CHAPITRE 1

Algèbre générale

1.1 Groupes

1.1.1 Groupes $\mathbb{Z}/n\mathbb{Z}$

Ici, n désignera un entier > 0.

PROPOSITION 1.1.1. *Les sous-groupes de $\mathbb{Z}$ sont de la forme $a\mathbb{Z}$ où $a \in \mathbb{Z}$.*

Dém : On a déjà $\forall a \in \mathbb{Z}$, $a\mathbb{Z} = \{ak,\ k \in \mathbb{Z}\}$ qui est un sous-groupe de $\mathbb{Z}$.
Soit G un sous-groupe de $\mathbb{Z}$, si $G \neq \{0\}$ alors on considère $G \cap \mathbb{N}^*$ qui est non vide [1] et qui possède un plus petit élément $a > 0$.

- G contient alors tous les éléments de la forme $a.n$ où $n \in \mathbb{Z}$ (immédiat, par récurrence) soit $a\mathbb{Z} \subset G$.
- Si $x \in G$ alors on fait la division euclidienne de x par a : $x = a.n + r$ où $0 \leqslant r < a$. Or $r = x - a.n \in G$ donc $r = 0$ par définition de a. On a donc $G \subset a\mathbb{Z}$.

Conclusion : par double inclusion, on a prouvé que $G = a\mathbb{Z}$ (avec éventuellement $a = 0$) ■

DÉFINITION 1.1.1. ***Congruence***
Soient $(a, b) \in \mathbb{Z}^2$ et n un entier > 0, on dit que a est congru à b modulo n $ssi_{déf}$ n divise $a - b$.
On écrira alors $a \equiv b\ [n]$ ou $a \equiv b \mod n$.

PROPOSITION 1.1.2. ***Propriétés de la congruence***

- *La relation modulo n réalise une partition de $\mathbb{Z}$ en n sous-ensembles : pour chaque élément p de $\mathbb{Z}$ on note $\overline{p}$ l'ensemble des éléments de $\mathbb{Z}$ qui ont le même reste dans la division par n (i.e. $q \in \overline{p} \Leftrightarrow n | p - q$ soit $\overline{p} = p + n\mathbb{Z}$).*
- *Cette relation est compatible avec l'addition i.e.*
  Soit $(a, b, c) \in \mathbb{Z}^3$, si $a \equiv b \mod n$ alors $a + c \equiv b + c \mod n$.

[1] On sait qu'il existe $x \neq 0$ dans G, si $x < 0$ alors $-x \in G$

Dém : On a deux propriétés à démontrer.

- Soit $\overline{p} = \{p + k.n,\ k \in \mathbb{Z}\}$ que l'on note $p + n\mathbb{Z}$ en notation ensembliste. Montrons que $\{\overline{p},\ p \in [\![0, n-1]\!]\}$ est une partition de $\mathbb{Z}$:
  - Si $x \in \mathbb{Z}$ alors $x \in \overline{p}$ où p est le reste (qui appartient à $[\![0, n-1]\!]$) de la division euclidienne de x par n donc $\bigcup_{p\in[\![0,n-1]\!]} \overline{p} = \mathbb{Z}$. [2]
  - Si $p \neq p'$ alors, en supposant par exemple que $0 \leqslant p' < p \leqslant n-1$, si $x \in \overline{p} \cap \overline{p'}$ on a $x = p + k.n = p' + k'.n$ soit $p - p' = (k' - k).n$ or $p - p' \in [\![1, n-1]\!]$ donc $k' - k = 0$ ce qui est impossible donc $\overline{p} \cap \overline{p'} = \emptyset$ ■
- La deuxième propriété est immédiate :
  si $b = a + k.n$ alors $b + c = a + c + k.n$ ■

DÉFINITION 1.1.2. $\mathbb{Z}/n\mathbb{Z}$
$\mathbb{Z}/n\mathbb{Z}$ désigne l'ensemble $\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

THÉORÈME 1.1. **Groupe $\mathbb{Z}/n\mathbb{Z}$**
On définit l'addition dans $\mathbb{Z}/n\mathbb{Z}$ par $\overline{a+b} = \overline{a}\,\overline{+}\,\overline{b}$
(soit $(a + n\mathbb{Z})\,\overline{+}\,(b + n\mathbb{Z}) = a + b + n\mathbb{Z}$).
L'ensemble $\mathbb{Z}/n\mathbb{Z}$ muni de l'addition est un groupe additif.

Dém :

- On prouve d'abord que $\overline{a}\,\overline{+}\,\overline{b}$ est indépendant du représentant choisi : en effet, soit $a' \in \overline{a}$, $b' \in \overline{b}$ alors $a' = a + k.n$, $b' = b + k'.n$ donc $a' + b' = a + b + (k + k').n$ soit $\overline{a' + b'} = \overline{a + b}$.
- La loi $\overline{+}$ ainsi définie est bien une loi de composition interne.
- Montrons l'associativité : $(\overline{a}\,\overline{+}\,\overline{b})\,\overline{+}\,\overline{c} = \overline{a+b}\,\overline{+}\,\overline{c} = \overline{a+b+c}$ et, par symétrie, $\overline{a}\,\overline{+}\,(\overline{b}\,\overline{+}\,\overline{c}) = \overline{a+b+c}$ d'où l'égalité.
- L'élément neutre est $\overline{0}$ et le symétrique de $\overline{a}$ est $\overline{-a} = \overline{n-a}$.
- $\overline{+}$ est évidemment commutative.
- $\mathbb{Z}/n\mathbb{Z}$ muni de cette loi est un groupe additif ■

Par la suite, lorsqu'il n'y aura pas de confusion possible, on notera $+$ à la place de $\overline{+}$.

Remarque* 1.1.1.** *Si $p \in \mathbb{Z}$ alors $p\overline{a} = \overline{pa}$. L'application qui à $p \in \mathbb{Z}$ fait correspondre $\overline{p}$ est un morphisme de groupe appelé* ***morphisme canonique *de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$.*

Dém : On définit $p\overline{a} = \underbrace{\overline{a} + \cdots + \overline{a}}_{p \text{ fois}}$ si $p > 0$ et $p\overline{a} = \underbrace{-\overline{a} - \cdots - \overline{a}}_{-p \text{ fois}}$ si $p < 0$. On a bien

$$\begin{aligned}(p + p')\overline{a} &= \overline{(p + p')a} = \overline{pa + p'a} \\ &= \overline{pa} + \overline{p'a} = p\overline{a} + p'\overline{a}\end{aligned}$$

donc l'application $p \in \mathbb{Z} \mapsto p\overline{a}$ est un morphisme de groupe ■

[2] On a montré l'inclusion $\mathbb{Z} \subset \bigcup_{p\in[\![0,n-1]\!]} \overline{p}$, l'inclusion dans l'autre sens étant immédiate.

PROPOSITION 1.1.3.
Si $n = \overline{a_p a_{p-1} \dots a_0}$ est l'écriture de n en base 10 alors
congruence modulo 9 : $\overline{a_p a_{p-1} \dots a_0} \equiv a_p + a_{p-1} + \dots + a_0 \mod 9$.
congruence modulo 11 : $\overline{a_p a_{p-1} \dots a_0} \equiv (-1)^p a_p + (-1)^{p-1} a_{p-1} + \dots + a_0 \mod 11$.

Dém : Cette démonstration peut se faire en utilisant la structure d'anneau de $\mathbb{Z}/n\mathbb{Z}$ que l'on verra au 1.2.2.

- On a $10 - 1 = 9 \equiv 0 \mod 9$, $10^2 - 1 = 99 \equiv 0 \mod 9$, plus généralement $10^p - 1 = \underbrace{\overline{99\dots9}}_{p \text{ fois}} = 9 \times \overline{11\dots1} \equiv 0 \mod 9$ (écriture en base 10). On en déduit que $a_k \times 10^k \equiv a_k \mod 9$ d'où

$$n = \sum_{k=0}^{p} a_k \times 10^k \equiv \sum_{k=0}^{p} a_k \mod 9.$$

- Pour la congruence modulo 11 : $10^p - (-1)^p = (10+1)[10^{p-1} + \dots + (-1)^{p-1}]$ alors $10^p \equiv (-1)^p \mod 11$ et on procède comme ci-dessus ■

THÉORÈME 1.2. **Générateurs du groupe $\mathbb{Z}/n\mathbb{Z}$**
$\overline{a}$ engendre $\mathbb{Z}/n\mathbb{Z}$ ssi $a \wedge n = 1$.

Dém : On dit que $\overline{a}$ engendre $\mathbb{Z}/n\mathbb{Z}$ lorsque le groupe engendré par $\overline{a}$ vaut $\mathbb{Z}/n\mathbb{Z}$ soit $\{\overline{pa},\ p \in \mathbb{Z}\} = \mathbb{Z}/n\mathbb{Z}$.

- $\Rightarrow$ Si $\overline{a}$ engendre $\mathbb{Z}/n\mathbb{Z}$ alors, comme $\overline{1} \in \mathbb{Z}/n\mathbb{Z}$, il existe p tel que $p\overline{a} = \overline{1}$ ce qui se traduit par $pa = 1 + kn$ ou bien $pa - kn = 1$, et, par Bézout, $a \wedge n = 1$.

- $\Leftarrow$ En fait, si $a \wedge n = 1$ alors $\overline{pa} = \overline{1} + \overline{kn}$ (en reprenant ce qui a été fait ci-dessus) donc $\overline{q} = \overline{q1} = \overline{qpa} = \overline{qp}\,\overline{a}$ d'où $\overline{a}$ engendre $\mathbb{Z}/n\mathbb{Z}$ ■

Si G est un groupe, $a \in G$, on a défini dans le cours de première année le morphisme canonique de $\mathbb{Z}$ dans le groupe engendré par a ($k \mapsto ka$ ou $k \mapsto a^k$ selon la notation).

PROPOSITION 1.1.4. *Le noyau du morphisme canonique $\varphi_a : k \mapsto a^k$ est un sous-groupe de $\mathbb{Z}$ (donc de la forme $p\mathbb{Z}$).*
L'image est le groupe engendré par a noté (a).

Attention aux lois qui sont notées multiplicativement dans G et additivement dans $\mathbb{Z}$.
Dém : Il suffit de prouver que, d'une manière générale, le noyau d'un morphisme de groupe est un sous-groupe :
soit $f : G \to G'$ un morphisme de groupe, $H = \operatorname{Ker} f$, $.$ et $*$ étant les lois dans G et G' (notées multiplicativement), e et e' étant les éléments neutres de G et G'.

- $e \in H$ donc $H \neq \emptyset$,

- si x et x' sont dans H alors $f(x.x') = f(x) * f(x') = e' * e' = e'$ donc $x.x' \in H$,

- si $x \in H$ alors $f(x^{-1}) = f(x)^{-1} = e'$ donc $x^{-1} \in H$.

Conclusion : H est bien un sous-groupe de G.
Pour l'image : c'est immédiat par définition, en effet, tout élément de l'image de φ_a s'écrit a^k ■

DÉFINITION 1.1.3. ***Groupe monogène, groupe cyclique***
Soit G un groupe, on dit que G est monogène ssi$_{déf}$ G est engendré par un seul élément.
Si G est monogène et fini alors on dit qu'il est cyclique.

THÉORÈME 1.3. Soit G un groupe monogène engendré par a alors
si $\operatorname{Ker}\varphi_a = \{0\}$, G est isomorphe à $\mathbb{Z}$,
si $\operatorname{Ker}\varphi_a = n\mathbb{Z}$, G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Dém : Si $\operatorname{Ker}\varphi_a = \{0\}$ alors φ_a est injective, en effet, $\varphi_a(x) = \varphi_a(x')$ entraîne que $\varphi_a(x' - x) = e$ (élément neutre de G) soit $x' - x = 0$. Comme par définition φ_a est surjective, on en déduit qu'elle est bijective donc est un isomorphisme.
Si $\operatorname{Ker}\varphi_a = n\mathbb{Z}$ alors on définit $\overline{\varphi}_a : \overline{k} \mapsto a^k$ et on prouve que $\overline{\varphi}_a$ est un isomorphisme de G sur $\mathbb{Z}/n\mathbb{Z}$:

- Par définition, on sait que $a^n = e$ (e est toujours l'élément neutre de G) donc, si $k' \in \overline{k}$, alors $a^{k'} = a^{k+nu} = a^k.a^{nu} = a^k.(a^n)^u = a^k$ grâce aux propriétés des puissances, par conséquent $\overline{\varphi_a}$ est bien définie.
- $\overline{\varphi_a}$ est un morphisme de groupe : en effet

$$\begin{aligned}\overline{\varphi_a}(\overline{k} + \overline{k'}) = \overline{\varphi_a}(\overline{k + k'}) = \varphi_a(k + k') = a^{k+k'} = a^k a^{k'} \\ = \varphi_a(k)\varphi_a(k') = \overline{\varphi_a}(k)\overline{\varphi_a}(k').\end{aligned}$$

- $\overline{\varphi_a}$ est injective : si $\overline{\varphi_a}(\overline{k}) = e$ alors $a^k = e$ soit $k \in \operatorname{Ker}\varphi_a$ donc $k \in n\mathbb{Z}$ et par conséquent $\overline{k} = \overline{0}$.

Finalement, comme $\overline{\varphi_a}$ est surjective par définition, $\overline{\varphi_a}$ est un isomorphisme ■

***Remarque* 1.1.2.** *Une conséquence du théorème précédent est que si G est cyclique d'ordre n alors il est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. C'est le cas en particulier du groupe multiplicatif $\mathbb{U}_n$ des racines $n^{ièmes}$ de l'unité.*

Question : Montrer que tout sous-groupe H d'un groupe monogène $G = (a)$ est monogène (considérer $\{n \in \mathbb{Z} \mid a^n \in H\}$).

1.1.2 Groupes

DÉFINITION 1.1.4. ***Produit de deux groupes***
Si G_1 et G_2 sont deux groupes, on définit sur $G_1 \times G_2$ une structure de groupe en posant

$$(x_1, x_2).(y_1, y_2) = (x_1 y_1, x_2 y_2).$$

avec une notation multiplicative.

On prouve que, muni de cette loi, $G_1 \times G_2$ est un groupe :

- La loi est interne (par définition),
- elle est associative :

$$[(x_1,x_2).(y_1,y_2)].(z_1,z_2) = (x_1y_1,x_2y_2).(z_1,z_2) = (x_1y_1z_1,x_2y_2z_2)$$
$$= (x_1,x_2).[(y_1,y_2).(z_1,z_2)]$$

  par symétrie,
- l'inverse de (x_1,x_2) est (x_1^{-1},x_2^{-1}),
- l'élément neutre est donné par (e_1,e_2) où e_1 et e_2 sont les éléments neutres de G_1 et G_2 ■

PROPOSITION 1.1.5. *L'intersection d'une famille quelconque de sous-groupes d'un groupe G est un sous-groupe de G.*

Dém : Soient $(H_i)_{i\in I}$ une famille de sous-groupes de G, on pose $H = \bigcap_{i\in I} H_i$ et on va montrer que H est un sous-groupe de G :

- $e \in H$ (où e est l'élément neutre de G) donc $H \neq \emptyset$,
- si $(x,y) \in H^2$ alors $\forall i \in I$, $(x,y) \in H_i$ donc $xy^{-1} \in H_i$ par conséquent $xy^{-1} \in H$.

Conclusion : $H = \bigcap_{i\in I} H_i$ est bien un sous-groupe de G ■
Si A est une partie de G alors l'ensemble des sous-groupes de G qui contiennent A est non vide et leur intersection, vu la propriété précédente, est non vide. On peut donc poser la définition suivante :

DÉFINITION 1.1.5. ***Groupe engendré par une partie***
C'est l'intersection de tous les sous-groupes qui contiennent cette partie : si A est cette partie, on notera $gr(A)$ le groupe engendré par A.
C'est aussi le plus petit sous-groupe de G qui contient A.

PROPOSITION 1.1.6. *Soit A une partie non vide de G un groupe alors*

$$gr(A) = \{x \in G \mid \exists p \in \mathbb{N},\ \exists (a_1,a_2,\ldots,a_p) \in (A \cup A^{-1})^p \ | x = a_1a_2\ldots a_p\}$$

(A^{-1} désignant l'ensemble des inverses des éléments de A).

Dém : Soit $H = \{a_1a_2\ldots a_p,\ \text{où } a_i \in A \cup A^{-1}\}$.

- Montrons que H est un sous-groupe de G :
  - $A \subset H$ donc H est non vide,
  - si $a = a_1a_2\ldots a_p \in H$ et $b = b_1b_2\ldots b_q \in H$ alors on a immédiatement $ab^{-1} = a_1a_2\ldots a_pb_q^{-1}\ldots b_2^{-1}b_1^{-1} \in H$.

  H est un donc un sous-groupe de G et comme $H \supset A$ alors $H \supset gr(A)$ par définition du groupe engendré.
- On prouve par une récurrence immédiate sur p que, si $a_i \in A \cup A^{-1}$ alors $a_1\ldots a_p \in gr(A)$ donc $H \subset gr(A)$.

Conclusion : on a $H = gr(A)$ par double inclusion ■

DÉFINITION 1.1.6. ***Partie génératrice d'un groupe***
On dit que la partie A engendre G $ssi_{déf}$ $gr(A) = G$.
S'il existe une famille finie qui engendre G alors on dit que G est de type fini.

Questions :

(*i*) Si H est un sous-groupe de G, on définit $f_a(H) = \{axa^{-1} \text{ où } x \in H\}$.
Montrer que $f_a(H)$ est un sous-groupe de G.
Soit H le groupe des rotations de centre O du plan affine euclidien, a l'affinité d'axe Ox, de direction Oy, de rapport m. Soit M un point du plan, déterminer l'ensemble des points M' du plan tels que $\exists g \in f_a(H)$ vérifiant $M' = g(M)$.

(*ii*) Montrer que le groupe des isométries du carré $ABCD$ du plan où $A(1,1)$, $B(-1,1)$, $C(-1,-1)$ et $D(1,-1)$ est engendré par la symétrie par rapport à Ox et la rotation d'angle $\frac{\pi}{2}$ de centre O.

(*iii*) Montrer que $\mathrm{GL}_2(\mathbb{K})$ est engendré par les matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}$, $a \in \mathbb{K}$.

1.2 Anneaux et corps

1.2.1 Idéaux d'un anneau commutatif

DÉFINITION 1.2.1. ***Morphisme d'anneaux, isomorphisme***
Soient $(A, +, .)$ et $(B, +, .)$ deux anneaux et $f : A \to B$.
On dit que f est un morphisme d'anneaux $ssi_{déf}$ f est compatible avec les lois $+$ et $.$ et $f(1) = 1$.
On dit que f est un isomorphisme d'anneaux $ssi_{déf}$ f est un morphisme d'anneaux et f est bijective.

Exemple : L'application qui a un élément a de $\mathbb{R}$ fait correspondre la matrice aI_n est un morphisme d'anneaux de $(\mathbb{R}, +, .)$ dans $(\mathcal{M}_n(\mathbb{R}), +, .)$.

PROPOSITION 1.2.1. *Si f est un isomorphisme d'anneaux alors f^{-1} est aussi un isomorphisme d'anneaux.*

Dém : $f : A \to B$ étant bijective, $f^{-1} : B \to A$ est bien définie. Montrons que f^{-1} est un isomorphisme d'anneaux :

- Compatibilité avec l'addition :

$$\begin{aligned} f([f^{-1}(b_1 + b_2)]) = b_1 + b_2 &= f[f^{-1}(b_1)] + f[f^{-1}(b_2)] \\ &= f[f^{-1}(b_1) + f^{-1}(b_2)] \text{ car } f \text{ est un morphisme d'anneaux} \end{aligned}$$

  donc, comme f est bijective, $f^{-1}(b_1 + b_2) = f^{-1}(b_1) + f^{-1}(b_2)$.

- La compatibilité avec la multiplication se fait de la même manière.

- $f[f^{-1}(1_B)] = 1_B$ or $f(1_A) = 1_B$ et f est injective donc $f^{-1}(1_B) = 1_A$.

Conclusion : f^{-1} est bien un isomorphisme d'anneaux. ■

DÉFINITION 1.2.2. ***Noyau et image d'un morphisme d'anneaux***
Si f est un morphisme de A dans B, on appelle image de f l'ensemble $\operatorname{Im} f = f(A)$ *et noyau de f l'ensemble* $\operatorname{Ker} f = f^{-1}(0)$.

DÉFINITION 1.2.3. ***Idéal***
Soit A un anneau commutatif et $\mathcal{I} \subset A$, on dit que $\mathcal{I}$ est un idéal de A ssi$_{déf}$

(i) $(\mathcal{I}, +)$ est un sous-groupe de $(A, +)$.

(ii) $\mathcal{I}$ est absorbant (i.e. $\forall a \in A$, $\forall \alpha \in \mathcal{I}$, $\alpha a \in \mathcal{I}$).

Exemples : $\mathcal{I} = \{0\}$, $\mathcal{I} = A$, $\mathcal{I} = xA$ (voir démonstration ci-dessous).

PROPOSITION 1.2.2. *L'intersection d'une famille quelconque d'idéaux est un idéal.*

Dém : Soient $(\mathcal{I}_i)_{i\in I}$ une famille d'idéaux de A, on pose $\mathcal{I} = \bigcap_{i\in I} \mathcal{I}_i$ et on va montrer que $\mathcal{I}$ est un idéal de A :

- $0 \in \mathcal{I}$ donc $\mathcal{I} \neq \emptyset$,
- si $(x, y) \in \mathcal{I}^2$ alors $\forall i \in I$, $(x, y) \in \mathcal{I}_i$ donc $x - y \in \mathcal{I}_i$ par conséquent $x - y \in \mathcal{I}$,
- si $\alpha \in A$ et $x \in \mathcal{I}$ alors, $\forall i \in I$, $x \in \mathcal{I}_i$ donc $\alpha x \in \mathcal{I}_i$ soit $\alpha x \in \mathcal{I}$.

Conclusion : $\mathcal{I} = \bigcap_{i\in I} \mathcal{I}_i$ est bien un idéal de A ■

PROPOSITION 1.2.3. ***Idéal engendré par un élément***
Si $x \in A$ alors $Ax = xA$ est un idéal, c'est l'idéal engendré par x (parfois noté (x)).

Dém : Ax est bien un idéal (vérification immédiate). Notons $\mathcal{I}_x$ l'idéal engendré par x i.e. l'intersection des idéaux qui contiennent x.

- Alors $\forall \alpha \in A$, $\alpha x \in \mathcal{I}_x$ donc $Ax \subset \mathcal{I}_x$.
- Ax est un idéal qui contient x donc, par définition de $\mathcal{I}_x$, $\mathcal{I}_x \subset Ax$.

Conclusion : on a $\mathcal{I}_x = Ax$ par double inclusion et on a la remarque suivante ■

***Remarque* 1.2.1.** *En fait, l'idéal engendré par un élément est l'intersection des idéaux qui contiennent cet élément.*

PROPOSITION 1.2.4. *Si f est un morphisme d'anneaux de A dans B alors* $\operatorname{Ker} f$ *est un idéal de A et $f(A)$ est un sous-anneau de B.*

Dém : On sait déjà que $\operatorname{Ker} f$ est un sous-groupe de A et il est facile de vérifier que $f(A)$ est un sous-groupe de B.

- Si $\alpha \in A$ et $x \in \operatorname{Ker} f$ alors $f(\alpha x) = f(\alpha) f(x) = 0$ donc $\alpha x \in \operatorname{Ker} f$, $\operatorname{Ker} f$ est bien un idéal de A.
- $f(1_A) = 1_B$ donc $1_B \in f(A)$ et, si $b_1 = f(a_1)$, $b_2 = f(a_2)$ sont dans $f(A)$ alors $b_1 b_2 = f(a_1) f(a_2) = f(a_1 a_2) \in f(A)$ donc $f(A)$ est un sous-anneau de B ■

DÉFINITION 1.2.4. ***Divisibilité dans un anneau intègre***
Soit A un anneau intègre, on dit que x divise y (noté $x|y$) ssi$_{déf}$ il existe $z \in A$ tel que $y = xz$.

PROPOSITION 1.2.5. *On a l'équivalence suivante : $x|y$ ssi $Ay \subset Ax$.*

Dém : L'équivalence est immédiate :

- Si $x|y$ alors $y = xz$ donc $\alpha y = \alpha zx$ pour tout $\alpha \in A$ soit $Ay \subset Ax$.
- Si $Ay \subset Ax$ alors $y \in Ax$ donc il existe $z \in A$ tel que $y = xz$ ■

Questions :

(*i*) Soit $f : (a,b) \in \mathbb{Z}^2 \mapsto a + ib\sqrt{3} \in \mathbb{C}$. f est-il un morphisme d'anneaux ?

(*ii*) Si $\mathcal{I}$ et $\mathcal{J}$ sont deux idéaux de A, on définit

$$\mathcal{I} + \mathcal{J} = \{x \in A \mid \exists (a,b) \in \mathcal{I} \times \mathcal{J},\ x = a + b\},$$

$$\mathcal{I}.\mathcal{J} = \{x \in A \mid \exists n \in \mathbb{N},\ \exists (a_i, b_i) \in \mathcal{I} \times \mathcal{J},\ x = \sum_{i=1}^{n} a_i b_i\}.$$

Montrer que $\mathcal{I} + \mathcal{J}$ et $\mathcal{I}.\mathcal{J}$ sont des idéaux. A-t-on $\mathcal{I}.\mathcal{J} = \mathcal{I} \cap \mathcal{J}$?

1.2.2 Idéaux de $\mathbb{Z}$, anneau $\mathbb{Z}/n\mathbb{Z}$

THÉORÈME 1.4. **Idéaux de $\mathbb{Z}$**
Les idéaux de $\mathbb{Z}$ sont de la forme $a\mathbb{Z}$ (on dit que $\mathbb{Z}$ est un anneau principal).

Dém : Soit $\mathcal{I}$ un idéal de $\mathbb{Z}$, $\mathcal{I}$ est un sous-groupe de $\mathbb{Z}$ donc il existe $a \in \mathbb{Z}$ tel que $\mathcal{I} = a\mathbb{Z}$. Tous les idéaux de $\mathbb{Z}$ sont donc de la forme $a\mathbb{Z}$.
On sait que $\forall a \in \mathbb{Z}$, $a\mathbb{Z}$ est un idéal donc on peut conclure ■

PROPOSITION 1.2.6. ***Caractérisation du P.G.C.D. et du P.P.C.M.***

(*i*) $(d = a \wedge b) \Leftrightarrow (a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z},\ d > 0)$.

(*ii*) $(m = a \vee b) \Leftrightarrow (a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z},\ m > 0)$.

Dém :

(*i*) ($\Rightarrow$) D'après le théorème de Bézout, on sait qu'il existe u et v dans $\mathbb{Z}$ tels que $d = au + bv$. On a donc $\forall k \in \mathbb{Z}$, $d.k \in a\mathbb{Z} + b\mathbb{Z} = \{au' + bv',\ (u',v') \in \mathbb{Z}^2\}$ et par conséquent $d\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z}$.
Inclusion dans l'autre sens : $d|a$ et $d|b \Rightarrow a\mathbb{Z} \subset d\mathbb{Z}$ et $b\mathbb{Z} \subset d\mathbb{Z}$ (propriété de la divisibilité) par conséquent $a\mathbb{Z} + b\mathbb{Z} \subset d\mathbb{Z}$ car $d\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.
On a donc $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$.
($\Leftarrow$) si $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$, soit $d' = a \wedge b$, on vient de prouver que $d'\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$ donc $d'\mathbb{Z} = d\mathbb{Z}$. On en déduit que $d|d'$ et $d'|d$ (toujours les propriétés de la divisibilité) soit $d = k'd'$ et $d' = kd$. Or $d' > 0$ et $d > 0$ donc $d = k'kd$ soit $k'k = 1$ avec k' et k positifs soit $k = k' = 1$.
Conclusion : on a bien $d = d'$ i.e. $d = a \wedge b$.

(*ii*) ($\Rightarrow$) On a $m = ka = k'b$ donc $m \in a\mathbb{Z} \cap b\mathbb{Z}$ d'où $m\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z}$ car $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.
Inclusion dans l'autre sens : $a\mathbb{Z} \cap b\mathbb{Z} = m'\mathbb{Z}$ ($a\mathbb{Z} \cap b\mathbb{Z}$ est un idéal donc il est engendré par un élément $m' \in \mathbb{Z}$). m' est un multiple commun à a et b. Or $m\mathbb{Z} \subset m'\mathbb{Z}$ i.e. $m = km'$ et $m' \geqslant m$ car m est le plus petit commun multiple de a et b donc $k = 1$ soit $m = m'$.
($\Leftarrow$) Si $m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$, soit $m' = a \vee b$, on vient de prouver que $m'\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$ donc $m'\mathbb{Z} = m\mathbb{Z}$ d'où $m = m'$ car on a supposé $m > 0$ (même argument que pour le P.G.C.D.) ■

Exemples illustratifs :

(*i*) Théorème de Bézout : si $a \wedge b = 1$ alors $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$ (ici, on a $d = 1$).

(*ii*) Théorème de Gauss : si $bc\mathbb{Z} \subset a\mathbb{Z}$ et $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$ alors $c\mathbb{Z} \subset a\mathbb{Z}$.

PROPOSITION 1.2.7. *Si* $a \equiv b \mod n$ *et* $c \equiv d \mod n$ *alors* $ac \equiv bd \mod n$.

Dém : $a = b + kn$, $c = d + k'n$ donc $ac = bd + (kd + k'b + kk'n)n$ ce qui signifie que $ac \equiv bd \mod n$ ■

THÉORÈME 1.5. Grâce à la propriété précédente, $(\mathbb{Z}/n\mathbb{Z}, +, .)$ est un anneau.

Dém : On sait déjà que $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe et $\overline{a}.\overline{b} = \overline{ab}$ est indépendant du représentant choisi vu la proposition précédente.
On vérifie alors que $\mathbb{Z}/n\mathbb{Z}$ est un anneau :

- La loi . est une loi interne par définition,
- elle est associative :

$$\begin{aligned}(\overline{a}.\overline{b}).\overline{c} &= \overline{ab}.\overline{c} = \overline{abc} \\ &= \overline{a}.(\overline{b}.\overline{c}) \text{ par symétrie}\end{aligned}$$

- $\overline{1}$ est l'élément neutre pour la multiplication,
- . est distributive par rapport à + (à droite et à gauche), là aussi, la vérification est immédiate ■

PROPOSITION 1.2.8. *L'application* $a \in \mathbb{Z} \mapsto \bar{a} \in \mathbb{Z}/n\mathbb{Z}$ *est un morphisme d'anneaux appelé morphisme canonique.*

Dém : On sait déjà que cette application est un morphisme de groupes, on la note φ. On vérifie alors que $\varphi(1) = \overline{1}$ élément neutre pour la multiplication dans $\mathbb{Z}/n\mathbb{Z}$ puis que $\varphi(ab) = \overline{ab} = \varphi(a)\varphi(b)$ ■

***Remarque* 1.2.2.** *Il n'existe qu'un seul morphisme de* $\mathbb{Z}$ *dans un anneau* A, *en effet* $\varphi(1) = 1_A$ *permet de définir sans ambiguïté* φ.

Dém : On pose en effet $\varphi(n) = n.1_A = \underbrace{1_A + \cdots + 1_A}_{n \text{ fois}}$ si $n > 0$, $\varphi(0) = 0$ et $\varphi(n) = (-n)(-1_A)$ si $n < 0$. φ est bien un morphisme d'anneaux.
Si ψ est un autre morphisme d'anneaux de $\mathbb{Z}$ dans A alors $\psi(1) = 1_A$ puis, par récurrence sur n, $\psi(n) = \varphi(n)$ si $n > 0$. Finalement $\psi(n) = \varphi(n)$ pour tout $n \in \mathbb{Z}$ ce qui permet de conclure à l'unicité ■
Attention à ne pas dire ici qu'il y a unicité par construction car c'est insuffisant, il n'y a peut-être pas unicité de la construction.

THÉORÈME 1.6. **Factorisation du morphisme de $\mathbb{Z}$ dans A**
Si φ est le morphisme canonique de $\mathbb{Z}$ dans un anneau A, $\operatorname{Ker}\varphi = n\mathbb{Z}$ son noyau alors il existe un unique isomorphisme $\overline{\varphi}$ de $\mathbb{Z}/n\mathbb{Z}$ dans $\varphi(\mathbb{Z}) \subset A$ telle que $\overline{\varphi}(\bar{a}) = \varphi(a)$.

Dém : $\overline{\varphi}$ est bien définie (la valeur de $\overline{\varphi}(\bar{a})$ ne dépend pas du représentant choisi), $\overline{\varphi}$ est bien un isomorphisme de groupe de $\mathbb{Z}/n\mathbb{Z}$ sur $\varphi(\mathbb{Z})$ cf. Th 1.3 page 174 [3] et on a $\overline{\varphi}(1) = \varphi(1) = 1_A$,

$$\begin{aligned}\overline{\varphi}(\overline{a}.\overline{b}) &= \overline{\varphi}(\overline{a.b}) = \varphi(a.b) = \varphi(a).\varphi(b)\\ &= \overline{\varphi}(\overline{a}).\overline{\varphi}(\overline{b})\end{aligned}$$

ce qui achève la démonstration ■

DÉFINITION 1.2.5. ***Caractéristique d'un corps***
Si $\mathbb{K}$ est un corps, φ l'unique morphisme que l'on peut définir de $\mathbb{Z}$ dans $\mathbb{K}$ et $p\mathbb{Z}$ le noyau de φ alors p est appelé caractéristique de $\mathbb{K}$.

***Remarque* 1.2.3.**

(*i*) *La caractéristique de $\mathbb{Z}/p\mathbb{Z}$ est p.*

Dém : Immédiat avec le théorème précédent, le noyau de $\varphi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ est $p\mathbb{Z}$ ■

(*ii*) *La caractéristique d'un corps est un nombre premier ou 0 (c'est la même chose pour un anneau intègre).*

Dém : Par l'absurde, si $p = qr$ avec $q > 1$ et $r > 1$ où p est la caractéristique du corps en question alors $p1_{\mathbb{K}} = qr1_{\mathbb{K}} = (q1_{\mathbb{K}})(r1_{\mathbb{K}}) = 0$ avec $q1_{\mathbb{K}} \neq 0$ et $r1_{\mathbb{K}} \neq 0$ ce qui est impossible, donc p est bien premier (et c'est effectivement encore vrai dans un anneau intègre) ■

PROPOSITION 1.2.9. ***Indicatrice d'Euler***
l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ est $\{\bar{a},\ a \wedge n = 1\}$.
On appelle indicatrice d'Euler le nombre d'éléments inversibles dans $\mathbb{Z}/n\mathbb{Z}$.

Dém : Immédiat avec l'égalité de Bézout : en effet on utilise la démonstration du théorème 1.2 et on a équivalence entre $\overline{a}$ engendre $\mathbb{Z}/n\mathbb{Z}$ et $\overline{a}$ inversible ■
Cette dernière fonction joue un grand rôle en arithmétique et en codage informatique.

[3] énoncé en notation multiplicative pour la loi de groupe, utilisé ici en notation additive

THÉORÈME 1.7. $\mathbb{Z}/p\mathbb{Z}$ est un corps ssi p est premier.

Dém : On sait déjà que si $\mathbb{Z}/p\mathbb{Z}$ est un corps alors p est premier (cf. remarque 1.2.3).
Réciproque : si p est premier alors, grâce à la proposition 1.2.9, tous les éléments de $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ sont inversibles donc $\mathbb{Z}/p\mathbb{Z}$ est un corps ■
Questions :

(*i*) Montrer que $10^6 \equiv 1\ [7]$, en déduire que $\sum_{k=1}^{12} 10^{10^k} \equiv -1\ [7]$.

(*ii*) Montrer que 121 ne divise jamais $n^2 + 3n + 5$.

(*iii*) Petit théorème de Fermat : si p est un nombre premier, montrer que, pour tout entier k, on a $k^p \equiv k\ [p]$.
En déduire que si $n \equiv 1[p-1]$ alors $k^n \equiv k\ [p]$.

(*iv*) Théorème de Wilson : montrer l'équivalence $(p-1)! + 1 \equiv 0\ [p] \Leftrightarrow p$ premier.

1.2.3 Application à la cryptographie

THÉORÈME 1.8. **Théorème Chinois**
Soient p et q deux entiers premiers entre eux et $(y, z) \in \mathbb{Z}^2$ alors il existe un entier x dans $\mathbb{Z}$ tel que $\begin{cases} x \equiv y \mod p \\ x \equiv z \mod q \end{cases}$.
Toutes les solutions de ce système sont congrues modulo pq.

Dém : Soit u, v tels que $up + vq = 1$ alors $y - z = up(y-z) + vq(y-z)$ soit $y + up(z-y) = z + vq(y-z)$. Il suffit alors de prendre $x = y + up(z-y) = z + vq(y-z)$.
Si x et x' sont deux solutions alors $p|x - x'$ et $q|x - x'$ et donc, en vertu du théorème de Gauss, comme p et q sont premiers entre-eux, $pq|x - x'$ soit $x - x' \equiv 0 \mod pq$.
Conclusion : toutes les solutions sont congrues modulo pq ■

COROLLAIRE 1.9.
Si p et q deux entiers premiers entre eux alors il existe un isomorphisme d'anneaux de $\mathbb{Z}/pq\mathbb{Z}$ sur $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ (muni de la structure produit).

Dém : On définit la structure produit dans un anneau de la manière suivante : si A_1 et A_2 sont deux anneaux alors $(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$ (loi de groupe produit) et $(x_1, y_1) \times (x_2, y_2) = (x_1 y_1, x_2, y_2)$ permettent de munir $A_1 \times A_2$ d'une structure d'anneau ($(1_{A_1}, 1_{A_2})$ étant le neutre pour la multiplication).
On prend alors $\Phi : x \in \mathbb{Z} \mapsto (x \mod p, x \mod q)$. $\Phi(x) = 0$ ssi $p|x$ et $q|x$ ce qui est encore équivalent à $pq|x$ donc $\operatorname{Ker}\Phi = pq\mathbb{Z}$. Φ est surjective grâce au théorème précédent.
(Si $(\overline{y}, \overline{z}) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ alors on sait qu'il existe $x \in \mathbb{Z}$ tel que $x \equiv y \mod p$ et $x \equiv z \mod q$ donc $\Phi(x) = (\overline{y}, \overline{z})$).
D'après le théorème 1.6 page 180, $\overline{\Phi}$ définie par $\overline{\Phi}(\overline{a}) = \Phi(a)$ est un isomorphisme d'anneaux ■

***Remarque* 1.2.4.**

(*i*) *On peut, grâce au dernier corollaire, en déduire l'expression de l'indicatrice d'Euler $\varphi(pq)$ égale au nombre d'éléments inversibles dans l'anneau $\mathbb{Z}/pq\mathbb{Z}$.*

$$\varphi(pq) = pq\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right) \text{ si } p \text{ et } q \text{ sont des nombres premiers.}$$

Dém : comme $\overline{\Phi}$ est un isomorphisme de $\mathbb{Z}/pq\mathbb{Z}$ sur $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z}$ alors $\overline{\Phi}$ transforme tout élément inversible de $\mathbb{Z}/pq\mathbb{Z}$ en un élément inversible de $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z}$. Il en est de même de $\overline{\Phi}^{-1}$ i.e. $\overline{\Phi}$ réalise une bijection de $U(\mathbb{Z}/pq\mathbb{Z})$ sur $U(\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z})$ ($U(A)$ désignant l'ensemble des éléments inversibles d'un anneau A). On a donc égalité des cardinaux.
Or $(\overline{y},\overline{z}) \in \mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z}$ est inversible ssi $\overline{y}$ et $\overline{z}$ le sont (vu la définition de l'anneau produit) donc

$$\begin{aligned}\operatorname{Card} U(\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z}) &= \operatorname{Card} U(\mathbb{Z}/p\mathbb{Z})\times \operatorname{Card}(U(\mathbb{Z}/q\mathbb{Z})) \\ &= \varphi(p)\varphi(q) = (p-1)(q-1) = pq\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right) \blacksquare\end{aligned}$$

(*ii*) *Une application de cette dernière égalité est le codage RSA.*

Questions :

(*i*) Montrer que si $n \equiv 1\ [\varphi(pq)]$ où p et q sont deux nombres premiers alors pour tout entier x on a $x^n \equiv x\ [pq]$ (utiliser la question (*iii*) page 181).

(*ii*) Montrer que si α est un nombre premier avec $\varphi(pq)$ et si β est un nombre tel que $\alpha\beta \equiv 1\ [\varphi(pq)]$ alors l'application

$$\mathcal{C} : x \in \mathbb{Z}/pq\mathbb{Z} \mapsto x^\alpha \in \mathbb{Z}/pq\mathbb{Z}$$

admet comme application réciproque

$$\mathcal{D} : x \in \mathbb{Z}/pq\mathbb{Z} \mapsto x^\beta \in \mathbb{Z}/pq\mathbb{Z}.$$

C'est le principe du codage RSA, en effet on donne le nombre α et le produit pq. Le codage est alors facile (on utilise l'algorithme d'exponentiation rapide) mais si on ne connaît pas les nombres p et q alors (pour p et q très grand) il est impossible de déterminer β. En effet il faut connaître $\varphi(pq)$ pour déterminer β. Dans la pratique on choisira des nombres α et β les plus petits possible.

1.2.4 Idéaux de $\mathbb{K}[X]$

On reprend dans ce paragraphe l'étude qui a été faite sur $\mathbb{Z}$ pour l'appliquer à $\mathbb{K}[X]$.

THÉORÈME 1.10. **Idéaux de $\mathbb{K}[X]$**
Les idéaux de $\mathbb{K}[X]$ sont de la forme $P\mathbb{K}[X]$ où P est un polynôme de $\mathbb{K}[X]$ (on dit que $\mathbb{K}[X]$ est un anneau principal).

Dém :

- On sait que $P\mathbb{K}[X]$ est un sous-groupe de $\mathbb{K}[X]$. Il est facile de vérifier qu'il est stable par produit d'un élément de $\mathbb{K}[X]$ donc c'est bien un idéal.
- Soit $\mathcal{I} \neq \{0\}$ un idéal de $\mathbb{K}[X]$, $E = \{\deg Q,\ Q \in \mathcal{I} \setminus \{0\}\} \subset \mathbb{N}^*$, $E \neq \emptyset$. Soit $p = \inf E$ et $P \in \mathbb{K}[X]$ de degré p. Si $Q \in \mathcal{I}$, $Q = PK + R$ (division euclidienne de Q par P) alors $R = Q - PK \in \mathcal{I}$ et $\deg R < \deg P$ donc $R = 0$ soit $Q \in P\mathbb{K}[X]$.

Conclusion : les idéaux de $\mathbb{K}[X]$ sont de la forme $\mathcal{I} = P\mathbb{K}[X]$ ■

PROPOSITION 1.2.10. ***Caractérisation du P.G.C.D. et du P.P.C.M.***

(*i*) *$(D = P \wedge Q) \Leftrightarrow (D\mathbb{K}[X] = P\mathbb{K}[X] + Q\mathbb{K}[X]$, D unitaire).*

(*ii*) *$(M = P \vee Q) \Leftrightarrow (M\mathbb{K}[X] = P\mathbb{K}[X] \cap Q\mathbb{K}[X]$, M unitaire).*

Dém : c'est la même chose que pour la proposition 1.2.6 page 178 :

(*i*) ($\Rightarrow$) D'après le théorème de Bézout, on sait qu'il existe U et V dans $\mathbb{Z}$ tels que $D = PU + QV$. On a donc

$$\forall K \in \mathbb{K}[X],\ D.K \in P\mathbb{K}[X] + Q\mathbb{K}[X] = \{PU' + QV',\ (U', V') \in \mathbb{K}[X]^2\}$$

et par conséquent $D\mathbb{K}[X] \subset P\mathbb{K}[X] + Q\mathbb{K}[X]$.
Inclusion dans l'autre sens : $D|P$ et $D|Q$ entraîne $P\mathbb{K}[X] \subset D\mathbb{K}[X]$ et $Q\mathbb{K}[X] \subset D\mathbb{K}[X]$ (propriété de la divisibilité) par conséquent on obtient $P\mathbb{K}[X] + Q\mathbb{K}[X] \subset D\mathbb{K}[X]$ car $D\mathbb{K}[X]$ est un sous-groupe de $\mathbb{K}[X]$.
($\Leftarrow$) si $D\mathbb{K}[X] = P\mathbb{K}[X] + Q\mathbb{K}[X]$, soit $D' = P \wedge Q$, on vient de prouver que $D'\mathbb{K}[X] = P\mathbb{K}[X] + Q\mathbb{K}[X]$ donc $D'\mathbb{K}[X] = D\mathbb{K}[X]$. On en déduit que $D|D'$ et $D'|D$ (toujours les propriétés de la divisibilité) soit $D = K'D'$ et $D' = KD$. Or D' et D sont unitaires donc $D = K'KD$ soit $K'K = 1$ avec K' et K unitaires (examiner les termes de plus haut degré dans les produits $D = K'D'$ et $D' = KD$) soit $K = K' = 1$.
Conclusion : on a bien $D = D'$ i.e. $D = P \wedge Q$.

(*ii*) ($\Rightarrow$) On a $M = KP = K'Q$ donc $M \in P\mathbb{K}[X] \cap Q\mathbb{K}[X]$ d'où on déduit $M\mathbb{K}[X] \subset P\mathbb{K}[X] \cap Q\mathbb{K}[X]$ car $P\mathbb{K}[X] \cap Q\mathbb{K}[X]$ est un sous-groupe de $\mathbb{K}[X]$.
Inclusion dans l'autre sens : $P\mathbb{K}[X] \cap Q\mathbb{K}[X] = M'\mathbb{K}[X]$ ($P\mathbb{K}[X] \cap Q\mathbb{K}[X]$ est un idéal donc il est engendré par un élément $M' \in \mathbb{K}[X]$). M' est un multiple commun à P et Q. Or $M\mathbb{K}[X] \subset M'\mathbb{K}[X]$ i.e. $M = KM'$ et $\deg M' \geqslant \deg M$ car M est le plus petit commun multiple de P et Q donc $K = 1$ soit $M = M'$.
($\Leftarrow$) Si $M\mathbb{K}[X] = P\mathbb{K}[X] \cap Q\mathbb{K}[X]$, soit $M' = P \vee Q$, on vient de prouver que $M'\mathbb{K}[X] = P\mathbb{K}[X] \cap Q\mathbb{K}[X]$ donc $M'\mathbb{K}[X] = M\mathbb{K}[X]$ d'où $M = M'$ car on a supposé $M0$ unitaire (même argument que pour le P.G.C.D.) ■

Exemples d'applications :

(*i*) Théorème de Bézout : si $P \wedge Q = 1$ alors $P\mathbb{K}[X] + Q\mathbb{K}[X] = \mathbb{K}[X]$.

(*ii*) Théorème de Gauss : si $QR\mathbb{K}[X] \subset P\mathbb{K}[X]$ et $P\mathbb{K}[X] + Q\mathbb{K}[X] = \mathbb{K}[X]$ alors $R\mathbb{K}[X] \subset P\mathbb{K}[X]$.

Questions :

(*i*) Montrer l'équivalence

$$D = P_1 \wedge (P_2 \wedge P_3) \Leftrightarrow D\mathbb{K}[X] = P_1\mathbb{K}[X] + P_2\mathbb{K}[X] + P_3\mathbb{K}[X].$$

Généraliser.

(*ii*) Déterminer $\mathcal{I}.\mathcal{J}$ lorsque $\mathcal{I} = P\mathbb{K}[X]$ et $\mathcal{J} = Q\mathbb{K}[X]$ (cf. question (*ii*) page 178).

(*iii*) Soit P, Q, R trois polynômes de $\mathbb{C}[X]$, on suppose $Q \wedge R = 1$ et $P^2 = Q^2 + R^2$. Montrer qu'il existe P_1 et P_2 2 polynômes premiers entre eux tels que

$$Q = \frac{1}{2}[P_1^2 + P_2^2],\ R = \frac{1}{2i}[P_1^2 - P_2^2].$$