# Cours d'Arithmétique

Isar Stubbe

version manuscrite de 2012 – 2013

Table des matières

# Structures de nombres

— 1 —

# Les nombres naturels

*Nous définissions un objet de nombres naturels (ONN) par une propriété universelle, et nous prouvons l'existence et l'unicité d'un tel ensemble. Nous prouvons qu'un ONN est un modèle de l'arithmétique de Péano (et laissons comme exercice que tout modèle de l'arithmétique de Péano est un ONN). Puis nous définissons par récurrence l'addition, la multiplication et une relation d'ordre sur un ONN, en laissant les preuves de quelques propriétés évidentes comme exercice. Nous démontrons la division euclidienne dans un ONN. Finalement, nous montrons que tout ONN est bien ordonné. (Seul ce dernier résultat est non-constructif.) Dans les exercices nous parlons de fonctions récursives et de diverses formes de récurrence.*

# 1 $\mathbb{N}$ – les nombres naturels

Rappels : Constructions et propriétés universelles de :

1°) produit $A \xleftarrow{p_A} A \times B \xrightarrow{p_B} B$

2°) somme $A \xrightarrow{s_A} A+B \xleftarrow{s_B} B$

3°) égalisateur $E \hookrightarrow A \underset{g}{\overset{f}{\rightrightarrows}} B$

4°) coégalisateur $A \underset{g}{\overset{f}{\rightrightarrows}} B \twoheadrightarrow Q$.

5°) objet initial $0 \xrightarrow{!} A$

6°) objet final $A \xrightarrow{!} 1$

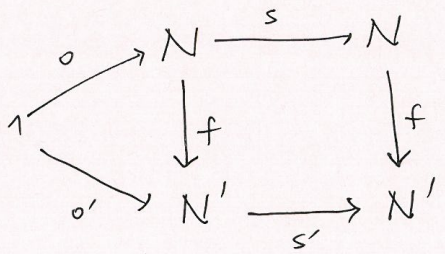
Exercice : Montrer que la propriété universelle caractérise les constructions.

~~Exercice : Montrer que dans $1 \xrightarrow{s_1} 1+1 \xleftarrow{s_2} 1$,~~ $s_1 \neq s_2$.

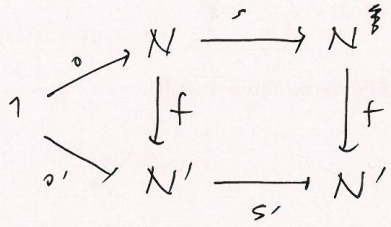
Remarque : 1°) Si $i : A \hookrightarrow B$ est une injection, on dira parfois que $A$ "est" un sous-ensemble de $B$, même si on devrait dire que $A \cong i(A) \subseteq B$.

2°) En particulier, un élément $x \in A$ sera parfois confondu avec une fonction (nécess. injective !) $1 \xrightarrow{x} A$.

Définition : Un objet de nombre naturels ("ONN") est la donnée de $1 \xrightarrow{0} N \xrightarrow{s} N$ telle que, pour tout autre $1 \xrightarrow{0'} N' \xrightarrow{s'} N'$, il existe un unique $f : N \to N'$ faisant commuter le diagramme



**Proposition ("Unicité")** : Si $(N, o, s)$ et $(N', o', s')$ sont des ONN, alors il existe une unique bijection $f : N \longrightarrow N'$ telle que




commute. □

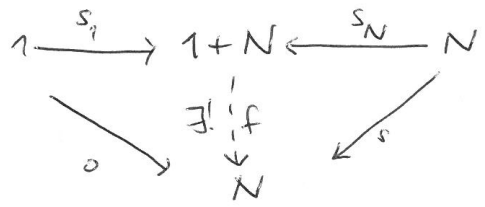
**Proposition ("Existence")** : $(\mathbb{N}, 0 \in \mathbb{N}, s(n) = n+1)$ est un ONN. □

**Remarque** : les nombres naturels "usuels" $\mathbb{N}$ forment donc (à bijection près !) l'unique ensemble, muni d'un élément $0 \in \mathbb{N}$ et une fonction "successeur" $s : \mathbb{N} \longrightarrow \mathbb{N} : n \longmapsto n+1$, qui satisfait au critère dans la définition de "ONN".

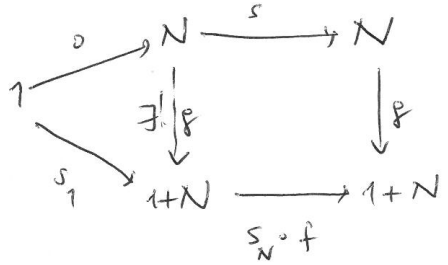
**Proposition** : Si $(N, 0, s)$ est un ONN, alors

$$1 \xrightarrow{0} N \xleftarrow{s} N \quad \text{est une somme.}$$

**Preuve** : On a certainement




mais aussi




On montre alors que $f^{-1} = g$. □

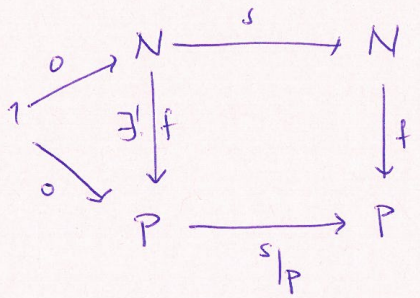
Corollaire : Si $(N, 0, s)$ est un ONN, alors

1°) $1 \xrightarrow{0} N$ et $N \xrightarrow{s} N$ sont injectifs

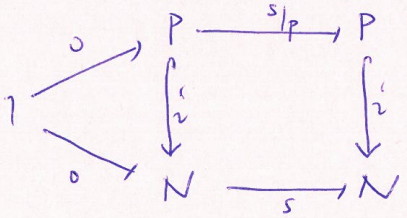
2°) $0 \notin s(N)$

Proposition ("Principle of induction") : Soit $(N, 0, s)$ un ONN. Si $P \subseteq N$, et $0 \in P$ et $s(P) \subseteq P$, alors $P = N$.

Preuve : On a




Mais aussi




d'où $if = 1_N$, donc $P = N$. □

On a donc prouvé :

**Théorème** : Si $(N, 0, s)$ est un ONN, alors

1) $\forall n \in N : \quad n = 0 \vee (\exists m \in N (n = s(m)))$

2) $\forall n \in N : \quad s(n) \neq 0$

3) $\forall n, m \in N : \quad s(n) = s(m) \Rightarrow n = m$

4) $\forall P \subseteq N : \quad (0 \in P \wedge (\forall n (n \in P \Rightarrow s(n) \in P))) \Rightarrow (P = N)$

C'est à dire, $(N, 0, s)$ est un modèle de l'arithmétique de Péano. □

**Remarque** : On peut également prouver qu'un modèle de l'arithmétique de Péano est nécessairement un ONN ; on a donc l'équivalence de ces deux concepts. ~~(T.D. ?)~~

Remarque : Encore une autre caractérisation :

$(N, 0, S)$ est un ONN si et seulement si

1°) $1 \xrightarrow{0} N \xleftarrow{S} N$ est une somme

2°) $N \underset{S}{\overset{1_N}{\rightrightarrows}} N \xrightarrow{!} 1$ est un coégalisateur.

Il est facile de prouver la nécessité de 1 et 2 (exercice !), mais plutôt difficile de prouver que 1 et 2 suffisent.

Dans la suite, on décrira la structure "arithmétique" ($+$ et $\cdot$, mais aussi $\leq$) d'un ONN.

**Proposition** ("Addition") : Si $(N, o, s)$ est un ONN, alors il existe $N \times N \xrightarrow{+} N$ (unique) telle que

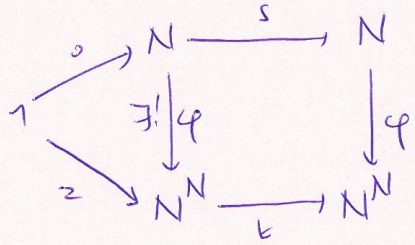
$$\begin{cases} n+o = n \\ n+s(m) = s(n+m) \end{cases}$$

**Preuve** : Soient

$$z : 1 \longrightarrow N^N : * \longmapsto 1_N$$

$$t : N^N \longrightarrow N^N : f \longmapsto s \circ f$$

alors




et on définit $n+m = \varphi(m)(n)$. □

Désormais on pourra écrire $1 := s(o)$, et donc $s(n) = n+1$ !

**Proposition ("Multiplication")** : Si $(N, 0, s)$ est un ONN, alors il existe (unique) $N \times N \xrightarrow{\cdot} N$ telle que

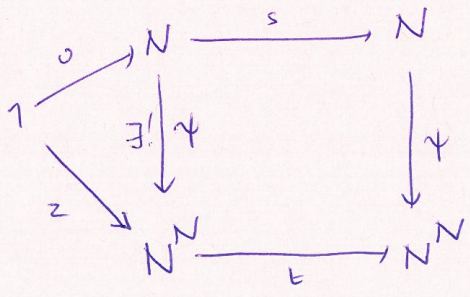
$$\begin{cases} n \cdot 0 = 0 \\ n \cdot s(m) = n \cdot m + n \end{cases}$$

**Preuve** : Soient ~~[illegible]~~

$z : 1 \longrightarrow N^N : * \longmapsto [n \overset{n}{\longmapsto} 0]$

$t : N^N \longrightarrow N^N : f \longmapsto [n \longmapsto f(n) + n]$

alors




et on définit $n \cdot m = \psi(m)(n)$. □

Exercice : Montrer, pour un ONN $(N, 0, s)$ :

1°) $l + (m + n) = (l + m) + n$

2°) $m + n = n + m$

3°) $m + l = n + l \Rightarrow m = n$

4°) $m + n = 0 \Rightarrow m = 0$ et $n = 0$

5°) $m \cdot 1 = m$ (où $1 = s(0)$).

6°) $l \cdot (m + n) = (l \cdot m) + (l \cdot n)$

7°) $l \cdot (m \cdot n) = (l \cdot m) \cdot n$

8°) $m \cdot n = n \cdot m$

9°) $m \cdot l = n \cdot l \Rightarrow m = n$ ou $l = 0$.

10°) $m \cdot l = 0 \Rightarrow m = 0$ ou $l = 0$.

Indication : ... induction, bien sûr !

**Proposition ("Ordre partiel")** : Si $(N, 0, s)$ est un ONN, alors

$$n \leq m \overset{\text{déf}}{\iff} \exists l : n + l = m$$

est un ordre partiel sur $N$. De plus,

$$n \leq m \text{ et } n \neq m \iff \exists l : n + l + 1 = m.$$
$$\overset{\text{déf}}{\iff} n < m.$$

~~Preuve : exercice !~~

Preuve : exercice ! □

**Proposition ("Trichotomie")** : Si $(N, 0, s)$ est un ONN, alors pour tout $m, n \in N$

- Soit $m \underset{\neq}{<} n$
- Soit $m = n$
- Soit $m \underset{\neq}{>} n$

Preuve : exercice (induction sur $m$). □

Exercice :

Proposition : Pour $(N, 0, s)$ un ONN, montrer que :

1°) $0 \leq n$

2°) $0 \leq_{\neq} n+1$

3°) $n \leq m \iff n+l \leq m+l$

4°) $n \leq_{\neq} m \iff n+l \leq_{\neq} n+l$

5°) $n \leq m \Rightarrow n.l \leq m.l$

6°) $n.l \leq m.l \Rightarrow l=0$ ou $n \leq m$

7°) $n \leq_{\neq} m$ et $l \neq 0 \Rightarrow n.l \leq_{\neq} m.l$

8°) $n.l \leq_{\neq} m.l \Rightarrow n \leq_{\neq} m$.

On a maintenant tous les ingrédients pour prouver le premier résultat d'arithmétique :

Théorème ("Division euclidienne") : Soit $(N, 0, s)$ un ONN. Pour tout $a, b \in N$, $b \neq 0$, il existe $q, r \in N$ unique tels que $a = b.q + r$ avec $r <_{\neq} b$.

Preuve : D'abord l'existence de $q$ et $r$ :

Soit $P_b = \{ a \in N \mid \exists q : b \cdot q \leq a \lneq b \cdot (q+1) \}$

Par induction (sur $a$) on montre que $P_b = N$.

Autrement dit,

$$\forall a \in N \quad \exists q : bq \leq a \lneq b(q+1)$$

$$\Leftrightarrow \exists q, r, t : bq + r = a \text{ et } a + t + 1 = bq + b$$

$$\Leftrightarrow \exists q, r, t : bq + r = a \text{ et } bq + r + t + 1 = bq + b$$

$$\Leftrightarrow \exists q, r : bq + r = a \text{ et } r \lneq b.$$

Ensuite, l'unicité de $q$ et $r$ : si $a = bq' + r'$ et $r' \lneq b$, alors $bq \leq a \lneq b(q'+1)$

donc $q \lneq q' + 1$ donc $\exists u : q + u + 1 = q' + 1$

donc $\exists u : q + u = q'$ donc $q \leq q'$. Similaire pour $q' \leq q$. Et donc aussi $bq + r = bq + r'$ d'où $r = r'$. □

Pour terminer ce chapitre, on prouve encore :

Théorème ("Bien ordonné"). Si $(N, o, s)$ est un ONN, alors $(N, \leq)$ est bien ordonné, ie. tout $\emptyset \neq S \subseteq N$ admet un minimum.

Preuve : Si $o \in S$, alors $o$ est le minimum de $S$ : parce que $x < o$ implique $x+y+1 = o$ donc $o = s(x+y)$, une contradiction.

Si $o \notin S$, on pose

$$M = \{ m \in N \mid \forall x \in S : m \leq x \}.$$

Puisque $\emptyset \neq S$, on a $x \in S$, et donc $x < s(x)$ ; par la trichotomie il suit que $s(x) \neq x$, donc $s(x) \notin M$. Ainsi $M \neq N$. Mais trivialement $o \in M$,

donc

$$\exists\, m_0 \in M : \quad s(m_0) \notin M$$

car sinon, par induction, on aurait $M = N$.

Si $m_0 \notin S$ alors

$$\forall x \in S : \quad m_0 < x$$

ou encore

$$\forall x \in S : \quad s(m_0) \leq x$$

donc $s(m_0) \in M$, une contradiction.

Conclusion : $m_0 \in S$ est le minimum de $S$.

□

Remarque : Contrairement à tous les autres résultats dans ce chapitre, ce dernier théorème n'est pas constructif (i.e. n'est pas valable dans tout topos, i.e. dépend de l'axiome du choix ...).

— 2 —

# Les nombres entiers

*Nous définissions le groupe (abélien) de Grothendieck d'un monoïde commutatif par une propriété universelle, et nous prouvons son existence et son unicité. Nous prouvons qu'un monoïde commutatif est inclus dans son groupe de Grothendieck si et seulement si le monoïde est simplifiable. Par définition, le groupe* $(\mathbb{Z}, +, 0)$ *est le groupe de Grothendieck du monoïde* $(\mathbb{N}, +, 0)$*, et nous laissons comme exercice de démontrer que* $(\mathbb{Z}, +, 0, \cdot, 1, \leq)$ *est un anneau ordonné. Nous prouvons ensuite que tout corps est un anneau euclidien, tout anneau euclidien est un PID, et tout PID est un UFD ; bien sûr,* $\mathbb{Z}$ *et* $K[X]$ *(pour* $K$ *un corps) sont nos principaux exemples d'anneaux euclidiens. En passant nous définissions les notions de pgcd, ppcd, éléments premiers entre eux, éléments irréductibles, et éléments premiers, et nous prouvons les théorèmes de Bezout et de Gauss (dans un PID quelconque). Dans les exercices nous parlons entre autre du théorème d'Euclide (dans un UFD quelconque) et de l'algorithme d'Euclide (dans un anneau euclidien quelconque).*

16

## 2 $\mathbb{Z}$ - les nombres entiers

Remarque : Désormais, on écrit $\mathbb{N}$ pour l'ensemble des nombres naturels, et nous allons faire des calculs (avec $+$, $\cdot$, division euclidienne, etc) "comme d'habitude". En particulier, nous adopterons l'axiome du choix (et toutes ses conséquences, comme "tiers exclu" etc).

Le but de ce chapitre est d'introduire et étudier $\mathbb{Z}$ en tant qu'"extension naturelle" de $\mathbb{N}$, plus précisément en tant que groupe abélien $(\mathbb{Z}, +, 0)$ contenant le

monoïde commutatif $(\mathbb{N}, +, 0)$. On

~~monoïde commutatif $(\mathbb{N}, +, 0)$. On~~

~~rappelle la définition pertinente :~~

rappelle la définition pertinente :

**Définition** : Soit $M$ un monoïde commutatif, $G$ un groupe abélien, et $f : M \to G$ un morphisme de monoïdes. On dit que $G$ est le groupe de Grothendieck de $M$ si, ~~pour tout autre $G'$~~ on a la propriété universelle suivante : pour tout groupe abélien $G'$ et tout homomorphisme de monoïdes $f' : M \to G'$, il existe un unique homomorphisme de groupes $\varphi : G \to G'$ faisant commuter le diagramme

$$\begin{array}{ccc} M & \xrightarrow{f} & G \\ & \searrow^{f'} & \downarrow \varphi \\ & & G' \end{array}$$

Proposition ("Unicité") : Soit un monoïde commutatif $M$, et $f : M \to G$ et $f' : M \to G'$ deux homomorphismes à valeurs dans des groupes abéliens, ayant la propriété universelle de la Définition précédente. Alors il existe un unique isomorphisme $\varphi : G \to G'$ tel que $\varphi f = f'$.

□

Proposition ("Existence") : Soit un monoïde commutatif $M = (M, *, u)$. On définit une relation sur $M \times M$ par :

$$(a,b) \sim (c,d) \overset{\text{def}}{\Longleftrightarrow} \exists e \in M : a*d*e = b*c*e$$

C'est une congruence sur le monoïde commutatif $M \times M$, dont le quotient $G(M)$

est "le" groupe de Grothendieck de $M$.

Preuve : Il est évident (grâce à la commutativité de $\Pi$ !) que $\sim$ est une relation d'équivalence sur $M \times M$.

Mais $M \times M$ est aussi un monoïde commutatif, pour l'opération

$$(a,b) * (c,d) := (a*c,\ b*d)$$

(avec neutre $(u,u)$), et il est facile de voir que $\sim$ est une congruence :

$$\left.\begin{array}{l}(a,b) \sim (c,d) \\ (a',b') \sim (c',d')\end{array}\right\} \Rightarrow (a,b) * (a',b') \sim (c,d) * (c',d') .$$

On prend ensuite les classes d'équivalence :

$$G(M) = \left\{ [(a,b)] \;\middle|\; (a,b) \in M \times M \right\},$$

et on obtient un groupe abélien, puisque

$$[(a,b)] * [(b,a)] = [(a*b,\, b*a)]$$
$$= [(u,u)]_{\sim}.$$

De plus, on a un homomorphisme

$$f : M \longrightarrow G(M)$$
$$: a \longmapsto [(a,u)],$$

Et pour tout autre groupe abélien $(G', *', u')$ et homomorphisme $f' : M \longrightarrow G'$,

$$\varphi : G(M) \longrightarrow G' : [(a,b)] \longmapsto f(a) *' \left(f'(b)\right)^{-1}$$

est l'unique homom. cherché. □

Définition : le groupe abélien $(\mathbb{Z}, +, 0)$ est $G(\mathbb{N}, +, 0)$ ; on écrit bien sûr

$$\begin{cases} n & \text{pour } [(n,0)] \\ -n & \text{pour } [(0,n)] \end{cases}$$

et on identifie $\mathbb{N} \hookrightarrow \mathbb{Z} : n \longmapsto n$.

Exercice : calculer $G(\mathbb{N}, \cdot, 1)$.

Indication : $(0,0) \sim (a,b) \quad \forall\, a,b$.

Le résultat suivant explique pourquoi $G(\mathbb{N}, +, 0)$ est un groupe intéressant mais $G(\mathbb{N}, \cdot, 1)$ ne l'est pas :

**Proposition :** Soit $M$ un monoïde commutatif et $f : M \longrightarrow G$ un homomorphisme à valeurs dans un groupe abélien ayant la propriété universelle. Alors $f$ est injectif si et seulement si $M$ est simplifiable, i.e. $ab = ac \Rightarrow b = c$

**Preuve :** Si $f$ est injectif alors

$$\begin{aligned} ab = ac &\Rightarrow (fa)(fb) = (fa)(fc) \\ &\Rightarrow (fa)^{-1}(fa)(fb) = (fa)^{-1}(fa)(fc) \\ &\Rightarrow fb = fc \\ &\Rightarrow b = c. \end{aligned}$$

Réciproquement, il suffit de montrer que $f : M \longrightarrow G(M)$ est injectif si $M$ est simplifiable (exercice : montrer

que le cas general, $f : M \to G$ ayant la prop univ., suit). Mais, pour $a, b \in M$,

$$f(a) = f(b) \iff [(a,u)] = [(b,u)]$$

$$\iff (a,u) \sim (b,u)$$

$$\iff \exists c \in M : \; a*u*c = b*u*c$$

$$\iff a = b$$

(grâce à la simplifiabilité !)

□.

Conclusion : tout monoïde commutatif simplifiable peut être considéré comme une partie d'un groupe abélien ("de manière optimale", ie. universelle).

Exercice : Dans $(\mathbb{Z}, +, 0) = G(\mathbb{N}, +, 0)$,

on définit

1°) $[(a,b)] \cdot [(c,d)] := [(\underbrace{ac+bd}_{\text{calculé dans } \mathbb{N}}, \underbrace{ad+bc}_{\text{calculé dans } \mathbb{N}})]$

2°) $[(a,b)] \leq [(c,d)] \overset{\text{déf}}{\Longleftrightarrow} \underbrace{a+d \leq c+b}_{\text{dans } \mathbb{N}}$

Ainsi on obtient un anneau commutatif

$(\mathbb{Z}, +, 0, \cdot, 1)$, resp. ensemble partiellement

ordonné $(\mathbb{Z}, \leq)$.

On vérifie que l'on dispose désormais de toutes les règles de calcul "habituelles".

~~40~~ 48

Dans la suite de ce chapitre, nous allons étudier l'anneau (ordonné) $\mathbb{Z}$.
commutatif

Exercice : Montrer que

1°) $\mathbb{Z}$ est un anneau intègre, ie.

$$a \cdot b = 0 \implies a = 0 \text{ ou } b = 0.$$

2°) la valeur absolue

$$|\cdot| : \mathbb{Z} \longrightarrow \mathbb{N} : a \longmapsto |a|$$

satisfait la propriété suivante ; ("division euclidienne") : pour tout $a, b \in \mathbb{Z}$, $b \neq 0$, il existe uniques $q, r \in \mathbb{Z}$ tels que

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

Indication pour 2°) : distinguer des cas selon les signes de $a, b$ ; appliquer div. euclid. dans $\mathbb{N}$ □

L'exercice ci-dessus montre que $\mathbb{Z}$ est un anneau euclidien, dans le sens suivant :

**Définition :** Un anneau $(A, +, 0, \cdot, 1)$ est un **anneau euclidien** si

0°) $A$ est commutatif,

1°) $A$ est intègre,

2°) il existe une fonction

$$v : A \setminus \{0\} \longrightarrow \mathbb{N}$$

telle que, pour tout $a, b \in A$, $b \neq 0$, il existe $q, r \in A$ (non-nécess. uniques !) tels que

$$a = b \cdot q + r \quad \text{et} \quad \begin{cases} \text{soit } r = 0 \\ \text{soit } v(r) < v(b) \end{cases}$$

27/92

Exercice : Montrer que les anneaux suivants sont euclidiens :

1°) $\mathbb{Z}$, $v(a) = |a|$

2°) $K$ un corps, $v(a) =$ [illegible]

3°) $K[X]$, $v(P) = \deg(P)$, [illegible]

(remarque : "$\deg(0) = -\infty$")

Indication : 1° évident

2° si $a, b \in K$ et $b \neq 0$, alors

$$a = b \cdot \frac{a}{b} + 0.$$

[illegible] note : dans $\mathbb{R}$, on peut écrire p.ex.

$$7 = 3 \cdot 2 + 1$$

mais, pour le $v : \mathbb{R} \to \mathbb{N}$ donné, on n'a pas

$$v(1) < v(3) \ !$$

~~[illegible]~~

C'est, avec $b$ et $r$ donné, on "force" la "division euclidienne" à produire le résultat

$$7 = 3 \cdot \frac{7}{3} + 0.$$

↑

3°) On prouve plutôt le lemme suivant :

Soit $A$ un anneau commutatif.
Pour tout $f, g \in A[X]$, avec $g = g_m X^m + \dots + g_1 X + g_0$ et $g_m$ inversible dans $A$, il existe $q, r \in A[X]$ uniques, tels que

$$f = g \cdot q + r, \quad 0 \leq \deg(r) < \deg(g).$$

preuve : Récurrence ("forte") sur $\deg(f)$ :

- si $\deg(f) < \deg(g)$ : $f = g \cdot 0 + f$.

- Si $\deg(f) \geq \deg(g)$ : on note

$$f = f_n X^n + \dots + f_1 X + f_0 \quad , \text{ et}$$

on suppose donc $n \geq m$, $f_n \neq 0$,

et on a donc un poly

$$f - \left( f_n \cdot g_m^{-1} \cdot X^{n-m} \right) \cdot g$$

de degré $< n$. Par induction, on sait que

$$f - f_n g_m^{-1} \cdot X^{n-m} \cdot g = g \cdot q' + r'$$

avec $0 \leq \deg(r') < \deg(g)$

donc aussi

$$f = \underbrace{\left( f_n g_m^{-1} X^{n-m} + q' \right)}_{q} \cdot g + \underbrace{r'}_{r} .$$

□

~~75~~ 70

Remarque : non-unicité de $q, r$.

ex. $+15 = 4 \cdot 4 - 1$

$= 3 \cdot 4 + 3$

et $|-1| \leq |4|$

mais aussi $|3| \leq 4$.

par contre, si on exige que $0 \leq r < |b|$,

alors on a une unique solution.

~~Démonstration~~

Théorème ~~Proposition~~ ("PID") : Dans un anneau euclidien $A$, tout idéal est principal ; i.e. si $I \trianglelefteq A$ alors $I = (a)$ pour un certain $a \in A$.

46

Preuve : Si $I = \{0\}$ alors $I = (0)$, donc rien à prouver. Si $I \neq \{0\}$, alors on peut prendre $a \in I$, $a \neq 0$ et

$$\forall b \in I : \quad v(a) \leqslant v(b).$$

Certainement $(a) \subseteq I$. Et si $b \in I$, alors $b = a \cdot q + r$, avec soit $r = 0$, soit $v(r) < v(a)$. Si $v(r) < v(a)$, alors

$$r = \underbrace{b}_{\in I} - \underbrace{a \cdot q}_{\in I} \in I$$

donc contradiction avec le choix de $a \in I$.

Donc nécessairement $r = 0$, d'où $b \in (a)$.

Ainsi, $I = (a)$. □

~~47~~ 52

**Définition :** Un anneau $(A, +, \circ, \cdot, 1)$ est un "PID" (= "principal ideal domain")

ssi 0°) $A$ est commutatif

1°) $A$ est intègre,

2°) $A$ est principal.

**Corollaire :** $\mathbb{Z}$, $K$ et $K[X]$ sont des PID.

Exercice

**~~Proposition~~ ("Nether") :** Tout PID $(A, +, \circ, \cdot, 1)$ est noetherien, i.e. toute ~~suite~~ chaîne ascendante d'idéaux

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$$

de $A$ devient constante :

$$\dots \subseteq I_k = I_{k+1} = \dots$$

Indication : $\bigcup_i I_i \trianglelefteq A$, donc $\bigcup_i I_i = (a)$,

donc $\exists k : a \in I_k$, et $I_k = I_{k+1} = \dots$.

□

Pour terminer ce chapitre, on va encore montrer que tout $n \in \mathbb{Z}$ admet une unique factorisation en nombres premiers. En fait, on va développer cela pour un PID quelconque (et donc le résultat sera aussi valable dans $K[X]$).

Dans la suite, $A$ est un anneau intègre commutatif non-trivial (un "domain", en anglais).

("Bezout")

**Proposition** : Soit $A$ un PID et $a, b \in A \setminus \{0\}$. Alors il existe un plus grand commun diviseur $d$ de $a$ et $b$, et il peut s'écrire comme

$$d = sa + tb$$

avec $s, t \in A$.

**Preuve** : $(a,b)$ = idéal engendré par $a$ et $b$

$$= \{ xa + yb \mid x, y \in A \}$$

est principal, donc $(a,b) = (d)$ pour un certain $d = sa + tb$. On a immédiatement que $d \mid a$ et $d \mid b$.

Si $c \mid a$ et $c \mid b$, alors $a = ca'$ et $b = cb'$

donc $d = sa + tb = (sa' + tb') \cdot c$, donc $c \mid d$.

□

Définition/Notation : Dans un PID $A$,

si $(a,b) = (1)$ alors $a$ et $b$ sont

premiers entre eux ( ou notés souvent $(a,b)=1$).

Dans ce cas, les seuls diviseurs communs

sont les éléments inversibles de $A$.

(Pour $\mathbb{Z}$ : $\pm 1$ ; Pour $K[X]$ : $a \in K \setminus \{0\}$).

Remarque : Dans $\mathbb{Z}$, $a, b \in \mathbb{Z}$ ont

un unique pgcd positif ; dans $K[X]$,

$f, g \in K[X]$ ont un unique pgcd unitaire.

Historiquement, le "Thm. de Bezout" dit

que, pour $a, b \in \mathbb{Z}$ premiers entre eux,

il existe $s, t$ tq.

$$1 = sa + tb.$$

§2.26

**Proposition** ("Gauss") : Dans un PID $A$,

si $a \mid bc$ et $(a, b) = 1$, alors $a \mid c$.

**Preuve** : $(a, b) = 1$, donc

$$1 = sa + tb .$$

$a \mid bc$ donc $bc = ad$.

Ainsi, $c = (sa + tb)c$

$= sac + tbc$

$= sac + tad$

$= (sc + td)a$

et $a \mid c$. □

**Exercice** : Si $A$ est un domaine et $p$ est premier, montrer que

$p \mid ab \Rightarrow p \mid a$ ou $p \mid b$. □

Exercice : Montrer que, dans un PID $A$, tout $a, b \in A$ admettent un ppcm.

Indication : $\{m \in A \mid a/m \text{ et } b/m\} \triangleq A$.

Exercice : Dans un anneau intègre $A$, montrer que $a/b$ et $b/a$ si et seulement si $a = ub$ pour $u$ inversible.

Indication : si $a, b \neq 0$ :

$a/b \Rightarrow b = ac$ et $b/a \Rightarrow a = bd$ $\Rightarrow b = bdc$

$\Rightarrow 1 = dc$,

$\Rightarrow d = c^{-1}$.

si $a = 0$ : $b/a \Rightarrow b = 0$ donc $a = 1 \cdot b$.

Réciproque : évident.

□

Exercice : Dans un anneau intègre $A$, montrer que tout $a \in A$ est divisible par tout élt inversible $u \in A$, et par tout produit $ua$ avec $u \in A$ inversible. (ce sont les "diviseurs impropres" de $a$).

Indication : si $u$ inversible, alors

$$a = u \cdot \frac{a}{u} \quad \text{et} \quad a = u^{-1} \cdot ua.$$

□

Définition : Dans un anneau intègre $A$, $0 \neq a \in A$ est un élt premier si $a$ n'est pas inversible et n'admet pas de diviseurs propres.

Exemple : dans $\mathbb{Z}$ : $\pm 1$, $\pm 2$, $\pm 3$, $\pm 5$, ...

dans $K[X]$ : polynômes irréductibles.

PID

Exercice : Montrer que dans un ~~anneau~~ A, ~~$a, b \in A$ admettent un ppcm~~

Indication : $\{m \in A \mid a/m \text{ et } b/m\} \subseteq A$.

Théorème ("UFD") : Soit A un PID, et $a \in A \setminus \{0\}$. Alors,

- soit a est inversible
- soit $a = p_1 \cdots p_m$ avec $p_i$ premiers.

De plus, si $a = q_1 \cdots q_n$ avec $q_j$ premiers, alors $n = m$, et il existe une permutation $\sigma$ de $\{1, \dots, n\}$ et des éléts inversibles $u_i \in A$ tels que $q_{\sigma(i)} = u_i p_i$ (et $u_1 \cdots u_n = 1$).

Preuve : Supposons $a \neq 0$ est non-inversible et n'admet pas de factorisation en élts premiers. Alors $a$ n'est pas premier (sinon $a = a$ est une fact. en premiers !), donc $a = a_1 \cdot b_1$. Si $a_1$ et $b_1$ admettent des factorisations en premiers, alors le produit des factorisations est une factorisation de $a$ ; quod non. Donc, disons que $a_1$ n'admet pas de factorisation en premiers. On itère l'argument pour obtenir une chaîne

$$(a) \underset{\neq}{\subset} (a_1) \underset{\neq}{\subset} (a_2) \subset \cdots$$

infinie, donc en contradiction avec

le fait que $A$ est noethérien !

Puis, l'"unicité" d'une factorisation :

récurrence sur $n$ :

Si $n=1$ : $a = p$ est premier, donc unicité est trivial.

Pour $n \to n+1$ : supposons que

$$a = p_1 \cdots p_n p_{n+1} = q_1 \cdots q_n . \quad (*)$$

Alors $p_{n+1} \mid q_1 \cdots q_n$, donc (par "Gauss")

$\exists i$ : $p_{n+1} \mid q_i$. Mais alors

$q_i = u \cdot p_{n+1}$ avec $u$ inversible

(puisque $q_i$ premier), donc $(*)$ implique

$$p_1 \cdots p_n = q_1 \cdots q_{i-1} q_{i+1} \cdots q_n .$$

On applique l'hypothèse de récurrence pour compléter la preuve. □

Dans $\mathbb{Z}$, ce théorème dit donc que, pour tout $n \in \mathbb{Z}$, on a une <u>unique</u> expression

$$n = \pm p_1^{e_1} \cdots p_k^{e_k}.$$

$2 \leq p_1 < p_2 < \cdots < p_k$

$e_i \in \mathbb{N}$

Dans $K[X]$, ce théorème dit que, pour tout $f \in K[X]$, on a une <u>unique</u> expression

$$f = c \cdot p_1^{e_1} \cdots p_k^{e_k}$$

$c \in K$

$p_i$ irréductibles et unitaires

$e_i \in \mathbb{N}$.

**Définition** : Un anneau $A$ est un anneau factoriel (ou un "unique factorisation domain", UFD) si

0°) $A$ est commutatif

1°) $A$ est intègre

2°) pour tout $0 \neq a \in A$ non-inversible il existe une factorisation

$$a = p_1 \cdots p_n$$

avec $p_i$ premiers, et "essentiellement uniques".

**Résumé** : Pour un anneau $A$,

euclidien $\Rightarrow$ PID $\Rightarrow$ UFD.

Remarque : Aucune "implication" ci-dessus est une bi-implication. En fait,

1°) $K[X,Y]$ est un UFD (on peut même prouver que $A$ UFD $\Rightarrow A[X]$ UFD) mais pas un PID ($(X,Y) \trianglelefteq K[X,Y]$ n'est pas principal)

2°) $\left\{ a + \frac{1+\sqrt{-19}}{2} \cdot b \mid a,b \in \mathbb{Z} \right\} \subseteq \mathbb{C}$ est un PID mais pas euclidien.

Ces exemples ne sont pas immédiats, et on ne fera pas les preuves.

— 3 —

# Les nombres rationnels

*Nous définissons le corps de fractions d'un anneau commutatif intègre par une propriété universelle, et nous prouvons son existence et son unicité. Le corps $\mathbb{Q}$ des nombres rationnels est alors défini comme le corps de fractions de l'anneau $\mathbb{Z}$, et le corps $K(X)$ des fractions rationnelles sur un corps $K$ est défini comme le corps de fractions de l'anneau $K[X]$. Dans les deux cas, nous revisons la notion de représentation irréductible d'un élément. Dans les exercices nous donnons une caractérisation alternative du corps de fractions, et nous travaillons sur la décomposition en éléments simples d'une fraction rationnelle.*

## 3 $\mathbb{Q}$ - Les nombres rationnels

Evidemment $(\mathbb{Z}, +, 0, \cdot, 1)$ n'est pas un corps ; en fait, ses seuls éléments inversibles sont $+1$ et $-1$.

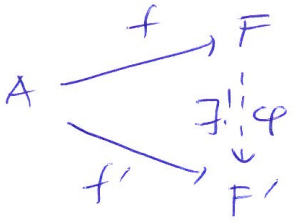
On s'intéresse donc à construire le "plus petit corps" contenant $\mathbb{Z}$. La définition pertinente est :

**Définition** : Soit $A$ un anneau commutatif intègre. Le corps de fractions de $A$ est la donnée d'un corps $F$ et un homomorphisme injectif d'anneaux

$$f : A \longrightarrow F$$

ayant la propriété universelle suivante :

pour tout corps $F'$ et tout homom. injectif d'anneaux $f' : A \longrightarrow F'$, il existe un unique homom. d'anneaux $\varphi : F \longrightarrow F'$ tel que commute.




("Unicité")

Proposition : Soit $A$ un anneau commutatif et intègre, et

$$A \xrightarrow{f} F$$
$$A \xrightarrow{f'} F'$$

deux homomorphismes d'anneaux à valeurs dans un corps, ayant tous les deux la propriété universelle de le

définition précédente. Alors il existe un unique isomorphisme de corps $\varphi : F \to F'$ tel que $f' \circ \varphi = f$. □

**Proposition ("Existence")** : Soit $A$ un anneau intègre et commutatif, et $A^* := A \setminus \{0\}$. Alors la relation sur $A \times A^*$ définie par

$$(a,b) \sim (c,d) \overset{\text{déf}}{\iff} ad = cb$$

est une congruence, et le quotient $F(A) := A \times A^* / \sim$ est "le" corps de fractions de A.

**Preuve** : Il est facile de vérifier que $\sim \subseteq (A \times A^*) \times (A \times A^*)$ est une relation d'équivalence (exercice). Même

L'ensemble $A \times A^*$ peut être muni d'une addition et d'une multiplication :

$$\begin{cases} (a,b) + (c,d) := (ad+cb,\ bd) \\ (a,b) \cdot (c,d) := (ac,\ bd) \end{cases}$$

(Puisque $A$ est intègre, $b, d \in A^* \Longrightarrow bd \in A^*$ !)

On vérifie facilement (exercice !) que, pour ces définitions de $+$ et $\cdot$, la relation $\mathcal{R}$ est une congruence :

$$\left.\begin{array}{l} (a,b)\ \mathcal{R}\ (c,d) \\ (a',b')\ \mathcal{R}\ (c',d') \end{array}\right| \Longrightarrow \begin{array}{l} (a,b) + (a',b') = (c,d) + (c',d') \\ \text{et } (a,b) \cdot (a',b') = (c,d) \cdot (c',d'). \end{array}$$

Ainsi, le quotient

$$F(A) = \left\{ [(a,b)] \;\middle|\; (a,b) \in A \times A^* \right\}$$

où $[(a,b)] = \left\{ (c,d) \in A \times A^* \mid (a,b)\ \mathcal{R}\ (c,d) \right\}$

est muni d'une addition et d'une multiplication bien définies :

$$\begin{cases} [(a,b)] + [(c,d)] := [(a,b)+(c,d)] \\ [(a,b)] \cdot [(c,d)] := [(a,b)\cdot(c,d)] \end{cases}$$

On vérifie facilement que ceci donne la structure d'un anneau commutatif ; le neutre additif est $[(0,1)]$, le neutre multiplicatif est $[(1,1)]$, et l'opposé d'un élément $[(a,b)]$ est $[(-a,b)]$.

De plus, $(F(A), +, 0, \cdot, 1)$ est un corps : si $[(a,b)] \neq [(0,1)]$, c'est à dire, si $a \cdot 1 \neq 0 \cdot b$, donc si $a \neq 0$ (et $b \neq 0$), alors $[(b,a)] \in F(A)$ aussi et on calcule que

5.

$$[(a,b)] \cdot [(b,a)]$$

$$= [(a,b) \cdot (b,a)]$$

$$= [(ab, ab)]$$

$$= [(1,1)].$$

Donc, $[(a,b)]^{-1} = [(b,a)]$.

Finalement, on a l'application

$$f : A \longrightarrow \bar{F}(A)$$

$$: a \longmapsto [(a,1)]$$

vérifiant

$$\begin{cases} f(a+b) = f(a) + f(b) \\ f(0) = [(0,1)] \\ f(1) = [(1,1)] \\ f(a \cdot b) = f(a) \cdot f(b). \end{cases}$$

...

C'est donc un homomorphisme d'anneaux, et son injectivité suit du fait que $A$ est intègre.

Supposons que $f' : A \longrightarrow F'$ injectif est aussi un homomorphisme d'anneaux ; on cherche alors un homomorphisme $\varphi : F(A) \to F'$ tel que $\varphi \circ f = f'$.

Mais alors, nécessairement,

$$\varphi([(a,b)]) = \varphi([(a,1)] \cdot [(1,b)])$$

$$= \varphi([(a,1)] \cdot [(b,1)]^{-1})$$

$$= \varphi(f(a) \cdot f(b)^{-1})$$

$$= \varphi(f(a)) \cdot (\varphi(f(b)))^{-1}$$

[ si on veut que $\varphi$ soit homom. d'anneaux

$$= f'(a) \cdot (f'(b))^{-1}$$

[ si on veut que $\varphi \circ f = f'$.

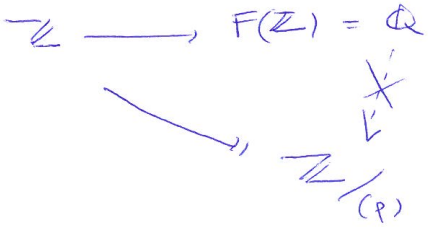
Autrement dit, on est obligé de définir

$$\varphi : F(A) \longrightarrow F$$
$$[(a,b)] \longmapsto f'(a) \cdot (f'(b))^{-1}$$

(donc on a l'unicité de $\varphi$), et on vérifie facilement que ce $\varphi$, ainsi défini, est un homomorphisme d'anneaux (donc on a l'existence de $\varphi$). □

Contrairement aux "problèmes d'injectivité" qu'on avait avec le groupe de Grothendieck d'un monoïde commutatif, nous avons ici par construction une injection $f : A \longrightarrow F(A)$.

Et d'ailleurs, pour tout corps $F'$, tout homomorphisme $\varphi : F(A) \to F'$ est nécessairement injectif. Cela explique pourquoi la prop. univ. de $f : A \to F(A)$ réfère aux homom. injectifs $f : A \to F'$. (Pour un contre-exemple, considérer




$p$ premier).

Bref, on peut donc toujours identifier un anneau commutatif et intègre $A$ avec une partie de son corps de fractions :

$$A \subseteq F(A).$$

**Définition :** Le corps des nombres rationnels est $(\mathbb{Q}, +, 0, \cdot, 1) = F(\mathbb{Z}, +, 0, \cdot, 1)$.

Bien sûr on écrit

$$\frac{m}{n} := [(m, n)]$$

(et donc on a $\frac{m}{n} = \frac{p}{q} \Leftrightarrow mq = pn$), et on identifie

$$m = \frac{m}{1}.$$

~~Dans la suite (et dans les exercices, voir ici !), nous allons détailler quelques propriétés du corps $\mathbb{Q}$.~~

~~Définition~~ Remarque : En choisissant $(m, n) = 1$ dans $\mathbb{Z}$, et $n \neq 0$, on peut toujours représenter un élément

~~[illegible] de manière unique~~

Remarque : Tout $q \in \mathbb{Q}$ s'écrit de manière unique comme

$$q = \frac{m}{n}, \quad (m,n) = 1, \quad n > 0.$$

On dit alors que $\frac{m}{n}$ est une représentation irréductible de $q$. Il suit que tous les autres représentations de $q$ sont ~~[illegible]~~ $\left\{ \frac{km}{kn} \mid k \in \mathbb{Z}^* \right\}$.

Notre cadre théorique est suffisamment large pour définir aussi :

**Définition** : Le corps des fractions rationnelles sur un corps donné $K$ est $(K(X), +, 0, \cdot, 1) = F(K[X], +, 0, \cdot, 1)$.

D'habitude on écrit $q \in K(X)$ comme

$$q = \frac{f}{g}, \quad f, g \in K[X], \ g \neq 0.$$

**Remarque** : De la même manière que pour $\mathbb{Q}$ (on utilise que $\mathbb{Z}$ et $K[X]$ sont des UFD's !), tout $q \in K(X)$ s'écrit de manière unique comme

$$q = \frac{f}{g}, \quad (f, g) = 1$$

et $g$ unitaire.
(donc $g \neq 0$)

C'est la représentation irréductible de $q$.

Attention, pour interpréter une telle "fraction rationnelle" comme une vraie fonction, on doit exclure de son domaine de définition les racines du nominateur. Ainsi, pour une représentation irréductible

$$q = \frac{f}{g}$$

on pose

$$D_q := K \setminus \{ a \in K \mid \tilde{g}(a) = 0 \}$$

et alors

$$\begin{aligned} \tilde{q} : D_q \subseteq K &\longrightarrow K \\ : a &\longmapsto \frac{f(a)}{g(a)} . \end{aligned}$$

C'est, par définition, une fonction rationnelle.

D'ailleurs, on appelle

1°) pôle de $q(X)$ : racine de $g(X)$.

2°) racine de $q(X)$ : racine de $f(X)$

où $\rho = \frac{f}{g}$ est une représentation irréductible.

(et donc aucune pôle de $q$ est une racine de $q$, puisque sinon $f$ et $g$ ne seraient pas premiers entre eux).

Exercice : Il y a un lien entre les deux définition précédentes : pour $A$ intègre et commutatif,

$$F(A)(\!(X)\!) = F(A[X]) \ !$$

Donc, en particulier, $\mathbb{Q}(\!(X)\!) = F(\mathbb{Z}[X])$.

# Arithmétique modulaire

— 4 —

# Le théorème chinois

*Nous définissons la notion de congruence modulo $m$ sur $\mathbb{Z} \times \mathbb{Z}$ ($\cdot \equiv \cdot \mod m$), en faisant le lien avec le quotient $\mathbb{Z}/(m)$. Un example simple montre l'utilité de l'arithmétique modulaire : un $f \in \mathbb{Z}[X]$ tel que $f(0)$ et $f(1)$ sont impaires, n'admet pas de racines sur $\mathbb{Z}$. Puis nous prouvons que $aX \equiv b(m)$ admet une solution (en $X$) si et seulement si $d = (a, m)$ divise $b$ ; et dans ce cas nous caracterisons les $d$ solutions de cette congruence. Nous notons quelques conséquences utiles : que $a$ est inversible dans $\mathbb{Z}/(m)$ si et seulement si $(a, m) = 1$, ou encore que, pour $m$ premier, $\mathbb{Z}/(m)$ est un corps. Ensuite nous prouvons le "théorème chinois" classique, pour la résolution d'un système de deux congruences avec des modules premiers entre eux. Nous reformulons d'abord ce théorème sous la forme d'un isomorphisme $\mathbb{Z}/(m_1 m_2) \cong \mathbb{Z}/(m_1) \times \mathbb{Z}/(m_2)$, et donnons ensuite la généralisation adéquate pour un PID quelconque au lieu de $\mathbb{Z}$, tout en remarquant que, si ce PID est un anneau euclidien, alors on dispose d'un algorithme (basé sur l'algorithme d'Euclide) pour la résolution d'un système de deux congruences. Pour finir nous montrons comment résoudre un système de $n$ congruences avec des modules deux-à-deux premiers entre eux. Dans les exercices nous traitons enfin le cas d'un système de congruences avec des modules qui ne sont pas forcemment deux-à-deux premiers entre eux.*

# 4 Le théorème Chinois

Le but de ce chapitre est la résolution de "Systèmes de congruences" dans $\mathbb{Z}$. Pour cela, on met d'abord les choses en place ! On note $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$.

Définition : Pour $a, b \in \mathbb{Z}$ et $m \in \mathbb{Z}^*$, on définit

$$a \equiv b \mod m$$

$$\Updownarrow$$

$$m \mid b - a.$$

C'est la "congruence modulo $m$" de $a$ et $b$.

**Proposition :** Pour $m \in \mathbb{Z}^*$, soit le quotient

$$q : \mathbb{Z} \longrightarrow \mathbb{Z}/(m) : n \longmapsto n+(m)$$

alors $a \equiv b \mod(m)$ si et seulement si $a+(m) = b+(m)$ (dans $\mathbb{Z}/(m)$).

Il suit donc que " $\cdot \equiv \cdot \mod(m)$ " est une relation d'équivalence sur $\mathbb{Z}$, compatible avec le $+$ et le $\cdot$ ; c'est donc bien une congruence ! □

**Exercice :** $\left|\mathbb{Z}/(m)\right| = m$.

---

Preuve : On montre que les éléments de $\mathbb{Z}/(m)$ sont $0+(m), 1+(m), \dots, m-1+(m)$ ; c'est à dire, si $0 \leq k < l < m$, alors $k+(m) \neq l+(m)$.

Indication : Pour abréger, on note parfois $\overline{k} = k+(m)$, si il ne peut pas y avoir de confusion.

On prouve que $\mathbb{Z}/(m) = \{\overline{0}, \overline{1}, \dots, \overline{m-1}\}$ :

- si $0 \leq k < l < m$, alors

$$\overline{k} = \overline{l}$$
$$\Leftrightarrow k+(m) = l+(m)$$
$$\Leftrightarrow k \equiv l \ (m)$$
$$\Leftrightarrow m \mid l-k \quad \dots \lightning$$

impossible, car $0 < l-k < m$ !

donc les éléments de $\{\overline{0}, \overline{1}, \dots, \overline{m-1}\}$ sont distincts.

- si $a \in \mathbb{Z}$, alors $a = q \cdot m + r$ par division euclidienne, donc

$$a \equiv r \ (m) \quad (\text{ie} \quad \overline{a} = \overline{r})$$

et $0 \leq r < m$. □

Exemple : Si $f \in \mathbb{Z}[X]$ et

$f(0)$ et $f(1)$ sont impairs, alors

$f$ n'a pas de racine dans $\mathbb{Z}$.

Parce que : pour $a, b \in \mathbb{Z}$, on a

$$a \equiv b \ (m) \implies a^n \equiv b^n \ (m) \quad \forall n,$$

donc aussi

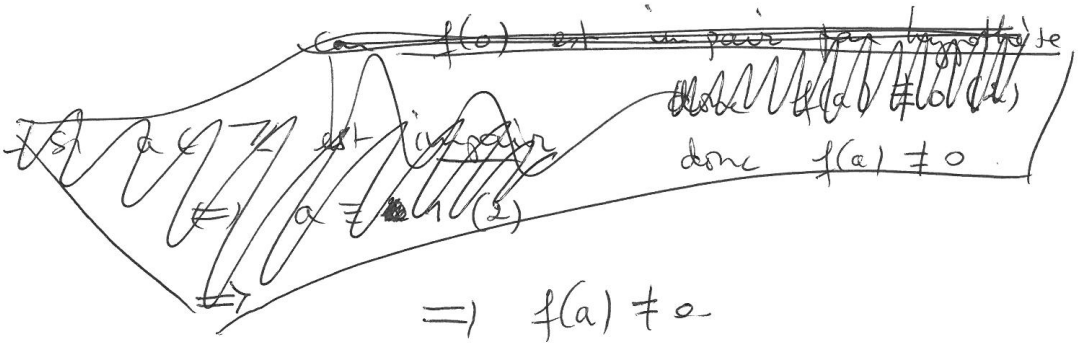
$$a \equiv b \ (m) \implies f(a) \equiv f(b) \ (m) \quad \forall f \in \mathbb{Z}[X].$$

Mais :

- si $a \in \mathbb{Z}$ est pair

$\iff a \equiv 0 \ (2)$

$\implies f(a) \equiv f(0) \ (2) \equiv 1 \ (2)$ par hypothèse




$\implies f(a) \neq 0.$

- si $a \in \mathbb{Z}$ est impair alors

$$a \equiv 1 \ (2)$$

$$\Rightarrow f(a) \equiv f(1) \ (2)$$

$$\equiv 1 \ (2) \quad \text{par hypothèse}$$

$$\Rightarrow f(a) \neq 0.$$

Donc $f$ n'a pas de racines (sur $\mathbb{Z}$) !

P.ex $f(X) = X^2 - 117X + 31$,

$f(X) = 2X^2 + 2X + 1$

etc. □.

Plus sérieusement, on va s'intéresser à la "résolution d'une congruence".

**Proposition** : Soient $a, b \in \mathbb{Z}$ et $m \in \mathbb{Z}^*$.
On note $\text{pgcd}(a, m) = d$

$aX \equiv b\ (m)$ admet une solution si et seulement si $d$ divise $b$.

Dans ce cas, il y a exactement $d$ solutions (modulo $m$). Et si $x_0$ est une solution, alors les autres solutions sont

$$\begin{array}{|l} x_0 + \frac{m}{d} \\ x_0 + \frac{2m}{d} \\ \vdots \\ x_0 + (d-1)\frac{m}{d} \end{array} .$$

**Preuve** : Supposons que $aX \equiv b\ (m)$ admet une solution, donc $ax_0 \equiv b\ (m)$ pour un certain $x_0 \in \mathbb{Z}$, donc $m \mid ax_0 - b$, donc $my_0 = ax_0 - b$ pour un certain $y_0 \in \mathbb{Z}$. Mais $d \mid ax_0 - my_0$ donc $d \mid b$.

Réciproquement, Supposons que $d \mid b$.

Par le thm de Bezout, on sait que

$$ax_0 + my_0 = d$$

pour certains $x_0, y_0 \in \mathbb{Z}$, donc

$$\underbrace{(ax_0 + my_0)}_{d} z_0 = b$$

pour un certain $z_0 \in \mathbb{Z}$, donc

$$ax_0z_0 = b - my_0z_0,$$

d'où $ax_0z_0 \equiv b\ (m)$ : on a donc une solution pour $aX \equiv b\ (m)$.

Ainsi on a prouvé l'équivalence.

Si maintenant $x_0$ et $x_1$ sont solutions,

alors $ax_0 \equiv b\ (m)$ et $ax_1 \equiv b\ (m)$

impliquent $a(x_1 - x_0) \equiv 0\ (m)$,

Mais donc $m \mid a(x_1 - x_0)$, et en

diviser par $d = \text{pgcd}(a, m)$,

$$\frac{m}{d} \mid \frac{a}{d} \cdot (x_1 - x_0).$$

où $\text{pgcd}\left(\frac{m}{d}, \frac{a}{d}\right) = 1$, donc en fait

$$\frac{m}{d} \mid x_1 - x_0$$

(par le lemme de Gauss.). Ainsi,

$$x_1 - x_0 = k \cdot \frac{m}{d}$$

donc $x_1 = x_0 + \frac{k \cdot m}{d}$. Pour finir la preuve, on vérifie encore que toute expression de la forme

$$x_0 + \frac{k \cdot m}{d}$$

est une solution de $aX \equiv b\ (m)$ (exercice) et qu'il y a exactement

de telles
d expressions distinctes modulo m (exercice). □

Exemple : $6X \equiv 3 \ (15)$

$pgcd(6,15) = 3$, donc il existe

exactement 3 solutions (modulo 15 !).

Par algo d'euclide, on trouve

$$\underset{a}{6} \cdot \underset{x_0}{3} + \underset{y_0}{(-1)} \cdot \underset{m}{15} = \underset{d}{3},$$

et (d'après la construction dans la preuve)

$$\underset{d}{3} \cdot \underset{z_0}{1} = \underset{b}{3}$$

donc $ax_0z_0 = 6.3.3 = 63$ est solution,

mieux dit (modulo 15), 3 est solution

les autres solutions sont $3 + 5 = 8$

et $3 + 2.5 = 13$.

□

Corollaire : la congruence $aX \equiv b(m)$ a une unique solution (modulo $m$) ssi $(a,m)=1$.
Donc si $m$ est premier, et $a \neq 0(m)$, alors $aX \equiv b(m)$ a toujours une unique solution (modulo $m$). □

En termes d'anneaux, cela donne :

Corollaire : Un élément $a+(m) \in \mathbb{Z}/(m)$ est inversible (dans $\mathbb{Z}/(m)$) ssi $(a,m)=1$.
Donc si $m$ est premier, alors $\mathbb{Z}/(m)$ est un corps. □

On sait donc résoudre une équation

$$aX \equiv b(m);$$

on va maintenant s'intéresser à la

résolution d'un système de telles équations. On commence avec un système à deux congruences :

Théorème ("Chinois") : Soit $m = m_1 \cdot m_2 \in \mathbb{Z}^*$ et $(m_1, m_2) = 1$. Pour tout $b_1, b_2 \in \mathbb{Z}$, le système

$$\begin{cases} X \equiv b_1 \ (m_1) \\ X \equiv b_2 \ (m_2) \end{cases}$$

admet une unique solution modulo $m$ ; autrement dit, ce système est équivalent à l'unique équation

$$X \equiv b \ (m)$$

pour un unique $b \in \mathbb{Z}/(m)$.

Preuve : Puisque $(m_1, m_2) = 1$,
on trouve par l'algo d'Euclide

$$r m_1 + s m_2 = 1.$$

Il suit que

$$x = r m_1 b_2 + s m_2 b_1$$

est une solution au système :

$$\begin{aligned} x(m_1) &\equiv \left( r m_1 b_2 + s m_2 b_1 \right) \bmod m_1 \\ &\equiv \left( r m_1 b_2 + (1 - r m_1) b_1 \right) \bmod m_1 \\ &\equiv b_1 (m_1) \end{aligned}$$

et pareil pour

$$x(m_2) \equiv b_2 (m_2).$$

Et si $x'$ est aussi une solution

au système, alors

$$\begin{cases} x - x' \equiv 0 \ (m_1) \\ x - x' \equiv 0 \ (m_2) \end{cases}$$

$$\Updownarrow$$

$$\begin{cases} m_1 \mid x - x' \\ m_2 \mid x - x' \end{cases}$$

$$\Updownarrow \longleftarrow \text{puisque } (m_1, m_2) = 1 \quad \text{cf. Lemme.}$$

$$m_1 \cdot m_2 \mid x - x'$$

$$\Updownarrow$$

$$x + (m) = x' + (m)$$

Donc la solution est unique modulo $m$.

□

On prouve le lemme dont on avait besoin :

Lemme : 1°) Si $(a_i, m) = 1 \quad \forall\, i : 1 \dots t$

alors $(a_1 \cdots a_t, m) = 1$

2°) Si $a_i \mid m \quad \forall\, i : 1 \dots t$ et $(a_i, a_j) = 1$

$\forall\, i \neq j$, alors $a_1 \cdots a_t \mid m$.

Preuve : 1) les $a_i + (m)$ sont inversibles

dans $\mathbb{Z}/(m)$, donc le produit

$a_1 \cdots a_t + (m)$ l'est aussi.

2) Récurrence sur $t$ :

$t = 1$ : rien à prouver

$t \to t+1$ : $(a_1 \cdots a_t, a_{t+1}) = 1$ par la première partie du lemme, donc

$m = a_1 \cdots a_t \cdot a'$ (par hypothèse de récurrence)

et $a_{t+1} \mid m$ impliquent (par Gauss) que

$a_{t+1} \mid a'$, d'où le résultat. □

Remarque : la preuve du théorème donne non seulement l'existence d'une unique solution, mais même une image pour la calculer (par l'algo d'Euclide !).

En termes d'anneaux, le théorème dit exactement :

Corollaire : Soit $(m_1, m_2) = 1$ dans $\mathbb{Z}$, alors l'homomorphisme d'anneaux

$$\varphi : \mathbb{Z} \longrightarrow \frac{\mathbb{Z}}{(m_1)} \times \frac{\mathbb{Z}}{(m_2)}$$

$$: a \longmapsto \left(a + (m_1),\ a + (m_2)\right)$$

induit un isomorphisme

$$\varphi : \frac{\mathbb{Z}}{(m_1 m_2)} \longrightarrow \frac{\mathbb{Z}}{(m_1)} \times \frac{\mathbb{Z}}{(m_2)}.$$

Preuve : Surjectivité de $\varphi$ revient à l'existence d'une sol au système

$$\begin{cases} X \equiv b_1 \ (m_1) \\ X \equiv b_2 \ (m_2) \end{cases}$$

et injectivité revient à l'unicité modulo $m = m_1 \cdot m_2$ d'une telle solution. □

D'ailleurs, le théorème Chinois est valable dans tout PID, avec "la même preuve" :

Théorème : Dans un PID $A$, soit $(a_1, a_2) = 1$. Alors l'homomorphisme d'anneaux canonique

$$\varphi : A \longrightarrow A/(a_1) \times A/(a_2)$$

induit un isomorphisme

$$\varphi : A/(a_1 \cdot a_2) \longrightarrow A/(a_1) \times A/(a_2) .$$

Preuve : Il est facile de vérifier que

$$\varphi(a) = \big(a + (a_1),\ a + (a_2)\big)$$

est un homomorphisme. Cet homom. est surjectif : si $b_1 \in A/(a_2)$ et $b_2 \in A/(a_2)$, alors on sait

par l'hypothèse $(a_1, a_2) = (1) = A$,

que

$$b_1 - b_2 \in A = (a_1, a_2)$$

$$\Updownarrow$$

$$b_1 - b_2 = ra_1 + sa_2 .$$

Autrement dit, l'élément

$$x = b_1 - ra_1 = b_2 + sa_2$$

est tel que

$$\varphi(x) = (b_1, b_2) .$$

Le noyau de $\varphi$ est

$$\ker(\varphi) = \{x \in A \mid \varphi(x) = (0,0)\}$$

7h

$$= \{ x \in A \mid x + (a_1) = 0 + (a_1) \text{ et } x + (a_2) = 0 + (a_2) \}$$

$$= \{ x \in A \mid a_1 | x \text{ et } a_2 | x \}$$

↓ Lemme !

$$= \{ x \in A \mid a_1 \cdot a_2 | x \}$$

$$= (a_1 \cdot a_2).$$

Donc, puisque $\mathrm{im}(\varphi) \cong A/\ker(\varphi)$ on retrouve

$$A/(a_1 a_2) \cong A/(a_1) \times A/(a_2).$$

□

Remarque : la preuve dans un PID quelconque utilise Bezout, pour l'existence de l'expression

" $r a_1 + s a_2 = b_1 - b_2$ ".

Si le PID est un anneau Euclidien, alors on peut se servir de l'algo. d'Euclide pour calculer le $r$ et le $s$ ! C'est le cas dans $\mathbb{Z}$, mais donc aussi dans $K[X]$.

Exemple : Dans $\mathbb{Z}$, résoudre

$$\begin{cases} x \equiv 2(3) \\ x \equiv 3(7) \end{cases}.$$

(Solution : $x \equiv 17(21)$).

**Proposition :** Soit $m = m_1 \cdots m_t \in \mathbb{Z}^*$ avec $(m_i, m_j) = 1 \quad \forall i \neq j$. Pour tout $b_1, \ldots, b_t \in \mathbb{Z}$ il existe un unique $b \in \mathbb{Z}$ modulo $m$ tel que

$$\begin{cases} X \equiv b_1 (m_1) \\ \vdots \\ X \equiv b_t (m_t) \end{cases}$$

$$\Updownarrow$$

$$X \equiv b (m)$$

**Preuve :** Par récurrence sur $t$ ;

$t = 2$ : C'est le théorème Chinois,

$t \to t+1$ : Le lemme assure que

$$(m_1 \cdots m_t , m_{t+1}) = 1$$

dont le théorème Chinois s'applique au système

$$\begin{cases} X \equiv b_1 (m_1) \\ \vdots \\ X \equiv b_k (m_k) \\ X \equiv b_{k+1} (m_{k+1}) \end{cases}$$

$\Updownarrow$ Hyp. de récurrence

$$\begin{cases} X \equiv b' (m_1 \cdots m_k) \\ X \equiv b_{k+1} (m_{k+1}) \end{cases}$$

$\Updownarrow$

$$X \equiv b (m_1 \cdots m_k m_{k+1}) .$$ □

Remarque : Comment faire pour résoudre un système $\begin{cases} a_1 X \equiv b_1 \ (m_1) \\ \vdots \\ a_t X \equiv b_t \ (m_t) \end{cases}$ ?

avec $(m_i, m_j) = 1$.

En plusieurs étapes :

1°) D'abord on vérifie que $(a_i, m_i) \mid b_i$ pour tout $i$ ; car sinon, il y a une équation sans solution, donc le système n'a pas de solution non plus.

2°) Supposons donc que $(a_i, m_i) \mid b_i \ (\forall i)$.
Soit $d_i = (a_i, m_i)$, alors

$$a_i X \equiv b_i \ (m_i)$$

$$\Updownarrow \qquad \frac{b_i}{d_i} \left(\frac{m_i}{d_i}\right)$$

$$\frac{a_i}{d_i} \cdot X \equiv \left(\frac{b_i}{d_i}\right)$$

et $\left(\frac{a_i}{d_i}, \frac{m_i}{d_i}\right) = 1$.

Par ailleurs si $(m_i, m_j') = 1$ on a toujours $\left(\frac{m_i}{d_i}, \frac{m_j'}{d_j'}\right) = 1$.

3°) Supposons donc que $(a_i, m_i) = 1 \ (\forall i)$.

Cela veut dire que $a_i$ est inversible dans $\mathbb{Z}/(m_i)$, donc $a_i \cdot a_i' \equiv 1 \ (m_i)$.

Mais alors

$$a_i X \equiv b_i \ (m_i)$$

$$\Updownarrow$$

$$X \equiv a_i' \cdot b_i \ (m_i').$$

Ainsi on a "transformé" le système sous la forme du Théorème Chinois.

4°) Puis on résout d'abord les deux premières équations, on les remplace par une seule, puis on résout

~~84~~

Exemple : 6 exercices.

Remarque : Dans les exercices, on va détailler comment on peut résoudre un système

$$\begin{cases} X \equiv b_1 \ (m_1) \\ \vdots \\ X \equiv b_t \ (m_t) \end{cases}$$

même quand les $m_i$ ne sont pas premiers entre eux.

---

— 5 —

# La fonction d'Euler

*Pour $m \geq 2$, soit $\varphi(m)$ le nombre d'éléments inversibles dans l'anneau $\mathbb{Z}/(m)$ (et soit $\varphi(1) = 1$) : ainsi nous définissons la fonction $\varphi$ d'Euler. Nous expliquons en détail comment le théorème chinois implique que $\varphi(mn) = \varphi(m)\varphi(n)$ pour $(m, n) = 1$. Par un argument directe nous calculons $\varphi(p^r)$ pour $p$ premier, et ainsi nous arrivons à la formule "classique" pour $\varphi(m)$. Ensuite nous rappelons la notion de groupe cyclique (en admettant aussi le cas infini), et nous prouvons que tout groupe cyclique est isomorphe soit à $(\mathbb{Z}, +, 0)$, soit à $(\mathbb{Z}/(m), +, 0)$. Nous parlons en particulier de l'ordre d'un élément d'un groupe quelconque, nous prouvons le théorème de Lagrange, et nous en déduisons d'abord le théorème d'Euler, puis le "petit thèorème" de Fermat. Pour terminer le chapître, nous prouvons encore que $\varphi(m)$ est exactement le nombre de générateurs d'un groupe cyclique d'ordre $m$, et puis nous montrons, pour $G$ un groupe cyclique d'ordre $n$ engendré par $g \in G$, que $S \subseteq G$ est un sous-groupe si et seulement si $S$ est un groupe cyclique d'ordre $k$, un diviseur de $n$, engendré par $g^{n/k}$. De là, nous déduisons la formule que $m = \sum_{d|m} \varphi(d)$ via la partition d'un groupe cyclique $G$ d'ordre $m$ selon l'ordre de ses éléments. Dans les exercices nous illustrons la théorie entre autre avec le procédé de codage RSA.*

## 5| La fonction indicatrice d'Euler

Dans ce chapitre nous allons étudier le nombre (pour $m \neq 0$)

$$\varphi(m) = \left| \left( \frac{\mathbb{Z}}{(m)} \right)^\times \right|$$

$$= \left| \left\{ 0 \leq a < m \mid (a, m) = 1 \right\} \right|$$

[illegible]. La fonction $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ ainsi obtenue, est la fonction indicatrice d'Euler.

On fait d'abord la "mise en place":

Proposition : Soit $A$ un anneau (commutatif), alors l'ensemble $A^\times$ des éléments inversibles de $A$ est

un groupe (abélien) pour la multiplication dans $A$. Si $f : A \longrightarrow B$ est un homomorphisme d'anneaux, alors

$$f^\times : A^\times \longrightarrow B^\times : a \longmapsto f(a),$$

est un homomorphisme de groupes. De plus la correspondance $f \longmapsto f^\times$ est fonctorielle :

- si $f : A \longrightarrow B$ et $g : B \longrightarrow C$ sont des homom. d'anneaux, alors

$$(g \circ f)^\times = g^\times \circ f^\times$$

- et pour l'identité $1_A : A \longrightarrow A$ on a

$$(1_A)^\times = 1_{A^\times}.$$

□

Corollaire : Si $f : A \longrightarrow B$ est un isomorphisme d'anneaux, alors $f^\times : A^\times \longrightarrow B^\times$ est un isomorphisme de groupes. □

Proposition : Pour des anneaux $A_1, \ldots, A_k$,

$$(A_1 \times \cdots \times A_k)^\times = A_1^\times \times \cdots \times A_k^\times .$$

□

Corollaire : Soit $(m, n) = 1$ dans $\mathbb{N}^*$, alors $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

Preuve : Par le théorème chinois, on sait que $\mathbb{Z}/(m \cdot n) \cong \mathbb{Z}/(m) \times \mathbb{Z}/(n)$.

Il suit donc que

$$\left(\mathbb{Z}/(m\cdot n)\right)^\times \simeq \left(\mathbb{Z}/(m)\right)^\times \times \left(\mathbb{Z}/(n)\right)^\times$$

d'où

$$\left|\left(\mathbb{Z}/(m\cdot n)\right)^\times\right| = \left|\left(\mathbb{Z}/(m)\right)^\times\right| \times \left|\left(\mathbb{Z}/(n)\right)^\times\right|$$

comme voulu. □

Avec le résultat suivant, il sera facile d'établir une formule pour $\varphi(m)$ :

Proposition : Soit $p \in \mathbb{N}^*$ premier.

Alors $\varphi(p^n) = p^n - p^{n-1} = p^n\left(1 - \frac{1}{p}\right)$.

$= p^{n-1}(p-1)$

Preuve : Un élément $q \in \mathbb{Z}/(p^n)$ est inversible ssi $(q, p^n) = 1$, ssi $p \nmid q$.

Donc, $q \in \mathbb{Z}/(p^n)$ est non-inversible ssi $q = k \cdot p$ pour $k \in \{1, \dots, p^{n-1}\}$. Ainsi,

$$\varphi(p^n) = p^n - p^{n-1}$$

- $p^n$ : le # d'élt dans $\mathbb{Z}/(p^n)$
- $p^{n-1}$ : le # d'élts non-inv. dans $\mathbb{Z}/(p^n)$
- $\varphi(p^n)$ : le # d'élts inv. dans $\mathbb{Z}/(p^n)$

□

Théorème : Pour $m \in \mathbb{N}^*$, on a

$$\varphi(m) = m \cdot \prod_{\substack{p \mid m \\ p \text{ premier}}} \left(1 - \frac{1}{p}\right).$$

Preuve : Soit $n = p_1^{n_1} \cdots p_k^{n_k}$ la factorisation en facteurs premiers de $n$.

Alors

$$\varphi(n) = \varphi\left(p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k}\right)$$

$\downarrow (p_1^{n_1}, p_2^{n_2} \cdots p_k^{n_k}) = 1$

$$= \varphi(p_1^{n_1}) \cdot \varphi\left(p_2^{n_2} \cdots p_k^{n_k}\right)$$

$$\vdots$$

$$= \varphi(p_1^{n_1}) \cdot \varphi(p_2^{n_2}) \cdots \cdot \varphi(p_k^{n_k})$$

$$= p_1^{n_1}\left(1 - \frac{1}{p_1}\right) \cdot p_2^{n_2}\left(1 - \frac{1}{p_2}\right) \cdots p_k^{n_k}\left(1 - \frac{1}{p_k}\right)$$

$$= p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

par les propositions et corollaires précédents.

□

Voici un autre résultat concernant $\varphi$ :

**Proposition** : Pour $n \in \mathbb{N}^*$, on a

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

**Preuve** : Par récurrence sur le nombre de diviseurs premiers de $n$ :

- si $n = p^n$ :

$$\sum_{d|n} \varphi(d) = \sum_{i=0}^{n} \varphi(p^i)$$

$$= 1 + (p-1) + (p^2 - p) + \dots + (p^n - p^{n-1})$$

$$= p^n$$

$$= n$$

- si $n = p^n \cdot m'$ où $p \nmid m'$ (donc $m'$ a strictement moins de diviseurs premiers que $n$) :

$$\sum_{d|n} \varphi(d) = \sum_{\substack{d_1|p^n \\ d_2|m'}} \varphi(d_1 \cdot d_2) \qquad \left(\text{puisque } (p^n, m') = 1 \text{ !}\right)$$

$$= \sum_{\substack{i \leq n \\ d_2|m'}} \varphi(p^i \cdot d_2)$$

$$= \sum_{\substack{i \leq n \\ d_2|m'}} \varphi(p^i) \cdot \varphi(d_2)$$

$$= \left(\sum_{i \leq n} \varphi(p^i)\right) \cdot \left(\sum_{d_2|m'} \varphi(d_2)\right)$$

$$= p^n \cdot m' \qquad \left(\text{par le cas précédent + hypothèse de récurr.}\right)$$

$$= m \qquad \square$$

Pour poursuivre notre étude de la fonction d'Euler $\varphi$, nous devons étudier de plus près la structure des $\left(\mathbb{Z}/(m)\right)^\times$.
groupe abélien

On peut se demander ce que la formule

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

veut "dire". Pour en donner une explication conceptuelle (plutôt qu'une preuve par calcul), on passera par les groupes cycliques ; et d'ailleurs, on découvrira d'autres résultats "arithmétiques" en faisant de l'"algèbre". (VAUT LE DÉTOUR, dirait le Guide Michelin !)

Définition : Un groupe $(G, \cdot, 1)$ est cyclique s'il existe un $g \in G$, appelé générateur de $G$, tel que

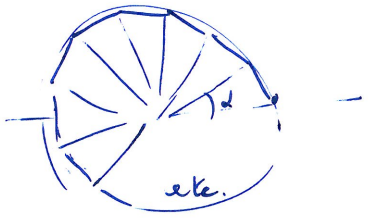
$$\{g^n \mid n \in \mathbb{Z}\} = G.$$

Remarque : Déjà dans la définition on voit le rôle que $\mathbb{Z}$ joue ! Ce n'est

donc pas étonnant qu'il y ait un lien intime entre l'arithmétique modulaire et les groupes cycliques !

Exemple : $(\mathbb{Z}, +, \circ)$ est cyclique, et $\forall m \in \mathbb{Z}^*$, $(\mathbb{Z}/(m), +, \circ)$ est cyclique.

Exemple : Soit le polygône régulier à $n$ côtés :




alors le groupe des rotations de ce polygône est cyclique.

Exemple : Soit $g \in G$ dans un groupe quelconque $(G, \cdot, 1)$, alors $\{g^n \mid n \in \mathbb{Z}\}$ est un sous-groupe cyclique.

**Proposition :** Soit $(G, \cdot, 1)$ un groupe quelconque, et $g \in G$, alors l'application

$$\varphi : \mathbb{Z} \longrightarrow G$$
$$: n \longrightarrow g^n$$

est un homomorphisme de groupes de $(\mathbb{Z}, +, 0)$ vers $(G, \cdot, 1)$. Cet homomorphisme est surjectif ssi $G$ est cyclique de générateur $g \in G$ ; dans ce cas on a

soit $(G, \cdot, 1) \simeq \left(\frac{\mathbb{Z}}{(m)}, +, 0\right)$ si $|G| = m$

soit $(G, \cdot, 1) \simeq (\mathbb{Z}, +, 0)$ si $|G| = \infty$.

**Preuve :** Il est évident que $\varphi$ est un homom de groupes (c'est "l'exponentielle

en base $g \in G$ "), et il est trivial que $\varphi$ est surjectif ssi $g$ engendre $G$. "Comme toujours" en algèbre, $\varphi$ induit un isomorphisme

$$\bar{\varphi} : \frac{\mathbb{Z}}{\ker(\varphi)} \longrightarrow G$$

où $\ker(\varphi) = \{ n \in \mathbb{Z} \mid g^n = 1 \}$. Il est facile de voir que tous les sous-groupes de $(\mathbb{Z}, +0)$ sont de la forme

$$(m) = \{ km \mid k \in \mathbb{Z} \}$$

(cela se fait de la même manière comme pour vérifier que $(\mathbb{Z}, +0, \cdot, 1)$ est un PID).

Ainsi on trouve

$$\frac{\mathbb{Z}}{(m)} \overset{\sim}{=} G$$

et le resultat suit selon le cas où $m = |G|$ ou $m = 0$ (si $|G| = \infty$). $\square$

Corollaire : Tout groupe cyclique est abélien.

Remarque : la théorie des groupes cycliques "est" donc la théorie des groupes additifs

$$(\mathbb{Z}, +, 0) \quad \text{et} \quad (\mathbb{Z}/(m), +, 0).$$

Autrement dit, c'est la théorie de l'arithmétique modulaire.

Mais il est utile de faire cette abstraction, car cela nous oblige à développer des arguments "purs" : des arguments qui ne dépendent de la structure de groupe cyclique de $(\mathbb{Z}/(m), +, 0)$, et non pas, p.e., de sa structure d'anneau.

Nous allons voir que, en particulier, la formule

$$\varphi(m) = \sum_{d \mid m} \varphi(d)$$

est significative dans le cadre des groupes cycliques...

**Définition** : Un groupe cyclique $(G, \cdot, 1)$ est d'ordre infini si $(G, \cdot, 1) \overset{\sim}{=} (\mathbb{Z}, +, 0)$, et d'ordre $m \in \mathbb{Z}^*$ si $(G, \cdot, 1) \overset{\sim}{=} (\mathbb{Z}/(m), +, 0)$.

**Définition** : Soit $(G, \cdot, 1)$ un groupe quelconque, et $g \in G$. L'ordre de $g \in G$ est par définition l'ordre de $\{g^n \mid n \in \mathbb{Z}\}$.

**Exercice** : L'ordre de $g \in G$ est le plus petit $n \in \mathbb{N}^*$ tel que $g^n = 1$ (si on suppose que $g$ est d'ordre fini, comme p.e. dans un groupe fini $G$).

**Exercice** : Donner l'ordre des éléments de $(\mathbb{Z}/(8), +, \cdot)$, et observer que ce sont tous des diviseurs de $8$...

Voici un résultat clé de la théorie des groupes :

Théorème ("de Lagrange") : Soit $(G, \cdot, 1)$ un groupe fini et $H \subseteq G$ un sous-groupe, alors

$$|H| \text{ divise } |G|.$$

Preuve : Pour tout $g \in G$, l'application

$$\varphi_g : H \longrightarrow G : h \longmapsto g \cdot h$$

est injective (exercice), et donc son image

$$\text{im}(\varphi_g) = gH = \{gh \mid h \in H\}$$

est en bijection avec $H$. Il suit que

$$|H| = |gH| \quad \forall g \in G.$$

Il est aussi clair que

$$\bigcup_{g \in G} gH = G.$$

Mais, en fait,

$$\begin{aligned} & x \in gH \cap g'H \\ \Rightarrow\ & x = gh = g'h' \qquad (h, h' \in H) \\ \Rightarrow\ & g = g'h'h^{-1} \quad \text{et} \quad g' = gh\,h'^{-1} \\ \Rightarrow\ & gH \subseteq g'H \quad \text{et} \quad g'H \subseteq gH \\ \Rightarrow\ & gH = g'H \end{aligned}$$

donc, pour tout $g, g' \in G$,

$$\begin{cases} \text{soit} & gH \cap g'H = \emptyset \\ \text{soit} & gH = g'H \end{cases}$$

Ainsi, en supprimant des sous-ensembles identiques dans la formule $G = \bigcup_{g \in G} gH$, on obtient une réunion disjointe ; et en comptant les éléments on trouve

$$\begin{aligned} |G| &= |H| \cdot (\#\text{ de classes } gH \text{ distinctes}) \\ &= |H| \cdot \underbrace{[G : H]}_{\substack{\text{"index" de } H \\ \text{dans } G}} \end{aligned}$$

□

**Corollaire** : L'ordre d'un élt d'un groupe fini, divise le # d'elts de ce groupe.

**Théorème ("d'Euler")** : Si $a, m \in \mathbb{Z}^*$ et $(a,m) = 1$, alors

$$a^{\varphi(m)} \equiv 1 \mod m.$$

**Preuve** : Puisque $(a,m) = 1$ on sait que $\bar{a} \in \left(\frac{\mathbb{Z}}{(m)}\right)^\times$. L'ordre de $\bar{a}$ divise donc $\varphi(m) = \left|\left(\frac{\mathbb{Z}}{(m)}\right)^\times\right|$ ;

et en particulier

$$\bar{a}^{\varphi(m)} = \overline{a^{\varphi(m)}} = \bar{1} \quad \text{dans } \frac{\mathbb{Z}}{(m)}.$$

Autrement dit,

$$a^{\varphi(m)} \equiv 1 \mod m.$$

□

**Corollaire ("Petit théorème de Fermat") :**

Pour tout nombre premier $p \in \mathbb{Z}$ et tout $a \in \mathbb{Z}$,

$$a^p \equiv a \mod p.$$

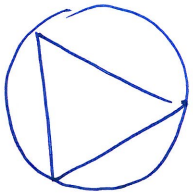
**Preuve :** Si $p \mid a$ alors $a^p \equiv 0 \equiv a \mod p$.

Si $p \nmid a$ alors $a^{p-1} \equiv 1 \mod p$ par Euler, donc $a^p \equiv a \mod p$. □

**Remarque :** Le théorème d'Euler dit que, si $(a, m) = 1$, alors l'ordre de $a$ *divise* $\varphi(m)$ ; il ne dit pas que l'ordre de $a$ est *égale* à $\varphi(m)$ ! En fait, l'exemple $m = 8$ montre qu'il n'y a pas toujours un élt de $(\mathbb{Z}/(m))^\times$ d'ordre $\varphi(m)$ : un tel groupe n'est donc pas toujours cyclique ...

On revient maintenant au problème d'"expliquer" la formule $\varphi(n) = \sum_{d|n} \varphi(d)$.
Pour cela, on décrit d'abord un autre lien fascinant entre groupes cycliques et $\varphi$ ...

Exemple : Pour un même groupe cyclique on peut avoir plusieurs générateurs distincts.
P.e.



les rotations du triangle sont engendrées par "1/3 de tour", mais aussi par "2/3 de tour".

où encore, $(\mathbb{Z}/(4), +, \circ)$ est (bien sûr) engendré par $\bar{1}$, mais aussi par $\bar{3}$ ! (exercice).

Question naturelle : combien de générateurs différents y a-t-il dans un groupe cyclique ?

Proposition : Dans un groupe cyclique d'ordre $n$ il y a $\varphi(n)$ générateurs distincts.

Preuve : Soit $(G, \cdot, 1)$ un groupe cyclique d'ordre $n$, engendré par $g \in G$. Un autre élément $g' = g^k \in G$ est aussi générateur ssi tout élt de $G$ est une puissance de $g'$ (par déf$^{n}$), ssi $g$ est une puissance de $g'$ (évident), ssi il existe $l \in \mathbb{Z}$ tel que $g = g^{kl}$, ssi il existe $l \in \mathbb{Z}$ tel que $kl \equiv 1 \bmod n$ (puisque l'ordre du générateur $g$ est $n$), ssi $(k, n) = 1$ (par un résultat du chap. précédent.) Il y a donc $\varphi(n) = \left|\left(\frac{\mathbb{Z}}{n}\right)^\times\right|$ choix pour un tel $k \in \mathbb{Z}$, donc pour un tel générateur $g' = g^k \in G$. □

On peut maintenant peaufiner le théorème de Lagrange pour les groupes cycliques :

Proposition : Soit $(G, \cdot, 1)$ un groupe cyclique d'ordre $m$, engendré par $g \in G$. Alors $S \subseteq G$ est un sous-groupe ssi $S$ est cyclique, d'ordre $k$, $k$ divise $m$, engendré par $g^{\frac{m}{k}}$.

Preuve : Soit $k \in \mathbb{N}^*$ le plus petit nombre naturel non-nul tel que $g^k \in S$. Par un argument typique (exercice ; on utilise la division euclidienne ...) il est facile de voir que alors

$$S = \{ g^{kn} \mid n \in \mathbb{Z} \} ;$$

ainsi, $S$ est cyclique d'ordre $k$, engendré par $g^k$. Et puisque $1 = g^m$

est un élément de $S$, il suit que $m = kn$ pour un certain $n \in \mathbb{Z}$, càd que $k$ divise $m$.

Réciproquement, si $k$ divise $m$ alors il est clair que $g^{\frac{m}{k}}$ engendre un sous-groupe cyclique d'ordre $k$. $\square$.

Remarque : On aurait pu prouver les deux propositions précédentes d'une autre manière : un groupe cyclique $(G, \circ, 1)$ d'ordre $m$ engendré par $g \in G$ est en isomorphisme avec $(\mathbb{Z}/(m), +, \circ)$ par

$$\bar{\varphi} : \mathbb{Z}/(m) \longrightarrow G : \bar{n} \longmapsto g^n$$

(cf. p. 95-96). Il suffit donc de

prouver les résultats pour $(\mathbb{Z}/(m), +_0)$, et puis de "transférer" ces résultats "par isomorphisme" aux groupes cycliques quelconques. Mais les preuves que nous avons données ici sont aussi instructives : car on y apprend à calculer avec un générateur quelconque.

On peut maintenant – finalement! – donner une explication à la formule $m = \sum_{d|m} \varphi(d)$.

Corollaire : Pour $m \in \mathbb{N}^*$, $m = \sum_{d|m} \varphi(d)$.

Preuve : Soit $(G, \cdot, 1)$ un groupe cyclique d'ordre $m$. Par la proposition précédente, pour chaque $d|m$ il existe

un unique sous-groupe d'ordre $d$ de $G$. (à savoir le sous-groupe engendré par $g^{\frac{m}{d}}$ où $g \in G$ est un générateur choisi de $G$). De l'autre côté, chaque élément $g' \in G$ engendre un sous-groupe de $G$, d'un certain ordre, divisant $m$. On a donc une partition

$$G = \bigcup_{d|m} G_d$$

où $G_d = \{$ élts d'ordre $d$ de $G\}$

$= \{$ générateurs de l'unique sous-groupe d'ordre $d$ de $G\}$

et en comptant les élts on trouve

$$m = |G| = \sum_{d|m} |G_d| = \sum_{d|m} \varphi(d).$$

□

— 6 —

# Racines primitives

*Nous définissons la notion de racine primitive modulo $m \in \mathbb{Z}$, et donnons quelques exemples illustrant leur utilité. Puis nous prouvons un critère de cyclicité pour un groupe commutatif fini donné, et observons que le groupe multiplicatif $K^\times$ d'un corps (commutatif) fini $K$ est cyclique. Ainsi il suit qu'il existe toujours une racine primitive modulo un nombre premier $p$. Faute de temps, nous donnons sans preuve un théorème caractérisant exactement ces $m \in \mathbb{Z}$ admettant une racine primitive. Pour terminer, nous définissons encore la notion de résidu de puissance $n$-ième modulo $m$ (faisant donc le lien avec la solvabilité de $X^n \equiv a \mod m$), et nous prouvons une caractérisation simple des résidus de puissance $n$ modulo $m$, pourvu que $m$ admette une racine primitive. Les exercices illustrent les techniques de calcul modulaire que nous avons développé dans ce chapître ainsi que dans les deux chapîtres précédents.*

Racines primitives

## 6 ~~Logarithme discret~~.

Habituellement ~~Dans un groupe cyclique~~, on définit le logarithme, pour $x, y, z \in \mathbb{R}$, comme

$$\log_x(y) = z \iff x^z = y.$$

C'est à dire, on cherche à déterminer un exposant (pour une base donnée). C'est dans ce sens-là, qu'il faudra comprendre le terme "logarithme discret" : dans un groupe cyclique $(G, \cdot, 1)$ de générateur $g \in G$, on veut, pour $h \in G$ donné, déterminer l'exposant $k \in \mathbb{Z}$ tel que $g^k = h$. Dans le cadre de l'arithmétique modulaire, ce sont

les groupes $\left(\mathbb{Z}/(m)\right)^\times$ qui nous intéressent... mais ils ne sont pas tous cycliques !

Exemple (cf. exercices) :

$\left(\mathbb{Z}/(7)\right)^\times$ est cyclique ; générateur 3

$\left(\mathbb{Z}/(8)\right)^\times$ n'est pas cyclique

$\left(\mathbb{Z}/(11)\right)^\times$ est cyclique ; générateur 3

(... donc il n'est pas nécessaire que $m$ soit premier !)

etc. □

Il nous faut une terminologie adéquate :

**Définition :** Soit $a, m \in \mathbb{Z}$. On dit que $a$ est une racine primitive modulo $m$ si $a + (m)$ est un générateur du groupe $\left(\mathbb{Z}/(m)\right)^\times$.

On dit qu'il existe une racine primitive modulo $m$ si le groupe $\left(\mathbb{Z}/(m)\right)^\times$ est cyclique.

**Proposition :** $a \in \mathbb{Z}$ est racine primitive modulo $m \in \mathbb{Z}$ si et seulement si $(a, m) = 1$ et $\varphi(m)$ est le plus petit élément de $\mathbb{N}^*$ tel que $a^{\varphi(m)} = 1$. □

L'utilité des racines primitives (si elles existent !) est illustré par l'exemple suivant :

Exemple : On peut facilement vérifier que $2+(11)$ est générateur de $\left(\mathbb{Z}/(11)\right)^\times$ :

1°) $2X \equiv 1 \pmod{11}$ a une solution, puisque $(2,11) = 1$, donc $2+(11) \in \left(\mathbb{Z}/11\right)^\times$,

2°)

| $k$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $2^k$ | 1 | 2 | 4 | 8 | 5 | 10 | 9 | 7 | 3 | 6 | 1 |

donc $\{1, \dots, 10\} = \{2^0, 2^1, \dots, 2^9\} \pmod{11}$.

Ceci nous aide à calculer des produits dans $\mathbb{Z}/(11)$ :

$$7 \cdot 9 \equiv 2^7 \cdot 2^6 \quad (11)$$

$$\equiv 2^{13} \quad (11)$$

$$\equiv 2^3 \quad (11)$$

$$\equiv 8 \quad (11)$$

$\varphi(11)$

$2^{\varphi(11)} \equiv 1 \ (11)$.

on encore

$$5^{372} \equiv (2^4)^{372} \quad (11)$$

$$\equiv 2^{1488} \quad (11)$$

$$\equiv 2^8 \quad (11)$$

$$\equiv 3 \quad (11).$$

$2^{372}_{4}$

$1488$

$2^{\varphi(11)} \equiv 1 \ (11)$

Mais aussi (et surtout) la résolution de carrés (et d'autres puissances) est facilitée : par exemple, existe-t-il un $x \in (\mathbb{Z}/11)^\times$ tel que

$$x^2 \equiv 7 \quad (11) \quad ?$$

Si oui, on sait que $x \equiv 2^k (11)$ et $7 \equiv 2^7 (11)$

donc l'équation devient

$$2^{2k} \equiv 2^7 \quad (11)$$

---

$$2k \equiv 7 \quad (\varphi(11))$$

$$\equiv 7 \quad (10)$$

pair — impair

donc il n'y a pas de solution ! □.

Voilà pour l'intérêt de l'existence d'une racine primitive modulo $m$, et donc l'intérêt de caractériser les $m \in \mathbb{Z}$ en admettant une ! On prouve d'abord un critère de cyclicité d'un groupe abélien fini quelconque (et bien sûr on retrouve

la fonction d'Euler !) :

Lemme : Soit $(G, \cdot, 1)$ un groupe fini commutatif. Alors $G$ est cyclique si et seulement si, pour tout $d \mid |G|$,

$$\left| \{ g \in G \mid g \text{ est d'ordre } d \} \right| \leq \varphi(d).$$

Preuve : Notons $m = |G|$ et, pour $d \mid m$,

$$G_d = \{ g \in G \mid g \text{ est d'ordre } d \}.$$

Alors, par le thm de Lagrange on sait qu'il y a une partition

$$G = \bigcup_{d \mid m} G_d,$$

donc, en comptant les élts des deux côtés,

$$m = \sum_{d \mid m} |G_d|.$$

Si $|G_d| \leq \varphi(d)$ pour tout $d|n$,

alors

$$n = \sum_{d|n} |G_d| \leq \sum_{d|n} \varphi(d) = n,$$

donc nécessairement

$$|G_d| = \varphi(d).$$

Cela veut dire que, en particulier,

$$|G_n| = \varphi(n) \neq 0,$$

donc il existe un élément d'ordre $n$ dans le groupe $G$, donc nécessairement un générateur de $G$ : $G$ est cyclique.

Réciproquement, si $G$ est cyclique d'ordre $n$, alors pour tout $d|n$,

il existe un unique sous-groupe d'ordre $d$ de $G_1$ et les éléments de $G_d$ en sont nécessairement les générateurs. Il suit donc que

$$|G_d| = \varphi(d)$$

ce qui implique l'inégalité voulue. □

Application du lemme :

Proposition : Pour tout nombre premier $p$, $\left(\frac{\mathbb{Z}}{(p)}\right)^{\times}$ est cyclique.

Preuve :

Une variante sur ce lemme sera tout aussi utile :

Lemme : Soit $(G, \cdot, 1)$ un groupe fini commutatif. Si, pour tout $d \mid |G|$,

$$\left| \{ g \in G \mid g^d = 1 \} \right| \leq d$$

alors $G$ est cyclique.

Preuve : On note $H_d = \{ g \in G \mid g^d = 1 \}$, cet on garde la notation $G_d \subseteq G$ de la preuve précédente ; il est clair que $G_d \subseteq H_d$.

Il est aussi clair que $H_d \subseteq G$ est un sous-groupe. Ainsi, si $g \in G_d$, alors le sous-groupe (d'ordre $d!$) engendré par $g$ est inclus dans $H_d$ :

$$\langle g \rangle \subseteq H_d .$$

Comme ces deux ensembles finis ont

le même nombre d'éléments (par hypothèse sur $H_d$), on obtient bien égalité : $\langle g \rangle = H_d$. Ceci implique que $H_d$ est l'unique sous-groupe d'ordre $d$ de $G$, que $G_d$ contient des générateurs de ce groupe cyclique, et que donc $|G_d| \leq \varphi(d)$. Le lemme précédent donne le résultat. □

Application des lemmes :

Proposition : Soit $K$ un corps fini commutatif, alors $(K^\times, \cdot, 1)$ est un groupe cyclique.

Preuve : le nombre de racines du polynôme $X^d - 1$ est inférieur ou égal à $d$ sur un corps $K$ (même si ce corps est fini) (exercice). □

La conséquence suivante est cruciale pour l'arithmétique modulaire :

Théorème ("de Gauss") : Pour tout nombre premier $p$, $\left(\frac{\mathbb{Z}}{(p)}\right)^\times$ est cyclique. Autrement dit, il existe toujours une racine primitive modulo $p$.

Preuve : $\frac{\mathbb{Z}}{(p)}$ est un corps fini. (exercice) □

~~Remarque~~ Il n'est pas super-difficile, mais quand-même un peu technique, de caractériser exactement les $m \in \mathbb{Z}$ tels que $\left(\mathbb{Z}/(m)\right)^\times$ soit cyclique. Nous n'allons pas le faire ici, mais voici le résultat, à titre informatif :

Théorème (donné sans preuve) : Il existe une racine primitive modulo $m \in \mathbb{Z}$ si et seulement si

- soit $m = 2$
- soit $m = 4$
- soit $m = p^n$ avec $p$ premier $\neq 2$ et $n \geqslant 1$
- soit $m = 2 \cdot p^n$ avec $p$ premier $\neq 2$ et $n \geqslant 1$.

□

Pour terminer le chapitre, voici une application : le calcul des "résidus de puissances".

Définition : Pour $m, n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$ tel que $(a, m) = 1$, on dit que $a$ est un résidu de puissance $n$-ième si

$$X^n \equiv a \mod m$$

admet une solution.

Exemple : 7 n'est pas un résidu d'un carré dans $\left(\frac{\mathbb{Z}}{(71)}\right)^\times$, comme nous avons vu au début du chapitre.

On va "généraliser" l'argument donné dans cet exemple, pour démontrer :

Proposition : Si $m \in \mathbb{N}^*$ admet une racine primitive, et $(a, m) = 1$, alors $a$ est un résidu de puissance $n$ si et seulement si

$$a^{\frac{\varphi(m)}{(n, \varphi(m))}} \equiv 1 \mod m.$$

Preuve : Soit $g \in \left(\frac{\mathbb{Z}}{(m)}\right)^\times$ un générateur, alors

$$\frac{X^n \equiv a \ (m)}{g^{nY} \equiv g^b \ (m)} \quad \downarrow \begin{cases} X = g^Y \\ a = g^b \end{cases}$$

$$\frac{}{nY \equiv b \ (\varphi(m))}$$

admet une solution (en $Y$) ssi

$$(n, \varphi(m)) \mid b .$$

(et dans ce cas il y a exactement $(n, \varphi(m))$ solutions, cf. un chapitre précédent !).

Notons $d = (n, \varphi(m))$.

Si $d \mid b$ alors $a^{\frac{\varphi(m)}{d}} \equiv g^{\frac{b}{d} \cdot \varphi(m)} \equiv 1 \ (m)$ par Euclide. Réciproquement, si $a^{\frac{\varphi(m)}{d}} \equiv 1 \ (m)$, alors

$$1 \equiv a^{\frac{\varphi(m)}{d}} \equiv g^{\frac{b}{d}\varphi(m)} \mod m$$

donc nécessairement $\varphi(m) \mid \frac{b}{d}\varphi(m)$, donc nécessairement $d\varphi(m) \mid d \cdot \frac{b}{d} \cdot \varphi(m)$, càd, $d \mid b$. □

Remarque : Le théorème chinois, le théorème (donné sans preuve) à la page 122 et la proposition ci-dessus permettent de vérifier si $a \in \mathbb{Z}$ est un résidu de puissance $n$ modulo $m$ de la manière suivante :

$$X^n \equiv a \ (m)$$

$$\Updownarrow \qquad \left( m = 2^e \cdot p_1^{e_1} \cdots p_k^{e_k} \text{ avec } 2 < p_1 < \cdots < p_k \text{ premiers} \right)$$

$$\begin{cases} X^n \equiv a \ (2^e) & \left.\right] \leftarrow \text{la proposition s'applique si } e = 1, 2. \\ X^n \equiv a \ (p_1^{e_1}) & \left.\right] \\ \vdots & \left.\right] \text{la proposition s'applique dans tous les cas} \\ X^n \equiv a \ (p_k^{e_k}) & \left.\right] \end{cases}$$

(Si $e \geq 3$, il existe d'autre résultats pour calculer le résidu $X^n \equiv a \ (2^e)$ que nous n'avons pas le temps de développer ici.)

Exemple : Existe-t-il une solution pour

$$X^6 \equiv 3 \ (28) \ ?$$

On a

$$X^6 \equiv 3(28) \iff \begin{cases} X^6 \equiv 3 \ (4) \\ X^6 \equiv 3 \ (7) \end{cases}$$

Or, $X^6 \equiv 3(4)$ admet une sol ssi $3^{\frac{\varphi(4)}{(6,\varphi(4))}} \equiv 1 \ (4)$

ssi $3^{\frac{2}{2}} \equiv 1 \ (4)$ : c'est ok.

Et, $X^6 \equiv 3(7)$ admet une sol ssi $3^{\frac{\varphi(7)}{(6,\varphi(7))}} \equiv 1 (4)$

ssi $3^{\frac{6}{6}} \equiv 1 \ (4)$ ; c'est ok.

Donc, oui, il existe un $X$ tq $X^6 \equiv 3 \ (28)$.

Remarque : Ce que l'on vient de faire dans ce chapitre (et les deux chapitres précédents), n'est que le tout début de l'arithmétique modulaire ! Il y

a encore plein de sujets intéressants (et très accessibles dans un cours au niveau M1), mais nous n'avons malheureusement pas le temps de les aborder. On peut penser notamment à la réciprocité quadratique, ou encore les nombres $p$-adiques (et le Principe de Hasse pour l'existence de racines d'un polynôme $ax^2 + by^2 = z^2$ sur $\mathbb{Q}$).

De l'autre côté, l'arithmétique modulaire est toujours un sujet de recherche, avec beaucoup de questions ouvertes ! Par exemple, il y a la célèbre conjecture d'Artin : "si $a \in \mathbb{Z} \setminus \{-1\}$ n'est pas un carré, alors il existe une infinité de

nombres premiers pour lesquels a est une racine primitive". D'ailleurs, la taille du plus petit a qui est racine primitive modulo p, est encore un mystère aussi. Il y a plein d'autres questions ouvertes de ce genre !

---

# Extensions de corps

— 7 —

# Corps de racines

*Nous donnons la définition d'extension de corps $L \supseteq K$ et de son degré $[L : K]$, et prouvons que $[M : K] = [M : L] \cdot [L : K]$ si $M \supseteq L \supseteq K$. Puis nous montrons que, pour un polynôme irreductible $f \in K[X]$, le corps $K[X]/(f)$ est une extension de $K$ de degré $\deg(f)$ engendré par la racine $a = X + (f)$ de $f$. Cela nous mène naturellement à la définition d'élément algébrique $a \in L \supseteq K$ et son polynôme minimal $\mathsf{min}(a, K)$, et d'extension algébrique, dont nous développons quelques propriétés générales. Finalement nous définissons le corps de racines d'un polynôme, et nous prouvons que pour tout $f \in K[X]$ il existe un corps de racines $L \supseteq K$ ; faute de temps, nous ne démontrons pas que ce corps est essentiellement unique. Dans les exercices, nous calculons en particulier des polynômes minimaux, et des extensions concrètes de $\mathbb{Q}$.*

## Corps de racines d'un polynôme

7 ~~[illegible]~~.

Le polynome

$$P(X) = X^2 - 3 \quad \in \mathbb{Q}[X]$$

n'a pas de racines sur $\mathbb{Q}$, car $\sqrt{3} \notin \mathbb{Q}$.

Pour résoudre ce polynôme, i.e. pour le scinder en facteurs linéaires, on devra donc "agrandir" le corps $\mathbb{Q}$ pour inclure les racines de $P(X)$. Mais on veut faire cela de la manière la "plus économe" qui soit, donc en ajoutant juste ce qu'il faut pour scinder $P(X)$, mais pas plus. (le théorème fondamental de l'algèbre nous garantit que $P(X)$ scinde sur $\mathbb{C}$, mais $\mathbb{C}$ ~~[illegible]~~ est "trop grand".)

Cela nous mène à la théorie des "corps de racines de polynômes".

Il existe une vaste "théorie de corps" comprenant notamment la "théorie de Galois" sur les extensions de corps ; faute de temps nous allons nous concentrer sur les "corps de racines". Voir la définition générale pertinente :

Définition : Soit $K \subseteq L$ une inclusion de corps (plus généralement on considère un homom. $K \xrightarrow{f} L$ et on identifie $K$ avec son image par $f$) : on dit que $L$ est une extension de $K$, et que

$$[L:K] = \dim_K(L)$$

est le <u>degré</u> de l'extension. On dit que $L:K$ est une <u>extension finie</u> si $[L:K] < \infty$.

<u>Proposition</u> : Soient $K \subseteq L \subseteq M$ des corps, alors

$$[M:K] = [M:L] \cdot [L:K].$$

(En particulier : $[M:K] = \infty \iff [M:L] = \infty$ et/ou $[L:K] = \infty$.)

<u>Preuve</u> : Si $(m_i)_{i=1}^r \in M$ est libre sur $L$, et $(l_j)_{j=1}^s \in L$ est libre sur $K$, alors $(m_i \cdot l_j)_{i,j} \in M$ est libre sur $K$ (<u>exercice</u>). Donc, si $[M:L] = \infty$ et/ou $[L:K] = \infty$, alors nécessairement $[M:K] = \infty$.

Supposons que $[M:L] = r$ et $[K:L] = s$; alors $(m_i \cdot l_j)_{i,j} \in M$ est une base sur $K$ (<u>exercice</u>), donc $[M:K] = r \cdot s$. □

Exemple : 1) $[\mathbb{C} : \mathbb{R}] = 2$ ; base $= \{1, i\}$.

2) $[K(X) ; K] = \infty$, car $K[X] \subset K(X)$ et $\dim_K(K[X]) = \infty$. (On n'écrit pas $[K[X] : K] = \infty$, car $K[X]$ n'est pas un corps ! )

3) $[\mathbb{R} : \mathbb{Q}] = \infty$. Pas trivial à voir : on sait que $\mathbb{Q}$ est dénombrable, mais que $\mathbb{R}$ ne l'est pas (Cantor), donc $\mathbb{R}$ ne peut pas être de dimension finie en tant que $\mathbb{Q}$-espace vectoriel.

~~Voici un lien intime entre la théorie des extensions de corps, et la théorie des polynômes :~~

~~Définition : Un élément $a \in L : K$ est algébrique s'il existe $f \in K[X]$ tel que~~ $\deg(f) \geq 1$

Comment peut-on ~~obtenir~~ construire une extension d'un corps ? L'exemple ci-dessous montre le lien avec les polynômes :

Exemple : Soit $f \in K[X]$ un polynôme irréductible ; il suit donc que

$$K \longrightarrow K[X] \longrightarrow \frac{K[X]}{(f)}$$

est un homomorphisme d'anneaux entre deux corps. En identifiant $K$ avec son image dans $\frac{K[X]}{(f)}$, on obtient une extension de $K$. C'est une extension finie, car (par application de la division euclidienne)

$$\left[ \frac{K[X]}{(f)} : K \right] = \deg(f).$$

De plus, si on note

$$a = X + (f) \in \frac{K[X]}{(f)}$$

(i.e. $a$ est la classe d'équivalence de $X$ dans le quotient de $K[X]$ par $(f)$) alors on obtient que

$$\frac{K[X]}{(f)} = \{ g(a) \mid g \in K[X] \}$$
$$\vdots\!\vdots$$
$$K[a]$$

(En effet, si

$$p(X) = p_n X^n + \cdots + p_1 X + p_0 \in K[X]$$

alors

$$\begin{aligned} p(a) &= p(X + (f(X))) \\ &= p_n (X + f(X))^n + \cdots + p_1 (X + f(X)) + p_0 \\ &= p_n X^n + \cdots + p_1 X + p_0 + q(X) \cdot f(X) \\ &= p(X) + q(X) \cdot f(X) \end{aligned}$$

donc $p(a) = p(X) + (f)$ .) De

plus, il est évident que

$$f(a) = f(X + (f))$$

$$= f(X) + q(X) \cdot f(X)$$

$$= 0 \qquad (\text{dans } \frac{K[X]}{(f)}) .$$

Autrement dit, avec le polynôme irréductible $f \in K[X]$ nous avons construit une extension finie $K[a] : K$ où $a$ est une racine de $f$ ! □

Exemple : $X^2+1 \in \mathbb{R}[X]$ est irréductible, donc $\frac{\mathbb{R}[X]}{(X^2+1)}$ est une extension finie (de degré 2, càd le degré de $X^2+1$)

de $\mathbb{R}$. Si on note $a = X + (X^2+1)$

alors on sait que

- $a$ est racine de $X^2+1$
- $\dfrac{\mathbb{R}[X]}{(X^2+1)} \simeq \mathbb{R}[a] = \{g(a) \mid g \in \mathbb{R}[X]\}$.

Autrement dit, on retrouve $\mathbb{C}$ (et on écrit $a = i$). □

Question naturelle : est-ce que toute extension (finie) peut être construite de cette manière ? Ça dépend ...

Exemple : Soit $a \in L : K$. On a certainement un homomorphisme

$$ev_a : K[X] \longrightarrow L : g \longmapsto g(a)$$

et donc

$$K[X]/\ker(ev_a) \cong \mathrm{im}(ev_a).$$

Par définition on a bien

$$\mathrm{im}(ev_a) = \{ g(a) \mid g \in K[X] \} =: K[a]$$

et puisque $K[X]$ est un PID on sait aussi que

$$\ker(ev_a) = (f) \text{ pour un } f \in K[X].$$

Mais, est-il toujours vrai que ce $f$ est irréductible ? (et de tel sorte que donc $\ker(ev_a) = (f)$ est un idéal premier (non-nul), donc maximal, donc $K[a] = K[X]/(f)$ un corps) ?

La réponse est non : il n'est a priori pas exclu que $f=0$ ! Mais, ceci est la seule obstruction :

Lemme : Avec les notations précédentes, $\ker(ev_a) \neq 0$ ssi $\ker(ev_a)$ est un idéal maximal de $K[X]$.

Preuve : Un idéal maximal est non-nul par définition. Réciproquement, si $g \cdot h \in \ker(ev_a)$, alors $g(a) \cdot h(a) = 0$ dans le corps $L$, donc $g(a) = 0$ ou $h(a) = 0$, donc $g \in \ker(ev_a)$ ou $h \in \ker(ev_a)$. Càd, $\ker(ev_a) \trianglelefteq K[X]$ est toujours premier ; et si $\ker(ev_a) \neq 0$ alors il est aussi maximal (car $K[X]$ PID). □

Par ailleurs, on voit facilement que :

Lemme : Avec les notations précédentes,
$\ker(ev_a) \neq 0$ ssi il existe $f \in K[X] \setminus K$
tel que $f(a) = 0$.

Preuve : "$\Leftarrow$" est évident, et pour "$\Rightarrow$"
on observe que $f \in \ker(ev_a) \setminus \{0\}$
implique $f \in K[X] \setminus K$ car $ev_a(f) = 0$.

□

Ceci motive finalement :

Définition : Un élément $a \in L : K$ est
algébrique s'il existe un $f \in K[X] \setminus K$
tel que $f(a) = 0$. Une extension $L : K$
est algébrique si tous les $a \in L$ sont
algébriques (sur $K$).
(non-algébrique = transcendant).

Etant donné un élt algébrique $a \in L : K$, on va maintenant caractériser les générateurs (irréductibles) de l'idéal $\ker(ev_a)$ :

Proposition : Avec les notations précédentes, on a pour un élt algébrique $a \in L : K$ l'équivalence des conditions suivantes pour un $f \in K[X] \setminus K$ :

(a) $\ker(ev_a) = (f)$,

(b) $f(a) = 0$ et $f$ irréductible,

(c) $f(a) = 0$ et pour tout $g \in K[X]$ tel que $g(a) = 0$ on a $\deg(f) \leq \deg(g)$

("$f$ est de degré minimale")

(d) $f(a) = 0$ et $f$ divise tout $g \in K[X]$ tel que $g(a) = 0$

De plus, si on choisit $f$ unitaire, alors c'est l'unique polynôme ayant ces propriétés : on l'appelle le polynôme minimale de $a \in L:K$, noté $\min(a, K)$.

Preuve :

(a) $\Leftrightarrow$ (b) $\Leftrightarrow$ (d) : par ce qui précède et par la déf$^{n}$ de $\ker(ev_a)$.

(c) $\Rightarrow$ (d) : si $g(a) = 0$ alors $\deg(f) \leq \deg(g)$ par hypothèse donc

$$g = f \cdot h + k$$

par division euclidienne ; mais $k = 0$ parce que $k(a) = 0$ (puisque $g(a) = 0$ et $f(a) = 0$), donc $f \mid g$.

(d) $\Rightarrow$ (c) : Evident

□

On peut maintenant "formaliser" les construction données dans l'exemple précédent :

Théorème : Soit $a \in L : K$ ; on note donc

$$ev_a : K[X] \longrightarrow L : g \longmapsto g(a)$$

et $K[a] = \mathrm{im}(ev_a)$.

Alors $a$ est algébrique ssi $K[a]$ est un corps et $[K[a] : K] < +\infty$.

Dans ce cas,

$$[K[a] ; K] = \deg\left(\min(a, K)\right)$$

$$K[a] \simeq \frac{K[X]}{(\min(a,K))}$$

et $K[a]$ est le plus petit sous-corps de $L$ contenant $K$ et $a$. On écrit alors $K(a) = K[a]$.

Preuve : Dans les exemples ci-dessus nous avons déjà vu que, si $a \in L : K$ est algébrique, alors

$$K[a] = \frac{K[X]}{(\min(a,K))}$$

est un corps et $[K[a] : K] = \deg(\min(a,K))$.

Réciproquement, si $K[a]$ est un corps et $[K[a] : K] = n < \infty$, alors

$$1, a, a^2, \dots, a^n$$

sont linéairement dépendents dans le $K$-espace $K[a]$ : cela dit exactement qu'il existe $k_0, k_1, \dots, k_n \in K$

tel que $a$ est racine du polynôme

$$k_n X^n + \dots + k_1 X + k_0 \in K[X],$$

donc $a$ est algébrique.

Finalement il est clair que $K(a)$ contient $K$ et $a$ ; et tout autre corps $K' \subseteq L$ contenant $K$ et $a$ contient aussi $g(a)$ pour tout $g \in K[X]$. Donc $K(a) \subseteq K'$. □

Remarque : L'argument du théorème peut être itéré : si $a_1, \dots, a_n \in L : K$ sont algébriques, alors

$$K(a_1, \dots, a_n) := K(a_1, \dots, a_{n-1})(a_n)$$

est le plus petit sous-corps de $L$

contenant $K$ et $a_1, \dots, a_n$. (En effet, si $a_n \in L$ est algébrique sur $K$, alors $a_n$ l'est aussi sur $K(a_1, \dots, a_{n-1})$ ! Même si le polynôme caractéristique de $a_n$ sur $K(a_1, \dots, a_{n-1})$ peut être différent de son polynôme caractéristique sur $K$ !)

On dit alors que $a_1, \dots, a_n$ sont les générateurs du corps $K(a_1, \dots, a_n)$. □

Enfin nous arrivons à la notion dans le titre de ce chapitre :

Définition : Si $f \in K[X]$ se décompose en facteurs linéaires dans une extension $L : K$, alors $L$ est un corps de déploiement de $f$. Si de plus $L$

est engendré par les racines de $f$,

alors $L$ est un corps de racines de $f$.

Tout polynôme peut être scindé !

Théorème : Pour tout $f \in K[X]$ il existe un corps de racine $L$, et

$$[L : K] \leq \deg(f)! .$$

Preuve : Si $p \in K[X]$, $\deg(p) \geq 1$ est un facteur irréductible de $f$, alors on pose $L_1 = \frac{K[X]}{(p)}$ et on aura une extension $L_1 : K$ telle que

$$[L_1 : K] = \deg(p) \leq \deg(f)$$

De plus, en posant $a_1 = X + (p)$ on

sait que $L_1 = K[a_1]$ et $p(a_1) = 0$,

donc aussi $f(a_1) = 0$. Il s'agit

donc d'une extension de $K$ par une

racine de $f$, et cette extension est de

degré $\leq \deg(f)$.

On sait donc que

$$f(X) = (X - a_1) \cdot g(X) \quad \text{dans } L_1[X]$$

et nécessairement $\deg(g) = \deg(f) - 1$. On

itère le procédé sur $g$, et après au

plus $\deg(f)$ itérations on aura trouvé

le corps $\overbrace{\quad}^{L:K}$ de racines de $f$, satisfaisant

$$[L : K] = [L_n : L_{n-1}] \cdot \ldots \cdot [L_1 : K]$$

$$\leq 1 \cdot 2 \cdot \ldots \cdot \deg(f)$$

$$\leq \deg(f)!$$

et aussi

$$L_n = L_{n-1}(a_n) = \dots = K(a_1, \dots, a_n).$$

où $a_1, \dots, a_n$ sont les racines de $f$ qui n'appartiennent pas à $K$. (Donc $n \leq \deg(f)$.)
Il va de soi que l'on peut encore ajouter les racines de $f$ dans $K$ à $K(a_1, \dots, a_n)$, cela n'agrandira pas ce corps. □

Remarque : Il est possible de montrer que, si $L$ et $L'$ sont deux corps de racines d'un même polynôme $f \in K[X]$, alors il existe un isomorphisme

$$\varphi : L \xrightarrow{\sim} L'$$

tel que $\varphi|_K = \text{identité}$. Autrement dit, "le" corps de racines de $f$ est essentiellement unique

la proposition suivante implique que toutes les extension que nous avons construite, sont algébriques :

Proposition : Toute extension $L:K$ finie est algébrique.

Preuve : Si $[L:K]=n$ et $a\in L$, alors $1, a, \dots, a^n$ sont liés dans le $K$-espace $L$. □

Corollaire : Si $a\in L:K$ est algébrique alors $K(a):K$ est algébrique. Si $f\in K[X]$ est irréductible alors $\frac{K[X]}{(f)}:K$ est algébrique. Et le corps de racines d'un $f\in K[X]$ quelconque est algébrique sur $K$. □

Exemple : $X^3 - 2 \in \mathbb{Q}[X]$

Il n'y a pas de racines rationnelles (exercice) donc ce polynôme est irréductible dans $\mathbb{Q}[X]$. (Alternative : critère d'Eisenstein.) On calcule le corps de racines :

1°) $K = \dfrac{\mathbb{Q}[X]}{(X^3-2)} = \mathbb{Q}(a)$ où

$a = X + (X^3 - 2)$

est racine de $X^3 - 2$.

dans $K[X]$ on a alors que

$$X^3 - 2 = (X - a) \cdot g$$

et on peut calculer $g \in K[X]$ :

$$\begin{array}{r|l} X^3-2 & X-a \\ \hline X^3-aX^2 & X^2+aX+a^2 \\ \hline aX^2-2 & \\ aX^2-a^2X & \\ \hline a^2X-2 & \\ a^2X-a^3 & \\ \hline a^3-2=0 & \end{array}$$

car $a$ est racine de $X^3-2$

donc $g(X) = X^2+aX+a^2$.

et donc $X^3-2 = (X-a)(X^2+aX+a^2)$

où $a$ est une racine (au choix !) de $X^3-2$

Le polynôme $X^2+aX+a^2$, est-il irréductible dans $\mathbb{Q}(a)[X]$ ?

Si oui, on continue le procédé,

Si non, on le scinde (et alors $\mathbb{Q}(a)$ est le corps de racine de $X^3-2$).

En fait, si on choisit

$$a = \sqrt[3]{2} \in \mathbb{R}$$

alors on voit que les racines de $X^2+aX+a^2$ sont

$$\frac{-a \pm \sqrt{-3a^2}}{2} \in \mathbb{C} \setminus \mathbb{R}$$

Donc, puisque

$$\mathbb{Q}(a) \subsetneq \mathbb{R}$$

on peut déduire que $X^2+aX+a^2$ est irréductible sur $\mathbb{Q}(a)$.

2°) $L = \dfrac{K[X]}{(X^2+aX+a^2)} = K(b) = \mathbb{Q}(a,b)$

où $b = X + (X^2+aX+a^2)$ est

racine de $X^2+aX+a^2$.

dans $L[X]$ on a alors que

$$X^2+aX+a^2 = (X-b)\cdot h$$

et en fait

$$\begin{array}{l|l} X^2+aX+a^2 & X-b \\ \hline X^2-bX & X+(a+b) \\ \hline (a+b)X+a^2 & \\ (a+b)X-(a+b)b & \\ \hline a^2+ab+b^2 = 0 \text{ car } g(b)=0. & \end{array}$$

donc

$$X^2+aX+a^2 = (X-b)(X+(a+b))$$

donc

$$X^3 - 2 = (X-a)(X-b)(X+(a+b))$$

où $a = \sqrt[3]{2}$

$b$ = racine de $X^2 + aX + a^2$,
donc $\dfrac{-a \pm \sqrt{-3a^2}}{2}$

dans $\mathbb{Q}(a,b)$.

D'ailleurs, $\mathbb{Q}\left(\underbrace{\sqrt[3]{2}}_{a}, \dfrac{-a \pm \sqrt{-3a^2}}{2}\right)$

$= \mathbb{Q}(a, \sqrt{-3a^2})$

~~$\neq \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}\cdot\sqrt[3]{2})$~~.

$= \mathbb{Q}(a, \sqrt{-3}\cdot a)$

$= \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$.

— 8 —

# Nombres constructibles

*Après avoir donné la définition "géométrique" d'un point constructible à la règle et au compas dans un plan, nous prouvons en détail qu'un point de $\mathbb{R}^2$ est constructible si et seulement si ses coordonnées peuvent être obtenues de $0$ et $1$ par une séquence finie d'opérations rationnelles et/ou extractions de racines carrées. Autrement dit, un nombre $a \in \mathbb{R}$ est constructible (i.e. le point $(a, 0) \in \mathbb{R}^2$ est constructible) si et seulement s'il existe une suite d'extensions de corps $\mathbb{Q} = K_0 \subseteq K_1 \subseteq ... \subseteq K_r$ telle que $a \in K_r$ et $[K_{i+1} : K_i] \leq 2$ pour tout $i$. Il suit que, si $a \in \mathbb{R}$ est constructible, alors $a$ est algébrique sur $\mathbb{Q}$ et $[\mathbb{Q}(a) : \mathbb{Q}]$ est une puissance de 2. Cela nous permet de montrer qu'il est impossible de construire un cube de volume 2, ou de trisecter l'angle $\alpha = \frac{\pi}{3}$, ou encore de faire la quadrature du cercle. Dans les exercices, nous regardons de plus près les polygones réguliers constructibles et les extensions cyclotomiques.*

## [8] Nombres constructibles

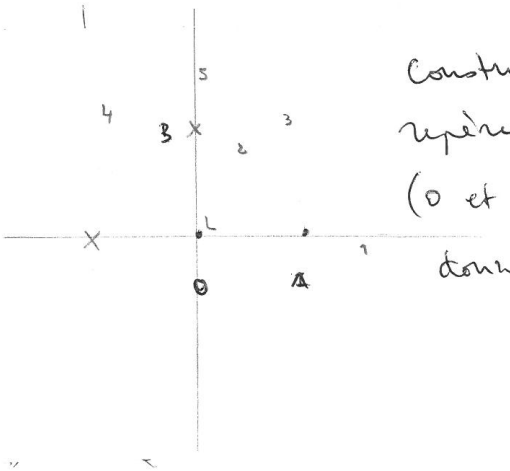
On se place dans le plan, et on choisit deux points, O et A. On se permet de "construire" de nouveaux points comme intersection de

- droites passant par deux points déjà construits

et/ou

- cercles ayant un centre déjà construit et passant par un point déjà construit.

Exemple :




Construction d'un repère orthogonal (O et A sont donnés).

Il est donc clair que l'on peut toujours construire une base orthogonale dans le plan, et donc on peut "faire de la géométrie analytique". Cela nous permet de formaliser (= algébriser) la notion de point constructible, en faisant le lien avec les extensions de corps $\mathbb{Q} \subseteq K \subseteq \mathbb{R}$ :

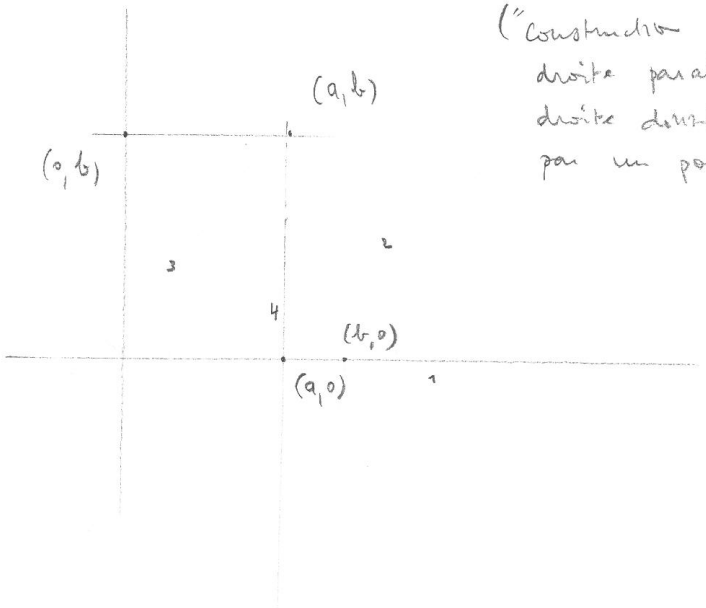
Théorème : Un point du plan est constructible par règle et compas de O et A si et seulement si ses coordonnées dans la base (OA, OB) peuvent être obtenues de 0 et 1 par une séquence finie d'opérations de type suivant :

- opération rationelles $(+, -, \times, :)$,
- racines carrées $(\sqrt{\ })$.

On donne la preuve de ce théorème comme une suite de lemmes :

Lemme : $(a, b)$ est constructible si et seulement si $(a, 0)$, et $(0, b)$ sont constructibles, si et seulement $(a, 0)$ et $(b, 0)$ sont constructibles.

Preuve : Géométrie élémentaire ...

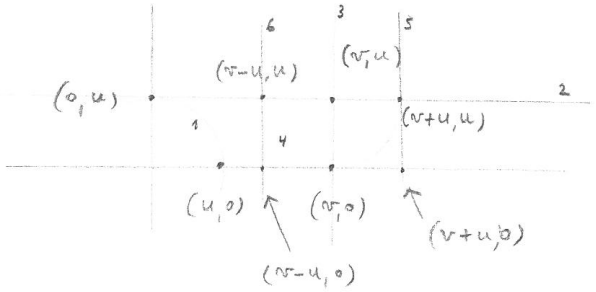


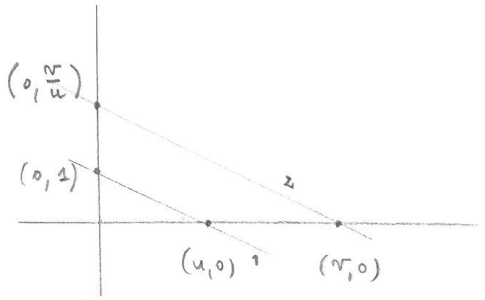

("construction d'une droite parallèle à une droite donnée, passant par un point")

□

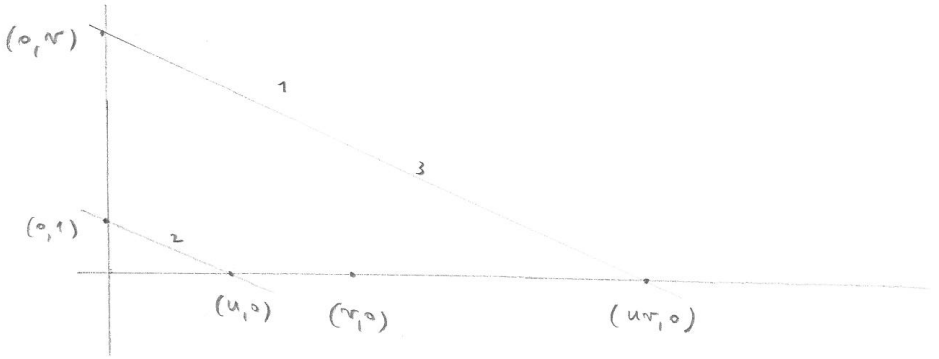
**Lemme** : Si $(u,0)$ et $(v,0)$ sont constructibles, alors aussi $(u+v,0)$, $(-u+v,0)$, $(uv,0)$ et $\left(\frac{v}{u},0\right)$ (pour $u \neq 0$).

**Preuve** : Géométrie élémentaire...



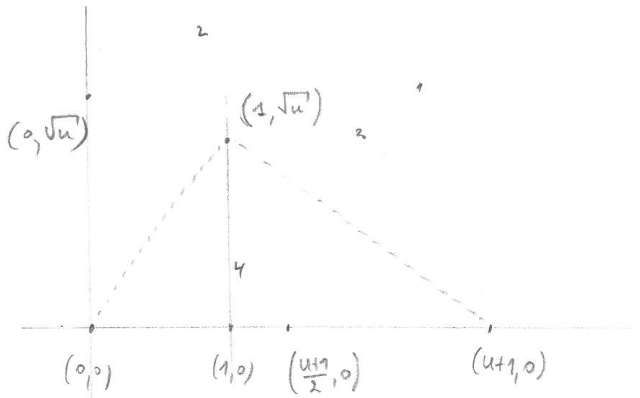

(triangles semblables, donc $\frac{A'}{A} = \frac{B'}{B}$.)




□

**Lemme :** Si $(u,0)$ est constructible, alors aussi $(\sqrt{u},0)$ est constructible (pour $u \geqslant 0$).

**Preuve :**





congruence de $\Rightarrow \frac{B'}{B} = \frac{A'}{A}$

et $B = A'$ donc $\frac{u}{B} = \frac{B}{1}$ donc $u = B^2$ donc $B = \sqrt{u}$.

□

Cela prouve déjà la moitié du théorème. Pour la réciproque, on observe d'abord :

158

Lemme : Si une droite passe par $(a_1, b_1)$ et $(a_2, b_2)$, alors son équation est

$$A \cdot X + B Y = C$$

avec $A, B$ et $C$ des expressions rationnelles en $a_1, a_2, b_1, b_2$. Si un cercle est de centre $(a_1, b_1)$ et passe par $(a_2, b_2)$, alors son équation est

$$X^2 + Y^2 = AX + BX + C$$

avec $A, B$ et $C$ des expressions rationnelles en $a_1, a_2, b_1, b_2$.

Preuve : Presque trivial : l'équation de la droite est

$$(b_2 - b_1) X + (a_1 - a_2) Y = b_1 a_2 - a_1 b_2$$

et celle du cercle est

$$(X-a_1)^2 + (Y-b_1)^2 = (a_1-a_2)^2 + (b_1-b_2)^2.$$

□

Lemme : Si $(a,b)$ est solution du système

$$\begin{cases} AX + BY = C \\ A'X + B'Y = C' \end{cases}$$

alors $a$ et $b$ sont des expressions rationnelles en $A, B, C, A', B', C'$.

Preuve : Algèbre linéaire (= résolution de système).

□

Lemme : Si $(a,b)$ est solution au système

$$\begin{cases} AX + BY = C \\ X^2 + Y^2 = A'X + B'Y + C' \end{cases} \qquad (1)$$

alors $a$ et $b$ peuvent être obtenus par opérations rationnelles et extraction de racine carrée sur $A, B, C, A', B', C'$.

Preuve : On ne peut pas avoir $A = 0 = B$ ; donc on peut supposer $A \neq 0$ ; donc on peut diviser (1) par $A$ ; donc on peut supposer $A = 1$ dans (1) : le système est donc

$$\begin{cases} X + BY = C \iff X = C - BY \\ X^2 + Y^2 = A'X + B'Y + C' \end{cases} \qquad (2)$$

Il suit de (2) que

$$(C - BY)^2 + Y^2 = A'(C - BY) + B'Y + C'$$

et ceci étant une équation de degré 2, on sait qu'il y a soit aucune solution, soit une, soit deux ; et s'il y a des solutions, elles sont données par la formule

$$Y = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

(pour $aY^2 + bY + c = 0$),

donc par opérations rationnelles et racine carrée. Il suit que $X = C - BT$ est aussi donné par opérations rationnelles et racine carrée. □

Lemme : Si $(a, b)$ est une solution au Système

$$\begin{cases} X^2 + Y^2 = AX + BY + C \\ X^2 + Y^2 = A'X + B'Y + C' \end{cases}$$

alors $a$ et $b$ sont données par opérations rationnelles et racines carrées sur $A, B, C, A', B', C'$.

Preuve : Le système étant équivalent à

$$\begin{cases} X^2 + Y^2 = AX + BY + C \\ (A - A')X + (B - B')Y + (C - C') = 0 , \end{cases}$$

le lemme précédent s'applique. □

Ainsi le théorème est prouvé !

On fera maintenant le lien avec les extensions de corps ; on dira qu'un nombre $a \in \mathbb{R}$ est constructible si le point $(a, 0)$ l'est.

Théorème : Un nombre $a \in \mathbb{R}$ est constructible si et seulement si il existe une suite d'extensions de corps

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r$$

telle que $a \in K_r$ et $[K_{n+1} : K_n] \leq 2$ pour tout $n$.

Preuve : C'est une "traduction" du théorème précédent : les coordonnées de l'intersection de deux droites, d'une droite avec un cercle, ou de deux cercles, dont les équations sont des polynômes avec coefficients dans $K_n$, se calcule en faisant des opérations

rationnelles sur ces coefficients (donc on reste dans $K_n$) et en prenant une racine carrée d'une expression rationnelle de ces coefficients (auquel cas on doit "agrandir" $K_n$ en ajoutant cette racine si elle n'y est pas encore) : ainsi, à chaque étape de la construction on fait "au plus" une extension quadratique (ie. une extension de degré 2) du corps précédent. Et il est clair que le corps de départ est $\mathbb{Q}$, puisque toutes les fractions $\frac{m}{n}$ sont constructibles.

□

Remarque : Malheureusement, le théorème ci-dessus ne donne pas une construction

géométrique explicite pour chaque nombre constructible ! Par exemple, Gauss savait que

$$\cos\left(\frac{2\pi}{17}\right) = -\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34-2\sqrt{17}}$$
$$+ \frac{1}{8}\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}$$

(à l'age de 18 ans ...) et donc il se réalisait que le 17-gone régulier était constructible ... en principe! Car la première construction a été donné quelques années après les travaux de Gauss sur ce sujet.

Corollaire : Si $a \in \mathbb{R}$ est constructible, alors $a$ est algébrique sur $\mathbb{Q}$, et $[\mathbb{Q}(a) : \mathbb{Q}]$ est une puissance de 2.

Preuve : Si $a$ est constructible, alors on a des extensions de corps

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \dots \subseteq K_r \ni a$$

et $[K_r : \mathbb{Q}]$ est une puissance de 2. Il suit que $\mathbb{Q} \subseteq \mathbb{Q}(a) \subseteq K_r$ donc

$$[\mathbb{Q}(a) : \mathbb{Q}] \text{ divise } [K_r : \mathbb{Q}] = [K_r : \mathbb{Q}(a)] \cdot [\mathbb{Q}(a) : \mathbb{Q}]$$

d'où le résultat. □

Ce corollaire permet de répondre à quelques questions "historiques" :

Exemple

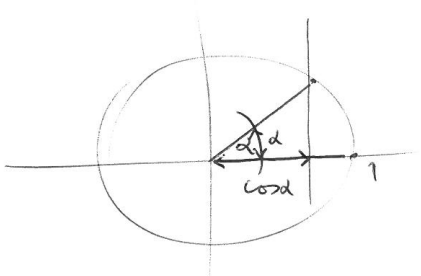
**~~Proposition~~** : Il est impossible de construire à règle et compas un cube de volume 2.

**~~Preuve~~** : En effet, le nombre $\sqrt[3]{2}$ n'est pas constructible, car $\deg(\min(\sqrt[3]{2}, \mathbb{Q})) = 3$ n'est pas une puissance de 2. □

Exemple

**~~Proposition~~** : Il est impossible de tri-secter un angle quelconque à règle et compas.

**~~Preuve~~** Construire un angle $\alpha$ est équivalent à construire $\cos\alpha$ :




Prenons $\alpha = \frac{\pi}{3}$, alors $\cos\alpha = \frac{1}{2}$ donc

c'est constructible. Mais on sait que

$$\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha$$

donc en particulier

$$4\cos^3\left(\frac{\pi}{9}\right) - 3\cos\left(\frac{\pi}{9}\right) = \cos\left(\frac{\pi}{3}\right) = \frac{1}{2}.$$

C'est à dire, le nombre $\cos\left(\frac{\pi}{9}\right) \in \mathbb{R}$ est algébrique, car racine de

$$4X^3 - 3X - \frac{1}{2},$$

ou encore de

$$8X^3 - 6X - 1.$$

Ce polynôme n'a pas de racines rationnelles, donc est irréductible, donc

$$\left[\mathbb{Q}\left(\cos\left(\tfrac{\pi}{9}\right)\right) : \mathbb{Q}\right] = 3.$$

Ainsi, $\cos\left(\frac{\pi}{9}\right)$ n'est pas constructible. □

Exemple : Il est impossible de construire un carré de même aire qu'un cercle de rayon 1.

: Ceci revient à construire le nombre $\sqrt{\pi}$, mais par un résultat (difficile!) de Lindemann - Weierstrass, $\sqrt{\pi}$ est transcendant sur $\mathbb{Q}$. Donc $[\mathbb{Q}(\sqrt{\pi}), \mathbb{Q}] = \infty$. □

Dans les exercices on va détailler l'exemple suivant :

Exemple : Un $n$-gone régulier peut être construit si et seulement si $\varphi(n)$ est une puissance de 2.

(En fait, nous allons prouver la nécessité de cette condition; nous n'aurons pas le temps pour développer assez de mathématiques pour prouver la suffisance.)

— 9 —

# Résolution par radicaux

*Nous commençons par poser le problème de déterminer les polynômes irréductibles $f \in \mathbb{Q}[X]$ qui sont résolubles par radicaux. Puis nous définissons le groupe de Galois $\mathsf{Gal}(L : K)$ d'une extension $L \supseteq K$, et remarquons que, si $M \supseteq L \supseteq K$, alors $\mathsf{Gal}(M : L) \subseteq \mathsf{Gal}(M : K)$ est un sous-groupe. Ainsi nous motivons le théorème ("de Galois"), que nous donnons sans preuve, disant qu'un irréductible $f \in \mathbb{Q}[X]$ est résoluble par radicaux si et seulement si le groupe de Galois de son corps de racines est résoluble. Ensuite nous montrons qu'un irréductible $f \in \mathbb{Q}[X]$ n'a pas de racines doubles (dans un corps de déploiement quelconque), et que donc son groupe de Galois est un sous-groupe du groupe symétrique $S_n$, où $n = \deg(f)$. Après avoir montré que tout sous-groupe d'un groupe résoluble est résoluble, et aussi que $S_2$, $S_3$ et $S_4$ sont des groupes résolubles, il suit que tout polynôme irréductible $f \in \mathbb{Q}[X]$ de $\deg(f) \leq 4$ est résoluble par radicaux. Pour $n \geq 5$, nous donnons sans preuve le résultat que $S_n$ n'est pas résoluble et qu'il existe un irréductible $f \in \mathbb{Q}[X]$ de degré $n$, ayant $S_n$ comme groupe de Galois : ainsi il suit qu'un polynôme de degré $n \geq 5$ n'est en général pas résoluble par radicaux. Nous illustrons ce résultat avec un exemple. Dans les exercices nous donnons explicitement une solution par radicaux pour les équations cubiques et quartiques, et nous parlons brièvement d'extensions galoisiennes.*

## 9| Résolution d'équations par radicaux

Pour $f \in \mathbb{Q}[X]$ donné par

$$f(X) = aX^2 + bX + c,$$

on sait calculer les racines dans $\mathbb{C}$ (qui, par le "thm fondamental de l'algèbre", est un corps de déploiement de $f$) :

$$r_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a}$$

$$r_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a}.$$

On s'aperçoit que les racines de $f$ sont données ~~plus~~, en fonction des

coefficients de $f$, par des opérations rationnelles et l'extraction de racines.

Autrement dit, les racines de $f$ sont des éléments de l'extension

$$\mathbb{Q}\left(\sqrt{b^2-4ac}\right) : \mathbb{Q},$$

et cette extension est (clairement) obtenue "en ajoutant une racine (carrée)" à $\mathbb{Q}$.

D'ailleurs, sur cette extension $f$ se déploie : $f$ se factorise en termes linéaires dans $\mathbb{Q}\left(\sqrt{b^2-4ac}\right)[X]$.

Plus généralement, on utilisera la définition suivante :

Définition : Un $f \in K[X]$ est résoluble par radicaux s'il existe une suite d'extensions de corps

$$K = L_0 \subseteq L_1 \subseteq \dots \subseteq L_m$$

telle que :

1°) $f$ est déployé dans $L_m[X]$,

2°) $\forall i$ : $L_{i+1} = L_i(\alpha_i)$ et $\alpha_i^{n_i} \in L_i$.

Remarque : Si $\beta = \alpha^n \in K$ mais $\alpha \notin K$, alors on appelle $K(\alpha) = K(\sqrt[n]{\beta})$ une extension $n$-radicale de $K$ : on ajoute à $K$ une racine $n$-ième. La définition ci-dessus exprime donc que $f$ admet

toutes ses racines dans un corps obtenu par extensions radicales successives.

Question naturelle : Quels $f \in K[X]$ sont résolubles par radicaux ?

Puisque les racines de $f$ sont exactement les racines des facteurs irréductibles de $f$, il suffit de considérer de $f \in K[X]$ qui sont irréductibles. Et pour nous simplifier la vie, on prendra $K = \mathbb{Q}$.

Réponse brillante de Galois : On passe par la théorie des groupes !

Dans le reste du chapitre nous allons étudier la résolubilité par radicaux des $f \in \mathbb{Q}[X]$ irréductibles. Faute

de temps, nous ne pouvons pas développer toutes les preuves ; mais nous essayons néanmoins de donner l'idée derrière la "théorie de Galois".

Définition : Soit une extension $L : K$.
Un K-automorphisme de L est un isomorphisme de corps

$$\varphi : L \longrightarrow L$$

tel que $\varphi_{|K} = id_K$ (ie $\varphi(x) = x \ \forall x \in K$).
Le groupe de Galois de $L : K$ est le sous-groupe de $Aut(L)$ des K-automorphismes ; on le note

$$Gal(L : K).$$

Exemple : Pour $\mathbb{C} : \mathbb{R}$, $\varphi(a+bi) = a-bi$ est un $\mathbb{R}$-automorphisme de $\mathbb{C}$.

Proposition : Soient des corps $K \subseteq L \subseteq M$, alors on a un sous-groupe

$$Gal(M:L) \subseteq Gal(M:K).$$

Preuve : Évident. □

Plus généralement, pour une suite d'extensions de corps

$$K = L_0 \subseteq L_1 \subseteq \dots \subseteq L_m,$$

on a une suite de sous-groupes

$$Gal(L_m : L_{m-1}) \subseteq \dots \subseteq Gal(L:K).$$

Par manque de temps nous ne pouvons malheureusement pas détailler le résultat (non-trivial !) suivant :

Théorème ("de Galois" ; donné sans preuve) :
Soit $f \in \mathbb{Q}[X]$ un polynôme irréductible et $K : \mathbb{Q}$ son corps de racines. Alors $f$ est résoluble par radicaux si et seulement si il existe une suite de sous-groupes

$$\{id\} = H_0 \subseteq H_1 \subseteq \dots \subseteq H_m = Gal(K:\mathbb{Q})$$

telle que

1°) $H_i \trianglelefteq H_{i+1}$ (sous-groupe normal), et

2°) $H_{i+1}/H_i$ est abélien. □

Remarque : Avec les notations du théorème, on dit que $Gal(K:\mathbb{Q})$ est le groupe de Galois de $f \in \mathbb{Q}[X]$. Et un groupe $G$ satisfaisant la condition du théorème, est appelé résoluble. Ainsi on peut donc résumer ce théorème comme :

> " un $f \in \mathbb{Q}[X]$ irréductible est résoluble (par radicaux) si et seulement si son groupe de Galois est résoluble ".

Dans la suite nous allons indiquer pourquoi tout $f \in \mathbb{Q}[X]$ de degré $\leq 4$ est résoluble, et pourquoi ce n'est pas le cas si $\deg(f) \geq 5$.

Lemme : Si $f \in \mathbb{Q}[X]$ est irréductible, alors $f$ n'a pas de racines multiples (dans des extensions de $\mathbb{Q}$).

Preuve : Supposons que $a \in K : \mathbb{Q}$ est tel que $f(a) = 0$. Alors

$$f(X) = (X - a) \cdot g(X)$$

dans $K[X]$, et il suit que

$$f'(X) = g(X) + (X - a) \cdot g'(X)$$

par "dérivation formelle". On voit donc que $a$ est une racine multiple de $f$ ssi $g(a) = 0$ ssi $f'(a) = 0$. Or, puisque $f$ est irréductible, il est le polynôme minimale de $a \in K : \mathbb{Q}$.

Comme $\deg(f') < \deg(f)$, il est donc impossible que $f'(a) = 0$. Il suit que $a$ ne peut pas être une racine multiple de $f$. □

Remarque : En général, un $f \in K[X]$ sans racines multiples est appelé séparable. Et une extension algébrique $L:K$ est dite séparable si le polynôme minimale de chaque $a \in L:K$ est séparable.
Le lemme ci-dessus implique que toute extension finie de $\mathbb{Q}$ est (algébrique et) séparable ; c'est en particulier le cas des corps de racines d'un $f \in \mathbb{Q}[X]$ irréductible.

**Proposition :** Soit $f \in \mathbb{Q}[X]$ irréductible, et $\deg(f) = n$. Si $K : \mathbb{Q}$ est le corps de racines de $f$, alors pour tout

$$\varphi \in \mathrm{Gal}(K : \mathbb{Q})$$

il existe un unique

$$\sigma \in S_n \quad (= \text{groupe symétrique des bijections de } \{1, \dots, n\})$$

tel que

$$\varphi(r_i) = r_{\sigma(i)} \qquad \forall\, i \in \{1, \dots, n\}$$

où $r_1, \dots, r_n$ sont les racines de $f$.

**Preuve :** Si $f(r) = 0$ ([illegible] pour $r \in K : \mathbb{Q}$) et $\varphi \in \mathrm{Gal}(K : \mathbb{Q})$, alors aussi

$$f(\varphi(r)) = \varphi(f(r)) = 0,$$

donc $\varphi(r)$ est aussi une racine de $f$ si $r$ en est une. Puisque $f$ est une bijection, il suit que $\varphi$ permute ainsi les racines de $f$. Autrement dit, si $r_1, \dots, r_n$ sont les racines de $f$, alors il existe une permutation $\sigma \in S_n$ telle que

$$\varphi(r_i) = r_{\sigma(i)}.$$

Le lemme précédent assure que $f$ n'a pas de racines doubles, donc cette permutation $\sigma \in S_n$, déterminée par $\varphi \in \mathrm{Gal}(K:\mathbb{Q})$, est unique. □

Corollaire : Dans la situation de la proposition précédente, $\mathrm{Gal}(K:\mathbb{Q})$ est un sous-groupe de $S_n$ (à isomorphisme près).

Remarque :

En fait, puisque $K = \mathbb{Q}(z_1, \dots, z_n)$ est le corps de racines de $f \in \mathbb{Q}[X]$, il n'est pas difficile de voir qu'une permutation $\sigma \in S_n$ est dans (une copie isomorphe de) $\mathrm{Gal}(K : \mathbb{Q})$ si et seulement si

$$\forall\, g \in K[X_1, \dots, X_n] :$$

$$g(z_1, \dots, z_n) = 0 \implies g(z_{\sigma(1)}, \dots, z_{\sigma(n)}) = 0.$$

(exercice !).

Il est un peu plus difficile, par contre, de prouver que

$$\left| \mathrm{Gal}(K : \mathbb{Q}) \right| = [K : \mathbb{Q}],$$

où $K$ est le corps de racines d'un $f \in \mathbb{Q}[X]$ irréductible. Mais, puisque $\mathrm{Gal}(K : \mathbb{Q}) \subseteq S_n$ (où $n = \deg(f)$), ceci

"confirme" le résultat (que nous avons prouvé) que $[K:\mathbb{Q}] \leq n!$ .

~~[illegible]~~

Le groupe de Galois d'un $f \in \mathbb{Q}[X]$ irréductible est donc un sous-groupe de $S_n$ ($n = \deg(f)$); et $f$ est résoluble par radicaux si et seulement si ce sous-groupe de $S_n$ est résoluble. Pour caractériser les $f \in \mathbb{Q}[X]$ qui sont résoluble par radicaux, nous devons donc étudier la résolubilité de (sous-groupes de) $S_n$ .

Lemme : Tout sous-groupe d'un groupe résoluble est résoluble.

Preuve : Soit $G$ résoluble, avec

$$\{id\} = H_0 \subseteq H_1 \subset \dots \subseteq H_m = G$$

une suite de sous-groupes telle que $H_i \trianglelefteq H_{i+1}$ est normal, et $H_{i+1}/H_i$ est abélien. Si $G' \subseteq G$ est un sous-groupe, alors on a une suite de sous-groupes

$$\begin{array}{ccccccc} G' \cap H_0 & \subseteq & G' \cap H_1 & \subseteq & \dots & \subseteq & G' \cap H_m \\ \| & & & & & & \| \\ \{id\} & & & & & & G' \end{array}$$

Il suit que :

1) si $x \in G' \cap H_i$ et $y \in G' \cap H_{i+1}$, alors $xyx'y' \in G' \cap H_i$ (parce que $H_i \trianglelefteq H_{i+1}$), donc $G' \cap H_i \trianglelefteq G' \cap H_{i+1}$ est normal,

2) si $x, y \in G' \cap H_{i+1}$ sont tels que $xy^{-1} \in H_i$, alors $xy^{-1} \in G' \cap H_i$.

Autrement dit, si $xH_i = yH_i$ dans $H_{i+1}/H_i$ alors $x(G' \cap H_i) = y(G' \cap H_i)$ dans $\dfrac{G' \cap H_{i+1}}{G' \cap H_i}$. On a donc une

injection $\dfrac{G' \cap H_{i+1}}{G' \cap H_i} \hookrightarrow \dfrac{H_{i+1}}{H_i}$

de groupes, montrant que $\dfrac{G' \cap H_{i+1}}{G' \cap H_i}$ est abélien.

□

Lemme : $S_2$, $S_3$ et $S_4$ sont des groupes résolubles.

Preuve : Trivial pour $S_2$ (en fait, tout groupe abélien est trivialement

résoluble). Pour $S_3$ on peut vérifier que

$$\{id\} \subset A_3 \subset S_3$$

est une suite de sous-groupe satisfaisant aux critères. Et pour $S_4$ on a la suite

$$\{id\} \subset H \subset A_4 \subset S_4$$

avec $H = \{id, (12)(34), (13)(24), (14)(23)\}$.

□

Il suit immédiatement que :

Proposition : Tout $f \in \mathbb{Q}[X]$ irréductible de degré $\leq 4$ est résoluble par radicaux. □

Question évidente : et si $n \geq 5$ ?

Malheureusement nous n'avons pas le temps pour démontrer le résultat suivant :

Théorème : Pour $n \geq 5$, $S_n$ n'est pas résoluble. Pour $n \geq 5$, il existe un $f \in \mathbb{Q}[X]$ irréductible ayant $S_n$ comme groupe de Galois. Donc, en général, un polynôme de degré $n \geq 5$ n'est pas résoluble par radicaux.

□

Nous allons illustrer ce théorème avec un exemple.

Exemple : Soit $f(X) = X^5 - 4X + 2$ dans $\mathbb{Q}[X]$ ; c'est un polynôme irréductible (par Eisenstein). Soit $K : \mathbb{Q}$ le corps de racines de $f$, et $G = Gal(K : \mathbb{Q})$ le groupe de Galois de $f$. On sait donc que $G \subseteq S_5$ est un sous-groupe, et

$$|G| = [K : \mathbb{Q}].$$

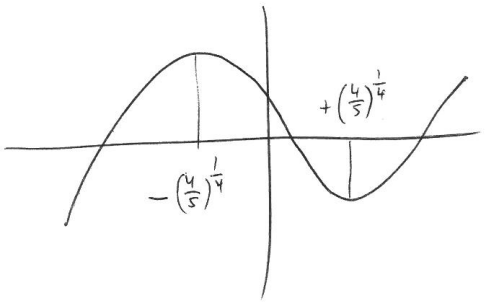
Mais si $a \in K$ est une racine de $f$, alors

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(a)] \cdot [\mathbb{Q}(a) : \mathbb{Q}]$$

et $[\mathbb{Q}(a) : \mathbb{Q}] = \deg(f) = 5$, donc $|G|$ est un multiple de 5 (et un diviseur de $|S_5| = 120$). Cela implique que $G$ a un élément d'ordre 5. (**)

189

A propos des racines de $f$, une "étude de fonction" indique que le "graphe" de $f$ (dans $\mathbb{R}^2$) est :




$f(X) = -\infty$ si $X \longrightarrow -\infty$

$f(X) = +\infty$ si $X \longrightarrow +\infty$

$f'(X) = 5X^4 - 4$ donc zéro en $\pm \sqrt[4]{\frac{4}{5}}$

(racines réelles de $f'$)

$f''(X) = 20X^3$ donc $\begin{cases} \text{négat en } -\left(\frac{4}{5}\right)^{\frac{1}{4}} \\ \text{posit en } +\left(\frac{4}{5}\right)^{\frac{1}{4}} \end{cases}$

Donc, $f$ admet 3 racines réelles, et nécessairement 2 racines complexes.

D'ailleurs, ces 2 racines complexes sont nécessairement conjugées (par le "théorème fondamental" de l'algèbre), et donc $G \subseteq S_5$ contient un élément de $S_5$ qui fixe 3 éléments et permute les 2 autres (cela correspond à l'automorphisme qui fixe les trois racines réelles et permute (par conjugaison) les deux racines complexes).

Mais si $G$ contient un élément d'ordre 5 (donc une "permutation totale" sur 5 élts) et une transposition (fixer 3 élts et permuter les deux autres), alors nécessairement $G = S_5$. (exercice!)

Conclusion: $f \in \mathbb{Q}[X]$ n'est pas résoluble par radicaux.

# Exercices et références

— 10 —

# Exercices

*Voici 9 fiches d'exercices—une pour chaque chapitre.*

EXERCICES EN ARITHMÉTIQUE (M1 MATH) – 1

Isar STUBBE

On fixe un objet de nombres naturels $(\mathbb{N}, 0 \in \mathbb{N}, s\colon \mathbb{N} \to \mathbb{N})$ et on écrit $1 = s(0)$, $2 = s(1)$, etc.

1. Démontrer avec les définitions récursives de $+$ et $\cdot$ que, pour tout $m, n, l \in \mathbb{N}$,
   a. $l + (m + n) = (l + m) + n$,
   b. $m + n = n + m$,
   c. $m + l = n + l \Rightarrow m = n$,
   d. $m + n = 0 \Rightarrow m = 0$ et $n = 0$,
   e. $m \cdot 1 = m$,
   f. $l \cdot (m + n) = l \cdot m + l \cdot n$,
   g. $l \cdot (m \cdot n) = (l \cdot m) \cdot n$,
   h. $m \cdot n = n \cdot m$,
   i. $m \cdot l = 0 \Rightarrow m = 0$ ou $l = 0$.
   j. $m \cdot l = n \cdot l \Rightarrow l = 0$ ou $m = n$.

2. Montrer, pour tout $m, n \in \mathbb{N}$, l'équivalence des assertions suivantes:
   a. $n \leq m$ et $n \neq m$,
   b. il existe $l \in \mathbb{N}$ tel que $n + s(l) = m$;
   on écrit $n < m$ (ou $m > n$) dans cette situation.

3. Prouver la "propriété de trichotomie" de l'ordre sur $\mathbb{N}$. Indication: Montrer d'abord que les trois sitations possibles ($m < n$, $m = n$ et $m > n$) sont exclusives. Montrer ensuite que chacune de ces situations implique une des situations $s(m) < n$, $s(m) = n$ ou $s(m) > n$ (sans oublier le cas $m = 0$ pour conclure par récurrence sur $m$).

4. Démontrer le principe de *récurrence à partir de* $n_0$ sur $\mathbb{N}$: soit un élément $n_0 \in \mathbb{N}$ et un sous-ensemble $M \subseteq \mathbb{N}$ tel que $n_0 \in M$ et $[\forall n \geq n_0, n \in M \Rightarrow n + 1 \in M]$, alors $M = \{n_0, n_0 + 1, ...\}$. Utiliser ce principe pour montrer que tout $n \geq 14$ s'écrit comme une somme de multiples de 8 et de 3.

5. Démontrer le principe de *récurrence double* sur $\mathbb{N}$: soit un sous-ensemble $Q \subseteq \mathbb{N}$ tel que $0, 1 \in Q$ et $[n, n + 1 \in Q \Rightarrow n + 2 \in Q]$, alors $Q = \mathbb{N}$. Utiliser ce principe pour montrer que, pour la suite de Fibonacci
   $$0, 1, 1, 2, 3, 5, 8, ..., f_{n+2} = f_n + f_{n+1}, ...$$
   on a $f_{n+m} = f_{n-1}f_m + f_n f_{m+1}$ (pour $n \neq 0$).

6. Démontrer le principe de *récurrence forte* sur $\mathbb{N}$: soit un sous-ensemble $R \subseteq \mathbb{N}$ tel que $0 \in R$ et $[(\forall k \leq n : k \in R) \Rightarrow n + 1 \in R]$, alors $R = \mathbb{N}$. Utiliser ce principe pour montrer que tout $n \geq 2$ dans $\mathbb{N}$ admet un diviseur premier.

7. Pour la suite de Fibonacci, prouver (en détaillant la récurrence utilisée) que
   a. $\sum_{i=0}^{n} f_i^2 = f_n f_{n+1}$,
   b. $f_n \leq (\frac{5}{3})^n$,
   c. $\sum_{i=0}^{2n} (-1)^{i+1} f_i + f_{2n-1} = 1$,
   d. $\sum_{i=0}^{n} \frac{1}{2^i} f_{i-1} + \frac{1}{2^n} f_{n+2} = 1$,
   e. $\sum_{i=0}^{2n} f_i f_{i-1} = f_{2n}^2$.

EXERCICES EN ARITHMÉTIQUE (M1 MATH) – 2

Isar STUBBE

1. Soit $A$ un anneau commutatif.

   (a) Montrer que l'application $A[X] \to A^A \colon f \mapsto \tilde{f}$ associant à chaque polynôme $f$ la fonction polynomiale $\tilde{f} \colon A \to A \colon a \mapsto f(a)$, est un homomorphisme d'anneaux.

   (b) Pour $a \in A$ et $f \in A[X]$, montrer que $X - a$ divise $f$ si et seulement si $a$ est une racine[1] de $f$.

   (c) Montrer que, si $A$ est intègre, alors $0 \neq f \in A[X]$ admet au plus $\deg(f)$ racines.

   (d) Montrer que, si $A$ est intègre et infini, alors l'application $f \mapsto \tilde{f}$ est injectif.

2. Démontrer le *Théorème d'Euclide*: dans un UFD, il existe infiniment beaucoup d'éléments premiers.

3. Dans un PID $A$, montrer que $a \in A$ est un élément premier (i.e. n'admet pas de diviseurs propres[2]) si et seulement si $(a) \trianglelefteq A$ est un idéal premier non-trivial.

4. Donner une injection de $\mathbb{N}^k$ dans $\mathbb{N}$ et une injection de $\mathbb{N}$ dans $\mathbb{N}^k$ (pour $k \geq 1$). (Par le Théorème de Cantor–Bernstein–Schröder il suit donc que $|\mathbb{N}^k| = |\mathbb{N}|$ pour $k \geq 1$.)

5. Soit $A$ un anneau commutatif intègre. Monter que $A[X]$ est un PID si et seulement si $A$ est un corps.

6. Pour $A$ un anneau commutatif intègre, montrer que les polynômes unitaires linéaires sont irréductibles dans $A[X]$.

7. Pour $K$ un corps et $f \in K[X]$ de degré 2 ou 3, montrer que $f$ est irréductible si et seulement si $f$ n'a pas de racine dans $K$.

8. (a) Dans un anneau euclidien $A$, construire l'*Algorithme d'Euclide* pour le calcul de $d, u, v \in A$ tel que $d = ua + vb$ (et donc $d = \operatorname{pgcd}(a, b)$ par le théorème de Bezout).

   (b) Appliquer cet algorithme à 180 et 252 dans $\mathbb{Z}$, à $X^3 - 1$ et $X^4 + X^3 + 2X^2 + X + 1$ dans $\mathbb{Q}[X]$, et à $X^m - 1$ et $X^n - 1$ dans $\mathbb{R}[X]$ $(m, n \in \mathbb{N})$.

[1] Par définition, $a$ est une racine du polynôme $f$ si la fonction polynomiale $\tilde{f}$ s'annule en $a$. Souvent on note simplement $f(a) = 0$, et non pas $\tilde{f}(a) = 0$; il n'y a pas de confusion lorsqu'on distingue bien l'indéterminée $X$ de l'élément $a \in A$.

[2] Certains auteurs disent que $a \in A$ est un *élément irreductible* si $a$ n'admet pas de diviseurs propres, et que $a$ est un *élément premier* si $(a) \trianglelefteq A$ est un idéal premier non-trivial. L'exercice montre donc que, dans un PID $A$, un élément est irrédictible si et seulement si il est premier.

EXERCICES EN ARITHMÉTIQUE (M1 MATH) – 3

Isar STUBBE

Désormais, $\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{Q}$ ont leurs significations usuelles; ce sera d'ailleurs aussi le cas pour $\mathbb{R}$ et $\mathbb{C}$, même si on n'a pas (encore) "construit" ces corps dans ce cours.

1. Montrer que le corps de fractions d'un corps $K$, est $K$ même (à isomorphisme près).

2. Soit $f\colon A \to K$ un homomorphisme injectif d'un anneau commutatif et intègre dans un corps. On note $A^* = A \setminus \{0\}$. Montrer l'équivalence de:
   (a) tout $x \in K$ est de la forme $x = f(a)f(b)^{-1}$ pour $(a, b) \in A \times A^*$,
   (b) $f\colon A \to K$ est le corps de fractions de $A$.

3. Prouver que $\mathbb{Q}(X)$ est isomorphe au corps de fractions de $\mathbb{Z}[X]$.

4. (a) Prouver que tout $a \in \mathbb{Q}$ s'écrit comme $a = b + c$ où $b \in \mathbb{Z}$ et $c \in \mathbb{Q} \cap [0, 1[$.
   (b) Enoncer et prouver une telle propriété pour les éléments du corps $K(X)$.

5. Soit $q = f/g \in K(X)$ tel que $\deg(f) < \deg(g)$.
   (a) Supposons que $g = g_1 ... g_n$ et $(g_i, g_j) = 1$ dans $K[X]$ pour tout $i \neq j$. Montrer qu'il existe $f_1, ..., f_n \in K[X]$ tels que $q = f_1/g_1 + ... + f_n/g_n$ et $\deg(f_i) < \deg(g_i)$ pour tout $i$.
   (b) Supposons que $g = h^n$ et $h$ irréductible dans $K[X]$. Montrer qu'il existe $k_1, ..., k_n \in K[X]$ tels que $q = k_1/h + ... + k_n/h^n$ et $\deg(k_i) < \deg(h)$ pour tout $i$.

6. Combiner les deux exercices précédents pour montrer comment toute fraction rationnelle sur un corps $K$ s'écrit comme une "somme d'éléments simples" (aussi appelée "somme de fractions partielles").
   Même si le principe de la décomposition d'une fraction rationnelle en éléments simples est assez facile, dans la pratique, c'est souvent le côté algorithmique – par exemple, la factorisation du dénominateur – qui peut être très difficile. D'ailleurs, la difficulté des calculs dépend fortement du corps de base. Cependant, cette technique est très utile, par exemple pour intégrer des fractions rationnelles, car on "isole" les pôles de la fraction donnée.

7. Sachant que les polynômes irréductibles sur $\mathbb{C}$ sont exactement les polynômes linéaires, décomposer les fractions rationnelles suivantes dans $\mathbb{C}(X)$:
   (a) $\dfrac{3X^2}{X^2+1}$ (b) $\dfrac{1}{X^3+1}$

8. Sachant que les polynômes irréductibles sur $\mathbb{R}$ sont exactement les polynômes linéaires et les polynômes de degré 2 de discriminant négatif, décomposer les fractions rationnelles suivantes dans $\mathbb{R}(X)$:
   (a) $\dfrac{X+3}{X^4-5X^2+4}$ (b) $\dfrac{25}{(X+2)(X^2+1)}$ (c) $\dfrac{10X^2+12X+20}{X^3-8}$

EXERCICES EN ARITHMÉTIQUE (M1 MATH) – 4

Isar STUBBE

1. Donner toutes les solutions de:
   (a) $493x \equiv 319 \bmod 899$
   (b) $493x \equiv 187 \bmod 899$.

2. Calculer, si possible, $14/89$ et $11/43$ dans l'anneau $\mathbb{Z}/(215)$.

3. Donner toutes les solutions de:
   (a) $\begin{cases} x \equiv 1 \bmod 3 \\ x \equiv 3 \bmod 5 \\ x \equiv 4 \bmod 7 \\ x \equiv 2 \bmod 11 \end{cases}$
   (b) $\begin{cases} x \equiv 997 \bmod 2001 \\ x \equiv 998 \bmod 2002 \\ x \equiv 999 \bmod 2003 \end{cases}$

4. Donner un algorithme pour résoudre un système
$$\begin{cases} x \equiv b_1 \bmod p^{r_1} \\ x \equiv b_2 \bmod p^{r_2} \end{cases}$$
   avec $p$ un nombre premier et $r_1, r_2 \neq 0$, et l'appliquer aux systèmes
$$\begin{cases} x \equiv 2 \bmod 4 \\ x \equiv 1 \bmod 16 \end{cases} \quad \text{et} \quad \begin{cases} x \equiv 7 \bmod 9 \\ x \equiv 7 \bmod 27 \end{cases}$$

5. Donner un algorithme pour résoudre un système
$$\begin{cases} x \equiv b_1 \bmod m_1 \\ x \equiv b_2 \bmod m_2 \end{cases}$$
   où $(m_1, m_2) \neq 1$ (indication: factoriser $m_1$ et $m_2$), et l'appliquer aux systèmes
$$\begin{cases} x \equiv 7 \bmod 12 \\ 2x \equiv 11 \bmod 15 \end{cases} \quad \text{et} \quad \begin{cases} x \equiv 7 \bmod 12 \\ 7x \equiv 11 \bmod 15 \\ x \equiv 3 \bmod 20 \end{cases}$$

6. Résoudre les systèmes
$$\begin{cases} x \equiv 18 \bmod 24 \\ 2x \equiv 24 \bmod 45 \\ x \equiv 42 \bmod 50 \end{cases} \quad \text{et} \quad \begin{cases} x \equiv 18 \bmod 24 \\ x \equiv 24 \bmod 45 \\ x \equiv 42 \bmod 50 \end{cases}$$

EXERCICES EN ARITHMÉTIQUE (M1 MATH) – 5

Isar STUBBE

Dans cette fiche, on note $\varphi$ pour la fonction indicatrice d'Euler.

1. Prouver qu'un groupe $G$ fini est cyclique si et seulement si il existe un element $g \in G$ d'ordre $|G|$.

2. Prouver que $(\mathbb{Z}/(m))^\times$ est cyclique si et seulement s'il existe un element $a \in \mathbb{Z}$ tel que $(a, m) = 1$ et $\varphi(m)$ est le plus petit nombre naturel non-nul tel que $a^{\varphi(m)} \equiv 1 \bmod m$.

   Dans ce cas, on dit que $a$ est une *racine primitive modulo* $m$.

3. Montrer que $(\mathbb{Z}/(7))^\times$ est un groupe cyclique et que $(\mathbb{Z}/(8))^\times$ ne l'est pas.

4. Déterminer les deux derniers chiffres en écriture décimale de $22^{2006}$.

5. Déterminer le dernier chiffre en écriture décimale de $7^{355}$.

6. Montrer que $\varphi(n) = 14$ n'a pas de solution. Indication: montrer d'abord que, si $p$ est un diviseur premier de $n$, alors $p - 1$ divise $\varphi(n)$; en déduire les facteurs premiers de $n$.

7. Chercher les $n$ tels que $\varphi(n) = 4$.

8. Observer que

$$1 + 2 = \tfrac{3}{2}\varphi(3), \quad 1 + 3 = \tfrac{4}{2}\varphi(4), \quad 1 + 2 + 3 + 4 = \tfrac{5}{2}\varphi(5), \quad 1 + 5 = \tfrac{6}{2}\varphi(6),$$
$$1 + 2 + 3 + 4 + 5 + 6 = \tfrac{7}{2}\varphi(7) \quad \text{et} \quad 1 + 3 + 5 + 7 = \tfrac{8}{2}\varphi(8),$$

   et deviner et prouver un théorème. (Pas facile.)

9. Soit $n = pq$ avec $p$ et $q$ deux nombres premiers distincts, et soient $e$ et $d$ deux nombres entiers tels que $ed \equiv 1 \bmod \varphi(n)$. Pour un entier $m$ tel que $(m, n) = 1$, on note $c \equiv m^e \bmod n$. Montrer alors que $m \equiv c^d \bmod n$.

   Ce résultat est au coeur du procédé de codage RSA (nommé d'après Rivest, Adleman et Schamir), utilisé dans OpenSSH, par exemple. Ce procédé fonctionne ainsi: Alice veut envoyer un message codé à Bob. D'abord Bob choisit deux nombres premiers $p$ et $q$, puis il calcule $n = pq$, et il choisit $e$ et $d$ tels que $ed \equiv 1 \bmod \varphi(n)$; il rend publique les nombres $e$ et $n$ (c'est son "public key") mais garde pour lui le nombre $d$ (son "private key"), et il efface les nombres $p$ et $q$. Supposons que le message d'Alice est un nombre $m < n$ tel que $(m, n) = 1$, alors elle calcule d'abord $c \equiv m^e \bmod n$, puis elle envoit $c$ à Bob. Pour connaître le message $m$, Bob calcule ensuite $c^d \bmod n$. La sécurité de ce procédé vient du fait que, pour décrypter le message codé $c$, il faudrait retrouver $d$ à partir de $e$ et $n$ sans connaître $p$ et $q$; or il n'existe aucun algorithme efficace pour cela.

EXERCICES EN ARITHMÉTIQUE (M1 MATH) – 6

Isar STUBBE

1. Donner l'ordre de chaque élément de $(\mathbb{Z}/(15))^\times$ et vérifier s'il existe des racines primitives module 15.

2. Calculer toutes les racines primitives modulo 17, puis calculer $11 \cdot 13$ modulo 17.

3. Chercher les $n \in \mathbb{N}$ tels que $8^{2011} \equiv 8^n \mod 27$.

4. Donner les solutions de $x^3 \equiv 1 \mod 19$ et de $x^4 \equiv 1 \mod 17$.

5. (a) Vérifier que 2 est racine primitive modulo 29.
   (b) Trouver toutes les racines primitives modulo 29.
   (c) Déterminer si $x^7 - 2$ admet une racine dans $\mathbb{Z}/(29)$.
   (d) Montrer que, pour tout $n \in \mathbb{Z}$, $x^3 \equiv n \mod 29$ admet une solution.
   (e) Résoudre $x^6 + ... + x + 1 \equiv 0 \mod 29$. Indication: $(x^6 + ... + x + 1)(x - 1) = x^7 - 1$, et $\mathbb{Z}/(29)$ est un corps, donc ...

6. Soit $p = 4t + 1$ un nombre premier. Montrer que $a$ est une racine primitive modulo $p$ si et seulement si $-a$ est une racine primitive modulo $p$.

7. Soit $p \geq 3$ un nombre premier.
   (a) Montrer que $a^{n-1} + ... + a + 1 \equiv 0 \mod p$ pour tout entier $a$ d'ordre $n > 1$ modulo $p$.
   (b) Montrer que, si $a$ est un entier d'ordre 3 modulo $p$, alors $a + 1$ est d'ordre 6 modulo $p$.

EXERCICES EN ARITHMÉTIQUE (M1 MATH) – 7

Isar STUBBE

Pour établir l'irréductibilité d'un polynôme sur $\mathbb{Q}$, on pourra utiliser le résultat suivant:

*Critère d'Eisenstein:* Soit $f(X) = X^n + f_{n-1}X^{n-1} ... + f_1X + f_0$ dans $\mathbb{Z}[X]$ et $p$ un nombre premier tel que $p$ divise chaque $f_i$ mais $p^2$ ne divise pas $f_0$. Alors $f(X)$ est irréductible dans $\mathbb{Q}[X]$.

1. (a) Calculer $\mathsf{min}(\sqrt{2}, \mathbb{Q})$, i.e. le polynôme minimal de $\sqrt{2}$ sur $\mathbb{Q}$.
   (b) Posons $\alpha = 1 + \sqrt{2}$. Montrer que $\mathsf{min}(\alpha, \mathbb{Q}) = X^2 - 2X - 1$.
   (c) Pour $\beta = \sqrt{\alpha}$, montrer que $\beta \notin \mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\alpha)$.
   (d) Calculer $\mathsf{min}(\beta, \mathbb{Q})$.
2. Soit $K$ une extension de degré 2 de $\mathbb{Q}$. Montrer qu'il existe $a \in \mathbb{Q}$ tel que $K = \mathbb{Q}(\sqrt{a})$.
3. Pour tout $n \geq 1$, montrer qu'il existe une extension de degré $n$ de $\mathbb{Q}$.
4. Soient $a, b \in \mathbb{C}$ des éléments algébriques sur $\mathbb{Q}$. Montrer que:
   (a) $[\mathbb{Q}(a, b) : \mathbb{Q}] \leq [\mathbb{Q}(a) : \mathbb{Q}] \cdot [\mathbb{Q}(b) : \mathbb{Q}]$.
   Supposons maintenant que $[\mathbb{Q}(a) : \mathbb{Q}]$ et $[\mathbb{Q}(b) : \mathbb{Q}]$ sont premiers entre-eux. Montrer que:
   (b) $[\mathbb{Q}(a, b) : \mathbb{Q}] = [\mathbb{Q}(a) : \mathbb{Q}] \cdot [\mathbb{Q}(b) : \mathbb{Q}]$,
   (c) $\mathbb{Q}(a) \cap \mathbb{Q}(b) = \mathbb{Q}$,
   (d) $\mathsf{min}(a, \mathbb{Q}) = \mathsf{min}(a, \mathbb{Q}(b))$.
5. Déterminer le corps de racines de $X^5 + X^4 - 2X - 2$ sur $\mathbb{Q}$.
6. Déterminer le corps de racines de $X^3 - 1$ sur $\mathbb{Q}$.
7. Prouver que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

EXERCICES EN ARITHMÉTIQUE (M1 MATH) – 8

Isar STUBBE

1. (a) Pour un corps $K$, montrer que tout sous-groupe fini de $(K^*, \cdot, 1)$ est cyclique.

   (b) En déduire que les solutions de $X^n = 1$ dans $\mathbb{C}$ forment un groupe cyclique. Quel est son ordre? Donner une déscription explicite des générateurs de ce groupe.

   Un $\omega \in \mathbb{C}$ tel que $\omega^n = 1$ est une *racine $n$-ième de l'unité*. Si l'ordre de $\omega$ est $n$, alors c'est une *racine primitive $n$-ième de l'unité*. Une extension $\mathbb{Q}(\omega)$ de $\mathbb{Q}$ par une racine primitive $n$-ième de l'unité $\omega$, est appelée une *extension cyclotomique*.

2. Pour $n \geq 3$, on note $\alpha = \frac{2\pi}{n}$.

   (a) Montrer que le polygone régulier à $n$ côtés est constructible si et seulement si $\cos\alpha$ est constructible.

   (b) Utiliser l'identité $e^{i\alpha} = \cos\alpha + i\sin\alpha$ dans $\mathbb{C}$ pour montrer que $\cos\alpha = \frac{1}{2}(e^{i\alpha} + e^{-i\alpha})$ et en déduire que $\mathbb{Q}(e^{i\alpha}) \supseteq \mathbb{Q}(\cos\alpha) \supseteq \mathbb{Q}$.

   (c) Montrer que $e^{i\alpha}$ est racine d'un polynôme de degré 2 sur $\mathbb{Q}(\cos\alpha)$ et en déduire $[\mathbb{Q}(e^{i\alpha}) : \mathbb{Q}(\cos\alpha)]$.

   (d) Donner $[\mathbb{Q}(\cos\alpha) : \mathbb{Q}]$ en fonction du degré du polynome minimal de $e^{i\alpha}$ sur $\mathbb{Q}$.

   (e) Formuler une condition nécessaire pour la constructibilité du polygone régulier à $n$ côtés en fonction du degré du polynome minimal d'une racine primitive $n$-ième de l'unité sur $\mathbb{Q}$.

3. Pour $n \geq 1$ on définit le *polynôme cyclotomique* comme $\Phi_n(X) = \prod_{i=1}^{k}(X - \omega_i) \in \mathbb{C}[X]$ avec $\omega_1, ..., \omega_k$ les racines *primitives* $n$-ièmes de l'unité.

   (a) En titre d'exemple, calculer $\Phi_1$, $\Phi_2$ et $\Phi_4$. En général, donner le degré de $\Phi_n$.

   (b) Pour $p$ un nombre premier, montrer que $\Phi_p(X) = X^{p-1} + ... + X + 1 \in \mathbb{Q}[X]$. Indication: Expliquer pourquoi $X^p - 1 = \prod_{i=1}^{p}(X - \omega_i)$ avec $\omega_1, ..., \omega_p$ *toutes* les racines $p$-ièmes de l'unité, puis diviser ce polynôme par $X - 1$.

   (c) Montrer qu'un nombre premier $p$ divise tout coefficient binomial $\binom{p}{k}$ si $0 < k < p$, et en déduire que $\Phi_p$ est irréductible dans $\mathbb{Q}[X]$. Quel est donc le degré d'une extension cyclotomique de $\mathbb{Q}$ par une racine primitive $p$-ième de l'unité? Indication: Simplifier $\Phi_p(X + 1)$ à l'aide de (b) et appliquer le critère d'Eisenstein.

   (d) Donner une condition nécessaire pour la constructibilité du polygone régulier à $p$ côtés.

   (e) Prouver que, si $p = 2^m + 1$ est un nombre premier impair, alors $m$ est une puissance de 2. Indication: Par l'absurde, si $m = 2^k l$ avec $l$ impair, montrer que $X + 1$ divise $X^l + 1$ et poser $X = 2^k$.

   Les nombres $p_n = 2^{2^n} + 1$ sont les *nombres de Fermat*. Nous avons donc établi une condition nécessaire pour la constructibilité d'un polygone régulier à $p$ côtés: il faut que $p$ soit un nombre premier de Fermat. (On peut calculer que $p_0, ..., p_4$ sont des nombres premiers, et (avec un ordinateur puissant) que $p_5, ..., p_{23}$ ne le sont pas; mais actuellement il n'est pas connu si $p_n$ est premier pour $n \geq 24$.)

   En fait, il est possible de montrer que chaque $\Phi_n(X)$ est un élément irréductible de $\mathbb{Q}[X]$. Cela implique, comme dans cet exercice, une condition nécessaire pour la constructibilité d'un polygone régulier à $n$ côtés. De plus, il est possible de montrer que cette condition nécessaire est aussi suffisante, donnant le résultat suivant: *Un polygone régulier à $n$ côtés est constructible si et seulement si $\varphi(n)$ est une puissance de 2, si et seulement si $n = 2^r p_1 ... p_k$ où $r \geq 0$ et les $p_i$ sont des nombres premiers de Fermat distincts.*

EXERCICES EN ARITHMÉTIQUE (M1 MATH) – 9

Isar STUBBE

Dans les exercices 1, 2 et 3, le corps de base est toujours $\mathbb{Q}$. Dans les exercices 4, 5 et 6 on pourra utiliser que, pour tout homomorphisme de groupes $f\colon G \to H$, $\mathrm{im}(f) \cong G/\ker(f)$, et que pour tout sous-groupe normal $K \trianglelefteq G$ d'un groupe fini, $|G/K| = |G|/|K|$.

1. (a) Quel est l'effet du changement de variable $X = Y - \frac{a}{3}$ sur l'équation $X^3 + aX^2 + bX + c = 0$?

   (b) En faisant le changement de variable $Y = \sqrt[3]{u} + \sqrt[3]{v}$, montrer que l'équation $Y^3 + pY + q = 0$ admet une solution si
   $$\begin{cases} u + v + q = 0 \\ 3\sqrt[3]{uv} + p = 0 \end{cases},$$
   puis résoudre ce système.

   (c) Montrer que toute équation cubique admet une solution par radicaux.

   (d) Appliquer à l'équation $X^3+X-2 = 0$ et à l'équation $X^3-15X-4 = 0$. Observations remarquables?

2. (a) Quel est l'effet du changement de variable $Y = X + \frac{a}{4}$ sur l'équation $X^4+aX^3+bX^2+cX+d = 0$?

   (b) Donner une solution par radicaux de l'équation $Y^4 + pY^2 + r = 0$.

   (c) Soit $h(Y) = Y^4+pY^2+qY+r$ avec $q \neq 0$. Poser $h(Y) = (Y^2+aY+b)(Y^2+cY+d)$, exprimer $b, c, d$ en fonction de $a, p, q$, et montrer que $a^2$ est la solution d'une équation cubique dont les coefficients dependent uniquement de $p$, $q$ et $r$.

   (d) Conclure que toute équation quartique admet une solution par radicaux.

3. Montrer que $X^5 - 10X + 2$ n'est pas résoluble par radicaux. Et $X^5 - 2$?

4. (a) Montrer que tout groupe d'ordre premier est cyclique. Indication: théorème de Lagrange.

   (b) Montrer que tout groupe cyclique est abélien. Indication: classification des groupes cycliques.

   (c) Montrer que tout groupe abélien est résoluble.

   (d) Conclure que le groupe symétrique $S_2$ est résoluble.

5. Pour une permutation $\sigma \in S_n$, on note $f_\sigma\colon \mathbb{R}^n \to \mathbb{R}^n$ l'application linéaire envoyant la base canonique (ou une autre base, peu importe) $e_1, ..., e_n$ sur la base $e_{\sigma(1)}, ..., e_{\sigma(n)}$.

   (a) Montrer que l'on a un homomorphisme surjectif de groupes $\mathrm{sgn}\colon S_n \to \{+1, -1\}\colon f_\sigma \mapsto \det(f_\sigma)$.

   (b) Montrer que le noyau d'un homomorphisme de groupes est toujours un sous-groupe normal.

   (c) Prouver que $\mathrm{sgn}(\sigma) = +1$ si et seulement si $\sigma$ s'écrit comme une composée d'un nombre paire de transpositions.

   (d) Conclure que le groupe alterné $A_n$ est normal dans $S_n$ et que le quotient $S_n/A_n$ est abélien.

   (e) Montrer que $A_3$ est abélien et que donc $S_3$ est résoluble.

6. (a) Identifier les éléments de $A_4$ d'ordre au plus 2, et vérifier qu'ils forment un sous-groupe abélien et normal de $A_4$: il s'agit du *groupe de Klein* (ou *Vierergruppe*) $V_4$.

(b) Vérifier que $V_4$ est un sous-groupe normal de $A_4$.

(c) Conclure que $S_4$ est résoluble.

7. Montrer qu'un sous-groupe d'un groupe résoluble est toujours résoluble.

*Les exercices suivants sont donnés à titre informatif:*

8. (a) Soit $K$ un corps et $G \subseteq \mathsf{Aut}(K)$ un sous-groupe. Montrer que $\mathsf{Fix}(G) = \{x \in K \mid \forall g \in G : g(x) = x\}$ est un sous-corps de $K$. Montrer que $G \subseteq \mathsf{Gal}(K : \mathsf{Fix}(G))$.

(b) Soit $L : K$ une extension. Montrer que $K \subseteq \mathsf{Fix}(\mathsf{Gal}(L : K))$.

(c) Soit $G$ le sous-groupe de $\mathsf{Aut}(\mathbb{C})$ contenant l'identité et la conjugaison. Calculer $\mathsf{Fix}(G)$.

(d) Calculer $\mathsf{Aut}(\mathbb{Q})$ et montrer que $\mathsf{Aut}(\mathbb{R}) = \mathsf{Gal}(\mathbb{R} : \mathbb{Q}) = \{\mathsf{id}\}$. Indication: Montrer qu'un automorphisme $\varphi\colon \mathbb{R} \to \mathbb{R}$ est strictement monotone, et donc continu; puis utiliser que $\mathbb{Q}$ est dense dans $\mathbb{R}$.

Une extension algébrique $L : K$ telle que $K = \mathsf{Fix}(\mathsf{Gal}(L : K))$ est appelée *galoisienne*.

9. Soit une extension $L : K$, $a \in L$ un élément algébrique sur $K$, et $f = \mathsf{min}(a, K)$ son polynôme minimal.

(a) Soit $\varphi \in \mathsf{Gal}(K(a) : K)$. Montrer que $\varphi$ est déterminé par $\varphi(a)$, et que $f(\varphi(a)) = 0$.

(b) Soit $b \in K(a)$ tel que $f(b) = 0$. Montrer qu'il y a un unique $\varphi \in \mathsf{Gal}(K(a) : K)$ tel que $\varphi(a) = b$.

(c) Conclure que $|\mathsf{Gal}(K(a) : K)|$ est égal au nombre de racines distinctes de $f$ dans $K(a)$.

(d) Admettons le résultat qu'une extension finie $L : K$ est galoisienne si et seulement si $[L : K] = |\mathsf{Gal}(L : K)|$. En déduire que $K(a)$ est une extension galoisienne de $K$ si et seulement si $f$ a $\deg(f)$ racines distinctes dans $K(a)$. Simplifier cette caractérisation si $K = \mathbb{Q}$.

(e) Est-ce que $\mathbb{Q}(\sqrt[3]{2})$ est une extension galoisienne de $\mathbb{Q}$?

— 11 —

# Bibliographie


1. (Tignol, 1988) *Galois' theory of algebraic equations*
2. (Carrega, 1989) *Théorie des corps, la règle et le compas*
3. (Birhoff et MacLane, 1989) *Algebra (3rd edition)*
4. (Ireland et Rosen, 1990) *A classical introduction to modern number theory*
5. (Borceux, 1992) *Handbook of categorical algebra (vol. 1)*
6. (McLarty, 1995) *Elementary categories, elementary toposes*
7. (Conway et Guy, 1996) *The book of numbers*
8. (Morandi, 1996) *Field and Galois theory*
9. (Fakir, 2003) *Algèbre et théorie des nombres, cryptographie, primalité*
10. (Lawvere et Rosebrugh, 2003) *Sets for mathematics*
11. (Milne, 2008) *Fields and Galois theory*
12. (Raczek et Tignol, 2009) *Arithmétique et théorie de Galois, notes de cours et exercices*