Corrigé du T.D. A

Arithmétique, polynômes & structures

11 octobre 2024

Exercice 1. Montrer que, pour tout entier p premier supérieur ou égal à 5 :

$$24 \mid (p^2 - 1).$$

Soit un entier p premier supérieur ou égal à 5.

D'une part $p-1$ et $p+1$ sont des entiers pairs et l'un des deux est un multiple de 4. Par suite $p^2-1=(p-1)(p+1)$ est un multiple de 8.

D'autre part $p-1$ ou $p+1$ est un multiple de 3 car p ne l'est pas. Par suite $p^2-1=(p-1)(p+1)$ est un multiple de 3.

Or 3 et 8 sont premiers entre eux, donc p^2-1 est un multiple de $3\times 8=24$.

Exercice 2. Soient (a,b) dans $\mathbb{Z}^2$ et n dans $\mathbb{N}^*$ tel que que $\text{pgcd}(a,b)=1$. Montrer que :

1. $\text{pgcd}(a+b,a-b)\in\{1;2\}$;
2. $\text{pgcd}(a^2+b^2,a+b)\in\{1;2\}$.

1. D'après le lemme de Bézout, il existe $(u,v)\in\mathbb{Z}^2$ tel que $ua+vb=1$.
   Soit d un diviseur commun à $a+b$ et $a-b$. Alors d divise $2a$ et $2b$. D'où d divise aussi $u2a+v2b=2$.
   Donc $\text{pgcd}(a+b,a-b)\in\{1;2\}$.
   Remarque — les 2 cas sont possibles car :
   - si (a,b)=(2,3), alors $\text{pgcd}(5,-1)=1$;
   - si (a,b)=(3,5), alors $\text{pgcd}(8,-2)=2$.
2. a^2 et b^2 sont aussi premiers entre eux, il existe donc $(u,v)\in\mathbb{Z}^2$ tel que $ua^2+vb^2=1$ d'après le lemme de Bézout.
   Soit d un diviseur commun à a^2+b^2 et $a+b$. Alors d divise $2a^2=(a^2+b^2)+(a+b)(a-b)$ et $2b^2=(a^2+b^2)-(a+b)(a-b)$.
   D'où d divise aussi $u2a^2+v2b^2=2$.
   Donc $\text{pgcd}(a^2+b^2,a+b)\in\{1;2\}$.
   Remarque — les 2 cas sont possibles car :
   - si (a,b)=(2,3), alors $\text{pgcd}(13,-1)=1$;
   - si (a,b)=(3,5), alors $\text{pgcd}(34,-2)=2$.

Exercice 3. Soit A un anneau commutatif non réduit à $\{0_A\}$, soit $x\in A$. On dit que x est *nilpotent* si

$$\exists n\in\mathbb{N},\ x^n=0_A.$$

Montrer que :

1. si x est nilpotent, alors x n'est pas inversible mais 1_A-x est inversible.
2. l'ensemble des éléments nilpotents de A est un idéal de A.

1. Soient $x \in A$ et $n \in \mathbb{N}$ tels que $x^n = 0_A$.
   Montrons que x n'est pas inversible. Par l'absurde : si x est inversible, alors $\exists y \in A,\ x \times y = y \times x = 1_A$. D'où, en élevant à la puissance n : $x^n \times y^n = 1_A$. Par suite $0_A y^n = 1_A$. C'est absurde car $0_A \neq 1_A$.
   Montrons que $1_A - x$ est inversible. Par un télescope : $(1_A - x) \times (1_A + x + x^2 + \cdots + x^{n-1}) = 1_A - x^n = 1_A$. Donc $1_A - x$ est inversible et son inverse est $1_A + x + x^2 + \cdots + x^{n-1}$.
2. Soit I l'ensemble des éléments nilpotents de A.
   D'une part $(I, +)$ est un sous-groupe de $(A, +)$ car $0_A \in I$ et $\forall (x, y) \in I^2,\ x - y \in I$. En effet, si $x^{n_1} = 0_A$ et $y^{n_2} = 0_A$, alors $(x-y)^{n_1+n_2} = \sum_{k=0}^{n_1+n_2} (-1)^{n_1+n_2-k} \binom{n_1+n_2}{k} x^k \times y^{n_1+n_2-k}$ car la loi $\times$ est commutative par hypothèse. Et chaque terme de cette somme est nul car la puissance k est supérieure ou égale à n_1 ou la puissance $n_1 + n_2 - k$ est supérieure ou égale à n_2.
   D'autre part, si $i \in I$, alors il existe n tel que $i^n = 0_A$. Pour tout $a \in A$, $i \times a \in I$ car $0_A = i^n \times a^n = (i \times a)^n$ car la loi $\times$ est commutative par hypothèse.

Exercice 4. Soit A un anneau commutatif. Si I est un idéal de A, alors on note

$$\sqrt{I} = \{x \in A \mid \exists n \in \mathbb{N}^*, x^n \in I\}.$$

1. Montrer que $\sqrt{I}$ est un idéal de A et que $I \subset \sqrt{I}$.
2. Soient I et J deux idéaux de A. Montrer que :
   (a) $I \cap J$ est un idéal de A ;
   (b) $I \subset J \implies \sqrt{I} \subset \sqrt{J}$;
   (c) $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.
3. Montrer que $\sqrt{\sqrt{I}} = \sqrt{I}$.

---

1. Soit $i \in I$. Alors $i^1 \in I$, d'où $i \in \sqrt{I}$. Donc $I \subset \sqrt{I}$.
   D'une part $(\sqrt{I}, +)$ est un sous-groupe de $(A, +)$. En effet $\sqrt{I}$ n'est pas vide car $0_A \in I \subset \sqrt{I}$. Et $\forall (x, y) \in \sqrt{I}^2,\ x - y \in I$.
   En effet, si $x^{n_1} \in I$ et $y^{n_2} = \in I$, alors $(x-y)^{n_1+n_2} = \sum_{k=0}^{n_1+n_2} (-1)^{n_1+n_2-k} \binom{n_1+n_2}{k} x^k \times y^{n_1+n_2-k}$ car la loi $\times$ est commutative par hypothèse. Et chaque terme de cette somme appartient à I car I est un idéal et la puissance k est supérieure ou égale à n_1 ou la puissance $n_1 + n_2 - k$ est supérieure ou égale à n_2.
   D'autre part, pour tout $(i, a) \in \sqrt{I} \times A$, $i \times a \in \sqrt{I}$ car $\exists n \in \mathbb{N}^*,\ i^n \in I$ et, parce que A est commutatif, $(i \times a)^n = i^n \times a^n \in I$ car $i^n \in I$ et I est un idéal.
   Donc $\sqrt{I}$ est un idéal.
2. (a) Voir la preuve dans le cours.
   (b) Soit $i \in \sqrt{I}$. Il existe alors n tel que $i^n \in I$. Or $I \subset J$, d'où $i^n \in J$, d'où $i \in \sqrt{J}$. Donc $\sqrt{I} \subset \sqrt{J}$.
   (c) On utilise la question précédente pour prouver une inclusion : $I \cap J \subset I$, d'où $\sqrt{I \cap J} \subset \sqrt{I}$. De même, $\sqrt{I \cap J} \subset \sqrt{J}$. Donc $\sqrt{I \cap J} \subset \sqrt{I} \cap \sqrt{J}$.
   Et pour l'autre inclusion : soit $x \in \sqrt{I} \subset \sqrt{J}$. Il existe alors $(n, p) \in \mathbb{N}^* \times \mathbb{N}^*$ tel que $x^n \in I$ et $x^p \in I$. Par suite $x^{n+p} = x^n \times x^p \in I$ car $x^n \in I$ et I est un idéal. Et, de même, $x^{n+p} \in J$. D'où $x^{n+p} \in I \cap J$. Donc $x \in \sqrt{I \cap J}$.
   Par double inclsusion, $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.
3. D'une part, $I \subset \sqrt{I}$ d'après la question 1. D'où $\sqrt{I} \subset \sqrt{\sqrt{I}}$ d'après la question 2b.
   D'autre part, $\sqrt{\sqrt{I}} \subset \sqrt{I}$. En effet : soit $x \in \sqrt{\sqrt{I}}$. Il existe alors n tel que $x^n \in \sqrt{I}$. Et il existe donc p tel que $(x^n)^p \in I$. D'où $x^{np} \in I$. D'où $x \in \sqrt{I}$. Donc $\sqrt{\sqrt{I}} \subset I$.
   Par double inclusion, $\sqrt{\sqrt{I}} = \sqrt{I}$.

Exercice 5. Soit n un entier naturel non nul.

1. Ecrire le cycle $(1, 2, 3, 4)$ comme la composée de transpositions de la forme $(1, i)$, où $i \in [\![1, 4]\!]$. Votre solution est-elle unique ?
2. Soient x et y deux éléments distincts de $[\![1, n]\!]$. Soit la permutation $f = (1, x) \circ (1, y) \circ (1, x)$. Calculer $f(z)$ pour chaque $z \in [\![1, n]\!]$.
3. Montrer que toute permutation de $[\![1, n]\!]$ est la composée de transpositions de la forme $(1, i)$, où $i \in [\![1, n]\!]$.

1. $(1,2,3,4) \overset{(1,2)}{\mapsto} (2,1,3,4) \overset{(1,3)}{\mapsto} (2,3,1,4) \overset{(1,4)}{\mapsto} (2,3,4,1)$
   d'où le cycle $(1,2,3,4)$ est égal à la composée $(1,4)\circ(1,3)\circ(1,2)$.
   Cette solution n'est pas unique car $(1,2)\circ(1,2) = \mathrm{id}$, d'où une autre solution :
   $(1,2)\circ(1,2)\circ(1,2)\circ(1,3)\circ(1,4)$.
2. Si $z \notin \{1,x,y\}$, alors $f(z) = z$.
   Si $x \neq 1$ et $y \neq 1$, alors $f(1) = 1$, $f(x) = y$ et $f(y) = x$, d'où $f = (x,y)$.
   Si $x = 1$, alors $f = (1,y)$.
   Si $y = 1$, alors $f = \mathrm{id}$.
3. Toute permutation est une composée de transpositions (x,y). Or toute transposition (x,y) est, d'après la question précédente, une composée de transpositions de la forme $(1,i)$. Donc toute permutation est une composée de transpositions $(1,i)$.

Exercice 6. Soit $n \geq 2$ et le cycle $c = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \end{pmatrix}$. Déterminer toutes les permutations σ de S_n telles que $\sigma \circ c = c \circ \sigma$.

Pour chaque $k \in \mathbb{N}$, la permutation c^k est une solution de l'équation $\sigma \circ c = c \circ \sigma$. Réciproquement, montrons que toute solution σ est de la forme c^k.

Si σ est une solution de $\sigma \circ c = c \circ \sigma$, alors (par récurrence), $\sigma \circ c^i = c^i \circ \sigma$ pour tout $i \in \mathbb{N}$. Le cycle $c = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \end{pmatrix}$ s'écrit aussi $\begin{pmatrix} c^0(1) & c^1(1) & \dots & c^{n-2}(1) & c^{n-1}(1) \end{pmatrix}$. D'où $\exists k \in [\![0, n-1]\!]$, $\sigma(1) = c^k(1)$. Par suite, pour tout $i \in [\![1,n]\!]$, $\sigma(i) = \sigma \circ c^{i-1}(1) = c^{i-1} \circ \sigma(1) = c^{i-1} \circ c^k(1) = c^k \circ c^{i-1}(1) = c^k(i)$. Donc $\sigma = c^k$.

Exercice 7. Pour chaque $n \in \mathbb{N}^*$, écrire le polynôme :

$$P_n = 1 - X + \frac{X(X-1)}{2} - \frac{X(X-1)(X-2)}{3!} + \ldots + (-1)^n \frac{X(X-1)\ldots(X-n+1)}{n!}$$

sous la forme d'un produit de n facteurs du premier degré.

On note $Q_n = (-1)^n \frac{X(X-1)\ldots(X-n+1)}{n!}$. On remarque que pour tout $k \in [\![1, n-1]\!]$ $Q(k) = 0$. Nous allons montrer par récurrence sur n que, pour tout $n \in \mathbb{N}$, l'ensemble des racines de P_n est $\{1,\ldots,n\}$:

Initialisation : $P_1 = 1 - X$. Donc l'ensemble des racines de P_1 est bien $\{1\}$.

Hérédité : Supposons que l'ensemble des racines de P_{n-1} est $\{1,\ldots,n-1\}$. D'après la remarque que nous avons fait au début l'ensemble des racines de $P_n = P_{n-1} + Q_n$ contient $\{1,\ldots,n-1\}$. Il reste à montrer que n est une racine.
Or on a :

$$\begin{aligned} P_n(n) &= 1 - n + \tfrac{n(n-1)}{2} + \ldots + (-1)^n \tfrac{n(n-1)\ldots(1)}{n!} \\ &= 1 - \tbinom{n}{1} + \tbinom{n}{2} + \ldots + (-1)^n \tbinom{n}{n} \\ &= \textstyle\sum_{k=0}^{n} \tbinom{n}{k} (-1)^k \\ &= (1-1)^n \\ &= 0. \end{aligned}$$

Donc l'ensemble des racines de P_n contient $\{1,\ldots,n\}$. Or ce polynôme est de degré n. Donc il a au plus n racines. Donc $\{1,\ldots,n\}$ est exactement l'ensemble des des racines de P_n

Donc $P_n = \lambda_n \Pi_{k=1}^n (X-k)$ et le coefficient dominant est $\frac{(-1)^n}{n!} = \lambda_n$. Donc

$$P_n = \frac{(-1)^n}{n!} \Pi_{k=1}^n (X-k) = \Pi_{k=1}^n \left(1 - \frac{X}{k}\right).$$

Exercice 8. On note $\Gamma = \{0,1\}$, $\Gamma[X]$ l'ensemble des polynômes dont les coefficients appartient à Γ et $\Gamma_n[X]$ l'ensemble des polynômes de $\Gamma[X]$ dont le degré est inférieur ou égal à n.

1. Quel est le cardinal de $\Gamma_n[X]$?
2. Montrer que, pour tout $P \in \Gamma_{2p}[X]$,

$$-2\frac{4^p - 1}{3} \leq P(-2) \leq \frac{4^{p+1} - 1}{3}.$$

3. Soient $P,\ Q \in \Gamma[X]$ tels que $P(-2) = Q(-2)$. Montrer que $P = Q$.
4. Montrer que, pour tout $N \in \mathbb{Z}$, il existe $P \in \Gamma[X]$ tel que $N = P(-2)$.

---

1. Le cardinal de $\Gamma_n[X]$ vaut 2^{n+1} car construire un polynôme de $\Gamma[X]$, c'est choisir ses $n+1$ coefficients de Γ.
2. Pour tout $P \in \Gamma_{2p}[X]$,
$$-2\frac{4^p-1}{3} = \sum_{k=0}^{p-1}(-2)^{2k+1} \leq P(-2) \leq \sum_{k=0}^{p}(-2)^{2k} = \frac{4^{p+1}-1}{3}.$$
3. Soient $P = \sum a_k X^k$ et $Q = \sum b_k X^k$ deux polynômes différents appartenant à $\Gamma[X]$. On note n_0 le plus grand entier tel que le coefficient de degré n_0 de P n'est pas égal au coefficient de degré n_0 de Q. On a donc :
$$\begin{aligned} |P(-2) - Q(-2)| &= \left|\sum_{k=0}^{n_0}(a_k - b_k)(-2)^k\right| \\ &\geq |a_{n_0} - b_{n_0}|2^{n_0} - \sum_{k=0}^{n_0-1}|a_k - b_k|2^k \\ &\geq 2^{n_0} - \sum_{k=0}^{n_0-1}2^k \\ &= 2^{n_0} - (2^{n_0}-1) = 1 \end{aligned}$$
Donc $P(-2)$ ne peut être égal à $Q(-2)$.
4. L'application
$$\begin{array}{ccc} \Gamma_n[X] & \to & \left[\!\left[2\frac{4^p-1}{3}, \frac{4^{p+1}-1}{3}\right]\!\right] \\ P & \mapsto & P(-2) \end{array}$$
est injective, d'après la question précédente. Or il y a $2\frac{4^p-1}{3} + \frac{4^{p+1}-1}{3} + 1 = 2^{2p+1}$ éléments dans $\left[\!\left[2\frac{4^p-1}{3}, \frac{4^{p+1}-1}{3}\right]\!\right]$ et il y a 2^{2p+1} polynômes dans $\Gamma_n[X]$. Cette application est donc aussi surjective. On en conclut que pour tout $N \in \mathbb{Z}$, en prenant p suffisamment grand, il existe un polynôme $P \in \Gamma_{2p}[X]$ tel que $P(-2) = N$.