montrer que $\sum \frac{1}{p_n}$ diverge. Pour cela, on suppose par l'absurde que la série converge. On sait alors qu'il existe $k \in \mathbb{N}$ tel que $\sum_{n=k}^{\infty} \frac{1}{p_n} < \frac{1}{2}$.

On note A l'ensemble des nombres de $[\![1, N]\!]$ dont tous les diviseurs premiers sont parmi $p_0, \ldots, p_{k-1}$, et $B = [\![1, N]\!] \setminus A$.

1) Pour tout $n \in A$, on écrit $n = a_n b_n^2$ où a_n n'est divisible par aucun carré de nombre premier et $b_n \in \mathbb{N}$.

a) Montrer que $\#\{a_n; n \in A\} = 2^k$.
b) Montrer que $\#\{b_n; n \in A\} \leqslant \sqrt{N}$.
c) En déduire que pour N suffisamment grand, $\#A \leqslant \frac{N}{2}$.

2) Montrer que $\#B < \frac{N}{2}$.
3) Conclure.

Solution:

1) a) Soit $n \in A$. Par définition de A, tous les facteurs premiers de a_n sont parmi $p_0, ..., p_{k-1}$. De plus, ils sont distincts, car a_n n'est pas divisible par le carré d'un nombre premier. Ainsi, choisir un a_n revient à choisir ses facteurs premiers parmi $p_0, ..., p_{k-1}$, soit 2^k choix. Donc $\#\{a_n; n \in A\} = 2^k$.
   b) Pour tout $n \in \mathbb{N}$, $b_n = \sqrt{\frac{n}{a_n}} \leqslant \sqrt{n} \leqslant \sqrt{N}$. Ainsi $\{b_n; n \in A\} \subseteq [\![1, \sqrt{N}]\!]$, d'où le résultat.
   c) D'après les deux questions précédentes, $\#A \leqslant 2^k\sqrt{N}$, donc pour $N \geqslant 2^{2k+2}$, $\#A \leqslant \frac{N}{2}$.
2) Pour tout $n \in \mathbb{N}$, on note B_n l'ensemble des multiples de p_n compris entre 1 et N. Alors $B = \bigcup_{n \geqslant k} B_n$, donc

$$\#B \leqslant \sum_{n=k}^{\infty} \#B_n = \sum_{n=k}^{\infty} \left\lfloor \frac{N}{p_n} \right\rfloor \leqslant N \sum_{n=k}^{\infty} \frac{1}{p_n} < \frac{N}{2}$$

3) D'après les deux questions précédentes, pour N suffisamment grand, $\#A \leqslant \frac{N}{2}$ et $\#B < \frac{N}{2}$, donc $\#A \cup B < N$. Mais $A \cup B = [\![1, N]\!]$: absurde.

Remarque : cette preuve est due à Erdős. Le premier à avoir démontré ce résultat est Euler.

Exercice 1.6.22 (⋆ ⋆ ⋆): Soit $x \in \mathbb{R}_+^*$. On note E_x l'ensemble des entiers naturels dont tous les diviseurs premiers sont inférieurs ou égaux à x.

1) Soit $\mathbb{P}$ l'ensemble des nombres premiers. Justifier que

$$\sum_{t \in E_x} \frac{1}{t} = \prod_{\substack{p \in \mathbb{P} \\ p \leqslant x}} \sum_{\alpha \in \mathbb{N}} \frac{1}{p^\alpha}$$

2) En déduire que $\ln x \leqslant \pi(x) + 1$, où $\pi(x)$ est le nombre de nombres premiers inférieurs ou égaux à x.
3) En déduire qu'il existe une infinité de nombres premiers

Solution:

1) Les éléments de E_x sont exactement les $\prod_{\substack{p \in \mathbb{P} \\ p \leqslant x}} p^{\alpha_p}$ où les α_p sont des entiers naturels, donc on a par sommation par paquets d'une famille de réels positifs

$$\sum_{t \in E_x} \frac{1}{t} = \sum_{(\alpha_p)_{\substack{p \in \mathbb{P} \\ p \leqslant x}}} \prod_{\substack{p \in \mathbb{P} \\ p \leqslant x}} \frac{1}{p^{\alpha_p}}$$

De plus, par le théorème de Fubini sur les familles de réels positifs,

$$\prod_{\substack{p\in\mathbb{P}\\ p\leqslant x}}\sum_{\alpha\in\mathbb{N}}\frac{1}{p^\alpha}=\sum_{(\alpha_p)_{\substack{p\in\mathbb{P}\\ p\leqslant x}}}\prod_{\substack{p\in\mathbb{P}\\ p\leqslant x}}\frac{1}{p^{\alpha_p}}$$

2) En comparant $\ln x=\int_1^x\frac{1}{t}\,\mathrm{d}t$ à $\sum_{t=1}^x\frac{1}{t}$, on voit que

$$\ln x\leqslant\sum_{t=1}^n\frac{1}{t}\leqslant\sum_{t\in E_x}\frac{1}{t}$$

D'autre part,

$$\prod_{\substack{p\in\mathbb{P}\\ p\leqslant x}}\sum_{\alpha\in\mathbb{N}}\frac{1}{p^\alpha}=\prod_{\substack{p\in\mathbb{P}\\ p\leqslant x}}\frac{1}{1-p}=\prod_{\substack{p\in\mathbb{P}\\ p\leqslant x}}1+\frac{1}{p-1}$$

Clairement, le k-ième nombre premier est toujours $\geqslant k+1$, donc

$$\prod_{\substack{p\in\mathbb{P}\\ p\leqslant x}}\sum_{\alpha\in\mathbb{N}}\frac{1}{p^\alpha}\leqslant\prod_{k=1}^{\pi(x)}\frac{k+1}{k}=\pi(x)+1$$

et la question 1 permet de conclure.

3) Il suffit de faire tendre x vers ∞ dans l'inégalité précédente.

Remarque : cette preuve de l'infinitude des nombres premiers est due à Euler.

Exercice 1.6.23 ($\star\star\star$): Soit $u\in\mathbb{Z}^{\mathbb{N}}$ une suite que l'on suppose être :

- presque injective, i.e. $\exists c\in\mathbb{N}^*,\forall n\in\mathbb{Z},\#u^{-1}(\{n\})\leqslant c$;
- sous-exponentielle, i.e. $\forall n\in\mathbb{Z},|u_n|\leqslant 2^{2^{f(n)}}$ où $f:\mathbb{N}\to\mathbb{R}_+$ et $f(n)=o(\log_2(n))$.

On note $\mathbb{P}_u$ l'ensemble des nombres premiers qui divisent au moins un terme de la suite u. On souhaite montrer que $\mathbb{P}_u$ est infini.

1) Justifier que l'on peut supposer sans perte de généralité que la fonction f est croissante.
2) Soit $N\in\mathbb{N}$. Montrer que $\#\{|u_n|;n<N,u_n\neq 0\}\geqslant\frac{N-c}{2c}$.
3) Soit $N\in\mathbb{N}$. On suppose par l'absurde que $\mathbb{P}_u$ est fini de cardinal k. Montrer que $\#\{|u_n|;n<N,u_n\neq 0\}\leqslant 2^{k(f(N)+1)}$.
4) Conclure.

Solution:

1) Si f n'est pas croissante, on peut la remplacer par $\tilde{f}:n\mapsto\max\{f(i);i\leqslant n\}$. Cette fonction est bien croissante et on a toujours $\forall n\in\mathbb{Z},|u_n|\leqslant 2^{2^{\tilde{f}(n)}}$ et $\tilde{f}(n)=o(\log_2(n))$.
2) Il y a N nombres $(|u_n|)_{n<N}$ (pas forcément distincts). Parmi eux, au plus c valent 0, donc il y a au moins $N-c$ nombres $(|u_n|)_{n<N}$ non nuls (pas forcément distincts). Comme u est presque injective, chaque valeur peut être prise par au plus $2c$ de ces nombres, d'où le résultat.
3) On note $\mathbb{P}_u=\{p_1,...,p_k\}$. Pour tout $n\in\mathbb{N}$, on note $u_n=\varepsilon_n p_1^{v_1(n)}...p_k^{v_k(n)}$ où $\varepsilon_n\in\{-1,0,1\}$ et $v_i(n)$ est la valuation p_i-adique de n (si $n=0$, on prend $v_i(n)=0$). On a alors, si $u_n\neq 0$:

$$2^{v_1(n)+...+v_k(n)} \leqslant |u_n| \leqslant 2^{2^{f(n)}}$$

donc $v_1(n) + ... + v_k(n) \leqslant 2^{f(n)}$. Du coup, si $n < N$ alors par croissance de f, pour tout $i \in [\![1, k]\!]$, $0 \leqslant v_i(n) \leqslant 2^{f(n)} \leqslant 2^{f(N)}$. Ainsi,

$$\#\{|u_n|; n < N, u_n \neq 0\} \leqslant \left(2^{f(N)} + 1\right)^k \leqslant 2^{k(f(N)+1)}$$

4) D'après les deux questions précédentes, pour tout $N \in \mathbb{N}$, $\frac{N-c}{2c} \leqslant 2^{k(f(N)+1)}$. On écrit $f(N) = \varepsilon_N \log_2(N)$ où $\varepsilon_N \longrightarrow 0$. On obtient $\frac{N-c}{2c} \leqslant 2^k N^{k\varepsilon_N}$ et on obtient une contradiction en faisant tendre N vers ∞.

Remarque : ce résultat est du à Christian Elsholtz. En prenant $u_n = n$, on retrouve l'existence d'une infinité de nombres premiers.

1.7. Généralités sur les corps

Définition 1.7.1 : On dit qu'un anneau $(K, +, \times)$ est un corps ssi c'est un anneau commutatif unitaire non trivial dans lequel tout élément non nul est inversible.

Lemme 1.7.1 : Si $(K, +, \times)$ est un corps alors c'est un anneau intègre.

Preuve : Soient $x, y \in K$ tels que $xy = 0$. Si $x \neq 0$ alors $y = x^{-1}0 = 0$, donc $x = 0 \vee y = 0$. ■

Lemme 1.7.2 : Soit $p \in \mathbb{N}$. Alors $\mathbb{Z}/p\mathbb{Z}$ est un corps ssi p est premier.

Preuve :

- Supposons que $\mathbb{Z}/p\mathbb{Z}$ soit un corps. Soient $a, b \in \mathbb{N}^*$ tels que $p = ab$. Alors $\overline{0} = \overline{a}\overline{b}$, mais $\mathbb{Z}/p\mathbb{Z}$ est intègre donc $\overline{a} = 0 \vee \overline{b} = 0$, i.e. $p|a \vee p|b$, i.e. $a = p \vee b = p$. Ceci montre que p est premier.
- Supposons que p est premier. Alors pour tout $n \in [\![1, p-1]\!]$, $n \wedge p = 1$ donc $\overline{n}$ est inversible dans $\mathbb{Z}/p\mathbb{Z}$. Ainsi $\mathbb{Z}/p\mathbb{Z}$ est un corps.

■

Définition 1.7.2 : Soit $(K, +, \times)$ un corps. On dit qu'une partie $L \subseteq K$ est un sous-corps de K (ou que K est une extension de corps de L) ssi $(L, +|_{L^2}, \times|_{L^2})$ est un corps.

Remarque 1.7.1 : L est un sous-corps de K ssi c'est un sous-anneau de K contenant 1.

Lemme 1.7.3 : Soient K un corps, A un anneau unitaire non trivial et $\varphi : K \to A$ un morphisme d'anneaux vérifiant $\varphi(1) = 1$. Alors φ est injectif.

Preuve : Soit $x \in K$ tel que $\varphi(x) = 0$. Si $x \neq 0$ alors $1 = \varphi(1) = \varphi(x)\varphi\left(\frac{1}{x}\right) = 0$, absurde. ■

Définition 1.7.3 : Si K et L sont deux corps, on appelle morphisme de corps de K vers L tout morphisme d'anneaux φ de K vers L tel que $\varphi(1) = 1$.

Remarque 1.7.2: D'après le lemme précédent, tout morphisme de corps est injectif.

Définition 1.7.4: Soit A un anneau commutatif unitaire intègre. On définit deux lois de composition interne $+$ et $\times$ sur $A \times (A \setminus \{0\})$ en posant :
- $(a,b) + (c,d) = (ad + bc, bd)$;
- $(a,b) \times (c,d) = (ac, bd)$.

On définit une relation binaire $\sim$ sur $A \times (A \setminus \{0\})$ en posant $(a,b) \sim (b,c) \iff ad = bc$.

Lemme 1.7.4: La relation $\sim$ est une relation d'équivalence sur $A \times A \setminus \{0\}$ compatible avec $+$ et $\times$.

Définition 1.7.5: Soit A un anneau commutatif unitaire intègre. On pose $K_A = (A \times (A \setminus \{0\}))/\sim$ le corps des fractions de A. Un élément $\overline{(a,b)} \in K_A$ sera noté $\frac{a}{b}$.

Théorème 1.7.1: Soit A un anneau commutatif unitaire intègre. Alors K_A est le plus petit corps contenant A. Plus exactement :
1) K_A est un corps ;
2) $\begin{cases} A \to K_A \\ a \mapsto \frac{a}{1} \end{cases}$ est un morphisme injectif d'anneaux donc on peut considérer que $A \subseteq K_A$;
3) tout corps possédant un sous-anneau isomorphe à A possède un sous-corps isomorphe à K_A.

Preuve:
1) Fastidieux mais facile. L'inverse de $\frac{a}{b}$ est $\frac{b}{a}$ dès lors que $a, b \neq 0$.
2) Facile.
3) Soit K un corps possédant un sous-anneau A' isomorphe à A, soit donc $\sigma : A' \to A$ un isomorphisme d'anneaux. On pose $S = \{ab^{-1}; (a,b) \in A' \times (A' \setminus \{0\})\}$. On vérifie facilement que S est un sous-corps de K.

   On pose alors

$$\varphi : \begin{cases} S & \to K_A \\ ab^{-1} & \mapsto \frac{\sigma(a)}{\sigma(b)} \end{cases}$$

   on vérifie facilement que φ est bien définie et que c'est un isomorphisme de corps.

■

2. Groupes

2.1. Actions de groupe

Définition 2.1.1: Action d'un groupe sur un ensemble
- $s \cdot (t \cdot x) = (st) \cdot x$
- $e \cdot x = x$

Exemple 2.1.1: G agit sur lui-même par l'application $(s, x) \mapsto sx$ (ou $(s, x) \mapsto xs^{-1}$ ou $(s, x) \mapsto sxs^{-1}$). $S(X)$ agit sur X par l'application $(s, x) \mapsto s(x)$.

Remarque 2.1.1: L'application

$$\varphi : \begin{cases} G \to S(X) \\ g \mapsto \begin{cases} X \to X \\ x \mapsto g \cdot x \end{cases} \end{cases}$$

est un morphisme de groupes. On pourrait aussi dire que G agit sur X ssi il existe un morphisme $\varphi : G \to S(X)$, et poser $g \cdot x = \varphi(g)(x)$.

Définition 2.1.2:
- Relation d'intransitivité : $xTy \iff \exists s \in G, y = s \cdot x$
- Classes d'équivalences pour T : orbites : $O_x = \{s \cdot x; s \in G\}$

Définition 2.1.3: Stabilisateurs : $S_x = \{s \in G; s \cdot x = x\}$

Lemme 2.1.1: S_x est un sous-groupe de G.

Définition 2.1.4:
- Une action est dite transitive ssi elle n'a qu'une seule orbite.
- Une action est dite libre ssi tous les stabilisateurs sont réduits à l'élément neutre.
- Une action est dite simplement transitive ssi elle est transitive et libre.

Remarque 2.1.2:
- Une action est transitive ssi $\forall x, y \in X, \exists g \in G, g \cdot x = y$.
- Une action est libre ssi $\forall x \in X, \forall g, g' \in G, g \cdot x = g' \cdot x \Rightarrow g = g'$.
- Une action est simplement transitive ssi $\forall x, y \in X, \exists! g \in G, g \cdot x = y$.

Théorème 2.1.1 (formule orbite-stabilisateur): Si G est fini alors $\forall x \in X, |G| = |O_x| \times |S_x|$.

Preuve: Soient $x \in X$ puis R_x la relation définie sur G par $sR_xt \iff s \cdot x = t \cdot x$, qui est une relation d'équivalence. Les classes d'équivalence sont les tS_x, donc elles sont de cardinal $|S_x|$, et il y en a $|O_x|$. ■

Théorème 2.1.2 (Formule du produit) : Soient G un groupe, et H, K deux sous-groupes finis de G. Alors $\#(HK)\#(H \cap K) = \#H\#K$.

Preuve : On considère l'action de $H \times K$ sur G définie par $(h,k) \cdot g = hgk^{-1}$ (on vérifie facilement que c'est une action de groupe). L'orbite de l'élément neutre vaut HK et son stabilisateur vaut $\{(h,h); h \in H \cap K\}$ de cardinal $\#(H \cap K)$, d'où le résultat par la formule orbite-stabilisateur. ■

Exercice 2.1.1 (⋆) : Déterminer le nombre d'anagrammes du mot « mathématiques », c'est-à-dire le nombre de mots distincts obtenus par permutation des lettres du mot « mathématiques ».

Solution : Soit X l'ensemble des anagrammes du mot « mathématiques ». On considère l'action naturelle de $G = \mathfrak{S}(X)$ sur X. Soit x le mot « mathématiques ». Par la formule orbite-stabilisateur, $|G| = |O_x| \times |S_x|$. Mais $|G| = 13!$, $|O_x| = |X|$ et $|S_x| = 8$. En effet, si $g \cdot x = x$ alors g échange éventuellement la première et la sixième lettre, la deuxième et la septième lettre, et la troisième et la huitième lettre, et laisse les autres lettres invariantes. Il y a donc $2 \times 2 \times 2 = 8$ permutations qui laissent x invariante. Finalement $|X| = \frac{13!}{8}$.

Corollaire 2.1.1 (Formule des classes) : Si X et G sont finis, et Θ est une partie de X contenant un représentant de chaque classe d'intransitivité alors $|X| = \sum_{x \in \Theta} \frac{|G|}{|S_x|}$.

Corollaire 2.1.2 : Soit G un groupe fini. Alors il existe une famille $(H_i)_{i \in I}$ de sous-groupes stricts de G telle que $|G| = |Z(G)| + \sum_{i \in I} \frac{|G|}{|H_i|}$.

Preuve : On prend $X = G$ et $g \cdot x = gxg^{-1}$. Alors $|G| = \sum_{x \in \theta} |O_x|$ pour une certaine partie $\theta \subseteq G$. Les éléments x tels que $|O_x| = 1$ sont exactement les éléments de $|Z(G)|$. Les autres ont un stabilisateur qui est un sous-groupe strict de G. ■

*Exercice 2.1.2 (*petit théorème de Fermat $\star\star$ ♥*)* : Soient $n \in \mathbb{N}^*$ et $p \in \mathbb{P}$.

1) On fait agir $\mathbb{Z}/p\mathbb{Z}$ sur $X = [\![1, n]\!]^p$ en posant $\overline{k} \cdot (a_1, ..., a_n) = \left(a_{\gamma^k(1)}, ..., a_{\gamma^k(n)}\right)$ où $\gamma = (1\ 2\ \dots\ p) \in S_p$. Déterminer les valeurs possibles de $|O_x|$ pour $x \in X$.
2) En déduire que $n^p \equiv n[p]$.

Solution :

1) Déjà, l'action de groupe est bien définie. Soit $x \in X$. D'après la formule orbite-stabilisateur, on a $p = |\mathbb{Z}/p\mathbb{Z}| = |O_x| \times |S_x|$. Ainsi $|O_x|$ divise p, donc $|O_x| = 1$ ou $|O_x| = p$.
2) Soit θ une partie de X contenant exactement un élément de chaque orbite. Par la formule des classes, $n^p = \sum_{x \in \theta} |O_x|$. Les orbites contenant un seul élément sont celles des éléments de la forme $(a, ..., a)$; il y en a n. Les autres sont de cardinal p d'après la question

précédente. Du coup $n^p \equiv n[p]$. (Voir ici pour une preuve plus élémentaire du petit théorème de Fermat.)

*Exercice 2.1.3 (*lemme de Cauchy ⋆⋆ ♥*)*: Soient G un groupe fini de cardinal $h \geqslant 2$, et p un facteur premier de h.

1) On pose $S = \{(a_1, ..., a_p) \in G^p; a_1...a_p = e\}$ et $\gamma \in \mathfrak{S}_p$ le cycle $(1\ \ 2\ \ \dots\ \ p)$ (ici $\mathfrak{S}_p$ désigne le groupe symétrique d'indice p). On fait opérer $\langle\gamma\rangle$ sur S en posant pour tout $k \in \mathbb{Z}$, $\gamma^k \cdot (a_1, ..., a_p) = \left(a_{\gamma^k(1)}, ..., a_{\gamma^k(p)}\right)$. Déterminer les valeurs possibles de $|O_a|$ pour $a \in S$.
2) Montrer que $A = |\{x \in G; x^p = e\}|$ est un multiple de p.
3) En déduire qu'il existe un élément de G d'ordre p.

Solution:

1) Déjà, l'action de groupe est bien définie. Soit $a \in S$. D'après la formule orbite-stabilisateur, on a $p = |\langle\gamma\rangle| = |O_a| \times |S_a|$. Ainsi $|O_a|$ divise p, donc $|O_a| = 1$ ou $|O_a| = p$.
2) On a $x^p = e \iff (x, ..., x) \in S$ donc A est le nombre d'éléments de S dont l'orbite contient un élément. Par la formule orbite-stabilisateur et par la question précédente, $A = |S| - pk$ où $k \in \mathbb{N}$ est le nombre d'orbites contenant au moins deux éléments.

   Or $S = \left\{\left(a_1, ..., a_{p-1}, \left(a_1...a_{p-1}\right)^{-1}\right); (a_1, ..., a_{p-1}) \in G^{p-1}\right\}$ donc $|S| = h^{p-1} \equiv 0[p]$. Du coup, A est un multiple de p.
3) A est un multiple de p et est strictement positif (car $e^p = e$), donc $A \geqslant 2$. Soit donc $x \neq e$ tel que $x^p = e$. Alors l'ordre de x divise p, donc vaut p !!

*Exercice 2.1.4 (*formule de Burnside et problème du collier ⋆⋆⋆*)*:

1) Soient G un groupe fini agissant sur un ensemble fini non vide X. On note X/G l'ensemble des orbites. Pour tout $g \in G$, on note $\mathrm{Fix}_g = \{x \in X; g \cdot x = x\}$.
   a) Montrer que $\sum_{g\in G} |\mathrm{Fix}_g| = \sum_{x\in X} |S_x|$.
   b) En déduire la formule de Burnside : $|X/G| = \frac{1}{|G|} \sum_{g\in G} |\mathrm{Fix}_g|$.
2) En déduire le nombre de colliers avec 4 perles bleues, 3 perles vertes et 2 perles rouges.

Solution:

1)
2) $\sum_{g\in G} |\mathrm{Fix}_g| = |\{(g, x) \in G \times X; g \cdot x = x\}| = \sum_{x\in X} |S_x|$
3) $|X/G| = \sum_{O\in X/G} 1 = \sum_{O\in X/G} \sum_{x\in O} \frac{1}{|O|} = \sum_{x\in X} \frac{1}{|O_x|} = \frac{1}{|G|} \sum_{x\in X} |S_x| = \frac{1}{|G|} \sum_{g\in G} |\mathrm{Fix}_g|$
4) Il faut faire attention que si on fait tourner ou que l'on retourne un collier, il s'agit encore du même collier. On va appliquer la formule de Burnside à l'action canonique de $G = D_9 = \{\mathrm{id}, r, ..., r^8, s, rs, ..., r^7 s\}$ sur l'ensemble X des coloriages des sommets de l'ennéagone régulier avec 4 sommets bleus, 3 sommets verts et 2 sommets bleus. Le nombre recherché sera alors $|X/G|$. Déjà, $|G| = \binom{9}{4}\binom{3}{5} = 1260$. De plus, $|\mathrm{Fix}_{\mathrm{id}}| = 1260$, $|\mathrm{Fix}_r| = |\mathrm{Fix}_{r^2}| = ... = 0$ et en bidouillant un peu, on voit que $|\mathrm{Fix}_s| = |\mathrm{Fix}_{rs}| = ... = 12$. La formule de Burnside donne alors $|X/G| = 76$.

2.2. Groupes abéliens finis

Lemme 2.2.1: $\varphi : \begin{cases} \mathbb{Z} \to \langle a \rangle \\ n \mapsto a^n \end{cases}$ est un morphisme surjectif de groupes. Si a est d'ordre fini d alors $\ker \varphi = d\mathbb{Z}$.

Preuve: φ est clairement un morphisme surjectif. $\ker \varphi$ est de la forme $n\mathbb{Z}$, et on dispose d'un isomorphisme de $\mathbb{Z}/n\mathbb{Z}$ dans $\langle a \rangle$ donc $n = d$. ■

Théorème 2.2.1: Avec les mêmes notations, $a^k = e \iff k \in d\mathbb{Z}$ et en particulier, $d = \min\{k \in \mathbb{N}^*, a^k = e\}$.

Théorème 2.2.2 (d'Euler): Soient $n \geqslant 2$ et k un entier premier avec n. Alors $k^{\varphi(n)} \equiv 1[n]$.

Preuve: Comme $k \wedge n = 1$, $\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$. Comme le groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$ vaut $\varphi(n)$, on a par le théorème de Lagrange que $\overline{k}^{\varphi(n)} = \overline{1}$, d'où le résultat. ■

Remarque 2.2.1: Si n est premier, on retrouve le petit théorème de Fermat (Théorème 1.6.5).

Exercice 2.2.1 (⋆ ♥):
1) Soient p un nombre premier et q un facteur premier de $2^p - 1$. Déterminer l'ordre de 2 dans le groupe multiplicatif $(\mathbb{Z}/q\mathbb{Z})^\times$.
2) À l'aide du théorème de Lagrange, en déduire qu'il existe une infinité de nombres premiers.

Preuve:
1) On a $2^p \equiv 1 \bmod q$ donc l'ordre de 2 dans le groupe multiplicatif $(\mathbb{Z}/q\mathbb{Z})^\times$ divise p. Comme p est premier, l'ordre est égal à p.
2) Avec les mêmes notations, on a par le théorème de Lagrange que $p|q-1$ donc $p < q$. Ainsi pour tout nombre premier p, on a trouvé un nombre premier q strictement plus grand : il existe une infinité de nombres premiers.

■

Exercice 2.2.2 (⋆): Soient $n \geqslant 2$ et k un entier premier avec n. Montrer que $k^{n!} \equiv 1[n]$.

Solution: D'après le théorème d'Euler, $k^{\varphi(n)} \equiv 1[n]$, mais $\varphi(n) \leqslant n$ donc $\varphi(n)|n!$, d'où le résultat.

*Exercice 2.2.3 (*test de Lucas-Lehmer $\star\star$*)*: Soit $n \geqslant 2$ un entier tel qu'il existe $a \in \mathbb{Z}$ tel que $a^{n-1} \equiv 1[n]$ et pour tout facteur premier q de $n-1$, $a^{\frac{n-1}{q}} \not\equiv 1[n]$. Montrer que n est premier.

Solution: Notons ω l'ordre de $\overline{a}$ dans le groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$. Alors $\omega \mid n-1$ car $\overline{a}^{n-1} = \overline{1}$. Si $\omega < n-1$ alors il existe un nombre premier q divisant $n-1$ tel que $\omega | \frac{n-1}{q}$. On a alors $a^{\frac{n-1}{q}} \equiv 1[n]$, absurde. Du coup $\overline{a}$ est d'ordre $n-1$, donc $|Z/n\mathbb{Z}| \geqslant n-1$ et n est premier.

Théorème 2.2.3 : Tout groupe cyclique est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, tout groupe monogène infini est isomorphe à $\mathbb{Z}$.

Lemme 2.2.2 :
- Si $g \in G$ est d'ordre fini n alors pour tout $d \geqslant 1$, g^d est d'ordre $\frac{n}{n \wedge d}$.
- Si $x, y \in G$ commutent et sont d'ordres finis premiers entre eux a et b alors xy est d'ordre ab.
- Si $\varphi : G \to G'$ est un morphisme et $g \in G$ est d'ordre fini n, alors $\varphi(G)$ est d'ordre fini divisant n.

Preuve:
- $\left(g^d\right)^k = e \iff n \mid dk \iff \frac{n}{n \wedge d} \mid k$
- $(xy)^k = e \implies x^k y^k = e \implies \begin{cases} x^{kb} = e \\ y^{ka} = e \end{cases} \implies \begin{cases} a \mid kb \\ b \mid ka \end{cases} \implies \begin{cases} a \mid k \\ b \mid k \end{cases} \implies ab \mid k$ et réciproque OK
- $\varphi(g)^n = \varphi(g^n) = \varphi(e) = e$

■

Exercice 2.2.4 (⋆): Soient G un groupe et $x, y \in G$. On suppose que xy est d'ordre fini n. Montrer que yx est également fini d'ordre n.

Solution : $\forall k \in \mathbb{Z}, (yx)^k = e \iff y(xy)^{k-1}x = e \iff (xy)^{k-1} = y^{-1}x^{-1} \iff (xy)^k = e \iff n \mid k$

Exercice 2.2.5 (⋆): Soient $G_1, ..., G_n$ des groupes cycliques. Trouver une condition nécessaire et suffisante portant sur les ordres de $G_1, ..., G_n$ pour que $G_1 \times ... \times G_n$ soit cyclique.

Solution : Notons $\alpha_1, ..., \alpha_n$ les ordres de $G_1, ..., G_n$. Remarquons que pour tout $x = (x_1, ..., x_n) \in G = G_1 \times ... \times G_n$, G est d'ordre $\mathrm{PPCM}(\beta_1, ..., \beta_n)$ où $\beta_1, ..., \beta_n$ sont les ordres de $x_1, ..., x_n$. En effet, $\forall k \in \mathbb{Z}, x^k = e \iff \left(\forall i \in [\![1, n]\!], x_i^k = e\right) \iff (\forall i \in [\![1, n]\!], \beta_i \mid k) \iff \mathrm{PPCM}(\beta_1, ..., \beta_n) \mid k$. Ainsi x est d'ordre $\mathrm{PPCM}(\beta_1, ..., \beta_n)$.
- Supposons que $G = G_1 \times ... \times G_n$ soit cyclique. Soit $x = (x_1, ..., x_n)$ un générateur de G. Alors x est d'ordre $|G| = \alpha_1 ... \alpha_n$, mais il est aussi d'ordre $\mathrm{PPCM}(\beta_1, ..., \beta_n)$ où $\beta_1, ..., \beta_n$ sont les ordres de $x_1, ..., x_n$. Ainsi $\mathrm{PPCM}(\beta_1, ..., \beta_n) = \alpha_1 ... \alpha_n$. Mais on a $\mathrm{PPCM}(\beta_1, ..., \beta_n) \leqslant \beta_1 ... \beta_n \leqslant \alpha_1 ... \alpha_n$. Il y a ainsi égalité dans les deux inégalités, ce qui implique que $(\alpha_1, ..., \alpha_n) = (\beta_1, ..., \beta_n)$ puis que les α_i sont premiers entre eux deux à deux.
- Réciproquement, supposons que les α_i sont premiers entre eux deux à deux. Soient $x_1, ..., x_n$ des générateurs de $G_1, ..., G_n$. Alors $(x_1, ..., x_n)$ est d'ordre $\mathrm{PPCM}(\alpha_1, ..., \alpha_n) = \alpha_1 ... \alpha_n$, donc est un générateur de G et G est cyclique.

Ainsi G est cyclique ssi les ordres des G_i sont premiers entre eux deux à deux.

Exercice 2.2.6 (⋆): Soient G un groupe abélien et H_1, H_2 deux sous-groupes de G d'ordres finis p et q, où p et q sont des nombres premiers distincts. Montrer que $H_1 H_2$ est un sous-groupe cyclique de G.

Solution : Déjà, comme G est abélien, on a $H_2H_1 \subseteq H_1H_2$, donc H_1H_2 est un sous-groupe de G.

Si $x \in H_1 \cap H_2$ alors l'ordre de x divise p et q, donc vaut 1. Ainsi $H_1 \cap H_2 = \{e\}$, donc $|H_1H_2| = pq$.

H_1 et H_2 sont d'ordres premiers donc cycliques, soient donc h_1 et h_2 des générateurs de H_1 et H_2 respectivement. Alors pour tout $n \in \mathbb{Z}$,

$$(h_1h_2)^n = e \iff h_1^n h_2^n = e \iff h_1^n = h_2^{-n} \iff \begin{cases} h_1^n = e \\ h_2^n = e \end{cases} \iff \begin{cases} p|n \\ q|n \end{cases} \iff pq|n$$

où la troisième équivalence vient du fait que $H_1 \cap H_2 = \{e\}$. Ainsi h_1h_2 est d'ordre $pq = |H_1H_2|$, donc H_1H_2 est cyclique.

Théorème 2.2.4 : Soit $G = \langle g \rangle$ est un groupe cyclique d'ordre n.
1) Les générateurs de G sont les g^k où $k \in [\![1, n-1]\!]$ et $k \wedge n = 1$.
2) Les sous-groupes de G sont les $\langle g^k \rangle$ où k est un diviseur positif de n.
3) Les endomorphismes de G sont les $x \mapsto x^p$ où $p \in [\![0, n-1]\!]$.

Preuve :
1) • Soit h un générateur de G. On écrit $h = g^k$ avec $k \in [\![1, n-1]\!]$. Soit $u \in \mathbb{Z}$ tel que $g = \left(g^k\right)^u = g^{ku}$. Alors $g^{1-ku} = e$ donc $n|1-ku$. Par le théorème de Bézout, $n \wedge k = 1$.
   • Réciproquement, si $k \wedge n = 1$, on écrit $ak + bn = 1$. Alors $g = g^{ak+bn} = g^{ak} \in \langle g^k \rangle$ donc g^k est un générateur de G.
2) Soit H un sous-groupe de G. Notons $d = |H|$ (qui est un diviseur de n par Lagrange), et $k = \frac{n}{d}$. Soit $h = g^l \in H$, alors $g^{dl} = 0$ donc $n \mid dl$ et donc $k \mid l$. On en déduit $h \in \langle g^k \rangle$. Ainsi $H \subseteq \langle g^k \rangle$, puis $H = \langle g^k \rangle$ par égalité des cardinaux. La réciproque est claire.
3) $\{x \mapsto x^p ; p \in [\![0, n-1]\!]\} \subseteq \mathrm{End}(G)$ car G est abélien. $\begin{cases} \mathrm{End}(G) \to G \\ \varphi \quad \mapsto \varphi(g) \end{cases}$ est un isomorphisme de groupes, donc $n = |\mathrm{End}(G)|$ et $\{x \mapsto x^p ; p \in [\![0, n-1]\!]\} = \mathrm{End}(G)$.

■

Remarque 2.2.2 : Du coup, le nombre de générateurs de G est $\varphi(|G|)$.

Définition 2.2.1 : L'exposant d'un groupe fini G est le plus petit $a \geqslant 1$ tel que $\forall x \in G, x^a = e$. On le note $\exp G$.

Remarque 2.2.3 :
• $\exp G$ est bien défini et divise $|G|$. C'est aussi le PPCM des ordres des éléments de G.
• Si $G = \prod_{i=1}^n \mathbb{Z}/a_i\mathbb{Z}$ alors $\exp G$ est le PPCM des a_i. Si de plus $a_1 | \ldots | a_n$ alors $\exp G = a_n$.

Lemme 2.2.3 : Si G est un groupe abélien fini alors G possède un élément d'ordre $\exp G$. Autrement dit, $\exp G$ est le maximum des ordres des éléments de G.

Preuve: On décompose $\exp G$ en facteurs premiers : $\exp G = \prod_i p_i^{\alpha_i}$. Pour tout i, il existe un élément g_i d'ordre $p_i^{\alpha_i} m_i$. Alors $g_i^{m_i}$ est d'ordre $\frac{p_i^{\alpha_i} m_i}{p_i^{\alpha_i} m_i \wedge m_i} = p_i^{\alpha_i}$, et $\prod_i g_i^{m_i}$ est d'ordre $\exp(G)$. ■

Théorème 2.2.5 : Soit K un corps. Alors tout sous-groupe fini du groupe multiplicatif $K^\times$ est cyclique.

Preuve: Soient G un sous-groupe fini de K^* et $r = \exp(G)$. Comme K est un corps, le polynôme $X^r - 1 \in K[X]$ admet au plus r racines dans K, donc au plus r racines dans G. Or par définition de l'exposant, $\forall x \in G, x^r = 1$. Du coup $|G| \leqslant r$. Mais on a toujours $r \leqslant |G|$. Ainsi $r = |G|$. Comme G est un groupe abélien fini, il possède un élément d'ordre $r = \exp(G)$, donc G est cyclique. ■

Théorème 2.2.6 : Soit $n \geqslant 2$. Alors le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique ssi l'une de ces conditions est vérifiée :
- soit $n = 2$ ou $n = 4$,
- soit $n = p^r$ où p est un nombre premier impair et $r \in \mathbb{N}^*$,
- soit $n = 2p^r$ où p est un nombre premier impair et $r \in \mathbb{N}^*$.

Preuve:
- Si n est premier alors $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique d'après le Théorème 2.2.5.
- Supposons que $n = p^r$ où p est un nombre premier impair et $r \in \mathbb{N}^*$. Montrons par récurrence que

$$\forall k \in \mathbb{N}, (1+p)^{p^k} \equiv 1 + p^{k+1} \bmod p^{k+2}$$

Le résultat est clair pour $k = 0$. Supposons-le au rang k et montrons-le au rang $k+1$. Soit

$$a_k = \frac{(1+p)^{p^k} - 1 - p^{k+1}}{p^{k+2}}$$

qui est un entier par hypothèse. Alors

$$(1+p)^{p^{k+1}} = \left((1+p)^{p^k}\right)^p = \left(1 + p^{k+1}(1 + a_k p)\right)^p$$

TODO https://fr.wikiversity.org/wiki/Introduction_%C3%A0_la_th%C3%A9orie_des_nombres/Devoir/Groupe_des_inversibles_des_entiers_modulo_n

■

Théorème 2.2.7 (de structure des groupes abéliens finis) : Soit G un groupe abélien fini. Il existe un unique entier r, et des uniques entiers $n_1, ..., n_r \geqslant 2$, tels que $n_1 | n_2 | \ ... \ | n_r$ et G est isomorphe à $\prod_{k=1}^r \mathbb{Z}/n_k\mathbb{Z}$.

Preuve:

- Existence : on raisonne par récurrence sur $\#G$. Si $\#G = 1$ c'est clair, et on suppose maintenant le résultat pour tous les groupes abéliens d'ordre $< \#G$. Soit $x \in G$ d'ordre $\exp G$.

  Par hypothèse de récurrence, $G/\langle x\rangle \simeq \prod_{k=2}^{r} \mathbb{Z}_{n_k}$ avec $n_2|...|n_r$. Du coup, pour tout $i \geqslant 2$, il existe $y_i \in G$ tel que $\overline{y_i} \in G/\langle x\rangle$ soit d'ordre n_i.

  Soit $y \in G$ tel que $\overline{y} \in G/\langle x\rangle$ soit d'ordre n. Montrons qu'il existe $z \in G$ tel que $\overline{y} = \overline{z}$ et z est d'ordre n dans G. On a $\overline{y^n} = \overline{y}^n = \overline{1}$ donc $y^n \in \langle x\rangle$. Soit donc j tel que $y^n = x^j$. Soit m l'ordre de y dans G, alors $n \mid m$ et $\overline{0} = y^m = y^{n\frac{m}{n}} = x^{j\frac{m}{n}}$, donc $\exp(G)|j\frac{m}{n}$ puis $n|j$ (ceci car $m|\exp(G)$). On peut donc poser $z = yx^{-\frac{j}{n}}$, et on a alors bien $\overline{y} = \overline{z}$. Enfin, $z^n = y^n x^{-j} = \overline{1}$ donc en notant m' l'ordre de z, on a $m'|n$. Mais comme $\overline{z}$ est d'ordre n, on a aussi $n|m'$, donc z est d'ordre n.

  Ainsi, on peut supposer que pour tout $i \geqslant 2$, y_i est d'ordre n_i. On considère alors

  $$\begin{aligned} \Phi : \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_r} &\to G \\ \left(\overline{k_1}, ..., \overline{k_r}\right) &\to y_1^{k_1}...y_r^{k_r} \end{aligned}$$

  où $y_1 = x$ et $n_1 = \exp G$. On voit facilement que Φ est un morphisme. Φ est injectif : si $\Phi\left(\overline{k_1}, ..., \overline{k_r}\right) = 1$ alors dans $G/\langle x\rangle \simeq \prod_{k=2}^{r} \mathbb{Z}_{n_k}$, on a $\overline{y_2}^{k_2}...\overline{y_r}^{k_r} = \overline{1}$ donc $\overline{k_2} = ... = \overline{k_r} = \overline{0}$. Enfin, Φ est un isomorphisme par égalité des cardinaux au départ et à l'arrivée.
- Unicité : supposons qu'il existe deux suites finies d'entiers $(n_1, ..., n_r)$ et $(m_1, ..., m_s)$ vérifiant les propriétés voulues. Si $r = 1$, alors $n_1 = \exp G = m_s$ et $s = 1$. Si $r \geqslant 2$ alors $s \leqslant 2$. Pour tout entier $m \geqslant 1$, l'image du groupe $\prod_{k=1}^{r} \mathbb{Z}_{n_k} \simeq \prod_{k=1}^{s} \mathbb{Z}_{m_k}$ par le morphisme $\varphi_m : x \mapsto mx$ est le groupe $\prod_{k=1}^{r} \langle m_{\mathbb{Z}_{n_k}}\rangle \simeq \prod_{k=1}^{s} \langle m_{\mathbb{Z}_{m_k}}\rangle$. En passant au cardinal, on en déduit $\prod_{k=1}^{r} \frac{n_k}{m\wedge n_k} = \prod_{j=1}^{s} \frac{m_j}{m\wedge m_j}$ pour tout $m \geqslant 1$. Comme de plus $\prod_{k=1}^{r} n_k = \prod_{j=1}^{s} m_j$, on en déduit pour tout $m \geqslant 1$, $\prod_{k=1}^{r} m \wedge n_k = \prod_{j=1}^{s} m \wedge m_j$.

  En particulier pour $m = n_r$, on obtient $\prod_{k=1}^{r} n_k = \prod_{j=1}^{s} n_r \wedge m_j$, donc $\prod_{j=1}^{s} m_j = \prod_{j=1}^{s} n_r \wedge m_j$, ou encore $\prod_{j=1}^{s} \frac{m_j}{n_r\wedge m_j} = 1$. Comme tous les facteurs du produit sont dans $\mathbb{N}^*$, on en déduit $\forall j \in [\![1, s]\!], m_j = n_r \wedge m_j$. En particulier, $m_s = n_r \wedge m_s | n_r$. Symétriquement, $n_r \mid m_s$, donc $n_r = m_s$. Par récurrence, on en déduit le résultat.

■

Exemple 2.2.1: Les groupes abéliens d'ordre 200 sont $\mathbb{Z}_{200}$, $\mathbb{Z}_{100} \times \mathbb{Z}_2$, $\mathbb{Z}_{50} \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_{40} \times \mathbb{Z}_5$, $\mathbb{Z}_{20} \times \mathbb{Z}_{10}$ et $\mathbb{Z}_{10} \times \mathbb{Z}_{10} \times \mathbb{Z}_2$.

Exercice 2.2.7 (⋆): Soient G un groupe et e son élément neutre. On suppose que $\forall x \in G, x^2 = e$.

1) Montrer que G est abélien.
2) On suppose que G est fini et non trivial. Montrer que G est isomorphe à $((\mathbb{Z}/2\mathbb{Z})^n, +)$ pour un certain $n \in \mathbb{N}^*$.

Solution:

1) On a pour tout $x \in G$, $x = x^{-1}$. Soient $x, y \in G$, alors $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$. Ainsi G est abélien.
2) Par théorème, G est isomorphe à $\prod_{i=1}^{n} \mathbb{Z}/a_i\mathbb{Z}$. Tous les a_i sont égaux à 2, sinon on aurait un élément d'ordre > 2.

2.3. Suites de composition

Ici, G désigne un groupe.

Définition 2.3.1:

- On appelle suite de composition de G toute suite de sous-groupes
$$\{e\} = H_0 \leq H_1 \leq ... \leq H_{n-1} \leq H_n = G$$
telle que $\forall i, H_i \trianglelefteq H_{i+1}$.
- Deux suites de composition $(H_0, ..., H_n)$ et $(K_0, ..., K_m)$ de G sont dites équivalentes ssi $m = n$ et il existe $\sigma \in \mathfrak{S}_r$ telle que pour tout i, $H_{i+1}/H_i \simeq K_{\sigma(i)+1}/K_{\sigma(i)}$.
- Une suite de composition $(H_0, ..., H_n)$ est dite suite de Jordan-Hölder ssi pour tout i, H_{i+1}/H_i est simple.
- On dit que G est résoluble ssi il existe une suite de composition $(H_0, ..., H_n)$ telle que pour tout i, H_{i+1}/H_i est abélien.

Exemple 2.3.1:

- $\{\mathrm{id}\} \leq \mathfrak{A}_n \leq \mathfrak{S}_n$ est une suite de composition de $\mathfrak{A}_n$.
- $\{0\} \leq \langle 12\rangle \leq \langle 6\rangle \leq \langle 3\rangle \leq \mathbb{Z}_{60}$ et $\{0\} \leq \langle 20\rangle \leq \langle 4\rangle \leq \langle 2\rangle \leq \mathbb{Z}_{60}$ sont des suites de composition de $\mathbb{Z}_{60}$. De plus, ce sont des suites de Jordan-Hölder et elles sont équivalentes : on a $\mathbb{Z}_{60}/\langle 3\rangle \simeq \mathbb{Z}_3 \simeq \langle 20\rangle/\{0\}$, $\langle 3\rangle/\langle 6\rangle \simeq \mathbb{Z}_2 \simeq \langle 2\rangle/\langle 4\rangle$, $\langle 6\rangle/\langle 12\rangle \simeq \mathbb{Z}_2 \simeq \langle \mathbb{Z}_{60}\rangle/\langle 2\rangle$ et $\langle 12\rangle/\{0\} \simeq \mathbb{Z}_5 \simeq \langle 4\rangle/\langle 20\rangle$.
- Pour tout $n \in \mathbb{N}^*$, le groupe diédral D_n est résoluble. En effet, si r est une rotation d'angle $\frac{2\pi}{n}$ alors on a une suite de composition $\{e\} \leq \langle r\rangle \leq D_n$ avec $\langle r\rangle/\{e\} \simeq \langle r\rangle \simeq \mathbb{Z}/n\mathbb{Z}$ et $D_n/\langle r\rangle \simeq \mathbb{Z}/2\mathbb{Z}$.

Lemme 2.3.1: Toute suite de composition de G de longueur maximale est une suite de Jordan-Hölder.

En particulier, si G est fini alors G possède une suite de Jordan-Hölder.

Preuve: Supposons que G possède une suite de composition de G de longueur maximale $\{e\} = H_0 \leq H_1 \leq ... \leq H_n$.

Soit $i \in [\![0, n-1]\!]$, montrons que H_{i+1}/H_i est simple. Soit $K \trianglelefteq H_{i+1}/H_i$. Par le théorème de correspondance, il existe $N \trianglelefteq H_{i+1}$ tel que $K = N/H_i$. On a donc une suite de composition $H_0 \leq ... \leq H_i \leq N \leq H_{i+1} \leq ... \leq H_n$. Par maximalité de $H_0 \leq ... \leq H_n$, on en déduit $N = H_i$ ou $N = H_{i+1}$, donc H_{i+1}/H_i est simple. Ainsi $H_0 \leq ... \leq H_n$ est une suite de Jordan-Hölder.

Si G est fini alors G possède une suite de composition de longueur maximale (en effet, il y a toujours au moins une suite de composition, à savoir $\{e\} \leq G$), et cette suite est une suite de Jordan-Hölder d'après ce qui précède. ■

Exemple 2.3.2: $\mathbb{Z}$ ne possède pas de suite de Jordan-Hölder. En effet, supposons par l'absurde que $\mathbb{Z}$ possède une suite de Jordan-Hölder $\{e\} = H_0 \leq ... \leq H_n = \mathbb{Z}$. En particulier, $H_1 \simeq H_1/\{e\}$ est simple. Comme $H_1 \leq \mathbb{Z}$, on a $H_1 = m\mathbb{Z}$ pour un certain $m \in \mathbb{Z}$. Or $2m\mathbb{Z}$ est un sous-groupe normal non trivial de $m\mathbb{Z}$: absurde.

Théorème 2.3.1 (de Jordan-Hölder): Deux suites de Jordan-Hölder de G sont équivalentes.

Preuve: TODO ■

Remarque 2.3.1: Si G est fini alors d'après le théorème de Jordan-Hölder ainsi que le lemme précédent, les suites de Jordan-Hölder de G sont exactement le suites de composition de G de longueur maximale.

Exemple 2.3.3: Pour tout $n \geqslant 5$, le groupe symétrique $\mathfrak{S}_n$ n'est pas résoluble. En effet, $\mathfrak{A}_n$ est simple donc on a une suite de Jordan-Hölder $\{\mathrm{id}\} \leq \mathfrak{A}_n \leq \mathfrak{S}_n$. Du coup, toutes les suites de composition de $\mathfrak{S}_n$ sont de longueur $\leqslant 2$. La seule suite de longueur 1 est $\{\mathrm{id}\} = \mathfrak{S}_n$, or $\mathfrak{S}_n$ n'est pas abélien. Une suite de longueur 2 est une suite de Jordan-Hölder, donc est équivalente à $\{\mathrm{id}\} \leq \mathfrak{A}_n \leq \mathfrak{S}_n$, mais $\mathfrak{A}_n$ n'est pas abélien. Ainsi $\mathfrak{S}_n$ n'est pas résoluble.

2.4. Théorèmes de Sylow

Ici, G désigne un groupe fini.

Lemme 2.4.1: On suppose que G est d'ordre p^α où p est un nombre premier et $\alpha \in \mathbb{N}^*$.
1) $Z(G) \neq \{e\}$.
2) Si $\alpha = 1$ alors G est cyclique.
3) Si $\alpha = 2$ alors G est abélien.

Preuve:
1) Par la formule des classes, il existe une famille $(H_i)_{i\in I}$ de sous-groupes de G telle que $|Z(G)| = |G| - \sum_{i\in I} \frac{|G|}{|H_i|}$. Par le théorème de Lagrange, on a pour tout $i \in I$, $|H_i| = p^{m_i}$ avec $1 \leqslant m_i \leqslant \alpha - 1$. Donc $|Z(G)| = p^\alpha - \sum_{i\in I} p^{\alpha - m_i}$ est un multiple de p. Comme $|Z(G)| > 0$, on en déduit que $|Z(G)| \neq 1$ donc $Z(G) \neq e$.
2) Si $\alpha = 1$ alors G est cyclique par le théorème de Lagrange.
3) Si $\alpha = 2$ alors par le théorème de Lagrange, pour tout $i \in I$, $|H_i| = p$, donc $|Z(G)| = p^2 - p|I|$. Or $Z(G)$ est un sous-groupe de G non-réduit à $\{e\}$, donc $|Z(G)| = p$ ou $|Z(G)| = p^2$. On va montrer que $|Z(G)| = p^2$ (i.e. que G est abélien). Pour cela, on suppose par l'absurde que $|Z(G)| = p$. On dispose alors d'un élément $x \in G \setminus Z(G)$. Considérons l'ensemble $S_x = \{y \in G; xy = yx\}$, qui est un sous-groupe de G. Alors $|Z(G)| \subseteq S_x$, et l'inclusion est stricte car $x \in S_x \setminus Z(G)$. Du coup, par le théorème de Lagrange, $|S_x| = p^2$ i.e. $S_x = G$. Mais ceci est absurde car $x \notin Z(G)$. On en déduit que $|Z(G)| = p^2 = |G|$ i.e. G est abélien.

■

Théorème 2.4.1 (premier théorème de Sylow): Soient p un nombre premier et r un entier naturel tels que $p^r \mid \#G$. Alors G a un sous-groupe d'ordre p^r.

Preuve: On procède par récurrence forte sur $h := \#G$.
- Pour $h = 1$, c'est évident.
- Soit $h \geqslant 2$, supposons le résultat au rang $h - 1$. Par la formule des classes, on dispose d'une famille $(H_i)_{i\in I}$ de sous-groupes stricts de G tels que $\#G = \#Z(G) + \sum_{i\in I}[G : H_i]$.
  - Premier cas : p^r divise l'un des $\#H_i$. Alors par hypothèse de récurrence, H_i admet un sous-groupe d'ordre p^r, qui est aussi un sous-groupe de G.

- Deuxième cas : p^r ne divise aucun des H_i. Par la formule des classes, on voit que p^r divise $\#Z(G)$. Par le théorème de structure des groupes abéliens finis, $Z(G)$ admet un sous-groupe K d'ordre p, qui est distingué dans G (car inclus dans $Z(G)$). On dispose de la surjection canonique $\pi : G \to G/K$. Si $r = 0$, le résultat est évident et on suppose maintenant $r > 0$. Alors $\#G/K$ est divisible par p^r donc par hypothèse de récurrence, G/K admet un sous-groupe d'ordre p^r, noté H. En appliquant le premier théorème d'isomorphisme à $\pi|_{\pi^{-1}(H)}$, on obtient $\#\pi^{-1}(H) = \#H \times \#K = p^r$ donc $\pi^{-1}(H)$ est un sous-groupe de G d'ordre p^r.

■

Définition 2.4.1 : Soient p un facteur premier de $\#G$. On appelle p-sous-groupe de Sylow (ou p-Sylow) de G tout sous-groupe de G d'ordre p^r, où r est tel que $p^r \mid \#G$ et $p^{r+1} \nmid \#G$.

Remarque 2.4.1 : D'après le théorème précédent, G possède un p-sous-groupe de Sylow pour tout facteur premier p de $\#G$.

Exercice 2.4.1 (⋆) : Soit G un groupe d'ordre 18. Quels sont les ordres des sous-groupes de Sylow de G ?

Solution : $18 = 2 \times 3^2$ donc les sous-groupes de Sylow de G ont pour ordre 2 et 9.

Lemme 2.4.2 : Soient P un p-sous-groupe de Sylow de G et $x \in G$ un élément d'ordre p^k pour un certain entier naturel k. On suppose que $x^{-1}Px = P$. Alors $x \in P$.

Preuve : On a $x \in N_G(P) := \{g \in G; g^{-1}Pg = P\}$. On sait que $P \trianglelefteq N_G(P)$. On considère le sous-groupe de $N_G(P)/P$ engendré par xP. Par le théorème de correspondance, il existe $H \leq N_G(P)$ tel que $\langle xP \rangle = H/P$.

On sait que $\#P$ est une puissance de p. Il en est de même pour $\#\langle xP \rangle$, puisque l'ordre de xP divise celui de x. Donc $\#H = \#P\#\langle xP \rangle$ est également une puissance de p. Mais $P \leq H$ et P est un p-sous-groupe de Sylow, donc $P = H$, i.e. $x \in P$. ■

Lemme 2.4.3 : Soient $H, K \leq G$. Alors $\#\{h^{-1}Kh; h \in H\} = [H : N_G(K) \cap H]$.

Preuve : On a une bijection

$$\{h^{-1}Kh; h \in H\} \to \{(N_G(K) \cap H)h; h \in H\}$$
$$h^{-1}Kh \mapsto (N_G(K) \cap H)h$$

■

Théorème 2.4.2 (deuxième théorème de Sylow) : G agit transitivement par conjugaison sur l'ensemble des p-sous-groupes de Sylow de G.

Preuve : Soit P un p-sous-groupe de Sylow de G, alors on voit facilement que pour tout $g \in G$, $g^{-1}Pg$ est encore un p-sous-groupe de Sylow de G. On en déduit facilement que G agit par

conjugaison sur l'ensemble des p-sous-groupes de Sylow de G. Soient P et Q deux p-sous-groupes de Sylow de G. Montrons qu'il existe $g \in G$ tel que $g^{-1}Pg = Q$.

On écrit $\#P = p^r$ où $r \in \mathbb{N}$. Soit $S = \{g^{-1}Pg; g \in G\}$. On écrit $S = \{P_1, ..., P_k\}$ où $P = P_1$ et les P_i sont distincts. Par le lemme précédent, $k = \#S = [G : N_G(P)]$. Comme $P \leqslant N_G(P)$, on a par le théorème de Lagrange $p^r \mid \#N_G(P)$. De plus $\#G = [G : N_G(P)]\#N_G(P) = k\#N_G(P)$ donc $p \nmid k$ (sinon on aurait $p^{r+1} \mid \#G$).

Soit $S_i = \{g^{-1}P_ig; g \in Q\}$. Alors on vérifie facilement que les S_i forment une partition de S. Par le lemme précédent, $\#S_i = [Q : N_G(P_i) \cap Q]$. Or $p^r = \#Q = [Q : N_G(P_i) \cap Q]\#N_G(P_i) \cap Q$, donc $\#S_i$ est une puissance de p. Mais la somme de $\#S_i$ vaut k et $p \nmid k$, donc il existe j tel que $\#S_j = 1$, i.e. $\forall g \in Q, g^{-1}P_jg = P_j$. Par le Lemme 2.4.2, $Q \subseteq P_j$, puis $Q = P_j$ par égalité des cardinaux. D'où le résultat. ■

Théorème 2.4.3 (troisième théorème de Sylow) : Soit n_p le nombre de p sous-groupes de Sylow de G. Alors $n_p \equiv 1 \bmod p$ et $n_p \mid \#G$.

Preuve : Soit P un p-sous-groupe de Sylow de G. Soit $S = \{P_1 = P, P_2, ..., P_k\}$ l'ensemble des p-sous-groupes de Sylow de G. Alors il est clair que P agit sur S par conjugaison.

Par la formule des classes, $k = \#S = \#S_P + \#O_{P_{i_1}} + ... + \#O_{P_{i_n}}$ où $S_P = \{P_i; \forall g \in P, g^{-1}P_ig = P_i\}$. Avec les notations de la preuve précédente, S_P est l'ensemble des S_i de cardinal 1. Mais on a vu dans la preuve précédente qu'un tel S_i vaut P, donc $S_P = \{P\}$. De plus, par la formule orbite stabilisateur, les cardinaux des orbites sont des puissances de p (différentes de 1). La formule des classes donne alors $k = 1 + p\alpha$ où $\alpha \in \mathbb{N}$, donc $n_p = k \equiv 1 \bmod p$.

Par le deuxième théorème de Sylow, $S = \{g^{-1}Pg; g \in G\}$, puis par le lemme précédent, $n_p = \#S = [G : N_G(P)]$. Ainsi $n_p \mid \#G$. ■

Exercice 2.4.2 (⋆) : Déterminer tous les 3-sous-groupes de Sylow de $\mathfrak{S}_4$.

Solution : Comme $3 \mid \#\mathfrak{S}_4 = 24$ et $3^2 \nmid \#\mathfrak{S}_4$, les 3-sous-groupes de Sylow de $\mathfrak{S}_4$ sont d'ordre 3. Ainsi, $\langle(1\ 2\ 3)\rangle$, $\langle(1\ 2\ 4)\rangle$, $\langle(1\ 3\ 4)\rangle$ et $\langle(2\ 3\ 4)\rangle$ sont des 3-sous-groupes de Sylow.

D'après le troisième théorème de Sylow, le nombre de 3-sous-groupes de Sylow de $\mathfrak{S}_4$ est congru à 1 modulo 3 et divise 24, donc vaut 1 ou 4. Il y en a donc exactement 4, et ils sont décrits ci-dessus.

Lemme 2.4.4 : Si G possède un unique p-sous-groupe de Sylow alors celui-ci est normal dans G.

Preuve : Clair par le deuxième théorème de Sylow. ■

Lemme 2.4.5 : On suppose que $\#G = pq$ où $p < q$ sont deux nombres premiers. Alors :
- G possède un sous-groupe normal d'ordre q ;
- si de plus $q \not\equiv 1 \bmod p$ alors G est cyclique.

Preuve :

- Par le troisième théorème de Sylow, $n_q \equiv 1 \bmod q$ et $n_q \mid pq$, donc $n_q \mid p$. Ainsi, $n_q \in \{1, 1+q, 1+2q, \ldots\}$ et $n_q \in \{1, p\}$. Comme $p < q$, on a $n_q = 1$. Soit donc Q l'unique q-sous-groupe de Sylow de G. Par le lemme précédent, $Q \trianglelefteq G$.
- Supposons $q \not\equiv 1 \bmod p$. Comme ci-dessus, on a $n_p \equiv 1 \bmod p$ et $n_p \in \{1, q\}$, donc $n_p = 1$. Ainsi $P \trianglelefteq G$.

  Or $P \cap Q = \{e\}$ car l'ordre de tout élément de $P \cap Q$ divise p et q. Par la formule du produit, $\#PQ = pq = \#G$. Ainsi $G = PQ$.

  Soient x et y des générateurs de P et Q respectivement. Comme P est normal, on a $y^{-1}xy \in P$, puis $x^{-1}y^{-1}xy \in P$. De même, $x^{-1}y^{-1}xy \in Q$, donc $x^{-1}y^{-1}xy = e$ puis $xy = yx$. On en déduit que $G = PQ \simeq P \times Q \simeq \mathbb{Z}_p \times \mathbb{Z}_q \simeq \mathbb{Z}_{pq}$ par le théorème chinois.

■

Exemple 2.4.1: On en déduit par exemple que tout groupe d'ordre 15 est cyclique.

Exemple 2.4.2: Soit G un groupe d'ordre $99 = 9 \times 11$.

On a $n_3 \equiv 1 \bmod 3$ et $n_3 \mid 11$ donc $n_3 = 1$. Ainsi G possède un unique 3-Sylow N, qui est normal dans G. Il est d'ordre $9 = 3^2$, donc abélien, donc isomorphe à $\mathbb{Z}_3 \times \mathbb{Z}_3$ ou à $\mathbb{Z}_9$. De même, on a $n_{11} \equiv 1 \bmod 11$ et $n_{11} \mid 9$ donc $n_{11} = 1$. Ainsi G possède un unique 11-Sylow M, qui est normal et isomorphe à $\mathbb{Z}_{11}$.

On a $M \cap N = \{e\}$ (l'ordre de tout élément de $M \cap N$ divise 9 et 11), donc par la formule du produit, $\#MN = \#M\#N = 99$. Ainsi $G = MN$.

Soient $m \in M$ et $n \in N$. Comme M est normal, on a $n^{-1}mn \in M$ puis $m^{-1}n^{-1}mn \in M$. De même, $m^{-1}n^{-1}mn \in N$, donc $m^{-1}n^{-1}mn \in M \cap N = \{e\}$, i.e. $mn = nm$. Du coup, G est isomorphe à $M \times N$.

Finalement, les groupes d'ordre 99 sont (à isomorphisme près) $\mathbb{Z}_{11} \times \mathbb{Z}_9$ et $\mathbb{Z}_{11} \times \mathbb{Z}_3 \times \mathbb{Z}_3$.

Exemple 2.4.3: Soit G un groupe d'ordre $56 = 2^3 \times 7$. Montrons que G n'est pas simple.

On a $n_2 \equiv 1 \bmod 2$ et $n_2 | 7$ donc $n_2 \in \{1, 7\}$. De même, $n_7 \equiv 1 \bmod 7$ et $n_7 | 8$ donc $n_7 \in \{1, 8\}$.

Si $n_7 = 1$ alors l'unique 7-Sylow de G est normal, donc G n'est pas simple.

On suppose maintenant $n_7 = 8$. Les éléments d'ordre 7 sont exactement les éléments des 7-Sylow de G, sauf e. Or l'intersection de deux 7-Sylow distincts de G vaut toujours $\{e\}$: un élément dans l'intersection est d'ordre 1 ou 7, mais s'il est d'ordre 7, alors les deux 7-Sylow sont les mêmes. Il y a donc $6 \times 8 = 48$ éléments de G d'ordre 7, et $56 - 48 = 8$ éléments d'ordre 1, 2, 4, 8 ou 56. Donc G possède un seul 2-Sylow, formé par les 8 éléments en question. Ce 2-Sylow est donc normal, ce qui conclut.

Exemple 2.4.4: Soit G un groupe d'ordre $6545 = 5 \times 7 \times 11 \times 17$. Montrons que G n'est pas simple.

On a $n_5 \equiv 1 \bmod 5$ et $n_5 | 7 \times 11 \times 17$, donc $n_5 \in \{1, 11\}$. De même, on trouve $n_7 \in \{1, 85\}$, $n_{11} \in \{1, 595\}$ et $n_{17} \in \{1, 35\}$.

Supposons par l'absurde que G n'est pas simple, alors $n_5 = 11$, $n_7 = 85$, $n_{11} = 595$ et $n_{17} = 35$.

En raisonnant comme dans l'exemple précédent, on voit que G possède exactement $11 \times 4 = 44$ éléments d'ordre 5, $85 \times 6 = 510$ éléments d'ordre 7, $595 \times 10 = 5950$ éléments d'ordre 11 et $35 \times 16 = 560$ éléments d'ordre 17. Mais $44 + 510 + 5950 + 560 > 6545$: absurde.

Lemme 2.4.6 : On suppose que G possède un sous-groupe $H \neq G$ tel que $[G : H]! < \#G$. Alors G n'est pas simple.

Preuve : G agit sur $G/R_H^G = \{xH ; x \in G\}$ par $g \cdot xH = gxH$. On a donc un morphisme de groupes $\varphi : G \to \mathfrak{S}(G/R_H^G)$, et $\ker \varphi$ est un sous-groupe normal de G. On a $\ker \varphi \neq \{e\}$ puisque $[G : H]! < \#G$. De plus, si $\ker \varphi = G$ alors pour tous $g, x \in G$, on a $gxH = xH$. En particulier pour $x = e$, on obtient $\forall g \in G, gH = H$ donc $H = G$, ce qui est absurde. Ainsi $\ker \varphi$ est un sous-groupe normal non trivial de G, donc G n'est pas simple. ■

Exemple 2.4.5 : Soit G un groupe d'ordre $48 = 2^3 \times 3$. Par le premier théorème de Sylow, G possède un 2-Sylow H. On a $[G : H]! = 6 < \#G$ donc par le Lemme 2.4.6, G n'est pas simple.

Exercice 2.4.3 (⋆) : Montrer qu'il n'existe pas de groupe simple d'ordre 21, 24, 35, 36, 45, 63 et 105.

Solution :

- Soit G un groupe d'ordre $21 = 3 \times 7$. Par le Lemme 2.4.5, G possède un sous-groupe normal d'ordre 7.
- Soit G un groupe d'ordre $24 = 2^3 \times 3$. Alors G possède un 2-Sylow d'ordre 8, et le Lemme 2.4.6 permet de conclure.
- Soit G un groupe d'ordre $35 = 5 \times 7$. Par le Lemme 2.4.5, G possède un sous-groupe normal d'ordre 7.
- Soit G un groupe d'ordre $36 = 2^2 \times 3^2$. Alors G possède un 3-Sylow d'ordre 9, et le Lemme 2.4.6 permet de conclure.
- Soit G un groupe d'ordre $45 = 3^2 \times 5$. On a $n_3 \equiv 1 \bmod 3$ et $n_3 | 5$ donc $n_3 = 1$: G possède un unique 3-Sylow, qui est normal.
- Soit G un groupe d'ordre $63 = 3^2 \times 7$. On a $n_7 \equiv 1 \bmod 7$ et $n_7 | 9$ donc $n_7 = 1$: G possède un unique 7-Sylow, qui est normal.
- Soit G un groupe d'ordre $105 = 3 \times 5 \times 7$. On a $n_3 \equiv 1 \bmod 3$ et $n_3 | 35$ donc $n_3 \in \{1, 7\}$. De même, $n_5 \equiv 1 \bmod 5$ et $n_5 | 21$ donc $n_5 \in \{1, 21\}$; et $n_7 \equiv 1 \bmod 7$ et $n_7 | 15$ donc $n_7 \in \{1, 15\}$. Supposons par l'absurde que G ne soit pas simple, alors $n_3 = 7$, $n_5 = 21$ et $n_7 = 15$. Donc G possède $7 \times 2 = 14$ éléments d'ordre 3, $21 \times 4 = 84$ éléments d'ordre 5 et $15 \times 6 = 90$ éléments d'ordre 7. On obtient plus de 105 éléments : absurde.

2.5. Groupe symétrique

Définition 2.5.1 : Groupes de permutations $S(E)$, groupes symétriques S_n

Définition 2.5.2 : Cycle, transposition, support

Lemme 2.5.1 : La longueur d'un cycle est son ordre dans S_n.

Lemme 2.5.2 : Deux cycles à supports disjoints commutent.

Définition 2.5.3 : Orbite $O_\sigma(x) = \{\sigma^k(x); k \in \mathbb{Z}\}$ (c'est l'orbite de x pour l'action naturelle de $\langle\sigma\rangle$ sur $[\![1,n]\!]$)

Lemme 2.5.3 : $\sigma(a_1 \ \dots \ a_p)\sigma^{-1} = (\sigma(a_1) \ \dots \ \sigma(a_p))$

Exercice 2.5.1 (⋆) : Soit $\sigma \in S_n \setminus \{\mathrm{id}\}$ où $n \geqslant 3$. Montrer qu'il existe $\tau \in S_n$ qui ne commute pas avec σ.

Solution : Comme $\sigma \neq \mathrm{id}$, on dispose de $i_0 \in [\![1,n]\!]$ tel que $\sigma(i_0) \neq i_0$. Soient $j_0 \in [\![1,n]\!] \setminus \{i_0, \sigma(i_0)\}$ (qui existe car $n \geqslant 3$), puis $\tau = (\sigma(i_0) \ \ j_0)$. Alors $\sigma\tau(i_0) = \sigma(i_0) \neq j_0 = \tau\sigma(i_0)$ donc τ ne commute pas avec σ.

Théorème 2.5.1 : Toute permutation se décompose en un produit de cycle à supports disjoints, de manière unique à l'ordre près des facteurs. De plus, dans une telle décomposition, l'ordre de la permutation est le PPCM des ordres des cycles.

Preuve :

- Existence. Soit $\sigma \in S_n$. On suppose $\sigma \neq \mathrm{id}$ (sinon c'est évident). Soient $O_1, \dots, O_p, \dots, O_r$ les orbites distinctes de σ, avec $|O_k| \geqslant 2$ pour $k \leqslant p$ et $|O_k| = 1$ pour $k > p$. Pour tout $k \in [\![1,p]\!]$, on pose $\gamma_k : \begin{cases} [\![1,n]\!] \to [\![1,n]\!] \\ x \quad \mapsto \begin{cases} \sigma(x) \text{ si } x \in O_k \\ x \quad \text{sinon} \end{cases} \end{cases} \in S_n$. Alors γ_k est un cycle de longueur $|O_k|$.

  Montrons que $\sigma = \prod_{j=1}^{p} \gamma_j$. Soit $x \in E$, soit donc k l'unique indice tel que $x \in O_k$. Si $k > p$ alors $\sigma(x) = x = \left(\prod_{j=1}^{p} \gamma_j\right)(x)$. Sinon, on a $\gamma_k(x) = \sigma(x)$ et $\gamma_j(x) = x$ pour $j \neq k$. Comme les γ_j commutent, on a $\left(\prod_{j=1}^{r} \gamma_j\right)(x) = \left(\gamma_k \prod_{j \neq k} \gamma_j\right)(x) = \gamma_k(x) = \sigma(x)$.
- Unicité. Si $\sigma = \prod_{k=1}^{p} \gamma_k$ avec $\gamma_1, \dots, \gamma_k$ des cycles à supports disjoints, alors les supports des γ_k sont exactement les orbites non réduites à un point de σ, donc les supports des γ_k sont uniques à l'ordre près des facteurs. En bidouillant, on voit que si deux cycles de deux décompositions de σ ont le même supports, ils sont égaux.
- Ordre d'une permutation. On garde les mêmes notations, et on note $\theta_1, \dots, \theta_p$ les ordres de $\gamma_1, \dots, \gamma_p$. Soit $k \in \mathbb{Z}$ tel que $\sigma^k = \mathrm{id}$. Soit $j \in [\![1,p]\!]$, alors pour tout $x \in O_j$, $\gamma_j^k(x) = \sigma(x) = x$, et pour tout $x \notin O_j$, $\gamma_j^k(x) = x$. Donc $\gamma_j^k = \mathrm{id}$, et donc $\theta_j | k$. Ceci vaut pour tout j, donc $\mathrm{ppcm}(\theta_1, \dots, \theta_p) | k$. Réciproquement, si $\mathrm{ppcm}(\theta_1, \dots, \theta_p) | k$ alors $\sigma^k = \mathrm{id}$. Ainsi σ est d'ordre $\mathrm{ppcm}(\theta_1, \dots, \theta_p)$.

■

Théorème 2.5.2 :

1) Les transpositions de la forme $(i \ \ i{+}1)$ où $i \in [\![1, n-1]\!]$ engendrent S_n.
2) Les transpositions de la forme $(1 \ \ i)$ où $i \in [\![2, n]\!]$ engendrent S_n.

Preuve: Montrons d'abord que les transpositions engendrent S_n. Soit $\sigma \in S_n$. σ s'écrit comme produit de cycles, et un cycle se décompose en produit de transpositions : $(a_1 \ \dots \ a_p) = (a_1 \ a_2)\dots(a_{p-1} \ a_p)$, d'où le résultat.

1) Comme les transpositions engendrent S_n, il suffit de montrer que toute transposition s'écrit comme produit de transpositions de la forme $(i \ i{+}1)$. Soit $\tau = (i \ j)$ une transposition, avec $i < j$.

   Montrons le résultat par récurrence sur $j - i$. Si $j - i = 1$ c'est évident. Soit $k \in [\![1, n-2]\!]$, supposons le résultat pour les transpositions de la forme $(l \ l{+}k)$ et supposons $j - i = k + 1$. Alors $(i \ j) = (i \ j{-}1)(j{-}1 \ j)(i \ j{-}1)$. Par hypothèse, $(i \ j{-}1)$ s'écrit comme produit de transpositions de la forme souhaitée, d'où le résultat.
2) On procède de même. On a $(i \ j) = (1 \ i)(1 \ j)(1 \ i)$ si $i \neq j$, et c'est clair si $i = j$.

■

Exercice 2.5.2 (⋆ ⋆): Montrer que pour tout entier $n \geqslant 3$, S_n est engendré par $(1 \ 2)$ et $(2 \ 3 \ \dots \ n)$.

Solution: Pour tout $i \in [\![2, n]\!]$, $(1 \ i) = (2 \ 3 \ \dots \ n)^{i-2}(1 \ 2)(2 \ 3 \ \dots \ n)^{-(i-2)}$. Comme les $(1 \ i)$ engendrent S_n, c'est gagné.

Exercice 2.5.3 (⋆ ⋆ ⋆): Soit $n \geqslant 2$ un entier.

1) Soit $\sigma \in S_n$ tel que $\sigma^2 = \mathrm{id}$. Dénombrer les éléments de S_n qui commutent avec σ.
2) On suppose $n \neq 6$. Soit Φ un automorphisme de $(S_n, \circ)$.
   a) Montrer que Φ envoie une transposition quelconque sur une transposition.
   b) En déduire que Φ est intérieur, i.e. du type $\sigma \mapsto s\sigma s^{-1}$ avec $s \in S_n$.

Solution:

1) On suppose $\sigma \neq \mathrm{id}$ (sinon il y a $n!$ éléments de S_n qui commutent avec σ). On écrit $\sigma = c_1 \dots c_k$ avec $c_1, \dots, c_k$ des cycles à supports disjoints. L'ordre de σ vaut au plus 2, et c'est aussi le PPCM ordres des c_i. Les c_i sont donc des transpositions à supports disjoints.

Soit $\tau \in S_n$ qui commute avec σ. On a $\sigma = \tau\sigma\tau^{-1} = (\tau c_1 \tau^{-1}) \dots (\tau c_k \tau^{-1})$ où les $\tau c_i \tau^{-1}$ sont des transpositions à supports disjoints. Par unicité de la décomposition en produit de cycles à supports disjoints, les $\tau c_i \tau^{-1}$ s'obtiennent par permutation des c_i, soit $k!$ possibilités.

Supposons l'une de ces permutations fixées, et considérons une transposition $c_i = (a \ b)$. Alors $(a' \ b') := \tau c_i \tau^{-1} = (\tau(a) \ \tau(b))$, donc $\{a', b'\} = \{\tau(a), \tau(b)\}$. Il y a donc 2 possibilités pour définir τ sur $\{a, b\}$. Au total, ça fait 2^k possibilités pour définir τ sur l'union des supports des c_i.

Il reste à définir τ sur les points fixes de σ. L'image d'un point fixe de σ par τ est un point fixe de σ, donc il y a $(n-2k)!$ possibilités.

Finalement, il y a $2^k k!(n-2k)!$ éléments de S_n qui commutent avec σ.

1) a) Soit $\sigma \in S_n$ une transposition. D'après ce qui précède, il y a $2(n-2)!$ permutations qui commutent avec σ. De plus $\Phi(\sigma)^2 = \Phi(\sigma^2) = \mathrm{id}$. On écrit $\Phi(\sigma) = c_1 \dots c_k$ avec $c_1, \dots, c_k$ des transpositions à supports disjoints, et il y a alors $2^k k!(n-2k)!$ permutations qui

commutent avec $\Phi(\sigma)$. Or Φ définit une bijection évidente entre le centralisateur de σ et celui de $\Phi(\sigma)$, donc $2(n-2)! = 2^k k!(n-2k)!$. Déduisons-en que $k = 1$.

On a $2^{k-1} = \frac{(n-2)!}{k!(n-2k)!} = \binom{n-k}{k}\frac{(n-2)!}{(n-k)!}$. Si $k \geqslant 3$ alors les entiers $n-2, n-3, ..., n-k+1$ sont consécutifs et tous pairs, donc il y en a un seul, i.e. $k = 3$. Mais on voit que ce cas est impossible, tout comme le cas $k = 2$. Donc $k = 1$, i.e. $\Phi(\sigma)$ est une transposition.

b) On montre par récurrence sur i qu'il existe $a_1, ..., a_n \in [\![1, n]\!]$ deux à deux distincts tels que $\Phi((1\ \ i)) = (a_1\ \ a_i)$. On a alors $\Phi : \sigma \mapsto s\sigma s^{-1}$ où $s : i \mapsto a_i$ car les $(1\ \ i)$ engendrent S_n.

Exercice 2.5.4 (⋆ ⋆ ⋆ ♥): Trouver les fonctions $f : \mathbb{Z} \to \mathbb{Z}$ telles que $\forall n \in \mathbb{Z}, f(f(n)) = n + 2023$.

Solution: Notons $a = 2023$. Soit $f : \mathbb{Z} \to \mathbb{Z}$ telle que $\forall n \in \mathbb{Z}, f(f(n)) = n + a$. Soit $n \in \mathbb{Z}$, alors $f(n + a) = f(f(f(n))) = f(n) + a$. Ainsi la valeur de $f(n)$ modulo a dépend uniquement de la valeur de n modulo a. On peut donc définir

$$\overline{f} : \begin{cases} \mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \\ \overline{n} \quad\quad \mapsto \overline{f(n)} \end{cases}$$

et on a alors $\overline{f} \circ \overline{f} = \mathrm{id}$, donc $\overline{f}$ est bijective. On peut donc voir $\overline{f}$ comme un élément de S_a.

On écrit $\overline{f}$ comme un produit de cycles à supports disjoints : $\overline{f} = c_1 \circ c_2 \circ ... \circ c_k$. Alors $\mathrm{id} = \overline{f} \circ \overline{f} = c_1^2 \circ c_2^2 \circ ... \circ c_k^2$ car les cycles à supports disjoints commutent. Par unicité de la décomposition en cycles à supports disjoints, on a pour tout i, $c_i^2 = \mathrm{id}$, donc c_i est une transposition. Il y a donc un nombre pair d'éléments qui ne sont pas laissés fixes par $\overline{f}$ (ce sont les éléments des supports des c_i). Mais a est impair donc $\overline{f}$ admet (au moins) un point fixe $\overline{b}$.

On a $\overline{f(b)} = \overline{b}$ donc il existe $k \in \mathbb{Z}$ tel que $f(b) = b + ka$. On a alors $b + a = f(f(b)) = f(b + ka) = f(b) + ka = b + 2ka$ donc $2k = 1$, ce qui est absurde. Il n'existe donc pas de telle fonction (et le résultat reste vrai en remplaçant 2023 par n'importe quel entier impair).

Définition 2.5.4: $\varepsilon(\sigma) = (-1)^{n-\mu(\sigma)}$ où $\mu(\sigma)$ est le nombre d'orbites

Lemme 2.5.4:
- $\varepsilon(\mathrm{id}) = 1$.
- Si σ est un r-cycle alors $\varepsilon(\sigma) = (-1)^{r-1}$.

Lemme 2.5.5: Si $\sigma \in S_n$ et τ est une transposition alors $\varepsilon(\tau\sigma) = -\varepsilon(\sigma)$.

Preuve: Très laborieux, distinguer dans quelles orbites de σ sont les deux éléments de $\mathrm{Supp}(\tau)$.
■

Théorème 2.5.3 : ε est l'unique morphisme non constant de S_n dans $\mathbb{R}^*$.

Preuve : ε est un morphisme par le lemme précédent et il est bien non constant de S_n dans $\mathbb{R}^*$. Soit φ un morphisme non constant de S_n dans $\mathbb{R}^*$. Soient $\tau_1 = (\alpha\ \ \beta)$ et $\tau_2 = (\gamma\ \ \delta)$ deux transpositions, et $\sigma \in S_n$ telle que $\sigma(\alpha) = \gamma$ et $\sigma(\beta) = \delta$. Alors $\sigma\tau_1\sigma^{-1} = (\sigma(\alpha)\ \ \sigma(\beta)) = \tau_2$, puis $\varphi(\tau_1) = \varphi(\sigma)\varphi(\tau_1)\varphi(\sigma^{-1}) = \varphi(\tau_2)$. Ainsi φ est constant sur les transpositions. Comme celles-ci engendrent S_n et que φ est non constant, on a $\varphi(\tau) = -1$ pour toute transposition τ. Soit $\sigma \in S_n$. Si on écrit σ comme produit de p transpositions, alors $\varphi(\sigma) = (-1)^p = \varepsilon(\sigma)$. ■

Lemme 2.5.6 : $\varepsilon(\sigma) = \prod_{i<j} \frac{\sigma(j)-\sigma(i)}{j-i}$

Preuve : $\sigma \mapsto \prod_{i<j} \frac{\sigma(j)-\sigma(i)}{j-i}$ est un morphisme non constant de S_n dans $\mathbb{R}^*$. ■

Définition 2.5.5 : $A_n = \ker \varepsilon$

Lemme 2.5.7 : $|A_n| = \frac{n!}{2}$

Preuve : Premier théorème d'isomorphisme ! ■

Exercice 2.5.5 :

1) Soit $n \geqslant 3$ un entier. Montrer que les cycles de longueur 3 engendrent A_n.
2) Soient p un nombre premier, et H un sous-groupe de S_p tel que $[G : H] \leqslant p - 1$.
   a) Montrer que H contient tous les cycles de longueur p.
   b) Montrer que $H = S_p$ ou $H = A_p$.

Solution :

1) Déjà, le sous-groupe engendré par les cycles de longueur 3 est inclus dans A_n. Soit $\sigma \in A_n$. On peut écrire $\sigma = \tau_1 ... \tau_{2k}$ où $\tau_1, ..., \tau_{2k}$ sont des transpositions (il y en a un nombre pair car $\varepsilon(\sigma) = 1$ et $\varepsilon(\tau_i) = -1$). Soit $i \in [\![1, 2k]\!]$ un entier impair. On écrit $\tau_i = (a\ \ b)$ et $\tau_{i+1} = (c\ \ d)$.

- Si τ_i et τ_{i+1} sont à supports disjoints alors $\tau_i\tau_{i+1} = (a\ \ d\ \ c)(a\ \ b\ \ c)$.
- Si les supports de τ_i et τ_{i+1} ont un élément en commun, disons $a = c$, alors $\tau_i\tau_{i+1} = (a\ \ d\ \ b)$.
- Si les supports de τ_i et τ_{i+1} sont les mêmes alors $\tau_i\tau_{i+1} = \mathrm{id}$.

Ainsi, dans tous les cas, $\tau_i\tau_{i+1}$ s'écrit comme un produit de cycles de longueur 3, donc σ aussi, ce qui montre que les cycles de longueur 3 engendrent A_n.

1) a) Soit $\gamma \in S_p$ un cycle de longueur p. Les $\gamma^i H$ pour $i \in [\![0, p-1]\!]$ sont de cardinal $|H| \geqslant \frac{p!}{p-1}$, donc ils ne peuvent pas être deux à deux disjoints. Soient donc $0 \leqslant i < j \leqslant p-1$ tels que $\gamma^i H \cap \gamma^j H \neq \emptyset$. Soient donc $h_1, h_2 \in H$ tels que $\gamma^i h_1 = \gamma^j h_2$. Alors $\gamma^{j-i} = h_1 h_2^{-1} \in H$. Or $j - i \wedge p = 1$, donc γ^{j-i} est un générateur de $\langle\gamma\rangle$. En particulier, $\gamma \in \langle\gamma^{j-i}\rangle \subseteq H$.
   b) Soit $(i\ \ j\ \ k)$ un cycle de longueur 3. Si $p > 3$, soient $a_1, ..., a_{p-3}$ les entiers distincts de $[\![1, p]\!] \setminus \{i, j, k\}$. Alors $(i\ \ j\ \ k) = (i\ \ k\ \ j\ \ a_1\ \ ...\ \ a_{p-3})(j\ \ i\ \ k\ \ a_{p-3}\ \ ...\ \ a_1) \in H$. Comme les 3-cycles engendrent A_p, on en déduit que A_p est un sous-groupe de H, d'où le résultat.

Si $p = 2$ alors $[G : H] \leqslant 1$ donc $G = H$ et si $p = 3$ alors H contient les 3-cycles, donc contient A_3 et on a le résultat.

2.6. Groupes d'isométries des polytopes réguliers

Définition 2.6.1 : Soit E un espace affine de dimension finie. On note $\mathrm{Iso}(E)$ l'ensemble des isométries affines de E (applications de la forme $X \mapsto AX + B$ où A est une matrice orthogonale). On a $\mathrm{Iso}(E) = \mathrm{Iso}^+(E) \cup \mathrm{Iso}^-(E)$.

Remarque 2.6.1 : $\mathrm{Iso}(E)$ agit canoniquement sur E par $\varphi \cdot A = \varphi(A)$.

Remarque 2.6.2 :
- Une application affine conserve le barycentre.
- Une application affine d'un espace affine E de dimension n est déterminée par l'image de $n + 1$ points qui engendrent E.
- Si $\mathcal{P}$ est le plan euclidien alors on peut décrire $\mathrm{Iso}(\mathcal{P})$: si $\varphi \in \mathrm{Iso}(\mathcal{P})$ possède :
  - 0 point fixe alors φ est une translation ou une symétrie glissée
  - 1 unique point fixe alors φ est une rotation
  - 2 points fixes alors φ est une symétrie orthogonale par rapport à la droite passant par ces deux points
  - 3 points fixes non alignés alors $\varphi = \mathrm{id}$.

Définition 2.6.2 : Soit E un $\mathbb{R}$-espace affine de dimension n. Soit $X \subseteq E$. On note $G_X = \{\varphi \in \mathrm{Iso}(E); \varphi(X) = X\}$, qui est un sous-groupe de $\mathrm{Iso}(E)$.

Définition 2.6.3 : Si X est un polygone régulier à n côtés dans le plan alors G_X est appelé groupe diédral D_n.

Remarque 2.6.3 :
- Comme une application affine conserve le barycentre, le centre du polygone est fixé par tout élément de D_n. D_n ne contient donc pas de translation ni de symétrie glissée.
- Un élément de $\varphi \in D_n$ envoie toujours un sommet du polygone sur un autre sommet. En effet, si A et B sont deux sommets dont la distance est maximale, alors $d(\varphi(A), \varphi(B))$ vaut cette même distance, donc $\varphi(A)$ et $\varphi(B)$ sont des sommets.

Lemme 2.6.1 : Notons $G_X^+ = G_X \cap \mathrm{Iso}^+(E)$ et $G_X^- = G_X \cap \mathrm{Iso}^-(X)$. Si $s \in G_X^-$ alors $G_X = G_X^+ \cup G_X^+ s$.

Preuve : On a $G_X = G_X^+ \cup G_X^-$. Soit $\psi \in G_X^-$, alors $\psi = (\psi s^{-1})s$ avec $\psi s^{-1} \in G_X^+$. ■

Lemme 2.6.2 : $D_n^+ = \{\mathrm{id}, r, ..., r^{n-1}\}$ où r est la rotation de centre O et d'angle $\frac{2\pi}{n}$.

Preuve : Déjà, on a clairement $\{\mathrm{id}, r, ..., r^{n-1}\} \subseteq D_n^+$. Considérons l'action de D_n^+ sur l'ensemble S des sommets du polygone. Soit $A \in S$, alors $O_A = S$. Soit $\varphi \in S_A$. Comme

$\varphi(O) = O$ et que φ n'est pas une symétrie, on a $\varphi = \mathrm{id}$. Par la formule orbite-stabilisateur, $|D_n^+| = |O_A| \times |S_A| = n$, d'où le résultat. ■

Théorème 2.6.1 : $D_n = \{\mathrm{id}, r, ..., r^{n-1}, s, rs, ..., r^{n-1}s\}$ où s est une symétrie axiale passant par le centre et un sommet de polygone, et r est une rotation de centre le centre du polygone et d'angle $\frac{2\pi}{n}$.

Preuve : C'est clair par les deux lemmes précédents. ■

Théorème 2.6.2 : Tout sous-groupe fini de $\mathrm{Iso}(\mathcal{P})$ est cyclique ou diédral.

Preuve : Soit G un sous-groupe fini de $\mathrm{Iso}(\mathcal{P})$. Notons $n = |G^+|$.

- Si $n = 1$ alors $G^+ = \mathrm{id}$ donc par un lemme précédent, $G = \{\mathrm{id}\}$ ou $G = \{\mathrm{id}, s\}$ avec $s \in G^-$. Dans les deux cas, G est cyclique.
- Supposons maintenant $n \geqslant 2$. Il existe un point A tel que $|O_A| > 1$ (où O_A est l'orbite pour l'action canonique de G^+). Notons O le barycentre des points de O_A. Soit $\psi \in G^+$, alors $\psi(O)$ est le barycentre de $\psi(O_A) = O_A$, donc $\psi(O) = O$. Comme ψ admet un point fixe et est positif, c'est une rotation de centre O. Notons r la rotation de centre O et d'angle $\frac{2\pi}{n}$. On a $\psi^n = \mathrm{id}$ donc $\psi \in \langle r \rangle$. Ainsi $G^+ \subseteq \langle r \rangle$ puis $G^+ = \langle r \rangle$ par égalité des cardinaux. Si $G = G^+$ alors G est cyclique. Sinon, soit $s \in G^-$. Alors $s^{-1}rs \in G^+$ donc $s^{-1}(r(s(O))) = O$, donc $r(s(O)) = s(O)$, donc $s(O) = O$. s est donc une symétrie orthogonale d'axe passant par O. Finalement $G = \{\mathrm{id}, r, ..., r^{n-1}, s, rs, ..., r^{n-1}s\}$: c'est un groupe diédral.

■

Remarque 2.6.4 :

- Le groupe de symétries du tétraèdre régulier est isomorphe à S_4. Il contient l'identité, 4 rotations d'angle 120°, 4 rotations d'angle 240°, 3 rotations d'angle 180°, et les compositions de ces isométries avec une symétrie orthogonale.
- Déterminons le groupe de symétries du cube. Soit A un sommet du cube. On a $|O_A| = 8$ et $|S_A| = 6$ donc le groupe du cube contient 48 éléments. Il contient l'identité, 4 rotations d'angle 120°, 4 rotations d'angle 240°, 3 rotations d'angle 90°, 9 rotations d'angle 180°, 3 rotations d'angle 270°, et la composition de ces éléments avec une symétrie orthogonale. Il est isomorphe à $\{\pm 1\} \times S_4$.
- Le groupe de symétries de l'octaèdre est le même que celui du cube.
- Le groupe de symétries du dodécaèdre (12 faces pentagonales) contient 120 éléments et est isomorphe à $\{\pm 1\} \times \mathcal{A}_5$.
- Le groupe de symétries de l'isocaèdre (20 faces triangulaires) est le même que celui du dodécaèdre.

3. Polynômes

Ici, $(A, +, \times)$ est un anneau commutatif unitaire non trivial.

3.1. Polynômes et arithmétique

Définition 3.1.1:
- On appelle polynôme à une indéterminée à coefficients dans A toute suite d'éléments de A nuls à partir d'un certain rang.
- On note $A[X]$ l'ensemble des polynômes à une indéterminée à coefficients dans A.
- Si $\lambda \in A$, $P = (p_n)_{n\in\mathbb{N}}$ et $Q = (q_n)_{n\in\mathbb{N}}$ sont deux éléments de $A[X]$, on pose $\lambda P = (\lambda p_n)_{n\in\mathbb{N}}$, $P + Q = (p_n + q_n)_{n\in\mathbb{N}}$, $PQ = \left(\sum_{k=0}^{n} a_k b_{n-k}\right)_{n\in\mathbb{N}}$ et $P(Q) = \sum_{k=0}^{n} p_k Q^k$.
- Si $P = (p_n)_{n\in\mathbb{N}} \in A[X]$, on appelle degré de P le nombre

$$\deg P = \begin{cases} \max\{n \in \mathbb{N}; p_n \neq 0\} & \text{si } P \neq 0 \\ -\infty & \text{si } P = 0 \end{cases}$$

Lemme 3.1.1: $(A[X], +, \times, \cdot)$ est une A-algèbre associative et commutative. De plus si $(A, +, \times)$ est intègre alors $(A[X], +, \times)$ est intègre.

Définition 3.1.2:
- Si $P = (p_n)_{n\in\mathbb{N}} \in A[X]$, on appelle coefficient de degré $n \in \mathbb{N}$ de P l'élément p_n. Si $P \neq 0$, on appelle coefficient dominant de P l'élément $p_{\deg P}$.
- On dit que $P \in A[X]$ est unitaire ssi sont coefficient dominant vaut 1.

Lemme 3.1.2: Soient $P, Q \in A[X]$, alors
1) $\deg(P + Q) \leqslant \max(\deg(P), \deg(Q))$ avec égalité si $\deg(P) \neq \deg(Q)$;
2) $\deg(PQ) \leqslant \deg(P) + \deg(Q)$ avec égalité ssi $P = 0$ ou $Q = 0$ ou le produit des coefficients dominants de P et Q est non nul ;
3) $\deg(P(Q)) \leqslant \deg(P) \times \deg(Q)$.

Lemme 3.1.3: Si A est intègre alors :
1) $\forall P, Q \in A[X], \deg(PQ) = \deg(P) + \deg(Q)$;
2) $\forall P, Q \in A[X], \deg(P(Q)) = \deg(P) \times \deg(Q)$;
3) $A[X]$ est intègre ;
4) $A[X]^\times = A^\times$.

Preuve:
1) Facile avec le lemme précédent.
2) Preuve similaire au point précédent.
3) Soient $P, Q \in A[X]$ tels que $PQ = 0$, alors $\deg(P) + \deg(Q) = \deg(PQ) = \deg(0) = -\infty$ donc $\deg(P) = -\infty$ ou $\deg(Q) = -\infty$ i.e. $P = 0$ ou $Q = 0$.
4) Si $a \in A$ est inversible alors il est clairement inversible dans $A[X]$. Réciproquement, soit $P \in A[X]$ un élément inversible, soit donc $Q \in A[X]$ tel que $PQ = 1$. Alors $\deg(P) + \deg(Q) = 0$ donc $\deg(P) = \deg(Q) = 0$ et $P \in A$.

■

Lemme 3.1.4: On note $X = (0, 1, 0, ...) \in A[X]$. Alors pour tout $P = (p_n)_{n\in\mathbb{N}} \in A[X]$,

$$P = \sum_{k=0}^{\infty} p_k X^k = \sum_{k=0}^{\deg P} p_k X^k$$

Définition 3.1.3 : Soit $n \in \mathbb{N}$. On note $A_n[X] = \{P \in A[X]; \deg P \leqslant n\}$.

Remarque 3.1.1:
- $A_n[X]$ est un sous-groupe de $(A[X], +)$.
- On identifie abusivement $A_0[X]$ à A.

Théorème 3.1.1:
1) Soient $P, B \in A[X]$ tels que B soit non nul et de coefficient dominant inversible. Alors il existe un unique couple $(Q, R) \in K[X]^2$ tel que $P = BQ + R$ et $\deg(R) < \deg(B)$. On dit qu'il s'agit du quotient et du reste de la division euclidienne de P par B.
2) Si A est un corps alors $A[X]$ est un anneau euclidien.

Preuve:
1) • Existence : On raisonne par récurrence sur $\deg P$.
   ‣ Supposons que $\deg(P) \leqslant 0$. Si $\deg B > 0$ alors $Q = 0$ et $R = A$ conviennent. Si $\deg B = 0$, alors $B \in A^\times$ et $Q = B^{-1}P$ et $R = 0$ conviennent.
   ‣ Soit $n \in \mathbb{N}^*$, supposons le résultat lorsque $\deg(P) < n$. Soit P un polynôme de degré n. Si $\deg P < \deg B$ alors $Q = 0$ et $R = P$ conviennent. Sinon, on considère le polynôme $P' = P - p_n b_m^{-1} X^{n-m} B$ où p_n et b_m sont les coefficients de P et B respectivement. Alors $\deg P' \leqslant \max(\deg P, \deg X^{n-m}B) \leqslant n$ et le terme de degré n de P' vaut $p_n - p_n b_m^{-1} b_m = 0$ donc $\deg P' \leqslant n-1$. Par hypothèse de récurrence, il existe $Q', R' \in A[X]$ tels que $P' = BQ' + R'$ avec $\deg R' < \deg B$. On pose $Q = a_n b_m^{-1} X^{n-m} + Q'$ et $R = R'$. Alors $P = BQ + R$ et $\deg R < \deg B$, ce qui achève la récurrence.
   • Unicité : Supposons que $P = BQ + R = BQ' + R'$ avec $\deg R, \deg R' < \deg B$. Alors $B(Q - Q') = R' - R$. Supposons par l'absurde que $Q - Q' \neq 0$, alors le coefficient dominant q_k de $Q - Q'$ existe et on a $b_m q_k \neq 0$ puisque b_m est inversible. Du coup $\deg(B(Q-Q')) = \deg(B) + \deg(Q - Q') \geqslant \deg(B) > \max(\deg R, \deg R') \geqslant \deg(R - R') = \deg(B(Q-Q'))$, absurde. Ainsi $Q = Q'$ puis $R = R'$.
2) Facile avec le premier point, le stathme est deg.

■

Remarque 3.1.2: On suppose que A est un corps. Deux polynômes $P, Q \in A[X]$ sont associés ssi $\exists \lambda \in A \setminus \{0\}, P = \lambda Q$. Dans une classe d'association, il y a exactement un polynôme unitaire (sauf pour la classe $\{0\}$).

Si $P_1, ..., P_n \in A[X]$, on appelle PGCD (resp. PPCM) de $P_1, ..., P_n$ et on note $P_1 \wedge ... \wedge P_n$ (resp. $P_1 \vee ... \vee P_n$) l'unique PGCD (resp. PPCM) unitaire de $P_1, ..., P_n$.

Exercice 3.1.1 (⋆ ⋆): Soit A un anneau unitaire et commutatif. Montrer que A est un corps ssi $A[X]$ est un anneau principal.

Solution : Si A est un corps alors $A[X]$ est un anneau euclidien, donc principal.
Réciproquement, supposons que $A[X]$ est un anneau principal. Soit $x \in A \setminus \{0\}$. Alors x et X

sont premiers entre eux : si d est un diviseur commun à x et X alors il est de degré 0 (car $A[X]$ est intègre) et comme il divise X, il est inversible. Comme $A[X]$ est principal, on a par le théorème de Bézout qu'il existe $U, V \in A[X]$ tels que $xU + XV = 1$. En identifiant les termes de degré 0, on obtient que x est inversible dans A. Ainsi A est un corps.

Exercice 3.1.2 (⋆): Soient K un corps, $a, b \in \mathbb{N}^*$, $A = X^a - 1 \in K[X]$ et $B = X^b - 1 \in K[X]$. Trouver le PGCD de A et B.

Solution : On suppose sans perte de généralité $a \geqslant b$. On écrit l'algorithme d'Euclide appliqué à a et b : pour tout $n \in [\![0, N]\!]$, $r_n = r_{n+1}q_n + r_{n+2}$ avec $(r_0, r_1) = (a, b)$, $r_{N+2} = 0$ et $\forall n \in [\![0, N-1]\!], 0 < r_{n+2} < r_{n+1}$. On a alors $a \wedge b = r_{N+1}$.

Pour tout $n \in [\![0, N]\!]$, la division euclidienne de $X^{r_n} - 1$ par $X^{r_{n+1}} - 1$ s'écrit

$$X^{r_n} - 1 = (X^{r_{n+1}} - 1)\left(\sum_{k=1}^{q_n} X^{r_n - kr_{n+1}}\right) + (X^{r_{n+2}} - 1)$$

Du coup, à nouveau par l'algorithme d'Euclide mais cette fois dans $K[X]$, le PGCD de A et B vaut la dernière valeur non nulle de $X^{r_{n+2}} - 1$, i.e.

$$A \wedge B = X^{a \wedge b} - 1$$

Exercice 3.1.3 (⋆): Soit K un corps de caractéristique nulle. Déterminer l'ensemble des polynômes $P \in K[X]$ tels que $P \equiv 1[(X-1)^3]$ et $P \equiv -1[(X+1)^3]$.

Solution : Comme $(X+1)^3$ et $(X-1)^3$ sont premiers entre eux, on sait d'après le théorème chinois que l'ensemble en question est de la forme $\Sigma = \{P + (X-1)^3(X+1)^3 Q ; Q \in K[X]\}$ où $P \in K[X]$ est n'importe quel polynôme solution. En appliquant l'algorithme d'Euclide, on trouve que $U_0(X-1)^3 + V_0(X+1)^3 = 1$ avec $U_0 = -\frac{3}{16}X^2 - \frac{9}{16}X - \frac{1}{2}$ et $V_0 = \frac{3}{16}X^2 - \frac{9}{16}X + \frac{1}{2}$. Du coup, on voit que $P = 1 - 2U_0(X-1)^3 = -1 + 2V_0(X+1)^3$ convient.

Lemme 3.1.5 : Soit I un idéal de A. Pour tout $P = \sum_{k=0}^{\infty} p_k X^k \in A[X]$, on note $\overline{P} = \sum_{k=0}^{\infty} \overline{p_k} X^k \in A/IA[X]$. Alors $P \mapsto \overline{P}$ est un morphisme d'anneaux.

Définition 3.1.4 : On suppose que A est factoriel. Soit $P \in A[X]$. On appelle contenu de P tout PGCD des coefficients de P. On dit que P est primitif ssi les coefficients de P sont premiers entre eux.

Lemme 3.1.6 *(de Gauss)*: On suppose que A est factoriel. Soient $P, Q \in A[X]$, et $c(P), c(Q), c(PQ) \in A$ des contenus de P, Q et PQ respectivement. Alors $c(PQ)$ et $c(P)c(Q)$ sont associés.

Preuve: Si $P = 0$ ou $Q = 0$ c'est clair. On suppose maintenant que P et Q sont non nuls.

On suppose d'abord que P et Q sont primitifs. Supposons par l'absurde que $c(PQ)$ n'est pas inversible, alors $c(PQ)$ est divisible par un élément irréductible $p \in A$. Comme A est factoriel, l'idéal pA est premier, donc A/pA est intègre, et donc $A/pA[X]$ aussi. Dans $A/pA[X]$, on a $\overline{P} \times \overline{Q} = \overline{PQ} = 0$ donc $\overline{P} = 0$ ou $\overline{Q} = 0$, i.e. $p|c(P)$ ou $p|c(Q)$, ce qui est absurde. Ainsi $c(PQ)$ est inversible, donc $c(P)$ et $c(Q)$ sont associés.

Dans le cas général, on considère les polynômes $\frac{P}{c(P)}$ et $\frac{Q}{c(Q)}$, qui sont primitifs. D'après ce qui précède, $\frac{P}{c(P)}\frac{Q}{c(Q)}$ est primitif, donc $c(PQ)$ et $c(P)c(Q)$ sont associés. ■

Théorème 3.1.2 : Soit A un anneau factoriel de corps des fractions K_A. Alors les éléments irréductibles de $A[X]$ sont :
- les éléments irréductibles de A ;
- les polynômes primitifs non constants qui sont irréductibles dans $K_A[X]$.

Preuve :

- Soit $P \in A[X]$ un polynôme irréductible.
  - Si P est constant alors on peut le voir comme un élément de A. Si $P = qr$ avec $q, r \in A$ alors $q \in A[X]^\times = A^\times$ ou $r \in A[X]^\times = A^\times$ donc P est irréductible dans A.
  - Si $\deg P \geqslant 1$ alors P est primitif, sinon on pourrait écrire $P = c(P)\frac{P}{c(P)}$ où $c(P)$ est un contenu de P, et $c(P)$ et $P/c(P)$ ne seraient pas inversibles. Montrons que P est irréductible dans $K_A[X]$. Soient $Q, R \in K_A[X]$ tels que $P = QR$. Alors il existe $q, r \in A \setminus \{0\}$ et $Q_1, R_1 \in A[X]$ tels que $qrP = Q_1R_1$. Soient $c(Q_1)$ et $c(R_1)$ des contenus de Q_1 et R_1, alors $qr \sim c(Q_1)c(R_1)$ par le lemme de Gauss. Du coup $P = QR = \frac{Q_1R_1}{qr} \sim \left(\frac{Q_1}{c(Q_1)}\right)\left(\frac{R_1}{c(R_1)}\right)$. Comme P est irréductible dans $A[X]$, l'un de ces facteurs est inversible dans $A[X]$, donc de degré 0. L'un des polynômes Q ou R est alors de degré 0, donc inversible dans $K_A[X]$. Ainsi P est irréductible dans $K_A[X]$.
- Réciproquement :
  - si P est un élément irréductible de A et qu'on écrit $P = QR$ avec $Q, R \in A[X]$ alors Q et R sont de degré 0, donc l'un des deux est inversible dans A donc dans $A[X]$; et donc P est irréductible dans $A[X]$;
  - si $P \in A[X]$ est primitif non constant irréductible dans $K_A[X]$ et qu'on écrit $P = QR$ alors l'un des facteurs, disons Q, est inversible dans $K_A[X]$, donc de degré 0. Mais $1 \sim c(P) \sim c(Q)c(R)$ (où $c(P), c(Q), c(R)$ sont des contenus de P, Q, R), donc Q et R sont tous deux primitifs, et Q est inversible dans $A[X]$. Ainsi P est irréductible dans $A[X]$.

■

Théorème 3.1.3 : Soit A un anneau factoriel. Alors $A[X]$ est factoriel.

Preuve :

- Existence de la décomposition en facteurs irréductibles : en écrivant $P = c(P)\frac{P}{c(P)}$ où $c(P)$ est un contenu de A et en décomposant $c(P)$ en produit d'irréductibles de A (qui sont irréductibles dans $A[X]$ par le théorème précédent), il suffit de traiter le cas où P est primitif non constant. L'anneau $K_A[X]$ (où K_A est le corps des fractions de A) est principal, donc factoriel, ce qui permet d'écrire P comme un produit de polynômes irréductibles dans

$K_A[X]$. En chassant les dénominateurs, on peut écrire $aP = P_1...P_r$ où $a \in A$ et $P_1, ..., P_r \in A[X]$ sont irréductibles dans $K_A[X]$. En prenant les contenus, on obtient par le lemme de Gauss $a \sim c(P_1)...c(P_r)$, d'où $P = u\frac{P_1}{c(P_1)}...\frac{P_r}{c(P_r)}$ avec $u \in A^*$. Les $\frac{P_i}{c(P_i)}$ sont primitifs et irréductibles dans $K_A[X]$, donc irréductibles dans $A[X]$ par le théorème précédent.

- Pour montrer que $A[X]$ est factoriel, il suffit maintenant de montrer que si $P \in A[X]$ est irréductible alors l'idéal $PA[X]$ est premier.
  - Si P est constant alors c'est un élément irréductible de A et comme A est factoriel, l'idéal PA est premier. Or les anneaux $A[X]/PA[X]$ et $(A/PA)[X]$ sont isomorphes : cela provient de la factorisation canonique du morphisme d'anneaux surjectif $A[X] \to (A/PA)[X]$. Comme PA est premier, A/PA est intègre, et il en est de même de $(A/PA)[X]$, donc aussi de $A[X]/PA[X]$, de sorte que $PA[X]$ est premier dans $A[X]$.
  - Supposons que $\deg P \geqslant 1$. D'après le théorème précédent, P est primitif et irréductible dans $K_A[X]$. On suppose que $P|QR$ avec $Q, R \in A[X]$. Comme P est irréductible dans $K_A[X]$, il divise par exemple Q dans $K_A[X]$. On peut donc écrire $aQ = PS$ avec $a \in A$ et $S \in A[X]$. En prenant les contenus, on obtient $ac(Q) = c(S)$ donc $a|c(S)$ et $S/a \in A[X]$. Comme $Q = P\frac{S}{a}$, on en déduit que P divise Q dans $A[X]$. Ceci montre que l'idéal $PA[X]$ est premier dans $A[X]$.

■

Remarque 3.1.3: Du coup, si A est factoriel alors $A[X_1, ..., X_n]$ est factoriel.

Théorème 3.1.4 (Critère d'Eisenstein) : Soient A un anneau factoriel de corps des fractions K_A et $P = \sum_{k=0}^{n} a_k X^k \in A[X]$ un polynôme de degré $n \in \mathbb{N}^*$. On suppose qu'il existe $p \in A$ irréductible tel que :

- p ne divise pas a_n ;
- p divise $a_{n-1}, ..., a_0$;
- p^2 ne divise pas a_0.

Alors P est irréductible dans $K_A[X]$ (et donc dans $A[X]$ s'il est primitif).

Preuve: Soit $c(P)$ un contenu de P. La première propriété entraîne que $c(P)$ n'est pas divisible par p. Le polynôme primitif $P/c(P)$ vérifie donc les trois propriétés et on peut supposer P primitif de degré $\geqslant 2$. Si P n'est pas irréductible dans $K_A[X]$, il ne l'est pas non plus dans $A[X]$ par un théorème précédent, donc il s'écrit $P = QR = (b_r X^r + ... + b_0)(c_s X^s + ... + c_0)$ avec $r = \deg Q \geqslant 1$ et $s = \deg R \geqslant 1$.

Comme $a_0 = b_0 c_0$ est divisible par p mais pas par p^2, exactement un des éléments b_0 et c_0 est divisible par p. Supposons par exemple qu'il s'agisse de c_0. Soit $t \in [\![0, s]\!]$ le plus petit entier tel que c_t n'est pas divisible par p (il existe car c_s n'est pas divisible par p). Alors $a_t = \sum_{k=0}^{t} b_k c_{t-k} \equiv b_0 c_t \not\equiv 0[p]$, ce qui contredit la deuxième hypothèse. ■

Exercice 3.1.4 (⋆ ⋆): Soient p un nombre premier, A un anneau factoriel et $P = \sum_{k=0}^{p-1} X^k$. Montrer à l'aide du critère d'Eisenstein que P est irréductible.

Solution : Il suffit de montrer que $P(X+1)$ est irréductible. On voit que $(X-1)P = X^p - 1$ donc $XP(X+1) = (X+1)^p - 1$ puis $P(X+1) = \sum_{k=1}^{p} \binom{p}{k} X^{k-1}$ (on peut aussi obtenir

cette expression à l'aide du binôme de Newton). Or p ne divise pas $\binom{p}{p} = 1$, p divise $\binom{p}{k}$ pour tout $k \in [\![1, p-1]\!]$ (car p est premier) et p^2 ne divise pas $\binom{p}{1} = p$. Par le critère d'Eisenstein, $P(X+1)$ est irréductible dans $K_A[X]$, donc dans $A[X]$ car c'est un polynôme unitaire, donc P aussi.

3.2. Fonction polynomiale

Définition 3.2.1 : Soit $P = \sum_{k=0}^{\infty} p_k X^k \in A[X]$. On pose

$$\tilde{P} : \begin{cases} A \to A \\ x \mapsto \sum_{k=0}^{\infty} p_k x^k \end{cases}$$

la fonction polynomiale associée à P.

Remarque 3.2.1 : On notera parfois abusivement P au lieu de $\tilde{P}$.

Lemme 3.2.1 :

$$\begin{cases} A[X] \to A^A \\ P \quad \mapsto \tilde{P} \end{cases}$$

est un morphisme d'anneaux.

Définition 3.2.2 : On dit que $x \in A$ est une racine de $P \in A[X]$ ssi $\tilde{P}(x) = 0$.

Lemme 3.2.2 : $x \in A$ est une racine de $P \in A[X]$ ssi $X - x | A$.

Preuve : Supposons que x est une racine de P. Comme le coefficient dominant de $X - x$ est inversible, on peut effectuer la division euclidienne de P par $X - x$: $P = (X-x)Q + R$ avec $\deg(R) < \deg(X-x) = 1$. On a alors $0 = \tilde{P}(x) = \tilde{R}(x) = R$ donc $P = (X-x)Q$ et $X - x | P$. La réciproque est claire. ■

Lemme 3.2.3 : On suppose que A est intègre. Soit $P \in A[X] \setminus \{0\}$. Si $x_1, ..., x_k$ sont des racines distinctes de P alors $(X - x_1)...(X - x_k) \mid P$. En particulier, $k \leqslant \deg(P)$.

Preuve : On raisonne par récurrence sur k. Le cas $k = 1$ provient du lemme précédent. Soit $k \in \mathbb{N}^*$, supposons le résultat au rang k. Supposons que P admette $k+1$ racines distinctes $x_1, ..., x_{k+1}$. Par hypothèse de récurrence, il existe $Q \in A[X]$ tel que $P = (X - x_1)...(X - x_k)Q$. On a alors $0 = \tilde{P}(x_{k+1}) = (x_{k+1} - x_1)...(x_{k+1} - x_k)\tilde{Q}(x_{k+1})$. Comme A est intègre et les x_i sont distincts, on en déduit $\tilde{Q}(x_{k+1}) = 0$, donc $X - x_{k+1} | Q$, d'où le résultat. ■

Lemme 3.2.4 : On suppose que A est intègre et infini. Alors le morphisme $P \mapsto \tilde{P}$ est injectif.

Preuve : Si $\tilde{P} = 0$ alors comme A est infini, P admet une infinité de racines. Comme A est intègre, on obtient par le lemme précédent que $P = 0$. ■

Définition 3.2.3 : Soit $P = \sum_{k=0}^{\infty} p_k X^k \in A[X]$.
- On appelle polynôme dérivé de P le polynôme $P' = \sum_{k=1}^{\infty} k p_k X^{k-1}$.
- On pose $P^{(0)} = P$ et pour tout $k \in \mathbb{N}$, $P^{(k+1)} = \left(P^{(k)}\right)'$ la dérivée k-ième de P.

Lemme 3.2.5 : Soient $P, Q \in A[X]$ et $\lambda \in A$, alors :
1) $\deg(P') \leqslant \deg(P) - 1$ avec égalité si A est intègre et de caractéristique nulle ;
2) $(\lambda P)' = \lambda P'$;
3) $(P+Q)' = P' + Q'$;
4) $(PQ)' = P'Q + PQ'$;
5) $(P(Q))' = P'(Q) \times Q'$;
6) $\forall n \in \mathbb{N}^*, (P^n)' = nP'P^{n-1}$.

Lemme 3.2.6 : Soient $P = \sum_{k=0}^{\infty} p_k X^k \in A[X]$ et $n \in \mathbb{N}$. Alors $P^{(n)} = \sum_{k=n}^{\infty} \frac{k!}{(k-n)!} p_k X^{k-n}$.

Lemme 3.2.7 : Si A est intègre et de caractéristique nulle alors pour tout $P \in K[X]$, $P' = 0$ ssi P est constant.

Théorème 3.2.1 (formule de Leibniz) : Soient $P, Q \in A[X]$ et $n \in \mathbb{N}$. Alors $(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$

Preuve : On montre le résultat par récurrence sur n. Pour $n = 0$ c'est clair. Soit $n \in \mathbb{N}$, supposons le résultat au rang n. Alors

$$\begin{aligned}
(PQ)^{(n+1)} &= \left(\sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}\right)' \\
&= \sum_{k=0}^{n} \binom{n}{k} P^{(k+1)} Q^{(n-k)} + \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n+1-k)} \\
&= \sum_{k=1}^{n+1} \binom{n}{k-1} P^{(k)} Q^{(n+1-k)} + \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n+1-k)} \\
&= Q^{(n+1)} + \sum_{k=1}^{n} \binom{n+1}{k} P^{(k)} Q^{(n+1-k)} + P^{(n+1)} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} P^{(k)} Q^{(n-k)}
\end{aligned}$$

■

Théorème 3.2.2 (formule de Taylor) : On suppose que A est un corps de caractéristique nulle. Soient $P \in A[X]$ et $a \in A$. Alors

$$P = \sum_{k=0}^{\infty} (k!1)^{-1} \widetilde{P^{(k)}}(a)(X-a)^k$$

Preuve: On écrit $P = \sum_{n=0}^{\infty} p_n X^n$. On montre d'abord le résultat pour $a = 0$. Pour tout $k \in \mathbb{N}$, $P^{(k)} = \sum_{n=k}^{\infty} \frac{n!}{(n-k)!} p_n X^{n-k}$, donc $\widetilde{P^{(k)}}(0) = k! p_k$. Comme A est un corps de caractéristique nulle, $k!1$ est non nul donc inversible. Ainsi $p_k = (k!1)^{-1}$, d'où le résultat pour $a = 0$.

Maintenant, en appliquant de qui précède au polynôme $Q = P(X + a)$, on obtient $Q = \sum_{k=0}^{\infty} (k!1)^{-1} \widetilde{Q^{(k)}}(0) X^k = \sum_{k=0}^{\infty} (k!1)^{-1} \widetilde{P^{(k)}}(a) X^k$ donc $P = Q(X - a) = \sum_{k=0}^{\infty} (k!1)^{-1} \widetilde{P^{(k)}}(a)(X - a)^k$. ■

Définition 3.2.4: Soient $P \in A[X]$, $a \in A$ et $m \in \mathbb{N}$. On dit que a est une racine de P de multiplicité m ssi $(X - a)^m \mid P$ et $(X - a)^{m+1}$ ne divise pas P. On dit que a est une racine simple de P ssi c'est une racine de multiplicité 1.

Théorème 3.2.3: On suppose que A est un corps de caractéristique nulle. Soient $P \in A[X] \setminus \{0\}$, $a \in A$ et $m \in \mathbb{N}$. Alors a est une racine de P de multiplicité m ssi $\forall k \in [\![0, m - 1]\!]$, $P^{(k)}(a) = 0$ et $P^{(m)}(a) \neq 0$.

Preuve: Facile avec la formule de Taylor. ■

Remarque 3.2.2: Si $P \in A[X] \setminus \{0\}$ et $a \in A$ alors a est une racine simple de P ssi $P(a) = 0$ et $P'(a) \neq 0$ (même si A n'est pas un corps de caractéristique nulle). En effet, si a est une racine de P alors on peut écrire $P = (X - a)Q$ et on a alors $P'(a) = Q(a)$. Du coup a est une racine simple ssi a n'est pas racine de Q, ssi $P'(a) \neq 0$.

Exercice 3.2.1 (⋆): Soit $n \geqslant 2$.
1) Montrer toutes les racines de $P_n = \sum_{k=0}^{n} \frac{X^k}{k!} \in \mathbb{C}[X]$ sont simples.
2) Montrer toutes les racines de $Q_n = X^n - X + 1 \in \mathbb{C}[X]$ sont simples.

Solution:
1) Soit a une racine de P_n. On a $P_n' = \sum_{k=0}^{n-1} \frac{X^k}{k!}$. Supposons par l'absurde que a n'est pas une racine simple, alors $P_n(a) = P_n'(a) = 0$ donc $\frac{a^n}{n} = 0$ donc $a = 0$, ce qui est absurde car 0 n'est pas racine de P_n.
2) Soit a une racine de Q_n. On a $Q_n' = nX^{n-1} - 1$. Supposons par l'absurde que a n'est pas une racine simple, alors $a^n - a - 1 = na^{n-1} - 1 = 0$. On en déduit facilement que $a = \frac{n}{n-1}$, et on a alors $Q_n'(a) = n\left(\frac{n}{n-1}\right)^{n-1} - 1 > n - 1 > 0$, ce qui est absurde.

Exercice 3.2.2 (⋆ ⋆ ♥): Soit K un corps. On suppose que le polynôme $X^4 + X + 1 \in K[X]$ admet une racine double. Montrer que K est de caractéristique 229.

Solution: Soit α une racine double de $P = X^4 + X + 1$. On a donc $P(\alpha) = \alpha^4 + \alpha + 1 = 0$ et $P'(\alpha) = 4\alpha^3 + 1 = 0$. Du coup $3\alpha + 4 = (4\alpha^4 + 4\alpha + 4) - (4\alpha^4 + \alpha) = 0$, donc $3\alpha = -4$, donc $27\alpha^3 = -64$, donc $-27 = 27 \times 4\alpha^3 = -256$, donc $229 = 0$. Or 229 est premier donc K est de caractéristique 229.

Définition 3.2.5 : Soit $P \in A[X]$. On dit que P est scindé ssi P s'écrit sous la forme $\lambda(X - x_1)...(X - x_n)$ où $n \in \mathbb{N}$ et $\lambda, x_1, ..., x_n \in A$.

Remarque 3.2.3 : Un polynôme est scindé ssi $P = 0$ ou P possède $\deg(P)$ racines comptées avec multiplicité.

Lemme 3.2.8 : On suppose que A est un corps. Soient $P, Q \in A[X]$.
1) Si P et Q sont premiers entre eux alors ils n'ont aucune racine commune.
2) Si P et Q sont scindés et n'ont aucune racine commune alors ils sont premiers entre eux.

Preuve :
1) Supposons que P et Q sont premiers entre eux. Comme $A[X]$ est un anneau principal, par le théorème de Bézout, on dispose de $U, V \in A[X]$ tels que $UP + VQ = 1$. Si P et Q admettent une racine commune x alors $1 = (UP + VQ)(x) = 0$, absurde.
2) Supposons que P et Q sont scindés et n'ont aucune racine commune. On écrit $P = \lambda(X - x_1)...(X - x_n)$ et $Q = \mu(X - y_1)...(X - y_m)$. Supposons par l'absurde que P et Q ne soient pas premiers entre eux, alors ils possèdent un diviseur commun irréductible D. Il existe $i \in [\![1, n]\!]$ et $j \in [\![1, m]\!]$ tels que $D|X - x_i$ et $D|X - y_j$. Mais P et Q n'ont aucune racine commune, donc $x_i \neq y_j$, et donc $X - x_i$ et $X - y_j$ sont premiers entre eux, absurde.

■

Théorème 3.2.4 (formules de Viète) : Soit $P = \sum_{k=0}^{n} a_k X^k \in A[X]$ un polynôme scindé de degré n. On note $x_1, ..., x_n$ ses racines. Alors pour tout $k \in [\![0, n]\!]$,

$$a_k = (-1)^{n-k} a_n \sum_{1 \leqslant i_1 < ... < i_{n-k} \leqslant n} x_{i_1} ... x_{i_{n-k}}$$

Preuve : On a $P = \sum_{k=0}^{n} a_k X^k = a_n \prod_{i=1}^{n} (X - x_i)$, d'où le résultat en identifiant les termes de degré k. ■

Remarque 3.2.4 : En particulier, $\sum_{i=1}^{n} x_i = -\frac{a_{n-1}}{a_n}$ et $\prod_{i=1}^{n} x_i = (-1)^n \frac{a_0}{a_n}$.

3.3. Application à la loi de réciprocité quadratique

Définition 3.3.1 : Soient $x \in \mathbb{Z}$ et p un nombre premier. On note

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{si } \exists y \in \mathbb{Z}, x \equiv y^2 [p] \text{ et } p \text{ ne divise pas } x \\ 0 & \text{si } p|x \\ -1 & \text{si } \forall y \in \mathbb{Z}, x \not\equiv y^2 [p] \text{ et } p \text{ ne divise pas } x \end{cases}$$

Lemme 3.3.1 : Soit p un nombre premier impair, alors

$$\left| \left\{ x \in [\![0, p-1]\!], \left(\frac{x}{p}\right) = 1 \right\} \right| = \frac{p-1}{2}$$

Preuve : L'application

$$\varphi : \begin{cases} (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times \\ x \qquad\quad \mapsto x^2 \end{cases}$$

est un morphisme de groupes. De plus $\forall x \in (\mathbb{Z}/p\mathbb{Z})^\times, x^2 = 1 \iff (x-1)(x+1) = 0 \iff x = \pm 1$. Comme $p \neq 2$, on en déduit $|\ker\varphi| = 2$ puis

$$\left|\left\{x \in [\![0, p-1]\!], \left(\frac{x}{p}\right) = 1\right\}\right| = |\operatorname{im}\varphi| = \frac{|(\mathbb{Z}/p\mathbb{Z})^\times|}{|\ker\varphi|} = \frac{p-1}{2}$$

. ■

Lemme 3.3.2 : Soient $x \in \mathbb{Z}$ et p un nombre premier impair. Alors

$$\left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}}[p]$$

Preuve : Notons $p' = \frac{p-1}{2}$ et $C_p = \{x^2; x \in (\mathbb{Z}/p\mathbb{Z})^\times\}$. Le résultat est clair si $p|x$, on suppose maintenant que ce n'est pas le cas. Alors par le petit théorème de Fermat, $\left(x^{p'}\right)^2 = x^{p-1} \equiv 1[p]$ donc $x^{p'} \equiv \pm 1[p]$.

Si $\left(\frac{x}{p}\right) = 1$ alors il existe $y \in \mathbb{Z}$ tel que $x \equiv y^2[p]$ et on a alors par le petit théorème de Fermat, $x^{p'} \equiv y^{p-1} \equiv 1[p]$. Ainsi tous les éléments de C_p sont racines du polynôme $X^{p'} - 1 \in \mathbb{Z}/p\mathbb{Z}[X]$. Or ce polynôme est de degré p' et par le lemme précédent, $|C_p| = p'$. Du coup $X^{p'} - 1$ n'admet pas d'autres racines, donc si $\left(\frac{x}{p}\right) = -1$ alors $x^{\frac{p-1}{2}} \equiv -1 \equiv \left(\frac{x}{p}\right)[p]$. ■

Lemme 3.3.3 : Soient $x, y \in \mathbb{Z}$ et p un nombre premier impair. Alors $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$.

Preuve : Facile avec le lemme précédent. ■

Lemme 3.3.4 *(de Gauss)* : Soient $x \in \mathbb{Z}$ et p un nombre premier impair ne divisant pas x. On note $p' = \frac{p-1}{2}$. Alors $\left(\frac{x}{p}\right) = (-1)^{\mu_{p,x}}$ où $\mu_{p,x}$ est le nombre d'entiers de $\{x, 2x, ..., p'x\}$ dont le reste de la division euclidienne par p est $> p'$.

Preuve : Soit S l'ensemble des restes des divisions euclidiennes des éléments de $\{x, 2x, ..., p'x\}$ par p. On note $a_1, ..., a_s$ les éléments de S inférieurs ou égaux à p' et $b_1, ..., b_u$ les éléments restants. On a alors $\{a_1, ..., a_s, p - b_1, ..., p - b_u\} \subseteq [\![1, p']\!]$. Les éléments $a_1, ..., a_s, p - b_1, ..., p - b_u$ sont deux à deux distincts : si $a_i = p - b_j$ alors en écrivant $a_i \equiv \alpha x[p]$ et $b_j \equiv \beta x[p]$ où $\alpha, \beta \in [\![1, p']\!]$, on obtient $p|(\alpha + \beta)x$, mais $p \wedge x = 1$ donc $p|\alpha + \beta$ et donc $p \leqslant \alpha + \beta \leqslant 2p' < p$, ce qui est absurde. Du coup, $\{a_1, ..., a_s, p - b_1, ..., p - b_u\} = [\![1, p']\!]$.

Du coup, $\prod_{x \in S} x \equiv (-1)^{\mu_{p,x}} p'![p]$. D'autre part, par définition de S, $\prod_{x \in S} x \equiv x^{p'} p'![p]$. On en déduit $\left(\frac{x}{p}\right) \equiv x^{p'} \equiv (-1)^{\mu_{p,x}}[p]$, d'où le résultat car $p \neq 2$. ■

Lemme 3.3.5 : Soit p un nombre premier impair. Alors

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \text{ et } \left(\frac{2}{p}\right) = (-1)^{\left\lfloor \frac{p+1}{4} \right\rfloor}$$

Preuve :

- $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}}[p]$, donc $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ car $p \neq 2$.
- Par le lemme de Gauss, $\left(\frac{2}{p}\right) = (-1)^{\mu_{p,2}}$. Pour tout $i \in [\![1, p']\!]$, $i \times 2 \in [\![1, p]\!]$ donc $\mu_{p,2}$ est le nombre d'entiers $i \in [\![1, p']\!]$ tels que $2i > p'$. Il y a $\left\lfloor \frac{p'}{2} \right\rfloor$ entiers $i \in [\![1, p']\!]$ tels que $2i \leqslant p'$, donc $\mu_{p,2} = p' - \left\lfloor \frac{p'}{2} \right\rfloor = \left\lfloor \frac{p'+1}{2} \right\rfloor = \left\lfloor \frac{p+1}{4} \right\rfloor$.

■

Théorème 3.3.1 (loi de réciprocité quadratique) : Soient p et q deux nombres premiers impairs distincts. Alors

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Preuve : On note $p' = \frac{p-1}{2}$, $q' = \frac{q-1}{2}$, $S_1 = \sum_{s=1}^{p'} \left\lfloor \frac{sq}{p} \right\rfloor$ et $S_2 = \sum_{s=1}^{q'} \left\lfloor \frac{sp}{q} \right\rfloor$.

Lemme 3.3.6 : $S_1 + S_2 = p'q'$

Preuve : Notons $R = [\![1, p']\!] \times [\![1, q']\!]$. On a

$$\begin{aligned} R &= \{(x,y) \in R; qx \geqslant py\} \cup \{(x,y) \in R; qx \leqslant py\} \\ &= \left(\bigcup_{s=1}^{p'} \{(s,y); y \in [\![1,q']\!], qs \geqslant py\}\right) \cup \left(\bigcup_{s=1}^{q'} \{(x,s); x \in [\![1,p']\!], qx \leqslant ps\}\right) \\ &= \left(\bigcup_{s=1}^{p'} \{s\} \times \left[\!\left[1, \left\lfloor \frac{sq}{p} \right\rfloor\right]\!\right]\right) \cup \left(\bigcup_{s=1}^{q'} \left[\!\left[1, \left\lfloor \frac{sp}{q} \right\rfloor\right]\!\right] \times \{s\}\right) \end{aligned}$$

De plus toutes les réunions sont disjointes : c'est clair pour la réunion de gauche et celle de droite, et pour la réunion centrale, si $qx = py$ alors comme $p \wedge q = 1$, $p|x$ ce qui est absurde. On en déduit le résultat en passant au cardinal. ■

Lemme 3.3.7 : $S_1 \equiv \mu_{p,q}[2]$

Preuve : Pour tout $s \in [\![1, p']\!]$, on note u_s le reste de la division euclidienne de sq par p. On a alors $\sum_{s=1}^{p'} sq = p\sum_{s=1}^{p'} \left\lfloor \frac{sq}{p} \right\rfloor + \sum_{s=1}^{p'} u_s = pS_1 + \sum_{s=1}^{p'} u_s$.

Notons $A = \{u_s; s \in [\![1,p']\!], u_s \leqslant p'\}$ et $B = \{u_s; s \in [\![1,p']\!], u_s > p'\}$. On a donc $|B| = \mu_{p,q}$. En travaillant modulo 2, on a

$$\sum_{s=1}^{p'} u_s = \sum_{u\in A} u + \sum_{u\in B} p - (p-u) \equiv \sum_{u\in A} u + \mu_{p,q} + \sum_{u\in B} (p-u)[2]$$

Mais on a vu dans la preuve du lemme de Gauss que $A \cup \{p-u; u \in B\} = [\![1,p']\!]$, donc $\sum_{s=1}^{p'} u_s \equiv \sum_{s=1}^{p'} s + \mu_{p,q}[2]$. Du coup $\sum_{s=1}^{p'} sq \equiv pS_1 + \sum_{s=1}^{p'} s + \mu_{p,q}[2]$, d'où le résultat puisque $p \equiv q \equiv 1[2]$. ■

Symétriquement, on a aussi $S_2 \equiv \mu_{q,p}[2]$. Du coup par le lemme de Gauss, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\mu_{p,q}\mu_{q,p}} = (-1)^{S_1+S_2} = (-1)^{p'q'}$.

Remarque 3.3.1 : Grâce à la loi de réciprocité quadratique et à la valeur de $\left(\frac{2}{p}\right)$, on peut facilement calculer $\left(\frac{x}{p}\right)$ pour tous $x \in \mathbb{Z}$ et $p \in \mathbb{P}$. Par exemple,

$$\left(\frac{56}{67}\right) = \left(\frac{2}{67}\right)^3 \left(\frac{7}{67}\right) = \left(\frac{67}{7}\right) = \left(\frac{4}{7}\right) = \left(\frac{2}{7}\right)^2 = 1$$

Exercice 3.3.1 (théorème de Proth et test de Pépin ⋆⋆⋆) :

1) Soient $m \geqslant 2$ un entier et $h \in [\![1, 2^m - 1]\!]$. On pose $n = h2^m - 1$. Soit p un nombre premier impair tel que $\left(\frac{n}{p}\right) = -1$. Montrer que n est premier ssi $p^{\frac{n-1}{2}} \equiv -1[n]$ (théorème de Proth).

2) Soit $k \in \mathbb{N}^*$. On note $F_k = 2^{2^k} + 1$ le k-ième nombre de Fermat. Montrer que F_k est premier ssi $3^{\frac{F_k-1}{2}} \equiv -1[F_k]$ (test de Pépin).

Remarque 3.3.2: Voir l'Exercice 1.6.7 pour des généralités sur les nombres de Fermat.

Solution:
1)

- Supposons que n est premier. On a $n \neq p$ puisque $\left(\frac{n}{p}\right) \neq 0$, donc par la loi de réciprocité quadratique, $\left(\frac{p}{n}\right) = \left(\frac{n}{p}\right)(-1)^{\frac{p-1}{2}\frac{n-1}{2}} = -1$. Mais d'autre part $\left(\frac{p}{n}\right) \equiv p^{\frac{n-1}{2}}[n]$, donc $p^{\frac{n-1}{2}} \equiv -1[n]$.
- Réciproquement, supposons que $p^{\frac{n-1}{2}} \equiv -1[n]$. Soit q un facteur premier de n. On a $p^{\frac{n-1}{2}} \equiv -1[q]$ et $p^{n-1} \equiv 1[q]$. Du coup, en notant d l'ordre de p modulo q, on a $d \nmid \frac{n-1}{2}$, $d|n-1$ et par le théorème de Lagrange, $d|q-1$. Les deux premières assertions s'écrivent aussi $d \nmid 2^{m-1}h$ et $d \mid 2^m h$, donc $2^m \mid d$ puis $2^m \mid q-1$.

  On écrit $n = qr$ avec $r \in \mathbb{N}$. Comme $n \equiv q \equiv 1[2^m]$, on a $r \equiv 1[2^m]$. On écrit $(q, r) = (2^m x + 1, 2^m y + 1)$ avec $x \in \mathbb{N}^*$ et $y \in \mathbb{N}$. On a alors $n = qr = 2^m(2^m xy + x + y) + 1$. Du coup $h = 2^m xy + x + y$, et on a $2^m xy < h < 2^m$, donc $y = 0$ et $n = q$. Ainsi n est premier.

1) On applique la question précédente avec $m = 2^k$, $h = 1$ et $p = 3$. On a alors $n = F_k \equiv (-1)^{2^k} + 1 \equiv 2[3]$ donc $\left(\frac{n}{3}\right) = -1$, ce qui permet de conclure.

Exercice 3.3.2 (⋆ ⋆):

1) a) Soit $p > 3$ un nombre premier. Montrer que -3 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ ssi $p \equiv 1[6]$.
   b) En déduire qu'il existe une infinité de nombres premiers congrus à 1 modulo 6.
2) a) Soit $p > 5$ un nombre premier. Montrer que 5 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ ssi $p \equiv \pm 1[10]$.
   b) En déduire qu'il existe une infinité de nombres premiers congrus à -1 modulo 10.

Remarque 3.3.3: Ce résultat est un cas particulier du théorème de Dirichlet, qui stipule que si si a et b sont premiers entre eux alors il existe une infinité de nombres premiers congrus à a modulo b. Voir l'Exercice 1.6.3 pour d'autres cas particuliers du théorème de Dirichlet.

Solution:
1)
2) Par la loi de réciprocité quadratique, $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}} = \left(\frac{p}{3}\right)$ donc -3 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ ssi p est un carré dans $\mathbb{Z}/3\mathbb{Z}$, ssi $p \equiv 1[3]$, ssi $p \equiv 1[6]$.
3) Supposons par l'absurde qu'il existe un nombre fini de nombres premiers congrus à 1 modulo 6, notés $p_1, ..., p_k$. On note $N = 1 + 2^2 \times 3 \times p_1^2 ... p_k^2$. Comme $N \geqslant 2$, N admet un diviseur premier p. De plus $p > 3$, sinon on aurait $p|N - (N-1) = 1$. On voit que $-3 \equiv (2 \times 3 \times p_1 ... p_k)^2[p]$ donc d'après la question précédente, $p \equiv 1[6]$. Mais alors $p|N - (N-1) = 1$, absurde.
4) a) Par la loi de réciprocité quadratique, $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$ donc 5 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ ssi p est un carré dans $\mathbb{Z}/5\mathbb{Z}$, ssi $p \equiv 1[5]$ ou $p \equiv 4[5]$, ssi $p \equiv \pm 1[10]$.
   b) Supposons par l'absurde qu'il existe un nombre fini de nombres premiers congrus à -1 modulo 10, notés $p_1, ..., p_k$. On note $N = -1 + 2^2 \times 3^2 \times 5 \times p_1^2 ... p_k^2$. Comme $N \geqslant 2$,

N admet un diviseur premier p. De plus $p > 5$, sinon on aurait $p|N-(N-1)=1$. On voit que $5 \equiv (2 \times 3 \times \times 5p_1...p_k)^2[p]$ donc d'après la question précédente, $p \equiv \pm 1[10]$. Si $p \equiv -1[10]$ alors $p|N-(N-1)=1$ ce qui est impossible, donc $p \equiv 1[10]$. Ceci vaut pour tout diviseur premier p de N, donc $N \equiv 1[10]$, absurde.

4. Corps et théorie de Galois

4.1. Extensions finies

Définition 4.1.1 : Soient K et L deux corps. On dit que L est un extension de K si et seulement si il existe un morphisme de corps de K dans L. Dans ce cas, on note $K \hookrightarrow L$. On dit que $K \hookrightarrow L$ est une extension de corps.

Remarque 4.1.1:
- Pour rappel, un morphisme de corps est toujours injectif. On pourra donc considérer une extension de corps $K \hookrightarrow L$ comme une inclusion $K \subseteq L$.
- Si K est un sous-corps de L alors $K \hookrightarrow L$.

Lemme 4.1.1 : Soit $K \hookrightarrow L$ une extension de corps. Alors L est une K-algèbre.

Définition 4.1.2 : Soit $K \hookrightarrow L$ une extension de corps. On dit que $K \hookrightarrow L$ est finie si et seulement si le K-espace vectoriel L est de dimension finie. Dans ce cas, on appelle degré de l'extension $K \hookrightarrow L$ la dimension de cet espace vectoriel, et on le note $[L : K]$.

Remarque 4.1.2 : Si L est fini alors $[L : K] = \frac{|L|}{|K|}$. En effet si $(e_1, ..., e_n)$ est une base de L (donc $n = [L : K]$) alors $L = \left\{\sum_{i=1}^{n} \lambda_i e_i ; \lambda_1, ..., \lambda_n \in K\right\}$, donc L est de cardinal n $|K|$.

Théorème 4.1.1 (de la base télescopique) : Soient $K \hookrightarrow L$ et $L \hookrightarrow M$ deux extensions de corps finies. Alors $K \hookrightarrow M$ est finie et $[M : K] = [M : L] \times [L : K]$.

Preuve : Notons $p = [L : K]$ et $q = [M : L]$. Soient donc $(e_i)_{i \in [\![1,p]\!]}$ une base du K-espace vectoriel L et $(f_j)_{j \in [\![1,q]\!]}$ une base du L-espace vectoriel M. On vérifie alors aisément que $(e_i f_j)_{(i,j) \in [\![1,p]\!] \times [\![1,q]\!]}$ est une base du K-espace vectoriel M, donc $K \hookrightarrow M$ est finie et $[M : K] = pq = [M : L] \times [L : K]$. ■

4.2. Extensions algébriques

Définition 4.2.1 : Soient $K \hookrightarrow L$ une extension de corps et $x \in L$. On dit que x est algébrique sur K ssi $\exists P \in K[X] \setminus \{0\}, P(x) = 0$. Dans le cas contraire, on dit que x est transcendant sur K.

L'extension $K \hookrightarrow L$ est dite algébrique ssi tous les éléments de L sont algébriques sur K.

Exemple 4.2.1 :
- L'extension $\mathbb{R} \hookrightarrow \mathbb{C}$ est algébrique : pour tout $z = x + iy \in \mathbb{C}$, z est racine de $P = (X - x)^2 + y^2 \in \mathbb{R}[X] \setminus \{0\}$.
- L'extension $\mathbb{Q} \hookrightarrow \mathbb{R}$ n'est pas algébrique car l'ensemble des nombres algébriques sur $\mathbb{Q}$ est dénombrable (car il existe un nombre dénombrable de polynômes non nuls sur $\mathbb{Q}$ et ils ont chacun un nombre fini de racines) alors que $\mathbb{R}$ ne l'est pas.
- Pour tout $n \in \mathbb{N}$, $\sqrt{n}$ est algébrique sur $\mathbb{Q}$.

Définition 4.2.2 : Soient $K \hookrightarrow L$ une extension de corps et S une partie de L. On note $K[S]$ le plus petit sous-anneau de L contenant S et $K(S)$ le plus petit sous-corps de L contenant S.

Remarque 4.2.1 :
- $K[S]$ et $K(S)$ existent bien, ce sont respectivement l'intersection des sous-anneaux de L contenant S et l'intersection des sous-corps de L contenant S.
- Les éléments de $K[S]$ sont ceux de la forme $P(s_1, ..., s_n)$ où $n \in \mathbb{N}$, $s_1, ..., s_n \in S$ et $P \in K[X_1, ..., X_n]$.
- $K(S)$ est le corps des fractions de $K[S]$.
- $K[S]$ et $K(S)$ sont des sous-K-algèbres de L.
- Si $x \in L$, on note $K[x] = K[\{x\}]$. $K[x]$ est l'image du morphisme d'anneaux

$$\varphi_x : \begin{cases} K[X] \to L \\ P \quad \mapsto P(x) \end{cases}$$

Théorème 4.2.1 : Soient $K \hookrightarrow L$ une extension de corps et $x \in L$.
1) Si x est transcendant sur K alors φ_x est injectif, le K-EV $K[x]$ est de dimension infinie et l'extension $K \hookrightarrow K(x)$. est de degré infini.
2) Si x est algébrique sur K alors il existe un unique polynôme unitaire $P \in K[X]$ de degré minimal vérifiant $P(x) = 0$. P est aussi l'unique polynôme irréductible de $K[X]$ vérifiant $P(x) = 0$. De plus $K[x] = K(x)$ et cette extension de K est finie de degré $\deg(P)$. On appelle P le polynôme minimal de x sur K.

Preuve :
1) Supposons que x est transcendant sur K. Alors φ_x est injectif par définition. Du coup $K[x] = \operatorname{im} \varphi_x$ est isomorphe à $K[X]$ donc c'est un K-EV de dimension infinie. De même, $K(x)$ est isomorphe à $K(X)$ donc c'est un K-EV de dimension infinie.
2) Supposons que x est algébrique sur K. Alors $\ker \varphi_x$ est un idéal non trivial de l'anneau $K[X]$, qui est principal. Donc c'est idéal est engendré par un polynôme non nul P. Celui-ci

annule x, est de degré minimal et est unique si on le prend unitaire. L'anneau $K[x]$ est alors isomorphe à $K[X]/PK[X]$. Mais $K[x]$ est intègre car c'est un sous-anneau de L, donc l'idéal $PK[X]$ est premier, et donc P est irréductible. De plus comme $K[X]$ est principal, $K[X]/PK[X]$ est un corps, donc $K[x]$ aussi. On a donc $K[x] = K(x)$. Enfin, on montre sans trop de problèmes que $1, x, ..., x^{\deg(P)-1}$ est une base de $K[x]$.

■

Exemple 4.2.2:
- Si $n \in \mathbb{N}$ n'est pas un carré parfait alors le polynôme minimal de $\sqrt{n}$ sur $\mathbb{Q}$ est $X^2 - n$.
- Si $a \in \mathbb{R}$ et $b \in \mathbb{R} \setminus \{0\}$ alors le polynôme minimal de $a + ib$ sur $\mathbb{R}$ est $(X - a)^2 + b^2$.

Corollaire 4.2.1: Toute extension de corps finie est algébrique.

Preuve: Soit $K \hookrightarrow L$ une extension de corps finie. Soit $x \in L$. Alors le K-EV $K[x]$ est un SEV de L, donc est de dimension finie. Par le théorème précédent, x est algébrique sur K. ■

Corollaire 4.2.2: Soit $K \hookrightarrow L$ une extension de corps engendrée par un nombre fini d'éléments algébriques sur K (i.e. $L = K(S)$ où S est un ensemble fini d'éléments algébriques sur K). Alors $K \hookrightarrow L$ est finie, donc algébrique.

Preuve: On raisonne par récurrence sur $|S|$. Si $S = \emptyset$ c'est évident. Sinon, on prend $x \in S$ et on pose $L' = K(S \setminus \{x\})$. Par hypothèse de récurrence, l'extension $K \hookrightarrow L'$ est finie. Comme x est algébrique sur K, il l'est sur L', donc l'extension $L' \hookrightarrow L = L'(x)$ est finie. Par le théorème de la base télescopique, $K \hookrightarrow L$ est finie, ce qui achève la récurrence. ■

Théorème 4.2.2: Soit $K \hookrightarrow L$ une extension de corps. Alors l'ensemble des éléments de L algébriques sur K est un sous-corps de L contenant K.

Preuve: Notons $\overline{K}$ l'ensemble des éléments de L algébriques sur K. Il est clair que $K \subseteq \overline{K}$ et $0, 1 \in \overline{K}$. Soient $x, y \in \overline{K}$. Par le théorème précédent, l'extension $K \hookrightarrow K(x, y)$ est algébrique, donc $x - y$ et $\frac{x}{y}$ sont algébriques, ce qui montre que $\overline{K}$ est un sous-corps de L. ■

Exemple 4.2.3: $\sqrt{2} + \sqrt{3} + i\sqrt{5}$ est algébrique sur $\mathbb{Q}$.

Corollaire 4.2.3: Soit $K \hookrightarrow L$ une extension de corps engendrée par des éléments algébriques sur K. Alors $K \hookrightarrow L$ est algébrique.

Preuve: On écrit $L = K(S)$ où S est un ensemble d'éléments algébriques sur K. Par le théorème précédent, l'ensemble des éléments algébriques sur K est un corps qui contient S, donc il contient $K(S) = L$, donc $K \hookrightarrow L$ est algébrique. ■

Théorème 4.2.3 : Soient $K \hookrightarrow L$ et $L \hookrightarrow M$ des extension des corps et $x \in M$. On suppose que x est algébrique sur L et que L est une extension algébrique de K. Alors x est algébrique sur K.

Preuve : Soit $P \in L[X] \setminus \{0\}$ un polynôme annulant x. Comme $K \hookrightarrow L$ est algébrique, l'extension L' de K engendrée par les coefficients de P est finie. Comme x est algébrique sur L', l'extension $L' \hookrightarrow L'(x)$ est finie. Par le théorème de la base télescopique, l'extension $K \hookrightarrow L'(x)$ est finie, donc algébrique, et x est algébrique sur K. ■

Remarque 4.2.2 : En particulier, si $K \hookrightarrow L$ et $L \hookrightarrow M$ sont deux extensions algébriques alors $K \hookrightarrow M$ est une extension algébrique.

Définition 4.2.3 : Soient K un corps et $P \in K[X]$ un polynôme irréductible. On appelle corps de rupture de P sur K toute extension $K \hookrightarrow L$ telle que $L = K(x)$ où $x \in L$ est une racine de P.

Exemple 4.2.4 : $\mathbb{C}$ est un corps de rupture du polynôme $X^2 + 1 \in \mathbb{R}[X]$.

Théorème 4.2.4 : Soient K un corps et $P \in K[X]$ un polynôme irréductible. Alors il existe un corps de rupture de P sur K, noté $K_P = K(x_P)$ où x_P est une racine de P.

Preuve : Notons $K_P = K[X]/PK[X]$. Comme P est irréductible et que $K[X]$ est principal, K_P est un corps, et on a naturellement une extension de corps $K \hookrightarrow K_p$. Soit $x_P \in K_P$ la classe de X dans K_P. Alors $\overline{P}(x_P) = \overline{P(X)} = 0$ et $K_P = K\big(x_p\big)$, d'où le résultat. ■

Définition 4.2.4 : Soient $K \hookrightarrow L$ et $K \hookrightarrow L'$ deux extensions de corps. On appelle K-morphisme de L dans L' tout morphisme de L dans L' dont la restriction à K vaut l'identité.

Lemme 4.2.1 : Soient $P \in K[X]$ un polynôme irréductible, $K \hookrightarrow L$ une extension et $x \in L$ une racine de P. Alors il existe un K-morphisme de K_P dans L qui envoie x_P sur x.

Preuve : Soit $\varphi : K[X] \to L$ l'unique K-morphisme qui envoie X sur x. Alors $\ker \varphi = PK[X]$, donc par passage au quotient on obtient un K-morphisme de K_P dans L qui envoie x_P sur x. ■

Corollaire 4.2.4 : Soit $P \in K[X]$ un polynôme irréductible. Alors deux corps de rupture de P sont isomorphes.

Définition 4.2.5 : Soient K un corps et $P \in K[X]$. On appelle corps de décomposition de P toute extension $K \hookrightarrow L$ dans laquelle P est scindé, de racines $x_1, ..., x_d$, telle que $L = K(x_1, ..., x_d)$.

Théorème 4.2.5 : Soient K un corps et $P \in K[X]$.
1) Il existe un corps de décomposition de P.
2) Deux tels corps sont isomorphes.

Preuve : On raisonne par récurrence sur $d = \deg P$. Si $d \leqslant 1$ alors K est le seul corps qui convient à isomorphisme près. Si $d > 1$, soit Q un facteur irréductible de P dans $K[X]$, et soit K_Q le corps de rupture de Q. Dans K_Q, P admet une racine x_Q donc s'écrit $P = (X - x_Q)R$ avec $R \in K_Q[X]$ de degré $d - 1$. Par hypothèse de récurrence, on a un corps de décomposition $K_Q \hookrightarrow L$ de R sur K_Q. Alors R est scindé dans $L[X]$, de racines $x_1, ..., x_{d-1}$, donc P est également scindé de racines $x_Q, x_1, ..., x_{d-1}$. De plus, $L = K_Q(x_1, ..., x_{d-1}) = K(x_Q, x_1, ..., x_{d-1})$ donc L est un corps de décomposition de P, ce qui montre l'existence.

Soient $K \hookrightarrow L$ et $K \hookrightarrow L'$ des corps de décomposition de P, $x \in L$ une racine de P et $x' \in L'$ une racine de P. Les corps $K(x)$ et $K(x')$ sont des corps de rupture de P sur K, donc il existe un isomorphisme de $K(x)$ dans $K(x')$ qui envoie x sur x'. On peut donc considérer L' comme une extension de $K(x)$. On écrit à nouveau $P = (X - x)R$ avec $R \in K(x)[X]$ de degré $d - 1$. Les extensions L et L' de $K(x)$ sont alors des corps de décomposition de R sur $K(x)$. Par hypothèse de récurrence, L et L' sont isomorphes, ce qui achève la récurrence. ■

4.3. Corps finis

Exercice 4.3.1 (⋆) : Soit K un corps fini. Montrer que K n'est pas algébriquement clos (i.e. qu'il existe un polynôme de $K[X]$ qui n'a pas de racine).

Solution : On écrit $K = \{a_1, ..., a_n\}$ et on pose $P = (X - a_1)...(X - a_n) + 1$. Alors $\forall x \in K, P(x) = 1$ donc P n'admet pas de racine.

Théorème 4.3.1 :
1) Si K est un corps fini alors sont cardinal est une puissance d'un nombre premier.
2) Pour tout nombre premier p et pour tout entier $n \geqslant 1$, il existe un corps fini à p^n éléments.
3) Un tel corps est un corps de décomposition de $X^{p^n} - X \in \mathbb{Z}/p\mathbb{Z}[X]$. En particulier, deux tels corps sont isomorphes.

On notera $\mathbb{F}_{p^n}$ l'unique corps (à isomorphisme près) à p^n éléments. En particulier, $\mathbb{F}_p$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Preuve :
1) Soit p la caractéristique de K. On sait que p est un nombre premier. Soit

$$\varphi : \begin{cases} \mathbb{Z} \to K \\ k \mapsto k1 \end{cases}$$

alors φ est un morphisme d'anneaux de noyau $p\mathbb{Z}$, donc φ induit un morphisme de corps $\mathbb{Z}/p\mathbb{Z} \to K$. On a donc une extension de corps $\mathbb{Z}/p\mathbb{Z} \hookrightarrow K$. Comme K est fini, cette extension est finie n, donc le $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel K est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^n$, donc de cardinal p^n.

2) Soit K un corps de décomposition de $P := X^{p^n} - X \in \mathbb{Z}/p\mathbb{Z}[X]$. Soit K' l'ensemble des racines de P dans K. On vérifie grâce au morphisme de Frobenius que K' est un sous-corps de K. Mais K est engendré par les racines de P, donc $K = K'$. Les racines de P sont toutes distinctes car sa dérivée vaut -1. En particulier, $|K| = p^n$.
3) Soit K un corps fini à p^n éléments. Le groupe $K^\times$ est d'ordre $p^n - 1$ donc par le théorème de Lagrange, pour tout $x \neq 0$, $x^{p^n-1} = 1$, donc les p^n éléments de K sont les racines de $P := X^{p^n} - X \in \mathbb{Z}/p\mathbb{Z}[X]$. Ce polynôme est ainsi scindé sur K, donc K est un corps de décomposition de P sur $\mathbb{Z}/p\mathbb{Z}$.

■

Désormais, nous allons étudier le corps $\mathbb{F}_q$, où $q = p^n$ avec p un nombre premier et $n \in \mathbb{N}^*$.

Théorème 4.3.2 : L'application

$$\Phi : \begin{cases} \mathbb{F}_q \to \mathbb{F}_q \\ x \mapsto x^p \end{cases}$$

est un automorphisme de corps, dit automorphisme de Frobenius, dont l'ensemble des points fixes est $\mathbb{F}_p$.

De plus, $\Phi^{\circ n}$, la n-ième itérée de Φ, vaut l'identité.

Preuve : On a déjà vu que Φ dans la partie sur les anneaux que Φ est un morphisme d'anneaux, donc de corps. Φ est donc injectif, donc bijectif pour des raisons de cardinal. Tous les éléments de $\mathbb{F}_p$ sont des points fixes de Φ (petit théorème de Fermat), et il n'y en a pas d'autre car les points fixes de Φ sont les racines de $X^p - X$, qui est de degré p donc a au plus p racines.

On a $\Phi^{\circ n} : x \mapsto x^q = x$ par le théorème de Lagrange. ■

Lemme 4.3.1 : Soit $m \in \mathbb{N}^*$. L'application

$$\Phi^{\circ n} : \begin{cases} \mathbb{F}_{q^m} \to \mathbb{F}_{q^m} \\ x \mapsto x^q \end{cases}$$

est un automorphisme de corps dont l'ensemble des points fixes est un sous-corps isomorphe à $\mathbb{F}_q$.

Preuve : C'est un automorphisme de corps comme itérée du morphisme de Frobenius. On en déduit facilement que l'ensemble des points fixes de $\Phi^{\circ n}$ est un sous-corps de $\mathbb{F}_{q^m}$. Les points fixes sont racines du polynôme $X^q - X$, donc il y en a au plus q.

On sait que le groupe des inversibles de $\mathbb{F}_{q^m}$ est cyclique d'ordre $q^m - 1$. Or $q - 1 | q^m - 1$ donc il admet un sous-groupe G d'ordre $q - 1$. Par le théorème de Lagrange, tous les éléments de G sont des points fixes de $\Phi^{\circ n}$. Il y a donc au moins q points fixes : les éléments de G et 0.

On a montré que l'ensemble des points fixes est un-sous corps de cardinal q, donc il est isomorphe à $\mathbb{F}_q$. ■

Théorème 4.3.3 : Pour tout diviseur positif d de n, il existe un unique sous-corps de $\mathbb{F}_q$ de cardinal $\mathbb{F}_{p^d}$. De plus ces sous-corps sont les seuls sous-corps de $\mathbb{F}_q$.

Preuve:
- Soit K un sous-corps de $\mathbb{F}_q$. Alors il existe $d' \in \mathbb{N}^*$ tel que $|K|^{d'} = |\mathbb{F}_q| = q$, donc $|K| = p^{\frac{n}{d'}} = p^d$ où $d = \frac{n}{d'}$ est un diviseur positif de n.
- Soit d un diviseur positif de n. D'après le lemme précédent (en remplaçant q par p^d et m par $\frac{n}{d}$), $\mathbb{F}_q$ admet un sous-corps isomorphe à $\mathbb{F}_{p^d}$. Par le théorème de Lagrange, ce sous-corps est l'ensemble des racines de $X^{p^d} - X$, il est donc unique.

■

Remarque 4.3.1: Si $\mathbb{F}_{p^d}$ est un sous-corps de $\mathbb{F}_q$ alors $\Phi^{\circ d} : x \mapsto x^{p^d}$ est un automorphisme de $\mathbb{F}_q$ dont l'ensemble des points fixes est $\mathbb{F}_{p^d}$.

Théorème 4.3.4 : Soit $d \geqslant 1$. Alors $X^{q^d} - X \in \mathbb{F}_q[X]$ est le produit des polynômes irréductibles unitaires dont le degré divise d.

Preuve:
- Déjà, $\left(X^{q^d} - X\right)' = -1$ donc $X^{q^d} - X$ est sans facteur carré.
- Soit P est un polynôme irréductible unitaire de degré k divisant $X^{q^d} - X$. L'application $x \mapsto x^{q^d}$ est un morphisme du corps $\mathbb{F}_q[X]/(P)$ (itéré du morphisme de Frobenius), donc l'ensemble de ses points fixes est un sous-corps. Or il contient la classe de X donc c'est le corps tout entier. Ainsi, un générateur α du groupe des inversibles de ce corps vérifie $\alpha^{q^n} = \alpha$, donc son ordre $q^d - 1$ divise $q^n - 1$, et on en déduit que $d|n$.
- Réciproquement, soit P irréductible de degré k divisant d. Supposons par l'absurde que $h \nmid X^{q^d} - X$, alors h et $X^{q^d} - X$ sont premiers entre eux dans $\mathbb{F}_q[X]$ donc dans $\big(\mathbb{F}_q[X]/(P)\big)[X]$. Mais dans cet anneau, la classe de X est une racine de ces deux polynômes, absurde.

■

Théorème 4.3.5 : Un polynôme $P \in \mathbb{F}_q$ de degré d est irréductible ssi $P | X^{q^d} - X$ et pour tout diviseur premier r de d, f est premier avec $X^{q^{d/r}} - X$.

Preuve:
- Le sens direct est facile avec le théorème précédent.
- Réciproquement, supposons $P | X^{q^d} - X$ et pour tout diviseur premier r de d, P est premier avec $X^{q^{d/r}} - X$. D'après le théorème précédent, P est un produit de facteurs irréductibles de multiplicité 1 et de degré divisant d, mais ne divisant pas d/r pour r diviseur premier de d. Mais tout diviseur propre de d divise l'un des d/r, donc les facteurs irréductibles de P sont de degré d. Comme P est de degré d, P est irréductible.

■

Exercice 4.3.2 (⋆ ⋆ ♥): Soit q une puissance d'un nombre premier. Pour tout $d \in \mathbb{N}^*$, on note u_d le nombre de polynômes unitaires irréductibles de $\mathbb{F}_q[X]$ de degré d.

1) Montrer que pour tout $n \in \mathbb{N}^*$, $q^n = \sum_{d|n} d u_d$ (où la somme porte sur les diviseurs positifs de n).
2) On note E l'ensemble des fonctions de $\mathbb{N}^*$ dans $\mathbb{Z}$. Pour tous $f, g \in E$, on pose

$$f * g : \begin{cases} \mathbb{N}^* \to \mathbb{Z} \\ n \mapsto \sum_{d|n} f(d) g\left(\frac{n}{d}\right) \end{cases}$$

(la loi de composition interne $*$ ainsi définie s'appelle convolution de Dirichlet).

a) Montrer que $(E, *)$ est un monoïde *(en fait, $(E, +, *)$ est un anneau intègre, mais cela ne servira pas dans l'exercice).*

b) Montrer 1 (la fonction constante égale à 1) admet pour inverse pour la loi $*$ la fonction de Möbius μ définie par

$$\forall n \in \mathbb{N}^*, \mu(n) = \begin{cases} 0 & \text{si } n \text{ est divisible par le carré d'un nombre premier} \\ 1 & \text{si } n \text{ est un produit d'un nombre pair} \\ & \text{de nombres premiers distincts} \\ -1 & \text{si } n \text{ est un produit d'un nombre impair} \\ & \text{de nombres premiers distincts} \end{cases}$$

3) En déduire une formule pour u_d.

Solution:

1) On sait que dans $\mathbb{F}_q[X]$, $X^{q^n} - X$ est le produit de tous les polynômes unitaires irréductibles dont le degré divise n. En identifiant les degrés, on obtient l'égalité voulue.
2) a) • Montrons que $*$ est associative. Soient $f, g, h \in E$ et $n \in \mathbb{N}^*$. Alors

$$((f * g) * h)(n) = \sum_{d|n} \sum_{e|d} f(e) g\left(\frac{d}{e}\right) h\left(\frac{n}{d}\right) = \sum_{e|n} f(e) \sum_{\substack{d \\ e|d|n}} g\left(\frac{d}{e}\right) h\left(\frac{n}{d}\right)$$

Soit e un diviseur positif de n. On vérifie facilement que l'application

$$\begin{cases} \{d \in \mathbb{N}^*; e|d|n\} \to \left\{k \in \mathbb{N}^*; k|\frac{n}{e}\right\} \\ d \mapsto \frac{d}{e} \end{cases}$$

est bien définie est bijective, donc

$$\sum_{\substack{d \\ e|d|n}} g\left(\frac{d}{e}\right) h\left(\frac{n}{d}\right) = \sum_{k|\frac{n}{e}} g(k) h\left(\frac{n}{ke}\right) = (g * h)\left(\frac{n}{e}\right)$$

ce qui permet de conclure.

• On vérifie facilement que

$$\delta : n \mapsto \begin{cases} 1 \text{ si } n = 1 \\ 0 \text{ sinon} \end{cases}$$

est un élément neutre pour $*$.

b) Soit $n \in \mathbb{N}^*$. Il s'agit de montrer que $\sum_{d|n} \mu(d) = \delta(n)$. Soit P l'ensemble des facteurs premiers de n. Les diviseurs d de n tels que $\mu(d) \neq 0$ sont les $\prod_{p \in Q} p$ où $Q \subseteq P$. On a alors $\mu(d) = 1$ si $|Q|$ est pair et $\mu(d) = -1$ sinon. Ainsi

$$\begin{aligned}\sum_{d|n} \mu(d) &= \sum_{Q \subseteq P} (-1)^{|Q|} = \sum_{k=0}^{|P|} \binom{n}{k} (-1)^k \text{(changement de variable } k = |Q|) \\ &= 0^{|P|} \text{ par la formule du binôme de Newton} \\ &= \delta(n) \text{ car 1 est le seul nombre divisible par aucun nombre premier}\end{aligned}$$

3) D'après la question 1, $f = g \star 1$ où $f : n \mapsto q^n$ et $g : d \mapsto du_d$. D'après la question précédente, on en déduit $g = f \star \mu$ donc

$$\forall d \in \mathbb{N}^*, u_d = \frac{1}{d} \sum_{n|d} q^n \mu\left(\frac{d}{n}\right)$$

Théorème 4.3.6 : Le corps de rupture d'un polynôme irréductible $P \in \mathbb{F}_q$ est aussi son corps de décomposition et dans ce corps, P est scindé à racines simples.

Preuve : Notons $K = \mathbb{F}_q[X]/(P)$ le corps de rupture de P. Dans ce corps, P admet une racine α.

Soit $d = \deg(P) = \left[K : \mathbb{F}_q\right]$, alors pour tout $i \in [\![0, d-1]\!]$, $P\left(\alpha^{q^i}\right) = P(\alpha)^{q^i} = 0$ donc P admet d racines $\alpha, \alpha^q, ..., \alpha^{q^{d-1}}$. Il reste à vérifier qu'elles sont bien distinctes. Si $\alpha^{q^i} = \alpha^{q^j}$ avec $0 \leqslant i \leqslant j < d$, alors en élevant à la puissance q^{d-j}, on obtient $\alpha^{q^{i+d-j}} = \alpha^{q^d} = \alpha$. Du coup $P | X^{q^{i+d-j}} - X$: si ce n'était pas le cas, P et $X^{q^{i+d-j}} - X$ seraient premiers entre eux dans $\mathbb{F}_q$, donc dans K, ce qui est absurde puisque α est une racine commune à ces deux polynômes. Donc d'après un lemme précédent, $d | i + d - j$, donc $i = j$. ■

5. Algorithmes

5.1. Primalité

5.1.1. Test de Solovay-Strassen

Définition 5.1.1.1 : On appelle nombre de Carmichael tout entier $n \in \mathbb{N}^*$ composé qui « vérifie le petit théorème de Fermat », c'est-à-dire tel que pour tout entier a premier avec n, on a $a^{n-1} \equiv 1 \bmod n$.

Théorème 5.1.1.1 (de Korselt) : Soit $n \in \mathbb{N}^*$. Les propositions suivantes sont équivalentes :
1) n est un nombre de Carmichael ;
2) n est sans facteur carré et pour tout diviseur premier p de n, on a $p - 1 \mid n - 1$;
3) pour tout entier a (non nécessairement premier avec n), on a $a^n \equiv a \bmod n$.

Preuve:

- Supposons 1). Soit p un diviseur premier de n. On écrit $n = p^r m$ où $p \nmid m$. Alors p est impair, car sinon n serait pair et on aurait $(-1)^{n-1} = -1 \not\equiv 1 \bmod n$. Par le Théorème 2.2.6, le groupe $\mathbb{Z}_{p^r}^\times$ est cyclique, soit donc x un générateur de ce groupe. Par le théorème chinois, $\mathbb{Z}_n^\times \simeq \mathbb{Z}_{p^r}^\times \times \mathbb{Z}_m^\times$, donc $(x, 1) \in \mathbb{Z}_{p^r}^\times \times \mathbb{Z}_m^\times$ correspond à un entier a qui est premier avec n et générateur de $\mathbb{Z}_{p^r}$.

  Comme n est un nombre de Carmichael, $a^{n-1} - 1$ est divisible par n donc par p^r, donc $n - 1$ est un multiple de l'ordre de a modulo p^r, à savoir $p^{r-1}(p-1)$. Ainsi p^{r-1} divise $n - 1$ et n, donc $r = 1$ et $p - 1 \mid n - 1$.

- Supposons 2). Soit a un entier. Soit p un facteur premier de n. Si $p \nmid a$ alors par le petit théorème de Fermat, $a^{p-1} \equiv 1 \bmod p$, donc $a^{n-1} \equiv 1 \bmod p$ puis $a^n \equiv a \bmod p$. Ce résultat reste vrai si $p \mid a$. Ainsi, a^n est congru à a modulo chacun des facteurs premiers de n, donc (comme n est sans facteur carré) modulo n.

- La dernière implication est claire.

■

Exercice 5.1.1.1 ($\star\star\star$):

1) Montrer qu'un nombre de Carmichael a au moins 3 facteurs premiers.
2) Soit p un nombre premier. Montrer qu'il n'existe qu'un nombre fini de nombres de Carmichael de la forme pqr où q et r sont des nombres premiers.

Solution:

1) Supposons qu'il existe un nombre de Carmichael $n = pq$ où p et q sont des nombres premiers. Posons $a = p - 1$ et $b = q - 1$. Par le théorème de Korselt, a et b divisent $n - 1 = (a+1)(b+1) - 1 = ab + a + b$, donc a divise b et b divise a. Ainsi $p = q$, ce qui est absurde car n est sans facteur carré par le théorème de Korselt.
2) Soit n un nombre de Carmichael de la forme $n = pqr$ où q et r sont premiers. Par le théorème de Korselt, $q - 1 \mid n - 1$, donc $q - 1 \mid (n-1) - (q-1) = q(pr - 1)$. Comme q et $q - 1$ sont premiers entre eux, on en déduit que $q - 1 \mid pr - 1$. Symétriquement, $r - 1 \mid pq - 1$, donc $(q-1)(r-1) \mid (pq-1)(pr-1)$, puis

$$(q-1)(r-1) \mid (pq-1)(pr-1) - p^2(q-1)(r-1) = p^2(r+q) - p(r+q) + 1 - p^2$$

   Par conséquent, $(q-1)(r-1) < p^2(r+q)$. On suppose sans perte de généralité $q < r$, alors $(q-1)^2 < 2p^2 r$ $(*)$. On a vu que $r - 1 \mid pq - 1$, donc $r \leqslant pq$ puis $r^2 \leqslant p^2 q^2 < p^2(4p^2 r)$ d'après $(*)$. Ainsi $r < 4p^4$, puis d'après $(*)$, $q < \sqrt{8}p^3 + 1$. Ainsi q et r sont bornés, ce qui montre qu'il n'y a qu'un nombre fini de nombres de Carmichael de la forme recherchée.

Remarque 5.1.1.1:

- Les premiers nombres de Carmichael sont $561 = 3 \times 11 \times 17$, 1105, 1729, 2465, 2821.
- On sait depuis 1994 qu'il existe une infinité de nombres de Carmichael, et même qu'il y a au moins $x^{2/7}$ nombres de Carmichael inférieurs à x si x est assez grand.

Définition 5.1.1.2 : Soit $n \in \mathbb{N}^*$ un entier. On appelle témoin de Solovay pour n, tout entier a premier avec n tel que $\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \bmod n$.

Remarque 5.1.1.2 : Si n est premier alors n ne possède pas de témoin de Solovay d'après le Lemme 3.3.2.

Lemme 5.1.1.1 : Soit $n \geqslant 2$ un entier impair composé. Alors n possède au moins $\varphi(n)/2$ témoins de Solovay.

Preuve : Supposons par l'absurde que n ne possède pas de témoin de Solovay. Alors pour tout entier a premier avec n, on a $a^{n-1} \equiv \left(\frac{a}{n}\right)^2 \equiv 1 \bmod n$ donc n est un nombre de Carmichael. Par le théorème de Korselt, n est sans facteur carrés. On écrit $n = \prod_{i=1}^{s} p_i$ où les p_i sont des nombres premiers distincts.

TODO

Ainsi, n possède au moins un témoin de Solovay. On considère maintenant le morphisme de groupes

$$\begin{aligned} \varphi : \mathbb{Z}_n^\times &\to \mathbb{Z}_n^\times \\ x &\mapsto \left(\frac{x}{n}\right) x^{-\frac{n-1}{2}} \end{aligned}$$

$\ker \varphi$ est l'ensemble des nombres qui ne sont pas témoins de Solovay. D'après ce qui précède, $\ker \varphi \neq \mathbb{Z}_n^\times$. Mais $\#\ker \varphi \mid \#\mathbb{Z}_n^\times = \varphi(n)$ donc $\#\ker \varphi \leqslant \varphi(n)/2$. ■

Test de Solovay-Strassen$(n \in \mathbb{N})$:

```
si n = 2 alors
    retourner « n peut être premier »
sinon si n est pair ou n ⩽ 1 alors
    retourner « n n'est pas premier »
choisir a ∈ ⟦2, n − 1⟧ aléatoirement
si a ∧ n ≠ 1 alors
    retourner « n n'est pas premier »
si (a/n) ≡ a^((n−1)/2) mod n alors
    retourner « n peut être premier »
sinon
    retourner « n n'est pas premier »
```

Remarque 5.1.1.3 : Soit $n \geqslant 4$ un nombre composé. Pour les $n - \varphi(n) + 1$ valeurs de a telles que $a \wedge n \neq 1$, le test de Solovay-Strassen déclare correctement que n n'est pas premier. Parmi les $\varphi(n) - 1$ valeurs de a restantes, le test déclare correctement que n n'est pas premier pour au moins $\frac{\varphi(n)}{2}$ d'entre elles. Donc la probabilité que n soit déclaré premier est inférieure à $\frac{1}{2}$.

Si on répète ce test pour une même valeur de n, la probabilité d'erreur diminue exponentiellement, ce qui permet d'avoir une probabilité d'erreur infime avec un temps de calcul raisonnable.

5.1.2. Test de Rabin-Miller

Lemme 5.1.2.1 : Soit p un nombre premier. On écrit $p-1 = 2^v m$ où m est impair et $v \in \mathbb{N}$. Alors pour tout $a \in \mathbb{F}_p^\times$, $a^m = 1$ ou $\exists d \in [\![0, v-1]\!], a^{2^d m} = -1$.

Preuve : Soient $a \in \mathbb{F}_p^\times$ et ω l'ordre de a dans le groupe $\mathbb{F}_p^\times$. Par le petit théorème de Fermat, $a^{p-1} = 1$, donc $\omega \mid p-1 = 2^v m$. Ainsi $\omega = 2^{d'} m'$ où $d' \in [\![0, v]\!]$ et $m' \mid m$.

- Si $d' = 0$ alors $a^{m'} = a^\omega = 1$ puis $a^m = 1$.
- Sinon, on pose $d = d' - 1 \in [\![0, v-1]\!]$ et on a $\left(a^{2^d m}\right)^2 = a^{2^{d'} m} = 1$ donc $a^{2^d m} = \pm 1$. On ne peut pas avoir $a^{2^d m} = 1$ car sinon $2^{d'} m' = \omega \mid 2^d m$ avec $d' > d$ et m impair. Donc $a^{2^d m} = -1$.

■

Définition 5.1.2.1 : Soit $n \geqslant 3$ un entier impair. On écrit $n - 1 = 2^v m$ où m est impair et $v \in \mathbb{N}$. Un élément $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ tel que $a^m \neq 1$ et $\forall d \in [\![0, v-1]\!], a^{2^d m} \neq -1$ s'appelle un témoin de Rabin-Miller pour n.

Lemme 5.1.2.2 : Soient $n \geqslant 3$ un entier impair et $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. Si a est un témoin de Solovay-Strassen pour n, alors a est un témoin de Rabin-Miller pour n.

En particulier, n possède au moins $\frac{\varphi(n)}{2}$ témoins de Rabin-Miller.

Preuve : On écrit $n - 1 = 2^v m$ où m est impair et $v \in \mathbb{N}$. On raisonne par contraposée et on suppose que a n'est pas un témoin de Rabin-Miller pour n.

- Premier cas : $a^m = 1$. Comme m est impair, on a $\left(\frac{a}{n}\right) = \left(\frac{a}{n}\right)^m = \left(\frac{a^m}{n}\right) = \left(\frac{1}{n}\right) = 1$. D'autre part, $a^{\frac{n-1}{2}} = \left(a^m\right)^{2^{v-1}} = 1$. Ainsi a n'est pas un témoin de Solovay-Strassen pour n.
- Deuxième cas : $a^{2^d m} = -1$ pour un certain $d \in [\![0, v-1]\!]$. TODO

■

```
Test de Rabin-Miller(n ∈ ℕ):
si n = 2 alors
    retourner « n peut être premier »
sinon si n est pair ou n ⩽ 1 alors
    retourner « n n'est pas premier »
choisir a ∈ ⟦2, n − 1⟧ aléatoirement
si a ∧ n ≠ 1 alors
    retourner « n n'est pas premier »
écrire n − 1 = 2^v m avec m impair
b ← a^m mod n
si b = 1 ou b = n − 1 alors
    retourner « n peut être premier »
répéter v − 1 fois
    b ← b^2 mod n
    si b = n − 1 alors
        retourner « n peut être premier »
retourner « n n'est pas premier »
```

Remarque 5.1.2.1: La Remarque 5.1.1.3 s'applique aussi pour le test de Rabin-Miller.

5.2. Cryptographie

5.2.1. RSA

RSA est un cryptosystème à clé publique. Il a deux principales applications :

- Le chiffrement à clé publique permet à une personne, Alice, de distribuer une clé publique, que d'autres peuvent utiliser pour chiffrer des messages. Alice peut ensuite déchiffrer les messages à l'aide de sa clé privée.
- La signature numérique permet à Alice de « signer » un message avec sa clé privée. N'importe qui peut utiliser sa clé publique pour vérifier que la signature a été créée avec la clé privée d'Alice et que le message n'a pas été falsifié.

Définition 5.2.1.1: Le cryptosystème RSA fonctionne de la façon suivante :

- Alice choisit deux nombres premiers distincts p et q, et calcule le module de chiffrement $N := pq$ ainsi que $\varphi(N) = (p-1)(q-1)$.
- Alice choisit un entier $e \in [\![1, \varphi(N)]\!]$ premier avec $\varphi(N)$.
- Alice publie sa clé publique (N, e).
- Alice calcule sa clé privée d qui est l'inverse de e modulo $\varphi(N)$.
- Bob chiffre son message $m \in [\![0, N-1]\!]$: il envoie $c = m^e \bmod N$ à Alice.
- Alice déchiffre le message de Bob en calculant $c^d \bmod N$.

Théorème 5.2.1.1 : Le cryptosystème RSA est correct : avec les mêmes notations, on a bien $m = c^d \bmod N$.

Preuve: Il s'agit de montrer que $m = m^{de} \bmod N$. On écrit $de = 1 + k\varphi(N)$ avec $k \in \mathbb{Z}$. Montrons que $m = m^{de} \bmod p$: si m est un multiple de p c'est clair et sinon, par le petit théorème de Fermat, $m^{p-1} \equiv 1 \bmod p$, donc $m^{k\varphi(N)} \equiv 1 \bmod p$ puis $m = m^{de} \bmod p$. De même, $m = m^{de} \bmod q$.

Ainsi, $m^{de} - m$ est divisible par p et q, donc par $N = pq$, ce qui conclut.

(Il est tentant d'utiliser le fait que $m = m^{\varphi(N)} \bmod N$, mais ceci n'est vrai que lorsque m est premier avec N.) ■

Remarque 5.2.1.1:
- La sécurité de RSA repose sur le fait que si p et q sont très grand, il est difficile de calculer $\varphi(N)$ sans connaître p et q.
- On choisit généralement $e = 65537$, c'est-à-dire 10001 en hexadécimal.
- Il est recommandé d'utiliser des nombres premiers p et q d'au moins 1024 bits.

Définition 5.2.1.2 : Voici comment Bob peut signer son message m à l'aide de la clé publique (N_0, e_0) d'Alice :
- Bob chiffre son message : il envoie $c = m^{e_0} \bmod N_0$ à Alice.
- Bob génère une clé publique (N_1, e_1) et la clé privée correspondante d_1.
- Bob signe son message : il calcule le haché $H(m)$ de son message, puis envoie $S = H(m)^{d_1} \bmod N_1$.
- Alice déchiffre le message de Bob en calculant $m = c^{d_0} \bmod N_0$, et vérifie la signature en vérifiant que $H(m) = s$.