Université de Strasbourg
MPA Algèbre S1
P. Guillot, bureau 314, `guillot@math.unistra.fr`

3 – Polynômes

Premiers calculs

Exercice 1 (Somme et produit de polynômes et leur degrés)**.** Étant donnés deux polynômes $P, Q \in \mathbb{K}[X]$ exprimer les degrés de $(-10)P$, de $P+Q$ et $P \cdot Q$ en fonction de $deg(P)$ et $deg(Q)$.

Exercice 2. Montrer que, si $\mathbb{K}$ est un corps, alors $\mathbb{K}[X]$ est un anneau intègre.

Exercice 3. Soit $P_n(X) = (1+X)(1+X^2)(1+X^4)(1+X^8)\cdots(1+X^{2^n})$. Calculer les coefficients de P_n. Pouvez-vous le faire sans récurrence ?

Exercice 4. Pour $n \neq 0$, trouver toutes les racines du polynôme $P_n(X) = 1 - X + \frac{X(X-1)}{2!} - \cdots + (-1)^n \frac{X(X-1)\cdots(X-n+1)}{n!}$.
Indication : commencer par regarder $P_n(n)$.

Division euclidienne de polynômes

Exercice 5. Trouvez le quotient et le reste des divisions suivantes : $(2X+5)$ par $(3X+1)$, (X^2-2X) par $(X-2)$, (X^2+6X+9) par $(X+3)$, (X^3-2X+3) par (X^2-1), (X^3-4X^2+2) par (X^2+i), $(X^4-2X^2+17X-10)$ par (X^4-3X^2+1).

Exercice 6. Déterminer p et q dans $\mathbb{R}$ pour que $P = X^3 + pX + q$ soit divisible par $Q = X^2 + 3X - 1$.

Exercice 7. Soit P un polynôme tel que les restes de la division euclidienne de P par $(X-1), (X-2)$ et $(X-3)$ soient $3, 7$ et 13 respectivement. Déterminer le reste de la division euclidienne de P par $(X-1)(X-2)(X-3)$.

Exercice 8. Soit $t \in \mathbb{R}$ un paramètre, $n \in \mathbb{N}$, et $P_n(X) = (\sin(t)X + \cos(t))^n$. Déterminer le reste de la division euclidienne de P par (X^2+1) .

Dérivées de polynômes

Par définition, si

$$P = a_0 + a_1 X + \cdots + a_n X^n \,,$$

sa dérivée est

$$P' = a_1 + 2a_2 X + \cdots + n a_n X^{n-1} \,.$$

Les règles habituelles s'appliquent, notamment $(PQ)' = P'Q + PQ'$, comme vous pouvez le montrer à titre d'exercice (pour les polynômes à coefficients dans $\mathbb{C}$, on ne peut pas le déduire de ce qu'on sait déjà des dérivées, puisque vous n'avez pas vu de théorie de la dérivation sur $\mathbb{C}$).

Exercice 9. Déterminer tous les polynômes P de $\mathbb{R}[X]$, non nuls, tels que $(X^2+1)P''(X) - 6P = 0$ et $P(1) = 2$.

Exercice 10. Soit P un polynôme et $a \in \mathbb{K}$. Montrer que les deux énoncés ci-dessous sont équivalents :

1. $(X-a)^m$ divise P, pour un certain $m \geq 2$.
2. $P(a) = 0$ et $P'(a) = 0$.

Dans ce cas on dit que a est une racine multiple de P. Cette notion et le résultat de l'exercice sont à connaître absolument.

Exercice 11 (Amélioration du résultat de l'exercice précédent)**.** Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $m \geq 1$ un entier. Montrer que les deux énoncés ci-dessous sont équivalents :

1. m est le plus grand entier tel que $(X-a)^m$ divise P.
2. On peut écrire $P = (X-a)^m Q$ avec $Q(a) \neq 0$.

Dans ce cas on dit que a est une racine de multiplicité m de P. Montrer ensuite que, dans ce cas, a est une racine de multiplicité $m-1$ de P'.

Est-il vrai, réciproquement, que si a est une racine de multiplicité $m-1$ de P', alors a est une racine de multiplicité m de P ? *Attention !*

Exercice 12. Soit $n \in \mathbb{N}$, montrer que le polynôme $P_n = 1 + X + \frac{X^2}{2!} + \cdots + \frac{X^n}{n!}$ n'a pas de racine multiple.

Exercice 13. Déterminer $a, b \in \mathbb{Z}$ de façon à ce que le polynôme $aX^{n+1} - bX^n + 1$ soit divisible par $(X-1)^2$.

Factorisations

Exercice 14. Décomposer dans $\mathbb{R}[X]$, sans déterminer ses racines, le polynôme $P = X^4 + 1$, en produit de facteurs irréductibles.

Exercice 15. Dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$, décomposer les polynômes suivants en facteurs irréductibles.

1. $X^3 - 3$.
2. $X^{12} - 1$.
3. $X^9 + X^6 + X^3 + 1$.

Calculs de PGCD

Exercice 16. Calculer $pgcd(1001, 221)$. Idem pour 33055 et 12621.

Exercice 17. Calculer $pgcd(P, Q)$ dans chaque cas : $(P = 2X+2, Q = 3X+4)$; $(P = X^2-3X, Q = X-4)$; $(P = X^2+6X+1, Q = X-3)$; $(P = X^4-3X^2+3; Q = X^3-2)$; $(P = X^5-4X^2+2, Q = X^3+i)$; $(P = X^6-3X^2+7X-11, Q = X^4-3X^2+1)$.

Exercice 18. Soient $P = X^5 + X^4 - 6X^3 - X^2 - X + 6$ et $Q = X^4 + 2X^3 - X - 2$. Déterminer $pgcd(P, Q)$ et en déduire les racines communes de P et Q.

Exercice 19. Soient $n, p \in \mathbb{N}$.

1. Trouver quotient et reste de la division de $(X^n - 1)$ par $X^p - 1$.
2. Trouver une condition nécessaire et suffisante pour que $X^p - 1$ divise $X^n - 1$.
3. Trouver le $pgcd$ de $X^n - 1$ et $X^p - 1$.

Théorème de Bézout

Exercice 20. Soient $P = 2X^4 + X^3 - 2X - 1$ et $Q = 2X^4 - X^3 - 3X^2 + X + 1$. Trouver $U, V \in \mathbb{C}[X]$ tels que $UP + QV = pgcd(P, Q)$. Quelles sont les racines communes de P et de Q ?

Exercice 21. Soit $n \in \mathbb{N}$. Déterminer $pgcd((X-1)^n, X^n - 1)$ en pensant aux racines communes. Pour $n = 3$ trouver $U, V \in \mathbb{C}[X]$ tels que $(X-1)^3V + (X^3-1)U = X - 1$.

Exercice 22.

1. Soient $P, Q \in \mathbb{K}[X]$ et U, V tels $PU + QV = 1$. Montrer qu'alors $pgcd(P, Q) = 1 = pgcd(U, V)$.
2. Soient $P, Q \in \mathbb{K}[X]$ et U, V tels que $PU + QV = pgcd(P, Q)$. Montrer qu'alors $pgcd(U, V) = 1$.

Ces résultats sont-ils valables avec $\mathbb{Z}$ plutôt que $\mathbb{K}[X]$?

Exercice 23. Soient P, Q deux polynômes premiers entre eux. Il existe alors U_0, V_0 tels que $PU_0 + QV_0 = 1$.

1. Determiner tous les couples (U, V) telles que $PU + QV = 1$.
2. Prouver qu'il existe un unique couple (U_0, V_0) tel que $PU_0 + QV_0 = 1$, $deg(U_0) < deg(Q)$ et $deg(V_0) < deg(P)$. (Indication : si U, V est une solution alors poser U_0, V_0 les restes des divisions respectivement de U par Q et de V par P.)

Ces résultats sont-ils valables avec $\mathbb{Z}$ plutôt que $\mathbb{K}[X]$?

Exercice 24. Soit

$$(E) \quad (X+1)^2A + (X-1)^2B = 1.$$

1. Trouver une solution particulière A_0, B_0 de (E) avec $A_0, B_0 \in \mathbb{R}[X]$.
2. En déduire toutes les solutions de (E).
3. Déterminer tous les polynômes P tels que $P - 1$ soit un multiple de $(X+1)^2$ et que $P + 1$ soit un multiple de $(X-1)^2$.

Arithmétique dans $\mathbb{Z}$

Exercice 25. Montrer que $2^n + 1$ et $2^{n+1} + 1$ sont premiers entre eux, pour $n \in \mathbb{N}$.

Exercice 26. Trouver tous les entiers x, y tels que $12x+8y = 1$.

Exercice 27. Soit p un nombre premier, et k un entier tel que $1 \leq k \leq p-1$. Montrer que p divise $\binom{p}{k}$. Quelles sont les conséquences pour la formule du binôme ?

Plus difficile : montrer que

$$\binom{p-1}{k} \equiv (-1)^k \text{ mod } p\,.$$

On pourra calculer de deux manières différentes les coefficients du polynôme $(X-1)^{p-1} \in \mathbb{Z}/p\mathbb{Z}[X]$.

Exercice 28 (Petit théorème de Fermat)**.** Soit p un nombre premier, et soit $t \in (\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$.

1. Montrer qu'il existe un plus petit entier $k \geq 0$ tel que $t^k = \bar{1}$. *On dit que k est l'ordre de t.*
2. Pour $x, y \in (\mathbb{Z}/p\mathbb{Z})^*$ on va noter $x \sim y$ lorsqu'il existe un entier $i \in \mathbb{Z}$ tel que $y = xt^i$. Montrer que $\sim$ est une relation d'équivalence.
3. Calculer la taille des classes d'équivalence.
4. En déduire que $t^{p-1} = \bar{1}$. Puis, montrer que pour tout $s \in \mathbb{Z}/p\mathbb{Z}$ on a $s^p = s$.
5. Reformuler ceci sous forme de congruences.

Exercice 29. Quel est le reste de la division euclidienne de 2^{49} par 7 ? de 28^{1000} par 13 ?
