Contrôle Continu 2

Algèbre – M1 Mathématiques et Informatique Cryptographique

14 novembre 2023

Durée : 1h30. Les documents et les calculatrices ne sont pas autorisés.

Exercice 1. (a) Soit A un anneau et $\mathfrak{p}$ un idéal vérifiant la propriété suivante : pour tous idéaux I_1, I_2 de A tels que $\mathfrak{p}$ contienne $I_1 I_2$, alors $\mathfrak{p}$ contient I_1 ou $\mathfrak{p}$ contient I_2. Montrer que $\mathfrak{p}$ est un idéal premier. Étudier la réciproque.

Réponse : Soit $x, y \in \mathfrak{p}$ deux éléments de $\mathfrak{p}$ tels que $xy \in \mathfrak{p}$. Soit $I_1 = (x)$ et $I_2 = (y)$. Alors $I_1 I_2 = (xy)$ est contenu dans $\mathfrak{p}$, donc $\mathfrak{p}$ contient I_1 ou $\mathfrak{p}$ contient I_2. Dans le premier cas, $x \in \mathfrak{p}$, et dans le second cas, $y \in \mathfrak{p}$. Ceci montre que $\mathfrak{p}$ est un idéal premier.

Réciproquement, supposons que $\mathfrak{p}$ est premier et que $I_1, I_2 \subset A$ sont deux idéaux tels que $I_1 I_2 \subset \mathfrak{p}$. Supposons que $\mathfrak{p}$ ne contienne ni I_1, ni I_2. Alors il existe des éléments $x \in I_1 \setminus \mathfrak{p}$ et $y \in I_2 \setminus \mathfrak{p}$. Comme $\mathfrak{p}$ est premier, $xy \notin \mathfrak{p}$. Or, $xy \in I_1 I_2 \subset \mathfrak{p}$, ce qui est absurde. On en déduit que $\mathfrak{p}$ contient I_1 ou $\mathfrak{p}$ contient I_2.

(b) Soit $f : A \to B$ un morphisme d'anneaux, et $\mathfrak{r}$ un idéal premier de B. Montrer que $f^{-1}(\mathfrak{r})$ est un idéal premier de A. Si $\mathfrak{r}$ est maximal, $f^{-1}(\mathfrak{r})$ est-il nécessairement maximal ?

Réponse : La préimage d'un idéal est toujours un idéal, donc $f^{-1}(\mathfrak{r})$ est un idéal de A. Démontrons qu'il est premier. Soit $x, y \in A$ deux éléments tels que $xy \in f^{-1}(\mathfrak{r})$. On a $f(x)f(y) = f(xy) \in \mathfrak{r}$. Or, $\mathfrak{r}$ est premier, donc $f(x) \in \mathfrak{r}$ ou $f(y) \in \mathfrak{r}$. Dans le premier cas, $x \in f^{-1}(\mathfrak{r})$, et dans le second cas, $y \in f^{-1}(\mathfrak{r})$. Ceci montre que $f^{-1}(\mathfrak{r})$ est un idéal premier.

Si r est maximal, il n'est pas vrai que $f^{-1}(\mathfrak{r})$ est nécessairement maximal. Considérons par exemple le morphisme d'anneaux $f : \mathbb{Z} \to \mathbb{Q}$, $x \mapsto x$. L'idéal $\mathfrak{r} = (0) \subset \mathbb{Q}$ est maximal car $\mathbb{Q}$ est un corps, mais sa préimage $f^{-1}((0)) = (0) \subset \mathbb{Z}$ n'est pas maximal car $\mathbb{Z}$ n'est pas un corps.

Exercice 2. Soit $\mathfrak{p}$ un idéal premier non nul de $\mathbb{Z}[X]$.

(a) Montrer que, pour tout $R \in \mathfrak{p}$ non nul, $\mathfrak{p}$ contient l'un des diviseurs irréductibles de R.

Réponse : Comme l'anneau $\mathbb{Z}$ est factoriel, l'anneau $\mathbb{Z}[X]$ l'est aussi. On peut donc écrire $R = Q_1 \cdots Q_n$, où les Q_i sont des polynômes irréductibles. Ce produit appartient à $\mathfrak{p}$, qui est premier, donc $\mathfrak{p}$ contient l'un des Q_i.

(b) Supposons que $\mathfrak{p}$ ne contienne qu'un seul polynôme irréductible P (à inversible près). Montrer que $\mathfrak{p} = (P)$.

Réponse : Comme $P \in \mathfrak{p}$ et que $\mathfrak{p}$ est un idéal, on a bien $(P) \subset \mathfrak{p}$. Réciproquement, soit $R \in \mathfrak{p}$. D'après la question précédente, $\mathfrak{p}$ contient un diviseur irréductible de R. Or, $\mathfrak{p}$ ne contient qu'un seul polynôme irréductible (à inversible près), donc ce diviseur irréductible est P (à inversible près). On en déduit que P divise R et donc que $R \in (P)$. On a donc $\mathfrak{p} \subset (P)$.

(c) Montrer que si $P \in \mathbb{Z}[X]$ est un polynôme irréductible, l'idéal $\mathfrak{p} = (P)$ est premier. Quels sont les irréductibles contenus dans $\mathfrak{p}$?

Réponse : Il s'agit d'une reformulation du lemme d'Euclide, qui est vérifié dans $\mathbb{Z}[X]$ car cet anneau est factoriel. Les irréductibles contenus dans $\mathfrak{p}$ sont les polynômes associés à P. En effet, si Q est un autre polynôme irréductible contenu dans $\mathfrak{p}$, alors P et Q sont associés car ils sont tous les deux irréductibles et que P divise Q.

Dans toute la suite, on suppose que $\mathfrak{p}$ contient au moins deux polynômes irréductibles non associés.

(d) Soient $P, Q \in \mathbb{Z}[X]$ deux polynômes irréductibles non associés. Quel est le pgcd de P, Q dans $\mathbb{Q}[X]$? En déduire qu'il existe un entier $m \geq 1$ et des polynômes $A, B \in \mathbb{Z}[X]$ tels que $A(X)P(X) + B(X)Q(X) = m$.

Réponse : Le PGCD de P et Q dans $\mathbb{Q}[X]$ est 1.

- Si $\deg P = 0$ ou $\deg Q = 0$, alors P ou Q est inversible dans $\mathbb{Q}[X]$ et donc le PGCD est 1.
- Supposons que $\deg P \geq 1$ et $\deg Q \geq 1$. Ce sont donc des polynômes primitifs et irréductibles dans $\mathbb{Q}[X]$. Soit D est un diviseur commun à P et Q. Si D n'était pas inversible, comme P et Q sont irréductibles, on aurait que D est associé à P et associé à Q, donc P et Q seraient associés, ce qui est contredit par l'hypothèse. À association près, le polynôme D est donc égal à 1.

Par le théorème de Bézout, il existe des polynômes $\tilde{A}, \tilde{B} \in \mathbb{Q}[X]$ tels que $\tilde{A}P + \tilde{B}Q = 1$. En multipliant par le PPCM $m \geq 1$ des dénominateurs des coefficients de $\tilde{A}$ et $\tilde{B}$, on obtient des polynômes $A = m\tilde{A}, B = m\tilde{B} \in \mathbb{Z}[X]$ tels que $AP + BQ = m$.

(e) En déduire que $\mathfrak{p}$ contient un nombre premier p.

Réponse : D'après la question précédente, $\mathfrak{p}$ contient un polynôme constant non nul. Comme $\mathfrak{p}$ est premier, d'après la question (a), $\mathfrak{p}$ contient un facteur irréductible de ce polynôme constant, c'est-à-dire un nombre premier.

(f) Soit $\varphi : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ le morphisme de réduction modulo p. Montrer que $\mathfrak{q} := \varphi(\mathfrak{p})$ est un idéal et que $\mathfrak{p} = \varphi^{-1}(\mathfrak{q})$. En déduire que $\mathfrak{q}$ est un idéal premier non nul.

Réponse : Remarque : en général, l'image d'un idéal n'est pas un idéal. Par exemple, si $f : \mathbb{Z} \to \mathbb{Q}$ est l'unique morphisme, $\mathbb{Z} \subset \mathbb{Z}$ est un idéal mais $f(\mathbb{Z}) = \mathbb{Z}$ n'est pas un idéal de $\mathbb{Q}$. C'est en revanche le cas pour les morphismes surjectifs, comme la preuve suivante le démontre.

L'image d'un sous-groupe par un morphisme de groupes est un sous-groupe donc $\mathfrak{q}$ est bien un sous-groupe (additif) de A. Démontrons que c'est un idéal. Soit $Q \in \mathfrak{q}$ et $R \in \mathbb{F}_p[X]$ deux polynômes. Il existe des polynômes $\tilde{Q} \in \mathfrak{p}, \tilde{R} \in \mathbb{Z}[X]$ tels que $\varphi(\tilde{Q}) = Q$ et $\varphi(\tilde{R}) = R$. Comme $\mathfrak{p}$ est un idéal, on a $\tilde{Q}\tilde{R} \in \mathfrak{p}$. Or $\varphi(\tilde{Q}\tilde{R}) = QR$ est donc un élément de $\mathfrak{q}$. Donc $\mathfrak{q}$ est un idéal.

Démontrons maintenant que $\mathfrak{p} = \varphi^{-1}(\mathfrak{q})$. On a clairement $\mathfrak{p} \subset \varphi^{-1}(\varphi(\mathfrak{p})) = \varphi^{-1}(\mathfrak{q})$. Soit maintenant $\tilde{R} \in \varphi^{-1}(\mathfrak{q})$, c'est-à-dire que l'on a $R = \varphi(\tilde{R}) \in \mathfrak{q}$. Par définition de $\mathfrak{q}$, cela signifie qu'il existe un polynôme $S \in \mathfrak{p}$ tel que $\varphi(S) = R$; on a donc $\varphi(S - \tilde{R}) = 0$. Tous les coefficients de $S - \tilde{R}$ sont donc divisibles par p, donc $S - \tilde{R} \in (p) \subset \mathfrak{p}$. Comme S est également un élément de $\mathfrak{p}$, on en déduit que $\tilde{R} \in \mathfrak{p}$, comme attendu.

Si on avait $\mathfrak{q} = (0)$, on aurait $\mathfrak{p} = \varphi^{-1}(\mathfrak{q}) = \varphi^{-1}((0)) = (p)$, ce qui est absurde car $\mathfrak{p}$ contient au moins deux polynômes irréductibles non associés. Donc $\mathfrak{q} \neq (0)$.

Démontrons enfin que $\mathfrak{q}$ est premier. Soit $Q, R \in \mathbb{F}_p[X]$ deux polynômes et supposons que $QR \in \mathfrak{q}$. Il existe des polynômes $\tilde{Q}, \tilde{R} \in \mathbb{Z}[X]$ tels que $\varphi(\tilde{Q}) = Q$ et $\varphi(\tilde{R}) = R$. Par hypothèse, $\varphi(\tilde{Q})\varphi(\tilde{R}) = QR \in \mathfrak{q}$, donc $\tilde{Q}\tilde{R} \in \mathfrak{p}$. Comme $\mathfrak{p}$ est premier, on a $\tilde{Q} \in \mathfrak{p}$ ou $\tilde{R} \in \mathfrak{p}$, donc $Q \in \mathfrak{q}$ ou $R \in \mathfrak{q}$. Ceci montre que $\mathfrak{q}$ est premier.

(g) Montrer que $\mathfrak{p}$ est engendré par un couple (p, P), où $P \in \mathbb{Z}[X]$ est unitaire et $\varphi(P)$ est irréductible, et que c'est un idéal maximal de $\mathbb{Z}[X]$.

Réponse : L'anneau $\mathbb{F}_p[X]$ est un anneau principal car $\mathbb{F}_p$ est un corps. L'idéal $\mathfrak{q}$ est donc engendré par un polynôme Q, qui est de plus irréductible car $\mathfrak{q}$ est premier. Il existe donc un polynôme $P \in \mathbb{Z}[X]$ tel que $\varphi(P) = Q$. Alors on a $\mathfrak{p} = \varphi^{-1}(\mathfrak{q}) = (p, P)$. En effet, si $R \in \mathfrak{p}$, on a $\varphi(R) \in \mathfrak{q} = (Q)$ donc il existe un polynôme $S \in \mathbb{Z}[X]$ tel que $\varphi(R) = \varphi(S)\varphi(P)$, donc $\varphi(R - SP) = 0$. Comme tous les coefficients de $R - SP$ sont divisibles par p, on a $R - SP \in (p)$, donc $R \in (p, P)$.

Exercice 3. (a) Pour $q = 2, 3, 7$, décomposer le polynôme $X^3 - X - 1$ en produit de facteurs irréductibles dans $\mathbb{F}_q[X]$.

Réponse : Un polynôme non constant de degré ≤ 3 à coefficients dans un corps est irréductible si et seulement si il n'a pas de racine dans $\mathbb{F}_q$. Vérifions donc si le polynôme $P = X^3 - X - 1$ a une racine ou non dans $\mathbb{F}_q$.

- Si $q = 2$, on a $P(0) = 1$ et $P(1) = 1$, donc P n'a pas de racine dans $\mathbb{F}_2$. Il est donc irréductible.
- Si $q = 3$, on a $P(0) = 2$, $P(1) = 2$ et $P(2) = 2$, donc P n'a pas de racine dans $\mathbb{F}_3$. Il est donc irréductible.

- Si $q = 7$, on vérifie que $P(5) = 0$ (et c'est la seule racine), donc P est divisible par $X - 5 = X + 2$ dans $\mathbb{F}_7[X]$. On effectue la division euclidienne de P par $X + 2$ pour trouver

$$P = (X + 2)(X^2 + 5X + 3) \in \mathbb{F}_7[X].$$

On vérifie sans peine que 5 n'est pas racine du second polynôme, donc il est irréductible car de degré ≤ 3.

(b) Démontrer que le polynôme $X^3 - 6X^2 + 9X - 27$ est irréductible dans $\mathbb{Z}[X]$.

Réponse : Le polynôme est primitif et de degré non nul, donc il est irréductible dans $\mathbb{Z}[X]$ si et seulement s'il est irréductible dans $\mathbb{Q}[X]$.

Première méthode, un peu longue. Comme il est de degré 3, il est irréductible si et seulement s'il n'a pas de racines dans $\mathbb{Q}$. Ses racines rationnelles potentielles seraient de la forme p/q avec $p, q \in \mathbb{Z}$ tels que $p \mid -27$ et $q \mid 1$. Comme $27 = 3^3$, les racines rationnelles sont donc à chercher dans l'ensemble :

$$\{\pm 1, \pm 3, \pm 9, \pm 27\}.$$

On vérifie (avec difficulté...) qu'aucun de ces nombres n'est racine de P, donc P est irréductible dans $\mathbb{Q}[X]$ et donc dans $\mathbb{Z}[X]$.

Autre méthode, plus rapide mais plus conceptuelle. On réduit le polynôme P modulo l'idéal premier $\mathfrak{p} = (2)$. On obtient le polynôme $P = X^3 + X + 1 \in \mathbb{F}_2[X]$. Ce polynôme n'admet aucune racine dans $\mathbb{F}_2$, donc il est irréductible dans $\mathbb{F}_2[X]$. De plus, il est de même degré que P. Donc d'après le critère d'irréductibilité modulo un idéal premier, on en déduit que P est irréductible dans $\mathbb{Q}[X]$ et donc dans $\mathbb{Z}[X]$.

(c) Démontrer que le polynôme $2X^3 - 36X^2 - 27X + 21$ est irréductible dans $\mathbb{Z}[X]$.

Réponse : Ce polynôme est primitif et de degré non nul, donc il est irréductible dans $\mathbb{Z}[X]$ si et seulement s'il est irréductible dans $\mathbb{Q}[X]$. On peut lui appliquer le critère d'Eisenstein avec $p = 3$ pour démontrer qu'il est irréductible dans $\mathbb{Q}[X]$. En effet, 3 divise tous les coefficients sauf le coefficient dominant, et 3^2 ne divise pas le terme constant. Le polynôme est donc irréductible.

(d) Lorsque k est un corps, montrer que $Y^2 - X^3 - 1$ est irréductible dans $k[X, Y]$.

Réponse : On voit ce polynôme comme un élément de $A[Y]$, où $A = k[X]$ est factoriel :

$$P = 1 \cdot Y^2 + 0 \cdot Y + (-X^3 - 1) \cdot Y^0.$$

Il est primitif (son coefficient dominant vaut 1) et de degré non nul. Il est donc irréductible si et seulement s'il est irréductible dans $K_A[Y]$, où $K_A = k(X)$ est le corps des fractions rationnelles en X.

Première méthode. Comme $\deg P = 2 \leq 3$, ce polynôme est irréductible si et seulement s'il n'a pas de racine dans K_A. Supposons que $Q/R \in k(X)$ est une

racine de P, où $Q, R \in k[X]$. On a l'équation suivante dans $k(X)$:

$$(Q/R)^2 - (X^3+1) = 0 \iff (Q/R)^2 = X^3+1 \iff Q^2 = R^2(X^3+1).$$

On a donc l'égalité entre les degrés :

$$\deg(Q^2) = \deg(R^2(X^3+1)) \implies 2\deg(Q) = 2\deg(R) + 3.$$

Le nombre de gauche est pair, tandis que le nombre de droite est impair, ce qui est absurde. Donc l'équation $Y^2 = X^3 + 1$ n'a pas de solution $Y \in k[X]$. Le polynôme P n'a donc pas de racine dans K_A, donc il est irréductible dans $K_A[Y]$ et donc dans $A[Y] = k[X,Y]$.
Autre méthode. On peut aussi utiliser le critère d'Eisenstein. Il faut néanmoins distinguer les cas suivant la caractéristique de k.

- Supposons que la caractéristique de k est différente de 3. On considère le polynôme $P = X+1 \in k[X]$, qui est irréductible. Ce polynôme divise tous les coefficients de $Y^2 - (X^3+1) \in k[X][Y]$ sauf le coefficient dominant. De plus, son carré ne divise pas le coefficient constant $X^3 + 1 = (X+1)(X^2 - X + 1)$. En effet, si c'était le cas, comme $k[X]$ est intègre, on aurait que $X+1$ divise $X^2 - X + 1$; or, -1 n'est pas racine de ce second polynôme (car la caractéristique de k est différente de 3), ce qui est absurde. On peut donc appliquer le critère d'Eisenstein pour démontrer que $Y^2 - (X^3+1)$ est irréductible dans $k(X)[Y]$ et donc dans $k[X][Y] = k[X,Y]$ (car il est primitif).
- Supposons maintenant que la caractéristique de k est différente de 2. On voit maintenant $-X^3 + (Y^2 - 1)$ comme un polynôme (primitif) de $k[Y][X]$. On peut appliquer le critère d'Eisenstein avec $Q = Y - 1$, qui divise tous les coefficients sauf le dominant, et son carré ne divise pas le coefficient constant $Y^2 - 1 = (Y-1)(Y+1)$ (car sinon on aurait $1 = -1$ mais la caractéristique n'est pas égale à 2).