Contrôle Continu 26/10/22

Durée : 2h
Documents, téléphones portables et appareils électroniques interdits
La redaction et la clarté de l'argumentation sera prise en compte dans la notation

Exercice 1 (Autour du cours) Soit A un anneau intègre.

1. Montrer que $P \in A[X] \setminus \{0\}$ possède au plus $\deg(P)$ racines distinctes dans A.
   Soient $P \in A[X] \setminus \{0\}$. Premièrement, comme A est intègre, il admet un corps de fraction $k = \mathrm{Fr}(A)$. On va alors montrer que P a au plus $\deg(P)$ racines dans k (ce qui impliquera à fortiori qu'il a au plus $deg(P)$ racines dans A).
   Si P est constant, i.e. $\deg(P) = 0$, comme P est non nul, il n'a pas de racine dans k donc c'est bon.
   On suppose maintenant que P n'est pas constant et qu'il a au moins une racine (sinon il a clairement moins de racine que son degré). Soit $a_1, a_2, \dots a_n \in k$ des racines distinctes de P. Pour tout $i \in \{1, 2, \dots, n\}$, on effectue dans $k[X]$, qui est euclidien, la division euclidien de P par $X - a_i$ pour voir que (en évaluant l'égalité obtenue en a_i) $X - a_i \div P$. Or les $X - a_i$ sont premiers entre deux à deux (on a par exemple la relation de Bezout suivante : $(X - a_i) - (X - a_j) = a_i - a_j \in k^\times = k[X]^\times$) et donc $\prod_{i=1}^n (X - a_i) \div P$. Ainsi, comme A est intègre, $n = \deg\left(\prod_{i=1}^n (X - a_i)\right) \leq \deg(P)$.

2. Si $P \in A[X]$ est irréductible et $\deg(P) \geq 2$, montrer que P ne possède pas de racines dans A.
   Soit $P \in A[X]$ avec $\deg(P) \geq 2$ et supposons que P possède une racine $a \in A$. Comme A est intègre et $X - a$ est unitaire, on peut faire la division euclidienne de P par $X - a$ ce qui montre, en évaluant l'égalité obtenue en a, que $X - a \div P$. Donc il existe $Q \in k[X]$ tel que $P = (X - a)Q$. En regardant les degrée, on a $\deg(Q) = 1$ et donc Q n'est pas inversible. Ainsi (comme $X - a$ n'est pas non plus inversible), P est le produit de deux polynômes non inversible. En particulier il n'est pas irréductible. Par contraposition, si $P \in A[X]$ est un polynôme de degré 2 et irréductible, il n'a pas de racine dans A.

3. On suppose $\deg(P) \in \{2, 3\}$. Pour chacune des hypothèses ci-dessous, la réciproque de 2. est-elle vérifiée ?

   (a) A est factoriel (b) A est un corps

   A factoriel ne suffit pas. Par exemple, en prenant $A = \mathbb{Z}$ qui est factoriel, on a $2(X^2 + 1) = 2X^2 + 2\mathbb{Z}[X]$ n'a pas de racine dans $\mathbb{Z}$ mais n'est pas irréductible (c'est le produit de deux éléments non inversibles de $\mathbb{Z}[X]$: 2 et $X^2 + 1$). On peut même trouver des polynômes de degré 2 sans racine non irréductibles mais de contenu 1 : par exemple $(2X - 1)^2$.
   Si A est un corps, la réciproque de 2 est vérifiée. En effet, si $P \in A[X]$ est un polynôme de degré 2 ou 3 n'est pas irréductible, comme $A[X] = A^\times$, P peut s'écrire $P = Q_1 Q_2$ avec $Q_1, Q_2 \in A[X]$ chacun de degré strictement positif. Comme $\deg(P) \in \{2, 3\}$, au moins l'un des deux, disons Q_1, est de degré 1 et donc $Q_1 = aX - b$ avec $a \in A \setminus \{0\}$ et $b \in A$. Comme A est un corps, a est inversible et $a^{-1}b$ est une racine de Q_1 et donc une racine de P. Donc, en contraposant, si P n'a pas de racine et est de degré 2 ou 3, P est irréductible.

Exercice 2 (Fonction polynomiale) Soient $n \in \mathbb{N}^*$ et $f \colon \mathbb{R}^n \to \mathbb{R}$ une fonction polynomiale. On suppose que f est nulle sur un ouvert non vide de $\mathbb{R}^n$ (pour la topologie induite par la norme euclidienne). Montrer que f est la fonction nulle.

Soit $P \in \mathbb{R}[X_1, X_2, \dots, X_n]$ tel que f soit la fonction polynomiale associée à P. Soit U un ouvert non vide de $\mathbb{R}^n$ sur lequel f (et donc P) s'annule (U existe par hypothèse sur f). Comme U est ouvert et non vide il existe des intervalles, chacun non réduit à un point, $I_1, I_2, \dots I_n$ de $\mathbb{R}$ tels que $I_1 \times I_2 \times \cdots \times I_n \subseteq U$ (on peut invoquer l'équivalence des normes sur $\mathbb{R}^n$ si on le souhaite). Ainsi P s'annule sur $I_1 \times I_2 \times \cdots \times I_n$ et, comme pour tout $i \in \{1, 2, \dots, n\}$ l'intervalle I_i est infini, $P = 0$.

Exercice 3 (Discriminant d'un polynôme) Soit $P \in \mathbb{Q}[X]$ unitaire de degré n. Notons $\alpha_1, \dots, \alpha_n$ ses racines dans $\mathbb{C}$, et $\beta_1, \dots, \beta_{n-1}$ les racines de P' dans $\mathbb{C}$. Rappelons que le discriminant de P est $\Delta = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$.

1. Si $\delta = \prod_{1 \leq i \neq j \leq n} (\alpha_i - \alpha_j)$, montrer que $\Delta = (-1)^{n(n-1)/2} \delta$.

   Pour tout $(i,j) \in \{1, 2, \dots, n\}^2$ avec $i < j$ il y a exactement deux facteurs dans δ avec α_i et α_j qui sont $(\alpha_i - \alpha_j)$ et $(\alpha_j - \alpha_i)$. Ainsi, en écrivant $(\alpha_i - \alpha_j)^2 = (-1)(\alpha_i - \alpha_j)(\alpha_j - \alpha_i)$, on obtient que $\delta = (-1)^a \Delta$ où $a = \mathrm{Card}\left(\{(i,j) \in \{1, 2, \dots, n\}^2 \mid i < j\}\right) = n(n-1)/2$.

$$\begin{aligned}
\delta = \prod_{1 \leq i \neq j \leq n} (\alpha_i - \alpha_j) &= \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)(\alpha_j - \alpha_i) \\
&= \prod_{1 \leq i < j \leq n} (-1)(\alpha_i - \alpha_j)^2 \\
&= (-1)^{n(n-1)/2} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 \\
&= (-1)^{n(n-1)/2} \Delta
\end{aligned}$$

   D'où la formule recherchée en passant le $(-1)^{n(n-1)/2}$ de l'autre coté.

2. Pour tout $i = 1, \dots, n$, établir $P'(\alpha_i) = \prod_{\substack{1 \leq j \leq n \\ j \neq i}} (\alpha_i - \alpha_j)$.

   Comme $P = \prod_{j=1}^n (X - \alpha_j)$, on a $P' = \sum_{i=1}^n \prod_{\substack{1 \leq j \leq n \\ j \neq i}} (X - \alpha_j)$. Ainsi, lorsqu'on évalue en α_i, un seul terme de la somme précédente peut ne pas s'annuler, et on obtient $P'(\alpha_i) = \prod_{\substack{1 \leq j \leq n \\ j \neq i}} (\alpha_i - \alpha_j)$ ce qui donne l'égalité recherchée.

3. En déduire $\Delta = (-1)^{n(n-1)/2} \prod_{i=1}^n P'(\alpha_i)$.

   Par définition de δ et la formule précédente, $\delta = \prod_{i=1}^n P'(\alpha_i)$ et donc, en utilisant la première question de cet exercice, $P = (-1)^{n(n-1)/2} \prod_{i=1}^n P'(\alpha_i)$.

4. Montrer que $P'(\alpha_i) = n \prod_{j=1}^{n-1} (\alpha_i - \beta_j)$ et en déduire $\Delta = (-1)^{n(n-1)/2} n^n \prod_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n-1}} (\alpha_i - \beta_j)$.

   Comme P' est de degré $n-1$, que son coefficient dominant est n et que $\beta_1, \beta_2, \dots \beta_n$ sont ses racines dans $\mathbb{C}$, on a que $P' = n \prod_{j=1}^{n-1} (X - \beta_j)$ et donc $P'(\alpha_i) = n \prod_{j=1}^{n-1} (\alpha_i - \beta_j)$. Ainsi, en remplaçant dans la formule précédente, on obtient bien $\Delta = (-1)^{n(n-1)/2} n^n \prod_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n-1}} (\alpha_i - \beta_j)$.

5. Établir

$$\Delta = (-1)^{n(n-1)/2} n^n \prod_{j=1}^{n-1} P(\beta_j).$$

   Comme $P = \prod_{i=1}^n (X - \alpha_i)$, on a

$$\begin{aligned}
\Delta = (-1)^{n(n-1)/2} n^n \prod_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n-1}} (\alpha_i - \beta_j) &= (-1)^{n(n-1)/2} n^n \prod_{j=1}^{n-1} \prod_{i=1}^{n} (\alpha_i - \beta_j) \\
&= (-1)^{n(n-1)/2} n^n \prod_{j=1}^{n-1} (-1)^n P(\beta_j) \\
&= (-1)^{n(n-1)/2} \underbrace{(-1)^{n(n-1)}}_{\text{=1 car n(n-1) pair}} \prod_{j=1}^{n-1} P(\beta_j) \\
&= (-1)^{n(n-1)/2} \prod_{j=1}^{n-1} P(\beta_j).
\end{aligned}$$

6. Pour $n \in \mathbb{N}^*$, calculer le discriminant du polynôme $X^n - 1$.
Notons $P = X^n - 1$ On a $P' = nX^{n-1}$ qui n'a que 0 comme racine (de multiplicité $n-1$. Ainsi, en utilisant la question précédente, le discriminant de P est

$$\Delta(P) = (-1)^{n(n-1)/2} n^n \prod_{j=1}^{n-1} \underbrace{P(0)}_{=-1} = (-1)^{n(n-1)/2+(n-1)} n^n = (-1)^{(n+2)(n-1)/2} n^n$$

Exercice 4 (Étude d'un anneau) Considérons l'anneau $A = \mathbb{C}[X,Y]/(Y^2 - X^3)$. On notera $x, y \in A$ les classes de X et Y.

1. Montrer que $Y^2 - X^3$ est irréductible dans $\mathbb{C}[X,Y]$. En déduire que A est intègre.
Dans $\mathbb{C}(X)[Y]$, le polynôme$Y^2 - X^3$ est sans racine. En effet, si $P(X)/Q(X) \in \mathbb{C}(X)$ est racine de $Y^2 - X^3$ alors $P(X)^2 = X^3 Q(X)^2$ Cela est impossible car le polynôme de gauche est de degré $2\deg(P)$ qui est pair et celui de droite et de degré $2\deg(Q) + 3$ qui est impair. Ainsi, on a que $Y^2 - X^3$ est un polynôme de degré 2 sans racine et il est donc irréductible dans $\mathbb{C}(X)[Y]$. Comme c'est un polynôme unitaire et donc primitif, il est aussi irréductible dans $\mathbb{C}[X][Y] \simeq \mathbb{C}[X,Y]$. On a alors que $(Y^2 - X^3)$ est un idéal premier de $\mathbb{C}[X,Y]$ ce qui est équivalent à $A = \mathbb{C}[X,Y]/(Y^2 - X^3)$ intègre.
2. Justifier rigoureusement l'existence d'un morphisme $f\colon A \to \mathbb{C}[T]$ envoyant x sur T^2, y sur T^3, et qui est l'identité sur $\mathbb{C}$.
On considère le morphisme d'évaluation $\mathrm{ev}\colon \mathbb{C}[X,Y] \to \mathbb{C}[T]$ envoyant X sur T^2, Y sur T^3 et qui est l'identité sur $\mathbb{C}$ (ce morphisme existe par propriété universelle de $\mathbb{C}[X,Y]$). On remarque alors que $\mathrm{ev}(Y^2 - X^3) = T^6 - T^6 = 0$ et donc $(Y^2 - X^3) \subseteq \mathrm{Ker}(\mathrm{ev})$. Ainsi, par théorème de factorisation, il existe $f : A \to \mathbb{C}[T]$ tel que, si on note $\pi\colon \mathbb{C}[X,Y] \to A$ l'application quotient, $f \circ \pi = \mathrm{ev}$. on a alors, $f(x) = f \circ \pi(X) = \mathrm{ev}(X) = T^2$, $f(y) = f \circ \pi(Y) = \mathrm{ev}(Y) = T^3$ et, pour tout $z \in \mathbb{C}$, $f(z) = f \circ \pi(z) = \mathrm{ev}(z) = z$.
3. Montrer que f est injectif (on pourra effectuer une division euclidienne par $Y^2 - X^3$ dans $\mathbb{C}[X][Y]$).

   Pour montrer que f est injectif, il suffit de vérifier que $\mathrm{Ker}(\mathrm{ev}) = (Y^2 - X^3)$ et il nous reste donc l'inclusion $\mathrm{Ker}(\mathrm{ev}) \subseteq (Y^2 - X^3)$. Soit $P \in Ker(\mathrm{ev})$. Comme $Y^2 - X^3 \in \mathbb{C}[X][Y]$ est unitaire, on peut effectuer la division euclidien de P par $Y^2 - X^3$ et donc il existe $Q, R \in \mathbb{C}[X][Y]$ tels que $P = Q(Y^2 - X^3) + R$ avec $\deg_Y(R) \leq 1$. On peut alors écrire R sous la forme $R = A(X)Y + B(X)$ avec $A(X), B(X) \in \mathbb{C}[X]$. En appliquant ev on obtient alors $0 = \mathrm{ev}(R) = A(T^2)T^3 + B(T^2)$ qu'on peut réécrire sous la forme $A(T^2)T^3 = -B(T^2)$. Dans cette dernière égalité, tout les monômes de droite sont de degré impair (s'il y en a) et tout ceux de gauche sont de degré pair. Ainsi, par identification, tout les coefficients de A et de B sont nuls et $R = 0$. Ainsi $Y^2 - X^3$ divise P et $\mathrm{Ker}(\mathrm{ev}) \subseteq (X^2 - Y^3)$. Ainsi, par factorisation f est injective.

   On identifiera par la suite A avec un sous-anneau de $\mathbb{C}[T]$ et $\mathrm{Fr}(A)$ avec un sous-anneau de $\mathbb{C}(T)$.
4. Montrer que $\mathrm{Im}(f) = \{P \in \mathbb{C}[T]; P'(0) = 0\}$ (on pourra montrer que $T \notin \mathrm{Im}(f)$).
On a que $P'(T) = 0$ si et seulement si P peut s'écrire sous la forme $P = a_0 + T^2 Q$ où $a_0 \in \mathbb{C}$ et $Q \in \mathbb{C}[T]$. Ainsi $\{P \in \mathbb{C}[T]; P'(0) = 0\}$ est engendrée, en tant que $\mathbb{C}$-espace vectoriel par $(1, T^2, T^3, T^4, \dots)$. Or $1 = f(1) \in \mathrm{Im}(f)$ et pour tout $n \geq 2$, si n est pair, $T^n = (T^2)^{n/2} = (f(x))^{n/2} \in \mathrm{Im}(f)$ et si n est impair (et donc $n \geq 3$), $T^n = (T^2)^{(n-3)/2} \times T^3 = (f(x))^{(n-3)/2} f(y) \in \mathrm{Im}(f)$. On a donc $\mathrm{Im}(f) \supseteq \{P \in \mathbb{C}[T]; P'(0) = 0\}$. Pour l'inclusion réciproque, considérons $P \in \mathbb{C}[T] \setminus \{P \in \mathbb{C}[T]; P'(0) = 0\}$. Donc $P = a_0 + a_1 T + T^2 Q$ avec $a_0 \in \mathbb{C}, a_1 \in \mathbb{C} \setminus \{0\}$ et $Q \in \mathbb{C}[T]$. Comme $a_0 \in \mathrm{Im}(f)$ et $T^2 Q \in \mathrm{Im}(f)$, $P \in \mathrm{Im}(f)$ si et seulement si $T \in \mathrm{Im}(f)$. Il nous suffit donc de vérifier que $T \notin \mathrm{Im}(f) = \mathrm{Im}(\mathrm{ev})$. On peut procéder par l'absurde et supposer qu'il existe $P \in \mathbb{C}[X,Y]$ tel que $\mathrm{ev}(P) = T$. Notons $P = \sum_{i,j} a_{i,j} X^i Y^j$ avec $a_{i,j} \in \mathbb{C}$. On a alors $\mathrm{ev}(P) = \sum_{i,j} a_{i,j} T^{2i+3j}$. Cependant, 1 ne peut pas s'écrire sous la forme $2i + 3j$ avec $i, j \in \mathbb{N}$. Donc le monôme T n'apparait pas dans l'expression de $\mathrm{ev}(P)$ ce qui est absurde.

5. Après avoir vérifié que $T \in \mathrm{Fr}(A)$, montrer que $\mathrm{Fr}(A) = \mathbb{C}(T)$.
   On a $T^2, T^3 \in A$ donc $T = T^3/T^2 \in \mathrm{Fr}(A)$. Ainsi, comme $\mathbb{C} \subseteq A \subseteq \mathrm{Fr}(A)$ et $T \in \mathrm{Fr}(A)$, $\mathbb{C}(T) \subseteq \mathrm{Fr}(A)$. Or $\mathrm{Fr}(A)$ est un sous corps de $\mathbb{C}(T)$ donc $\mathbb{C}(T) = \mathrm{Fr}(A)$.
6. Montrer que $T \in \mathrm{Fr}(A)$ est entier sur A (*i.e.* il existe un polynôme unitaire $Q \in A[Z]$ tel que $Q(T) = 0$).
   T est racine de $Z^2 - T^2 \in A[Z]$ et est donc entier sur A.
7. En déduire que A n'est pas factoriel (on pourra utiliser un exercice du TD).
   Par un exercice de TD, une anneau factoriel B est intégralement clos : tout élément $x \in \mathrm{Fr}(B)$ entier sur B est dans B. Cela n'est pas vérifier par l'anneau A ici présent. Donc A n'est pas factoriel.