Exercice 1.
Dans chacun des cas suivants, déterminer si l'ensemble B est un sous-anneau, un idéal à gauche, un idéal à droite, un idéal bilatère de l'anneau A ou s'il ne possède aucune de ces propriétés:

(a) $A = \mathbb{Z}$ et $B = 9\mathbb{Z}$;

(b) $A = \mathbb{F}_{11}$ et $B = \{[0], [2], [4], [6], [8], [10]\}$;

(c) $A = \mathbb{Z}[t]$ et $B = t^2 \cdot \mathbb{Z}[t^2]$;

(d) $A = \mathbb{F}_2[t]$ et $B = t^2 \cdot \mathbb{F}_2[t]$;

(e) $A = \mathbb{Q}$ et $B = \mathbb{Z}[\sqrt{5}]$;

(f) $A = \mathbb{Z}/15\mathbb{Z}$ et $B = \{[0], [5], [10]\}$;

(g) $A = M_n(\mathbb{R})$, $B = \{M \mid m_{ij} = 0 \text{ si } i < j\}$;

(h) $A = \mathbb{Z}_{(p)} = \left\{\frac{a}{b} \in \mathbb{Q} \mid p \text{ ne divise pas } b\right\}$ et $B = p^n\mathbb{Z}_{(p)}$, où p est un premier et $n \in \mathbb{N}$;

(i) $A = M_3(\mathbb{R})$ et $B = \left\{ \begin{pmatrix} a & a & 0 \\ b & b & 0 \\ c & c & 0 \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\}$;

(j) $A = \mathbb{C}[S_3]$ et $B = \left\{ \sum_{g \in S_3} \lambda \cdot g \mid \lambda \in \mathbb{C} \right\}$;

(k) $A = \mathbb{C}[S_3]$ et $B = \{\lambda(123) + \lambda(132) \mid \lambda \in \mathbb{C}\}$.

Solutions.

(a) $1 \notin B$, therefore B is not a subring of A. On the other hand, B is a bilateral ideal in A (Definition 1.4.4).

(b) $[1] \notin B$, hence B is not a subring of A and, as A is a field, B is neither an ideal in A.

(c) $1 \notin B$, therefore B is not a subring of A. For $t \in A$ and $t^2 \in B$ we have that $t \cdot t^2 = t^3 \notin B$, hence B is not a left ideal in A and moreover, as A is commutative, B is neither a right ideal.

(d) $[1] \notin B$, therefore B is not a subring of A. Let $f(t) \in A$ and let $t^2g(t) \in B$, for some $g(t) \in A$. Then $f(t) \cdot (t^2g(t)) = t^2(f(t)g(t)) \in B$ and thus B is a left ideal in A. Furthermore, as A is commutative, B is a bilateral ideal.

(e) $B \not\subseteq A$.

(f) $[1] \notin B$, therefore B is not a subring of A. Moreover, as $B = ([5])$, B is a bilateral ideal of A.

(g) B is the set of lower triangular matrices in $M_n(\mathbb{R})$, hence it is a subgring of A. If $n > 1$ then B is not an ideal of A. if $n = 1$ then $B = A$ and we conclude that B is a bilateral ideal in A.

(h) If $n = 0$ then $A = B$ and thus B is both a subring and a bilateral ideal of A. If $n > 0$, then $1 \notin B$,hence B is not a subring of A, but, on the other hand, as $B = (p^n)$, we have that B is a bilateral ideal of A.

(i) $\mathrm{I}_3 \notin B$, hence B is not a subring of A. We check to see if B is a left ideal in A. For this let $A = (a_{ij}) \in A$ and we have

$$A \begin{pmatrix} a & a & 0 \\ b & b & 0 \\ c & c & 0 \end{pmatrix} = \begin{pmatrix} a_{11}a + a_{12}b + a_{13}c & a_{11}a + a_{12}b + a_{13}c & 0 \\ a_{21}a + a_{22}b + a_{23}c & a_{21}a + a_{22}b + a_{23}c & 0 \\ a_{31}a + a_{32}b + a_{33}c & a_{31}a + a_{32}b + a_{33}c & 0 \end{pmatrix} \in B.$$

Therefore B is a left ideal of A. On the other hand, B is not a right ideal as

$$\begin{pmatrix}1&1&0\\2&2&0\\3&3&0\end{pmatrix}\begin{pmatrix}0&0&0\\1&0&0\\0&0&0\end{pmatrix}=\begin{pmatrix}1&0&0\\2&0&0\\3&0&0\end{pmatrix}\notin B.$$

(j) B is not a subring of A as $\mathrm{Id}\notin B$. Let $a=a_0\,\mathrm{Id}+a_1(12)+a_2(13)+a_3(23)+a_4(123)+a_5(132)\in A$ and let $b=\lambda[\mathrm{Id}+(12)+(13)+(23)+(123)+(132)]\in B$. Then

$$a\cdot b=b\cdot a=\lambda(a_0+a_1+a_2+a_3+a_4+a_5)\sum_{g\in S_3}g\in B$$

and we deduce that B is a bilateral ideal of A.

(k) Once more, B is not a subring of A, as $\mathrm{Id}\notin B$. One checks that:

$$\begin{cases}(12)\cdot[\lambda(123)+\lambda(132)]=\lambda(23)+\lambda(13)\notin B\\ [\lambda(123)+\lambda(132)]\cdot(12)=\lambda(13)+\lambda(23)\notin B\end{cases},$$

hence B is neither a left, nor a right ideal of A.

Exercice 2.
Soit K un corps et $M_n(K)$ l'anneau des matrices carrées de taille $n\times n$.

1. Soit $i,j\in\{1,\dots,n\}$ fixés. Soit I un idéal à gauche de $M_n(K)$ contenant la matrice e_{ij}. Montrer que I contient aussi toutes les matrices "concentrées dans la j-ème colonne", i.e. (b_{rs}) avec $b_{rs}=0$ si $s\neq j$.

2. Montrer que le sous-ensemble des matrices concentrées dans la j-ème colonne forme un idéal à gauche de $M_n(K)$.

3. Montrer que les seuls idéaux bilatères de $M_n(K)$ sont $\{0\}$ et $M_n(K)$.

Solution.

1. Let $A=(a_{ij})\in M_n(K)$ be a matrix which is concentrated in the j^{th} column, i.e. $a_{rs}=0$ for all $s\neq j$. For all $1\leq r\leq n$ consider the matrix $B_r=a_{rj}e_{ri}\in M_n(K)$. Then $B_re_{ij}\in I$, where

$$(B_re_{ij})_{kl}=\sum_{m=1}^{n}(a_{rj}e_{ri})_{km}(e_{ij})_{ml}=a_{rj}\sum_{m=1}^{n}\delta_{rk}\delta_{im}\delta_{jl}=a_{rj}\delta_{rk}\delta_{jl}=\begin{cases}a_{rj},\ \text{if } k=r \text{ and } l=j\\ 0,\ \text{otherwise}\end{cases}.$$

Lastly, as $A=\sum_{r=1}^{n}(B_re_{ij})$, we conclude that $A\in I$.

2. Let $S\subseteq M_n(K)$ be the subset of matrices which are concentrated in the j^{th} column. Clearly, S is an additive subgroup of $M_n(K)$. Now, let $A=(a_{rs})\in M_n(K)$ and let $B=(b_{rs})\in S$. As

$$(A\cdot B)_{rs}=\sum_{m=1}^{n}a_{rm}b_{ms},$$

it follows that $(A\cdot B)_{rs}=0$ for all $s\neq j$, and we deduce that $A\cdot B\in S$. Therefore, S is a left ideal in $M_n(K)$.

3. Let $\{0\} \neq I$ be a bilateral ideal in $M_n(K)$. Let A be a non-zero matrix in I. Then A admits a non-zero coefficient a_{ij}. As I is an ideal and K is a field we have that $\frac{1}{a_{ij}} \mathrm{I}_n \cdot A \in I$ and so, we can assume without loss of generality that $a_{ij} = 1$. Since I is a bilateral ideal, it follows that for all $1 \leq r, s \leq n$, the product $e_{ri} A e_{js} \in I$. We compute

$$\begin{aligned}(e_{ri}Ae_{js})_{kl} &= \sum_{q=1}^{n} (e_{ri}A)_{kq}(e_{js})_{ql} = \sum_{q=1}^{n} \big[\sum_{p=1}^{n} (e_{ri})_{kp} a_{pq}\big] \delta_{jq}\delta_{sl} = \sum_{p=1}^{n} \delta_{rk}\delta_{ip}a_{pj}\delta_{sl} \\ &= \delta_{rk}a_{ij}\delta_{sl} = \delta_{rk}\delta_{sl} = (e_{rs})_{kl}\end{aligned}$$

and it follows that $e_{rs} \in I$ for all $1 \leq r, s \leq n$. Lastly, as I is an additive subgroup of $M_n(K)$, we conclude that $I = M_n(K)$.

Exercice 3.
Soit R un anneau commutatif.

(a) Montrer que $R[\mathbb{Z}/n\mathbb{Z}] \cong R[t]/(t^n - 1)$.

(b) Montrer que $R[\mathbb{Z}] \cong R[x, y]/(xy - 1)$.

Réfléchissez où doivent être envoyés les éléments des groupes/les variables.

Solution.

(a) Donnons deux preuves de ce fait:

(a) Soit $f\colon R[t] \to R[\mathbb{Z}/n\mathbb{Z}]$ le morphisme évaluant t en $e_{[1]}$ (i.e. l'élément correspondant à $[1] \in \mathbb{Z}/n\mathbb{Z}$). Ce morphisme est certainement surjectif: l'élément $\sum_{[j]\in\mathbb{Z}/n\mathbb{Z}} a([j])e_{[j]} \in R[\mathbb{Z}/n\mathbb{Z}]$ a par exemple comme préimage $\sum_{j=0}^{n-1} a([j])t^j$. Montrons que $\ker(f) = (t^n - 1)$. Tout d'abord, comme

$$f(t^n - 1) = e_{[1]}^n - 1 = e_{[n]} - 1 = e_{[0]} - 1 = 1 - 1 = 0,$$

on en déduit que $t^n - 1 \in \ker(f)$ (et donc $(t^n - 1) \subseteq \ker(f)$).
Il nous reste à montrer l'autre inclusion, et donc soit $a(t) \in \ker(f)$. Vu que le coefficient dominant de $t^n - 1$ est inversible, on peut effectuer la division euclidienne de $a(t)$ par $t^n - 1$, i.e. on peut écrire $a(t) = b(t)(t^n - 1) + c(t)$, avec $\deg(c) < n$. Vu que $a(t) \in \ker(f)$ et $t^n - 1 \in \ker(f)$, on déduit de l'équation ci-dessus que $c(t) \in \ker(f)$. Nous allons montrer qu'en fait, $c(t) = 0$ (et donc $a(t) \in (t^n - 1)$!). Ecrivons $c(t) = \sum_{j=0}^{n-1} c_j t^j$. Alors son image est $\sum_{j=0}^{n-1} c_j e_{[j]}$. Comme $[i] \neq [j]$ pour tout $i \neq j$ dans $\{0, \ldots, n-1\}$, on en déduit que $c_j = 0$ pour tout j, et donc $c(t) = 0$.

On a donc montré que $\ker(f) = (t^n - 1)$ et que f est surjective, on conclut donc la preuve par le premier théorème d'isomorphisme.

(b) Soit $f\colon R[t] \to R[\mathbb{Z}/n\mathbb{Z}]$ le morphisme évaluant t en $e_{[1]}$. Comme avant, on calcule que $(t^n - 1) \subseteq \ker(f)$ (c'était l'inclusion facile), et donc que on obtient un morphisme $\overline{f}\colon R[t]/(t^n - 1) \to R[\mathbb{Z}/n\mathbb{Z}]$. Trouvons un inverse explicite.
Comme expliqué dans la preuve de l'exercice 5 de la série 1.2, trouver un morphisme $R[\mathbb{Z}/n\mathbb{Z}] \to R[t]/(t^n - 1)$ est équivalent à trouver un morphisme d'anneaux $R \to R[t]/(t^n - 1)$ et un morphisme de groupes $\mathbb{Z}/n\mathbb{Z} \to (R[t]/(t^n - 1))^\times$. Dans notre cas, on prend la composition $R \to R[t] \to R[t]/(t^n - 1)$, et le morphisme de groupes défini par envoyer $[1] \in \mathbb{Z}/n\mathbb{Z}$ sur $[t] \in (R[t]/(t^n - 1))^\times$ (notez que cela a du sens, car $[t]$ est inversible et d'ordre n dans cet anneau, vu que $[t]^n = [1]$). Ainsi, on a un morphisme d'anneaux explicite $g\colon R[\mathbb{Z}/n\mathbb{Z}] \to R[t]/(t^n - 1)$, qui "fixe" R et envoie $e_{[1]}$ sur t.

Montrons enfin que ces deux morphismes sont inverses l'un de l'autre. Le calcul peut se simplifier de la facon suivante: dans $R[t]/(t^n-1)$ (resp. $R[\mathbb{Z}/n\mathbb{Z}]$), tout élément s'écrit comme somme et multiples des éléments de R et de t (resp. des éléments de R et de $e_{[1]}$). Ainsi, pour montrer que deux morphismes sont égaux, il suffit de montrer qu'ils envoient R et t (resp. R et $e_{[1]}$) au même endroit. Dans notre cas, on sait que $\overline{f}$ et g "fixent" R, et permutent t et $e_{[1]}$, donc ils sont bel et bien inverses de l'autre. Remarquez que cette méthode est plus conceptuelle que la précédente, et a permis d'éviter certains calculs.

(b) Nous allons précéder comme dans la deuxième preuve du point précédent. Soit $f\colon R[x,y] \to R[\mathbb{Z}]$ le morphisme défini en fixant R, et en envoyant x (resp. y) sur e_1 (resp. e_{-1}). Alors

$$f(xy-1) = f(x)f(y) - 1 = e_1e_{-1} - 1 = e_0 - 1 = 1 - 1 = 0,$$

et donc il se factorise en un morphisme $R[x,y]/(xy-1) \to R[\mathbb{Z}]$.

Trouvons le morphisme dans l'autre sens. Notez que $[x]$ en inversible dans $R[x,y]/(xy-1)$. En effet,

$$[x][y] = [xy] = [xy] - [xy-1] = [1].$$

Ainsi, on peut définir un morphisme de groupes $\mathbb{Z} \to (R[x,y]/(xy-1))^\times$ envoyant 1 sur $[x]$. On a aussi un morphisme d'anneaux $R \to R[x,y]/(xy-1)$ défini par la composition $R \to R[x,y] \to R[x,y]/(xy-1)$, et donc on obtient un morphisme $g\colon R[\mathbb{Z}] \to R[x,y]/(xy-1)$. Notez que vu que $[x]^{-1} = [y]$ (c.f. le calcul précédent) et que $e_{-1} = e_1^{-1}$, on en déduit que e_{-1} est envoyé sur y.

La preuve que $\overline{f}$ et g sont inverses l'un de l'autre est exactement la même que dans le point précédent (tout élément de $R[\mathbb{Z}]$ (resp. $R[x,y]/(xy-1)$) est somme et multiple d'éléments de R et de e_1 et e_{-1} (resp. d'éléments de R et de $[x]$ et $[y]$)).

Exercice 4.
Dans chacun des cas suivants, déterminer si l'affirmation suivante est vraie ou fausse. Justifier la réponse par un raisonnement ou un contre-exemple.

(a) Si A est un anneau intègre, et I et J sont deux idéaux non nuls de A, alors $I \cap J$ est aussi un idéal non nul de A.

(b) Si K est un corps, alors les deux seuls idéaux de K sont $\{0\}$ et K.

(c) Si K est un anneau n'ayant que deux idéaux bilatères, alors tout élément non-nul de K possède un inverse à gauche et à droite.

(d) Si K est un anneau commutatif n'ayant que deux idéaux, alors K est un corps.

(e) Si K est un anneau tel que les seuls idéaux à gauche sont $\{0\}$ et K, alors tout élément non-nul de K possède un inverse à gauche et à droite.

(f) Si K est un anneau tel que les seuls idéaux à droite sont $\{0\}$ et K, alors tout élément non-nul de K possède un inverse à gauche et à droite.

Solution.

(a) Let $0 \neq x \in I$ and let $0 \neq y \in J$. Then $xy \neq 0$, as A is integral, and $xy \in I \cap J$;

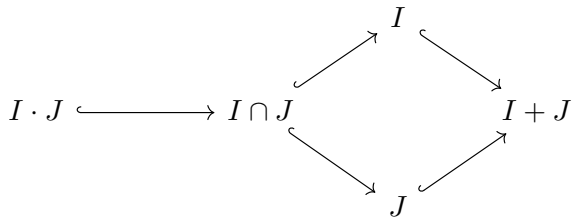
(b) Proposition 2.4.7;

(c) Non, c.f. l'exercice 2;

(d) Proposition 2.4.7.

Pour les points (e) et (f), l'argument suivant s'applique. Soit $x \in K$ non-nul. Alors $Kx = K$. En particulier, il existe $y \in K$ tel que $yx = 1$. Comme $Ky = K$, il existe $z \in K$ tel que $zy = 1$. En multipliant par x à droite, on obtient, $zyx = x$, et donc $z = x$. Ainsi y est un inverse à droite et à gauche de x.

Exercice 5.
Considérons $\mathbb{Q}[x, y]$ et soient $I = (xy)$ et $J = (y^2)$. Montrer que chacune des inclusions dans le diagramme suivant sont strictes.



Solution. Calculons des générateurs de chaque idéal. Par la remarque 2.4.30, on a que $I \cdot J = (xy^3)$ et que $I + J = (xy, y^2)$. Montrons que $I \cap J = (xy^2)$. Tout d'abord, $xy^2 \in I \cap J$, donc $(xy^2) \subseteq I \cap J$. Pour l'autre inclusion, soit $f \in I \cap J$. On peut alors écrire $f = xyg$ et $f(x, y) = y^2 h$ pour certains $g, h \in \mathbb{Q}[x, y]$. En particulier,

$$xyg = y^2 h,$$

et donc

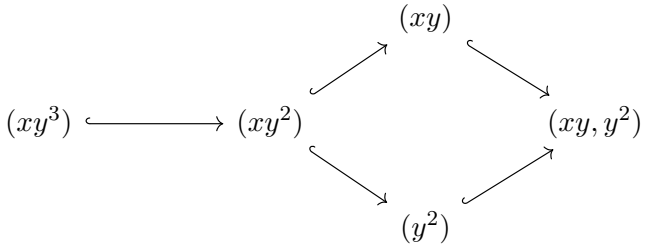
$$y(xg - yh) = 0.$$

Comme $\mathbb{Q}[x, y]$ est intègre, on en déduit que $xg = yh$. En particulier, y divise xg. Un calcul explicite montre alors que y divise en fait g, et donc on peut écrire $g = yg'$ pour un certain $g' \in \mathbb{Q}[x, y]$. Ainsi,

$$f = xyg = xy^2 g' \in (xy^2),$$

et donc on a bien montré que $I \cap J = (xy^2)$.

Il faut donc montrer que chaque inclusion



est stricte. Faisons juste un exemple, car c'est à chaque fois le même argument. On a que $xy^2 \in (xy^2) \setminus (xy^3)$, car sinon $xy^2 = qxy^3$ pour un certain $q \in \mathbb{Q}[x, y]$. Or, le premier polynome a degré 2 en y, alors que cela ne peut pas être le cas du deuxième (il est soit en moins 3, soit ce polynôme lui-même est zéro si $q = 0$).

Exercice 6.
Soit A un anneau commutatif. Montrer les isomorphismes suivants:

(a) $A[t]/(t - a) \cong A$ pour $a \in A$.

(b) $M_n(A)/M_n(I) \cong M_n(A/I)$ si I est un idéal bilatère de A.

(c) $\mathbb{Z}[\sqrt{7}]/(5 + 2\sqrt{7}) \cong \mathbb{Z}/3\mathbb{Z}$ (on pourra commencer par identifier le noyau de l'unique homomorphisme d'anneaux $\varphi\colon \mathbb{Z} \to \mathbb{Z}[\sqrt{7}]/(5 + 2\sqrt{7})$).

Exercice 7.
Soit A un anneau commutatif. Montrer les isomorphismes suivants:

(a) $A[t]/(t-a) \cong A$ pour $a \in A$.

(b) $M_n(A)/M_n(I) \cong M_n(A/I)$ si I est un idéal bilatère de A.

(c) $\mathbb{Z}[\sqrt{7}]/(5+2\sqrt{7}) \cong \mathbb{Z}/3\mathbb{Z}$ (on pourra commencer par identifier le noyau de l'unique homomorphisme d'anneaux $\varphi\colon \mathbb{Z} \to \mathbb{Z}[\sqrt{7}]/(5+2\sqrt{7})$).

Solution.

(a) Example 2.4.10;

(b) Recall the quotient homomorphism $\xi : A \to A/I$ given by $a \xrightarrow{\xi} [a]$ (Proposition 1.4.13). This induces the surjective ring homomorphism $f : M_n(A) \to M_n(A/I)$ given by $(a_{ij}) \xrightarrow{\mathrm{f}} ([a_{ij}])$. The kernel of f consists of those matrices in $M_n(A)$ whose coefficients are zero in A/I, hence $\ker(f) = M_n(I)$. We conclude that $M_n(A)/M_n(I) \cong M_n(A/I)$.

(c) Let $\varphi : \mathbb{Z} \to \mathbb{Z}[\sqrt{7}]/I$, where $\varphi(n) = [n]$, for all $n \in \mathbb{Z}$. Clearly, φ is a ring homomorphism and $\ker(\varphi) = \{n \in \mathbb{Z} \mid n \in I\}$. Let $n \in \ker(\varphi)$. Then there exist $a, b \in \mathbb{Z}$ such that $n = (5+2\sqrt{7})(a+b\sqrt{7})$. We make the computations and arrive at $2n = 3b$. As $\gcd(2,3) = 1$, we have $n \in (3)$, hence $\ker(\varphi) \subseteq (3)$. Conversely, let $n \in (3)$. Then $n = 3m$, for some $m \in \mathbb{Z}$, and $\varphi(n) = \varphi(3)\varphi(m) = 0$. We deduce that $\ker(\varphi) = (3)$.

The only thing left to prove is that φ is surjective. Before we proceed, we remark that $\sqrt{7}(5+2\sqrt{7}) = 14 + 5\sqrt{7} \in I$ and $(14+5\sqrt{7}) - 2(5+2\sqrt{7}) = 4 + \sqrt{7} \in I$. Now, let $[a+b\sqrt{7}] \in \mathbb{Z}[\sqrt{7}]/I$. We have that

$$[a+b\sqrt{7}] = [a] + [b\sqrt{7}] = [a] + [-4b] = \varphi(a) + \varphi(-4b) = \varphi(a-4b).$$

We use the isomorphism theorem to conclude that $\mathbb{Z}/(3) \cong \mathbb{Z}[\sqrt{7}]/(5+2\sqrt{7})$.

Exercice 8.
Soit $1 \neq \epsilon \in \mathbb{C}$ une racine cubique de l'unité.

(a) Montrer que $\mathbb{Z}[\varepsilon] \cong \mathbb{Z}[t]/(t^2+t+1)$.

(b) Montrer que $\mathbb{Q}[\varepsilon] = \mathrm{Frac}(\mathbb{Z}[\varepsilon])$.

(c) Montrer que la dimension de $\mathbb{Q}[\varepsilon]$ en tant que $\mathbb{Q}$-espace vectoriel est 2.

Solution.

(a) Soit le morphisme $f\colon \mathbb{Z}[t] \to \mathbb{Z}[\varepsilon]$ définit par l'évaluation de t en ε. Ce morphisme est surjectif, et donc il suffit de montrer que $\ker(f) = (t^2+t+1)$. Vu que

$$0 = \varepsilon^3 - 1 = (\varepsilon - 1)(\varepsilon^2 + \varepsilon + 1)$$

et que $\varepsilon \neq 1$, on en déduit que

$$\varepsilon^2 + \varepsilon + 1 = 0.$$

Ainsi, $t^2+t+1 \in \ker(f)$, et donc $(t^2+t+1) \subseteq \ker(f)$. Soit maintenant $g \in \ker(f)$. Vu que t^2+t+1 est unitaire, on peut effectuer la division euclidienne de g par t^2+t+1: on peut alors écrire $g = (t^2+t+1)q + r$, où $q, r \in \mathbb{Z}[t]$ et $\deg(r) < 2$. Vu que g et $t^2+t+1 \in \ker(f)$, on en déduit qu'aussi $r \in \ker(f)$. Montrons qu'en fait $r = 0$ (et donc que $g \in (t^2+t+1)$). Si l'on écrit $r = at + b$, alors on obtient que $a\varepsilon + b = 0$. Si $a = 0$, alors $b = 0$ et on est bon.

Si $a \neq 0$, alors on a que $\varepsilon = \frac{b}{a}$, et donc en particulier $\varepsilon \in \mathbb{Q}$. Ceci est impossible, car l'unique racine cubique de l'unité rationelle (même réelle) est 1, et que $\epsilon \neq 1$.

Ainsi, on a bel est bien montré que $\ker(f) = (t^2 + t + 1)$, et donc on conclut par le premier théorpme d'isomorphisme.

(b) Tout d'abord, rappelons que $\mathbb{Q}[\varepsilon]$ est l'anneau engendré par $\mathbb{Q}$ et ε dans $\mathbb{C}$ les nombres complexes. Autrement dit ce sont éléments de $\mathbb{C}$ de la forme

$$\mathbb{Q}[\varepsilon] = \left\{ \sum_{i=0}^{n} q_i \varepsilon^i \mid q_i \in \mathbb{Q} \right\}.$$

Mais comme $\varepsilon^2 = -(\varepsilon + 1)$, ce sont les éléments de la forme

$$\mathbb{Q}[\varepsilon] = \{ q_0 + q_1 \varepsilon \mid q_0, q_1 \in \mathbb{Q} \}.$$

Mais comme $\varepsilon = \cos(2\pi/3) + i\sin(2\pi/3) = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, on peut encore reformuler cet anneau comme

$$\mathbb{Q}[\varepsilon] = \left\{ q_0 + q_1 i\sqrt{3}\varepsilon \mid q_0, q_1 \in \mathbb{Q} \right\}.$$

Maintenant, on peut montrer que aisément que c'est un corps. En effet, l'inverse de $q_0 + q_1 i\sqrt{3}$ est $\frac{q_0 - q_1 i\sqrt{3}}{q_0^2 + 3q_1^2} \in \mathbb{Q}[\varepsilon]$.

Maintenant, notons qu'on a une inclusion $\mathbb{Z}[\varepsilon] \subset \mathbb{Q}[\varepsilon]$. Si on prend un élément $q_0 + q_1\varepsilon$ en multipliant par les dénominateurs de q_0 et q_1, on se retrouve dans $\mathbb{Z}[\varepsilon]$. Dès lors, en utilisant le critère de la série précédente, on conclut.

(c) On prétend qu'une base est $(1, \varepsilon)$. La génération suit de la discussion ci-dessus. La liberté de la famille suit par exemple de l'observation suivante: si $a + b\epsilon = 0$ pour $a, b \in \mathbb{Q}$ alors $a - \frac{1}{2}b + i\frac{\sqrt{3}}{2}b = 0$. Alors comme on sait que $\mathbb{C}$ est un $\mathbb{R}$-espace vectoriel de dimension 2 de base $(1, i)$ on voit que $b = 0$, et donc par suite que $a = 0$.