Agrégation, septembre 2006

Soit A un anneau commutatif unitaire, on se propose de donner quelques premiers exercices sur la A algèbre $A[X]$ des polynômes à une indéterminée.

Quelques références :

- [Gour] Les maths en tête, Algèbre, X. Gourdon, Ellipse
- [Dema] Cours d'Algèbre, Michel Demazure, Cassini
- [Bri-Mai] Éléments d'algèbre commutative, J. Briançon, Ph. Maisonobe, Ellipse
- [Per] Cours d'algèbre commutative, Daniel Perrin , Ellipse
- [Be-Ma-Pe] Objectif agrégation, V. Beck, J. Malick, A. Peyré, H K
-[Fr-Gi-Ni-1] Exercice de mathématiques , oraux x-ens, algèbre 1

Il faut savoir ce qu'on entends par sructure de A-algèbre de $A[X]$. Le degré d'un polynôme est une définition incourtounable. Par convention, on pose $\deg(0) = -\infty$. L'algorithme de division est l'outil de base de l'étude des polynômes.

Exercice 1 – Si A est intègre, montrer que pour tout $P_1, P_2 \in A[X]$:

$$\deg(P_1P_2) = \deg(P_1) + \deg(P_2) \quad .$$

Montrer : A intégre $\quad \Longleftrightarrow \quad A[X]$ intégre.

Rappelons l'énnoncé du lemme de division :

Lemme 1.1 *(algorithme de division) Soit $P \in A[X]$ un polynôme dont le coefficient du monôme de plus haut degré, noté $ct(P)$, est inversible. Alors, pour tout $V \in A[X]$, il existe un couple unique (Q, R) de $A[X]$ tel que :*

$$V = QP + R \quad \deg(R) < \deg(P) \quad .$$

Exercice 2 – Montrer l'unicité dans l'algorithme de division.
Puis étudier la suite $(Q_i,\ R_i)$ de couples de polynômes définies par :

$$Q_0 = 0 \quad , \quad R_0 = V \, ,$$

pour $i \in \mathbf{N}$, si $\deg(R_i) \geq \deg(P)$:

$$\begin{cases} Q_{i+1} &= Q_i + ct(P)^{-1} ct(R_i)\, X^{\deg(R_i)-\deg(P)} \,, \\ R_{i+1} &= R_i - ct(P)^{-1} ct(R_i)\, X^{\deg(R_i)-\deg(P)} P \,; \end{cases}$$

et pour $i \in \mathbf{N}$, si $\deg(R_i) < \deg(P)$:

$$\begin{cases} Q_{i+1} &= Q_i \,, \\ R_{i+1} &= R_i \,. \end{cases}$$

Étudier cette suite et démontrer le lemme de division.

Exercice 3 – Diviser dans $\mathbf{Q}[X]$ le polynôme $X^3 + 3X + 1$ par $2X + 1$. Pouvait-on prévoir que les coefficients du quotient et du reste sont des fractions rationnelles dont le dénominateur est une puisance de 2 ?

Exercice 4 – On suppose A intègre. Quels sont les éléments inversibles de $A[X]$? Donner un polynôme inversible de degré 1 dans $\mathbf{Z}/4\mathbf{Z}[X]$.

Exercice 5 – Montrer : K est un corps $\iff$ $K[X]$ est principal.
(Dans le sens droite gauche, on pourra étudier pour $a \in K - \{0\}$, l'idéal (X, a) de K[X]).

Soit $P = a_0X^n + a_1X^{n-1} + \cdots + a_n \in A[X]$ où A est un sous-anneau d'un anneau commutatif B. On note $P(b) = a_0b^n + a_1b^{n-1} + \cdots + a_n$ et on dit que b est une racine de P dans B si $P(b) = 0$. On rappelle que l'application $A \to B$, $P \mapsto P(b)$ est alors un morphisme d'anneau ; on note $A[b]$ le sous-anneau de B image de ce morphisme.

Exercice 6 – Soit $P \in A[X]$ et $a \in A$. Montrer a est racine de P si et seulement si P est divisible par $X - a$.
Soit $a_1, \ldots, a_p$ des éléments distincts de A. Montrer que si A est intègre, alors $a_1, \ldots, a_p$ racines de P équivaut à P est divisible par $(X - a_1) \cdots (X - a_p)$.
Monter que si A est intègre, tout polynôme de $A[X]$ a moins de racines dans A que son degré. Donner un contre-exemple à cette assertion si A n'est pas supposé intègre.

Exercice 7 – (fonction polynomiale) Soit $P \in A[X]$. On considère la fonction polynomiale associée à P, c'est à dire l'application :

$$A \to A \quad , \quad a \mapsto P(a) \quad .$$

Montrer que si A est intègre de cardinal infini, la fonction polynomiale associé à un polynôme est nul si et seulement si ce polynôme est nul. Donner un contre-exemple à cette assertion si A n'est pas supposé de cardinal infini.

Exercice 8 – Montrer que tout élément de $Z[i]$ sécrit de façon unique $a+ib$ avec a et $b \in \mathbf{Z}$. Montrer que l'anneau quotient $\mathbf{Z}[X]/(X^2+1)$ est naturellement isomorphe à $Z[i]$.
Montrer que tout élément de $Z[\sqrt{2}]$ sécrit de façon unique $a+b\sqrt{2}$ avec a et $b \in \mathbf{Z}$. Montrer que l'anneau quotient $\mathbf{Z}[X]/(X^2-2)$ est naturellement isomorphe à $Z[\sqrt{2}]$.

Soit $P \in A[X]$. On dit que $a \in A$ est une racine de multiplicité $l \in \mathbf{N}$ de P si $(X-a)^l$ divise P mais pas $(X-a)^{l+1}$. Une racine de multiplicité 1 est appelé racine simple. Si $P = a_0X^n + \cdots + a_n$, on appelle dérivée de P et on note P' le polynôme $P' = na_0X^{n-1} + \cdots + a_1$. Si $P, Q \in A[X]$, on peut vérifier que $(P+Q)' = P' + Q'$ et $(PQ)' = P'Q + PQ'$.

Exercice 9 – Soit $P \in A[X]$ et $a \in A$. Montrer que a est une racine simple de P si et seulement si $P(a) = 0$ et $P'(a) \neq 0$.
Soit K un corps de caractéristique 0, $P \in K[X]$ et $a \in K$. Démontrer la formule de Taylor. Donner un critère portant sur les dérivées succesives de P pour que a soit de multiplicité l.

Exercice 10 – En utilisant que tout polynôme à coefficient dans $\mathbf{C}[X]$ admet une racine (autrement dit que $\mathbf{C}$ est algébriquement clos), déterminer tous les polynômes irréductibles de $\mathbf{C}[X]$. Déterminer ensuite les polynômes irréductibles de $\mathbf{R}[X]$.

Exercice 11 – Montrer que $X^{17} - 2$ est irréductible dans $\mathbf{Q}[X]$ et $\mathbf{Z}[X]$.
Déterminer les polynômes irréductibles de $\mathbf{Z}/2\mathbf{Z}[X]$ de degré inférieur ou égal à 3.

Exercice 12 – (thórême de Liouville, [Fr-Gi-Ni-1] exercice 6 chapitre 5) Trouver deux fractions rationnelles A et B à coefficients dans $\mathbf{Q}$ non constantes telles que $A^2 + B^2 = 1$. En déduire sur le cercle unité de $\mathbf{R}^2$ centré à l'origine des points à coefficients rationnels. Pour $n \geq 3$, montrer qu'ils n'existents pas de fractions rationnelles à coefficients dans $\mathbf{C}$ non constantes telles que $A^n + B^n = 1$. Pour cela on montrera que si $P, Q, R \in \mathbf{C}[T]$ vérifie $P^n + Q^n + R^n = 1$, alors à une constante multiplicative près P, Q, R sont des polynômes égaux. On utilisera que $\mathbf{C}[T]$ est un anneau principal et qu'un anneau principal vérifie la propriété du lemme d'Euclide et du théorème de Gauss.