# TD ∗ Polynômes et Fractions Rationnelles

## Solution de 1 : X

Soient $x_1 < \ldots < x_n$ les racines de $P$ de multiplicités $m_1, \ldots, m_n$.

Alors $x_1, \ldots, x_n$ sont racines de $P'$ de multiplicités $m_1-1, \ldots, m_n-1$. De plus, le théorème de Rolle nous fournit $n-1$ autres racines de $P'$ intercalées entre deux racines successives de $P$ : $x_k$ et $x_{k+1}$.

Cela montre classiquement que $P'$ est scindé (on a trouvé autant de racines comptées avec multiplicité que son degré).

1. Si $a=0$, il n'y a rien à faire. Sinon, quitte à diviser par $a$ ce qui ne change pas le caractère scindé, on montre que $P'+\alpha P$ est scindé.
   On a toujours que $x_1 < \ldots < x_n$ sont racines de $P'+\alpha P$ de multiplicités au moins $m_1-1, \ldots, m_n-1$. Pour trouver d'autres racines, c'est plus délicat.
   Une idée est de reconnaître un début de dérivée de produit (comme dans la technique du facteur intégrant de résolution d'équations différentielles.)
   Soit $f : x \mapsto P(x)\mathrm{e}^{\alpha x}$, dérivable, de dérivée $f' : x \mapsto (P'(x)+\alpha P(x))\mathrm{e}^{\alpha x}$.
   On peut appliquer le théorème de Rolle $n-1$ fois, entre deux racines successives de $P$ et en déduire $n-1$ nouvelles racines distinctes de $P'+\alpha P$. Si $\alpha \neq 0$, il en manque une pour en avoir autant comptées avec multiplicité que le degré de $P'+\alpha P$ qui est égal au degré de $P$. Plusieurs arguments possible pour conclure :
   - $P'+\alpha P$ admet nécessairement une dernière racine complexe car est scindé dans $\mathbb{C}$ et si cette dernière n'était pas réelle, son conjugué serait une autres racines différente de toutes les autres ce qui est exclus pour des raisons de degré.
   - $P'+\alpha P$ est alors divisible dans $\mathbb{R}[X]$ par une polynôme de degré $\deg(P'+\alpha P)-1$. Le quotient est un polynôme réel de degré $1$ qui admet une racine réelle, la racine de $P'+\alpha P$ qui nous manquait.
   - On peut appliquer une nouvelle fois le théorème de Rolle ou plutôt une de ses extensions car $f(x) \xrightarrow[x\to+\infty]{} 0$ si $\alpha<0$ et $f(x) \xrightarrow[x\to-\infty]{} 0$ si $\alpha>0$, ce qui permet d'appliquer une dernier théorème de Rolle soit entre $x_n$ et $+\infty$, soit entre $-\infty$ et $x_1$, ce qui fournit une autre racine de $P'+\alpha P$ différente de toutes celles que l'on avait déjà.
2. Pour la deuxième question, question amusante, qu'on aurait pu poser de manière moins déroutante...
   On a
   $$\sum_{k=0}^{d} a_k P^{(k)} = [P(D)](P)$$
   Mais $P = \lambda \prod_{i=1}^{d}(X-\alpha_i)$, les $\alpha_i$ n'étant pas distincts. Donc
   $$[P(D)](P) = \lambda(D-\alpha_q Id)\circ\cdots\circ(D-\alpha_1 Id)(P)$$
   Or la question précédente permet de montrer par récurrence que, pour tout $k \geqslant 1$,
   $$[(D-\alpha_q Id)\circ\cdots\circ(D-\alpha_1 Id)](P)$$
   est scindé...

## Solution de 2 : X-ENS

Le seul polynôme constant solution est le polynôme nul.

Si $P$ n'est pas constant, il est scindé et on peut le supposer unitaire : $P = \prod_{k=1}^{N}(X-z_k)^{m_k}$ où les $z_k$ sont deux à deux distincts.

Alors $P' = nQ\prod_{k=1}^{N}(X-z_k)^{m_k-1}$ où $n = \deg P$. Comme toute racine de $P'$ est racine de $P$ par hypothèse, $Q$ ne peut avoir de racine et est unitaire, donc $Q=1$.

Pour des raisons de degré, on a alors $N=1$ et $P$ de la forme $(X-z)^n$.
Réciproquement, les $\lambda(X-z)^n$ sont bien solutions.

### Solution de 3 : X-ENS

FGN 1 4.18

1. Pour des raisons de degré et d'irréductibilité, $P' \wedge P = 1$ dans $\mathbb{Q}$ donc dans $\mathbb{C}$ car le PGCD ne dépend pas du corps de base (l'algorithme d'Euclide est le même dans tout corps), ce qui justifie qu'il n'y ait pas de diviseur commun à $P$ et $P'$ de la forme $X-z$ où $z \in \mathbb{C}$.
2. Soit $z$ une racine complexe multiple. Supposons, par l'absurde, que $P$ n'a pas de racine rationnelle.
   Comme $P$ n'est pas irréductible d'après la première question, il s'écrit $P = QR$ avec $Q$ et $R$ non constant, et de degré différent de $1$. On peut supposer par exemple que $\deg Q = 2$ et $\deg R = 3$. Comme $P$ n'a pas de racine rationnelle, ce n'est pas le cas non plus pour $Q$ et $R$, qui sont donc irréductibles dans $\mathbb{Q}[X]$.
   Alors $z$ est racine soit de $Q$, soit de $R$, mais pas les deux. En effet, si c'était le cas, $Q \wedge R \neq 1$ dans $\mathbb{C}$ et donc dans $\mathbb{Q}$. Mais comme ils sont irréductibles et comme $Q \wedge R$ divise $Q$ et $R$, on aurait, vu les degré $Q \wedge R$ proportionnel $Q$ et divisant $R$ qui contredit leur irréductibilité.
   C'est donc que $z$ est une racine d'ordre au moins 2 de $Q$ ou de $R$ ce qui contredit la première question.
   On en déduit que $P$ a une racine rationnelle.

### Solution de 4 : X-ENS

FGN 1 4.29

Pour le sens direct, dans le cas où $P$ n'est pas constant : on remarque que la forme $P = A^2 + B^2$ fait penser à un module au carré. L'idée est donc d'écrire $P = C\overline{C}$ où $C \in \mathbb{C}[X]$.

En calculant la limite en $+\infty$, que le cœfficient dominant est strictement positif. Puis, pour une racine $a$ réelle d'ordre $m$, en factorisant $P = (X-a)^m Q$ avec $Q(a) \neq 0$, pour garder un signe constant, on a nécessairement $m$ pair.

On peut donc décomposer $P \in \mathbb{R}[X]$ avec $a_1, \dots, a_p$ ses racines réelles de multiplicités $m_1, \dots, m_p$ et $z_1, \overline{z_1}, \dots, z_q, \overline{z_q}$ ses racines non réelles de multiplicités $n_1, \dots, n_q$,

$$P = \lambda \prod_{j=1}^{p} (X-a_j)^{m_j} \prod_{k=1}^{p} \left[ (X-z_k)^{n_k} (X-\overline{z_k})^{n_k} \right].$$

On pose alors

$$C = \sqrt{\lambda} \prod_{j=1}^{p} (X-a_j)^{\frac{m_j}{2}} \prod_{k=1}^{p} (X-z_k)^{n_k},$$

de telle sorte que $P = C\overline{C}$.

En écrivant $C = A + \mathrm{i}B$ avec $A, B \in \mathbb{R}[X]$, on obtient $P = A^2 + B^2$.

### Solution de 5 : X-ENS – Critère d'Eisenstein et polynômes cyclotomiques

FGN 1 – 4.20 et 4.21

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 cœfficients 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 cœfficients de $P$ ou bien de tous les cœfficients 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 $\dfrac{1}{c(A)}A$ et $\dfrac{1}{c(B)}B$ sont primitifs, donc, d'après la question précédente, $\dfrac{1}{c(A)c(B)}AB$ l'est et donc, par définition, $c\left(\dfrac{1}{c(A)c(B)}AB\right) = 1$ et donc, par propriété du PGCD, comme $c(A)c(B) \in \mathbb{N}$,
   $$c(A)c(B) = c(A)c(B)c\left(\frac{1}{c(A)c(B)}AB\right) = c\left(\frac{c(A)c(B)}{c(A)c(B)}AB\right) = c(AB).$$

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 cœfficients 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 $qr\,c(A) = c(qrA) = c(Q_1R_1) = c(Q_1)c(R_1)$ 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 $a_0, a_1, \ldots, a_{n-1}$ ;
   (c) $p^2$ ne divise pas $a_0$.

   alors, pour montrer que $A$ est irréductible dans $\mathbb{Q}[X]$, il suffit de montrer qu'il l'est sur $\mathbb{Z}[X]$ d'après la question précédente.
   Sinon, on peut écrire $A = BC$ avec $B, C \in \mathbb{Z}[X]$ non constants.
   On écrit $B = b_kX^k + \cdots + b_1X + b_0$ et $C = c_{n-k}X^{n-k} + \cdots + c_1X + c_0$ avec $1 \leqslant k \leqslant n-1$.
   On a alors $a_n = b_kc_{n-k}$ non divisible par $p$ et $a_0 = b_0c_0$ divisible par $p$ mais pas par $p^2$.
   On a alors $p$ qui divise soit $b_0$, soit $c_0$. Supposons par exemple que $p|b_0$ (l'autre cas est symétrique), et donc $p \not| c_0$ (car $p^2 \not| b_0c_0$).
   On a ensuite $p$ qui divise $a_1 = b_1c_0 + b_0c_1$ donc $p|b_1c_0$ et comme $p \not| c_0$, $p|b_1$.
   On montre alors par récurrence finie, comme $p|a_\ell = b_\ell c_0 + \cdots + b_0c_\ell$ que $p|b_\ell$ pour tout $\ell \in [\![0, k]\!]$ ce qui conduit à la contradiction : $p|a_n$.
5. (a) $P = \displaystyle\sum_{i=0}^{p-1}(X+1)^i = \sum_{i=0}^{p-1}\sum_{k=0}^{i}\binom{i}{k}X^k = \sum_{k=0}^{p-1}\left(\sum_{i=k}^{p-1}\binom{i}{k}\right)X^k$.
   Comme, par la formule de Pascal, $\dbinom{i}{k} = \dbinom{i+1}{k+1} - \dbinom{i}{k+1}$, 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
      i. $p$ ne divise pas $a_{p-1} = 1$ ;
      ii. $p$ divise $a_0 = \dbinom{p}{1}$, $a_1 = \dbinom{p}{2}$, ..., $a_{p-2} = \dbinom{p}{p-1}$ (comme dans la preuve du petit théorème de Fermat) ;
      iii. $p^2$ ne divise pas $a_0 = p$.

   Par le critère d'Eisenstein, $P$ est irréductible sur $\mathbb{Q}[X]$.
   (b) Si $\Phi_p$ était réductible sur $\mathbb{Q}[X]$, $P = \Phi_p(X+1)$ le serait aussi, ce qui contredit la question précédente.
   (c) $I$ est un idéal de $\mathbb{Q}[X]$, donc engendré par un polynôme unitaire non constant $Q$. Comme $\Phi_p(\omega) = 0$, $Q|\Phi_p$. Par irréductibilité et comme les polynômes sont unitaires, $Q = \Phi_p$.
   (d) $\mathbb{Q}[\omega] = \{P(\omega),\ P \in \mathbb{Q}[X]\} = \mathrm{Vect}_{\mathbb{Q}}\left(1, \omega, \ldots, \omega^{p-2}\right)$ (car $\Phi_p(\omega) = 0$ donc $\omega^{p-1} \in \mathrm{Vect}\left(1, \ldots, \omega^{p-2}\right)$) est une partie non réduite à $0$ de $\mathbb{C}$ facilement stable par combinaison linéaire et par produit. La seule chose à vérifier est la stabilité par passage à l'inverse.
   Or, si $P(\omega) \neq 0$, $\Phi_p$ ne divise pas $P$ et est irréductible, donc $P \wedge \Phi_p = 1$. On a donc une relation de Bézout $PU + \Phi_pV = 1$ dans $\mathbb{Q}[X]$. On évaluant en $\omega$, on tire $P(\omega)U(\omega) = 1$ donc $\dfrac{1}{P(\omega)} = U(\omega) \in \mathbb{Q}[\omega]$.
   On vérifie enfin que $\left(1, \omega, \ldots, \omega^{p-2}\right)$ est libre par minimalité du degré de $\Phi_p$ en tant que polynôme annulateur de $\omega$, donc $\dim_{\mathbb{Q}} \mathbb{Q}[\omega] = p-1$.