ÉNS Lyon — 2017 - 2018

Préparation à l'agrégation externe — Option C

Polynômes en une variable : Localisation de racines - Méthodes d'interpolation - Factorisation dans $\mathbb{Z}[X]$

Méthodes de localisation de racines

Majoration brutale du module des racines

On dispose de méthodes directes qui permettent de borner le module des racines d'un polynôme à l'aide de ses coefficients. Nous en présentons ici deux : la première est très élémentaire, et la seconde est connue sous le nom de *borne de Mignotte* (ou de *théorème de Landau-Mignotte*).

Exercice 1. — Soit $P(X) = X^n + \sum_{k=0}^{n-1} a_k X^k \in \mathbb{C}[X]$ un polynôme unitaire et $z \in \mathbb{C}$ une racine de P.

1. Prouver tout d'abord que l'on a
$$|z| \leq \max\left(1, \sum_{k=0}^{n-1} |a_k|\right) .$$
2. Démontrer que l'on a plus généralement le résultat suivant.

   Lemme 1. *Soient $0 < c_0 \leq c_1 \leq \ldots \leq c_{n-1}$ des réels tels que $\sum_{i=0}^{n-1} c_i \leq 1$. Posons*
$$M := \max_{0 \leq i \leq n-1} \left(\frac{|a_i|}{c_i}\right)^{\frac{1}{n-i}} .$$
   Alors on a $|z| \leq M$.
3. En déduire que l'on a par exemple la majoration suivante : $|z| \leq 1 + \max_{0 \leq i \leq n-1} |a_i|$.

Théorème de Landau et borne de Mignotte

Si $P(X) = \sum_{k=0}^{n} a_k X^k$ est un élément de $\mathbb{C}[X]$, on rappelle que l'on peut lui associer les quantités suivantes :
$$\|P\|_\infty := \max_{0 \leq k \leq n} |a_k| \ ; \ \|P\|_2 := \sqrt{\sum_{k=0}^{n} |a_k|^2} \ ; \ \|P\|_1 := \sum_{k=0}^{n} |a_k| .$$
En outre, si l'on a $P(X) = a_n \prod_{k=1}^{n} (X - z_k)$, on pose aussi $M(P) := |a_n| \prod_{k=1}^{n} \max(1, |z_k|)$.

Exercice 2. — **Quelques résultats préliminaires** —

1. Vérifier que $\|.\|_\star$ définit une norme sur $\mathbb{C}[X]$ pour $\star \in \{1, 2, \infty\}$.
2. Vérifier que pour tous polynômes $P, Q \in \mathbb{C}[X]$, on a $M(PQ) = M(P)M(Q)$.
3. Montrer que pour tout polynôme $P \in \mathbb{C}[X]$ et tout élément $z \in \mathbb{C}$, on a
$$\|(X - z)P(X)\|_2 = \|(\bar{z}X - 1)P(X)\|_2 .$$

Exercice 3. — Théorème de Landau et borne de Mignotte —

Soit $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{C}[X]$ un polynôme de degré $n \geq 1$.

1. Démontrer le théorème de Landau : $M(P) \leq \|P\|_2$.
   On pourra introduire le polynôme $\tilde{P} = a_n \prod_{i=1}^{k}(\overline{z_i}X - 1)\prod_{i=k+1}^{n}(X - z_i)$ *où* $z_1, \ldots, z_k$ *sont des racines bien choisies de* P.

Soit $Q(X) = \sum_{k=0}^{m} b_k X^k \in \mathbb{C}[X]$ un diviseur de P de degré $m \geq 1$.

2. Montrer que l'on dispose des inégalités suivantes :
$$\|Q\|_\infty \leq \|Q\|_2 \leq \|Q\|_1 \leq 2^m M(Q) \leq \left|\frac{b_m}{a_n}\right| 2^m \|P\|_2 \ .$$
3. En déduire que si P et Q sont tous deux à coefficients entiers avec Q divisant P dans $\mathbb{Z}[X]$, alors
$$\|Q\|_1 \leq 2^{\deg Q}\|P\|_2 \ .$$

Suites de Sturm et localisation de racines réelles

Les suites de Sturm constituent un moyen efficace pour déterminer les zéros réels d'un polynôme à coefficients réels. Bien qu'un peu lente, cette méthode présente l'avantage d'être sûre. De plus, elle est particulièrement intéressante si l'on sait par ailleurs prouver que tous les zéros du polynôme considéré sont réels. Avant cela, nous présentons la méthode de Descartes : elle donne un résultat un peu plus faible puisqu'elle ne fournit qu'une majoration du nombre de racines contenues dans un intervalle donné, mais permet d'introduire les outils utilisés dans la preuve de la méthode de Sturm.

Exercice 4. — Méthode de Descartes — Soit $P(X) \in \mathbb{R}[X]$ un polynôme de degré $n \geq 1$ sans facteur carré. Pour tout réel x, on note $s(x)$ le nombre de changements de signe [1] dans la suite $[P(x), P'(x), \ldots, P^{(n)}(x)]$.

1. Soient $a < b$ deux réels. Montrer que le nombre de racines de P contenues dans l'intervalle $]a, b[$ est majoré par $s_{a,b} := s(a) - s(b)$ et de même parité que $s_{a,b}$.
2. Montrer que si $P(X) = \sum_{k=0}^{n} a_k X^k$, alors le nombre de racines strictement positives de P est majoré par le nombre de changements de signe dans la suite $[a_0, \ldots, a_n]$.

Exercice 5. — Suites de Sturm : partie théorique — On suppose toujours que $P(X) \in \mathbb{R}[X]$ est un polynôme non constant à racines simples. On définit alors les polynômes $P_0, \ldots, P_n$ comme suit :
- on pose $P_0 := P$ et $P_1 := P'$;
- pour tout $i \geq 2$, on note P_i l'opposé du reste de la division euclidienne de P_{i-2} par P_{i-1}. Autrement dit, il existe un polynôme $Q_{i-1} \in \mathbb{R}[X]$ tel que l'on ait $P_{i-2}(X) = Q_{i-1}(X)P_{i-1}(X) - P_i(X)$ avec $P_i(X) = 0$ ou $\deg P_i < \deg P_{i-1}$.

1. Considérons un réel x et un indice $i \geq 1$. Montrer que si $P_i(x) = 0$, alors $P_{i-1}(x)P_{i+1}(x) < 0$.
2. Pour tout réel x, notons $s(x)$ le nombre de changements de signe [1] dans la suite $[P_0(x), \ldots, P_n(x)]$.
   (a) Montrer que la fonction s ne peut changer de valeur qu'en les racines de P.
   (b) Soient $a < b$ deux réels tels que $P(a), P(b) \neq 0$. Montrer que le nombre de racines de P dans l'intervalle $]a, b[$ est égal à $s(a) - s(b)$.
3. Quel est le nombre de racines réelles du polynôme $X^2 + pX + q$?

1. On supprime les éventuels termes nuls de la suite, et on compte le nombre de changements de signe.

4. Quel est le nombre de racines réelles du polynôme $X^4 - X^3 + 2X + 3$?
5. Que se passe-t-il si l'on ne suppose plus que P est à racines simples ?

Exercice 6. — Suites de Sturm : partie pratique — On se place sous les hypothèses et notations de l'Exercice **??**.

1. Supposons tout d'abord que les coefficients de P soient connus de manière exacte (ce qui est par exemple le cas si P est à coefficients rationnels). A l'aide de l'Exercice **??**, construire un algorithme qui renvoie une liste d'intervalles disjoints contenant chacun exactement une racine de P.
2. Supposons maintenant que les coefficients de P ne soient pas connus de manière exacte, mais que l'on puisse en obtenir une approximation avec une précision arbitrairement grande. Pourquoi ne peut-on plus utiliser l'algorithme précédent ?

Méthodes d'interpolation

Nous présentons maintenant quelques constructions de polynômes interpolateurs, que nous retrouverons dans la feuille sur les familles de polynômes orthogonaux. Dans toute cette partie, on fixe un corps k et l'on travaille avec des polynômes à coefficients dans ce corps.

Exercice 7. — Interpolation de fonctions régulières et majoration de l'erreur —
Soit I un intervalle de $\mathbb{R}$ et $f : I \to \mathbb{R}$ une fonction de classe $\mathcal{C}^n$ sur I. Fixons un n-uplet $(x_1, \ldots, x_n)$ de points deux à deux distincts de I et notons $P \in \mathbb{R}[X]$ le polynôme de degré $\leq n-1$ qui interpole f aux points $x_1, \ldots, x_n$. Montrer que l'on dispose, pour tout réel $x \in I$, de la majoration suivante :

$$|f(x) - P(x)| \leq \left(\prod_{k=1}^{n} |x - x_k| \right) \frac{\|f^{(n)}\|_{\infty,I}}{n!} \; .$$

Indication : Pour un $x \in I$ fixé, on pourra considérer la fonction $g(t) = f(t) - P(t) - C(t-x_1)\cdots(t-x_n)$ avec $C \in \mathbb{R}$ bien choisi.

La méthode d'interpolation de Lagrange est bien adaptée lorsque l'on veut construire des polynômes interpolateurs à points d'interpolation $x_1, \ldots, x_n$ **fixés** et à valeurs $y_1, \ldots, y_n$ variables. Cependant, elle n'est pas très efficace lorsque l'on souhaite ajouter un point d'interpolation x_{n+1}, ce qui explique qu'on lui préfère alors d'autres méthodes, telle la méthode de Newton présentée ci-après.

Interpolation de Newton et différences divisées

Exercice 8. — Méthode d'interpolation de Newton —
Soient $x_1, \ldots, x_n$ des éléments de k deux à deux distincts.

1. Montrer que tout polynôme $Q(X) \in k[X]_{\leq n-1}$ peut s'écrire de manière unique sous la forme
$$Q(X) = \sum_{j=1}^{n} a_j \prod_{i=1}^{j-1} (X - x_i). \tag{1}$$
2. Donner un algorithme qui permet d'écrire un polynôme de degré $\leq n-1$ sous la forme (**??**).

On se donne $y_1, \ldots, y_n \in k$.

3. Écrire un algorithme qui permet de construire le polynôme $P \in k[X]_{\leq n-1}$ vérifiant $P(x_i) = y_i$ pour tout $i \in \{1, \ldots, n\}$. Le polynôme ainsi obtenu est appelé *polynôme d'interpolation de Newton.*
4. Quel est le coût de l'algorithme décrit dans la question précédente ?
5. Combien coûte l'ajout d'un point d'interpolation supplémentaire (x_{n+1}, y_{n+1}) dans l'algorithme de la question 3 ?

Exercice 9. — **Lien avec les différences divisées** — Soient $x_0, \dots, x_n$ et $y_0, \dots, y_n$ deux suites d'éléments de k, avec les x_i deux à deux distincts. Pour tout indice $i \in \{0, \dots, n\}$, on pose $[y_i] := y_i$ et, lorsque $i \leq n-1$, on pose $[y_{i+1}, y_i] := \dfrac{[y_{i+1}] - [y_i]}{x_{i+1} - x_i}$. Pour toute paire d'indice $i, j \in \{0, \dots, n\}$ telle que $i + j \leq n$, on définit par récurrence $[y_{i+j}, \dots, y_i]$, appelé *différence divisée d'ordre* j, en posant

$$[y_{i+j}, \dots, y_i] := \frac{[y_{i+j}, \dots, y_{i+1}] - [y_{i+j-1}, \dots, y_i]}{x_{i+j} - x_i} .$$

Lorsqu'il existe une fonction f telle que $f(x_i) = y_i$ pour tout indice $0 \leq i \leq n$, on note $f[x_{i+j}, \dots, x_i]$ la quantité $[y_{i+j}, \dots, y_i]$.

1. Notons $P(X) = a_0 + a_1(X - x_0) + \ldots + a_n \prod_{i=0}^{n-1}(X - x_i)$ le polynôme d'interpolation de Newton associé aux points d'interpolation (x_i, y_i). Montrer que $a_i = [y_i, \dots, y_0]$ pour tout indice $0 \leq i \leq n$.
2. Montrer que la quantité $[y_{i+j}, \dots, y_i]$ ne dépend que des paires (x_ℓ, y_ℓ) avec $\ell \in \{i, \dots, i+j\}$.
3. Montrer que pour toute permutation σ de l'ensemble $\{i, \dots, i+j\}$, on a $[y_{\sigma(i+j)}, \dots, y_{\sigma(i)}] = [y_{i+j}, \dots, y_i]$.
4. Déterminer le coût (en termes d'opérations dans k) du calcul de $[y_{i+j}, \dots, y_i]$.

Exercice 10. — **Lien avec les différences divisées (suite)** — On considère un intervalle I de $\mathbb{R}$ dans lequel on fixe $n+1$ points $x_0, \dots, x_n$ deux à deux distincts et l'on considère une fonction $f : I \to \mathbb{R}$.

1. Supposons que f soit de classe $\mathcal{C}^n$ sur I.
   (a) Montrer qu'il existe un élément $\xi \in I$ tel que $f[x_n, \dots, x_0] = \dfrac{f^{(n)}(\xi)}{n!}$.
   (b) Généraliser ce résultat aux différences divisées d'ordre j arbitraire $f[x_{i+j}, \dots, x_i]$.
2. Supposons maintenant que f soit de classe $\mathcal{C}^{n+1}$ sur I et notons P le polynôme d'interpolation de Newton attaché à f et aux points x_i (i.e. tel que $P(x_i) = f(x_i)$ pour tout indice $i \in \{0, \dots, n\}$). Montrer que pour tout $x \in I$, il existe $\xi \in I$ tel que

$$f(x) - P(x) = \left(\frac{f^{(n+1)}(\xi)}{(n+1)!} \right) \prod_{i=0}^{n} (x - x_i) .$$

Interpolation de Hermite

La méthode d'interpolation de Hermite consiste à déterminer un polynôme interpolateur en fixant son développement de Taylor à l'ordre m_i en x_i pour tout indice i.

Exercice 11. — Fixons un entier $n \geq 1$, des éléments deux à deux distincts $x_1, \dots, x_n$ dans le corps k et des entiers strictement positifs $m_1, \dots, m_n$. Pour tout $j \in \{1, \dots, n\}$ et tout entier $\ell \in \{0, \dots m_j - 1\}$, on se donne un élément $y_{j,l}$ de k. Posons enfin $m := \sum_{j=1}^{n} m_j$ et supposons que k est de caractéristique soit nulle, soit supérieure à $\max_{1 \leq j \leq n} m_j$.

1. Montrer qu'il existe un unique polynôme $P \in k[X]$ de degré strictement inférieur à m et vérifiant $P^{(\ell)}(x_j) = y_{j,\ell}$ pour tous indices $j \in \{1, \dots, n\}$ et $\ell \in \{0, \dots, m_j - 1\}$. Ce résultat reste-t-il valable sans l'hypothèse effectuée sur la caractéristique de k ?
2. Comment interpréter le résultat de la question précédente à l'aide du module $k[X]/\prod_{i=1}^{n}(X - x_i)^{m_i}$?
3. En s'inspirant des algorithmes d'interpolation précédemment vus, écrire un algorithme permettant de calculer le polynôme P de la Question 1. Quel est son coût en termes d'opérations dans k ?

Factorisation des polynômes à coefficients entiers

On commence par décrire une méthode ancienne permettant de factoriser des polynômes à coefficients entiers en ne travaillant que dans $\mathbb{Z}[X]$. On connaît maintenant des méthodes bien plus rapides, mais celle-ci présente l'avantage de pouvoir être effectuée à la main lorsque le degré du polynôme concerné n'est pas trop grand. On s'intéresse ensuite à une seconde méthode de factorisation qui repose sur l'utilisation des corps finis via le lemme de Hensel et l'algorithme de Berlekamp.

Une méthode directe

On considère un polynôme $P \in \mathbb{Z}[X]$ de degré $n \geq 1$ et l'on pose $m := \lfloor \frac{n}{2} \rfloor$.

Exercice 12. — Montrer que P est irréductible s'il n'existe pas de polynôme non trivial de degré $d \leq m$ divisant P.
Remarque : On rappellera ce que signifie "non trivial" dans ce contexte.

Exercice 13. — Soient $a_0, \ldots, a_m$ des entiers deux à deux distincts et soit $Q \in \mathbb{Z}[X]$ un diviseur de P.

i) Montrer que $Q(a_i)$ divise $P(a_i)$ pour tout indice $i \in \{0, \ldots, m\}$.

ii) Montrer que Q est tel que $\deg Q \leq m$, alors Q est entièrement déterminé par la donnée des $Q(a_i)$.

$\rightsquigarrow$ Considérons alors l'algorithme suivant :

- On fixe des entiers deux à deux distincts $a_0, \ldots, a_m$.
- Pour tout $i \in \{0, \ldots m\}$, on calcule $P(a_i)$ puis on le factorise dans $\mathbb{Z}$.
- On pose $\Delta := \{(d_0, \ldots, d_m) \in \mathbb{Z}^{m+1} \mid \forall\ 0 \leq i \leq m,\ d_i \text{ divise } P(a_i)\}$.
- Pour tout $\delta = (d_0, \ldots, d_m) \in \Delta$, on calcule le polynôme $Q_\delta \in \mathbb{Q}[X]$ de degré $\leq m$ qui vérifie $Q_\delta(a_i) = d_i$ pour tout $i \in \{0, \ldots, m\}$. Si Q_δ est à coefficients entiers, on teste s'il divise P ou non.

Exercice 14. —

1. Expliquer pourquoi la méthode d'interpolation de Lagrange est plus appropriée que celle de Newton pour calculer les polynômes Q_δ.
2. Estimer le coût d'un tel calcul en fonction de n, du nombre d'éléments de Δ et d'un majorant M des coefficients de P.

Exercice 15. — Montrer que si P n'est pas irréductible, alors il existe un diviseur non trivial de P dans la famille de polynômes $\{Q_\delta,\ \delta \in \Delta\}$. En déduire que l'algorithme précédent permet d'obtenir les facteurs irréductibles de P. Obtient-on leur multiplicité ?

Exercice 16. — Factoriser dans $\mathbb{Z}[X]$ le polynôme $X^5+3X^4-X^3-8X^2-2X+6$ à l'aide de l'algorithme précédent.

Exercice 17. — Comment adapter cette méthode au cas des polynômes à coefficients dans $\mathbb{Q}$?

Utilisation des corps finis

Exercice 18. — **Lemme de Hensel** — On rappelle l'énoncé du Lemme de Hensel, qui assure l'existence de racines modulo certaines puissances d'un nombre premier bien choisi.

Lemme 2 (Lemme de Hensel)**.** *Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire, soit $n \geq 1$ un entier et soit p un entier premier. Supposons que $x \in \mathbb{Z}$ vérifie $P(x) \equiv 0 \bmod p^n$ et $P'(x) \not\equiv 0 \bmod p$. Alors il existe un entier $x_0 \in \mathbb{Z}$ tel que $P(x_0) \equiv 0 \bmod p^{2n}$ et $x \equiv x_0 \bmod p^n$. En outre, la classe de congruence de x_0 modulo p^{2n} est uniquement définie.*

1. Démontrer le Lemme de Hensel.
2. En déduire que si $x \in \mathbb{Z}$ est une racine modulo p^n de P qui vérifie $P'(x) \not\equiv 0 \bmod p$, alors elle se relève de manière unique en une racine modulo p^m de P pour tout entier $m \geq n$.
3. Démontrer l'énoncé suivant à l'aide du lemme de Hensel. [2]

2. Cet énoncé est parfois appelé lui-même Lemme de Hensel, pourriez-vous expliquer pourquoi ?

Lemme 3. *Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire, soit $N \geq 1$ un entier et soit $x \in \mathbb{Z}$. Soit p un entier premier tel que p divise $P(x)$ mais ne divise pas $P'(x)$. Notons x_0 la classe de x dans $\mathbb{Z}/p^N\mathbb{Z}$ et, pour tout $n \geq 0$, définissons $x_{n+1} \in \mathbb{Z}/p^N\mathbb{Z}$ par la relation de récurrence suivante :*

$$x_{n+1} := x_n - \frac{P(x_n)}{P'(x_n)} \ .$$

Alors la suite $(x_n)_{n\in\mathbb{N}}$ est bien définie, constante à partir d'un certain rang et, pour n assez grand, on a $P(x_n) = 0$.

4. De quel type de résultats peut-être rapproché l'énoncé du Lemme **??** ?

Exercice 19. — Algorithme de Berlekamp —Soit p un entier premier et k un corps fini à $q = p^N$ éléments (on pourra, dans un premier temps, supposer $k = \mathbb{F}_p$). L'algorithme de Berlekamp permet de déterminer, à l'aide d'outils d'algèbre linéaire, tous les facteurs irréductibles d'un polynôme sans facteurs carrés de $k[X]$.

1. Soit $P \in k[X]$ un polynôme quelconque.
   Montrer que l'application $\varphi_P : k[X]/(P) \to k[X]/(P)$ définie par $\varphi_P(Q(X) \bmod P) := Q(X^q) \bmod P$ est un morphisme d'anneaux bien défini qui coïncide avec l'élévation à la puissance q dans $k[X]/(P)$.
   Indication : Penser à utiliser les propriétés universelles.
2. Soit maintenant $P \in k[X]$ un polynôme sans facteur carré et soient $P_1, \ldots P_r \in k[X]$ ses facteurs irréductibles. Notons x l'image de l'indéterminée X dans l'anneau quotient $k[X]/(P)$ et notons $\mathcal{B} = \{1, x, \ldots, x^{\deg P - 1}\}$ la base canonique du k-espace vectoriel $k[X]/(P)$.
   (a) Posons $K_i := k[X]/(P_i)$ pour tout indice $i \in \{1, \ldots r\}$. Rappeler pourquoi l'on dispose d'un isomorphisme de k-algèbres
   $$\psi : k[X]/(P) \xrightarrow{\simeq} \prod_{i=1}^{r} K_i \ .$$
   (b) Démontrer que l'on a $r = \dim_k \ker(\varphi_P - \mathrm{Id})$, puis exprimer cette quantité à l'aide de $\deg P$ et de $\mathrm{rg}(\varphi_P - \mathrm{Id})$.
   (c) Supposons que P ne soit pas irréductible dans $k[X]$.
      i) Justifier l'existence d'un polynôme $Q(X) \in k[X]$ non congru modulo P à un polynôme constant et tel que $Q(X) \bmod p$ appartienne à $\ker(\varphi_P - \mathrm{Id})$.
      ii) Montrer que l'on a alors $P = \prod_{\alpha\in k} \mathrm{pgcd}(P,\ V - \alpha)$.
   (d) Déduire de ce qui précède un algorithme permettant de déterminer le nombre de facteurs irréductibles de P ainsi que ses facteurs irréductibles. Quel est son coût ?

Exercice 20. — Factorisation dans $\mathbb{Z}[X]$ et dans $\mathbb{Q}[X]$: cas séparable —
Considérons l'algorithme suivant : soit $P \in \mathbb{Z}[X]$ un polynôme unitaire de discriminant $\Delta(P)$ non nul.
- On choisit un entier premier p ne divisant pas $\Delta(P)$.
- On détermine un entier $M \geq 2^{\deg P}\|P\|_2$ puis un entier $N \geq 1$ vérifiant $p^N \geq 2M + 1$.
- Par algorithme de Berlekamp, on détermine les facteurs irréductibles unitaires $\pi_1, \ldots, \pi_r \in \mathbb{F}_p[X]$ de $\pi := P \bmod p$.
- Par lemme de Hensel, on détermine des polynômes unitaires $P_1, \ldots, P_r \in \mathbb{Z}/p^N\mathbb{Z}[X]$ admettant respectivement $\pi_1, \ldots, \pi_r$ pour réduction modulo p et tels que la réduction modulo p^N de P soit égale à $\prod_{i=1}^{r} P_i$.
- Pour toute partie stricte et non vide I de $\{1, \ldots, r\}$, on calcule le polynôme $P_I := \prod_{i\in I} P_i$ et l'on choisit un représentant unitaire $Q_I \in \mathbb{Z}[X]$ de P_I vérifiant $\|Q_I\|_\infty \leq \lfloor \frac{p^N}{2} \rfloor$.
- On teste si Q_I divise P dans $\mathbb{Z}[X]$.

- Si oui, alors Q_I est un facteur non trivial de P dans $\mathbb{Z}[X]$; de plus, si aucun Q_J avec J strictement inclus dans I ne divise P, alors Q_I est un facteur irréductible de P et l'on peut se limiter à étudier les polynômes Q_J avec J inclus dans le complémentaire de I pour obtenir les autres facteurs irréductibles de P.
- Si aucun Q_I ne divise P, alors P est un polynôme irréductible.

1. Pourquoi fait-on l'hypothèse $\Delta(P) \neq 0$?
2. Expliquer pourquoi dans ce cas, l'algorithme présenté fonctionne et permet effectivement d'obtenir tous les facteurs irréductibles de P. Quel est son coût ?
3. Démontrer que pour tout polynôme unitaire $P(X) \in \mathbb{Q}[X]$, il existe un entier $n \geq 1$ tel que le polynôme $Q(X) = n^{\deg P} P(\frac{1}{n}X)$ soit à coefficients entiers.
4. En déduire un algorithme de factorisation des polynômes unitaires séparables de $\mathbb{Q}[X]$.

Exercice 21. — Factorisation dans $\mathbb{Z}[X]$ et dans $\mathbb{Q}[X]$: cas des facteurs multiples — Soit k un corps et $P \in k[X]$.

1. Si k est de caractéristique nulle, comment ramener la factorisation de P à celle de polynômes séparables ? Quel est le coût de cette opération ?
2. On suppose à présent que k est un corps fini de caractéristique positive p.
   (a) Donner une condition nécessaire et suffisante pour que P soit de polynôme dérivé nul.
   (b) Supposons que Q soit un facteur irréductible de P de multiplicité $m \geq 1$. Déterminer la multiplicité de Q comme facteur irréductible de $\mathrm{pgcd}(P, P')$.
   (c) En déduire un algorithme de factorisation de P.
3. A l'aide de l'Exercice **??** et de ce qui précède, construire un algorithme qui prend en entrée un polynôme unitaire à coefficients entiers (ou rationnels) et fournit ses facteurs irréductibles avec multiplicité.

Exercice 22. — Comparer les algorithmes de factorisation obtenus ci-avant sur quelques exemples de petit degré : lequel vous semble le plus efficace ? Que se passe-t-il si l'on augmente le degré des polynômes à factoriser ?