Anneaux de polynômes et corps de fractions rationnelles

Dans toute cette feuille, A est un anneau commutatif.

1 Corps des fractions

Proposition 1.1. *Si A est un anneau intègre, il existe un unique corps $\mathrm{Frac}(A)$ contenant A tel que pour tout corps K et tout morphisme d'anneaux injectif $f : A \to K$, il existe un unique morphisme d'anneaux $g : \mathrm{Frac}(A) \to K$ tel que $g_{|A} = f$. Ce corps est appelé le **corps des fractions** de A.*

Démonstration. La construction est parfaitement similaire à la construction de $\mathbb{Q}$ à partir de $\mathbb{Z}$: on considère l'ensemble-quotient $A \times (A \setminus \{0\})/\sim$, où $(a, b) \sim (c, d)$ si et seulement si $ad = bc$. On vérifie à la main qu'il s'agit bien d'un corps. En notant $\frac{a}{b}$ la classe de (a, b), il contient un anneau isomorphe à A sous la forme de $\left\{\frac{a}{1} \mid a \in A\right\}$ et la propriété universelle se vérifie via $g : \frac{a}{b} \mapsto \frac{f(a)}{f(b)} \in K$. □

Remarque 1.2. Ainsi, $\mathrm{Frac}(A)$ est le « plus petit » corps contenant A.

Proposition 1.3. *Soit A un anneau factoriel. Alors tout élément de $\mathrm{Frac}(A)$ admet une écriture unique sous la forme $\frac{a}{b}$ avec $a, b \in A, b \neq 0$ et a et b premiers entre eux.*

Démonstration. L'existence se montre en simplifiant numérateur et dénominateur par un PGCD de a et b. L'unicité provient du lemme de Gauss : si $\frac{a}{b} = \frac{c}{d}$ avec a et b premiers entre eux et c et d premiers entre eux, alors $ad = bc$, d'où $a \mid c$ et $b \mid d$. Si on écrit $c = ak$ et $d = bk'$ alors $k = k'$ d'où $a = c$ et $d = b$. □

2 Propriétés générales d'anneaux de polynômes

Définition 2.1. *Soit $P = \sum_{k\in\mathbb{N}} a_k X^k \in A[X]$. Le **degré** de P est $-\infty$ si $P = 0$ et le plus grand entier k tel que $a_k \neq 0$ si $P \neq 0$.*

Proposition 2.2. *Soit $P, Q \in A[X]$. Alors :*

1. $\deg(P + Q) \leq \max(\deg P, \deg Q)$, *avec inégalité stricte si et seulement si* $\deg P = \deg Q$ *et les coefficients dominants de P et Q sont opposés.*
2. $\deg(PQ) \leq \deg P + \deg Q$, *avec inégalité stricte si et seulement si les coefficients dominants de P et Q ont un produit nul. En particulier, si A est intègre, il y a toujours égalité.*

Corollaire 2.3. *Si A est intègre, alors $A[X]^\times = A^\times$.*

Exercice 1. *Trouver un contre-exemple quand A n'est pas intègre.*

Théorème 2.4 (Division euclidienne)**.** *Soit $S, T \in A[X]$ tels que le coefficient dominant de T est inversible. Alors il existe un unique couple $(Q, R) \in A[X]$ vérifiant $S = QT + R$ et $R = 0$ ou $\deg R < \deg T$.*

Exercice 2. *Poser la division euclidienne de $X^5 - 3X^3 - 2X^2 + X + 6$ par $X^3 - X + 1$.*

Proposition 2.5. *L'anneau $A[X]$ est euclidien si et seulement si $A[X]$ est principal si et seulement si A est un corps.*

Démonstration. Si $A[X]$ est euclidien, alors il est principal. Si $A[X]$ est principal, il est intègre et donc A aussi. Il est alors clair que X est un élément irréductible de $A[X]$ pour des raisons de degré, et donc (X) est maximal dans $A[X]$. Ainsi $A[X]/(X) \simeq A$ est un corps. Enfin, si A est un corps, alors le coefficient dominant d'un polynôme non nul est toujours inversible, et donc $A[X]$ est euclidien pour le stathme degré. $\square$

Définition 2.6. *Supposons que A soit un anneau factoriel et soit $P \in A[X]$. Le **contenu** de P, noté $c(P)$, est 0 si $P = 0$ et le PGCD de ses coefficients sinon. On dit que P est **primitif** lorsque $c(P) = 1$.*

Lemme 2.7 (de Gauss)**.** *Supposons que A est factoriel. Alors pour tout $P, Q \in A[X]$, $c(PQ) = c(P)c(Q)$.*

Démonstration. Le résultat est clair si P ou Q est nul, donc supposons $P, Q \neq 0$. Écrivons $P = \sum_{k\in\mathbb{N}} a_k X^k$ et $Q = \sum_{k\in\mathbb{N}} b_k X^k$. Clairement, on a $P = c(P)A$ et $Q = c(Q)B$ avec A et B primitifs, donc il suffit de montrer le résultat quand P et Q sont primitifs. Supposons par l'absurde que PQ n'est pas primitif et soit p irréductible divisant $c(PQ)$. Soit k_1 le plus petit entier k tel que p ne divise pas a_k et k_2 le plus petit entier k tel que p ne divise pas b_k. Alors le coefficient devant $X^{k_1+k_2}$ de PQ est

$$\sum_{i+k=k_1+k_2} a_i b_j = a_{k_1} b_{k_2} + \sum_{\substack{i+j=k_1+k_2 \\ i<k_1 \text{ ou } j<k_2}} a_i b_j.$$

Comme celui-ci est divisible par p tout comme la deuxième somme, p divise $a_{k_1} b_{k_2}$, bien qu'il n'en divise aucun des deux, ce qui est absurde d'après le lemme d'Euclide. Donc PQ est primitif. $\square$

Remarque 2.8. Dans ce qui précède, il suffisait de supposer que A est un anneau à PGCD.

Corollaire 2.9. *Supposons que A est factoriel et soit K son corps des fractions. Alors les irréductibles de $A[X]$ sont les constantes irréductibles dans A et les polynômes non constants primitifs irréductibles dans $K[X]$.*

Démonstration. Pour des raisons de degré, les constantes irréductibles dans A sont irréductibles dans $A[X]$. Si $P \in A[X]$ est non constant, primitif, et irréductible dans $K[X]$, supposons qu'on ait $P = QR$ avec $Q, R \in A[X]$. Comme P est irréductible dans $K[X]$, Q ou R est inversible dans $K[X]$, donc est constant. On a donc (quitte à échanger les rôles), $P = aQ \in A[X]$ pour un $a \in A \setminus \{0\}$. Finalement, on a $c(P) = 1 = ac(Q)$ et donc $a \in A^\times \subset A[X]^\times$.

Réciproquement, soit $P \in A[X]$ irréductible. Si P est constant, alors il est irréductible dans A. Sinon, P est primitif car, dans le cas contraire, son contenu admettrait un facteur irréductible p, qui serait également un facteur irréductible de P dans $A[X]$. Enfin, P est irréductible dans $K[X]$. En effet, si on a $P = QR$ avec $Q, R \in K[X]$, on écrit $Q = \frac{a}{b}\tilde{Q}$ et $R = \frac{c}{d}\tilde{R}$ avec

$a, b, c, d \in A$, a et b premiers entre eux, c et d premiers entre eux et $\tilde{Q}, \tilde{R} \in A[X]$ primitifs. Alors $bdP = ac\tilde{Q}\tilde{R}$ d'où, d'après le lemme de Gauss, $bd = ac$. Ainsi, $P = \frac{ac}{bd}\tilde{Q}\tilde{R} = \tilde{Q}\tilde{R}$, et comme P est irréductible dans $A[X]$, $\tilde{Q} \in A[X]^\times = A^\times \subset K^\times$ ou $\tilde{R} \in A[X]^\times = A^\times \subset K^\times$. □

Notons qu'au passage, on a montré la chose suivante.

Corollaire 2.10. *Soit A un anneau factoriel, K son corps des fractions et $P \in A[X]$ tel que $P = QR$ avec $Q, R \in K[X]$. Alors il existe $\tilde{Q}, \tilde{R} \in A[X]$ de mêmes degrés que Q et R respectivement tels que $P = \tilde{Q}\tilde{R}$.*

Corollaire 2.11. *L'anneau $A[X]$ est factoriel si et seulement si A l'est. En particulier, en notant $A[X_1, \ldots, X_n] = A[X_1][X_2]...[X_n]$, alors $A[X_1, \ldots, X_n]$ est factoriel si et seulement si A l'est.*

3 Racines de polynômes

Définition 3.1. *Soit $a \in A$. Il existe un unique morphisme de A-algèbres $\mathrm{ev}_a : A[X] \to A$ envoyant X sur a, appelé* ***morphisme d'évaluation*** *en a. Si $P \in A[X]$, on note $\mathrm{ev}_a(P) = P(a)$ et on dit que a est* ***racine*** *de P lorsque $P(a) = 0$.*

Proposition 3.2. *Soit $P \in A[X]$. Pour tout $a \in A$, a est racine de P si et seulement si $(X - a) \mid P$ dans $A[X]$.*

Démonstration. La condition $(X - a) \mid P$ implique clairement que $P(a) = 0$.

Réciproquement, supposons que $P(a) = 0$. Comme le coefficient dominant de $X - a$ est 1, inversible dans A, on peut poser la division euclidienne $P = (X - a)Q + R$ avec $\deg R < \deg(X - a) = 1$. Ainsi, R est une constante et en évaluant en a on obtient $R = 0$. □

Remarque 3.3. Ce résultat est le plus souvent énoncé quand A est un corps, mais il reste valable dans n'importe quel anneau commutatif. Face au jury, il ne faut pas oublier de préciser que c'est bien parce que le coefficient dominant de $X - a$ est inversible !

Corollaire 3.4. *Si A est intègre et $P \in A[X] \setminus \{0\}$ alors P admet au plus $\deg P$ racines dans A.*

Exercice 3. *Donner un contre-exemple quand A n'est pas intègre.*

Corollaire 3.5. *Si A est intègre et infini, alors l'application $P \mapsto (x \mapsto P(x))$ de $A[X]$ dans A^A est injective.*

Exercice 4. *Donner un contre-exemple quand A est intègre fini.*

Proposition 3.6 (Polynômes interpolateurs de Lagrange)**.** *Soit K un corps, $x_0, \ldots, x_n, y_0, \ldots, y_n \in K$ avec les x_i deux à deux distincts. Il existe un polynôme $P \in K[X]$ de degré au plus n tel que pour tout $i \in \{1, \ldots, n\}, P(x_i) = y_i$. Si de plus K est de caractéristique nulle, alors ce polynôme est unique.*

Démonstration. L'existence peut se justifier avec un déterminant de Vandermonde, ou en construisant explicitement le polynôme

$$P = \sum_{i=0}^{n} y_i \prod_{\substack{j \neq i \\ 0 \leq j \leq n}} \frac{X - x_j}{x_i - x_j}.$$

L'unicité vient du fait que la différence de deux tels polynômes s'annule en $n + 1$ points. □

Exercice 5. *Soit K un corps fini (il en existe !). Montrer que l'application $P \mapsto (x \mapsto P(x))$ de $K[X]$ dans K^K est surjective.*

Définition 3.7. *Soit $P = \sum_{k=0}^{n} a_k X^k \in A[X]$. Le* ***polynôme dérivé*** *(ou la* ***dérivée****) de P est*

$$P' = \sum_{k=1}^{n} k a_k X^{k-1} = \sum_{k=0}^{n-1} (k+1) a_{k+1} X^k.$$

Pour tout $k \in \mathbb{N}$, on note $P^{(k)}$ la k-ième dérivée de P.

Exercice 6. *Donner une condition nécessaire et suffisante sur P pour que $P' = 0$. Qu'est-ce que cela donne quand A est intègre ?*

Remarque 3.8. Il est clair que (si $P \neq 0$) $\deg P' < \deg P$, et donc si P est de degré $n \in \mathbb{N}$ alors $P^{(n)} = 0$.

Proposition 3.9 (Formule de Taylor)**.** *Soit K un corps de caractéristique 0. Alors pour tout $P \in K[X]$ et $a \in K$, on a*

$$P = \sum_{k \in \mathbb{N}} \frac{(X-a)^k}{k!} P^{(k)}(a).$$

Démonstration.

1. Méthode calculatoire : Poser la division euclidienne de P par $(X-a)^n$ et itérer.
2. Par la dualité : Les applications $P \mapsto P^{(k)}(a)$, pour $0 \leq k \leq n$ forment une base du dual de $K_n[X]$, dont la base antéduale est la famille des $\frac{(X-a)^k}{k!}$.

□

Remarque 3.10. La formule reste valable en caractéristique $p > 0$, du moment que le degré de P est strictement inférieur à p.

Définition 3.11. *Soit $P \in A[X]$ et $a \in A$. On dit que la* ***multiplicité algébrique*** *de a en tant que racine de P est l'entier $k \in \mathbb{N}$ tel que $(X-a)^k \mid P$ et $(X-a)^{k+1} \nmid P$, et la* ***multiplicité analytique*** *de a en tant que racine de P est l'entier $k \in \mathbb{N}$ tel que $P^{(k-1)}(a) = 0$ et $P^{(k)}(a) \neq 0$. On dit que a est une* ***racine simple*** *de P lorsque sa multiplicité algébrique est 1 et que c'est une* ***racine multiple*** *lorsque cette multiplicité est supérieure ou égale à 2.*

Exercice 7. *Comparer ces deux multiplicités.*

Remarque 3.12. ⚠ Si a est une racine multiple de P, alors P et P' ont a comme racine commune et ne sont donc pas premiers entre eux, mais la réciproque est fausse en général car, en caractéristique non nulle, il se peut que $P' = 0$ sans que P ne soit constant.

Proposition 3.13. *Si A est intègre de caractéristique 0 alors la multiplicité algébrique et la multiplicité analytique de n'importe quel $a \in A$ coïncident.*

4 Des critères d'irréductibilité

Proposition 4.1. *Soit $P \in A[X]$. Si P est irréductible dans $A[X]$ et de degré au moins 2 alors P n'a pas de racines dans A. Si A est un corps, P est de degré 2 ou 3 et n'a pas de racine dans A, alors P est irréductible dans $A[X]$.*

Exercice 8. *Donner un polynôme non constant, à coefficients dans un corps, sans racine et non irréductible. Donner un polynôme de degré 2 sans racine et non irréductible.*

Exercice 9. *Montrer que $X^2 - 180$ est irréductible dans $\mathbb{Q}[X]$.*

Corollaire 4.2. *Soit K un corps de caractéristique différente de 2 et $P = aX^2 + bX + c \in K[X]$ de degré 2. Alors P est irréductible dans $K[X]$ si et seulement si son discriminant $b^2 - 4ac$ n'est pas un carré dans K.*

Remarque 4.3. ⚠ En caractéristique 2 il n'y a pas de méthode générale ! Le morphisme de Frobenius peut aider à faire des calculs, mais il n'y a pas d'équivalent du discriminant pour détecter l'absence ou non de racines.

Proposition 4.4. *Soit A un anneau intègre, $P \in A[X]$ unitaire et I un idéal premier de A. Si $\overline{P}$ est irréductible dans $A/I[X]$ alors P est irréductible dans $A[X]$.*

Démonstration. Si P était réductible dans $A[X]$, on aurait $P = QR$ avec $Q, R \in A[X]$ non inversibles et de coefficients dominants inversibles puisque leur produit fait 1. En particulier, $\deg \overline{Q} = \deg Q, \deg \overline{R} = \deg R \geq 1$. Alors dans $A/I[X]$, $\overline{P} = \overline{QR}$ avec $\overline{Q}$ et $\overline{R}$ non inversibles puisque A/I est intègre. □

Remarque 4.5. ⚠ La réciproque est fausse. Par exemple, $X^4 + 1$ est réductible dans tous les corps $\mathbb{Z}/p\mathbb{Z}$ mais est irréductible dans $\mathbb{Z}[X]$, voir la feuille sur les corps finis.

Exercice 10. *Montrer que le polynôme $X^4 + X + 1$ est irréductible dans $\mathbb{Z}[X]$.*

Théorème 4.6 (Critère d'Eisenstein)**.** *Soit A un anneau factoriel et $P = \sum_{k=0}^{n} a_k X^k \in A[X]$ de degré $n \geq 1$. Supposons qu'il existe un élément premier $p \in A$ tel que*

1. *$p \mid a_i$ pour $0 \leq i \leq n-1$.*
2. *$p \nmid a_n$.*
3. *$p^2 \nmid a_0$.*

Alors P est irréductible dans $\mathrm{Frac}(A)[X]$.

Démonstration. Supposons P réductible dans $\mathrm{Frac}(A)[X]$, $P = QR$ avec $Q, R \in \mathrm{Frac}(A)[X]$ et $\deg Q, \deg R \geq 1$. D'après le lemme de Gauss, on peut supposer que $Q, R \in A[X]$. Alors dans $A/(p)[X]$, on a $\overline{P} = \overline{QR} = \overline{a_n X^n}$. Par intégrité de $A/(p)$, cela veut dire que $\overline{Q} = \overline{\lambda X^k}$ et $\overline{R} = \overline{\mu X^{n-k}}$ pour un $k \in \{1, \ldots, n-1\}$. En particulier, $p \mid Q(0), R(0)$ d'où $p^2 \mid P(0)Q(0) = a_0$, ce qui est absurde. □

Remarque 4.7. Si de plus, P est primitif alors il est irréductible dans $A[X]$.

Exercice 11. *Montrer que $\mathbb{Z}[X]$ possède des polynômes irréductibles de tout degré $n \geq 1$.*

5 Polynômes symétriques

Définition 5.1. *Un polynôme $P \in A[X_1, \ldots, X_n]$ est* ***symétrique*** *lorsque pour tout $\sigma \in \mathfrak{S}_n$,*

$$P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = P.$$

Les ***polynômes symétriques élémentaires*** *(en n variables) sont les*

$$\Sigma_k = \sum_{1 \leq i_1 < \cdots < i_k \leq n} X_{i_1} \ldots X_{i_k}$$

avec $1 \leq k \leq n$.

Exercice 12. *Écrire $\Sigma_1, \Sigma_2, \Sigma_3$ et Σ_4 en 4 variables.*

Proposition 5.2 (Relations coefficients-racines)**.** *Soit $P = \sum_{k=0}^{n} a_k X^k \in A[X]$ avec $a_n \neq 0$. Supposons qu'il existe une factorisation de la forme*

$$P = a_n \prod_{i=1}^{n} (X - \lambda_i),$$

avec $\lambda_1, \ldots, \lambda_n \in A$. Alors pour $1 \leq k \leq n$, on a

$$a_k = (-1)^{n-k} a_n \Sigma_{n-k}(\lambda_1, \ldots, \lambda_n).$$

Théorème 5.3 (Théorème fondamental des polynômes symétriques)**.** *Soit $P \in A[X_1, \ldots, X_n]$ symétrique. Alors il existe un unique polynôme $Q \in A[X_1, \ldots, X_n]$ tel que $P = Q(\Sigma_1, \ldots, \Sigma_n)$.*

Démonstration. La démonstration est algorithmique : On élimine les monômes de P dans l'ordre décroissant pour l'ordre lexicographique sur les degrés. L'unicité se fait par récurrence sur n, en montrant que si $Q(\Sigma_1, \ldots, \Sigma_n) = 0$ alors $Q = 0$. □

Exercice 13. *Exprimer le polynôme symétrique $X_1^2X_2 + X_1^2X_3 + X_2^2X_1 + X_2^2X_3 + X_3^2X_1 + X_3^2X_2$ comme un polynôme en $\Sigma_1, \Sigma_2, \Sigma_3$.*

Corollaire 5.4. *Soit $P \in A[X]$ et soit B un anneau commutatif contenant A tel que*

$$P = \prod_{i=1}^{n} (X - \lambda_i) \in B[X].$$

Alors pour tout polynôme symétrique $Q \in A[X_1, \ldots, X_n], Q(\lambda_1, \ldots, \lambda_n) \in A$.

Exercice 14. *Montrer, sans calcul, que pour tout $n \in \mathbb{N}$, $\alpha_1^n + \alpha_2^n + \alpha_3^n + \alpha_4^n \in \mathbb{Z}$, où*

$$\alpha_1 = \sqrt{2 + \sqrt{2}}, \alpha_2 = \sqrt{2 - \sqrt{2}}, \alpha_3 = -\sqrt{2 + \sqrt{2}}, \alpha_4 = -\sqrt{2 - \sqrt{2}}.$$

Proposition 5.5 (Sommes de Newton)**.** *Pour tout $k \in \mathbb{N}^*$, notons $\sigma_k = \sum_{j=1}^{n} X_j^k$. Alors on a*

$$k\Sigma_k = \sum_{i=1}^{k} (-1)^{i-1} \Sigma_{k-i} \sigma_i.$$

Démonstration. Développer $\prod_{i=1}^{n} (T - X_i)$, évaluer en chaque X_i et sommer. □

Remarque 5.6. ⚠ Cette formule permet d'exprimer chaque σ_k par récurrence, du moment que A est un corps de caractéristique nulle !

6 Fractions rationnelles

Dans cette section, K désigne un corps.

Définition 6.1. *Le corps des fractions $K(X)$ de $K[X]$ est appelé le* ***corps des fractions rationnelles*** *sur K. Le degré de la fraction rationnelle $\frac{P}{Q}$ est $\deg P - \deg Q$.*

Remarque 6.2. Le degré de $\frac{P}{Q}$ ne dépend pas de P et Q.

Théorème 6.3. *Toute fraction rationnelle $F \in K(X)$ admet une décomposition unique sous la forme $P + R$ avec $P \in K[X]$ (appelé* ***partie polynomiale*** *de F) et $\deg R < 0$ (appelé* ***partie polaire*** *de F).*

Démonstration. Si $F = \frac{A}{B}$, on pose la division euclidienne de A par B : $A = BQ + R$ avec $\deg R < \deg B$. Alors $F = Q + \frac{R}{B}$. L'unicité vient en considérant les degrés des différences. $\square$

Corollaire 6.4 (Décomposition en éléments simples)**.** *Soit $F = \frac{A}{B} \in K(X)$. Factorisons $B = \prod_{i=1}^{n} Q_i^{m_i}$ avec les Q_i irréductibles. Alors il existe des uniques $P, P_{1,1}, \dots, P_{1,m_1}, \dots, P_{n,1}, \dots, P_{n,m_n} \in K[X]$ avec $\deg P_{i,k} < \deg Q_i$ tels que*

$$F = P + \sum_{i=1}^{n} \sum_{k=1}^{m_i} \frac{P_{i,k}}{Q_i^k}.$$

Exercice 15. *Donner la décomposition en éléments simples de $\frac{1}{X^4-1}$ dans $\mathbb{R}(X)$ et $\mathbb{C}(X)$.*

7 Exercices

Exercice 16. *Poser la division euclidienne de $5X^3 + X + 8$ par $8X^2 + 4X + 1$ dans $\mathbb{Z}/15\mathbb{Z}[X]$.*

Exercice 17. *Déterminer les racines du polynôme $X^2 + 3X - 1$ dans $\mathbb{Z}/35\mathbb{Z}$.*

Exercice 18. *Soit $a, b \in \mathbb{N}^*$. Déterminer le reste de la division euclidienne de $X^a - 1$ par $X^b - 1$ dans $\mathbb{Z}[X]$.*

Exercice 19. *Décomposer en éléments simples la fraction rationnelle $\frac{X^5+X^4+1}{X^3-X}$ dans $\mathbb{Q}(X)$.*

Exercice 20. *Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$. Montrer que si $\frac{p}{q} \in \mathbb{Q}$ avec p et q premiers entre eux est une racine de P alors $q \mid a_n$ et $p \mid a_0$. En déduire que le polynôme $X^3 + 5X^2 - X + 7$ est irréductible dans $\mathbb{Q}[X]$.*

Exercice 21. *Soit K un corps, $n \in \mathbb{N}, n \geq 2$ et $a \in K$. Notons $P = X^n - a$.*

1. *Montrer que si p est un nombre premier divisant n et $a = b^p$ pour un certain $b \in K$, alors P est réductible dans $K[X]$.*

2. *Montrer que si n est divisible par 4 et $a = -4b^4$ pour un certain $b \in K$, alors P est réductible dans $K[X]$.*

Remarque. Il se trouve que la réciproque est vraie : si P est réductible dans $K[X]$ alors a est de l'une des formes ci-dessus.

Exercice 22. *Montrer la généralisation suivante du critère d'Eisenstein : Soit A un anneau factoriel, $P = \sum_{k=0}^{n} a_k X^k$, $d \in \{1, \dots, n\}$, $p \in A$ premier tel que :*

1. $p \mid a_i$ *pour* $0 \leq i \leq d-1$.
2. $p \nmid a_d$.
3. $p^2 \nmid a_0$.

Alors P admet un facteur irréductible dans $A[X]$ de degré au moins d.

Exercice 23. *Soit A un anneau commutatif, $n \in \mathbb{N}^*$ et $k \in \{1, \dots, n\}$. Quel est le degré et le nombre de monômes de $\Sigma_k \in A[X_1, \dots, X_n]$?*

Exercice 24. *Exprimer les coefficients du polynôme caractéristique d'une matrice à coefficients dans un corps K en fonction de ses valeurs propres.*

Exercice 25. *Soit K un corps. Pour $F = \frac{P}{Q} \in K(X)$, on note $F' = \frac{P'Q - PQ'}{Q^2}$. Montrer qu'il n'existe aucune fraction rationnelle $F \in K(X)$ telle que $F' = \frac{1}{X}$.*

Exercice 26. *Soit K un corps.*

1. *Montrer qu'un endomorphisme de K-algèbre de $K(X)$ est de la forme $P \mapsto P \circ F$ avec $F \in K(X)$.*
2. *Dans le cas d'un automorphisme, montrer que F est un quotient non constant de polynômes de degré 1.*
3. *En déduire une description du groupe $\mathrm{Aut}(K(X))$.*

Exercice 27. *Soit A un anneau noethérien. On va montrer que $A[X]$ est noethérien. Rappelons que la noetherianité est équivalente au fait que toute famille d'idéaux admet un élément maximal pour l'inclusion.*

1. *Soit I un idéal de $A[X]$. Pour $n \in \mathbb{N}$, notons $c_n(I)$ l'ensemble des coefficients dominants des éléments de I de degré n, auquel on ajoute 0. Montrer que $c_n(I)$ est un idéal de A.*
2. *Montrer que $c_n(I)$ est croissant par rapport à I et par rapport à n.*
3. *Montrer que si I et J sont des idéaux de $A[X]$ avec $I \subset J$, alors $I = J$ si et seulement si $\forall n \in \mathbb{N}, c_n(I) = c_n(J)$.*
4. *Soit $(I_n)_{n\in\mathbb{N}}$ une suite croissante d'idéaux de $A[X]$. En considérant la famille d'idéaux $\{c_k(I_n) \mid k, n \in \mathbb{N}\}$, montrer que la suite $(I_n)_{n\in\mathbb{N}}$ est stationnaire.*
5. *Montrer qu'un quotient d'anneau noethérien est noethérien. En déduire que toute A-algèbre de type fini est noethérienne.*

Exercice 28. *Soit K un corps et $n \in \mathbb{N}^*$. On définit le **corps des fractions rationnelles en n variables** sur K comme le corps des fractions $K(X_1, \dots, X_n)$ de $K[X_1, \dots, X_n]$. Une fraction rationnelle $F \in K(X_1, \dots, X_n)$ est dite symétrique lorsque pour tout $\sigma \in \mathfrak{S}_n$, $F(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = F$. Montrer que toute fraction rationnelle symétrique est une fraction rationnelle en les polynômes symétriques élémentaires.*

Exercice 29. *Soit K un corps de caractéristique différente de 2 et $n \in \mathbb{N}^*$. On appelle* ***polynôme alterné*** *tout polynôme $P \in K[X_1, \dots, X_n]$ tel que pour tout $\sigma \in \mathfrak{A}_n$, $\sigma.P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P$.*

1. *Montrer que le polynôme $\Delta = \prod_{1 \leq i < j \leq n}(X_j - X_i)$ est alterné et non symétrique.*
2. *Soit $P \in K[X_1, \dots, X_n]$ alterné et $\tau \in \mathfrak{S}_n \setminus \mathfrak{A}_n$. Montrer que $\tau.P$ est alterné.*
3. *On pose $A = P + \tau.P$ et $B = P - \tau.P$. Montrer que A est symétrique et que $B = \Delta Q$ pour un certain $Q \in K[X_1, \dots, X_n]$ symétrique.*
4. *En déduire que $K[X_1, \dots, X_n]^{\mathfrak{A}_n} = K[X_1, \dots, X_n]^{\mathfrak{S}_n}[\Delta]$.*

Remarque. Le résultat reste vrai sur tout anneau commutatif de caractéristique différente de 2. En caractéristique 2, Δ est symétrique, et le résultat est plus difficile à énoncer.

Exercice 30. *Soit K un corps. Si $P = \sum_{k=0}^{n} a_k X^k \in K[X]$ et $Q = \sum_{k=0}^{m} b_k X^k \in K[X]$ sont de degrés n et m respectivement, leur* ***matrice de Sylvester*** *est la matrice carrée de taille $(m+n)$ donnée par*

$$S(P,Q) = \begin{pmatrix} a_n & 0 & \cdots & 0 & b_m & 0 & \cdots & 0 \\ a_{n-1} & a_n & \ddots & \vdots & \vdots & b_m & \ddots & \vdots \\ \vdots & a_{n-1} & \ddots & 0 & \vdots & & \ddots & 0 \\ \vdots & \vdots & \ddots & a_n & b_1 & & & b_m \\ a_0 & & & a_{n-1} & b_0 & \ddots & \vdots & \vdots \\ 0 & \ddots & & \vdots & 0 & \ddots & b_1 & \vdots \\ \vdots & \ddots & a_0 & \vdots & \vdots & \ddots & b_0 & b_1 \\ 0 & \cdots & 0 & a_0 & 0 & \cdots & 0 & b_0 \end{pmatrix}.$$

On définit le ***résultant*** *de P et Q comme $\mathrm{Res}(P,Q) = \det S(P,Q)$.*

1. *Montrer que pour tout $a, b \in K$, $\mathrm{Res}(aP, bQ) = a^m b^n \mathrm{Res}(P,Q)$ et que $\mathrm{Res}(Q,P) = (-1)^{mn}\mathrm{Res}(P,Q)$.*
2. *Montrer que $S(P,Q)$ est la matrice de l'application linéaire $(U,V) \mapsto PU + QV$ définie sur $K_{m-1}[X] \times K_{n-1}[X]$ dans une base bien choisie.*
3. *En déduire que $\mathrm{Res}(P,Q) = 0$ si et seulement si P et Q ne sont pas premiers entre eux.*

Remarque. Le **discriminant** d'un polynôme P est définie comme $\mathrm{Res}(P, P')$.

Exercice 31. *Montrer que le polynôme $X^2 + 1$ admet une infinité de racines dans l'algèbre des quaternions $\mathbb{H}$ (voir la feuille 1 pour la définition). On pourra calculer le carré d'un quaternion imaginaire pur.*

Exercice 32. *Montrer que si $P = \sum_{k=0}^{n} a_k X^k \in A[X] \backslash \{0\}$ avec $a_n \neq 0$, alors P est inversible dans $A[X]$ si et seulement a_0 est inversible dans A et $a_A, \dots, a_n$ sont nilpotents. (Indication : Pour l'implication directe, faire une récurrence sur n, en notant que la somme d'un inversible et d'un nilpotent qui commutent est inversible. Utiliser ce dernier fait pour l'implication réciproque.)*