Exercice 89 (radical)**.** Soit I un idéal d'un anneau A. on appelle *radical* de I l'ensemble

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

(1) Montrer que $\sqrt{I}$ est un idéal de A.
(2) En déduire que l'ensemble des nilpotents d'un anneau est un idéal.
(3) Montrer que si J est un autre idéal $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$
(4) Calculer $\sqrt{2\mathbb{Z}}$, $\sqrt{4\mathbb{Z}}$ et $\sqrt{6\mathbb{Z}}$
(5) Plus généralement, montrer que si p est premier alors $\sqrt{p^n\mathbb{Z}} = p\mathbb{Z}$.
(6) Déterminer $\sqrt{n\mathbb{Z}}$ dans le cas général.

Exercice 90. Dans $\mathbb{Z}[X]$, l'anneau des polynomes à coefficients entiers. On considère le sous-ensemble $I = \{P \in \mathbb{Z}[X] | P(0) \text{ est divisible par } 5\}$

(1) Montrer que I est un idéal mais n'est pas principal
(2) Déterminer deux polynomes P et Q tels que $I = (P, Q)$.

Exercice 91. On considère l'anneau $\mathbb{Z}[i]$ des entiers de Gauss. Soit ϕ l'application définie par :

$$\phi : \mathbb{Z}[i] \longrightarrow \mathbb{Z}/10\mathbb{Z}$$
$$(a + ib) \longmapsto \bar{a} + 3\bar{b}$$

(1) Montrer que ϕ est un morphisme d'anneau.
(2) En déduire que $\mathbb{Z}[i]/(1 + 3i)$ est isomorphe à $\mathbb{Z}/10\mathbb{Z}$

Exercice 92 (Théorème chinois)**.** Soient I et J deux idéaux d'un anneau commutatif unitaire. On suppose que I et J sont étrangers, c'est à dire $I + J = A$.

(1) Montrer que $(A/I) \times (A/J)$ est isomorphe à $A/(I \cdot J)$.
(2) Soit $J_1, \ldots, J_k$ des idéaux. Montrer que si I est étranger avec chacun des $J_1, \ldots, J_k$, alors il est étranger avec $(J_1 \cdots J_k)$.
(3) En déduire que si $I_1, \ldots, I_k$ sont des idéaux étrangers deux à deux on a $(A/I_1) \times \cdots \times (A/I_k)$ est isomorphe à $A/(I_1 \cdots I_k)$
(4) En déduire que si $n_1, \ldots, n_k \in \mathbb{Z}$ sont premiers entre eux, alors on a le Théorème des restes chinois :

$$(\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z}) \cong \mathbb{Z}/(n_1 \cdots n_k)\mathbb{Z}$$

Exercice 93 (Quotient de polynômes)**.**
On se place dans l'anneau des polynômes. Pour un polynome P, on notera $\mathbb{R}[X]/(P)$ l'anneau quotient de $\mathbb{R}[X]$ par l'idéal engendré par P.

(1) Montrer que $\mathbb{R}[X]/(X - 1)$ et $\mathbb{R}[X]/(X + 1)$ sont tous les deux isomorphes à $\mathbb{R}$.
(2) Montrer que $\mathbb{R}[X]/(X^2 - 1)$ est isomorphe à l'anneau produit $\mathbb{R} \times \mathbb{R}$.
(3) Montrer que $\mathbb{R}[X]/(X^2)$ n'est pas isomorphe à l'anneau $\mathbb{R} \times \mathbb{R}$.
(4) On définit la loi de composition $\otimes$ sur $\mathbb{R}^2$ par $(a, b) \otimes (a', b') = (aa' + bb', ab' + ba')$. Montrer que $(\mathbb{R}^2, +, \otimes)$ est un anneau isomorphe à $\mathbb{R}[X]/X^2$.

Exercice 94. Montrer que l'anneau $\mathbb{R}[X]/(X^2 + 1)$ est isomorphe à $\mathbb{C}$.

Exercice 95. on se place dans l'anneau $\mathbb{Z}[X]$.

(1) Montrer que l'idéal engendré par 2 et X n'est pas principal.
(2) En déduire que l'idéal principal (X) est premier mais n'est pas maximal.

Exercice 96. Soit Soit A, B deux anneaux commutatifs unitaires, et $f : A \to B$ un morphisme d'anneaux unitaire. Soit J un idéal de B et $I = f^{-1}(J)$ (on rappelle que I est également un idéal).

(1) Montrer que si J est premier alors I est premier.
(2) On se place dans le cas où f est surjective et J est maximal.
    (a) Montrer que si $x \notin I$ alors il existe $y \in A$ tel que $f(xy) - 1 \in J$.
    (b) En déduire que $\overline{x}$ est inversible dans A/I.
    (c) Conclure que I est maximal.
(3) Trouver un exemple avec J maximal, et $f^{-1}(J)$ n'est pas maximal. (Penser à $\mathbb{Z}(X)$ et $\mathbb{R}(X)$)

Exercice 97. Soit A un anneau commutatif non nul tel que tout idéal différent de A est premier. Montrer que A est un corps.

Exercice 98. Soit P un idéal premier non nul d'un anneau A. On suppose que P est principal. Soit I un anneau principal tel que $P \subset I$. Montrer que $I = P$ ou bien $I = A$.

Exercice 99 (Divisibilité dans les entiers de Gauss).
On se place dans l'anneau des entiers de Gauss $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$.
Pour $z = a + ib \in \mathbb{Z}[i]$ On définit $N(z) = |z|^2 = a^2 + b^2$.

(1) En utilisant le fait que $N(xy) = N(x)N(y)$, déterminer tous les inversibles de $\mathbb{Z}[i]$.
(2) Montrer que si $N(z)$ est un nombre premier alors z est irreductible.
(3) Montrer que pour tout $z \in \mathbb{Z}[i]$, on a $N(z) \neq 3$. En déduire que 3 est irreductible dans $\mathbb{Z}[i]$.
(4) Montrer que 5 n'est pas un irreductible dans $\mathbb{Z}[i]$.
(5) Parmi les nombres $2, 3, 5, 7, 11, 13, 17, 19$ (qui sont premiers dans $\mathbb{Z}$), déterminer lesquels sont irréductibles dans $\mathbb{Z}[i]$.

Exercice 100.
Soit A un anneau intègre commutatif et unitaire.

(1) Montrer que les inversibles de $A[X]$ sont les polynômes constants $P(X) = a$ avec a inversible dans A.
(2) Montrer que tout élément irreductible de A est un élément irreductible de $A[X]$.
(3) Lorsque $A = \mathbb{Z}/4\mathbb{Z}$, déterminer un polynome de $A[X]$ qui soit non constant et inversible.

Exercice 101. On regarde l'anneau $\mathbb{Z}[\sqrt{10}] = \{a + b\sqrt{10} | a, b \in \mathbb{Z}\}$.

(1) Montrer que $a + b\sqrt{10}$ est inversible dans $\mathbb{Z}[\sqrt{10}]$ si et seulement si $a^2 - 10b^2 = \pm 1$.
(2) Montrer que l'équation $a^2 - 10b^2 = 2$ n'a pas de solutions dans $\mathbb{Z}$.
(3) En déduire que 2 est irreductible dans l'anneau $\mathbb{Z}[\sqrt{10}]$.
(4) En écrivant 10 de deux façons différentes dans $\mathbb{Z}[\sqrt{10}]$, montrer que 2 n'est pas premier.

Exercice 102 (L'anneau des entiers de Gauss est Euclidien)**.**
On va montrer que l'anneau $\mathbb{Z}[i]$ est euclidien. Soit $x, y \in \mathbb{Z}[i]$ avec $y \neq 0$.

(1) Montrer qu'il existe $q \in \mathbb{Z}[i]$ tel que $\left|q - \frac{x}{y}\right| < 1$.
(2) En déduire qu'il existe $r \in \mathbb{Z}[i]$ tel que $|r| < |y|$ et $x = qy + r$.
(3) Conclure que $\mathbb{Z}[i]$ est euclidien.

Exercice 103. Soit A un anneau commutatif et unitaire.
Montrer que $A[X]$ est principal si et seulement si A est un corps.

Exercice 104. [Nombre de racines d'un polynôme]
Soit $\mathbb{K}$ un corps, $a \in K$ et $P \in \mathbb{K}[X]$.

(1) Montrer que le reste de la division euclidienne de P par $(X - a)$ est $P(a)$.
(2) En déduire que $P(a) = 0$ si et seulement si P est dans l'idéal engendré par $(X - a)$.
(3) Supposons que $P \neq 0$. Montrer qu'il existe au plus $d^\circ(P)$ éléments x de $\mathbb{K}$ tels que $P(x) = 0$.
(4) En considérant l'*exposant* du groupe des unités, montrer la proposition suivante.
   Si p est premier alors $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p - 1$.
(5) Lorsque $A = \mathbb{Z}/8\mathbb{Z}$ (qui n'est pas un corps), montrer que le polynôme $P = X^2 - 1 \in A[X]$ possède 4 racines.

Exercice 105 (Anneaux d'entiers non principaux)**.**
Soit $n \in \mathbb{Z}$ un nombre entier sans facteur carré, et soit $\omega \in \mathbb{C}$ tel que $\omega^2 = n$. (Par exemple pour $n = -5$ on peut prendre $\omega = i\sqrt{5}$). On définit

$$\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$$

et on définit également la fonction $N(a + b\omega) = a^2 - nb^2$

(1) Vérifier que $\mathbb{Q}[\omega]$ et $\mathbb{Z}[\omega]$ sont des sous-anneaux de $\mathbb{C}$.
(2) Montrer que $\forall x, y \in \mathbb{Q}[\omega], N(xy) = N(x)N(y)$. En déduire que $\mathbb{Q}[\omega]$ est un corps.
(3) Montrer que x est inversible dans $\mathbb{Z}[\omega]$ si et seulement si $N(x) = \pm 1$.
(4) Montrer que si 2 est réductible dans $\mathbb{Z}[\omega]$ alors il existe $x \in \mathbb{Z}[\omega]$ tel que $N(x) = 2$.
(5) Montrer que l'idéal $I = (2, n + \omega)$ est tel que $I \neq (2)$ et $I \neq \mathbb{Z}[\omega]$ (Montrer qu'on ne peut pas obtenir de nombre entier impair.)
(6) En déduire que si 2 est irréductible dans $\mathbb{Z}[\omega]$, l'anneau $\mathbb{Z}[\omega]$ n'est pas principal.
(7) Montrer que si $n \leq -3$, l'anneau n'est pas principal.
(8) Montrer que si $n \equiv 1[4]$ alors l'anneau n'est pas principal.

Exercice 106 (Quotient et polynomes)**.**
Soient A un anneau commutatif unitaire, I et J deux idéaux de A et $\phi : A \to A/I$ la surjection canonique.

(1) Montrer que $(A/I)/\phi(J)$ est isomorphe à $A/(I + J)$.
(2) Montrer que si p est un nombre premier, $(\mathbb{Z}/p\mathbb{Z})[X]$ est isomorphe à $(\mathbb{Z}[X])/(p)$.
(3) Déduire des questions précédentes que

$$\mathbb{Z}[i]/(p) \text{ est isomorphe à } (\mathbb{Z}/p\mathbb{Z})[X]/(X^2 + 1).$$

Exercice 107. Le but de cet exercice est de montrer le résultat suivant :

Théorème (des deux carrés)**.** *Un nombre premier $p \in \mathbb{Z}$ s'écrit comme la somme de deux carrés si et seulement si $p = 2$ ou $p \equiv 1 \mod (4)$.*

Soit donc p un nombre premier

(1) (a) Montrer que si $p = 2$, le polynôme $X^2 + 1$ est réductible.
 Prenons maintenant p impair.
 (b) Montrer que $X^2 + 1$ est réductible dans $(\mathbb{Z}/p\mathbb{Z})[X]$ si et seulement si -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$.
 (c) Montrer que si -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ alors $(-1)^{\frac{p-1}{2}} = 1$.
 (d) En utilisant le fait que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique montrer que si $p = 4k + 1$ alors -1 est un carré.
 (e) Déduire des questions précédentes que $X^2 + 1$ est irreductible dans $\mathbb{Z}/p\mathbb{Z}[X]$ si et seulement si $p \equiv -1 \mod (4)$.

(2) Montrer que p est irreductible dans $\mathbb{Z}[i]$ si et seulement si $p \equiv -1 \mod (4)$. (Penser à utiliser l'exercice précédent)

(3) Si p est réductible dans $\mathbb{Z}[i]$ montrer qu'il existe u et v dans $\mathbb{Z}[i]$ tels que $p = uv$ avec $N(u) = N(v) = p$. (ou N est la fonction définie dans l'exercice 99)

(4) En déduire le Théorème des deux carrés.

Exercice 108. Soit K un corps. Le but de l'exercice est de montrer que l'anneau des séries formelles $K[[X]]$ est euclidien. Cet anneau est défini par :

$$K[[X]] = \left\{ S = \sum_{i \in \mathbb{N}} a_i X^i \,\middle|\, \forall i \in \mathbb{N}, a_i \in K \right\}$$

avec les lois d'addition et de multiplication usuelles (qui prolongent celles sur les polynômes). On définit pour $S \neq 0$, la valuation de S définie par

$$\nu(S) = \min \{n \in \mathbb{N} | a_n \neq 0\} \in \mathbb{N}$$

C'est le plus petit degré n pour lequel le coefficient a_n est non nul. Ce degré existe toujours dès que $S \neq 0$. Par convention, si S est la série nulle on dira que sa valuation est $+\infty$.

(1) Montrer que pour tous $S, T \in K[[X]]$ on a $\nu(ST) = \nu(S) + \nu(T)$.
(2) En déduire que $K[[X]]$ est intègre et montrer que si S est inversible alors $\nu(S) = 0$.
(3) Réciproquement, montrer que si $\nu(S) = 0$ alors S est inversible.
(4) Montrer que tout élément $T \in K[[X]]$ s'écrit sous la forme $T = X^{\nu(T)}U$ avec U inversible.
(5) En déduire que $K[[X]]$ est principal.
(6) Montrer que $S \in K[[X]]$ est irreductible si et seulement si $\nu(S) = 1$.
(7) Soient S et T non nuls. Montrer que si $\nu(S) \leq \nu(T)$ alors S divise T.
(8) Montrer que $K[[X]]$ est euclidien.