Chapitre 14

Compléments sur les anneaux et les idéaux, arithmétique

1 Compléments sur les produits d'anneaux

1.1 Théorème chinois

Exercice 1. Si on distribue équitablement n bonbons à 4 enfants, il en reste 3, mais si on les distribue équitablement aux 3 enfants les plus sages, il en reste 1. Combien y a t-il de bonbons ?

Théorème 1. ***(des restes chinois)*** *Soient $m, n \in \mathbb{N}$ tels que $m \wedge n = 1$. Alors on a un isomorphisme d'anneaux $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.*

Remarques :
- L'isomorphisme naturel à considérer est tout simplement $\overline{k}\ [mn] \mapsto (\overline{k}\ [m], \overline{k}\ [n])$.
- Cet isomorphisme implique en pratique qu'un système de congruence :

$$\begin{cases} x \equiv a\ [m] \\ x \equiv b\ [n] \end{cases}$$

admet toujours une solution dans $\mathbb{Z}$ lorsque m et n sont premiers entre eux, et que l'ensemble des solution est une classe de congruence modulo mn.

Méthode : On peut envisager deux méthodes pour trouver explicitement x pour un tel système de congruence.

a) méthode «exhaustive» : on liste parmi les entiers de $[\![0, mn-1]\!]$ ceux qui sont dans la classe de a modulo m et ceux qui sont dans la classe b modulo n, on trouve alors l'unique nombre x qui est dans les deux listes : c'est la plus petite solution particulière possible.

b) méthode «calculatoire» : il s'agit de
- déterminer un représentant u de l'inverse de n modulo m ;
- déterminer un représentant v de l'inverse de m modulo n ;
- $x = aun + bvm$ donne alors une solution particulière.

Dans tous les cas, on a une solution particulière x et sa classe $\overline{x}$ modulo mn donne l'ensemble des solutions. La méthode «exhaustive» est clairement plus pratique pour des petits nombres m et n mais la méthode «calculatoire» est algorithmiquement plus efficace pour des grands nombres et lorsqu'on généralise à plus de deux équations (voir plus loin).

Exercice 2. Résoudre le système de congruence : $\begin{cases} x \equiv 2\ [3] \\ x \equiv 3\ [5] \end{cases}$.

Remarques :
- Lorsque m et n ne sont pas premiers entre eux, l'application $\overline{k}\ [mn] \mapsto (\overline{k}\ [m], \overline{k}\ [n])$ n'est plus un isomorphisme. Pour avoir l'injectivité il faut en fait partir de $\mathbb{Z}/(m \vee n)\mathbb{Z}$ et on n'a clairement plus la surjectivité.

- On peut généraliser le théorème chinois a plus de deux facteurs : Si $n_1, \dots, n_k$ sont premiers entre eux deux à deux alors en notant $n = n_1 \times \cdots \times n_k$, on a

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

Pour résoudre explicitement un système de k congruences $x \equiv a_i\ [n_i]$, les méthodes vues précédemment se généralisent. Concernant la méthode «calculatoire» on détermine pour tout $i \in [\![1, k]\!]$ un représentant u_i de l'inverse de $\hat{n_i}$ modulo n_i, où $\hat{n_i} = \dfrac{n_1 \cdots n_k}{n_i}$, et on pose $x = \displaystyle\sum_{i=1}^{n} a_i u_i \hat{n_i}$.

Exercice 3. (Sun Zi 450) Soit des objets dont on ignore le nombre. En les comptant 3 par 3 il en reste 2, en les comptant 5 par 5, il en reste 3 et en les comptant 7 par 7, il en reste 2. Combien y a-t-il d'objets ?

1.2 Indicatrice et théorème d'Euler

Rappel : On rappelle que pour $n \geqslant 2$, et $k \in \mathbb{Z}$, la classe $\overline{k}$ modulo n est un élément inversible de $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si, k est premier avec n.

Définition 1. On appelle *indicatrice d'Euler* l'application $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ qui à tout n associe le nombre d'entiers de $[\![0, n-1]\!]$ premiers avec n.

Proposition 1. *$\varphi(1) = 1$ et pour tout $n \geqslant 2$: $\varphi(n) = \mathrm{card}\big((\mathbb{Z}/n\mathbb{Z})^\times\big)$.*

Exercice 4. Déterminer les valeurs de $\varphi(n)$ pour $n \in [\![1, 12]\!]$.

Lemme 1. *Si m et n sont premiers entre eux, les groupes multiplicatifs $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ et $(\mathbb{Z}/mn\mathbb{Z})^\times$ sont isomorphes.*

Proposition 2.
- *Si m et n sont premiers entre eux, $\varphi(mn) = \varphi(m)\varphi(n)$.*
- *Si p est un nombre premier, $\varphi(p^k) = p^{k-1}(p-1)$ pour tout $k \in \mathbb{N}^*$.*

Proposition 3. *Soit $n \geqslant 2$ avec $n = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k}$ sa décomposition en produit de facteurs premiers (les p_i deux à deux distincts et $\alpha_i > 0$). Alors*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

Remarques :

- Cette formule peut aussi s'écrire $\varphi(n) = \displaystyle\prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1)$.
- En pratique, on peut utiliser récursivement la formule $\varphi(mn) = \varphi(m)\varphi(n)$ (tant que $m \wedge n = 1$) jusqu'à tomber sur des puissances de nombres premiers.

Exercice 5. Calculer $\varphi(120)$.

Théorème 2. ***(d'Euler)*** *Soit $n \geqslant 2$ un entier naturel et soit $a \in \mathbb{Z}$ premier avec n. Alors $a^{\varphi(n)} \equiv 1\ [n]$.*

Remarque : Si n est premier, on a $\varphi(n) = n - 1$ et on retrouve le (petit) théorème de Fermat.

Théorème 3. ***(de Fermat)*** *Soit p premier et soit $a \in \mathbb{Z}$ non divisible par p. Alors $a^{p-1} \equiv 1\ [p]$.*

Corollaire 1. ***(de Fermat bis)*** *Si p est premier et $a \in \mathbb{Z}$, $a^p \equiv a\ [p]$.*

Exercice 6. Déterminer les élements inversibles de l'algèbre $\mathcal{M}_2(\mathbb{F}_2)$ et montrer que $GL_2(\mathbb{F}_2) \simeq S_3$.

2 Opérations sur les idéaux

Dans toute cette section, on considère un anneau commutatif A non nul, c'est-à-dire tel que $1_A \neq 0_A$.

Proposition 4. *Toute intersection d'idéaux de A est un idéal de A.*

Définition 2. Soit P une partie de A. On appelle *idéal engendré* par P l'intersection de tous les idéaux de A contenant P. On le note (P).

Définition 3. Soient I et J deux idéaux de A. On appelle *somme* de I et J l'ensemble :

$$I + J = \{a + b, (a, b) \in I \times J\}$$

Proposition 5. *$I + J$ est l'idéal engendré par $I \cup J$.*

Remarques :
- On a $I + J = J + I$.
- On montre facilement que si I, J, K sont trois idéaux, $(I + J) + K = I + (J + K)$. On notera simplement $I + J + K$.
- Plus généralement, on peut définir $I_1 + \cdots + I_n$ pour une famille finie $(I_k)_{1 \leqslant k \leqslant n}$. On a :

$$I_1 + \cdots + I_n = \left(\bigcup_{k=1}^{n} I_k \right)$$

Définition 4. Soit $a \in A$. on appelle *idéal engendré* par a l'idéal engendré par $\{a\}$. On le note (a).
Un idéal engendré ainsi par un seul élément est appelé un idéal *principal*.

Proposition 6. *Soit $a \in A$. L'idéal (a) est l'ensemble*

$$aA = \{ax, x \in A\}$$

On peut aussi le noter Aa.

Remarque : Plus généralement, l'idéal engendré par n éléments $a_1, \ldots, a_n$ est :

$$(\{a_1, \ldots, a_n\}) = (a_1) + \cdots + (a_n) = \{a_1 x_1 + \cdots + a_n x_n,\ (x_1, \ldots, x_n) \in A^n\}$$

Rappel : On a $(a) = (b)$ si, et seulement si, $a|b$ et $b|a$. Lorsque A est intègre et a et b non nul, cela implique que a et b sont associés : il existe un unique $u \in A^\times$ tel que $a = ub$.

Remarque : Cela ne fonctionne pas dans un anneau non intègre : par exemple dans $\mathbb{Z}/6\mathbb{Z}$, $(\overline{2}) = (\overline{4})$ et on a $\overline{4} = \overline{2} \times \overline{2}$ et $\overline{2} = \overline{2} \times \overline{4}$, mais ni $\overline{2}$ ni $\overline{4}$ ne sont inversibles.

L'anneau $\mathbb{K}[X]$ partage avec $\mathbb{Z}$ une propriété remarquable à savoir que tout idéal est engendré par un seul élément. C'est au final cette propriété qui permettra de définir les notions de pgcd et de ppcm :

Définition 5. On dit que l'anneau commutatif A est *principal* lorsque :
- A est intègre
- Tout idéal de A est principal, c'est-à-dire engendré par un seul élément.

Remarque : Pour chaque idéal non nul, il peut y avoir plusieurs générateurs, mais ils sont tous associés. Suivant la structure de $A^\times$ on peut ajouter un critère le rendant unique.

Théorème 4.
- *L'anneau $\mathbb{Z}$ est principal.*
- *L'anneau $\mathbb{K}[X]$ est principal.*

Remarques :
- Pour un idéal non nul de $\mathbb{Z}$, il y a un unique générateur dans $\mathbb{N}^*$
- Pour un idéal non nul de $\mathbb{K}[X]$, il a un unique générateur unitaire.

3 Compléments d'arithmétique dans $\mathbb{Z}$ et $\mathbb{K}[X]$

3.1 PGCD et PPCM dans les anneaux principaux

La notion pgcd vue dans $\mathbb{Z}$ et dans $\mathbb{K}[X]$ peut en fait être définie de façon très générale dans un anneau principal, en terme de générateur d'idéal.

Définition 6. Soit A un anneau principal et $a_1, \dots, a_n \in A$, avec $n \geqslant 2$.
- On appelle pgcd de $a_1, \dots, a_n$ tout générateur de l'idéal $(a_1) + \cdots + (a_n)$.
- On appelle ppcm de $a_1, \dots, a_n$ tout générateur de l'idéal $(a_1) \cap \cdots \cap (a_n)$.

Remarque : L'*identité de Bézout* est alors directement relié à cette définition : Si a est un pgcd de $a_1, \dots, a_n$, il existe $x_1, \dots, x_n \in A$ tels que :

$$a = a_1 x_1 + \cdots + a_n x_n$$

Exercice 7.

a) Montrer que a est un pgcd de $a_1, \dots, a_n$ si, et seulement si,
- $\forall k \in [\![1, n]\!],\ a | a_k$
- $\forall b \in a,\ (\forall k \in [\![1, n]\!],\ b | a_k) \Rightarrow b | a$

b) Énoncer et démontrer un énoncé similaire pour le ppcm.

Remarque : Rappelons que la relation de divisibilité | n'est qu'un *préordre* sur A (il manque l'antisymétrie). Puisqu'avoir $a|b$ $(b) \subset (a)$ (attention à l'ordre !), la relation de divisibilité peut s'interpréter alors comme la relation d'inclusion $\subset$ sur l'ensemble des idéaux de A, qui pour le coup est bien un ordre. Les notions de pgcd et de ppcm s'identifient alors respectivement aux notions de borne supérieure et de borne inférieure sur l'ensemble des ideaux muni de cet ordre. Autrement dit :
- a est un pgcd de $a_1 \dots, a_n$ si, et seulement si, $(a) = \sup\{(a_1), \dots, (a_n)\}$
- a est un ppcm de $a_1 \dots, a_n$ si, et seulement si, $(a) = \inf\{(a_1), \dots, (a_n)\}$

Exemples :
- 2 est un pgcd de 4 et 6 dans $\mathbb{Z}$ (-2 également !), ce qui se traduit par $(2) = 2\mathbb{Z} = \sup(4\mathbb{Z}, 6\mathbb{Z})$: $\mathbb{Z}$ et $2\mathbb{Z}$ sont les seul idéaux contenant $4\mathbb{Z}$ et $6\mathbb{Z}$, et $2\mathbb{Z}$ est le plus petit d'entre eux.
- 12 est un ppcm de 4 et 6 dans $\mathbb{Z}$, ce qui se traduit par $(12) = 12\mathbb{Z} = \inf(4\mathbb{Z}, 6\mathbb{Z})$: les idéaux contenus dans $4\mathbb{Z}$ et $6\mathbb{Z}$ sont $\{0\}$, $12\mathbb{Z}$, $24\mathbb{Z}$, $36\mathbb{Z}$, etc ...et $12\mathbb{Z}$ est le plus grand d'entre eux (il contient tous les autres).

3.2 Éléments premiers entre eux et théorème de Bézout

Définition 7. A étant un anneau principal, on dit que $a_1, \dots, a_n \in A$ sont *premiers entre eux* lorsque 1_A est un pgcd de $a_1, \dots, a_n$.

Remarque : Cela revient à dire que l'idéal $(a_1) + \cdots + (a_n)$ engendré par $a_1, \dots, a_n$ est A tout entier.

Proposition 7 (Théorème de Bézout)**.** *$a_1, \dots, a_n$ sont premiers entre eux si, et seulement si, il existe $x_1, \dots, x_n \in A$ tels que :*

$$1_A = a_1 x_1 + \cdots + a_n x_n$$

3.3 Cas des anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$

- Puisque $\mathbb{Z}^\times = \{1, -1\}$, on peut décider, pour tout idéal non nul de $\mathbb{Z}$, de choisir son unique générateur positif.
- Puisque $(\mathbb{K}[X])^\times = \mathbb{K}^*$ (ensemble des polynômes constants non nuls, c'est-à-dire de degré 0), on peut décider, pour tout idéal non nul de $\mathbb{K}[X]$, de choisir son unique générateur unitaire.

Dans ces deux cas, pgcd et ppcm deviennent uniques lorsqu'on ajoute ces contraintes.

Définition 8. Soient $a_1, \dots, a_n \in \mathbb{Z}$, avec $n \geqslant 2$.
- Si les a_i sont non tous nuls, on appelle PGCD de $a_1, \dots, a_n$ l'unique générateur strictement positif de l'idéal $(a_1) + \cdots + (a_n)$. On le note $a_1 \wedge \cdots \wedge a_n$, ou $\text{PGCD}(a_1, \dots, a_n)$.
- Si les a_i sont tous non nuls, on appelle PPCM de $a_1, \dots, a_n$ l'unique générateur strictement positif de $a_1\mathbb{Z} \cap \cdots \cap a_n\mathbb{Z}$. On le note $a_1 \vee \cdots \vee a_n$, ou $\text{PPCM}(a_1, \dots, a_n)$.

Remarque : Si on se restreint à $\mathbb{N}^*$, la relation de divisibilité $|$ devient un ordre. Les notions de PGCD et de PPCM s'identifient alors aux notions de borne inférieure et borne inférieure sur N^* muni de cet ordre.

Définition 9. Soient $P_1, \dots, P_n \in \mathbb{K}[X]$, avec $n \geqslant 2$.
- Si les P_i sont non tous nuls, on appelle PGCD de $P_1, \dots, P_n$ l'unique générateur unitaire de l'idéal $(P_1) + \cdots + (P_n)$. On le note $P_1 \wedge \cdots \wedge P_n$ ou $\text{PGCD}(P_1, \dots, P_n)$.
- Si les P_i sont tous non nuls, on appelle PPCM de $P_1, \dots, P_n$ l'unique générateur unitaire de l'idéal $(P_1) \cap \cdots \cap (P_n)$. On le note $P_1 \vee \cdots \vee P_n$ ou $\text{PPCM}(P_1, \dots, P_n)$.

Remarque : Si on se restreint à l'ensemble des polynômes non nuls unitaires, la relation de divisibilité $|$ devient un ordre. Les notions de PGCD et de PPCM s'identifient alors aux notions de borne inférieure et borne inférieure sur cet ensemble muni de cet ordre.