

Contrôle Final

Mardi 12 mai 2026 — 10h – 12h

Corrigé

Exercice 1 : (2+1+3 pts) Soit A un anneau (commutatif) et I un idéal de A . On note

$$\sqrt{I} = \{x \in A : \exists n \in \mathbb{N}^* x^n \in I\},$$

le *radical* de I .

1. Montrer que $\sqrt{I}$ est un idéal de A .
2. Montrer que $\sqrt{\sqrt{I}} = \sqrt{I}$.
3. Montrer que pour tout idéal J on a $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$ et $\sqrt{I+J} \supseteq \sqrt{I} + \sqrt{J}$.

Solution.

1. Soient $a, b \in \sqrt{I}$ et $m, n \in \mathbb{N}^*$ avec $a^m, b^n \in I$. Alors

$$(a \pm b)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} a^i b^{m+n-i} \in I,$$

puisque chaque terme est soit un multiple de a^m , soit un multiple de b^n . De plus, pour $c \in A$ on a $(ca)^m = c^m a^m \in I$. Ainsi $\sqrt{I}$ est un idéal.

2. Soit $a \in A$ et $n \in \mathbb{N}^*$ avec $a^n \in \sqrt{I}$. Alors il y a $m \in \mathbb{N}^*$ avec $(a^n)^m \in I$, et donc $a^{mn} \in I$, ce qui montre $a \in \sqrt{I}$ et $\sqrt{\sqrt{I}} \subseteq \sqrt{I}$. Réciproquement, si $a \in I$ on a $a^1 \in I$ et $a \in \sqrt{I}$, ce qui montre $I \subseteq \sqrt{I}$ et donc $\sqrt{I} \subseteq \sqrt{\sqrt{I}}$.
3. Si $a^n \in I \cap J$ alors $a^n \in I$, ce qui montre $\sqrt{I \cap J} \subseteq \sqrt{I}$, et par symétrie $\sqrt{I \cap J} \subseteq \sqrt{I} \cap \sqrt{J}$. Réciproquement, soit $a \in \sqrt{I} \cap \sqrt{J}$. Alors il y a $m, n \in \mathbb{N}^*$ avec $a^m \in I$ et $a^n \in J$, et donc $a^k \in I \cap J$, où $k = \max\{m, n\}$. Ainsi $a \in \sqrt{I \cap J}$, et $\sqrt{I} \cap \sqrt{J} \subseteq \sqrt{I \cap J}$. On a donc égalité.

La somme $I + J$ est un idéal qui contient I et J . Donc si $a^n \in \sqrt{I}$ trivialement $a^n \in I + J$ et $\sqrt{I} \subseteq \sqrt{I+J}$; de même $\sqrt{J} \subseteq \sqrt{I+J}$. Puisqu'un idéal est clos par addition, $\sqrt{I} + \sqrt{J} \subseteq \sqrt{I+J}$.

Exercice 2 : (2+1+3+1 pts) Soit A l'ensemble des suites rationnelles convergentes (mais dont la limite peut être irrationnelle), et I le sous-ensemble des suites rationnelles convergentes vers 0. Dans cet exercice vous pouvez utiliser librement des résultats connus sur les suites.

1. Montrer que l'addition et la multiplication de suites fait de A un anneau (commutatif) unitaire.
2. Montrer que I est un idéal dans A .
3. Montrer que tout élément de $A \setminus I$ est inversible dans A modulo I . En déduire que I est un idéal maximal de A , et que A/I est un corps.
4. Montrer que $\lim_{n \rightarrow \infty}$ donne un isomorphisme d'anneau unitaire entre A/I et $\mathbb{R}$.

Remarque : Une suite $(u_n)_n$ est convergente ssi $\forall k \in \mathbb{N}^* \exists N \in \mathbb{N} \forall j, \ell > N |u_j - u_\ell| < 1/k$ (suite de Cauchy). Ainsi la définition de l'ensemble A n'a pas besoin de l'existence *a priori* de $\mathbb{R}$. Ceci donne donc une construction de $\mathbb{R}$ à partir de $\mathbb{Q}$.

Solution.

1. La somme, la différence et le produit de deux suites rationnelles convergentes est une suite rationnelle convergente, avec

$$\lim_{\infty}(u_n \pm v_n) = \lim_{\infty} u_n \pm \lim_{\infty} v_n \quad \text{et} \quad \lim_{\infty}(u_n v_n) = \lim_{\infty} u_n \lim_{\infty} v_n.$$

Ainsi A est un sous-anneau de l'anneau des suites réelles. Alternativement, on voit facielement que la somme et le produit sont associatives et commutatives, on a la loi distributive, la suite constante $(0)_n$ est élément neutre additif, la suite constante $(1)_n$ est élément neutre multiplicatif, et la suite $(-u_n)_n$ est l'inverse additif de la suite $(u_n)_n$. Donc A est un anneau commutatif unitaire.

- Si $\lim_{\infty} u_n = 0 = \lim_{\infty} v_n$, alors $\lim_{\infty} (u_n \pm v_n) = 0$. De plus $(0)_n \in I$, et I est un sous-groupe additif. Si $(w_n)_n \in A$, alors $(w_n)_n$ est convergente et donc borné, et $(w_n u_n)_n$ converge toujours vers 0. Ainsi I est un idéal.
- Si $(u_n)_n \in A \setminus I$, alors $u_n \neq 0$ à partir d'un certain rang N , et on pose $v_n = 1$ si $n < N$ et $v_n = 1/u_n$ si $n \geq N$. Notons que $(v_n)_n \in A$ puisque $\lim_{\infty} v_n = 1/\lim_{\infty} u_n$. Alors $(u_n)_n(v_n)_n$ est égal à $(1)_n$ à partir du rang N , et $(u_n)_n(v_n)_n - (1)_n \in I$. Ceci montre que $(u_n)_n$ est inversible modulo I , et $(1)_n \in (I, (u_n)_n)$, ce qui implique $(I, (u_n)_n) = A$. Donc I est un idéal maximal. D'après un théorème du cours, A/I est un corps.
- On considère l'application $f : A \rightarrow \mathbb{R}$ donnée par $f((u_n)_n) = \lim_{\infty} u_n$. Comme la limite d'une somme, différence ou produit de deux suites convergentes est la somme, différence ou produit de leurs limites, et $f((0)_n) = 0$ et $f((1)_n) = 1$, l'application f est un morphisme d'anneaux unitaires. Son noyau est clairement I . De plus f est surjectif, puisque chaque réel est la limite d'une suite rationnelle par densité de $\mathbb{Q}$ dans $\mathbb{R}$. Donc f induit un isomorphisme entre A/I et $\mathbb{R}$.

Exercice 3 : (3 pts) Soit K un corps et P un polynôme sur K de degré n . Montrer que si P n'a pas de racine dans une extension de K de degré inférieur ou égale à $n/2$, alors P est irréductible sur K .

Solution. Supposons P réductible. Alors il y a deux polynômes $Q, R \in K[X]$ non-inversibles avec $P = QR$. Puisque $n = \deg P = \deg Q + \deg R$, et la non-inversibilité implique $\deg Q, \deg R > 0$, on a $\deg Q \leq n/2$ ou $\deg R \leq n/2$. Par symétrie on peut supposer $\deg Q \leq n/2$. D'après un théorème du cours, Q (et donc P) a une racine dans une extension de K de degré au plus $\deg Q \leq n/2$. Le résultat en découle par contraposée.

Exercice 4 : (2+2 pts) En utilisant les réductions mod 2 ou mod 3, montrer que les polynômes suivants sont irréductibles dans $\mathbb{Z}[X]$:

$$(a) -5X^5 + 8X^4 + 4X^3 - 2X^2 + 5 \quad (b) X^4 + 2X^3 - 13X^2 + 6X - 11.$$

Solution.

- (a) La réduction modulo 2 donne $X^5 + 1 = (X + 1)(X^4 + X^3 + X^2 + X + 1)$. Or, ni 0 ni 1 est racine de $X^4 + X^3 + X^2 + X + 1$ dans $\mathbb{F}_2$, et le seul polynôme irréductible dans $\mathbb{F}_2[X]$ de degré 2 est $X^2 + X + 1$, qui ne divise pas $X^4 + X^3 + X^2 + X + 1$. Donc $X^4 + X^3 + X^2 + X + 1$ est irréductible sur $\mathbb{F}_2$.

La réduction modulo 3 donne $X^5 - X^4 + X^3 + X^2 - 1$, qui est annulé par -1 , mais pas par 0 ni 1 modulo 3. Mais si le polynôme était réductible sur $\mathbb{Z}$, il y aurait donc un facteur linéaire $X - z$ avec $z \equiv 1 \pmod{2}$ et $z \equiv -1 \pmod{3}$, soit $z \equiv -1 \pmod{6}$.

On note que $|z| > \frac{8+4+2+2}{5} = \frac{19}{5}$, alors $|-5z^5| > |8z^4 + 4z^3 - 2z^2 + 5|$ et $-5z^5 + 8z^4 + 4z^3 - 2z^2 + 5 \neq 0$. Il n'y a donc pas de solution entière pour $z \geq 5$. Le seul entier dans $] -5, 5[$ congru à $-1 \pmod{6}$ est -1 , qui n'est pas racine du polynôme. Il n'y a donc pas de facteur linéaire sur $\mathbb{Z}$, et le polynôme est irréductible sur $\mathbb{Z}$.

- (b) La réduction modulo 2 donne $X^4 + X^2 + 1 = (X^2 + X + 1)^2$, et $X^2 + X + 1$ est irréductible sur $\mathbb{F}_2$. La réduction modulo 3 donne $X^4 - X^3 - X^2 + 1 = (X - 1)(X^3 - X - 1)$. Or, $X^3 - X - 1$ n'est pas annulé par 0, 1 ou -1 modulo 3, et est donc irréductible sur $\mathbb{F}_3$. Puisque les degrés (2, 2) et (1, 3) de la décomposition modulo 2 et modulo 3 sont différents, d'après un théorème du cours le polynôme est irréductible.

Exercice 5 : (1+1+2+2+2 pts) On rappelle que le $n^{\text{ième}}$ polynôme cyclotomique est $\Phi_n(X) = \prod_{\zeta \in \mathbb{U}_n^*} (X - \zeta)$, où $\mathbb{U}_n^*$ est l'ensemble des racines primitives $n^{\text{ièmes}}$ de 1, et que $\Phi_n \in \mathbb{Z}[X]$ pour tout $n \in \mathbb{N}$. Le but de cet exercice est de montrer que Φ_8 est réductible sur tout corps fini.

- Montrer que $\Phi_8(X) = X^4 + 1$.
- Donner la décomposition de Φ_8 dans $\mathbb{F}_2$.
- Soit p premier impair. Montrer que $p^2 - 1 \equiv 0 \pmod{8}$. En déduire que $\mathbb{F}_{p^2}^\times$ contient toujours un élément a d'ordre 8.
- En déduire que Φ_8 est scindé sur $\mathbb{F}_{p^2}$.
- Conclure.

Solution.

1. Les racines non-primitives 8ièmes sont les racines 4ièmes de 1, donc les racines de $X^4 - 1$. Ainsi

$$\Phi_8(X) = \frac{X^8 - 1}{X^4 - 1} = X^4 + 1.$$

2. Sur $\mathbb{F}_2$ on a $X^4 + 1 = (X + 1)^4$, puisque $(x + y)^2 = x^2 + y^2$ en caractéristique 2.
3. Si p est impair, on a que $4 \mid p + 1$ ou $4 \mid p - 1$, et $2 \mid p \pm 1$. Ainsi $8 = 2 \cdot 4 \mid (p - 1)(p + 1) = p^2 - 1$, et $p^2 - 1 \equiv 0 \pmod{8}$. Or, $F_{p^2}^\times$ est un groupe cyclique d'ordre $p^2 - 1$ d'après un théorème du cours, qui contient donc un élément a d'ordre 8.
4. L'élément a de la question précédente est une racine primitive 8ième. On a donc $a^8 - 1 = 0$ et $a^4 - 1 \neq 0$. Ainsi a est racine de $X^8 - 1$ mais pas de $X^4 - 1$; puisque $X^8 - 1 = (X^4 - 1)(X^4 + 1)$ on a que a est racine de $X^4 + 1 = \Phi_8(X)$. Les autres racines primitives 8ièmes sont a^3 , a^5 et a^7 , qui sont également racines de $X^4 - 1$. Ainsi

$$\Phi_8(X) = X^4 + 1 = (X - a)(X - a^3)(X - a^5)(X - a^7)$$

est scindé sur $\mathbb{F}_{p^2}$.

5. Le polynôme minimal de a sur $\mathbb{F}_p$ est un facteur irréductible de $X^4 - 1$ de degré au plus 2. Ainsi Φ_8 est réductible sur $\mathbb{F}_p$.