Programme de colle : semaine 11

I Arithmétique

I.1 Questions de cours

Enoncer et démontrer la propriété fondamentale de $\mathbb{Z}$.

Théorème 12.1

Toute partie non vide et minorée de $\mathbb{Z}$ admet un plus petit élément.

Soit A une partie non vide et minorée de $\mathbb{Z}$.
On note $\mathcal{M}$ l'ensemble des minorants de A.
Par hypothèse, $\mathcal{M} \neq \emptyset$.
Supposons par l'absurde que :

$$\forall a \in \mathbb{Z}, a \in \mathcal{M} \Rightarrow a+1 \in \mathcal{M}$$

D'après le principe de récurrence, si $a_0 \in \mathcal{M}$ est fixé :

$$\forall n \geq a_0, n \in \mathcal{M}$$

En particulier, pour $n \in A$ ($A \neq \emptyset$) on a :

$$n \geq a_0 \ (a_0 \text{ est un minorant})$$

Donc $n \in \mathcal{M}$.
Donc $n+1 \in \mathcal{M}$.
Donc $n+1$ est un minorant de A.
Donc $n+1 \leq n$.
Absurde.

Ainsi, on choisit $a \in \mathbb{Z}$ avec $a \in \mathcal{M}$ et $a+1 \notin \mathcal{M}$.
On choisit donc $n \in A$ tel que :

$$a \leq n < a+1$$

Donc $n = a \in A$.
Donc $a = \min(A)$.

Enoncer et démontrer le théorème de la division euclidienne.

Théorème 12.4

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$. Il existe un unique coupe $(q,r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

$$a = bq + r$$

avec $0 \leq r < |b|$. Cette égalité est appelée **division euclidienne de a par b**, l'entier q est alors appelé **quotient** et l'entier r le **reste**, tandis que a porte le nom de dividende et b celui de diviseur.

Existence :
On suppose dans un premier temps que $b > 0$.
Soit $a \in \mathbb{Z}$.
On note $A = \{n \in \mathbb{Z}, bn \leq a\}$.
A est un sous-ensemble non vide de $\mathbb{Z}$ et majoré.
Il admet donc un plus grand élément, noté q. On a donc $q \in A$ et $q+1 \notin A$.

$$bq \leq a < b(q+1)$$
$$\text{donc } 0 \leq a - bq < b$$

On pose alors $r = a - bq$. L'exsitence est alors prouvée pour $b > 0$.
Si $b < 0$, alors $-b > 0$ et on choisit $(q,r) \in \mathbb{Z}^2$ tel que :

$$a = -b \times q + r \text{ avec } 0 \leq r < -b$$

Le couple $(-q, r)$ convient.

Unicité :
On suppose $a = bq + r = bq' + r'$ avec $0 \leq r,' < |b|$.
Donc $b(q - q') = r' - r$.
Donc $\underbrace{|b|}_{>0} \times |q - q'| = |r' - r| < \underbrace{|b|}_{>0}$.
Donc $|q - q'| < 1$.
Donc $q = q'$.
Puis $r = r'$.

Enoncer et démontrer le théorème de Bézout.

Théorème 12.26

Soit a et b deux entiers. Alors a et b sont premiers entre eux si et seulement si il existe $(u,v) \in \mathbb{Z}^2$ tel que

$$au + bv = 1$$

$\boxed{\Rightarrow}$
On suppose a et b premiers entre eux.
Donc $\mathcal{D}_{a,b} = \{\pm 1\}$.
Soit r le dernier reste non nul dans l'algorithme d'Euclide,

$$\mathcal{D}_r = \mathcal{D}_{a,b} = \{\pm 1\}$$

Donc $r = \pm 1$.
D'après le théorème de Bézout, il existe deux entiers u et v tels que :

$$au + bv = 1$$

$\boxed{\Leftarrow}$
Réciproquement, si $au+bv=1$, alors pour tout $d\in\mathcal{D}_{a,b}$ $d|au+bv$ donc $d|1$ donc $d=\pm 1$.
Donc $\mathcal{D}_{a,b}=\{\pm 1\}$.

Enoncer et démontrer la proposition caractérisant le pgcd par les idéaux.

Propostion 12.37

Soit a et b deux entiers, alors d est le *pgcd* de a et b si et seulement si $a\mathbb{Z}+b\mathbb{Z}=d\mathbb{Z}$.

Soit $(a,b)\in\mathbb{Z}^2$. $a\mathbb{Z}$ et $b\mathbb{Z}$ dont des idéaux de $\mathbb{Z}$.
Donc $a\mathbb{Z}+b\mathbb{Z}$ est un idéal de $\mathbb{Z}$, donc en particulier un sous-groupe de $\mathbb{Z}$.
On choisit donc $d\geq 0$ tel que $a\mathbb{Z}+b\mathbb{Z}=d\mathbb{Z}$.
Montrons que $d=pgcd(a,b)=a\wedge b$.
D'une part :

$$\begin{aligned} d\in d\mathbb{Z} &\qquad \text{donc } d=au+bv \text{ (avec } (u,v)\in\mathbb{Z}^2\\ \in a\mathbb{Z}+b\mathbb{Z} &\\ \text{or } a\wedge b|a \text{ et } a\wedge b|b &\qquad \text{donc } a\wedge b|au+bv\\ &\qquad \text{soit } a\wedge b|d \end{aligned}$$

D'autre part, $a\wedge b$ est le dernier reste non nul de l'algorithme d'Euclide, donc (12.23) :

$$\begin{aligned} a\wedge b &= au+bv \text{ (avec } (u,v)\in\mathbb{Z}^2)\\ &\in a\mathbb{Z}+b\mathbb{Z}\\ &\in d\mathbb{Z} \end{aligned}$$

Donc $d|a\wedge b$.
Ainsi, d et $a\wedge b$ sont positifs et associés, donc égaux.

I.2 Exercices types

Exercice type 1

Exercice 1

Soit $a\geq 2$ et $n\geq 2$. On suppose que a^n-1 premier.

1. Proposer une factorisation non triviale de a^n-1 en produit de deux entiers et montrer que $a=2$.
2. Montrer de même que n est premier.

1. On a :

$$\begin{aligned} a^n-1 &= a^n-1^n\\ &= (a-1)\sum_{k=0}^{n-1} a^k\times 1^{n-k-1}\\ &= (a-1)\sum_{k=0}^{n-1} a^k \end{aligned}$$

Or a^n-1 est premier, donc $a-1=a^n-1$ ou $a-1=\sum_{k=0}^{n-1} a$.
Comme $a\geq 2$ et $n\geq 2$, $a^n-1\neq a-1$.
Donc :

$$\begin{aligned} a^n-1 &= \sum_{k=0}^{n-1} a^k\\ \text{donc } a-1 &= 1\\ \text{soit } a &= 2 \end{aligned}$$

2. On suppose que $n \notin \mathbb{P}$.
   Donc on choisit $(u, v) \in [\![2, n-1]\!]^2$ tel que :

$$n = uv$$

   Ainsi on a :

$$\begin{aligned} 2^n - 1 &= (2^u)^v - (1^u)^v \\ &= \underbrace{(2^u - 1)}_{\geq 2} \underbrace{\sum_{k=0}^{v-1} 2^{uk}}_{\geq 2} \\ &\notin \mathbb{P} \end{aligned}$$

   Donc n est premier.

Exercice type 2

Exercice 2

1. (a) Factoriser $a^{2n+1} + b^{2n+1}$ par $a + b$ pour tout $n \in \mathbb{N}$ et $(a, b) \in \mathbb{C}^2$.
   (b) Pour tout $n \in \mathbb{N}^*$, montrer que si $2^n + 1$ est premier, alors n est une puissance de 2.
   Pour tout $n \in \mathbb{N}$, on pose $F_n = 2^{2^n} + 1$ (n-ème nombre de Fermat).
2. (a) Montrer que pour tout $n \in \mathbb{N}$,

$$F_{n+1} = F_0 \times \cdots \times F_n + 2$$

   (b) En déduire que F_m et F_n sont premiers entre eux pour tout m et n entiers naturels distincts.

1. (a)

$$a^{2n+1} + b^{2n+1} = (a+b) \sum_{k=0}^{2n} (-1)^k a^k b^{2n-k}$$

   (b) Par contraposée. On suppose que n n'est pas une puissance de 2.
   On choisit $(q, p) \in \mathbb{N}^* \times \mathbb{N}$ tel que :

$$n = (2q+1)2^p$$

   On a alors :

$$\begin{aligned} 2^n + 1 &= (2^{2^p})^{2q+1} + 1^{2q+1} \\ &= (2^{2^p} + 1) \sum_{k=0}^{2q} (-1)^k (2^{2p})^k \end{aligned}$$

   Or ces facteurs sont strictement supérieurs à 1, donc $2^n + 1$ n'est pas premier.
2. (a) Soit $n \in \mathbb{N}$

$$P(n) : "F_{n+1} = F_0 \times \ldots \times F_n + 2"$$

   Pour $n = 0$, $F_1 = 2^{2^1} + 1 = 5 = (2^{2^0} + 1) + 2 = F_0 + 2$ donc $P(0)$ est vrai.
   Soit $n \in \mathbb{N}$. On suppose que $P(n)$ est vrai.

$$\begin{aligned} F_{n+2} &= 2^{2^{n+2}} + 1 \\ &= (2^{2^{n+1}})^2 + 1 \\ &= (F_{n+1} - 1)^2 + 1 \\ &= F_{n+1}(F_{n+1} - 2) + 1 + 1 \\ &= F_{n+1} \times \prod_{k=0}^{n} F_k + 2 \text{ (Hypothèse de récurrence)} \\ &= \boxed{\prod_{k=0}^{n+1} F_k + 2} \end{aligned}$$

$P(n+1)$ est vrai, donc d'après le principe de récurrence :

$$\forall n \in \mathbb{N}, P(n)$$

(b)

$$\begin{aligned} F_n \wedge F_m &= F_n \wedge \left(\prod_{m-1}^{k=0} F_k + 2 \right) \\ &= F_n \wedge 2 \text{ (car } n \in [\![0, m-1]\!]) \\ &= 1 \text{ (car } F_n \text{ est impair)} \end{aligned}$$

Donc F_n et F_m sont premiers entre eux.

Exercice type 3

Exercice 3

Soit $p \in \mathbb{P}$.

1. Montrer que
$$\forall y \in [\![1, p-1]\!], \exists! x \in [\![1, p-1]\!], xy \equiv 1[p]$$
2. En déduire le théorème de Wilson :
$$(p-1)! \equiv -1[p]$$
3. On suppose p impair. Montrer que
$$\left(\left(\frac{p-1}{2} \right)! \right)^2 \equiv (-1)^{\frac{p+1}{2}}[p]$$

II Polynômes

II.1 Questions de cours

Démontrer que $\mathbb{A}[X]$ est un anneau.

Théorème 13.7

La somme et le produit définis ci-dessus munissent $\mathbb{A}[X]$ d'une structure d'anneau commutatif.

— $(\mathbb{A}[X], +)$ est un sous-groupe de $(\overbrace{\mathbb{A}^{\mathbb{N}}}^{\text{suites d'éléments de } \mathbb{A}}, +)$ abélien donc est bien un sous-groupe abélien.
— Montrons que $\times$ est associative. Soit $(P, R, Q) \in \mathbb{A}[X]$.
On note $P = (p_k)_{k\in\mathbb{N}}$, $R = (r_k)_{k\in\mathbb{N}}$, $Q = (q_k)_{k\in\mathbb{N}}$.
Soit $n \in \mathbb{N}$.

$$\begin{aligned} (P \times (RQ))_n &= \sum_{k=0}^{n} p_k (RQ)_{n-k} \\ &= \sum_{i+j=n} p_i (RQ)_j \\ &= \sum_{i+j=n} \left(p_i \sum_{k+l=j} r_k q_l \right) \\ &= \sum_{i+k+l=n} p_i r_k q_l \\ &= ((PR) \times Q)_n \end{aligned}$$

— Notons $E = (1, 0, \ldots) = (\delta_{0n})_{n\in\mathbb{N}}$.

On a pour tout $n \in \mathbb{N}$:

$$\begin{aligned}(E \times P)_n &= \sum_{i+j=n} E_i \times P_j \\ &= \sum_{i+j=n} \delta_{0i} \times P_j \\ &= P_n \ (i=0,\ j=n) \\ &= (P \times E)_n\end{aligned}$$

Donc E est l'élément neutre de $\mathbb{A}[X]$.

—

$$\begin{aligned}[P \times (R+Q)]_n &= \sum_{i+j=n} p_i (R+q)_j \\ &= \sum_{i+j=n} p_i (r_j + a_j) \\ &= \sum_{i+j=n} p_i r_j + \sum_{i+j=n} p_i q_j \\ &= (PR)_n + (PQ)_n \\ &= [PR + PQ]_n\end{aligned}$$

Donc $\times$ est distributive sur $+$.

— Comme $\mathbb{A}$ est commutatif :

$$\sum_{i+j=n} p_i q_j = \sum_{i+j=n} q_j p_i$$

Donc $\times$ est commutatif.

Enoncer et démontrer la formule de la dérivée d'un produit de deux polynômes. Enoncer la formule de Leibniz.

Propostion 13.26

— Soit P et Q deux polynômes à coefficients dans $\mathbb{A}$. Alors

$$(PQ)' = P'Q + Q'P.$$

— Soit $P_1, \dots, P_n$ des polynômes à coefficients dans $\mathbb{A}$, alors

$$(P_1 \dots P_n)' = \sum_{i=1}^{n} P_1 \dots P_{i-1} P_i' P_{i+1} \dots P_n.$$

— **Formule de Leibniz** : Soit P et Q deux polynômes à coefficients dans $\mathbb{A}$ et $n \in \mathbb{N}$. Alors

$$(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}.$$

— Soit $P = \sum_{k\geq 0} a_k X^k, P' = \sum_{k\geq 1} k a_k X^{k-1}$ et $Q = \sum_{k\geq 0} b_k X^k, Q' = \sum_{k\geq 1} k b_k X^{k-1}$.

On a :

$$PQ = \sum_{k\geq 0} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) X^n$$

Donc :

$$(PQ)' = \sum_{n\{geq1} \left[n \sum_{k=0}^{n} a_k b_{n-k} \right] X^{n-1}$$

$$\text{et } P'Q = \sum_{n\geq 0} \left[\sum_{k=0}^{n} (k+1) a_{k+1} b_{n-k} \right] X^n$$

$$\text{et } PQ' = \sum_{n\geq 0} \left[\sum_{k=0}^{n} a_k (n-k+1) b_{n-k+1} \right] X^n$$

$$\begin{aligned}
\text{donc } P'Q + Q'P &= \sum_{n\geq 0} \left[\sum_{k=0}^{n} (k+1) a_{k+1} b_{n-k} \right] X^n + \sum_{n\geq 0} \left[\sum_{k=0}^{n} (n-k+1) a_k b_{n-k+1} \right] X^n \\
&= \sum_{n\geq 0} \left[\sum_{k=1}^{n+1} k a_k b_{n-k+1} \right] X^n + \sum_{n\geq 0} \left[\sum_{k=0}^{n} (n-k+1) a_k b_{n-k+1} \right] X^n \\
&= \sum_{n\geq 0} \left[(n+1) a_{n+1} b_0 + \sum_{k=1}^{n} (n+1) a_k b_{n-k+1} + (n+1) a_0 b_{n+1} \right] X^n \\
&= \sum_{n\geq 0} \left[(n+1) \sum_{k=0}^{n+1} a_k b_{n-k+1} \right] X^n
\end{aligned}$$

— Récurrence immédiate.

Enoncer la formule de la dérivée d'une composition de polynômes.

Propostion 13.28

Soit P et Q dans $\mathbb{A}[X]$, alors

$$(Q \circ P)' = P' \times (Q' \circ P)$$

Soit $Q = \sum_{k\geq 0} a_k X^k$.
Ainsi $Q \circ P = \sum_{k\geq 0} a_k p^k$.
Donc :

$$\begin{aligned}
(Q \circ P)' &= \sum_{k\geq 0} a_k (p_k)' \quad (13.24) \\
&= \sum_{k\geq 1} k a_k p' p^{k-1} \quad (13.27) \\
&= P' \times \sum_{k\geq 1} k a_k p^{k-1} \\
&= P' \times Q' \circ P
\end{aligned}$$

II.2 Exercices types

Exercice type 1

Exercice 1

Simplifier $\sum_{k=0}^{r} \binom{a}{k} \binom{b}{r-k}$ pour tout $a, b, r \in \mathbb{N}$.

Soit $(a, b) \in \mathbb{N}^2$.

$$(1+X)^a (1+X)^b = (1+X)^{a+b}$$

$$\text{donc } \left(\sum_{k=0}^{a} \binom{a}{k} X^k \right) \left(\sum_{k=0}^{b} \binom{b}{k} X^k \right) = \sum_{k=0}^{a+b} \binom{a+b}{k} X^k$$

Soit $r \in \mathbb{N}$. On identifie les coefficients en X^r, et on obtient :

$$\sum_{k=0}^{r} \binom{a}{k}\binom{b}{r-k} = \binom{a+b}{n}$$

Exercice type 2

Exercice 3

Résoudre les équations suivantes :

1. $X(X+1)P'' + (X+2)P' - P = 0$, d'inconnue $P \in \mathbb{R}[X]$.
2. $P(2X) = P'(X)P''(X)$ d'inconnue $P \in \mathbb{C}[X]$.

1. Par analyse-synthèse.
   Analyse : On suppose que $\deg P \geq 2$
   Soit a_n le coefficient constant. On obtient :

$$(n^2-1)a_n X^n + \ldots = 0$$

   Abusrde.
   Donc $\deg P < 2$.

   Synthèse : Soit $P = aX + b$.

$$\begin{aligned} Psd' &\Leftrightarrow a(X+2) - (aX+b) = 0 \\ &\Leftrightarrow 2a - b = 0 \\ &\text{donc } \mathcal{S} = R(X+2) \end{aligned}$$

2. Par analyse-synthèse.
   Analyse : On suppose P solution de $P(2X) = P'(X)P''(X)$.
   $\mathbb{C}$ est intègre est de caractéristique nulle donc :

$$\begin{aligned} &\deg P(2X) = \deg P'(X) + \deg P''(X) \\ \text{donc } &\deg P \leq 3 \end{aligned}$$

   Synthèse : Soit $(a,b,c,d) \in \mathbb{C}^4$ et $P = aX^3 + bX^2 + cX + d$.

$$\begin{aligned} P(2X) = P'(X)P''(X) &\Leftrightarrow 8aX^3 + 4bX^2 + 2cX + d = (3aX^2 + 2bX + c)(6aX + 2b) \\ &\Leftrightarrow 8aX^3 + 4bX^2 + 2cX + d = 18a^2X^3 + 18abX^2 + (4b^2 + 6ac)X + 2bc \\ &\Leftrightarrow \begin{cases} 8a = 18a^2 \\ 4b = 18ab \\ 2c = 4b^2 + 6ac \\ d = 2bc \end{cases} \\ &\Leftrightarrow \begin{cases} a = \frac{4}{9} \\ b = 0 \\ c = 0 d = 0 \end{cases} \quad \text{ou} \quad \begin{cases} a = 0 \\ b = 0 \\ c = 0 \\ d = 0 \end{cases} \\ &\Leftrightarrow \mathcal{S} = \left\{0, \frac{4}{9}X^3\right\} \end{aligned}$$