Arithmétique des polynômes, PGCD de deux polynômes

N'oubliez pas de sauvegarder vos sessions (format .xws) sur la plate-forme, ainsi que les programmes (format .cxx).
ATTENTION : Il est obligatoire de rendre certains de ces exercices avant la fin du TP.

Manipulations de base

Exercice 0. *Polynômes, opérations, division euclidienne*

1) Pour entrer un polynôme dans Xcas, **l'indéterminée étant par défaut la variable `x` (`x` minuscule)**, il suffit de le rentrer de façon naturelle. Par exemple, le polynôme de $\mathbb{Q}[X]$, $P(X) = \frac{1}{2}X^2 - 3X + \frac{5}{6}$, peut se rentrer par la commande `P :=1/2*x^2-3x+5/6`. (Attention : `P :=1/2x^2-3x+5/6` ne donne pas le résultat attendu. Pourquoi ?)
Il faut parfois ne pas oublier le signe `*` entre les coefficients et les puissances de `x`. D'autre part, vous pouvez choisir une autre inconnue : `X` (comme dans votre cours de mathématiques), `y`, `Y`... Mais, dans ce cas, il faudra souvent **spécifier le nom de l'inconnue** dans l'appel des fonctions. Par exemple, si vous avez rentré `P :=3*X^2+X-2`, son coefficient dominant s'obtient par la commande `lcoeff(P,X)` (cf ci-après, 3)).
Vous pouvez rentrer des polynômes dans $\mathbb{R}[X]$, comme $P_1 = X^3 - 2\sqrt{2}X + 3$, des polynômes dans $\mathbb{Q}[X]$, comme $P_2 = X^3 - \frac{1}{2}X + 3$, des polynômes dans $\mathbb{Z}[X]$, comme $P_3 = X^3 - 2X + 3$, des polynômes dans $\mathbb{Z}/p\mathbb{Z}[X]$ (avec p nombre premier), comme $P_4 = X^3 - 2X + 3 \mod 5$ (en tapant `P4 :=x^3-2x+3 % 5`). Le logiciel Xcas reconnaît s'il a affaire à un polynôme à coefficients réels, rationnels, entiers, ou entiers modulaires.

2) Nous pouvons ensuite effectuer les opérations classiques sur les polynômes d'un même anneau $K[X]$: addition, soustraction, multiplication, et même une division (si l'on travaille avec les fractions rationnelles). Faites des essais. Que se passe-t-il, concernant l'affichage ?
Pour que le résultat soit rendu sous une forme simplifiée, il faut utiliser la fonction `normal(P)`, où P est le polynôme que vous voulez simplifier (cette fonction renvoie une expression développée et simplifiée ; on peut éventuellement l'utiliser plusieurs fois à la suite ; de plus, il existe aussi la fonction `simplifier(P)`). Reprenez tous vos calculs précédents.

3) Nous pouvons récupérer le degré du polynôme P par la fonction `degree(P)`, son coefficient dominant (coefficient du terme de plus haut degré) par `lcoeff(P)`, et la liste de tous ses coefficients par `coeff(P)`.

4) Nous pouvons effectuer une division euclidienne dans $K[X]$, si K est un corps. Les fonctions de Xcas correspondantes sont `quo(P,Q)`, `rem(P,Q)` ou `quorem(P,Q)` pour calculer respectivement le quotient, le reste, le quotient et le reste de la division euclidienne de P par Q non nul.
La division euclidienne existe aussi dans $A[X]$, où A est un anneau commutatif intègre (par exemple $\mathbb{Z}$), si le coefficient dominant de Q est inversible dans A.

5) Le calcul de résultant s'effectue avec la commande `resultant(P,Q,variable)`.

Calculs de PGCD

Exercice 1. *PGCD dans* $\mathbb{Q}[X]$

Reprenez votre programme de calcul du PGCD dans $\mathbb{Z}$ par l'algorithme d'Euclide et adaptez le au calcul du PGCD de deux polynômes de $\mathbb{Q}[X]$. Pour avoir l'unicité du PGCD obtenu, ce dernier doit être un

polynôme unitaire (son coefficient de plus haut degré est égal à 1). La sortie de votre programme doit donc être exactement ce polynôme là.
Comparez avec la fonction gcd(P,Q) de Xcas. Obtenez-vous le même résultat si les polynômes sont dans $\mathbb{Z}[X]$? (essayez avec $P(X) = 18X^3 - 42X^2 + 30X - 6$ et $Q(X) = -12X^2 + 10X - 2$)

Exercice 2. *Dans $\mathbb{Z}[X]$: Contenu, polynôme primitif*

Lorsque nous allons travailler seulement dans $\mathbb{Z}[X]$, nous aurons besoin de calculer le **contenu** d'un polynôme non nul, c'est-à-dire le pgcd de tous ses coefficients. Implémentez la fonction `co(P)` qui renvoie cet entier, lorsque $P \in \mathbb{Z}[X]\backslash\{0\}$. Rappel : Xcas peut faire des calculs directement sur des listes ; par exemple, il peut calculer le PGCD de l'ensemble des termes d'une liste d'entiers `L` par la commande `gcd(L)`.

Un polynôme de $\mathbb{Z}[X]$ sera dit **primitif** si son contenu est égal à 1. On peut associer à tout polynôme P non nul un polynôme primitif : le polynôme $pp(P) = P/co(P)$; implémentez cette fonction `pp(P)`.
Vérifiez sur des exemples les propriétés suivantes : le produit de deux polynômes primitifs est primitif, et pour deux polynômes P et Q, $co(PQ) = co(P)co(Q)$, $pp(PQ) = pp(P)pp(Q)$.

On pourra comparer avec les fonctions déjà implémentées dans Xcas : `content()` pour le contenu et `primpart()`, pour le polynôme primitif associé.

Pour aller plus loin : on pourra intégrer le cas du polynôme nul. Par convention, si $P = 0$, on définira : $co(P) = 0$, et $pp(P) = P = 0$.

Exercice 3. *PGCD dans $\mathbb{Z}[X]$, méthode "simple"*

Une première façon de faire pour implémenter le calcul de PGCD de deux polynômes P et Q de $\mathbb{Z}[X]$ est de calculer leur PGCD dans $\mathbb{Q}[X]$ (cf exercice 1), et de se ramener dans $\mathbb{Z}[X]$.

Pour cela, nous pouvons utiliser les propriétés suivantes :
(i) Si P et Q sont deux polynômes de $\mathbb{Z}[X]$, alors

$$PGCD_{\mathbb{Z}[X]}(P,Q) = PGCD_{\mathbb{Z}}(co(P), co(Q)) \cdot PGCD_{\mathbb{Z}[X]}(pp(P), pp(Q)).$$

(ii) Si S et T sont deux polynômes primitifs de $\mathbb{Z}[X]$, alors

$$PGCD_{\mathbb{Z}[X]}(S,T) = pp(PGCD_{\mathbb{Z}}(lc(S), lc(T)) \cdot PGCD_{\mathbb{Q}[X]}(S,T)),$$

où $lc(P)$ désigne le coefficient dominant du polynôme P.

Utilisez ces deux propriétés, ainsi que les exercices 1 et 2, pour implémenter un algorithme calculant le PGCD dans $\mathbb{Z}[X]$ de deux polynômes de $\mathbb{Z}[X]$.
Vous pourrez comparer votre programme avec la fonction `gcd` de Xcas.

Un exemple : si $P(X) = 18X^3 - 42X^2 + 30X - 6$ et $Q(X) = -12X^2 + 10X - 2$, alors $PGCD_{\mathbb{Z}[X]} = 6X - 2$.

Exercice 4. *PGCD dans $\mathbb{Q}[X]$: taille des coefficients*

Un des problèmes concernant le calcul du PGCD dans $\mathbb{Q}[X]$ est que les coefficients des polynômes apparaissant dans les divisions euclidiennes successives font apparaître souvent de très grands entiers.
Reprenez votre programme de l'exercice 1, et modifiez le pour qu'il affiche les coefficients des polynômes "restes" des différentes divisions euclidiennes effectuées.

Appliquez le sur des exemples : $P1(X) = 824X^5 - 65X^4 - 814X^3 - 741X^2 - 979X - 764$, et $Q1(X) = 216X^4 + 663X^3 + 880X^2 + 617$; ou bien $P2(X) = X^8 + X^6 - 3X^4 + 8X^2 + 2X - 5$ et $Q2(X) = 3X^6 + 5X^4 - 4X^2 - 9X + 21$.
Qu'en pensez-vous ?

Suite aux conclusions de l'exercice 4, nous souhaitons avoir des méthodes permettant de contrôler la taille des coefficients mis en jeu dans l'algorithme d'Euclide. Plusieurs solutions existent, comme le méthode des pseudo-reste primitifs, ou bien le calcul modulaire de PGCD.

Exercice 5. *PGCD modulaire de polynômes de $\mathbb{Z}[X]$*

Pour la suite, afin de rentrer des polynômes à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ (où p est un nombre premier), je vous recommande de faire comme suit pour plus de simplicité et de commodité pour l'enchainement des exercices :
- écrivez vos polynômes comme des polynôme de $\mathbb{Z}[X]$; par exemple `P := x^3+2x^2-7`, `Q :=4x^4-2x^3+x^2+3`.
- réduisez les modulo p, en leur donnant éventuellement un autre nom ; par exemple, `a :=P % 3` ou `a :=P mod 3`, et `b :=Q % 3` ou `b :=Q mod 3`.
- faites alors les calculs, ou opérations, avec ces nouveaux polynômes ; par exemple, `rem(b,a)`.
- attention aux choix de la variable des polynômes : par défaut choisissez `x`, sinon, il faudra spécifier votre variable dans l'appel des fonctions de Xcas.

A. *PGCD dans $\mathbb{Z}/p\mathbb{Z}[X]$*

1) Implémentez l'algorithme d'Euclide pour le calcul du PGCD de deux polynômes de $\mathbb{Z}/p\mathbb{Z}[X]$ (p étant un nombre premier). Pour avoir l'unicité du PGCD obtenu, ce dernier doit être un polynôme unitaire.
On pourra reprendre le programme de l'exercice 1, sinon, on pourra aussi utiliser directement la fonction `gcd` de Xcas.

2) Soit $P = X^8+5X^7+3X^6+5X^4+5X^3+5X^2+2X+2$, et $Q = X^7+4X^6+4X^5+2X^4+X^3+5X^2+X+3$, deux polynômes de $\mathbb{Z}[X]$. On notera P_p et Q_p les polynômes de $\mathbb{Z}/p\mathbb{Z}[X]$ correspondant aux polynômes P et Q réduits modulo p.
Déterminez le PGCD des polynômes P_p et Q_p, pour tous les nombres premiers p inférieurs à 15. Pour quel nombre premier obtient-on un polynôme de plus grand degré ?
A-t-on $PGCD(P_p, Q_p) = PGCD(P, Q) \mod p$? Comment cela s'explique-t-il ?

On rappelle le résultat suivant :
Théorème : Soit P, Q des polynômes non nuls de $\mathbb{Z}[X]$, soit p un nombre premier ne divisant pas les coefficients dominants de P et de Q. Soient P_p et Q_p les réductions de P et Q modulo p. Soit D le PGCD de P et Q dans $\mathbb{Z}[X]$. Alors :
(i) $deg(PGCD(P_p, Q_p)) \geqslant deg(D)$, où deg est le degré d'un polynôme,
(ii) Si p ne divise pas le résultant de P/D et Q/D, alors $PGCD(P_p, Q_p) = D \mod p$.

B. *PGCD modulaire, méthode des petits premiers*

Le principe général est le suivant : nous voulons déterminer le PGCD de deux polynômes primitifs P et Q de $\mathbb{Z}[X]$. Pour cela, nous déterminons les PGCD dans $\mathbb{Z}/p\mathbb{Z}[X]$ des polynômes réduits modulo p (premier) pour quelques valeurs de p, ne divisant pas leurs coefficients dominants. Ensuite, à l'aide du théorème des restes chinois, nous pouvons reconstituer le PGCD de P et Q.

1) Soient $P = X^6 - 4X^5 + 12X^4 - 13X^3 + 8X^2 + 18X - 42$, et $Q = X^5 - 3X^4 + 22X^2 - 52X + 7$.
Déterminez les PGCD des polynômes réduits de P et Q modulo p, notés P_p et Q_p, pour $p = 2, 3, 5, 7$. Quel nombre premier doit être éliminé ? Pourquoi ?
A l'aide de trois de ces valeurs, et de la commande `ichinrem`, déterminez le PGCD de P et Q dans $\mathbb{Z}[X]$. Vérifiez que le polynôme obtenu divise bien P et Q dans $\mathbb{Z}[X]$.

La fonction `ichinrem([`a_1`,`m_1`],...,[`a_r`,`m_n`])`, ou `ichinrem([`a_1`%`m_1`,...,`a_n`%`m_n`])` fournit une solution particulière au système de congruences : $x \equiv a_1 \mod m_1$, ..., $x \equiv a_n \mod m_n$ lorsque les entiers m_1, ..., m_n sont premiers entre eux deux à deux.

2) Soient $P = X^4 + 25X^3 + 145X^2 - 171X - 360$ et $Q = 2X^3 + 27X^2 + 16X - 15$.
Déterminez le PGCD de P et Q par la technique du PGCD modulaire. Vous indiquerez les nombres premiers p utilisés, et les résultats des calculs intermédiaires des PGCD de P_p et Q_p obtenus (cf 1) pour la notation).

3) *Pour aller plus loin :*

Vous pouvez traiter le cas de deux polynômes primitifs tels que leurs coefficients dominants soient de PGCD égal à d non réduit à 1 (cf vos feuilles de TD). Attention alors au coefficient dominant du PGCD des deux polynômes. Après vos choix de nombres premiers p_1,.., p_r, et obtenu un polynôme candidat D par les restes chinois par rapport à ces premiers, il faudra en effet considérer le polynôme $\Delta = pp(dD \ mod \ p_1 \cdots p_r)$.

Ensuite, vous pourriez essayer d'implémenter un programme déterminant le PGCD de deux polynômes quelconque de $\mathbb{Z}[X]$ par la technique modulaire. (Difficile !)

Exercice 6. *PGCD dans $\mathbb{Z}[X]$: méthode des pseudo-restes primitifs*

Si nous voulons calculer le PGCD de deux polynômes de $\mathbb{Z}[X]$ par la méthode d'Euclide, il serait pratique d'obtenir à chaque division euclidienne un quotient et un reste qui soient dans $\mathbb{Z}[X]$. Ce n'est malheureusement pas possible avec la division euclidienne classique, puisque $\mathbb{Z}[X]$ n'est pas euclidien. Par exemple, si $A(X) = X^2 + 2X + 3$, $B(X) = 2X - 1$, alors $A = (\frac{X}{2} + \frac{5}{4})B + \frac{17}{4}$ est la division euclidienne de A et B dans $\mathbb{Q}[X]$, mais elle n'existe pas dans $\mathbb{Z}[X]$.

1) Nous allons alors définir une **"pseudo-division euclidienne"** dans $\mathbb{Z}[X]$. Elle est définie de la façon suivante :
Si $A(X) = a_n X^n + \cdots + a_0$, $B(X) = b_m X^m + \cdots + b_0 \neq 0$, avec a_i et b_i dans $\mathbb{Z}$ et $n \geqslant m$, alors il existe un unique couple $(Q, R) \in \mathbb{Z}[X]^2$ tel que,

$$b_m^{n-m+1} A = QB + R, \quad \text{avec } deg(R) < deg(B).$$

On remarquera que cela peut être généralisé au cas où $n < m$, auquel cas $Q = 0$ et $R = B$.
Pour l'exemple ci-dessus, cela donne : $4(X^2 + 2X + 3) = (2X + 5)(2X - 1) + 17$.

Implémentez dans Xcas, une fonction `pseudorem(A,B)` donnant le reste de la pseudo-division euclidienne de deux polynômes A et B de $\mathbb{Z}[X]$.

2) Il ne reste plus qu'à calculer le PGCD de deux polynômes A et B selon l'algorithme d'Euclide, mais cette fois-ci en utilisant la pseudo-division euclidienne à chaque étape. Mais ce n'est pas aussi simple !
Pour que cela donne bien le résultat attendu, il faut appliquer l'algorithme aux polynômes primitifs associés aux polynômes A et B, et utiliser la formule vue à l'exercice 3

$$PGCD_{\mathbb{Z}[X]}(A, B) = PGCD_{\mathbb{Z}}(co(A), co(B)) \cdot PGCD_{\mathbb{Z}[X]}(pp(A), pp(B)).$$

D'autre part, il faut également, pour chaque pseudo-division euclidienne effectuée dans le calcul de $PGCD_{\mathbb{Z}[X]}(pp(A), pp(B))$ par l'algorithme d'Euclide, prendre le polynôme primitif associé au polynôme reste.
Implémentez cet algorithme.

3) A-t-on résolu le problème de l'apparition de grands coefficients dans les différentes divisions effectuées ? Affichez les différents polynômes "restes" obtenus sur les exemples de l'exercice 4.