Corrigé des exercices ∗ de la colle 8

1 Critère d'Eisenstein

1. On dit qu'un polynôme non nul de $\mathbb{Z}[X]$ est **primitif** si le pgcd de ses coefficients est égal à 1. Montrer que le produit de deux polynômes primitifs l'est encore.
2. Pour $A\in\mathbb{Z}[X]$ non nul, on appelle **contenu** de A, noté $c(A)$, le PGCD de ses coefficients. Montrer le **lemme de Gauß** : si A et B sont deux polynômes non nuls de $\mathbb{Z}[X]$, alors $c(AB)=c(A)c(B)$.
3. Montrer que si $A\in\mathbb{Z}[X]$ est irréductible sur $\mathbb{Z}[X]$, alors il l'est sur $\mathbb{Q}[X]$.
4. Montrer le **critère d'Eisenstein** : si $A=a_nX^n+\cdots+a_1X+a_0\in\mathbb{Z}[X]$ et p premier tel que
   (a) p ne divise pas a_n ;
   (b) p divise $a_0,a_1,\dots,a_{n-1}$;
   (c) p^2 ne divise pas a_0.
   alors A est irréductible dans $\mathbb{Q}[X]$.

Solution de 1 : Critère d'Eisenstein

1. Notons $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$. Par opération sur les entiers modulo p, on a, pour $P,Q\in\mathbb{Z}[X]$, $\overline{PQ}=\overline{P}\times\overline{Q}$.
   Si PQ n'est pas primitif, on a p est un diviseur premier de tous les coefficients de PQ.
   Alors on a $0_{\mathbb{F}_p[X]}=\overline{PQ}=\overline{P}\times\overline{Q}$.
   Mais comme $\mathbb{F}_p$ est un corps, $\mathbb{F}_p[X]$ est intègre et donc $\overline{P}=0_{\mathbb{F}_p[X]}$ ou $\overline{Q}=0_{\mathbb{F}_p[X]}$ et alors p est un diviseur premier de tous les coefficients de P ou bien de tous les coefficients de Q.
   Ainsi, soit P, soit Q n'est pas primitif.
   Par contraposée, le produit de deux polynômes primitifs l'est encore.
2. Soit A et B sont deux polynômes non nuls de $\mathbb{Z}[X]$, alors $c(AB)=c(A)c(B)$.
   Alors $\frac{1}{c(A)}A$ et $\frac{1}{c(B)}B$ sont primitifs, donc, d'après la question précédente, $\frac{1}{c(A)c(B)}AB$ l'est et donc, par définition, $c\left(\frac{1}{c(A)c(B)}AB\right)=1$ et donc, par propriété du PGCD, comme $c(A)c(B)\in\mathbb{N}$,
   $$\boxed{c(A)c(B)}=c(A)c(B)c\left(\frac{1}{c(A)c(B)}AB\right)=c\left(\frac{c(A)c(B)}{c(A)c(B)}AB\right)=\boxed{c(AB).}$$
3. Soit $A\in\mathbb{Z}[X]$ réductible sur $\mathbb{Q}[X]$. On peut alors écrire $A=QR$ avec $Q,R\in\mathbb{Q}[X]$.
   Soit $q,r\in\mathbb{N}$ les ppcm des dénominateurs des coefficients de Q et R respectivement, $Q_1=qQ\in\mathbb{Z}[X]$ et $R_1=rR\in\mathbb{Z}[X]$.
   Alors $qrA=Q_1R_1$ dans $\mathbb{Z}[X]$ donc $qrc(A)=c(qrA)=c(Q_1R_1)=c(Q_1)c(R_1)$ avec la question précédente.
   On a alors $A=\dfrac{Q_1R_1}{qr}=c(A)\dfrac{Q_1R_1}{c(Q_1)c(R_1)}=\underbrace{\left(c(A)\dfrac{Q_1}{c(Q_1)}\right)}_{\in\mathbb{Z}[X]}\underbrace{\dfrac{R_1}{c(R_1)}}_{\in\mathbb{Z}[X]}$.
   Par contraposée, si A est irréductible sur $\mathbb{Z}[X]$, il l'est sur $\mathbb{Q}[X]$.
4. Soit $A=a_nX^n+\cdots+a_1X+a_0\in\mathbb{Z}[X]$ et p premier tel que
   (a) p ne divise pas a_n ;
   (b) p divise $a_0,a_1,\dots,a_{n-1}$;
   (c) p^2 ne divise pas a_0.
   En réduisant modulo p dans $\mathbb{F}_p[X]$, on obtient $\overline{A}=\overline{a}_nX^n$ avec $\overline{a}_n\neq\overline{0}$ dans le corps $\mathbb{F}_p$ puisque $p\nmid a_n$.
   Supposons par l'absurde que A ne soit pas irréductible dans $\mathbb{Z}[X]$. On peut alors l'écrire sous la forme $A=BC$ avec $B,C\in\mathbb{Z}[X]$ non constants. Notons $k=\deg(B)\geqslant1$ et $n-k=\deg(C)\geqslant1$, de sorte que $1\leqslant k\leqslant n-1$.
   On a alors, avec des notations évidentes $a_n=b_kc_{n-k}$, donc $\overline{a_n}=\overline{b_k}\,\overline{c_{n-k}}\neq\overline{0}$. Ainsi $\overline{b}_k\neq\overline{0}$ et $\overline{c}_{n-k}\neq\overline{0}$, ce qui assure que $\deg\overline{B}=\deg B=k$ et $\deg\overline{C}=\deg C=n-k$.
   Or on a $\overline{A}=\overline{B}\,\overline{C}=\overline{a}_nX^n$. Puisque $\mathbb{F}_p$ est un corps, l'anneau $\mathbb{F}_p[X]$ est factoriel et les seuls diviseurs de X^n à une constante multiplicative près sont des monômes. Compte tenu de leurs degrés respectifs, $\overline{B}$ et $\overline{C}$ sont nécessairement de la forme
   $$\overline{B}=\overline{b}_kX^k\quad\text{et}\quad\overline{C}=\overline{c}_{n-k}X^{n-k}.$$
   Comme $k\geqslant1$ et $n-k\geqslant1$, leurs termes constants respectifs $\overline{b}_0$ et $\overline{c}_0$ sont nuls dans $\mathbb{F}_p$, ce qui signifie que p divise b_0 et que p divise c_0, donc p^2 divise a_0, ce qui contredit la troisième hypothèse.
   Le polynôme A est donc irréductible dans $\mathbb{Z}[X]$ et dans $\mathbb{Q}[X]$ d'après la question précédente.

2 Polynômes cyclotomiques

Soit $n \in \mathbb{N}^*$, $\mathbb{U}_n^*$ l'ensemble des racines primitives n^{e} de l'unité, c'est-à-dire engendrant $\mathbb{U}_n$. Pour $d \in \mathbb{N}^*$, on pose $\Phi_d = \prod_{z \in \mathbb{U}_d^*} (X - z)$.

1. Montrer que $X^n - 1 = \prod_{d|n} \Phi_d$. et en déduire que $\sum_{d|n} \varphi(d) = n$.
2. Justifier rapidement que Φ_n est un polynôme à coefficients entiers.
3. En utilisant le critère d'Eisenstein, montrer que pour tout nombre premier p, le polynôme $(X+1)^{p-1} + \cdots + (X+1) + 1$ est irréductible sur $\mathbb{Q}[X]$, et en déduire que Φ_p l'est aussi.

Solution de 2 : Polynômes cyclotomiques

1. $\mathbb{U}_n$ est un groupe à n éléments. Les éléments de ce groupe ont un ordre divisant n et pour tout divisant n, les éléments du groupe $\mathbb{U}_n$ d'ordre d sont exactement ceux de $\mathbb{U}_d^*$. On en déduit que $\mathbb{U}_n$ est la réunion disjointe des $\mathbb{U}_d^*$ pour d parcourant les diviseurs de n. On en déduit $\boxed{X^n - 1 = \prod_{z \in \mathbb{U}_d} (X - z) = \prod_{d|n} \Phi_d.}$

   Le polynôme Φ_n est de degré $\varphi(n)$ car les racines de l'unité d'ordre n sont les $\mathrm{e}^{2\mathrm{i}k\pi/n}$ avec $k \in [\![1, n]\!]$ et $k \wedge n = 1$.

   L'identité précédente donne $\boxed{\sum_{d|n} \varphi(d) = n.}$ en passant celle-ci au degré.

2. Par récurrence forte sur l'entier $n \geqslant 1$.

   La propriété est immédiate quand $n = 1$. Soit $n \geqslant 2$. Supposons la propriété vérifiée jusqu'au rang $n-1$. On a

   $$X^n - 1 = \prod_{d|n, d \neq n} \Phi_d \times \Phi_n$$

   Le polynôme $X^n - 1$ est à coefficients entiers et $\prod_{d|n, d \neq n} \Phi_d$ l'est aussi. De plus, le coefficient dominant de ce dernier vaut 1. On réalisant une division euclidienne, $\boxed{\text{le calcul de } \Phi_n \text{ détermine un polynôme à coefficients entiers.}}$

3. $P = \sum_{i=0}^{p-1} (X+1)^i = \sum_{i=0}^{p-1} \sum_{k=0}^{i} \binom{i}{k} X^k = \sum_{k=0}^{p-1} \left(\sum_{i=k}^{p-1} \binom{i}{k} \right) X^k$.

   Comme, par la formule de Pascal, $\binom{i}{k} = \binom{i+1}{k+1} - \binom{i}{k+1}$, on a, par télescopage,

   $$a_k = \sum_{i=k}^{p-1} \binom{i}{k} = \binom{p}{k+1} - \binom{k}{k+1} = \binom{p}{k+1}$$

   donc

   (a) p ne divise pas $a_{p-1} = 1$;

   (b) p divise $a_0 = \binom{p}{1}$, $a_1 = \binom{p}{2}$, ..., $a_{p-2} = \binom{p}{p-1}$ (comme dans la preuve du petit théorème de Fermat) ;

   (c) p^2 ne divise pas $a_0 = p$.

   Par le critère d'Eisenstein, $\boxed{P \text{ est irréductible sur } \mathbb{Q}[X].}$

   Si Φ_p était réductible sur $\mathbb{Q}[X]$, $P = \Phi_p(X+1)$ le serait aussi, ce qui contredit la question précédente.

   Ainsi, $\boxed{\Phi_p \text{ est irréductible sur } \mathbb{Q}[X].}$