Quelques résultats sur les polynômes à coefficients entiers

Merci d'indiquer sur la première page de votre copie le temps passé sur le devoir.

Le but de ce devoir est de donner quelques résultats dans « l'adhérence du programme » sur les polynômes à coefficients entiers, nécessaires pour toute étude sérieuse du sujet.

Les notations suivantes sont valables dans tout le devoir :

- Étant donné deux entiers $m \in \mathbb{N}^*$ et $k \in \mathbb{Z}$, on notera $[k]_m$ la classe de k dans $\mathbb{Z}/m\mathbb{Z}$.
- Étant donné un nombre premier p, on notera $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$.
- Étant donné un anneau commutatif A (en pratique $A = \mathbb{Z}$ ou $A = \mathbb{Z}/m\mathbb{Z}$), on utilisera la notation A[X] pour les polynômes à coefficients dans A.
  On pourra utiliser sans démonstration que A[X] est un anneau commutatif et que la réduction modulo m, coefficient par coefficient, fournit un morphisme d'anneaux $\mathbb{Z}[X] \to (\mathbb{Z}/m\mathbb{Z})[X]$.

A. Généralités sur les polynômes cyclotomiques

Soit $n \in \mathbb{N}^*$.
On notera $\zeta_n = \exp\left(i\frac{2\pi}{n}\right)$, de telle sorte que $\mathbb{U}_n = \{\zeta_n^k \,|\, k \in \mathbb{Z}\}$.

1. Soit $\omega \in \mathbb{U}_n$. Montrer que les assertions suivantes sont équivalentes :
   (i) Pour tout $d \in [\![1, n-1]\!]$, $\omega \notin \mathbb{U}_d$.
   (ii) Pour tout $d \in [\![1, n-1]\!]$ divisant n, $\omega \notin \mathbb{U}_d$.
   (iii) Il existe $k \in [\![0, n-1]\!]$ premier avec n tel que $\omega = \zeta_n^k$.
   Quand ces assertions sont vraies, on dit que ω est une *racine primitive n-ième de l'unité*. L'ensemble des racines primitives n-ièmes de l'unité sera noté $\widehat{\mathbb{U}}_n$.

On définit maintenant le *n-ième polynôme cyclotomique* $\Phi_n = \prod_{\omega \in \widehat{\mathbb{U}}_n} (X - \omega)$.

2. Déterminer Φ_p, pour tout nombre premier p, les polynômes Φ_n pour $n \in [\![1, 8]\!]$ et Φ_{12}.
3. Montrer $X^n - 1 = \prod_{d|n} \Phi_d$, où le produit porte sur les diviseurs positifs de n.
4. Soit p un nombre premier et $k \in \mathbb{N}^*$. Montrer $\Phi_{p^k} = \Phi_p(X^{p^{k-1}})$.
5. Calculer $\Phi_n(1)$. *(Une fois une conjecture raisonnable identifiée, on pourra raisonner par récurrence.)*

B. Contenu et lemme de Gauss (1801)

Un polynôme non nul à coefficients entiers sera dit *primitif* si ses coefficients sont premiers entre eux dans leur ensemble. On note $\mathbb{Z}[X]_{\text{prim}}$ l'ensemble des polynômes primitifs.

6. Soit K un corps. Montrer que l'anneau K[X] est intègre.
7. Soit $P \in \mathbb{Q}[X]$ non nul. Montrer qu'il existe un unique couple $(c, \tilde{P}) \in \mathbb{Q}_+^* \times \mathbb{Z}[X]_{\text{prim}}$ tel que $P = c\tilde{P}$.

Ce nombre $c \in \mathbb{Q}_+^*$ sera noté $c(P)$ et appelé le *contenu* du polynôme P.

8. Soit $P \in \mathbb{Q}[X]$ non nul. Montrer que $P \in \mathbb{Z}[X]$ si et seulement si $c(P) \in \mathbb{N}^*$.
9. **Lemme de Gauss, première version.** Montrer que $\mathbb{Z}[X]_{\text{prim}}$ est stable par produit.
(On pourra procéder par l'absurde et appliquer la question 6. à $K = \mathbb{F}_p$, pour un premier p bien choisi.)
10. **Lemme de Gauss, deuxième version.** Soit $P_1, P_2 \in \mathbb{Q}[X]$ non nuls. Montrer que $c(P_1P_2) = c(P_1)c(P_2)$.
11. **Lemme de Gauss, version originale.**[1] Soit $P_1, P_2 \in \mathbb{Q}[X]$ unitaires. Montrer que si le produit P_1P_2 est à coefficients entiers, alors il en va de même de P_1 et P_2.
12. **Descente de la divisibilité.** Soit $A \in \mathbb{Z}[X]_{\text{prim}}$ et $B \in \mathbb{Z}[X]$. On suppose que A divise B *sur* $\mathbb{Q}$, c'est-à-dire $\exists Q \in \mathbb{Q}[X] : B = AQ$. Montrer que A divise B sur $\mathbb{Z}$, c'est-à-dire $\exists Q \in \mathbb{Z}[X] : B = AQ$.
13. Donner un exemple montrant que, dans la question précédente, on ne peut pas omettre l'hypothèse de primitivité de A.
14. Soit $m \in \mathbb{N}^*$. Construire un polynôme $\Pi \in \mathbb{Z}[X]$ tel que $\left\{P \in \mathbb{Z}[X] \,\middle|\, P\left(\frac{1}{m}\right) = 0\right\} = \{\Pi Q \,|\, Q \in \mathbb{Z}[X]\}$.
15. **Application aux polynômes cyclotomiques.** Soit $n \geq 1$. Montrer que Φ_n est un polynôme à coefficients entiers. Quel est son coefficient dominant ? *(On pourra procéder par récurrence.)*
16. Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ un polynôme de degré n. On note $\frac{u_1}{v_1}, \dots, \frac{u_r}{v_r}$ ses racines rationnelles, écrites sous forme irréductible et répétées selon leur multiplicité. Montrer que $v_1 \cdots v_r \mid a_n$ et $u_1 \cdots u_r \mid a_0$.
17. Montrer que le polynôme $X^3 - 2X + 7$ est irréductible dans $\mathbb{Q}[X]$.

C. Irréductibilité de polynômes à coefficients entiers

On « rappelle » que si K est un corps, un polynôme non constant de K[X] est dit *irréductible* s'il est impossible de l'écrire comme un produit de polynômes non constants de K[X].

On fixe par ailleurs un nombre premier p, et on note $\pi : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ le morphisme d'anneaux obtenu par réduction modulo p.

18. **Condition suffisante d'irréductibilité.** Soit $P \in \mathbb{Z}[X]$ unitaire non constant tel que $\pi(P) \in \mathbb{F}_p[X]$ soit irréductible. Montrer que P est irréductible dans $\mathbb{Q}[X]$.
19. **Critère d'Eisenstein.** Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ unitaire de degré $n \geq 1$. On suppose que $v_p(a_0) = 1$ et $\forall k \in [\![1, n-1]\!], v_p(a_k) \geq 1$, où v_p désigne la valuation p-adique.
Montrer que P est irréductible dans $\mathbb{Q}[X]$.
20. Soit $n \in \mathbb{N}^*$. Montrer qu'il existe un polynôme irréductible de degré n dans $\mathbb{Q}[X]$.
21. Soit K un corps et $P \in K[X]$. Montrer que P est irréductible dans K[X] si et seulement si $P(X+1)$ l'est.
22. En déduire que Φ_p est irréductible dans $\mathbb{Q}[X]$.

Remarque. On peut en fait montrer que Φ_n est irréductible pour tout entier $n \geq 1$ (Kronecker, 1854).

1. Pour être tout à fait honnête, la version originale est : *« 42. Si coefficientes* A, B, C … N; $a, b, c \dots n$ *duarum functionum formae* $x^m + Ax^{m-1} + Bx^{m-2} + Cx^{m-3} \dots + N$ *(P)* $x^\mu + ax^{\mu-1} + bx^{\mu-2} + cx^{\mu-3} \dots + n$ *(Q) omnes sunt rationales, neque vero omnes integri, productumque ex (P) et (Q)* $= x^{m+\mu} + \mathfrak{A}x^{m+\mu-1} + \mathfrak{B}x^{m+\mu-2} + etc. + \mathfrak{Z}$ *omnes coefficientes* $\mathfrak{A}, \mathfrak{B} \dots \mathfrak{Z}$ *integri esse nequeunt. »*

D. Cyclicité de $\mathbb{F}_p^\times$

Soit p un nombre premier. Dans cette section, pour tout $m \in \mathbb{N}^*$, on notera $\overline{\Phi}_m = \pi(\Phi_m) \in \mathbb{F}_p[X]$ la réduction modulo p du m-ième polynôme cyclotomique.

On note $\mathbb{F}_p^\times$ le groupe des inversibles de $\mathbb{F}_p$, c'est-à-dire le groupe $(\mathbb{F}_p \setminus \{0\}, \times)$.

23. Soit $x \in \mathbb{F}_p^\times$. Montrer qu'il existe $m = m(x) \in \mathbb{N}^*$ minimal tel que $x^m = 1$, puis que $m(x)$ divise $p-1$.
24. Montrer que le polynôme $X^{p-1} - 1 \in \mathbb{F}_p[X]$ est scindé à racines simples et déterminer ses racines.
25. Montrer que le polynôme $\overline{\Phi}_{p-1} \in \mathbb{F}_p[X]$ possède (au moins) une racine $z \in \mathbb{F}_p$.
26. Soit $d \in \mathbb{N}^*$ un diviseur de $p-1$ *strict*, c'est-à-dire différent de $p-1$.
Montrer que $(X^d - 1)\Phi_{p-1}$ divise $X^{p-1} - 1$ et en déduire $z^d \neq 1$.
27. Montrer $m(z) = p-1$ puis $\mathbb{F}_p^\times = \{z^0, z^1, \dots, z^{p-2}\}$.

E. Lemme de Hensel et congruences modulo p^k

On fixe dans cette dernière section un nombre premier p et un polynôme $P \in \mathbb{Z}[X]$.

28. Soit $a \in \mathbb{Z}$ et $k \in \mathbb{N}^*$.
Montrer que $[a]_p \in \mathbb{F}_p$ est inversible si et seulement si $[a]_{p^k} \in \mathbb{Z}/p^k\mathbb{Z}$ est inversible.
29. Soit $a, h \in \mathbb{Z}$ et $k \in \mathbb{N}^*$. On suppose $h \equiv 0 \pmod{p^k}$. Montrer que $P(a+h) \equiv P(a) + P'(a)\,h \pmod{p^{2k}}$.
30. **Lemme de Hensel.** Soit $a \in \mathbb{Z}$ et $k \in \mathbb{N}^*$. On suppose $P(a) \equiv 0 \pmod{p^k}$ et $P'(a) \not\equiv 0 \pmod{p}$.
Montrer qu'il existe $\tilde{a} \in \mathbb{Z}$ tel que $\tilde{a} \equiv a \pmod{p^k}$, $P(\tilde{a}) \equiv 0 \pmod{p^{2k}}$ et $P'(\tilde{a}) \not\equiv 0 \pmod{p}$.
31. Montrer qu'avec les notations précédentes, $\tilde{a}$ est unique modulo p^{2k} : si $\hat{a}$ vérifie les mêmes propriétés, alors $\tilde{a} \equiv \hat{a} \pmod{p^{2k}}$.
32. En déduire que si $a \in \mathbb{Z}$ vérifie $P(a) \equiv 0 \pmod{p}$ et $P'(a) \not\equiv 0 \pmod{p}$, alors pour tout $k \in \mathbb{N}^*$, il existe un entier $\alpha_k \in \mathbb{Z}$, unique modulo p^k, tel que $P(\alpha_k) \equiv 0 \pmod{p^k}$ et $\alpha_k \equiv a \pmod{p}$.
33. Montrer que pour tout entier $n \in \mathbb{N}$, il existe $x \in \mathbb{Z}$ tel que $2^n \mid x^3 + 7$.

Terminons par un dernier calcul, sans lien direct avec le lemme de Hensel.

34. On suppose p impair. Montrer $\forall k \in \mathbb{N}^*, (1+p)^{p^k} \equiv 1 + p^{k+1} \pmod{p^{k+2}}$.
(On pourra raisonner par récurrence, en faisant attention aux petites valeurs.)

35. Avec un peu de théorie des groupes, les questions 27. et 34. permettront de montrer le résultat suivant.

> **Théorème.** Soit p un nombre premier impair et $k \geq 1$. Alors le groupe multiplicatif $(\mathbb{Z}/p^k\mathbb{Z})^\times$ est *cyclique*, c'est-à-dire que l'on peut trouver $z \in (\mathbb{Z}/p^k\mathbb{Z})^\times$ tel que $(\mathbb{Z}/p^k\mathbb{Z})^\times = \left\{z^n \,\middle|\, n \in \mathbb{Z}\right\}$.

Montrer que la propriété correspondante est fausse pour $(\mathbb{Z}/8\mathbb{Z})^\times$, puis pour $(\mathbb{Z}/2^k\mathbb{Z})^\times$, dès que $k \geq 3$.