Résumé de CM9

Quelques propriétés de $\mathbb{Z}$

Le théorème suivant est apparu en 1640 :

Théorème (le « petit théorème de Fermat ») Soit a un entier non null et soit p un nombre premier. Supposons que a et p sont premiers entre eux. Alors, p divise $a^{p-1} - 1$. □

Deux preuves de ce théorème se trouvent dans la Feuille X. Le théorème suivant est fondamental :

Théorème (Décomposition en facteurs premiers) Soit $n \in \mathbb{N}$ un entier tel que $n > 1$. Il existe une unique écriture de n sous la forme $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ où

1. les entiers p_i sont premiers,
2. les exposants α_i sont entiers strictement positifs,
3. $p_1 < p_2 < p_3 < \cdots < p_s$. □

Preuve (l'existence) Démo. par récurrence forte.
Pour $n = 2$, l'énoncé est claire. Fixons $n \geqslant 3$. Soit p le plus petit diviseur (de n) > 1. D'après le lemme ci-dessus, p est premier et, par hypothèse de récurrence, $\dfrac{n}{p}$ admet une telle décomposition.
(l'unicité) Démo. par récurrence forte avec le lemme de Gauss. □

Le théorème suivant est un corollaire simple :

Théorème Soient $a, b \in \mathbb{N}^*$ deux entiers. Soient $p_1, p_2, \cdots, p_s$ nombres premiers deux à deux distincts tels qu'ils existent $\alpha_1, \alpha_2, \cdots, \alpha_s$ et $\beta_1, \beta_2, \cdots, \beta_s \in \mathbb{N}$ tels que

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} \qquad \text{et} \qquad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}.$$

Alors,

1. $\text{ppcm}(a, b) = p_1^{\max\{\alpha_1, \beta_1\}} p_2^{\max\{\alpha_2, \beta_2\}} \cdots p_s^{\max\{\alpha_s, \beta_s\}}$,
2. $\text{pgcd}(a, b) = p_1^{\min\{\alpha_1, \beta_1\}} p_2^{\min\{\alpha_2, \beta_2\}} \cdots p_s^{\min\{\alpha_s, \beta_s\}}$. □

Congruence

Définition Soit $n \in \mathbb{N}$ tel que $n > 1$. Les deux entiers a et b sont dits **congrus modulo** n lorsque n divise $a - b$. On notera $a \equiv b\,[n]$ ou $a \equiv b \mod n$. □

Par définition, cette relation «≡» vérifie

1. (réflexivité) $a \equiv a[n]$,
2. (symétrie) $a \equiv b[n] \iff b \equiv a[n]$,
3. (transitivité) $a \equiv b[n]$ et $b \equiv c[n] \implies a \equiv c[n]$.

On dit que cette relation «≡» est une **relation d'équivalence**.

Exemples Soit $m \in \mathbb{Z}$.

1. mod 2: $m \equiv 0[2] \Leftrightarrow m$: **pair** et $m \equiv 1[2] \Leftrightarrow m$: **impair**.
   Donc, mod 2 nous donne la **parité**.
2. mod 10: $m \mod 10$ ne regard que le dernier chiffre de m.
3. mod n: $m \mod n$ ne regarde que le reste de la division euclidienne par n.

Compatibilité de cette relation «≡» avec la somme + et le produit ×: soit $n \in \mathbb{N}$ tel que $n > 1$.

Pour $a, b, c, d \in \mathbb{Z}$ tels que $a \equiv b[n]$ et $c \equiv d[n]$,

1. $a + c \equiv b + d[n]$,
2. $a \cdot c \equiv b \cdot d[n]$.

Quelques équations

1. Soient $a, m \in \mathbb{N}^*$ tels que i) $\text{pgcd}(a, m) = 1$ et ii) $m > 1$. Soit $b \in \mathbb{Z}$.

$$\text{Résoudre } (E) : \quad ax \equiv b\,[m] \text{ pour } x \in \mathbb{Z}.$$

Le théorème de Bézout implique $\exists\,(u, v) \in \mathbb{Z}^2$ tel que $au + mv = 1$.
Alors, $au = 1 - mv \equiv 1[m]$. Multipliant u sur (E): $x \equiv aux[m] \equiv bu[m]$,
i.e., $x \equiv bu[m]$.

2. Soient $a_i, m_i \in \mathbb{N}^*$ $(i = 1, 2)$ tels que i) $\text{pgcd}(m_1, m_2) = 1$ et ii) $m_i > 1$ $(i = 1, 2)$.

$$\text{Résoudre } (E) : \quad x \equiv a_i\,[m_i] \ (i = 1, 2) \text{ pour } x \in \mathbb{Z}.$$

Le théorème de Bézout implique $\exists\,(u_1, u_2) \in \mathbb{Z}^2$ tel que $m_1u_1 + m_2u_2 = 1$.
Posons $s_0 = a_1m_2u_2 + a_2m_1u_1$. Alors,
$s_0 \equiv a_1m_2u_2[m_1] \equiv a_1(1 - m_1u_1)[m_1] \equiv a_1[m_1]$,
$s_0 \equiv a_2m_1u_1[m_2] \equiv a_2(1 - m_2u_2)[m_2] \equiv a_2[m_2]$,
d'où $x = s_0$ **est une solution particulière de** (E).

En particulier, $y := x - s_0$ vérifie $(E') : y \equiv 0\,[m_i]$ $(i = 1, 2)$,
i.e., y est un multiple commun de m_1 et m_2, donc un multiple de $\text{ppcm}(m_1, m_2)$.
$\text{pgcd}(m_1, m_2) = 1$ implique que $\text{ppcm}(m_1, m_2) = m_1m_2$, d'où $y \in m_1m_2\mathbb{Z}$.

Donc, l'ensemble des solutions de (E) est $s_0 + m_1m_2\mathbb{Z}$.
Par la division euclidienne, $\exists\,!(n, k_0) \in \mathbb{Z}^2$ tel que i) $s_0 = m_1m_2n + k_0$ et ii) $0 \leqslant k_0 < m_1m_2$.
Alors, $s_0 + m_1m_2\mathbb{Z} = k_0 + m_1m_2(n + \mathbb{Z}) = k_0 + m_1m_2\mathbb{Z}$.

En résumé, on obtient le théorème suivant :

Théorème (Reste chinois) Soient m_1 et m_2 deux entiers naturels > 1 qui sont premiers entre eux. Soient $a_1, a_2 \in \mathbb{Z}$. Notons l'ensemble des solutions de l'équation

$$x \equiv a_i[m_i] \quad (i = 1, 2)$$

par $\mathcal{S}$. Alors, $\exists\, ! k_0 \in \mathbb{N}$ tel que

1. $\mathcal{S} = k_0 + m_1 m_2 \mathbb{Z}$,
2. $0 \leqslant k_0 < m_1 m_2$. □

Annexe : **Relation binaire sur un ensemble**

Sur un ensemble E, on considère une proposition qui lie entre eux certains éléments de cet ensemble. Une **relation binaire** $\mathcal{R}$ sur l'ensemble E est définie par une partie $\mathcal{G}$ de $E \times E$; si $(x, y) \in \mathcal{G}$ on dit que x **est en relation avec** y ou tout simplement x **et** y **sont liés**, noté $x\mathcal{R}y$.

Exemples

1. Soit $E = \mathbb{Z}^*$ ou $\mathbb{N}^*$. Posons $\mathcal{G} = \{\, (k, l) \mid k|l \,\}$.
   Alors, $k\mathcal{R}l \iff k|l$.
2. Soit $E = \mathbb{Z}$ et soit $n \in \mathbb{N}^*$ tel que $n > 1$. Posons $\mathcal{G} = \{\, (k, l) \mid n|k - l \,\}$.
   Alors, $k\mathcal{R}l \iff k \equiv l[n]$. (**relation de congruence modulo** n)
3. Soit $E = \mathbb{R}$ ou $\mathbb{Q}$. Posons $\mathcal{G} = \{\, (x, y) \mid y - x \geqslant 0 \,\}$.
   Alors, $x\mathcal{R}y \iff x \leqslant y$.
4. Soit $E = \mathcal{P}(F)$, l'ensemble des parties d'un ensemble F. Posons $\mathcal{G} = \{\, (A, B) \in E \times E \mid \forall\, x \in A \;\Rightarrow\; x \in B \,\}$. Alors, $A\mathcal{R}B \iff A \subset B$. (**relation d'inclusion**)
5. Soient E et F deux ensembles et soit $f : E \to F$ une application.
   Posons $\mathcal{G} = \{\, (x, y) \in E \times E \mid f(x) = f(y) \,\}$. Alors, $x\mathcal{R}y \iff f(x) = f(y)$.

Ces exemples vérifient quelques propriétés caractéristiques :

1. (réfléxivité) $\forall\, x \in E, \quad x\mathcal{R}x$,
2. (transitivité) $\forall\, x, y, z \in E$, ($x\mathcal{R}y$ et $y\mathcal{R}z$) $\implies x\mathcal{R}z$,
3. (symétrie) $\forall\, x, y \in E, \quad x\mathcal{R}y \implies y\mathcal{R}x$,
4. (antisymétrie) $\forall\, x, y \in E$, ($x\mathcal{R}y$ et $y\mathcal{R}x$) $\iff x = y$.

Relations d'équivalence

Définition Une relation binaire $\mathcal{R}$ sur un ensemble E est appelée **relation d'équivalence** sur E si elle est réflexive, transitive et symétrique. □

Parmi les exemples ci-dessus, 2. et 5. sont des relations d'équivalence.

Définition La **classe d'équivalence** de $x \in E$, notée $\mathrm{Cl}_{\mathcal{R}}(x)$, est une partie de E formée par les éléments qui sont en relation avec x :

$$\mathrm{Cl}_{\mathcal{R}}(x) = \{\, y \in E \,|\, x\mathcal{R}y \,\}.$$

Un élément quelconque de $\mathrm{Cl}_{\mathcal{R}}(x)$ est appelé **représentant** de la classe. □

Par définition, on a les propriétés suivantes:

Proposition Soit E un ensemble et soit $\mathcal{R}$ une relation d'équivalence sur E.

1. $\forall\, x \in E,\ x \in \mathrm{Cl}_{\mathcal{R}}(x)$.
2. Soit $y \in E$.
   i) Si $y \in \mathrm{Cl}_{\mathcal{R}}(x)$, alors $\mathrm{Cl}_{\mathcal{R}}(y) = \mathrm{Cl}_{\mathcal{R}}(x)$, et
   ii) si $y \notin \mathrm{Cl}_{\mathcal{R}}(x)$, alors $\mathrm{Cl}_{\mathcal{R}}(x) \cap \mathrm{Cl}_{\mathcal{R}}(y) = \varnothing$. □

Ceci dit, l'ensembles des classes d'équivalence de E forme une **partition** de E.

Définition L'**ensemble quotient** d'un ensemble E par la relation d'équivalence $\mathcal{R}$, noté $E/\mathcal{R}$, est l'ensemble des classes d'équivalence de E suivant $\mathcal{R}$:

$$E/\mathcal{R} = \{\, \mathrm{Cl}_{\mathcal{R}}(x) \,|\, x \in E \,\}.$$ □

N.B. Dans l'ensemble quotient $E/\mathcal{R}$, chaque classe $\mathrm{Cl}_{\mathcal{R}}(x)$ est vue comme un élément. □

Exemple Soit $E = \mathbb{Z}$ et soit $n \in \mathbb{N}^*$ tel que $n > 1$. Pour $k, l \in \mathbb{Z}$, on définit $k\mathcal{R}l$ par $k \equiv l[n]$. Alors, chaque classe d'équivalence de E admet un unique représentant $k \in \{0, 1, \cdots, n\}$. L'ensemble quotient $E/\mathcal{R}$, noté $\mathbb{Z}/n\mathbb{Z}$, est constitué par n éléments $\{\, k + n\mathbb{Z} \,\}_{k \in \{0,1,\cdots,n\}}$. □

Relations d'ordre

Définition Une relation binaire $\mathcal{R}$ sur un ensemble E est appelée **relation d'ordre** sur E si elle est réflexive, transitive et antiymétrique. □

On note une relation d'ordre souvent par $\leqslant$ ou $\preceq$. Un ensemble E muni d'une relation d'ordre $\preceq$ est dit **ordonné**, noté $(E, \preceq)$. Parmi les exemples ci-dessus, 1., 3. et 4. sont des relations d'ordre.

Définition Soit $(E, \preceq)$ un ensemble ordonné et soit A une partie de E.

1. Un élément M de E est un **majorant** de A si $\forall\, x \in A,\ x \preceq M$.
2. Un élément m de E est un **minorant** de A si $\forall\, x \in A,\ m \preceq x$. □

Une partie admettant un majorant (resp. minorant) est dite **majorée** (resp. **minorée**).

Un élément d'une partie A de E est appelé le **plus grand élément** (ou le **maximum**) s'il majore toues les éléments de A. De même, un élément de d'une partie A de E est appelé le **plus petit élément** (ou le **minimum**) s'il minore tous les élément de A.

Définition Soit $(E, \preceq)$ un ensemble ordonné et soit A une partie de E.

1. Si l'ensemble des majorants de A admet un minimum, cet élément est appelé **borne supérieur** et est noté par $\sup A$.
2. Si l'ensemble des minorants de A admet un maximum, cet élément est appelé **borne inférieur** et est noté par $\inf A$. □

N.B. Soit $E = \mathbb{R}$ et soient $a < b$ deux nombres réels.

1. Pour un intervalle $I =]-\infty, b]$ (resp. $I =]-\infty, b[$), $\sup I = b \in I$ (resp. $\sup I = b \notin I$).
2. Pour un intervalle $I =]a, +\infty[$ (resp. $I = [a, +\infty[$), $\inf I = a \notin I$ (resp. $\inf I = a \in I$). □