

Examen Session 2 : Vendredi 19 Juin 2026, 9h-11h30.

Aucun document, aucun appareil électronique n'est autorisé (téléphone, calculatrice, ...).  
Le nombre total de points est 20.

Exercice 1 : Image réciproque d'un idéal premier

Total de la partie 1 : 11 pts

Soient  $A$  et  $B$  deux anneaux commutatifs. Soit  $f : A \rightarrow B$  un morphisme d'anneaux de  $A$  vers  $B$ . Soit  $I$  un idéal de  $B$ . On désigne l'image réciproque  $f^{-1}(I)$  de  $I$  par  $\bar{I}$ .

- (a) (1 point) Montrer que  $\bar{I}$  est un idéal de  $A$ .

**Solution:**  $f(0) = 0 \in I$ . Donc  $0 \in \bar{I}$ . Soient  $x$  et  $y \in \bar{I}$ . Alors  $f(x)$  et  $f(y)$  appartiennent à  $I$ . Donc  $f(x + y) = f(x) + f(y) \in I$ . Donc  $x + y \in \bar{I}$ . Et  $f(-x) = -f(x) \in I$ . Donc  $-x \in \bar{I}$ . Nous avons donc montré que comme  $f$  est un morphisme de groupes, l'image réciproque d'un sous-groupe de  $B$  est un sous-groupe de  $A$ .

Soient  $a \in A$  et  $x \in \bar{I}$ . Alors  $f(ax) = f(a)f(x) \in I$ . Donc  $ax \in \bar{I}$ .

- (b) (1 point) Montrer qu'il existe une unique application  $\bar{f} : A/\bar{I} \rightarrow B/I$  telle que la classe d'équivalence de  $a$  dans  $A/\bar{I}$  s'envoie sur la classe d'équivalence de  $f(a)$  dans  $B/I$ , pour tout  $a \in A$ .

**Solution:** l'unicité est claire, car les éléments de  $A/\bar{I}$  sont les classes d'équivalence des éléments de  $A$  et on a défini leur image.

Existence : il faut montrer que la classe d'équivalence  $\overline{f(a)}$  de  $f(a)$  dans  $B/I$  ne dépend que de la classe d'équivalence  $\bar{a}$  de  $a$  dans  $A/\bar{I}$ . C'est à dire pour tout  $a, b \in A$ , si  $\bar{a} = \bar{b}$  alors  $\overline{f(a)} = \overline{f(b)}$ . Preuve : supposons que  $\bar{a} = \bar{b}$  alors  $a - b \in \bar{I}$ . Alors  $f(a) - f(b) = f(a - b) \in I$ . Donc  $\overline{f(a)} = \overline{f(b)}$ .

- (c) (1 point) Montrer que  $\bar{f}$  est un morphisme d'anneaux.

**Solution:** Par définition,  $\overline{f(\bar{a})} = \overline{f(a)}$ ,  $\bar{0} = 0$ ,  $\overline{a + b} = \overline{a + b}$ ,  $\overline{ab} = \overline{ab}$  dans  $A/\bar{I}$  et dans  $B/I$ . Donc  $\overline{f(\bar{0})} = \overline{f(0)} = \bar{0}$ ,

$$\overline{f(\bar{a} + \bar{b})} = \overline{f(a + b)} = \overline{f(a) + f(b)} = \overline{f(a)} + \overline{f(b)} = \overline{f(\bar{a})} + \overline{f(\bar{b})}.$$

de même, on montre que  $\overline{f(\bar{a}\bar{b})} = \overline{f(\bar{a})f(\bar{b})}$  et que  $f(\bar{1}) = \bar{1}$ .

- (d) (1 point) Montrer que  $\bar{f}$  est injectif.

**Solution:** Soit  $\bar{a} \in \ker \bar{f} \subset A/\bar{I}$ . Alors  $\bar{f}(\bar{a}) = \overline{f(a)} = 0$ . Donc  $f(a) \in I$ . Donc  $a \in \bar{I}$ . Donc  $\bar{a} = 0$ . Donc  $\ker \bar{f} = \{0\}$ . Donc  $\bar{f}$  est injectif.

- (e) (1 point) Montrer que si  $I$  est un idéal premier de  $B$  (en particulier différent de  $B$ ) alors  $\bar{I}$  est un idéal premier de  $A$  (en particulier différent de  $A$ ).

**Solution:** Supposons que  $\bar{I} = A$ . Alors  $1 \in \bar{I}$ . Donc  $1 = f(1) \in I$ . Donc  $I = B$ . Comme  $I \neq B$ ,  $\bar{I} \neq A$ . Soient  $a$  et  $b$  deux éléments de  $A$  tel que  $ab \in \bar{I}$ . Alors  $f(a)f(b) = f(ab) \in I$ . Comme  $I$  est premier, cela implique que  $f(a) \in I$  (ou  $f(b) \in I$ ), c'est à dire  $a \in \bar{I}$ .

Seconde preuve : comme  $I$  est un idéal premier de  $B$ ,  $B/I$  est un anneau intègre. Comme  $\bar{f}$  est un morphisme injectif d'anneaux,  $A/\bar{I}$  est aussi un anneau intègre. Donc  $\bar{I}$  est un idéal premier.

- (f) (1 point) Montrer que si  $B$  est un anneau intègre, le noyau de  $f$ ,  $\ker f$ , est un idéal premier de  $A$ .

**Solution:** Si  $B$  est un anneau intègre, alors  $I = \{0\}$  est un idéal premier. D'après ce qui précède,  $\ker f = f^{-1}(I) = \bar{I}$  est un idéal premier de  $A$ .

Cette question a déjà été démontré dans l'exo 1 de l'examen de Mai 2026. D'ailleurs, a) et e) sont de simples generalisations de cet exo 1 de l'examen de Mai 2026 dans le cas où  $I$  n'est pas l'idéal trivial  $\{0\}$ .

- (g) (2 points) En déduire que si  $I$  est un idéal premier de  $A$  alors l'ensemble  $I[X]$  des polynômes à coefficients dans  $I$  est un idéal premier de  $A[X]$ . Indication : considérer l'application naturelle  $\varphi : A[X] \rightarrow (A/I)[X]$  donnée par la réduction modulo  $I$  de chacun des coefficients d'un polynôme de  $A[X]$ .

**Solution:** [?, 9.1 Proposition 2]. L'application de passage au quotient  $A \rightarrow A/I$  est un morphisme d'anneaux. Donc elle induit un unique morphisme d'anneaux  $\varphi : A[X] \rightarrow (A/I)[X]$  qui la prolonge et qui envoie l'indéterminée  $X$  de  $A[X]$  sur l'indéterminée  $X$  de  $(A/I)[X]$ . Son noyau est  $I[X]$ . Comme  $I$  est un idéal premier de  $A$ , alors l'anneau  $A/I$  est intègre. Donc l'anneau  $(A/I)[X]$  des polynômes sur  $A/I$  est lui aussi intègre. D'après f),  $I[X]$  le noyau de  $\varphi$ ,  $\ker \varphi$  est un idéal premier.

- (h) (2 points) On suppose que  $f$  est surjectif. Montrer que si  $I$  est un idéal maximal alors  $\bar{I}$  est aussi maximal. Indication : on pourra montrer que  $\bar{f}$  est un isomorphisme d'anneaux.

**Solution:** Supposons que  $f$  est surjectif. Alors  $\bar{f}$  est clairement surjectif. Preuve : pour tout  $b \in B$ , il existe  $a \in A$  tel que  $f(a) = b$ . Donc soit  $\bar{b} \in B/I$ . Comme  $f$  est surjectif, il existe  $a \in A$  tel que  $f(a) = b$ . Donc  $\bar{f}(\bar{a}) = \overline{f(a)} = \bar{b}$ . Donc  $\bar{f}$  est surjectif. Comme  $\bar{f}$  est un morphisme d'anneaux et injectif,  $\bar{f}$  est un isomorphisme d'anneaux. Donc si  $I$  est un idéal maximal, alors  $B/I$  est un corps. Par l'isomorphisme,  $A/\bar{I}$  est aussi un corps donc  $\bar{I}$  est un idéal maximal. Seconde preuve directe en utilisant la définition d'idéal maximal.

- (i) (1 point) Donner un exemple de morphisme d'anneaux  $f : A \rightarrow B$  non surjectif et d'idéal maximal  $I$  de  $B$  tel que  $\bar{I}$  ne soit pas maximal.

**Solution:** On reprend les exemples donnés dans l'exercice 1 de l'examen de Mai 2026 qui correspondent au cas où  $I = \{0\}$ .

Prenons  $B = \mathbb{Q}$ . Alors comme  $\mathbb{Q}$  est un corps,  $I = \{0\}$  est un idéal maximal de  $B$ .

$A = \mathbb{Z}$  est un anneau intègre mais pas un corps donc  $(0)$  est un idéal premier mais pas un idéal maximal. Soit  $f : \mathbb{Z} \rightarrow \mathbb{Q}$  l'inclusion des entiers dans les rationnels. Alors  $f$  est injectif donc  $\ker f = \{0\}$ . Si  $A$  est un anneau principal alors tout idéal premier non nul est maximal. Donc pour trouver un exemple d'idéal premier non nul et maximal, il faut considérer un anneau non principal, par exemple  $A = \mathbb{Z}[X]$ . Soit  $ev : \mathbb{Z}[X] \rightarrow \mathbb{Q}$  l'application qui à tout polynôme  $P$  à coefficients entiers associe son terme constant  $P(0)$ . Alors  $ev$  est un morphisme d'anneaux d'image  $\mathbb{Z}$  et de noyau  $(X)$ , l'idéal principal engendré par le monôme  $X$ . Donc  $\mathbb{Z}[X]/(X)$  est isomorphe à  $\mathbb{Z}$ . Comme  $\mathbb{Z}$  est intègre,  $(X)$  est un idéal premier. Comme  $\mathbb{Z}$  n'est pas un corps,  $(X)$  n'est pas un idéal maximal. Donc  $\mathbb{Z}[X]$  n'est pas un anneau principal.

### Exercice 2 : Théorème des restes chinois

Total de la partie 2 : 5 pts

- (a) (2 points) Trouver tous les polynômes réels  $P$  tel que  
 -le reste de la division euclidienne de  $P$  par  $X^2 + X - 5$  soit le polynôme  $3X + 3$   
 -et le reste de la division euclidienne de  $P$  par  $2X - 4$  soit le polynôme constant 7.

**Solution:** Soient  $A = X^2 + X - 5$  et  $B = 2X - 4$ . Les polynômes  $A$  et  $B$  sont premiers entre eux. Car  $B$  polynôme de degré 1 est irréductible ne divise pas le polynôme  $A$  car 2 n'est pas racine de  $A$ . Soit  $U = 1$  et  $V = -\frac{1}{2}(X + 3)$ . alors

$$AU + BV = X^2 + X - 5 - (X - 2)(X + 3) = X^2 + X - 5 - (X^2 - 2X + 3X - 6) = 1.$$

En particulier  $BV \equiv 1 \pmod{A}$  et  $BV \equiv 0 \pmod{B}$ ,  $AU \equiv 0 \pmod{A}$  et  $AU \equiv 1 \pmod{B}$ .

Soit

$$P_0 = BV(3X + 3) + AU(7) = -(X - 2)(X + 3)(3X + 3) + 7(X^2 + X - 5)$$

$$\begin{aligned}
&= -(X^2+X-6)3(X+1)+7(X^2+X-5) = -3(X^3+X^2-6X+X^2+X-6)+7(X^2+X-5) \\
&= -3(X^3 + 2X^2 - 5X - 6) + 7X^2 + 7X - 35 = -3X^3 + X^2 + 22X - 17.
\end{aligned}$$

Donc  $P_0 \equiv 3X + 3 \pmod{A}$  et  $P_0 \equiv 7 \pmod{B}$ .

Donc d'après le théorème des restes chinois, l'ensemble des  $P$  tel que  $P \equiv 3X + 3 \pmod{A}$  et  $P \equiv 7 \pmod{B}$  est l'ensemble des polynômes  $P$  tel que  $P \equiv P_0 \pmod{AB}$ .  $AB = 2X^3 + 2X^2 - 10X - 4X^2 - 4X + 20 = 2X^3 - 2X^2 - 14X + 20$ . Donc  $P_0 + 3/2(AB) = -3X^3 + X^2 + 22X - 17 + 3/2(2X^3 - 2X^2 - 14X + 20) = -2X^2 + X + 13$ . Bilan : les polynômes réels  $P$  tel que

-le reste de la division euclidienne de  $P$  par  $X^2 + X - 5$  soit le polynôme  $3X + 3$   
-et le reste de la division euclidienne de  $P$  par  $2X - 4$  soit le polynôme  $7$   
sont les polynômes réels  $P$  que le reste de la division euclidienne de  $P$  par  $2X^3 - 2X^2 - 14X + 20$  soit le polynôme  $-2X^2 + X + 13$ .

- (b) (3 points) Trouver tous les polynômes réels  $P$  tel que  
-le reste de la division euclidienne de  $P$  par  $X^3 - X^2$  soit le polynôme  $X^2 + X + 1$   
-et le reste de la division euclidienne de  $P$  par  $X^2 - 3X + 2$  soit le polynôme  $5X - 2$ .

**Solution:** Soient  $A = X^3 - X^2$  et  $B = X^2 - 3X + 2$ . Alors  $A = X^2(X - 1)$  et  $B = (X - 1)(X - 2)$ . Donc es polynômes  $A$  et  $B$  ont pour pgdc  $A \wedge B = (X - 1)$ . Soit  $P$  un polynôme réel tel que

$$\begin{cases} P \equiv X^2 + X + 1 & \pmod{X^3 - X^2} \\ P \equiv 5X - 2 & \pmod{X^2 - 3X + 2} \end{cases}$$

Alors

$$\begin{cases} P \equiv X^2 + X + 1 & \pmod{X - 1} \\ P \equiv 5X - 2 & \pmod{X - 1} \end{cases}$$

Or les polynômes  $X^2 + X + 1$  et  $5X - 2$  prennent tous les deux, la valeur 3 pour  $X = 1$ . Donc  $X^2 + X + 1 \equiv 3 \pmod{X - 1}$  et  $5X - 2 \equiv 3 \pmod{X - 1}$ . Donc  $P \equiv 3 \pmod{X - 1}$ . Soit  $Q$  tel que  $P = Q(X - 1) + 3$ . Alors comme  $X^2 + X + 1 - 3 = (X - 1)(X + 2)$  et  $5X - 2 - 3 = 5(X - 1)$ , en retranchant 3 puis en divisant par  $(X - 1)$ ,

$$\begin{cases} P \equiv X^2 + X + 1 & \pmod{X^3 - X^2} \\ P \equiv 5X - 2 & \pmod{X^2 - 3X + 2} \end{cases}$$

$$\Leftrightarrow \begin{cases} Q \equiv X + 2 & \pmod{X^2} \\ Q \equiv 5 & \pmod{X - 2} \end{cases}$$

Nous allons maintenant pouvoir appliquer le théorème des restes chinois comme à la question précédente pour trouver  $Q$ .

$$\frac{1}{4}X^2 - \frac{1}{4}(X+2)(X-2) = 1.$$

En particulier  $-\frac{1}{4}(X^2 - 4) \equiv 1 \pmod{X^2}$  et  $-\frac{1}{4}(X^2 - 4) \equiv 0 \pmod{X-2}$ ,  
 $\frac{1}{4}X^2 \equiv 0 \pmod{X^2}$  et  $\frac{1}{4}X^2 \equiv 1 \pmod{X-2}$ .

Soit  $Q_0 = 5\frac{1}{4}X^2 - (X+2)\frac{1}{4}(X^2 - 4) = \frac{1}{4}(5X^2 - (X^3 - 4X + 2X^2 - 8)) =$   
 $\frac{1}{4}(-X^3 + 3X^2 + 4X + 8)$ . Alors  $Q_0 \equiv X+2 \pmod{X^2}$  et  $Q_0 \equiv 5 \pmod{X-2}$ .  
 Comme  $Q_0 + \frac{1}{4}X^2(X-2) = \frac{1}{4}(-X^3 + 3X^2 + 4X + 8 + X^3 - 2X^2) = \frac{1}{4}(X^2 + 4X + 8)$ ,  
 $\frac{1}{4}(X^2 + 4X + 8) \equiv X+2 \pmod{X^2}$  et  $\frac{1}{4}(X^2 + 4X + 8) \equiv 5 \pmod{X-2}$ . Donc  
 d'après le théorème des restes chinois,  $Q \equiv X+2 \pmod{X^2}$  et  $Q \equiv 5 \pmod{X-2}$   
 ssi  $Q = \frac{1}{4}(X^2 + 4X + 8) \pmod{X^2(X-2)}$  ssi  $P = \frac{1}{4}(X^2 + 4X + 8)(X-1) + 3$   
 $\pmod{X^2(X-2)(X-1)} = \frac{1}{4}(X^3 + 3X^2 + 4X + 4) \pmod{X^2(X-2)(X-1)}$ .

### Exercice 3 : Irréductibilités

Total de la partie 3 : 4 pts

- (a) (2 points) Le polynôme  $27X^2 - 18X - 21$  est-il irréductible dans  $\mathbb{Q}[X]$ ? dans  $\mathbb{Z}[X]$ ?

**Solution:** Soit  $P = 27X^2 - 18X - 21 = 3(9X^2 - 6X - 7)$ . Or 3 et  $9X^2 - 6X - 7$   
 ne sont pas des polynômes inversibles de  $\mathbb{Z}[X]$ . Donc  $P$  est réductible dans  $\mathbb{Z}[X]$ .  
 Donnons les racines de  $9X^2 - 6X - 7$ . Alors  $\Delta' = 9 + 7 \times 9 = 72 = 8 \times 9$ . Les  
 racines réelles de  $P$  sont  $\frac{3 \pm 3\sqrt{8}}{9} = \frac{1 \pm 2\sqrt{2}}{3}$ . Ces racines ne sont pas des rationnels.  
 Donc  $P$  n'admet pas de racines dans  $\mathbb{Q}$  donc  $P$  est irréductible dans  $\mathbb{Q}[X]$ .

- (b) (2 points) Donner la décomposition de  $15 + 21i$  en facteurs irréductibles dans l'an-  
 neau de Gauss  $\mathbb{Z}[i]$ .

**Solution:**  $15 + 21i = 3(5 + 7i)$ .

$$(5 + 7i)(5 - 7i) = 25 + 49 = 74 = 2 \times 37 = (1 + i)(1 - i) \times (6 + i)(6 - i).$$

$$\frac{5 + 7i}{1 + i} = \frac{(5 + 7i)(1 - i)}{(1 + i)(1 - i)} = \frac{5 + 2i - 5i - 7i^2}{2} = \frac{12 + 2i}{2} = 6 + i.$$

Donc  $5 + 7i = (1 + i)(6 + i)$  et  $15 + 21i = 3(1 + i)(6 + i)$ .