EPFL - Printemps 2023 | Prof. Z. Patakfalvi
Anneaux et Corps | **Exercices**
Solutions 1

Exercice 1.
Puisque nous considérons des sous-ensembles d'anneaux, les propriétés de compatibilité et de distributivité sont automatiquement vérifiées. Il s'agit seulement de vérifier si le sous-ensemble est stable par addition et multiplication, et s'il contient l'élément neutre et le zéro.

1. Les matrices triangulaires supérieures forment un sous-anneau. Les vérifications sont aisées.
2. Ce sous-ensemble ne contient pas la matrice identité.
3. Les matrices diagonales forment un sous-anneau, et les vérifications sont aisées.
4. Cet ensemble (il s'agit de $\mathbb{Z}[i]$) est un sous-anneau. Les vérifications sont aisées.
5. Cet ensemble (il s'agit de $\mathbb{Z}[\sqrt{3}]$) est un sous-anneau. Les vérifications sont aisées.
6. Ce sous-ensemble ne contient pas l'identité.
7. On vérifie par calculs directs que cet ensemble est un sous-anneau.

Exercice 2.
Notons G multiplicativement, et les éléments de $\mathbb{Z}[G]$ comme des sommes $\sum_{g\in G} a(g)e_g$ où $a(g) \in \mathbb{Z}$. Prenons $g \in G$ distinct de l'élément neutre $\epsilon \in G$. Puisque G est fini et que g n'est pas l'élément neutre, il existe $n > 1$ tel que $g^n = \epsilon$. On a alors :

$$0 = e_\epsilon - e_{g^n} = (e_\epsilon - e_g)(e_\epsilon + e_g + e_{g^2} + \cdots + e_{g^{n-1}})$$

et ni $e_\epsilon - e_g$ ni $e_\epsilon + e_g + \cdots + e_{g^{n-1}}$ n'est égal à zéro.

Exercice 3. 1. Si $f\colon \mathbb{Z} \to \mathbb{Z}$ est un homomorphisme, alors

$$f(n) = f(\underbrace{1 + \cdots + 1}_{n \text{ fois}}) = \underbrace{f(1) + \cdots + f(1)}_{n \text{ fois}} = \underbrace{1 + \cdots + 1}_{n \text{ fois}} = n$$

donc $f = \mathrm{Id}_\mathbb{Z}$.

2. Le même raisonnement qu'au point précédent donne que, s'il existe un homomorphisme, alors il est donné par $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, s \mapsto [s]_n$. On vérifie sans peine qu'il s'agit bien d'un homomorphisme.
3. Si $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$ est un homomorphisme, alors $n \cdot f([1]) = f([n]) = f([0]) = 0$ d'une part, et $n \cdot f([1]) = n \cdot 1 = n$ d'autre part, ce qui est une contradiction. Donc il n'existe pas d'homomorphisme $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$.
4. Le même raisonnement qu'au second point donne que, s'il existe un homomorphisme, alors il est donné par $f\colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, [s]_m \mapsto [s]_n$. Cependant, cette fonction n'est pas toujours bien définie. Par exemple, si $n = 2$ et $m = 3$, alors on devrait avoir

$$[0]_2 = f([0]_3) = f([1]_3) + f([1]_3) + f([1]_3 = [1]_2 + [1]_2 + [1]_2 = [1]_2,$$

ce qui est absurde.

On prétend que f est bien définie si et seulement si n divise m. Il s'agit d'abord d'une condition nécessaire, puisque

$$[0]_n = f([0]_m) = f(m \cdot [1]_m) = m \cdot f([1]_m) = m \cdot [1]_n = [m]_n.$$

Inversément, supposons que $m = nk$. Alors f est une fonction bien définie, puisque

$$f([s + lm]_m) = [s + lm]_n = [s + lnk]_n = [s]_n = f([s]_m)$$

et l'on vérifie sans peine que f est bien un homomorphisme d'anneaux.

5. Soit $f\colon \mathbb{Q} \to \mathbb{R}$ un homomorphisme. Puisque $f(1) = 1$, on a $0 = f(0) = f(1-1) = 1 + f(-1)$ et donc $f(-1) = -1$. Par additivité on obtient que $f(n) = n$ pour tout $n \in \mathbb{Z}$. Pour $n \in \mathbb{Z}^*$ on a
$$1 = f(1) = f(n \cdot n^{-1}) = n \cdot f(n^{-1})$$
et donc $f(n^{-1}) = n^{-1}$. Par multiplicativité on obtient $f(x) = x$ pour tout $x \in \mathbb{Q}$. Donc f est l'homomorphisme d'inclusion.

6. Soit $f\colon \mathbb{R} \to \mathbb{R}$ un homomorphisme. Par le point précédent, la restriction $f|_{\mathbb{Q}}$ est l'inclusion. Nous allons montrer qu'en fait $f = \mathrm{Id}_{\mathbb{R}}$.

   Prenons un nombre réel $x > 0$. Alors il existe un nombre réel y tel que $y^2 = x$. Ainsi $f(x) = f(y^2) = f(y)^2 > 0$. En particulier si $a > b$, alors $f(a) - f(b) = f(a-b) > 0$. Donc f préserve l'ordre usuel sur les réels.

   Prenons maintenant un nombre réel x, et choisissons deux suites de nombres rationnels (y_i) et (z_j) tels que $y_i < x < z_j$ pour tous i, j et $\lim_i y_i = x = \lim_j z_j$. Par les observations précédentes, on a
$$y_i = f(y_i) < f(x) < f(z_j) = z_j$$
pour tous i, j. Les conditions sur les limites nous assurent alors, par un simple argument d'analyse, que $f(x) = x$.

7. Il n'existe pas d'homomorphisme $f\colon \mathbb{R} \to \mathbb{Q}$. En effet, si un tel f existait, alors la composition
$$\mathbb{R} \xrightarrow{f} \mathbb{Q} \hookrightarrow \mathbb{R}$$
serait un homomorphisme d'anneaux non-surjectif, en particulier distinct de l'identité, ce qui contredit le point précédent.

8. Par la propriété universelle des anneaux polynomiaux, un homomorphisme $\mathbb{R}[t] \to \mathbb{R}$ est équivalent au choix d'un homomorphisme $\mathbb{R} \to \mathbb{R}$ et d'un élément $a \in \mathbb{R}$ (qui sera l'image de t). En vertu de ce qui précède, on obtient que
$$\mathbb{R} \xrightarrow{1:1} \mathrm{Hom}(\mathbb{R}[t], \mathbb{R}), \quad a \mapsto [p(t) \mapsto p(a)].$$

9. De manière générale, un morphisme d'anneaux doit envoyer un élément inversible vers un élément inversible (la preuve en est aisée). Donc si $f\colon \mathbb{R} \to \mathbb{R}[t]$ est un homomorphisme, tout élément $x \in \mathbb{R}^*$ étant inversible, son image $f(x) \in \mathbb{R}[t]$ est inversible. Or les polynômes inversibles sont les constantes non-nulles. Ainsi f se co-restreint à un homomorphisme $f\colon \mathbb{R} \to \mathbb{R}$, qui est nécessairement l'identité par ce qui précède. Ceci établit que $f\colon \mathbb{R} \to \mathbb{R}[t]$ est l'homomorphisme d'inclusion.

Exercice 4.
Par souci de clarté, si G est un groupe fini nous écrirons les éléments de $\mathbb{Z}[G]$ sous la forme $\sum_{g\in G} a(g)e_g$, où $a(g) \in \mathbb{Z}$.

Soit $f\colon \mathbb{Z}[S_3] \to \mathbb{Z}[\mathbb{Z}/2\mathbb{Z}]$ un homomorphisme. Puisque $(123)^3$ est l'élément neutre de S_3, on doit avoir

$$f(e_{(123)})^3 = e_0.$$

On peut écrire $f(e_{(123)}) = ne_0 + me_1$ pour certains $n, m \in \mathbb{Z}$. Puisque $\mathbb{Z}/2\mathbb{Z}$ est un groupe commutatif, son algèbre de groupe sur $\mathbb{Z}$ est un anneau commutatif. On calcule donc

$$(ne_0 + me_1)^3 = (n^3 + 3nm^2)e_0 + (m^3 + 3n^2m)e_1.$$

Ainsi $m(m^2+3n^2) = 0$ et $n(n^2+3m^2) = 1$. Si $m = 0$ alors $n = 1$; si $m^2+3n^2 = 0$ alors $m = 0 = n$, ce qui n'est pas possible en vue de la seconde condition. On a donc montré que $f(e_{(123)}) = e_0$.

Faisons le même raisonemment pour $e_{(12)}$. Si $f(e_{(12)}) = ae_0 + be_1$, alors on obtient

$$e_0 = (a^2 + b^2)e_0 + 2abe_1$$

et donc (a, b) vaut $(0, 1), (0, -1), (1, 0)$ ou $(-1, 0)$.

Puisque (12) et (123) génèrent S_3, la connaissance de $f(e_{(123)})$ et de $f(e_{(12)})$ permet de déterminer f entièrement. On voit donc qu'il existe au plus 4 possibilités pour f.

Pour montrer qu'il existe exactement 4 morphismes, on peut montrer à la main avec les formules qu'envoyer les 2-cycles sur ae_0+be_1 pour $(a, b) \in \{(1, 0), (-1, 0), (0, 1), (0, -1)\}$ et les 3-cycles ainsi que l'élément neutre sur e_0 se prolonge en unique morphisme. Pour démontrer cela on peut passer par l'argument suivant, qui met en situation ce "prolongement".

On remarque que $\mathbb{Z}[-]$: Grp $\to$ Ring si Grp désigne la catégorie des groupes et Ring la catégorie des anneaux (non nécessairement commutatifs) est adjoint à gauche de $(A, +, \cdot) \mapsto (A^\times, \cdot)$. Notez également que l'abélianisé de S_3 est $\mathbb{Z}/2\mathbb{Z}$. Dès lors, en utilisant l'adjonction ci-dessus et l'adjonction abélianisé $\dashv$ oubli entre Ab et Grp on obtient

$$\begin{aligned}&\mathrm{Hom}_{\mathrm{Ring}}(\mathbb{Z}[S_3], \mathbb{Z}[\mathbb{Z}/2\mathbb{Z}]) \cong \mathrm{Hom}_{\mathrm{Grp}}(S_3, \mathbb{Z}[\mathbb{Z}/2\mathbb{Z}]^\times)\\ &\cong \mathrm{Hom}_{\mathrm{Ab}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}[\mathbb{Z}/2\mathbb{Z}]^\times)\end{aligned}$$

ce qui conclut car le calcul au-dessus démontre que les seuls éléments $a \in \mathbb{Z}[\mathbb{Z}/2\mathbb{Z}]^\times$ tel que $a^2 = 1$ sont $ae_0 + be_1$ pour $(a, b) \in \{(1, 0), (-1, 0), (0, 1), (0, -1)\}$.

Exercice 5.
Par souci de clarté, notons n_A l'élément $\underbrace{1_A + \cdots + 1_A}_{n \text{ fois}} \in A$.

1. Puisque $a \in A$ génère le groupe additif, tout élément de A peut s'écrire comme une somme $a + \cdots + a$. Par distributivité on a

$$(\underbrace{a + \cdots + a}_{n \text{ fois}}) \cdot (\underbrace{a + \cdots + a}_{m \text{ fois}}) = \underbrace{a^2 + \cdots + a^2}_{nm \text{ fois}} = (\underbrace{a + \cdots + a}_{m \text{ fois}}) \cdot (\underbrace{a + \cdots + a}_{n \text{ fois}}).$$

   Donc A est commutatif.

2. Il découle du calcul précédent que la connaissance de a^2 détermine la multiplication de A.

3. Puisque a génère A additivement, il existe $s \geq 1$ tel que

$$s_A \cdot a = \underbrace{a + \cdots + a}_{s \text{ fois}} = 1_A$$

   et donc s_A est un inverse à gauche de a. Puisque A est commutatif, s_A est aussi un inverse à droite et ainsi $a^{-1} = s_A$.

4. Il existe un $t \geq 1$ tel que $t_A \cdot a = a^2$. On a alors

$$a = a \cdot a \cdot a^{-1} = a^2 \cdot a^{-1} = t_A \cdot a \cdot a^{-1} = t_A \cdot 1_A.$$

En particulier 1_A génère aussi le groupe additif $(A, +)$. Puisque A est d'ordre n, on a nécessairement $A = \{0_A, 1_A, 2_A, \ldots, (n-1)_A\}$. Ceci permet de définir

$$f \colon \mathbb{Z}/n\mathbb{Z} \to A, \quad [r]_n \mapsto r_A$$

car $r_A + (nk)_A = r_A$. Il est clair qu'il s'agit un homomorphisme bijectif, donc d'un isomorphisme.

Exercice 6.
Notons tout d'abord que l'application de la donnée est un morphisme d'anneau par la propriété universelle des anneaux de polynômes appliquée à $A \to A[t]$ canonique et l'élément $t+a$. Maintenant l'inverse est donné par

$$A[t] \to A[t], \quad p(t) \mapsto p(t-a),$$

ce qui conclut.

Exercice 7.
On utilise la notation suivante (symbole delta de Kronecker) : $\delta^i_j = 0$ si $i \neq j$, et $\delta^i_i = 1$.

1. Soient $A = (a_{ij}), B = (b_{ij}) \in M(k)$. L'addition est donnée par

$$(a_{ij}) + (b_{ij}) := (a_{ij} + b_{ij})$$

et la multiplication par

$$(a_{ij}) \cdot (b_{ij}) := \left(\sum_{k=1}^{\infty} a_{ik} b_{kj} \right)_{i,j \in \mathbb{N}}$$

La multiplication est bien définie, puisque la condition de finitude assure que la série est en fait une somme finie. Pour montrer que chaque colonne du produit est à support fini, prenons un indice j quelconque. Soit N suffisamment grand tel que pour tous les indices $i \geq N$ on a $b_{ij} = 0$. Maintenant si M est suffisamment grand pour que pour tout $i \geq M$ et tout les $j \leq N$ on a $a_{ij} = 0$, on obtient que si $i \geq M$ que $(A \cdot B)_{ij} = 0$. L'associativité, la distributivité et autres propriétés des axiomes d'anneaux sont facilement. vérifiées, ce sont les même calculs que dans le cas fini. La matrice nulle est l'élément neutre additif et la matrice $(a_{ij} = \delta^i_j)$ est l'élément neutre multiplicatif. Donc $M(k)$ est un anneau.

2. Prenons

$$A := \left(a_{ij} = \delta^i_{j+1}\right)_{i,j}, \quad B := \left(b_{ij} = \delta^{i+1}_j\right)_{i,j},$$

ce sont des éléments de $M(k)$. Visuellement, on peut se représenter A comme la matrice identité dont on a décalé la diagonale d'une ligne vers le bas — et B comme la matrice identité dont on a décalé la diagonale d'une colonne vers la droite.

On vérifie alors que $BA = 1_{M(k)} \neq AB$. Cela implique que A n'a pas d'inverse à droite : car s'il existait B' tel que $AB' = 1_{M(k)}$, alors $B = BAB' = B'$.

Remarque. On peut également remarquer que cet anneau de matrices est isomorphe à l'anneau des endomorphismes k-linéaires de $k^{\oplus \mathbb{N}}$. Dès lors si on représente les éléments de cet espace comme des vecteurs à support fini d'éléments de k écrits de gauche à droite la matrice A correspond au décalage d'un cran vers la droite avec zéro en première composante et B au décalage d'un cran vers la gauche.

Exercice 8. 1. Un anneau A intègre et fini est un corps. En effet, prenons $a \neq 0$ et considérons la fonction

$$A \to A, \quad x \mapsto ax.$$

Puisque $a \neq 0$ et que A est intègre, cette fonction est injective. Mais A est un ensemble fini, donc cette fonction est en fait bijective. Ainsi il existe un $y \in A$ tel que $ay = 1$. Le même raisonnement appliqué à la fonction $x \mapsto xa$ donne un $y' \in A$ tel que $y'a = 1$. Ainsi $y = y'ay = y'$, et $a^{-1} = y$. Donc A est un corps.

On peut aussi montrer que si A est un anneau fini sans diviseur de zéro, alors A est nécessairement un corps (commutatif), mais cela est bien moins facile — il s'agit du (petit) théorème de Wedderburn.

2. Un anneau A dans lequel $x = x^2$ pour tout $x \in A$, est commutatif. En effet, prenons $a, b \in A$. On a alors

$$a + b = (a + b)^2 = a^2 + ab + ba + b^2 = a + b + ab + ba$$

et ainsi $ab = -ba$. Or $-1 = (-1)^2 = 1$, donc $ab = -ba = ba$, comme désiré.

Les anneaux qui vérifient cette condition sont appelés *algèbres booléennes*. Elles ont des liens surprenants avec la topologie et la logique mathématique. Voir *dualité de Stone* sur wikipedia ou sur le n-lab.

Exercice 9. 1. Montrons que $f(t) = \sum_{i=0}^{\infty} a_i t^i$ est inversible si et seulement si $a_0 \neq 0$.

C'est une condition nécessaire : si $g(t) = \sum_{i=0}^{\infty} b_i t^i$ est tel que $f(t)g(t) = 1$, alors $a_0 b_0 = 1$.

Inversément, supposons $a_0 \neq 0$. Nous allons définir inductivement des coefficients b_i tels que $1 - f(t) \cdot \sum_{i=0}^{n} b_i t^i \in (t^{n+1})$.

- $b_0 := a_0^{-1}$.
- Supposons $b_0, \ldots, b_{n-1}$ construits. On a

$$1 - f(t) \cdot \sum_{i=0}^{n} b_i t^i = \underbrace{1 - f(t) \cdot \sum_{i=0}^{n-1} b_i t^i}_{\in (t^n)} - f(t) \cdot b_n t^n$$

et donc la condition $1 - f(t) \cdot \sum_{i=0}^{n} b_i t^i \in (t^{n+1})$ est équivalente à

$$\sum_{i=0}^{n-1} a_{n-i} b_i = -a_0 b_n.$$

On prend ainsi $b_n := -a_0^{-1} \sum_{i=0}^{n-1} a_{n-i} b_i$.

Posons $g(t) := \sum_{i=0}^{\infty} b_i t^i$. Par construction, le terme constant du produit $f(t)g(t)$ vaut 1. On prétend qu'en fait $f(t)g(t) = 1$. Si ce n'est pas le cas, alors il existe un certain $n \geq 1$ tel que $1 - f(t)g(t) \in (t^n)$, et on peut prendre un tel n maximal. Mais par construction

$$1 - f(t)g(t) = \underbrace{\left[1 - f(t) \cdot \sum_{i=0}^{n} b_i t^i\right]}_{\in (t^{n+1})} - \underbrace{t^{n+1} \left[f(t) \cdot \sum_{i=0}^{\infty} b_{i+n+1} t^i\right]}_{\in (t^{n+1})}$$

donc $1 - f(t)g(t) \in (t^{n+1})$, contradiction puisque n est maximal. Ceci prouve que $g(t) = f(t)^{-1}$.

Remarquez que même si $f(t)$ est un polynôme, son inverse $f(t)^{-1}$ sera seulement une série formelle. Donc l'anneau $k[t]$ est très différent de l'anneau $k[[t]]$. Cette différence est comparable (dans un sens que nous n'élaborerons pas) à celle qui sépare les fonctions holomorphes définies sur $\mathbb{C}$, de celles qui ne sont définies que sur un voisinage de $0 \in \mathbb{C}$.

Voici un autre solution, qui s'inspire de la relation

$$(1-t) \cdot \sum_{i=0}^{\infty} t^i = 1.$$

Etant donné $g(t) = \sum_{i=0}^{\infty} a_i t^i$, on peut être tenté de remplacer t par $g(t)$ dans la relation ci-dessus, et en déduire que $\sum_{i \geq 0} g(t)^i$ est l'inverse de $1-g(t)$. Puisque n'importe quelle série formelle peut s'écrire sous la forme $1-g(t)$, on aurait montré l'existence d'inverses — pour *tous* les éléments de $k[[t]]$, ce qui est bien sûr absurde. Le problème est que la somme infinie $\sum_{i \geq 0} g(t)^i$ n'est pas forcément bien définie (par exemple si $g(t) = \lambda \in k^*$). En fait, on vérifie aisément que cette somme infinie n'a de sens que si $g(t)$ n'a pas de terme constant, auquel cas le terme de degré n de cette série se définit comme le terme de degré n de la somme finie $1 + g(t) + \cdots + g(t)^n$.

Ceci étant dit, soit $f(t)$ une série possédant un terme constant. Si $\lambda \in k^*$, alors il est équivalent de trouver un inverse de $f(t)$ et de trouver un inverse de $\lambda f(t)$. Donc on peut supposer que le terme constant de $f(t)$ vaut 1. Dans ce cas $F(t) := 1 - f(t)$ n'a pas de terme constant, la somme infinie $\sum_{i \geq 0} F(t)^i$ peut être définie, et nous allons vérifier qu'il s'agit bien d'un inverse de $f(t)$. La vérification est semblable à ce qui a été fait précédemment : le terme constant de $f(t) \cdot \sum_{i=0}^{\infty} F(t)^i$ vaut 1, donc si ce produit ne vaut pas 1 il existe un $N > 0$ maximal tel que

$$1 - f(t) \cdot \sum_{i=0}^{\infty} F(t)^i \in (t^N).$$

Or

$$\begin{aligned}
1 - f(t) \cdot \sum_{i=0}^{\infty} F(t)^i &= 1 - (1 - F(t)) \cdot \sum_{i=0}^{N} F(t)^i + t^{N+1} f(t) \sum_{i=N+1}^{\infty} \frac{F(t)^i}{t^{N+1}} \\
&= 1 - (1 - F(t)^{N+1}) + t^{N+1} f(t) \sum_{i=N+1}^{\infty} \frac{F(t)^i}{t^{N+1}} \\
&= F(t)^{N+1} + t^{N+1} f(t) \sum_{i=N+1}^{\infty} \frac{F(t)^i}{t^{N+1}} \\
&\in (t^{N+1})
\end{aligned}$$

ce qui est une contradiction. Donc $f(t)^{-1} = \sum_{i=0}^{\infty} F(t)^i$.

2. Montrons d'abord que $k((t))$ est un corps. Il est facile de vérifier qu'il s'agit d'un anneau commutatif intègre (avec les opérations évidentes — la multiplication est définie de la même manière que dans $k[[t]]$), et que $k[[t]]$ est un sous-anneau de $k((t))$. Prenons $0 \neq f(t) = \sum_{i \geq n} a_i t^i \in k((t))$, où l'on fait la convention que $a_n \neq 0$. Alors $t^{-n} f(t) = \sum_{i \geq 0} a_{i+n} t^i \in k[[t]]$ est un élément inversible par le premier point, donc il existe $g(t) \in k[[t]]$ tel que $t^{-n} f(t) g(t) = 1$. On en déduit que $t^{-n} g(t) \in k((t))$ est l'inverse de $f(t)$. Donc $k((t))$ est bien un corps.

   Montrons maintenant que chaque élément de $k((t))$ peut s'écrire comme un ratio d'éléments de $k[[t]]$. Considérons à nouveau $0 \neq f(t) = \sum_{i \geq n} a_i t^i$. Si $n \geq 0$ alors $f(t) \in k[[t]]$. Si $n < 0$, alors $t^{-n} f(t) = h(t) \in k[[t]]$ et ainsi

$$f(t) = \frac{h(t)}{t^{-n}}$$

   où le numérateur et le dénominateur appartiennent à $k[[t]]$.

Exercice 1. (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 $t^2 g(t) \in B$, for some $g(t) \in A$. Then $f(t) \cdot (t^2 g(t)) = t^2(f(t)g(t)) \in B$ and thus B is a left ideal in A. Furthermore, as A is commutative, B is a bilateral ideal.

(e) $B \nsubseteq A$.

(f) $B \nsubseteq A$.

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

(h) 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.

(i) 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.

(j) $\mathrm{I}_3 \notin B$, hence B not a subring. Since

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ a & b & 0 \end{pmatrix} \notin B,$$

it follows that B is not a left ideal in A. Similarly, as

$$\begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & b \\ 0 & 0 & d \\ 0 & 0 & 0 \end{pmatrix} \notin B,$$

it follows that B is also not a right ideal in A.

(k) B is a subring of A: we have that $\mathrm{I}_3 \in B$, $(B, +)$ is a subgroup of $M_n(\mathbb{R})$ and B is stable under matrix multiplication. As $B \neq A$ and $\mathrm{I}_3 \in B$, it follows that B is neither a left nor a right ideal of A.

(l) $\mathrm{I}_3 \notin B$, 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

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

(m) 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.

(n) Again, 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 $b = \lambda\,\mathrm{Id} - \lambda(12) - \lambda(13) - \lambda(23) + \lambda(123) + \lambda(132) \in B$. One checks that

$$\begin{aligned} a \cdot b = {} & \lambda(a_0 - a_1 - a_2 - a_3 + a_4 + a_5)\,\mathrm{Id} - \lambda(a_0 - a_1 - a_2 - a_3 + a_4 + a_5)(12) - \\ & - \lambda(a_0 - a_1 - a_2 - a_3 + a_4 + a_5)(13) - \lambda(a_0 - a_1 - a_2 - a_3 + a_4 + a_5)(23) + \\ & + \lambda(a_0 - a_1 - a_2 - a_3 + a_4 + a_5)(123) + \lambda(a_0 - a_1 - a_2 - a_3 + a_4 + a_5)(132) \\ = {} & \sum_{g \in S_3} (-1)^{\mathrm{sgn}(g)} \mu \cdot g, \end{aligned}$$

where $\mu = \lambda(a_0 - a_1 - a_2 - a_3 + a_4 + a_5) \in \mathbb{C}$. Therefore B is a left ideal of A. Analogously, one shows that:

$$b \cdot a = \sum_{g \in S_3} (-1)^{\mathrm{sgn}(g)} \mu \cdot g,$$

where $\mu = \lambda(a_0 - a_1 - a_2 - a_3 + a_4 + a_5) \in \mathbb{C}$, and therefore B is a bilateral ideal of A.

(o) Again, 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 $b = \lambda\,\mathrm{Id} + \lambda\varepsilon(123) + \lambda\varepsilon^2(132) + \mu(12) + \mu\varepsilon(23) + \mu\varepsilon^2(13) \in B$. We compute:

$$\begin{aligned} a \cdot b = {} & (\lambda a_0 + \mu a_1 + \mu\varepsilon^2 a_2 + \mu\varepsilon a_3 + \lambda\varepsilon^2 a_4 + \lambda\varepsilon a_5)\,\mathrm{Id} + (\lambda\varepsilon a_0 + \mu\varepsilon a_1 + \mu a_2 + \mu\varepsilon^2 a_3 + \lambda a_4 + \\ & + \lambda\varepsilon^2 a_5)(123) + (\lambda\varepsilon^2 a_0 + \mu\varepsilon^2 a_1 + \mu\varepsilon a_2 + \mu a_3 + \lambda\varepsilon a_4 + \lambda a_5)(132) + (\mu a_0 + \lambda a_1 + \\ & + \lambda\varepsilon a_2 + \lambda\varepsilon^2 a_3 + \mu\varepsilon a_4 + \mu\varepsilon^2 a_5)(12) + (\mu\varepsilon a_0 + \lambda\varepsilon a_1 + \lambda\varepsilon^2 a_2 + \lambda a_3 + \mu\varepsilon^2 a_4 + \mu a_5)(23) + \\ & + (\mu\varepsilon^2 a_0 + \lambda\varepsilon^2 a_1 + \lambda a_2 + \lambda\varepsilon a_3 + \mu a_4 + \mu\varepsilon a_5)(13) \end{aligned}$$

Set $x = \lambda a_0 + \mu a_1 + \mu\varepsilon^2 a_2 + \mu\varepsilon a_3 + \lambda\varepsilon^2 a_4 + \lambda\varepsilon a_5$ and $y = \mu a_0 + \lambda a_1 + \lambda\varepsilon a_2 + \lambda\varepsilon^2 a_3 + \mu\varepsilon a_4 + \mu\varepsilon^2 a_5$. Then, $x, y \in \mathbb{C}$ and we see that

$$a \cdot b = x\,\mathrm{Id} + x\varepsilon(123) + x\varepsilon^2(132) + y(12) + y\varepsilon(23) + y\varepsilon^2(13) \in B$$

and conclude that B is a left ideal of A.

On the other hand, let $a = a_0\,\mathrm{Id} + a_1(12) \in A$ and $b = \lambda\,\mathrm{Id} + \lambda\varepsilon(123) + \lambda\varepsilon^2(132) + \mu(12) + \mu\varepsilon(23) + \mu\varepsilon^2(13) \in B$. Then:

$$\begin{aligned} b \cdot a = {} & (\lambda a_0 + \mu a_1)\,\mathrm{Id} + \varepsilon(\lambda a_0 + \mu\varepsilon a_1)(123) + \varepsilon^2(\lambda a_0 + \mu\varepsilon^2 a_1)(132) + (\mu a_0 + \lambda a_1)(12) + \\ & + \varepsilon(\mu a_0 + \lambda\varepsilon a_1)(23) + \varepsilon^2(\mu a_0 + \lambda\varepsilon^2 a_1)(13) \notin B. \end{aligned}$$

Hence B is not a right ideal of A.

(p) 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. 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 $B_r e_{ij} \in I$, where

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

Lastly, as $A = \sum_{r=1}^{n}(B_r e_{ij})$, 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 $e_{ri}Ae_{js} \in I$. 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. (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 1.4.6;

(c) Exercice 2;

(d) Proposition 1.4.6.

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 4. (a) Example 1.4.9;

(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 5.
We recall that, by convention, the degree of the zero polynomial is $-\infty$ and that $-\infty + n = -\infty$ for all positive integers n. We can therefore assume that $f, g \neq 0$. We write $f(t) = \sum_{i=0}^{m} a_i t^i$, where $a_m \neq 0$, hence $\deg(f) = m$, and $g(t) = \sum_{j=0}^{n} b_j t^j$, where $b_n \neq 0$, hence $\deg(g) = n$. Now $f(t)g(t) = \sum_{i=0}^{m}\sum_{j=0}^{n} a_i b_j t^{i+j}$ and so $\deg(fg) = n + m$, as the leading coefficient of fg is $a_m b_n \neq 0$, by integrity of A.

Exercice 6.
Consider the evaluation homomorphism $\mathrm{ev}_\varepsilon : \mathbb{Z}[t] \to \mathbb{Z}[\varepsilon]$. Clearly ev_ε is surjective and so, the only thing we need to show is that $(t^2 + t + 1) = \ker(\mathrm{ev}_\varepsilon)$.

Let $f(t) \in (t^2 + t + 1)$. Then $f(t) = (t^2 + t + 1)g(t)$ for some $g(t) \in \mathbb{Z}[t]$ and we have

$$\mathrm{ev}_\varepsilon(f(t)) = \mathrm{ev}_\varepsilon(t^2 + t + 1)\,\mathrm{ev}_\varepsilon(g(t)) = 0.$$

Therefore $(t^2 + t + 1) \subseteq \ker(\mathrm{ev}_\varepsilon)$.

Conversely, let $f(t) \in \ker(\mathrm{ev}_\varepsilon)$. We will show that $f(t) \in (t^2 + t + 1)$ by recurrence on $\deg(f)$.

If $\deg(f) = 0$, then $f(t) = a_0$ and as $\mathrm{ev}_\varepsilon(f) = 0$, it follows that $f = 0$.

If $\deg(f) = 1$, then $f(t) = a_1 t + a_0$, for some $a_1, a_0 \in \mathbb{Z}$, and, as $\mathrm{ev}_\varepsilon(f(t)) = 0$, it follows that $a_1 = a_0 = 0$, hence $f(t) = 0$.

We can now assume that $\deg(f) \geq 2$. We write $f(t) = \sum_{i=0}^{m} a_i t^i$, where $\deg(f) = m$ and $a_i \in \mathbb{Z}$. Then, as $f(t) \in \ker(\mathrm{ev}_\varepsilon)$ and $a_m t^{m-2}(t^2 + t + 1) \in \ker(\mathrm{ev}_\varepsilon)$, it follows that:

$$g(t) = f(t) - a_m t^{m-2}(t^2 + t + 1) = \sum_{i=0}^{m-3} a_i t^i + (a_{m-2} - a_m)t^{m-2} + (a_{m-1} - a_m)t^{m-1} \in \ker(\mathrm{ev}_\varepsilon).$$

Now $\deg(g(t)) \leq m - 1$ and so, by recurrence, we have $g(t) \in (t^2 + t + 1)$. Consequently, $f(t) = g(t) + a_m t^{m-2}(t^2 + t + 1) \in (t^2 + t + 1)$ and so $\ker(\mathrm{ev}_\varepsilon) = (t^2 + t + 1)$.

We now apply the isomorphism theorem to conclude that $\mathbb{Z}[t]/(t^2 + t + 1) \cong \mathbb{Z}[\varepsilon]$.

Exercice 7.
On dit qu'un élément $r \in R$ est *nilpotent* si $r^n = 0$ pour un $n \geq 1$.

On commence par démontrer le fait suivant valide dans n'importe quel anneau commutatif A : si $\lambda \in A^\times$ et $n \in A$ nilpotent, alors $\lambda - n$ est inversible. En effet,

$$\frac{1}{\lambda - n} = \frac{1}{\lambda} \sum_{i=0}^{\infty} (n/\lambda)^i.$$

Ainsi, on voit que tout polynôme $f(t) = \sum_{i=0}^{m} a_i t^i \in R[t]$ avec coefficient constant inversible et tout les autres coefficients nilpotents est inversible. En effet, dans ce cas on peut écrire $f(t) = \tilde{f}(t) - a_0$, avec $\tilde{f}(t)$ un polynôme dont tout les coefficients sont nilpotents. Comme il suit de la formule du binôme qu'une somme d'éléments nilpotents est un élément nilpotent, on voit que $\tilde{f}(t)$ est nilpotent.

Dans ce qui suit, on montre qu'un polynôme inversible est forcément de cette forme.

Soit $f(t) \in (R[t])^\times$. Notons encore $f(t) = \sum_{i=0}^{m} a_i t^i$. On remarque tout d'abord avec $\mathrm{ev}_0 : R[t] \to R$ que $a_0 \in R^\times$. On montre dans ce qui suit que a_i est nilpotent pour $i > 0$. Pour montrer cela, on suppose sans perte de généralité que $a_0 = 1$. On note alors $f(t) = 1 - tg(t)$, et on cherche à démontrer que tout les coefficients du polynôme $g(t)$ sont nilpotents.

On considère l'inclusion $R[t] \subset R[[t]]$. L'inverse de $f(t) = 1 - tg(t)$ dans $R[[t]]$ est (voir remarque après la preuve)

$$\sum_{i=0}^{\infty} t^i (g(t))^i.$$

En effet,

$$(1 - tg(t)) \left(\sum_{i=0}^{\infty} t^i (g(t))^i \right) = \sum_{i=0}^{\infty} t^i (g(t))^i - \sum_{i=1}^{\infty} t^i (g(t))^i = 1.$$

Comme on suppose que $f(t)$ est inversible dans $R[t]$, cet élément est en fait un polynôme, *i.e.* il existe $I \in \mathbb{N}$ tel que pour tout $i \geq I$ on a $t^i (g(t))^i = 0$. Comme t n'est pas un diviseur de zéro, on a même $(g(t))^i = 0$ pour tout $i \geq I$. En particulier, on voit que le coefficient dominant a_m est nilpotent. Maintenant, on peut appliquer l'argument qu'on vient d'appliquer pour $f(t)$ au polynôme $h(t) = f(t) - a_m t^m$ pour conclure que a_{m-1} est nilpotent. Par récurence descendante avec le même procédé, on conclut que tout les coefficients de $g(t)$ sont nilpotents.

Remarque. Pour faire sens de toute somme infinie avec $g(t)$ un polynôme

$$\sum_{i=0}^{\infty} t^i (g(t))^i$$

on laisse le soin au lecteur de vérifier que l'application naturelle $R[[t]] \cong \varprojlim_{n \geq 1} R[t]/(t^n)$ est un isomorphisme, où le terme à droite est,

$$\varprojlim_{n \geq 1} R[t]/(t^n) = \{(f_n(t)) \in \prod_{n \geq 1} R[t]/(t^n) \mid f_{n+1}(t) \equiv f_n(t) \mod t^n \quad \forall n \geq 1\} \subseteq \prod_{n \geq 1} R[t]/(t^n)$$

Ainsi, pour définir un élément de $R[[t]]$ il suffit de le faire de manière compatible dans $R[t]/(t^n)$ pour $n \geq 1$. En particulier la collection indicée par $n \geq 1$,

$$f_n(t) = \sum_{i=0}^{n-1} t^i (g(t))^i \mod t^n$$

défini bel et bien un élément de $R[[t]]$.

Exercice 8. 1. On a $\nu(1) = \nu(1^2) = 2\nu(1)$, donc $\nu(1) = 0$. Comme $0 = \nu(1) = \nu(-1^2) = 2\nu(-1)$, on a également $\nu(-1) = 0$.

2. La stabilité de R_ν par l'addition et la multiplication est assurée par a) et b).

3. Immédiat car si $k \in K$, soit k ou k^{-1} est dans R_ν.

4. Comme $\nu(1) = \nu(-1) = 0$, cela suit par b) par récurrence.

5. Suit par la décomposition en nombres premiers et a).

6. Notons d'abord que pour tout $n \in \mathbb{Z}$ et $q \in \mathbb{Q}$. Alors $\nu(nq) \geq \nu(q)$ par a) et le point 4. Si p et q deux premiers distincts avec $\nu(p), \nu(q)$ non-nuls, alors comme par Bézout il existe $a, b \in \mathbb{Z}$ tel que $ap + bq = 1$,

$$0 = \nu(1) = \nu(ap + bq) \geq \min(\nu(ab), \nu(bq)) \geq \min(\nu(p), \nu(q)) > 0$$

une contradiction.

7. Cela suit par a) si on note $c = \nu(p)$ et le point précédent.

8. Si q est un premier distinct de p, alors $q^{-1} \in R_{\nu_p}$.

EPFL - Printemps 2023	Prof. Zs. Patakfalvi
Anneaux et Corps	**Exercices**
Solutions 3	

Exercice 1. 1. Wrong, for example, one can see that for the inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$, the image of the ideal $(2) \subseteq \mathbb{Z}$ is not an ideal in $\mathbb{Q}$.

2. Correct according to *Lemma 1.4.30.*

Exercice 2.
Assume that $\xi_p^{-1}(I)$ is principal, meaning that $\xi_p^{-1}(I) = (f)$ for some $f \in \mathbb{Z}[t]$. Since I is by definition an additive group, it contains 0, and therefore $p \in \xi_p^{-1}(I) = \mathbb{Z}[t] \cdot f$. It follows that $p = g \cdot f$ for some $g \in \mathbb{Z}[t]$. We recall that by Exercise 5 on Sheet 2, $\deg(f \cdot g) = \deg(f) + \deg(g)$. It follows that

$$0 = \deg(p) = \deg(f \cdot g) = \deg(f) + \deg(g).$$

Therefore, $\deg(f) = 0$ and $\deg(g) = 0$ and so $f, g \in \mathbb{Z}$. But then $p = g \cdot f$. Since p is prime, it follows that either $f = \pm 1$ or $f = \pm p$. If $f = \pm 1$, then $I = \mathbb{F}_p[t]$. If $f = \pm p$, then $I = \{0\}$. Those are contradictions to the assumption and therefore, $\xi_p^{-1}(I)$ is not principal.

Exercice 3. 1. **Identité de Bézout.** Let d be the biggest common divisor of m and n. Define the set $E := \{cm + dn \big| c, d \in \mathbb{Z}\}$. Let $e = am + bn$ be the smallest non-zero positive integer in E. Dividing n by e with rest, we get $n = qe + r$ for some $q \in \mathbb{Z}, 0 \leq r < e$. Then

$$r = n - qe = n - q(am + bn) = \underbrace{(-qa)}_{\in \mathbb{Z}} m + \underbrace{(1 - qb)}_{\in \mathbb{Z}} n \in E.$$

But since $r < e$, it follows that $r = 0$, and therefore $e \big| n$. Similarly, we show that $e \big| m$. It follows that e is a common divisor of m and n. It remains to show that e is indeed the biggest common divisor. Since $d \big| m$ and $d \big| n$, it holds that $d \big| (am + bn) = e$, and hence $e = d$.

2. We have

- $(m)(n) = (mn)$ by *Remarque 1.4.28.*
- $(m) + (n) = (m, n)$ by *Remarque 1.4.28.* According to Bézout, this is equal to (d).
- $(m) \cap (n) = (\text{ppmc}\{m, n\})$. The inclusion $\supseteq$ holds due the definition, which states that $(m) \cap (n)$ contains elements that are simultaneously in (m) and (n), which means that they are simultaneously multiples of (m) and of (n). For the other inclusion, let k be an element contained in $(m) \cap (n)$. That means that k is a multiple of both (m) and (n). Let p be the least common multiple of m and n. As in the first part of this exercise, we can divide k by p with rest, from which it follows that k is a multiple of p, and therefore $k \in (\text{ppmc}\{m, n\})$.

Exercice 4.
Let $\iota_A : \mathbb{Z} \to A$ be the unique ring homomorphism with source $\mathbb{Z}$. By definition, $\text{car}(A) = n$, where $\ker(\iota_A) = (n)$.

1. Consider the composition $\iota_B \colon \mathbb{Z} \xrightarrow{\iota_A} A \xrightarrow{f} B$. Since the kernel of the first homomorphism is contained in the kernel of the composition, it holds that $(n) = \ker(\iota_A) \subseteq \ker(\iota_B) =: (m)$, with m being $\operatorname{car}(B)$. Therefore, $m \big| n$, and so $\operatorname{car}(B) \big| \operatorname{car}(A)$.

   In general, $\operatorname{car}(B) \neq \operatorname{car}(A)$, as one can see when considering the reductions modulo 2, $f : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$.

2. If f is injective, then its kernel is trivial, meaning that $\ker(\iota_A) = \ker(f \circ \iota_A) = \ker(\iota_B)$.

3. In order to show that F is a ring homomorphism, we show that $\forall a, b \in A$,

   - $F(1) = 1^p = 1$,
   - $F(ab) = (ab)^p = a^p b^p = F(a)F(b)$,
   - lastly, $F(a+b) = (a+b)^p = a^p + b^p$. This holds due to the fact that A is commutative, and the fact that the binomial coefficients that would appear for expressions of the form $a^i b^j$, $i, j \neq 0, i, j \neq p$ are all divisible by p, and hence they are zero in A.

4. Denote by g the unique homomorphism $g : \mathbb{Z} \to \mathbb{Z}[i]/(i-2)$. The characteristic of $\mathbb{Z}[i]/(i-2)$ is $k \in \mathbb{Z}$, where $(k) = \ker(g)$. The kernel is $\ker(g) = \{n \in \mathbb{Z} \big| \exists a, b \in \mathbb{Z} \text{ s.t } n = (a+ib)(i-2)\}$. Let $n \in \mathbb{Z}$ be contained in the kernel. Then, with $a, b \in \mathbb{Z}$,

   $$n = (a+ib)(i-2) = (-2a-b) + i(a-2b).$$

   It follows that $n = -5b$, and so $n \in (5)$. Conversely, for $m \in (5)$, we have $m = 5\alpha$ for some $\alpha \in \mathbb{Z}$ and $g(m) = g(5\alpha) = g(5)g(\alpha) = 0$. This shows that $\ker(g) = (5)$.

Exercice 5.
Let $A = \mathbb{Z}/250\mathbb{Z}$.

1. The zero divisors are the divisors of 250 and their multiples, stictly bigger than 1. The divisors of 250 (1 excluded) are $2, 5, 10, 25, 50, 125$ and 250.

   - For the divisor 2, we get 124 multiples, up to the last multiple 248.
   - For the divisor 5, we get 49 multiples, up to the last multiple 245. However, as half of these multiples are even, they have already been counted as multiples of 2. We get 25 new zero divisors.
   - The remaining divisors $10, 25, 50$ and 125 are multiples of 5 and have therefore already been counted into those zero divisors.

   Summing up, we get $124 + 25 = 149$ zero divisors.

   The remaining 100 elements are all invertible. Such an element $x \in A$ is prime to 250, meaning that x and 250 don't have any common divisors other than 1. With Bézout's identity there are two $a, b \in \mathbb{Z}$ such that $1 = ax + b \cdot 250$. With this, $ax \equiv 1 \bmod 250$.

2. By the correspondence described in *Propositon 1.4.36*, the ideals of $A = \mathbb{Z}/250\mathbb{Z}$ correspond to ideals of $\mathbb{Z}$ which contain (250). Ideals of $\mathbb{Z}$ are principal, of the form (n). With $(250) \subseteq (n)$ we get that $n \big| 250$ and so $n = 1, 2, 5, 10, 25, 50, 125$ and 250. Additionally, if the ideal in A contains 50, then the ideals in $\mathbb{Z}$ need to contain the preimage of the class [50]. In particular, they need to contain 50. Hence n is reduced to $1, 2, 5, 10, 25, 50$. The ideals in A are $A, ([2]), ([5]), ([10]), ([25])$ and $([50])$.

Exercice 6.

Soit A le sous-anneau de $M_2(\mathbb{Z})$ des matrices de la forme $\begin{pmatrix} a & c \\ 0 & b \end{pmatrix}$ où $a, b, c \in \mathbb{Z}$. Montrer que le sous-ensemble K des matrices pour lesquelles $5 \mid a$ et $11 \mid b$ est un idéal bilatère et construire un isomorphisme (en deux temps) $A/K \to \mathbb{Z}/5 \times \mathbb{Z}/11$.

One verifies easily that the subset K is an additive subgroup, and that the product of a matrix in A and a matrix in K is a matrix in K, with multiplication in both directions. Therefore, K is a two-sided ideal.

To construct the isomorphism, we define the ideal I as

$$I := \left\{ \begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix} \middle| c \in \mathbb{Z} \right\}.$$

Again, verifying that this is an ideal is easy. Since $I \subset K$, we may apply the *Proposition 1.4.39 (Quotient en deux temps).* Let $\xi : A \to A/I$. Then,

$$A/K \cong (A/I)/\xi(K).$$

We have that

$$\xi(K) = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle| a, b \in \mathbb{Z}, 5 \mid a, 11 \mid b \right\}.$$

Furthermore, we note that A/I can be described as classes of matrices with representatives of the form $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ with $a, b \in \mathbb{Z}$. This is isomorphic to $\mathbb{Z} \times \mathbb{Z}$ via the obvious isomorphism

$$\phi : \begin{array}{ccc} A/I & \to & \mathbb{Z} \times \mathbb{Z} \\ \left[\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \right] & \mapsto & (a, b) \end{array}.$$

With ϕ, $\xi(K)$ is sent to $(5) \times (11)$, and therefore, $(A/I)/\xi(K) \cong (\mathbb{Z} \times \mathbb{Z})/((5) \times (11)) \cong \mathbb{Z}/(5) \times \mathbb{Z}/(11)$.

Exercice 7.

1. We use *Proposition 1.2.2.* applied to the identity on $\mathbb{C}[y]$. The proposition then states that there exists a unique ring homomorphism $ev_0 : \mathbb{C}[y][x] \to \mathbb{C}[y]$ s.t. $id_{\mathbb{C}[y]} = \iota \circ ev_0$, where ι denotes the inclusion $\iota : \mathbb{C}[y] \to \mathbb{C}[y][x]$. ev_0 acts by sending a polynomial $p(x, y) \in \mathbb{C}[y][x] \cong \mathbb{C}[x, y]$ to $p(0, y) \in \mathbb{C}[y]$. One easily verifies that ev_0 is surjective, as the identity on $\mathbb{C}[y]$ is surjective. The kernel of ev_0 consists of all polynomials $p(x, y) \in \mathbb{C}[x, y]$ for which $p(0, y) = 0$. These are exactly those polynomials that are multiples of x, and hence $\ker(ev_0) = (x)$. By the isomorphism theorem it follows that $\mathbb{C}[y] \cong \mathbb{C}[x, y]/(x)$.

2. As above, consider the two evaluations

$$ev_{0,x} := \begin{array}{ccc} \mathbb{C}[x, y] & \to & \mathbb{C}[y] \\ p(x, y) & \mapsto & p(0, y) \end{array}, \quad ev_{0,y} := \begin{array}{ccc} \mathbb{C}[x, y] & \to & \mathbb{C}[x] \\ p(x, y) & \mapsto & p(x, 0) \end{array}.$$

It holds that $\ker(ev_{0,y}) = (y)$. Using the universal property of products, *Proposition 1.4.45*, we get a unique homomorphism

$$\phi : \begin{array}{ccc} \mathbb{C}[x, y] & \to & \mathbb{C}[x] \times \mathbb{C}[y] \\ p(x, y) & \mapsto & (p(x, 0), p(0, y)) \end{array}.$$

The kernel of ϕ is equal to $\ker(ev_{0,x}) \cap \ker(ev_{0,y}) = (x) \cap (y) = (xy)$.

3. We note that for a polynomial $p(x,y) \in \mathbb{C}[x,y]$ the constant term of $ev_{0,x}(p)$ and of $ev_{0,y}(p)$ is the same. This suggests that the image of ϕ is as stated. To show that every such element is in the image of ϕ, we let $p(x) \in \mathbb{C}[x]$ and $q(y) \in \mathbb{C}[y]$. Consider the pair $(a + xp(x), a + yq(y)) \in \mathbb{C}[x] \times \mathbb{C}[y]$ with $a \in \mathbb{C}$. Then

$$\phi(a + xp(x) + yq(y)) = (a + xp(x), a + yq(y)).$$

Therefore, the pair $(a + xp_x(x), a + yp_y(y))$ is contained in the image of ϕ. We conclude with the isomorphism theorem.

Exercice 8. 1. By the definition of a valuation we have that $\nu_p(q^{-1}) = 0$ too, because $\nu_p(q) + \nu_p(q^{-1}) = \nu_p(1) = 0$. Therefore $q^{-1} \in R$ and q is invertible.

2. The zero ideal is trivially an ideal of R. Now, take a non-zero ideal I, and let n be the smallest valuation that appears among the elements of I. Then there is an element of the form $y = p^n q$, where q is a unit. Take now any $x \in I$ non-zero. Then $\nu_p(x/y) \geq 0$, again by the properties of valuations and by the minimality of n, hence $x/y \in R$, and hence $I = (y)$

3. Consider the composition $\phi : \mathbb{Z} \to R \to R/(p^n)$. Where the first map is the inclusion and the second one is the quotient map. Then we can apply the isomorphism theorem to $\mathbb{Z}$, because

   a) ϕ is surjective because let $a/b \in R$ (with $a, b \in \mathbb{Z}$ and $p \nmid b$). Then we can write $cp^n + db = 1$ for some $c, d \in \mathbb{Z}$. Hence $[d][b] = [1] \in R/(p^n)$. Hence, for every $[ab^{-1}]$ in $R/(p^n)$ we have $[a][b^{-1}] = [a][b^{-1}][b][d] = [a][d] = [ad] = \phi(ad)$.

   b) The kernel of ϕ is generated by p^n as an ideal of $\mathbb{Z}$, because if x is in the kernel, that means that $x = (a/b)p^n \in R$, where a and b are as in the previous point. That is, $bx = ap^n$. Now, using that $p \nmid b$ we obtain that p^n divides $x \in \mathbb{Z}$.

4. From the previous points we know all the non-trivial ideals of R_p are of the form (p^n) for some $n \in \mathbb{N}$, and we know that their quotient is isomorphic to $\mathbb{Z}/(p^n)$. If R_p and R_q were isomorphic for two different prime numbers p and q, there would be isomorphism between their quotients. This is impossible because $\mathbb{Z}/p^m\mathbb{Z}$ and $\mathbb{Z}/q^n\mathbb{Z}$ are not isomorphic since their size is different (p^m and q^n respectively). Moreover, R_p is not isomorphic to $\mathbb{Z}$. Indeed, if we take q a prime number different from p, then $\mathbb{Z}/q\mathbb{Z}$ is a quotient of size q, and R_p has no quotients of such size.

EPFL - Printemps 2023 | Prof. Zs. Patakfalvi
Anneaux et Corps | **Exercices**
Solutions 4

Exercice 1. 1. $(0) \subset \mathbb{Z}$ est premier car $\mathbb{Z}$ est intègre (Proposition 1.5.2), non maximal car $(0) \subsetneq (2)$.

2. $(t) \subset \mathbb{Z}[t]$ est premier car le quotient $\mathbb{Z}$ est intègre, non maximal car $(t) \subsetneq (t, 2) \neq \mathbb{Z}[t]$.
3. $(t) \subset \mathbb{R}[t]$ est premier et maximal car le quotient est un corps.
4. $(101) \subset \mathbb{Z}[t]$ est premier. En effet, considérons l'homomorphisme

$$\xi \colon \mathbb{Z}[t] \longrightarrow (\mathbb{Z}/101\mathbb{Z})[t], \quad \sum_i a_i t^i \mapsto \sum_i [a_i]_{101} t^i.$$

Il est clair que $f(t) = \sum_i a_i t^i \in \ker \xi$ si et seulement si $[a_i]_{101} = 0$ pour chaque i, donc si et seulement si 101 divise chaque coefficient, donc si et seulement 101 divise $f(t)$. Cela prouve que $\ker \xi = (101)$. Pour conclure, il suffit de montrer que $(\mathbb{Z}/101\mathbb{Z})[t]$ est un anneau intègre. Puisque 101 est un nombre premier, $\mathbb{Z}/101\mathbb{Z}$ est un anneau intègre. De manière générale, si A est un anneau intègre alors $A[t]$ est aussi intègre (la preuve est un bon exercice), ce qui conclut.

5. $(42) \subset \mathbb{Z}[t]$ n'est pas premier car $6 \cdot 7 = 42$, donc non maximal.
6. $(t^2 - 2) \subset \mathbb{Z}[t]$ est premier. En effet, considérons l'homomorphisme d'évaluation

$$\mathrm{ev}_{\sqrt{2}} \colon \mathbb{Z}[t] \longrightarrow \mathbb{R}, \quad t \mapsto \sqrt{2}.$$

On montre comme dans l'Exemple 1.4.18 que $\ker \mathrm{ev}_{\sqrt{2}} = (t^2 - 2)$. Comme $\mathbb{Z}[t]/(t^2 - 2)$ est isomorphe à un sous-anneau de $\mathbb{R}$, c'est un anneau intègre, et donc $(t^2 - 2)$ est premier.
Ce n'est pas un ideal maximal, puisque $(t^2 - 2) \subsetneq (t^2 - 2, 3) \neq \mathbb{Z}[t]$. Alternativement, on peut vérifier que $\mathrm{im}\, \mathrm{ev}_{\sqrt{2}} = \mathbb{Z}[\sqrt{2}]$ n'est pas un corps (par exemple 3 n'a pas d'inverse).

7. $(t^2 - 2) \subset \mathbb{R}[t]$ n'est pas premier car $t^2 - 2 = (t - \sqrt{2})(t + \sqrt{2})$ dans $\mathbb{R}[t]$.
8. $(t + 5, 10) \subset \mathbb{Z}[t]$ n'est pas premier car $10 = 2 \cdot 5$.
9. $(t + 5, 11) \subset \mathbb{Z}[t]$ est maximal (donc premier) car le quotient est le corps $\mathbb{Z}/11\mathbb{Z}$.
10. $(t^2 + 1, 2) \subset \mathbb{Z}[t]$ n'est pas premier car $(t + 1)^2 = t^2 + 1 + 2t \in (t^2 + 1, 2)$.

Exercice 2. 1. Le premier système n'a pas de solutions. En effet, si $x = 7 + 12k$, alors $x = 1 + 3 \cdot (2 + 4k)$, ce qui contredit $x \equiv 2 \pmod 3$.
Le second système admet une infinité de solutions. En effet, si $x = 8 + 12k$, alors $x = 2 + 3 \cdot (2 + 4k)$. Donc le système est équivalent à $x \equiv 8 \pmod{12}$, qui admet une infinité de solutions.

2. Pour voir que $\mathbb{Z}/36\mathbb{Z} \ncong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ on peut par exemple utiliser le fait que le deuxième anneau n'est pas cyclique en tant que groupe abélien : tout élément est d'ordre un diviseur de 12.

Exercice 3. 1. Prenons $x \in f^{-1}(I)$. Alors $f(x) \in I$ et, par définition de I, on peut écrire

$$f(x) = \sum_{i=1}^{n} \beta_i b_i, \quad \text{pour certains } \beta_i \in B.$$

Puisque f est surjective, on peut choisir des $\alpha_i \in A$ tels que $f(\alpha_i) = \beta_i$. Posons

$$x' := \sum_{i=1}^{n} \alpha_i c_i.$$

Par construction $f(x) = f(x')$, et donc $x - x' \in \ker f$. Ainsi il existe des $\gamma_i \in A$ tels que

$$x - x' = \sum_{i=1}^{m} \gamma_i a_i$$

et cette égalité se réarrange en

$$x = \sum_{i=1}^{m} \gamma_i a_i + \sum_{i=1}^{n} \alpha_i c_i \in (a_1, \ldots, a_m, c_1, \ldots, c_n).$$

Comme x est arbitraire, cela montre que $f^{-1}(I) \subseteq (a_1, \ldots, a_m, c_1, \ldots, c_n)$. L'inclusion inverse est immédiate, puisque

$$f(a_i), f(c_j) \in I \quad \forall i, j.$$

On a donc démontré l'égalité désirée.

2. L'Exemple 1.4.10.a montre que $\ker \mathrm{ev}_b = (y - b)$ et $\ker \mathrm{ev}_a = (x - a)$. Puisque $\ker \xi = \mathrm{ev}_b^{-1}(\ker \mathrm{ev}_a)$ (l'égalité est facile à vérifier), par le point précédent on obtient que $\ker \xi = (x - a, y - b)$.
   Puisque $\xi(\lambda) = \lambda$ pour tout $\lambda \in k$, on voit que ξ est surjective. Par le premier théorème d'isomorphisme, on obtient $k \cong k[x, y]/\ker \xi$. Par la Proposition 1.5.5, on obtient que $\ker \xi$ est un idéal maximal.

Exercice 4.
Nota bene : la discussion des deux derniers points de cet exercice pourra être grandement simplifiée une fois à disposition les propriétés des polynômes irréductibles.

1. Par l'Exemple 1.4.18 on a $\mathbb{Z}[i] \cong \mathbb{Z}[t]/(t^2 + 1)$. Par la Proposition 1.4.41 on a

$$\mathbb{Z}[i]/(p) \cong \frac{\mathbb{Z}[t]/(t^2+1)}{p \cdot (\mathbb{Z}[t]/(t^2+1))} \cong \mathbb{Z}[t]/(p, t^2 + 1) \cong \frac{\mathbb{Z}[t]/(p)}{(t^2 + [1]_p) \cdot (\mathbb{Z}[t]/(p))} \cong \mathbb{F}_p[t]/(t^2 + [1]_p).$$

2. Dans le cas où $p = 5$, on remarque que $[2]_5$ et $[3]_5$ sont des racines de $t^2 + [1]_5 \in \mathbb{F}_5[t]$. En particulier on a la factorisation

$$t^2 + [1]_5 = (t - [2]_5) \cdot (t - [3]_5). \tag{1}$$

   Remarquez que $(t - [2]_5) - (t - [3]_5) = [1]_p$. Donc les idéaux générés respectivement par $t - [2]_5$ et par $t - [3]_5$ sont premiers entre eux. Le théorème des restes chinois (Théorème 1.4.50) donne alors

$$\frac{\mathbb{F}_5[t]}{(t - [2]_5) \cap (t - [3]_5)} \cong \frac{\mathbb{F}_5[t]}{(t - [2]_5)} \times \frac{\mathbb{F}_5[t]}{(t - [3]_5)}. \tag{2}$$

   L'évaluation en $t = [2]_5$ induit un ismorphisme

$$\mathbb{F}_5 \cong \frac{\mathbb{F}_5[t]}{(t - [2]_5)}$$

   et d'une manière similaire on a

$$\mathbb{F}_5 \cong \frac{\mathbb{F}_5[t]}{(t - [3]_5)}.$$

   On prétend pour finir que $(t - [2]_5) \cap (t - [3]_5) = (t^2 + [1]_5)$. L'inclusion $\supseteq$ est claire, en vue de la factorisation (1). Inversément, prenons un élément $f(t)$ appartenant à l'intersection des deux idéaux. On peut écrire

$$(t - [2])g(t) = f(t) = (t - [3])h(t)$$

pour certains $g(t), h(t) \in \mathbb{F}_5[t]$. Considérons l'image de $f(t)$ par l'évaluation $\mathrm{ev}_{[2]}$ en $t = [2]$. On a

$$\mathrm{ev}_{[2]}(f(t)) = \mathrm{ev}_{[2]}((t-[2])g(t)) = 0$$

d'une part, et

$$\mathrm{ev}_{[2]}(f(t)) = \mathrm{ev}_{[2]}((t-[3])h(t)) = -\mathrm{ev}_{[2]}(h(t))$$

d'autre part. Ainsi $\mathrm{ev}_{[2]}(h(t)) = 0$, et puisque $\ker \mathrm{ev}_{[2]} = (t-[2])$ on en déduit que $h(t) = (t-[2])j(t)$ pour un certain $j(t) \in \mathbb{F}_5[t]$. On peut ainsi écrire

$$f(t) = (t-[3])(t-[2])j(t) = (t^2+[1])j(t)$$

ce qui montre que $f(t) \in (t^2+[1])$.
En combinant tout cela dans (2), on obtient

$$\frac{\mathbb{F}_5[t]}{(t^2+[1])} \cong \mathbb{F}_5 \times \mathbb{F}_5,$$

ce qui implique que $\mathbb{Z}[i]/(5) \cong \mathbb{F}_5 \times \mathbb{F}_5$ en vue du point précédent.

3. On prétend qu'*il existe un isomorphisme $\mathbb{Z}[i]/(p) \cong \mathbb{F}_p \times \mathbb{F}_p$ si et seulement si -1 possède deux racines carrées distinctes modulo p.*
   Supposons d'abord que l'on puisse écrire $a^2 = [-1]_p = b^2$ dans $\mathbb{F}_p$ avec $a \neq b$. Puisque $\ker \mathrm{ev}_a = (t-a)$, on peut écrire

$$t^2 + [1]_p = (t-a)(t-b')$$

et on prétend que $b' = b$. En effet,

$$\mathbb{F}_p \ni 0 = b^2 + [1] = \mathrm{ev}_b(t^2+[1]) = \underbrace{(b-a)}_{\neq 0}(b-b')$$

et comme $\mathbb{F}_p$ est intègre, on obtient que $b - b' = 0$. De plus, $(t-a) - (t-b) = b - a \neq 0$ est un élément inversible de $\mathbb{F}_p$, donc les idéaux $(t-a)$ et $(t-b)$ sont premiers entre eux. En appliquant le théorème des restes chinois comme dans la partie précédente, on trouve que

$$\frac{\mathbb{F}_p[t]}{(t-a)\cap(t-b)} \cong \mathbb{F}_p \times \mathbb{F}_p.$$

Puisque $b - a \neq 0$ est inversible dans $\mathbb{F}_p$, on obtient comme dans le point précédent que $(t-a)\cap(t-b) = (t^2+[1])$ (où l'on avait utilisé que $[2]_5 - [3]_5 = -[1]_5$ est inversible dans $\mathbb{F}_5$), et donc que

$$\mathbb{Z}[i]/(p) \cong \frac{\mathbb{F}_p[t]}{(t^2+[1])} \cong \mathbb{F}_p \times \mathbb{F}_p.$$

Remarquons si $a \in \mathbb{F}_p$ est une racine carrée de $[-1]_p$, alors $-a$ en est aussi une. Or si $p \neq 2$ on a $a \neq -a$. Il nous reste ainsi à traiter deux cas : celui de $p = 2$, et celui où $[-1]_p$ n'a pas de racine carrée dans $\mathbb{F}_p$.
Commençons avec le cas $p = 2$. Alors $t^2 + [1]_2 = (t + [1]_2)^2$, et ainsi il existe un élément $0 \neq x$ de $\mathbb{F}_2[t]/(t^2+[1])$ tel que $x^2 = 0$ (on dit que cet anneau quotient est *non-réduit*) : on peut prendre x comme étant l'image de $t + [1]_2$ dans le quotient. Or il n'existe pas d'élément non-nul dans $\mathbb{F}_2 \times \mathbb{F}_2$ satisfaisant une telle propriété, donc il ne peut y avoir d'isomorphisme entre ces deux anneaux.
Pour finir, supposons qu'il n'existe pas de racine carrée de -1 dans $\mathbb{F}_p$. On prétend que $\mathbb{F}_p[t]/(t^2+[1])$ est un anneau intègre. Fixons une clotûre algébrique $\overline{\mathbb{F}_p}$ de $\mathbb{F}_p$, et choisissons une racine carrée $i \in \overline{\mathbb{F}_p}$ de -1. On considère l'homomorphisme d'évaluation

$$\mathrm{ev}_i \colon \mathbb{F}_p[t] \longrightarrow \overline{\mathbb{F}_p}, \quad t \mapsto i.$$

Puisque $\mathbb{F}_p[t]/\ker \mathrm{ev}_i \cong \mathrm{im}\,\mathrm{ev}_i \subset \overline{\mathbb{F}_p}$ et que $\overline{\mathbb{F}_p}$ est intègre, on voit que $\mathbb{F}_p[t]/\ker \mathrm{ev}_i$ est un anneau intègre. On prétend que $\ker \mathrm{ev}_i = (t^2 + [1]_p)$. L'argument est le similaire à celui de l'Exemple 1.4.18. Pour finir, on prétend que $\mathbb{F}_p[t]/(t^2 + [1])$ n'est pas isomorphe à $\mathbb{F}_p \times \mathbb{F}_p$: en effet, cet anneau produit n'est pas intègre.

Exercice 5.
Soit $J \leq A \times B$ un idéal. Noter que $(0,1)J \leq \{0\} \times B$ et $(1,0)J \leq A \times \{0\}$ sont des idéaux de $A \times B$ inclus dans J. De plus, noter que $J = (1,0)J \times (0,1)J$. On conclut donc que tout idéal du produit est de la forme $I_A \times I_B$ pour I_A et I_B des idéaux quelconques de A et B respectivement.

En ce qui est des idéaux premiers, on voit en utilisant qu'un idéal est premier si et seulement si le quotient par cet idéal est intègre que les idéaux premiers sont de la forme

$$\mathfrak{p}_A \times B \quad A \times \mathfrak{p}_B$$

pour $\mathfrak{p}_A$ et $\mathfrak{p}_B$ des idéaux premiers de A et B respectivement.

Exercice 6.
On suppose d'abord que R est intègre. Grâce à la formule du degré, on voit que $R[t]^\times = R^\times$, donc les inversibles de R en degré zéro.

On traite maintenant le cas général. Soit $\mathfrak{p}$ in idéal premier de R. Soit $f(t)$ un élément inversible. L'image dans $(R/\mathfrak{p})[t]$ est encore inversible. Ainsi, par le cas intègre, on voit que les coefficients en degré strictement positif de $f(t)$ sont dans l'idéal $\mathfrak{p}$ et le terme constant n'est pas dans l'idéal. Ainsi, comme $\mathfrak{p}$ est quelconque,*

$$R[t]^\times \subseteq t\,\mathrm{nil}(R)[t] + R^\times.$$

L'inclusion inverse est également vérifiée. En effet, si $f(t) \in t\,\mathrm{nil}(R)[t] + R^\times$, alors $f(t) - a_0$ est nilpotent car c'est une somme d'éléments nilpotents. On conclut par le fait suivant valide dans n'importe quel anneau commutatif A : si $\lambda \in A^\times$ et $n \in A$ nilpotent, alors $\lambda - n$ est inversible. En effet,

$$\frac{1}{\lambda - n} = \frac{1}{\lambda} \sum_{i=0}^{\infty} (n/\lambda)^i.$$

Exercice 7.
To see that $D(A)$ is a sub-ring of $\mathrm{End}_K(A)$ as

$$[\varphi \circ \psi, m_a] = \varphi \circ [\psi, m_a] + [\varphi, m_a] \circ \psi$$

a double induction on n and m if $\varphi \in D_{\leq n}(A)$ and $\psi \in D_{\leq m}(A)$ concludes.

1. Before we show that the Lie bracket is K-bilinear, we first mention the K-vector space structure of $D(K[x])$. As $K \subset K[x]$, the scalar multiplication in $K[x]$ is just defined by the usual multiplication in $K[x]$. Elements of $D(K[x])$ are K-linear transformations $K[x] \to K[x]$. Therefore, scalar multiplication can be defined for $\phi \in D([K[x]])$ and $\lambda \in K$ as

   $$(\lambda\phi)(p(x)) = \lambda\dot{\phi}(p(x)) \in K[x]$$

   for $p(x) \in K[x]$. This is equivalent to $\lambda\phi = m_\lambda \circ \phi$.
   We note that since ϕ is by definition K-linear, it holds that for all $p(x) \in K[x]$, and for all $\lambda \in K$

   $$\phi(\lambda p(x)) = \lambda\phi(p(x))$$

   and therefore $\phi \circ m_\lambda = m_\lambda \circ \phi$.
   Now onto the exercise, let $F, F_1, F_2, G \in D(K[x])$ and $\lambda \in K$. To show K-bilinearity we show that

*. Un élément dans l'intersection de tout les premiers est nilpotent. Un élément dans aucun idéal maximal est inversible. Notons également que pour voir que le terme constant de $f(t)$ est inversible on peut évaluer en zéro.

— $[F_1 + F_2, G] = [F_1, G] + [F_2, G]$. By the distributive property of a ring, we have

$$\begin{aligned}[F_1 + F_2, G] &= (F_1 + F_2) \circ G - G \circ (F_1 + F_2) = F_1 \circ G + F_2 \circ G - G \circ F_1 - G \circ F_2 \\ &= F_1 \circ G - G \circ F_1 + F_2 \circ G - G \circ F_2 = [F_1, G] + [F_2, G]\end{aligned}$$

— $[\lambda F, G] = \lambda[F, G]$. Due to the remark above, for all $\lambda \in K$, we have $G \circ m_\lambda = m_\lambda \circ G$. Additionally, we use the associativity of the composition to get

$$\begin{aligned}[\lambda F, G] = [m_\lambda \circ F, G] &= (m_\lambda \circ F) \circ G - G \circ (m_\lambda \circ F) = m_\lambda \circ (F \circ G) - (G \circ m_\lambda) \circ F \\ &= m_\lambda \circ (F \circ G) - (m_\lambda \circ G) \circ F = m_\lambda \circ (F \circ G - G \circ F) = m_\lambda \circ [F, G] = \lambda[F, G]\end{aligned}$$

The same properties for the second components are analogous.

2. Let $p(x) = \sum_{i=0}^{n} a_i x^i \in K[x]$. We exhibit how $\left[\frac{\partial}{\partial x}, m_x\right]$ acts on this polynomial and compare it to the action of m_1. Using K-linearity of $\frac{\partial}{\partial x}$, we get

$$\begin{aligned}\left[\frac{\partial}{\partial x}, m_x\right](p(x)) &= \left[\frac{\partial}{\partial x}, m_x\right]\left(\sum_{i=0}^{n} a_i x^i\right) \\ &= \frac{\partial}{\partial x}\left(m_x\left(\sum_{i=0}^{n} a_i x^i\right)\right) - m_x\left(\frac{\partial}{\partial x}\left(\sum_{i=0}^{n} a_i x^i\right)\right) \\ &= \frac{\partial}{\partial x}\left(\sum_{i=0}^{n} a_i x^i \cdot x\right) - m_x\left(\sum_{i=0}^{n} a_i \frac{\partial}{\partial x}\left(x^i\right)\right) \\ &= \frac{\partial}{\partial x}\left(\sum_{i=0}^{n} a_i x^{i+1}\right) - m_x\left(\sum_{i=1}^{n} a_i \cdot i \cdot x^{(i-1)})\right) \\ &= \sum_{i=0}^{n} a_i \frac{\partial}{\partial x}\left(x^{i+1}\right) - \sum_{i=1}^{n} a_i \cdot i \cdot x^{(i-1)} \cdot x \\ &= \sum_{i=0}^{n} a_i \cdot (i+1) x^i - \sum_{i=1}^{n} a_i \cdot i \cdot x^i \\ &= \sum_{i=1}^{n} a_i \cdot i \cdot x^i + \sum_{i=0}^{n} a_i x^i - \sum_{i=1}^{n} a_i \cdot i \cdot x^i \\ &= \sum_{i=0}^{n} a_i x^i = p(x) = m_1(p(x)).\end{aligned}$$

3. Let $p(x) = \sum_{i=0}^{n} a_i x^i \in K[x]$. We exhibit how $\left[\frac{\partial}{\partial x}, m_{x^j}\right]$ acts on this polynomial and compare

it to the action of $j \cdot m_{x^{(j-1)}}$. Using K-linearity of $\frac{\partial}{\partial x}$, we get

$$\begin{aligned}
\left[\frac{\partial}{\partial x}, m_{x^j}\right](p(x)) &= \left[\frac{\partial}{\partial x}, m_{x^j}\right]\left(\sum_{i=0}^{n} a_i x^i\right) \\
&= \frac{\partial}{\partial x}\left(m_{x^j}\left(\sum_{i=0}^{n} a_i x^i\right)\right) - m_{x^j}\left(\frac{\partial}{\partial x}\left(\sum_{i=0}^{n} a_i x^i\right)\right) \\
&= \frac{\partial}{\partial x}\left(\sum_{i=0}^{n} a_i x^i \cdot x^j\right) - m_{x^j}\left(\sum_{i=0}^{n} a_i \frac{\partial}{\partial x}\left(x^i\right)\right) \\
&= \frac{\partial}{\partial x}\left(\sum_{i=0}^{n} a_i x^{i+j}\right) - m_{x^j}\left(\sum_{i=1}^{n} a_i \cdot i \cdot x^{(i-1)}\right) \\
&= \sum_{i=0}^{n} a_i \frac{\partial}{\partial x}\left(x^{i+j}\right) - \sum_{i=1}^{n} a_i \cdot i \cdot x^{(i-1)} \cdot x^j \\
&= \sum_{i=0}^{n} a_i \cdot (i+j) x^{(i+j-1)} - \sum_{i=1}^{n} a_i \cdot i \cdot x^{(i+j-1)} \\
&= \sum_{i=1}^{n} a_i \cdot i \cdot x^{(i+j-1)} + \sum_{i=0}^{n} a_i \cdot j \cdot x^{(i+j-1)} - \sum_{i=1}^{n} a_i \cdot i \cdot x^{(i+j-1)} \\
&= j \cdot x^{(j-1)} \sum_{i=0}^{n} a_i x^{(i)} = j \cdot x^{(j-1)} p(x) = j \cdot m_{x^{(j-1)}}(p(x)).
\end{aligned}$$

4. By definition, a differential operator ϕ is of degree 1 if $[\phi, m_p]$ is a differential operator of degree 0 for all $p \in K[x]$. This means that $[\phi, m_p] = m_q$ for some $q \in K[x]$.
Let $p(x) = \sum_{i=0}^{n} a_i x^i \in K[x]$. Note that $m_{p(x)} = \sum_{i=0}^{n} a_i m_{x^i}$. Then, using the K-bilinearity of the Lie brackets and the third part of the exercise, we get

$$\begin{aligned}
\left[\frac{\partial}{\partial x}, m_p\right] &= \left[\frac{\partial}{\partial x}, \sum_{i=0}^{n} a_i m_{x^i}\right] = \sum_{i=0}^{n} a_i \left[\frac{\partial}{\partial x}, m_{x^i}\right] \\
&= \sum_{i=1}^{n} a_i \cdot i \cdot m_{x^{i-1}} = m_{\sum_{i=1}^{n} a_i \cdot i \cdot x^{i-1}} = m_{\sum_{j=0}^{n-1} a_{j+1} \cdot (j+1) \cdot x^j}.
\end{aligned}$$

We conclude with the fact that $\sum_{j=0}^{n-1} a_{j+1} \cdot (j+1) \cdot x^j \in K[x]$. Furthermore, $\sum_{j=0}^{n-1} a_{j+1} \cdot (j+1) \cdot x^j = \frac{\partial}{\partial x}(p(x))$.

Exercice 1. (a) Notons tout d'abord qu'un élément de $x \in k[t]/t^2$ s'écrit uniquement sous la forme $x = \lambda + \mu t$ avec $\lambda, \mu \in k$. Notons aussi qu'un élément est inversible si et seulement si $\lambda \neq 0$. En effet si $\lambda = 0$, on a que x est nilpotent, et si $\lambda \neq 0$, on a $x^{-1} = \lambda^{-1}(1 - \mu\lambda^{-1}t)$. Autrement dit on a $(t) = (k[t]/t^2) \setminus (k[t]/t^2)^\times$. Comme tout idéal propre est inclus dans $(k[t]/t^2) \setminus (k[t]/t^2)^\times = (t)$ (sinon l'idéal contient un inversible et n'est pas propre), on obtient par le théorème de correspondance que les idéaux propres de $k[t]/t^2$ sont en bijection avec les idéaux J de $k[t]$ tel que

$$(t^2) \subset J \subset (t).$$

Mais comme $(t)/(t^2)$ est un k-espace vectoriel de dimension 1, on voit que $J = (t^2)$ ou $J = (t)$.

On conclut que les idéaux sont : l'idéal impropre, l'idéal nul et l'unique idéal maximal (t).

(b) Let $I \subseteq M \subseteq A$ be two ideal in A. By Proposition 1.4.41 we have that:

$$A/M \cong (A/I)\Big/\pi(M).$$

Now M is a maximal ideal in A if and only if A/M is a field. Now, by the above, A/M is a field if and only if $(A/I)\Big/\pi(M)$ is a field, hence if and only if $\pi(M)$ is a maximal ideal in A/I.

Exercice 2. (a) Let $f(t), g(t) \in A[t]$. We have that

$$\mathrm{ev}(f+g)(a) = (f+g)(a) = f(a) + g(a) = \mathrm{ev}(f)(a) + \mathrm{ev}(g)(a) = (\mathrm{ev}(f) + \mathrm{ev}(g))(a)$$

for all $a \in A$. Therefore $\mathrm{ev}(f+g) = \mathrm{ev}(f) + \mathrm{ev}(g)$.

Similarly,

$$\mathrm{ev}(fg)(a) = (fg)(a) = f(a)g(a) = \mathrm{ev}(f)(a)\,\mathrm{ev}(g)(a) = (\mathrm{ev}(f)\,\mathrm{ev}(g))(a)$$

for all $a \in A$. Therefore $\mathrm{ev}(fg) = \mathrm{ev}(f)\,\mathrm{ev}(g)$.

Lastly, we have that $\mathrm{ev}(1)(a) = 1$ for all $a \in A$ and thus $\mathrm{ev}(1) = 1$, where the constant polynomial function 1 is the unity of $\mathcal{F}(A)$.

(b) Let $A = \mathbb{Z}/p\mathbb{Z}$ and let $f(t) = t^p - t \in A[t]$. Then $\mathrm{ev}(f)(a) = f(a) = a^p - a = 0$ for all $a \in A$ and thus $f \in \ker(\mathrm{ev})$.

(c) Let $A = \mathbb{R}$ and let $f(t) \in \ker(\mathrm{ev})$. Then, for all $a \in \mathbb{R}$ we have that $\mathrm{ev}(f)(a) = f(a) = 0$, which implies that all elements of $\mathbb{R}$ are roots of f. As f can have at most $\deg(f)$ real roots, we conclude that $f = 0$.

Exercice 3. 1. Soit $f(x,y) \in k[x,y]/(x^2y^3)$ nilpotent. On écrit $f(x,y) = xyh_1(x,y) + xh_2(x) + yh_2(y) + \lambda$, avec $\lambda \in k$. Comme xy est nilpotent, il suit que $xh_2(x) + yh_2(y) + \lambda$ est nilpotent. Comme l'image dans le quotient par (x) et (y) dans $k[y]$ et $k[x]$ respectivement est encore nilpotente et que ces anneaux sont intègres, il suit que $h_2(x) = h_2(y) = \lambda = 0$. Dès lors on conclut que $\mathrm{nil}(A) = (xy)$.

On peut aussi utiliser que les éléments nilpotents sont l'intersection de tous les premiers (Théorème 2.5.17). Comme (x) et (y) sont premiers, on a $\mathrm{nil}(A) \subset (x) \cap (y) = (xy)$. *Comme l'autre inclusion est également vérifiée, on a égalité.*

2. Notons que $(x) \cap (y) = (xy)$. En effet si $f(x,y) \in (x) \cap (y)$ alors $f(x,y) = xh_1(x,y) = yh_2(x,y)$. Comme (x) est un idéal premier, et que $y \notin (x)$ il suit que $h_2(x,y) \in (x)$, et donc que $f(x,y) \in (xy)$. Dès lors $\mathrm{nil}(A) = (x) \cap (y)$. Cette intersection est bien minimale, en effet sinon $\mathrm{nil}(A)$ serait premier. Mais $x, y \notin \mathrm{nil}(A)$ et $xy \in \mathrm{nil}(A)$.

3. Si $\mathfrak{p}$ est un premier qui contient x^2y^3, alors x ou y appartient à $\mathfrak{p}$ comme cet idéal est premier. Ainsi (x) ou (y) est inclus dans $\mathfrak{p}$. Comme ces idéaux sont premiers on conclut que ces premiers sont minimaux. En effet, en utilisant le raisonnement précédent si $\mathfrak{p} \subset (x)$, alors soit $(y) \subset \mathfrak{p} \subset (x)$ ou $(x)\mathfrak{p} \subset (x)$. Dans le deuxième cas, on a $\mathfrak{p} = (x)$. Notez que le premier cas est impossible car $y \notin (x)$. Ainsi (x) est minimal. Un raisonnement symétrique pour y s'applique.

   On avait d'abord pensé à cette preuve trop alambiquée.

   On avait donné en indication,

   Pour ce dernier point, on fait remarquer le fait suivant. Si A commutatif et $I_1, \dots I_r$ des idéaux et $\mathfrak{p}$ un idéal premier, alors si $\cap_{i=1}^r I_i \subset \mathfrak{p}$, alors il existe j tel que $I_j \subset \mathfrak{p}$.

   Pour prouver cela, notons que si par l'absurde $i_k \in I_k \setminus \mathfrak{p}$ pour tout les k, alors $i_1 \cdots i_r \in \mathfrak{p}$. Mais comme $\mathfrak{p}$ est premier, on obtient une contradiction. En particulier si

$$\mathrm{nil}(A) = \mathfrak{p}_1 \cap \mathfrak{p}_2$$

   comme dans le cas de l'exercice, en utilisant que $\mathrm{nil}(A)$ contient tout les premiers, si $\mathfrak{p}$ est minimal, on a $\mathfrak{p}_1 \cap \mathfrak{p}_2 \subset \mathfrak{p}$ et donc en utilisant le lemme et la minimalité $\mathfrak{p}_i = \mathfrak{p}$ pour $i = 1$ ou $i = 2$. Ainsi on conclut dans le cas de l'exercice que l'ensemble des premiers minimaux (qui est non-vide, voir remarque après la preuve) est contenu dans $\{(x), (y)\}$. Or comme $\mathrm{nil}(A)$ n'est pas premier, il ne peut exister un unique premier minimal, et donc les idéaux premiers minimaux sont (x) et (y).

   Remarque. On note que tout idéal premier contient un premier minimal par le lemme de Zorn. (On vérifie qu'une intersection emboîtée de premiers est encore un idéal premier.)

Exercice 4. (a) We first note that $\mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$ is an $\mathbb{F}_p$-algebra: $\mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$ is a commutative ring and $\psi : \mathbb{F}_p \to \mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$ given by $\psi(a) = a \cdot [0]$, for $a \in \mathbb{F}_p$, is a ring homomorphism with the property that $\psi(\mathbb{F}_p) \subseteq \mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$. In particular, we have that $\mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$ is an $\mathbb{F}_p$ vector space with basis $\{[0], [g], [2g], \dots, [(p-1)g]\}$, where $[g]$ is a fixed generator of $\mathbb{Z}/p\mathbb{Z}$.

We now consider the evaluation homomorphism

$$\mathrm{ev}_{[g]} : \mathbb{F}_p[x] \to \mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$$

$$\mathrm{ev}_{[g]}(x) = 1 \cdot [g].$$

We have that $(x^p - 1) \subseteq \ker(\mathrm{ev}_{[g]})$, as $\mathrm{ev}_{[g]}(x^p - 1) = 1 \cdot [pg] - 1 \cdot [0] = 0$. On the other hand, as $\mathbb{F}_p$ is a field, by Corollary 2.2.5, it follows that $\mathbb{F}_p[x]$ is a principal ring and thus there exists $f \in \mathbb{F}_p[x]$ such that $\ker(\mathrm{ev}_{[g]}) = (f)$. Therefore, as $x^p - 1 \in (f)$, it follows that $x^p - 1 = f \cdot g$ for some $g \in \mathbb{F}_p[x]$ and by Lemma 2.1.1 we deduce that $\deg(f) \leq p$.

We write $f(x) = \sum_{i=0}^{p} a_i x^i$, where $a_i \in \mathbb{F}_p$. Then:

$$\mathrm{ev}_{[g]}(f(x)) = \sum_{i=0}^{m} a_i \cdot [ig] = (a_0 + a_p) \cdot [0] + \sum_{i=1}^{p-1} a_i \cdot [ig] = 0$$

and, as $[0], [g], [2g], \dots, [(p-1)g]$ are linearly independent, we have $a_0 = -a_p$ and $a_i = 0$ for all $1 \leq i \leq p-1$. We deduce that $f(x) = a_p(x^p - 1)$, where $a_p \in \mathbb{F}_p$, and thus $\ker(\mathrm{ev}_{[g]}) = (x^p - 1)$.

In conclusion, we have shown that $\mathbb{F}_p[x]/(x^p - 1) \cong \mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$.

(b) Recall that the characteristic is the natural number n such that $n\mathbb{Z}$ is the kernel of the unique ring homomorphism from $\mathbb{Z}$ to $\mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$. Note the unique ring homomorphism from $\mathbb{Z}$ to $\mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$ sends $x \in \mathbb{Z}$ to $[x]_p \in \mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$. Its kernel is $p\mathbb{Z}$ therefore $\mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$ has characteristic p.

(c) Let $a = \sum_{i=0}^{p-1} a_i' \cdot ([g]-1)^i$ be an idempotent element of $\mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$. Then

$$a^2 = \sum_{i,j} a_i a_j \cdot [(i+j)g] = \sum_{k=0}^{p-1} a_k \cdot [kg] = a$$

and, as $[0], [g], \ldots, [(p-1)g]$ are linearly independent, it follows that $a_k = \sum_{i+j=k} a_i a_j$ for all $0 \leq k \leq p-1$. In particular, we have $a_0 = a_0^2$ and so $a_0 = 0$ or $a_0 = 1$. As $a_1 = a_0 a_1 + a_1 a_0$ we see that in both cases we obtain $a_1 = 0$. Recursively, we deduce that

$$a_{k+1} = \sum_{i+j=k+1} a_i a_j = a_0 a_{k+1} + \Big(\sum_{\substack{i+j=k+1 \\ 1 \leq i,j \leq k}} a_i a_j \Big) + a_0 a_{k+1} = a_0 a_{k+1} + a_{k+1} a_0$$

and therefore $a_{k+1} = 0$. Hence, if $a_0 = 0$, it follows that $a = 0 \cdot [0]$, while, if $a_0 = 1$, it follows that $a = 1 \cdot [0]$. We have shown that the only idempotents of $\mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$ are $0 \cdot [0]$ and $1 \cdot [0]$. By Proposition 2.4.55 and Remark 2.4.56 we conclude that $\mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$ cannot be decomposed as a product of non-zero rings.

On propose également une résolution qui évite tout calcul.

On montre le petit lemme suivant qui peut être utile.

Lemme. Soit A un anneau commutatif tel que $A \setminus A^\times$ est un idéal. Alors c'est l'unique idéal maximal de A.

Preuve. Notons que tout idéal propre est contenu dans $A \setminus A^\times$. En effet si un élément inversible appartient à un idéal, celui-ci est forcément égal à A. Dès lors si $\mathfrak{m}$ est maximal (en particulier propre), on a $\mathfrak{m} \subset A \setminus A^\times$. Mais comme on a supposé que $A \setminus A^\times$ est un idéal, on a par maximalité $\mathfrak{m} = A \setminus A^\times$.

Maintenant, notons qu'un produit d'anneaux $A \times B$ non-nuls contient toujours au-moins deux idéaux maximaux : si $\mathfrak{m}_A$ et $\mathfrak{m}_B$ sont des idéaux maximaux de A et B respectivement, alors $\mathfrak{m}_A \times B$ et $A \times \mathfrak{m}_B$ sont maximaux.

Maintenant, dans l'anneau

$$A = \mathbb{F}_p[t]/(t-1)^p,$$

notons que $t-1$ est nilpotent. Si $f(t) \in \mathbb{F}_p[t]$, on peut écrire

$$f(t) = f(1) + (t-1)g(t)$$

par division euclidienne. Ainsi l'image dans le quotient $\overline{f(t)}$ peut s'écrire $\overline{f(t)} = f(1) - n$ avec $n \in A$ nilpotent. Dès lors, on voit que* $\overline{f(t)}$ est inversible si et seulement si $f(1) \neq 0$ ou autrement dit $\overline{f(t)} \notin (\bar{t}-1) = \ker(ev_1)$. Ainsi on a $A \setminus A^\times = (\bar{t}-1)$ qui est un idéal, et donc l'unique idéal maximal. Dès lors, il suit que A ne peut être un produit de deux anneaux non-nuls.

*si $\lambda \in A^\times$ et $n \in A$ nilpotent, alors $\lambda - n$ est inversible. En effet,

$$\frac{1}{\lambda - n} = \frac{1}{\lambda} \sum_{i=0}^{\infty} (n/\lambda)^i.$$

Exercice 5. 1. We define $\overline{a+b\sqrt{5}} = a - b\sqrt{5}$ and note that for all $z \in \mathbb{Z}[\sqrt{5}]$, the norm $N(z) = z\overline{z}$. The fact that N is a multiplicative function then follows from the fact that $\forall y, z \in \mathbb{Z}[\sqrt{5}]$, it holds that $\overline{yz} = \overline{y}\,\overline{z}$. With this, we get that $N(yz) = yz\overline{yz} = yz\overline{y}\,\overline{z} = y\overline{y}z\overline{z} = N(y)N(z)$.

Furthermore, if $z \in \mathbb{Z}[\sqrt{5}]$ is invertible, then $N(z) = \pm 1$ is necessary. If we denote its inverse by z^{-1}, then $N(z)N(z^{-1}) = N(1) = 1$, and therefore, $N(z) = \pm 1$. On the other hand, if $N(z) = \pm 1$ for some $z \in \mathbb{Z}[\sqrt{5}]$, then $\pm 1 = N(z) = z\overline{z}$ and hence $\pm\overline{z}$ is the inverse of z.

2. We note that $N(9 + 4\sqrt{5}) = 9^2 - 5 \cdot 4^2 = 1$, and so by the first point, $9 + 4\sqrt{5}$ is invertible. Furthermore, by the multiplicative property of the norm, the norm of $(9+4\sqrt{5})^n$ is 1 as well, for $n \in \mathbb{N}$. This means that we have created infinitely many invertible elements, and $(\mathbb{Z}[\sqrt{5}])^\times$ is infinite.

3. We first show that no elements of norm 2 exist. For this, we note that $N(a+\sqrt{5}b) = a^2 - 5b^2$, which is equal to a^2 modulo 5, a square. But all squares in $\mathbb{Z}/5\mathbb{Z}$ are either 0,1 or 4, as one checks by taking the square of all elements in $\mathbb{Z}/5\mathbb{Z}$.

   Now let $z \in \mathbb{Z}[\sqrt{5}]$ be of norm 4, and we assume that $z = v \cdot w$ for $v, w \in \mathbb{Z}[\sqrt{5}]$. Then $4 = N(z) = N(v)N(w)$. But as there are no elements of norm 2, we have that either $N(v) = \pm 1, N(w) = \pm 4$ or $N(v) = \pm 4, N(w) = \pm 1$. In either cases one of the two elements is of norm ± 1, which means that that element is invertible. Hence z is irreducible.

4. We have

   - $4 = 2 \cdot 2$ and $N(2) = 4$, hence by the previous part, 2 is irreducible
   - $4 = (1+\sqrt{5})(-1+\sqrt{5})$ and $N(1+\sqrt{5}) = -4, N(-1+\sqrt{5}) = -4$, hence both $1+\sqrt{5}, -1+\sqrt{5}$ are irreducible.
   - $4 = (3+\sqrt{5})(3-\sqrt{5})$ and $N(3+\sqrt{5}) = 4, N(3-\sqrt{5}) = 4$, hence both $3+\sqrt{5}, 3-\sqrt{5}$ are irreducible.

5. As we see from the previous point, $2 \cdot 2 = 4 = (3+\sqrt{5})(3-\sqrt{5})$, from which it follows that $2 \cdot 2 \in (3+\sqrt{5})$. But as $2 \notin (3+\sqrt{5})$, the ideal $(3+\sqrt{5})$ is not prime.

   We remark (all these notions will be defined later in the course) that irreducible does not imply prime in a ring that is not factorial or principal.

Exercice 6. 1. Soit $x = a + bi\sqrt{d} \in A$ avec $a^2 + b^2 d \leq d + 1$. Donc

$$a^2 + (b^2 - 1)d \leq 1.$$

On voit dès lors que $|b| \leq 1$. On distingue deux cas. Tout d'abord traitons le cas où $b = \pm 1$. Alors on a nécessairement $a = 0$ ou $a = \pm 1$, c'est à dire

$$x = \pm i\sqrt{d} \quad x = \pm(1 - i\sqrt{d}) \quad x = \pm(1 + i\sqrt{d}).$$

Traitons maintenant le cas où $b = 0$. On alors $x = a \in \mathbb{Z}$ avec la condition que $|a| \leq \sqrt{1+d}$.

2. On montre d'abord que $i\sqrt{d}$ est irréductible. On a $N(i\sqrt{d}) = d$. Ainsi si $x \mid i\sqrt{d}$ avec x ni inversible ni associé, il faut que $1 < N(x) < d$. Selon la liste établie au point 1, on a alors $x = a \in \mathbb{Z}$ avec $|a| < \sqrt{d}$. Mais comme on a supposé que $x \mid i\sqrt{d}$, il existe $e, f \in \mathbb{Z}$ tel que

$$a(e + fi\sqrt{d}) = i\sqrt{d}.$$

Donc $e = 0$ et $fa = 1$ ce qui contredit $N(a) > 1$.

On montre maintenant que $1 + i\sqrt{d}$ est irréductible. Comme la conjugaison complexe est un automorphisme d'anneau qui envoie $1 + i\sqrt{d}$ sur $1 - i\sqrt{d}$ cela montrera que $1 - i\sqrt{d}$ est également irréductible. Comme $N(1 + i\sqrt{d}) = 1 + d$, si $x \mid 1 + i\sqrt{d}$ avec x ni irréductible ni associé à $1 + i\sqrt{d}$, alors $1 < N(x) < 1 + d$. Comme il faut aussi que $N(x) \mid 1 + d$, on voit que $N(x) < d$. Ainsi un argument similaire à celui au-dessus conclut.

3. Supposons que $1+d$ n'est pas premier dans $\mathbb{Z}$. Alors on a
$$1+d=(1+i\sqrt{d})(1-i\sqrt{d})=p_1\cdots p_r$$
pour $p_1,\ldots,p_r$ des premiers avec $p_i\leq d$ comme on a supposé $d+1$ pas premier. Comme $1+i\sqrt{d}$ est irréductible, si $1+d$ admet une factorisation *unique* en produit d'irréductibles (en supposant par l'absurde que A est factoriel) cela impliquerait que $1+i\sqrt{d}\mid p_j$ pour un indice j. Mais dès lors il existerait $e,f\in\mathbb{Z}$ avec
$$(1+i\sqrt{d})(e+fi\sqrt{d})=p_j$$
Donc $e+f=0$ et $p_j=e-df=(1+d)e$. Comme $p_j\leq d$, c'est une contradiction. Ainsi on conclut que $1+d$ n'admet pas de factorisation unique en produit d'irréductibles. En particulier, on conclut que dans ce cas A n'est pas factoriel.

4. Supposons maintenant $q:=1+d$ premier dans $\mathbb{Z}$. On a
$$1+d=(1+i\sqrt{d})(1-i\sqrt{d}),$$
qui est une décomposition en irréductibles. On veut montrer que si $x\mid 1+d$ et est ni inversible ni associé à $1+d$, alors x est associé à $1+i\sqrt{d}$ ou $1-i\sqrt{d}$. Comme $N(1+d)=(1+d)^2=q^2$, un tel diviseur x satisfait forcément $N(x)=q=1+d$. Selon la liste au-dessus on a dès lors
$$x=\pm(1-i\sqrt{d})\quad x=\pm(1+i\sqrt{d}).$$
ou $x\in\mathbb{Z}$ avec $x^2=q$, mais cela n'est pas possible comme q est premier.

Exercice 7. (a) Let $\sum_{g\in G}a_g\cdot g\in\mathbb{Z}(A)$ and let $h\in G$. Then $1\cdot h\in A$ is invertible with inverse $(1\cdot h)^{-1}=1\cdot h^{-1}$ and we have
$$(1\cdot h)(\sum_{g\in G}a_g\cdot g)(1\cdot h)^{-1}=\sum_{g\in G}a_g\cdot hgh^{-1}=\sum_{g'\in G}a_{h^{-1}g'h}\cdot g'=\sum_{g'\in G}a_{g'}\cdot g'.$$
It follows that $a_{h^{-1}gh}=a_g$ for all $h\in G$ and thus the map $g\to a_g$ is constant over equivalence classes.

Conversely, assume that $g\to a_g$ is constant over equivalence classes. Let $1\cdot h\in A$. Then:
$$(1\cdot h)(\sum_{g\in G}a_g\cdot g)(1\cdot h)^{-1}=\sum_{g'\in G}a_{h^{-1}g'h}\cdot g'=\sum_{g'\in G}a_{g'}\cdot g'$$
and thus
$$(1\cdot h)(\sum_{g\in G}a_g\cdot g)=(\sum_{g\in G}a_g\cdot g)(1\cdot h),\text{ for all }h\in G.$$
Therefore
$$(\sum_{h\in G}a_h\cdot h)(\sum_{g\in G}a_g\cdot g)=\sum_{h\in G}a_h\cdot h\sum_{g\in G}a_g\cdot g=\sum_{h\in G}a_h(\sum_{g\in G}a_gg)h=(\sum_{g\in G}a_g\cdot g)(\sum_{h\in G}a_h\cdot h)$$
and consequently $\sum_{g\in G}a_g\cdot g\in\mathbb{Z}(A)$.

(b) Fix $A=\mathbb{C}[S_3]$. By (a) we have that $e_1,e_2,e_3\in\mathbb{Z}(A)$. We will now show that they are idempotents. First,
$$\begin{aligned}e_1^2&=\frac{1}{36}(\sum_{g\in S_3}g)(\sum_{h\in S_3}h)\\&=\frac{1}{36}\Big[\sum_{g\in S_3}g+\sum_{g\in S_3}g(12)+\sum_{g\in S_3}g(13)+\sum_{g\in S_3}g(23)+\sum_{g\in S_3}g(123)+\sum_{g\in S_3}g(132)\Big]\\&=\frac{1}{6}\sum_{g\in S_3}g=e_1.\end{aligned}$$

In the above we have used the fact that for all $x \in S_3$, the map $S_3 \to S_3$ sending $a \to ax$ is bijective. Hence $\sum_{g\in S_3} gx = \sum_{g\in S_3} g$ for all $x \in S_3$. Secondly,

$$\begin{aligned}
e_2^2 &= \frac{1}{36}(\sum_{g\in S_3} \operatorname{sgn}(g)g)(\sum_{h\in S_3} \operatorname{sgn}(h)h) \\
&= \frac{1}{36}\Big[\sum_{g\in S_3} \operatorname{sgn}(g)g - \sum_{g\in S_3} \operatorname{sgn}(g)g(12) - \sum_{g\in S_3} \operatorname{sgn}(g)g(13) - \sum_{g\in S_3} \operatorname{sgn}(g)g(23) + \\
&\quad + \sum_{g\in S_3} \operatorname{sgn}(g)g(123) + \sum_{g\in S_3} \operatorname{sgn}(g)g(132)\Big] \\
&= \frac{1}{36}\Big[\sum_{g\in S_3} \operatorname{sgn}(g)g - \sum_{g\in S_3} \operatorname{sgn}(g(12))g - \sum_{g\in S_3} \operatorname{sgn}(g(13))g - \sum_{g\in S_3} \operatorname{sgn}(g(23))g + \\
&\quad + \sum_{g\in S_3} \operatorname{sgn}(g(132))g + \sum_{g\in S_3} \operatorname{sgn}(g(123))g\Big] \\
&= \frac{1}{6}\sum_{g\in S_3} \operatorname{sgn}(g)g = e_2.
\end{aligned}$$

In the above we have used the fact that $\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$ for all $\sigma, \tau \in S_3$.

Lastly, we will show that f_1 and f_2 are idempotents and that $f_1 f_2 = f_2 f_1 = 0$. We have that:

$$\begin{aligned}
f_1^2 &= \frac{1}{9}\Big[\operatorname{Id} + \varepsilon(123) + \varepsilon^2(132) + \varepsilon(123) + \varepsilon^2(132) + \operatorname{Id} + \varepsilon^2(132) + \operatorname{Id} + \varepsilon(123)\Big] \\
&= \frac{1}{3}\Big[\operatorname{Id} + \varepsilon(123) + \varepsilon^2(132)\Big] = f_1.
\end{aligned}$$

Analogously one shows that $f_2^2 = f_2$. Keeping in mind that $\varepsilon^2 + \varepsilon = -1$, we have

$$\begin{aligned}
f_1 f_2 &= \frac{1}{9}\Big[\operatorname{Id} + \varepsilon(123) + \varepsilon^2(132) + \varepsilon^2(123) + (132) + \varepsilon \operatorname{Id} + \varepsilon(132) + \varepsilon^2 \operatorname{Id} + (123)\Big] \\
&= \frac{1}{9}(1 + \varepsilon + \varepsilon^2)\Big[\operatorname{Id} + (123) + (132)\Big] = 0.
\end{aligned}$$

Analogously one shows that $f_2 f_1 = 0$. Therefore $e_3^2 = (f_1 + f_2)^2 = f_1^2 + f_1 f_2 + f_2 f_1 + f_2^2 = f_1 + f_2 = e_3$.

We have shown that e_1, e_2, e_3 are central idempotents. We will now show that they are pairwise orthogonal. We have

$$e_1 e_2 = \frac{1}{36}\Big[\sum_{g\in G} g - \sum_{g\in G} g(12) - \sum_{g\in G} g(13) - \sum_{g\in G} g(23) + \sum_{g\in G} g(123) + \sum_{g\in G} g(132)\Big] = 0.$$

Analogously one shows that $e_2 e_1 = 0$. We note that $e_3 = \frac{1}{3}(2\operatorname{Id} - (123) - (132))$. Then

$$e_1 e_3 = \frac{1}{18}\Big[2\sum_{g\in G} g - \sum_{g\in G} g(123) - \sum_{g\in G} g(132)\Big] = 0$$

and

$$\begin{aligned}
e_2 e_3 &= \frac{1}{18}\Big[2\sum_{g\in G} \operatorname{sgn}(g)g - \sum_{g\in G} \operatorname{sgn}(g)g(123) - \sum_{g\in G} \operatorname{sgn}(g)g(132)\Big] \\
&= \frac{1}{18}\Big[2\sum_{g\in G} \operatorname{sgn}(g)g - \sum_{h\in G} \operatorname{sgn}(h(132))h - \sum_{h\in G} \operatorname{sgn}(h(123))h\Big] \\
&= 0.
\end{aligned}$$

Now $e_1 + e_2 = \frac{1}{3}[\mathrm{Id} + (123) + (132)]$ is a central idempotent in A, as $(e_1 + e_2)^2 = e_1^2 + e_1e_2 + e_2e_1 + e_2^2 = e_1 + e_2$. Furthermore, one checks that $(e_1 + e_2)e_3 = 0$ and $e_1 + e_2 + e_3 = \mathrm{Id}$. Thus, by Proposition 1.4.55, we have that $A \cong A(e_1 + e_2) \times Ae_3$.

Similarly, e_1 and e_2 are central orthogonal idempotents in $A(e_1 + e_2)$ and, as $e_1 + e_2$ is the identity in $A(e_1+e_2)$, we once more apply Proposition 1.4.55 to obtain $A(e_1+e_2) \cong Ae_1 \times Ae_2$. We have shown that:

$$A \cong Ae_1 \times Ae_2 \times Ae_3.$$

(c) Let $x \in Ae_1$. Then $x = ye_1$, where $y = a_0\,\mathrm{Id} + a_1(12) + a_2(13) + a_3(23) + a_4(123) + a_5(132) \in A$. We compute

$$\begin{aligned} x &= a_0 \sum_{g\in G} g + a_1 \sum_{g\in G} g(12) + a_2 \sum_{g\in G} g(13) + a_3 \sum_{g\in G} g(23) + a_4 \sum_{g\in G} g(123) + a_5 \sum_{g\in G} g(132) \\ &= (a_0 + a_1 + a_2 + a_3 + a_4 + a_5) \sum_{g\in G} g \\ &= (\sum_{i=0}^{5} a_i)e_1. \end{aligned}$$

Therefore if $x \in Ae_1$ then $x = c_xe_1$, for some $c_x \in \mathbb{C}$. Analogously, one shows that if $x \in Ae_2$ then $x = c_xe_2$, for some $c_x \in \mathbb{C}$. (In this case, computations will show that $c_x = a_0 - a_1 - a_2 - a_3 + a_4 + a_5$.)

For $i = 1, 2$ consider the map $\varphi : Ae_i \to \mathbb{C}$ given by $\varphi(x) = c_x$. One checks that φ is a ring isomorphism and concludes that $Ae_i \cong \mathbb{C}$, for $i = 1, 2$.

(d) Let $x \in Ae_3$. Then $x = ye_3$, where $y = a_0\,\mathrm{Id} + a_1(12) + a_2(13) + a_3(23) + a_4(123) + a_5(132) \in A$. We compute

$$yf_1 = (a_0 + a_5\varepsilon + a_4\varepsilon^2)f_1 + (a_1 + a_2\varepsilon + a_3\varepsilon^2)(12)f_1$$

and

$$yf_2 = (a_0 + a_4\varepsilon + a_5\varepsilon^2)f_2 + (a_1 + a_3\varepsilon + a_2\varepsilon^2)(12)f_2$$

to determine that

$$\begin{aligned} x &= (a_0 + a_5\varepsilon + a_4\varepsilon^2)f_1 + (a_1 + a_2\varepsilon + a_3\varepsilon^2)(12)f_1 + (a_0 + a_4\varepsilon + a_5\varepsilon^2)f_2 + (a_1 + a_3\varepsilon + a_2\varepsilon^2)(12)f_2 \\ &= x_1f_1 + x_2(12)f_1 + x_3(12)f_2 + x_4f_2, \end{aligned}$$

where $x_1, x_2, x_3, x_4 \in \mathbb{C}$.

Define the map $\varphi : Ae_3 \to M_2(\mathbb{C})$ by $\varphi(x) = \begin{pmatrix} x_1 & x_3 \\ x_2 & x_4 \end{pmatrix}$. Clearly φ is a bijective map, $\varphi(x + y) = \varphi(x) + \varphi(y)$ for all $x, y \in Ae_3$ and $\varphi(e_3) = \mathrm{I}_2$. What remains to show is that $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in Ae_3$.

We first remark that

$$(12)f_1 = \frac{1}{3}[(12) + \varepsilon(23) + \varepsilon^2(13)] = f_2(12)$$

and

$$f_1(12) = \frac{1}{3}[(12) + \varepsilon(13) + \varepsilon^2(23)] = (12)f_2.$$

Now, keeping in mind that $f_1^2 = f_1$, $f_2^2 = f_2$, $f_1f_2 = f_2f_1 = 0$, $(12)f_1 = f_2(12)$ and

$f_1(12) = (12)f_2$, we have

$$\begin{aligned}
xy &= (x_1f_1 + x_2(12)f_1 + x_3(12)f_2 + x_4f_2)(y_1f_1 + y_2(12)f_1 + y_3(12)f_2 + y_4f_2) \\
&= x_1y_1f_1^2 + x_2y_1(12)f_1f_1 + x_3y_1(12)f_2f_1 + x_4y_1f_2f_1 + x_1y_2f_1(12)f_1 + x_2y_2(12)f_1(12)f_1 + \\
&+ x_3y_2(12)f_2(12)f_1 + x_4y_2f_2(12)f_1 + x_1y_3f_1(12)f_2 + x_2y_3(12)f_1(12)f_2 + x_3y_3(12)f_2(12)f_2 + \\
&+ x_4y_3f_2(12)f_2 + x_1y_4f_1f_2 + x_2y_4(12)f_1f_2 + x_3y_4(12)f_2f_2 + x_4y_4f_2^2 \\
&= x_1y_1f_1 + x_2y_1(12)f_1 + x_3y_2f_1 + x_4y_2(12)f_1 + x_1y_3(12)f_2 + x_2y_3f_2 + x_3y_4(12)f_2 + x_4y_4f_2 \\
&= (x_1y_1 + x_3y_2)f_1 + (x_2y_1 + x_4y_2)(12)f_1 + (x_1y_3 + x_3y_4)(12)f_2 + (x_2y_3 + x_4y_4)f_2.
\end{aligned}$$

Thus $\varphi(xy) = \begin{pmatrix} x_1y_1 + x_3y_2 & x_1y_3 + x_3y_4 \\ x_2y_1 + x_4y_2 & x_2y_3 + x_4y_4 \end{pmatrix} = \begin{pmatrix} x_1 & x_3 \\ x_2 & x_4 \end{pmatrix} \cdot \begin{pmatrix} y_1 & y_3 \\ y_2 & y_4 \end{pmatrix} = \varphi(x)\varphi(y)$. We conclude that φ is a ring isomorphism and thus $Ae_3 \cong M_2(\mathbb{C})$.

Exercice 1. 1. We first do this division in $\mathbb{C}$. There, we obtain that

$$\frac{(5+5i)}{(4+2i)} = \frac{(5+5i)(-4+2i)}{(4+2i)(-4+2i)} = \frac{3}{2} + \frac{1}{2}i.$$

By either rounding up or down both the real and imaginary part, we find the closest elements in $\mathbb{Z}[i]$ to be the quotients $1, 2, 1+i, 2+i$. The division by these with rest are

- $(5+5i) = 1 \cdot (4+2i) + (1+3i)$
- $(5+5i) = 2 \cdot (4+2i) + (-3+i)$
- $(5+5i) = (1+i) \cdot (4+2i) + (3-i)$
- $(5+5i) = (2+i) \cdot (4+2i) + (-1-3i)$

Remark that we need to take the closest elements in $\mathbb{Z}[i]$ to $\frac{3}{2} + \frac{1}{2}i \in \mathbb{C}$ as otherwise the norm of the rest would exceed the norm of $4+2i$, which is a contradiction. In all of the above cases, this is satisfied. This also shows that the quotent and rest of the euclidean division are not unique.

2. We have

- $2 = (1+i)(1-i)$ and since $1+i, 1-i \notin (\mathbb{Z}[i])^\times$ it follows that 2 is not irreducible. On note que *en tant qu'idéaux* $(2) = (1+i)^2$.
- Assume that $3 = x \cdot y$, with $x, y \in \mathbb{Z}[i]$. Then by Proposition 3.4.8, it follows that both $N(x)$ and $N(y)$ divide $N(3) = 9$. This is possible if $N(x), N(y) \in \{1, 3, 9\}$. If $N(x) = 1$, then x is a unit. If $N(x) = 9$, then $N(y) = 1$ and y is a unit. If $N(x) = 3$, with $x = a+ib$ for $a, b \in \mathbb{Z}$, then $N(x) = a^2 + b^2$, but for natural numbers a and b this is impossible. So $N(x) \neq 3$, and the only way to write 3 as a product of two elements x, y in $\mathbb{Z}[i]$ is if either of them is a unit, which means that 3 is irreducible.
- $5 = (2+i)(2-i)$ is not irreducible, as both factors are not units.
- $2i = (1+i)^2$ is not irreducible, as $1+i$ is not a unit.
- Since $N(2-3i) = 13$ is irreducible in $\mathbb{Z}$, it follows by Proposition 3.4.8 that $2-3i$ is irreducible in $\mathbb{Z}[i]$.

  Remarque. Comme $\mathbb{Z}[i]$ est euclidien, donc principal, donc *factoriel*, un élément est irréductible si et seulement si l'idéal associé est premier. Ainsi pour $a+bi \in \mathbb{Z}[i]$ le quotient
  $$\mathbb{Z}[t]/(t^2+1, a+bt)$$
  est intègre si et seulement si $a+bi$ est irréductible.

3. We note that $\mathbb{Z}[i]$ is Euclidean by Example 3.2.7, from which it follows by Proposition 3.3.3 that $\mathbb{Z}[i]$ is principal. The Proposition 3.4.13 then states that since 3 is irreducible in $\mathbb{Z}[i]$, the ideal (3) is maximal in $\mathbb{Z}[i]$. It follows that $\mathbb{Z}[i]/(3)$ is a field.

   Comme
   $$\mathbb{Z}[i]/(3) \cong \mathbb{F}_3[t](t^2+1)$$
   c'est un $\mathbb{F}_3$ espace vectoriel de dimension 2, donc de cardinalité 9.

4. Le cas $p = 2$ étant clair, on suppose que $p > 2$ pour la suite. Notons que dans un anneau Euclidien, un élément est irréductible si et seulement si l'idéal associé est maximal (Proposition 3.6.3).

   (a) On montre que $(a) \implies (b)$. Si $p = a^2 + b^2$, alors $p = (a + bi)(a - bi)$, un produit de deux éléments non-invesibles. Ainsi (p) n'est pas premier. Dès lors comme

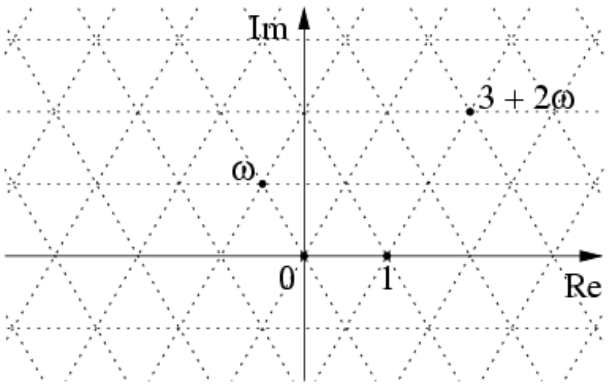
   $$\mathbb{Z}[i]/(p) \cong \mathbb{F}_p[t]/(t^2 + 1),$$

   on a que $(t^2 + 1)$ n'est pas premier dans $\mathbb{F}_p[t]$ et le polynôme $t^2 + 1$ a donc une racine. Cela signifie donc qu'il existe un élément d'ordre 4 dans $\mathbb{F}_p^\times$. Ainsi $4 \mid p - 1$.

   (b) On montre que $(b) \implies (a)$. Si $4 \mid p - 1$, cela implique qu'il existe un élément d'ordre 4 dans $\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$. Ainsi $t^2 + 1$ a une racine dans $\mathbb{F}_p[t]$ et donc p n'est pas irréductible dans $\mathbb{Z}[i]$. Cela signifie qu'il existe un élément $a + bi \in \mathbb{Z}[i]$ avec $a + bi \mid p$ tel que $1 < N(a + bi) = a^2 + b^2 < p^2 = N(p)$ et $N(a + bi) \mid N(p)$. Ainsi on conclut que $a^2 + b^2 = p$.

Exercice 2. 1. On one hand, we have $\mid a + b\omega \mid^2 = (a + b\omega)(a + b\bar{\omega}) = a^2 + ab(\omega + \bar{\omega}) + b^2\omega\bar{\omega}$. On the other hand, we see that both $\omega = e^{\frac{2\pi i}{3}}$ and its complex conjugate $\bar{\omega} = e^{-\frac{2\pi i}{3}}$ are roots of the polynomial $z^3 - 1 = 0$. Since $z^3 - 1 = (z - 1)(z^2 + z + 1)$, both ω and $\bar{\omega}$ are roots of the polynomial $(z^2 + z + 1)$ and therefore $(z^2 + z + 1) = (z - \omega)(z - \bar{\omega}) = z^2 - (\omega + \bar{\omega})z + \omega\bar{\omega}$, from which it follows by comparing coefficients that $\omega + \bar{\omega} = -1$ and $\omega\bar{\omega} = 1$. Therefore, $\mid a + b\omega \mid^2 = a^2 - ab + b^2 = N(a + b\omega)$.

2. La norme au carré étant toujours positive, la formule définissant N montre que cette norme prend des valeurs entières. Pour montrer qu'il s'agit d'une fonction euclidienne on procède comme pour les entiers de Gauss. Soit $a+b\omega$ un entier d'Eisenstein et $(a+b\omega)$ l'idéal principal correspondant. Cet idéal est un réseau dans $\mathbb{Z}[\omega]$. Voici une illustration tirée d Wikipedia de $\mathbb{Z}[\omega]$:



La maille fondamentale de ce réseau est un losange de côté 1 dont les sommets sont par exemples $0, 1, \omega$ et $1 + \omega$, ce dernier étant aussi de norme $1 - 1 + 1 = 1$. Ainsi la petite diagonale est de longueur 1 et la grande est de longueur $\sqrt{3} = \sqrt{N(1 - \omega)}$.

L'idéal $(a + b\omega)$ est donc obtenu à partir du réseau ci-dessus par une dilatation d'un facteur $\sqrt{N(a + b\omega)}$ et rotation d'angle l'argument de $a + b\omega$. Pour nos considérations il suffira de considérer la taille d'un losange de ce réseau homothétique, choisissons le losange de sommets $0, a + b\omega, \omega(a + b\omega)$ et $(1 + \omega)(a + b\omega)$ (que l'on pourra dessiner sur l'illustration précédente pour $3 + 2\omega$ par exemple.) La petite diagonale est de longueur $\mid a + b\omega \mid$ et la grande de longueur $\sqrt{3} \cdot \mid a + b\omega \mid$. Par conséquent le cercle dont le centre est le milieu du losange (point d'intersection des diagonales) et dont le rayon vaut $\sqrt{3}/2 \cdot \mid a + b\omega \mid$ contient toute la maille.

Ceci démontre que tout point de $\mathbb{Z}[\omega]$ se trouve à une distance d'au plus $\sqrt{3}/2 \cdot \mid a+b\omega \mid$ d'un point de ce réseau $(a+b\omega)$.

Autrement dit, pour tout entier d'Eisenstein $c+d\omega$, il existe un entier $q = q_0 + q_1\omega$ tel que $r = c+d\omega - q(a+b\omega)$ est de norme plus petite ou égale à $3/4 \cdot N(a+b\omega) < N(a+b\omega)$. On choisira alors q pour quotient et r comme reste de la division.

3. Let $z \in \mathbb{Z}[\omega]$ be invertible, with inverse element denoted by z^{-1}. Then by the multiplicative properties of the norm, we have that $1 = N(1) = N(z) \cdot N(z^{-1})$, and therefore, $N(z) \in \mathbb{N}$ needs to be equal to 1. This is obtained for the elements $z = \pm 1, \pm\omega, \pm(1+\omega)$. One checks that these are indeed units: ± 1 is clearly a unit, and by the first point, we have that $\omega + \bar{\omega} = -1$. From this, it follows with $\omega^2 = \bar{\omega}$ that $\omega(1+\omega) = \omega + \omega^2 = \omega + \bar{\omega} = -1$. Hence the inverse of $\pm\omega$ is $\mp(1+\omega)$.

Exercice 3. 1. We calculate the complex roots of the polynomial $3+2t+2t^2$. They are $\frac{-2 \pm i\sqrt{20}}{4} = \frac{-1 \pm i\sqrt{5}}{2}$. The roots are elements in $\mathbb{Q}[i\sqrt{5}]$ and we have that $3+2t+2t^2 = 2(t+\frac{1+i\sqrt{5}}{2})(t+\frac{1-i\sqrt{5}}{2})$. This means that $3+2t+2t^2$ is not irreducible in $\mathbb{Q}[i\sqrt{5}]$, as we can express it as the product of $2(t+\frac{1+i\sqrt{5}}{2})$ and $(t+\frac{1-i\sqrt{5}}{2})$, both of which are not units.

On the other hand, if we try to decompose $3+2t+2t^2$ into a product of two non-invertible elements in $\mathbb{Z}[i\sqrt{5}]$, then we have two option: we assume that $3+2t+2t^2 = f(t)g(t)$ with f, g polynomials in $\mathbb{Z}[i\sqrt{5}][t]$. Now the sum of the degree of f plus the degree of g is equal to 2, which means that either f is of degree 2, and g of degree 0 (or vice versa), or the degree of both is 1.

If g is of degree 0, then g is in $\mathbb{Z}[i\sqrt{5}]$, and it holds that g times the leading coefficient of f is equal to 2. But since 2 is irreducible in $\mathbb{Z}[i\sqrt{5}]$, (this can be seen by checking that $N(2) = 4$, and verifying that not element in $\mathbb{Z}[i\sqrt{5}]$ exists with norm 2) it follows that either $g = \pm 1$ or $g = \pm 2$. If $g = \pm 1$, then the decomposition of $3+2t+2t^2$ is the decomposition into a unit multiplied by a non-unit. The other decomposition with $g = \pm 2$ does not exist, since not all coefficients of $3+2t+2t^2$ are divisible by 2.

Therefore, our only possibility for a decomposition into a product of two non-invertible elements is if both f and g are of degree 1. Let $f(t) = (\alpha t + \beta), g(t) = (\gamma t + \delta)$ with $\alpha, \ldots, \delta \in \mathbb{Z}[i\sqrt{5}]$. Since the leading coefficient of $3+2t+2t^2$ is 2, which is irreducible in $\mathbb{Z}$, it follows that $\alpha = \pm 2, \gamma = \pm 1$ (or vice versa). We now note that the ring $\mathbb{C}[t]$ is integral by Proposition 3.2.3. Since furthermore, it is principal by Corollary 3.3.5, it holds that every irreducible element is prime by Proposition 3.4.13. Then by Proposition 3.5.4, if an element $c(t) \in \mathbb{C}[t]$ admits a decomposition into irreducible factors, then that decomposition is unique (up to multiplication by units). This means that if a decomposition of $3+2t+2t^2$ in $\mathbb{Z}[i\sqrt{5}]$ exists, then it must agree with the decomposition in $\mathbb{C}[t]$ we have found above. So if $3+2t+2t^2 = (2t+\beta)(t+\delta)$ is a decomposition in $\mathbb{Z}[i\sqrt{5}][t]$, then it needs to agree with the decomposition in $\mathbb{C}[t]$, which would force the decomposition to be of the form $3+2t+2t^2 = (2t+1+\sqrt{5}i)(t+\frac{1-i\sqrt{5}}{2})$ or $3+2t+2t^2 = (t+\frac{1+\sqrt{5}i}{2})(2t+1-i\sqrt{5})$. But clearly one of the roots is not a root in $\mathbb{Z}[i\sqrt{5}]$, which is a contradiction. We conclude that in $\mathbb{Z}[i\sqrt{5}]$, the polynomial can not be written as a product of non-invertible elements, making it irreducible.

2. **Généralisation.** We calculate

$$(a+ct)(b+ct) = ab + (cb+ac)t + c^2t = cd + (cb+ac)t + c^2t = c(d + (a+b)t + ct^2)$$

which shows that the roots of $d+(a+b)t+ct^2$ are $-a/c$ and $-b/c$ in K. This shows that in K, we can write the polynomial $d+(a+b)t+ct^2$ as the product $c(t+\frac{a}{c})(t+\frac{b}{c})$, with both terms $c(t+\frac{a}{c})$ and $(t+\frac{b}{c})$, not units. Hence the polynomial is not irreducible in K.

On the other hand, over A, the polynomial is irreducible. This we prove as in the exercise above. We assume that the polynomial decoposes into a product of two non-invertible polynomials f and g. There are two options. Firstly, we suppose that g is of degree 0, and f is of degree 2. Then, g multiplied with the leading coefficient of f is equal to c. But since c is irreducible in A, it follows that $g = u, u \in A^\times$ or $g = uc, u \in A^\times$ If $g = u$, then the decomposition is the decomposition into a unit and non-unit. The other decomposition, with $g = uc$ does not exist, since c does not divide at least one coefficient of our polynomial. In fact, c does not divive d because they are irreducible and not associated.

So we now assume that the degree of f and g is 1. Then, $f(t) = \alpha t + \beta, g(t) = \gamma t + \delta$, with $\alpha, \ldots, \delta \in A$. Since the leading coefficient is c, which is irreducible in A, it follows that $\alpha = uc, u \in A^\times$. The argument above only uses the fact that $\mathbb{C}$ is a field to show that if an element over $\mathbb{C}[t]$ admits a decomposition into irreducible factors, then it is unique. Hence we apply the same propositions to the field K and see that the decomposition of $d+(a+b)t+ct^2$ as the product $c(t+\frac{a}{c})(t+\frac{b}{c})$ is unique. From this, it follows that if there exists a decomposition of the polynomial in A, then it must agree with the decomposition in K, which is of the form $d+(a+b)t+ct^2 = (ct+a)(t+\frac{b}{c})$, or $d+(a+b)t+ct^2 = (t+\frac{a}{c})(ct+b)$. But clearly in both cases, one of the roots is not a root in A, which is a contradiction. Hence the polynomial is irreducible in A.

3. By divide $-2+i\sqrt{5}$ by $1+i\sqrt{5}$ with rest, and then calculate the norm of the rest. If $\mathbb{Z}[i\sqrt{5}]$ with the norm $N(a+i\sqrt{5}b) = a^2+5b^2$ was Euclidean, then the norm of the rest would need to be smaller than the norm of $1+i\sqrt{5}$, which is 6. We perform the division over $\mathbb{C}$, and obtain $\frac{-2+i\sqrt{5}}{1+i\sqrt{5}} = \frac{1}{2}+i\frac{1}{2}\sqrt{5}$. The closest elements in $\mathbb{Z}[i\sqrt{5}]$ are $0, i\sqrt{5}, 1, 1+i\sqrt{5}$. It holds that

   - $-2+i\sqrt{5} = (1+i\sqrt{5})\cdot 0 + (-2+i\sqrt{5}) = 0 + (-2+i\sqrt{5})$ with $N(-2+i\sqrt{5}) = 9$
   - $-2+i\sqrt{5} = (1+i\sqrt{5})\cdot i\sqrt{5} + 3 = (-5+i\sqrt{5}) + 3$ with $N(3) = 9$
   - $-2+i\sqrt{5} = (1+i\sqrt{5})\cdot 1 + (-3) = (1+i\sqrt{5}) + (-3)$ with $N(-3) = 9$
   - $-2+i\sqrt{5} = (1+i\sqrt{5})\cdot(1+i\sqrt{5}) + (2-\sqrt{5}) = (-4+i2\sqrt{5}) + (2-\sqrt{5})$ with $N(2-\sqrt{5}) = 9$

   As the norm of every rest is bigger than 6, we can not find $q, r \in \mathbb{Z}[i\sqrt{5}]$ such that $-2+i\sqrt{5} = q(1+i\sqrt{5}) + r$ with $N(r) < N(1+i\sqrt{5})$, which means that $\mathbb{Z}[i\sqrt{5}]$ equipped with N is not Euclidean.

   Note that we can also look at the calculations above in a geometric way. The four elements 0, $1+i\sqrt{5}$, $-5+i\sqrt{5}$ et $-4+2i\sqrt{5}$ are the edges of the rectangle of the lattice spanned by $(1+i\sqrt{5})$ that contains $-2+i\sqrt{5}$.

Exercice 4.
La technique de l'exemple 3.7.4.(3) s'applique texto car (en reprenant les notations de l'exemple)

$$\left|\Re e\left(\frac{b}{a}-q\right)\right| \leq \frac{1}{2} \qquad \text{et} \qquad \left|\Im m\left(\frac{b}{a}-q\right)\right| \leq \frac{1}{\sqrt{2}}$$

Ceci implique que

$$\left|\frac{b}{a}-q\right|^2 \leq \frac{1}{2^2}+\frac{1}{2} = \frac{3}{4} < 1$$

et on conclut comme dans l'exemple.

Exercice 5.
For any field K, we know that by Corollary 3.3.5, $K[t]$ is a principal ideal domain. By Proposition 3.4.13, in a PID, the following are equivalent, for q in the PID:

- q prime
- q irreducible
- (q) prime
- (q) maximal.

1. For $\mathbb{C}[t]$, we know by Example 2.3.7(c) that

$$f(t) \in \mathbb{C}[t] \text{ irreducible} \Leftrightarrow f(t) = ct + d, c \in \mathbb{C} \setminus \{0\}, d \in \mathbb{C}.$$

   Hence the prime=maximal ideals in $\mathbb{C}[t]$ are of the form $(ct + d)$.

   For $\mathbb{R}[t]$, we know by Example 3.4.7 that the ideal $(t - d)$ is prime=maximal for all $d \in \mathbb{R}$. Furtermore, by Example 3.4.7, we know that if $f \in \mathbb{R}[t], \deg(f) \leq 3$, then

$$f(t) \in \mathbb{R}[t] \text{ irreducible} \Leftrightarrow \forall c \in \mathbb{R} : f(c) \neq 0$$

   Let $f(t) = at^2 + bt + c = a\left(t^2 + \frac{b}{a}t + \frac{c}{a}\right)$, with $a \in \mathbb{R}$ invertible. It suffices therefore to study $f(t) = x^2 + bx + c$. The complex roots of f are $\frac{-b \pm \sqrt{b^2-4c}}{2}$. Both roots are not in $\mathbb{R}$ if $b^2 - 4c < 0$. Hence f is irreducible if $b^2 - 4c < 0$. The ideals $(x^2 + bx + c)$ are prime=maximal for $b^2 - 4c < 0$.

   There are no irreducible polynomials of higher degree, since a polynomial in $\mathbb{R}[t]$ of degree 3 or higher has at least one root that is contained in $\mathbb{R}$.

2. We consider the evaluation of $K[s, t]$ at $t = a$, defined as

$$ev_a : K[s, t] \to K[s],\ s \mapsto s, t \mapsto a.$$

   Similar to Example 1.4.10, we show that $\ker(ev_a) = (t - a)$. With the first isomorphism theorem (and ev_a being surjective), it follows that $K[s, t]/(t - a) \cong K[s]$. With Proposition 3.2.3, it follows from K being a field, and hence in particular being integral, that $K[s]$ is integral as well. From Proposition 2.5.2 it follows that $(t - a)$ is a prime ideal. On the other hand, it holds that $K[s]$ is not a field, and therefore, with Proposition 2.5.5 it follows that $(t - a)$ is not a maximal ideal.

3. Consider the evaluation of $\mathbb{C}[s, t]$ at $s = t^2$ defined as

$$ev_{s=t^2} : \mathbb{C}[s, t] \to \mathbb{C}[t],\ s \mapsto t^2, t \mapsto t.$$

   Again, by the usual argument, $\ker(ev_{s=t^2}) = (s - t^2)$. It follows with surjectivity by the first isomorphism theorem that $\mathbb{C}[s, t]/(s - t^2) \cong \mathbb{C}[t]$. By Corollary 3.3.5, using that $\mathbb{C}$ is a field, it follows that $\mathbb{C}[t]$ is a principal ideal domain.

4. We want to apply the Chinese remainder theorem to the ideals $(t - a_i)$ in $K[t]$. We may do so, since from $a_i \neq a_j$ for all i, j it follows that $(t - a_i)$ is prime to $(t - a_j)$. With the remainder theorem, we get that

$$K[t]/((t - a_1) \cap \ldots \cap (t - a_n)) \cong K[t]/(t - a_1) \times \ldots \times K[t]/(t - a_n).$$

   First, we remark that $(t - a_1) \cap \ldots \cap (t - a_n) = ((t - a_1) \cdot \ldots \cdot (t - a_n))$, and we denote $f(t) := (t - a_1) \cdot \ldots \cdot (t - a_n)$. Seondly, the $K[t]/(t - a_i)$ are isomorphic to K, using the evaluation at a_i. It follows that

$$K[t]/(f(t)) \cong K \times \ldots \times K \cong K^n.$$

We now take $(b_1, \ldots, b_n) \in K^n$. Via the isomorphism above, there exists $g(t) \in K[t]$ modulo $f(t)$ that corresponds to $(b_1, \ldots, b_n) \in K^n$. Since the isomorphism above is constructed using the evaluations as a_i, it follows that $g(a_i) = b_i$ for all $i = 1, \ldots, n$. Lastly, since $f(t)$ is of degree n, we may represent a class (modulo f) by a polynomial of degree strictly smaller than n. Hence $g(t)$ is of degree at most $n - 1$.

Exercice 6.
By Example 3.2.7, we have that $\mathbb{Z}[i]$ is euclidean. From Proposition 3.3.3 it follows that $\mathbb{Z}[i]$ is principal. This means that every ideal in $\mathbb{Z}[i]$ is generated by a single element. So let $a \in \mathbb{Z}[i]$ such that $(5) \subsetneq (a) \subsetneq \mathbb{Z}[i]$. From Remark 3.4.5 it follows that $a \mid 5$ and then with Proposition 3.4.8 it follows that $N(a) \mid N(5) = 25$. The only options for $N(a)$ are 1,5, or 25. But since (a) is not equal to both (5) and $\mathbb{Z}[i]$, it follows that $N(a) \neq 25$ and $N(a) \neq 1$. Hence $N(a) = 5$, and we let $a = c + id$ with $c, d \in \mathbb{Z}$. In order for $N(c + id) = 5$ to hold, we have that either $c = \pm 1, d = \pm 2$ or vice versa. The possibilities for a are $a = 1 + 2i, 1 - 2i, -1 + 2i, -1 - 2i$ and $a = 2 + i, 2 - i, -2 + i, -2 - i$. But the elements $-1 - 2i, 1 + 2i$ and $-2 + i$ are all associated to $2 - i$ and the elements $-1 + 2i, 1 - 2i$ and $-2 - i$ are all associated to $2 + i$. We obtain two ideals $(a) = (2 - i)$ and $(a) = (2 + i)$. Since the elements $2 - i$ and $2 + i$ are not associated, these ideals are distinct.

We now let $b \in \mathbb{Z}[i]$ such that $(2) \subsetneq (b) \subsetneq \mathbb{Z}[i]$. As above, $b \mid 2$, from which it follows that $N(b) \mid N(2) = 4$. The options for $N(b)$ are 1,2 and 4, but since (b) is not equal to (2) or $\mathbb{Z}[i]$, it follows that $N(b) = 2$. This is satisfied for b of the form $1 + i, 1 - i, -1 + i, -1 - i$. As all of these elements are associated, the only ideal we obtain is $(b) = (1 + i)$.

Exercice 7. 1. It holds that

- $(S^{-1}A, +)$ is a subgroup of $(\mathrm{Frac}(A), +)$, since $\frac{0}{1} \in S^{-1}A$, as $0 \in A, 1 \in S$. Furthermore, $\forall \frac{a}{b}, \frac{c}{d} \in S^{-1}A$, we have that $\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd} \in S^{-1}A$, since $ad + cb \in A$, and $bc \in S$ for $b \in S, c \in S$. Lastly, the additive inverse of $\frac{a}{b} \in S^{-1}A$ is $\frac{-a}{b}$, which is contained in $S^{-1}A$ as well.
- Since $1_A \in S$, it holds that $\frac{1}{1} \in S^{-1}A$.
- $\forall \frac{a}{b}, \frac{c}{d} \in S^{-1}A$ we have that $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \in S^{-1}A$ since $ac \in A$, and $bd \in S$ for $b \in S, d \in S$.

This means that $S^{-1}A$ is a ring.

2. We show that $S := A \setminus \mathfrak{p} = \{a \in A \mid a \notin \mathfrak{p}\}$ is closed under multiplication.

- It holds that $1 \in S$, since if 1 were contained in $\mathfrak{p}$, then $\mathfrak{p}$ would be the whole ring A.
- For $a, b \in S$, it holds that $a \cdot b \in S$, which means that $a \cdot b \notin \mathfrak{p}$. This holds because if $a \cdot b$ were contained in $\mathfrak{p}$, then since $\mathfrak{p}$ is prime, it would follow that either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, which is not possible due to the assumption that both a and b are contained in S.

For the ring $A = \mathbb{Z}$, you have seen the localization at a prime ideal in Example 2.1.7.

3. We note that the elements in the ring $\mathbb{Z}_{(2)}$ are of the form

$$\mathbb{Z}_{(2)} = \{\frac{a}{b} \in \mathrm{Frac}(\mathbb{Z}) \mid b \in \mathbb{Z} \setminus (2)\} = \{\frac{a}{b} \in \mathbb{Q} \mid 2 \nmid b\}.$$

We remark that the elements $\frac{a}{b} \in \mathbb{Z}_{(2)}$ with $2 \nmid a$ are the units of $\mathbb{Z}_{(2)}$, since the inverse of $\frac{a}{b}$ is $\frac{b}{a}$, which is contained in $\mathbb{Z}_{(2)}$ due to the fact that $2 \nmid a$.

We define $m \subseteq \mathbb{Z}_{(2)}$ to be $m := \{\frac{a}{b} \in \mathbb{Z}_{(2)} \mid a \in (2)\}$. This is an ideal, since for $\frac{a}{b} \in m$, $\frac{c}{d} \in \mathbb{Z}_{(2)}$, it holds that $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \in m$, since $a \in (2), c \in \mathbb{Z}$, and hence $ac \in (2)$. Furthermore, it is clearly an additive group. We show that this ideal is maximal. For this, we assume that there

exists an ideal I such that $m \subset I$ and $m \neq I$. So there must exist an element $\frac{a}{b} \in I$ which is not contained in m. This means that $a \notin (2)$, and hence $2 \nmid a$. But as we remarked above, then $\frac{a}{b}$ is a unit in $\mathbb{Z}_{(2)}$, and so I is equal to $\mathbb{Z}_{(2)}$.

Other proper ideals in $\mathbb{Z}_{(2)}$ are of the following form $I = \{\frac{a}{b} \in \mathbb{Z}_{(2)} \mid a \in (n)\}$ where (n) is an ideal such that $(n) \subseteq (2) \Leftrightarrow 2 \mid n$. These are clearly ideals. They are all ideals, since if there was an ideal that contained an element $\frac{a}{b}$ such that a is not a multiple of 2, then $\frac{a}{b}$ is a unit and hence the ideal is the whole ring.

Lastly, we remark that the only prime ideal is the maximal ideal. The other ideals of the form $I = \{\frac{a}{b} \in \mathbb{Z}_{(2)} \mid a \in (n)\}$ with $(n) \subseteq (2)$ but $n \neq 2$ are not prime, since we have that $\frac{n}{1} \in I$, and we may write $n = 2m$ for some $m \in \mathbb{Z}, m < n$. But then $\frac{n}{1} = \frac{2}{1} \cdot \frac{m}{1}$ and both $\frac{2}{1} \notin I$ and $\frac{m}{1} \notin I$.

4. It holds that $\mathbb{Z}_2 = \{\frac{a}{b} \in \mathbb{Q} \mid b \in \{1, 2, 2^2, 2^3, \ldots\}\} = \{\frac{a}{2^i} \in \mathbb{Q} \mid i \in \mathbb{N}\}$. Hence for $i = 0$, we obtain elements $\frac{a}{2^0} = a \in \mathbb{Z}$, and for $i > 0$, we obtain elements of the form $\frac{a}{2^i}$ with $2 \nmid a$. The units are elements that have an inverse in $\mathbb{Z}_2$. These are the elements of the form $2^i \in \mathbb{Z}$, since their inverse is of the form $\frac{1}{2^i}$, which is contained in $\mathbb{Z}_2$, and elements of the form $\frac{1}{2^i}$, since their inverse is of the form $\frac{2^i}{1}$, which is contained in $\mathbb{Z}_2$. The other elements are not units, since seen as elements in $\mathbb{Q}$ they have an inverse, which is unique, but their inverse in not contained in $\mathbb{Z}_2$ (i.e. the inverse of $\frac{a}{2^i}$ with $2 \nmid a$ in $\mathbb{Q}$ is $\frac{2^i}{a}$, but since $2 \nmid a$, this is not an element of $\mathbb{Z}_2$.)

   The irreducible elements are the elements of the form $\frac{p}{2^i}$ and $2^i \cdot p$ with $p \in \mathbb{Z}$ prime. To prove this, we let $\frac{a}{2^i} \in \mathbb{Z}_2$. Then $a \in \mathbb{Z}$ has a prime decomposition of the following form, $a = p_1^{k_1} \cdot \ldots \cdot p_r^{k^r}$ for some prime numbers $p_i \in \mathbb{Z}$, and $r \geq 1, k_i \geq 1$. There are two cases.

   - If all the prime numbers p_i are odd, then we can write

     $$\frac{a}{2^i} = \frac{1}{2^i} \cdot p_1^{k_1} \cdot \ldots \cdot p_r^{k^r},$$

     with $\frac{1}{2^i}$ a unit in $\mathbb{Z}_2$. It follows that $\frac{a}{2^i}$ is irreducible if and only if $r = 1$ and $k_1 = 1$. This means that $\frac{a}{2^i}$ is of the form $\frac{p}{2^i}$ with p prime im $\mathbb{Z}$.
   - If the prime number 2 appears in the decomposition of a, then we have the following: We may assume that $p_1 = 2$, and that $i = 0$ (since we assume that the fractions in $\mathbb{Z}_2$ are shortened). We can write

     $$\frac{a}{2^0} = a = 2^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k^r},$$

     with 2^{k_1} a unit in $\mathbb{Z}_2$. It follows that a is irreducible if and only if $r = 2$ and $k_2 = 1$. This means that $\frac{a}{2^i}$ is of the form $2^j \cdot p$ with p prime in $\mathbb{Z}$.

EPFL - Printemps 2023	Prof. Zs. Patakfalvi
Anneaux et Corps	**Exercices**
Solutions 7	

Exercice 1. 1. Soit A un anneau euclidien, avec une fonction euclidienne $\nu\colon A\setminus\{0\}\to\mathbb{N}$. Etant donnés $a_0\in A$ et $0\neq a_1\in A$, on construit une suite d'éléments $a_i\in A$ de la manière récursive suivante :

(a) a_0, a_1 sont donnés ;

(b) pour $i\geq 1$, si $a_i\neq 0$, il existe une expression $a_{i-1}=a_iq_i+a_{i+1}$ où $\nu(a_{i+1})<\nu(a_i)$.

La condition $\nu(a_{i+1})<\nu(a_i)$ implique que l'algorithme s'arrête, c'est-à-dire qu'il existe un n tel que $a_{n+1}=0$. On prétend que

$$a_n \text{ est un pgdc de } a_0 \text{ et } a_1.$$

Prouvons cette assertion. On prétend d'abord que a_n divise tous les a_i ($i\leq n$). On procède par induction descendante sur i. Puisque $a_{n+1}=0$, on a $a_n|a_{n-1}$. Si a_n divise $a_i,\dots,a_n$, alors comme

$$a_{i-1}=a_iq_i+a_{i+1}$$

on voit que a_n divise a_{i-1}.

On prétend ensuite que si b divise a_0 et a_1, alors b divise a_n. En effet, comme $a_2=a_0-a_1q_1$, on voit que b divise a_2 ; et par induction croissante sur i, on voit que b divise tous les a_i, en particulier a_n.

La combinaison de ces deux observations montre que a_n est un pgdc de a_0 et de a_1.

Faisons la remarque suivante, qui sera utile dans la suite : si une étape de l'algorithme fournit une unité, c'est-à-dire si $a_i\in A^\times$ pour un certain i, alors a_0 et a_1 sont premiers entre eux. En effet, puisque a_i est une unité, l'étape suivante sera

$$a_{i-1}=(a_{i-1}a_i^{-1})a_i+0$$

donc $a_{i+1}=0$ et ainsi a_i est un pgdc de a_0 et a_1. Par définition cela implique que a_0 et a_1 sont premiers entre eux.

2. La division de $27-23i$ par $8+i$ donne $\frac{193}{65}-\frac{211}{65}i$. On arrondit au nombre entier le plus proche pour trouver $q=3-3i$. Attention: on ne peut pas arrondir indifféremment vers le haut ou vers le bas, sans quoi le reste de la division aura une norme trop grande! On calcule alors

$$27-23i=(3-3i)(8+i)+(-2i)$$

Le reste vaut donc $-2i$. On poursuit la recherche du pgdc avec l'algorithme d'Euclide dans cet anneau euclidien. Comme

$$8+i=-4i^2+i=4i\cdot(-2i)+i$$

Le reste de cette division est i, un élément inversible de $\mathbb{Z}[i]$. On conclut que ces deux nombres sont premiers entre eux.

3. On calcule $11+3i=(1-i)(1+8i)+2-4i$. La division suivante $\frac{1+8i}{2-4i}=\frac{(1+8i)(2+4i)}{20}=\frac{-3+2i}{2}$ et nous retrouvons la possibilité de choisir deux quotients distincts: $q=-1+i$ ou

$q' = -2 + i$. Les restes correspondants sont $r = -1 + 2i$ et $r' = 1 - 2i$ respectivement. Dans les deux cas on constate que $2 - 4i$ est un multiple de ce reste.

Ainsi le dernier reste non nul dans l'algorithme d'Euclide est $-1 + 2i$ ou $1 - 2i$. Chacun est un pgdc (de norme 5). Plus généralement, le pgdc est uniquement défini dans un anneau factoriel modulo la relation d'être associé.

4. Pour décomposer les idéaux premiers $(11 + 3i)$ et $(1 + 8i)$ on commence par décomposer leur normes dans les entiers.

$$(11 + 3i)(11 - 3i) = 130 = 13 \cdot 5 \cdot 2 \quad (1 + 8i)(1 - 8i) = 65 = 13 \cdot 5.$$

Ensuite on décompose dans $\mathbb{Z}[i]$

$$13 = (3 + 2i)(3 - 2i) \quad 5 = (1 + 2i)(1 - 2i) \quad 2 = (1 + i)(1 - i).$$

Notons que comme ces éléments ont norme première, ils sont forcément irréductibles, donc que leur idéal associé est un idéal premier (par factorialité de l'anneau.) Comme on sait déjà que $1 - 2i$ divise $1 + 8i$ on voit avec une division par $1 - 2i$ que c'est $3 - 2i$ qui divise également $1 + 8i$. Ainsi, en termes de multiplication d'idéaux (noter qu'en termes d'idéaux la décomposition est unique)

$$(1 + 8i) = (3 - 2i)(1 - 2i).$$

Comme on sait de plus que le pgcd de $11 + 3i$ et $1 + 8i$ est $3 - 2i$ on conclut que

$$(11 + 3i) = (3 + 2i)(1 - 2i)(1 + i).$$

Exercice 2. 1. Pour $x \in [0, 1]$, considérons l'application d'évaluation

$$\mathrm{ev}_x \colon \mathcal{C} \to \mathbb{R}, \quad f \mapsto f(x).$$

Alors ev_x est surjective et $\ker \mathrm{ev}_x = I_x$. Donc $\mathcal{C}/I_x \cong \mathbb{R}$ par le premier théorème d'isomorphisme, et ainsi I_x est maximal puisque $\mathbb{R}$ est un corps.

2. Il est facile de trouver $f, g \in \mathcal{C}$ tels que $f(x) = 0 = g(y)$ et $f(y) \neq 0 \neq g(x)$ (on peut construire de telles fonctions linéaires par parties). Donc ni f ni g n'appartient à $I_x \cap I_y = \{h \in \mathcal{C} \mid h(x) = 0 = h(y)\}$, tandis que $fg \in I_x \cap I_y$.

3. Pour chaque $x \in [0, 1]$, par hypothèse il existe $0 \neq f_x \in I$ tel que $f_x(x) \neq 0$. Puisque f_x est continue, l'ensemble $\mathcal{U}_x := \{y \in [0, 1] \mid f_x(y) \neq 0\}$ est ouvert (dans la topologie euclidienne de $[0, 1]$) et contient x. Ainsi

$$[0, 1] = \bigcup_{x \in [0,1]} \mathcal{U}_x.$$

Puisque la topologie euclidienne fait de $[0, 1]$ un espace compact, la propriété de Heine–Borel implique qu'il existe $x_1, \ldots, x_n \in [0, 1]$ tels que

$$[0, 1] = \bigcup_{i=1}^{n} \mathcal{U}_{x_i}.$$

Considérons maintenant la fonction continue

$$F := \sum_{i=1}^{n} f_{x_i}^2.$$

Alors $F \in I$ et par construction F est strictement positive sur $[0, 1]$. Ainsi $1/F \in \mathcal{C}$, et $1 = F \cdot 1/F \in I$. Donc $I = \mathcal{C}$.

4. Soit $I \subset \mathcal{C}$ un idéal maximal. En vertu du point précédent, puisque $I \neq \mathcal{C}$ il existe un I_x tel que $I \subseteq I_x$. Puisque I est maximal, on en déduit que $I = I_x$.

Il est également possible de définir une topologie sur l'ensemble $\{I_x \mid x \in [0,1]\}$ (la topologie la moins fine pour laquelle les sous-ensembles $\{I_x \mid f \in I_x\}$ sont ouverts pour des $f \in \mathcal{C}$ quelconques), pour laquelle la bijection

$$[0;1] \to \{\text{idéaux maximaux de } \mathcal{C}\}, \quad x \mapsto I_x$$

devient un homéomorphisme. En d'autres termes, il est possible de reconstruire l'espace topologique $[0,1]$ à partir de son anneau de fonctions réelles continues. C'est une forme de *dualité* entre $[0,1]$ et $\mathcal{C}$. Le même résultat est vrai plus généralement pour les espaces topologiques Hausdorff et compacts (voir Gelfand-Kolomogorov duality sur le n-lab).

Exercice 3. 1. On vérifie que

$$f(x) = (x-2)(x^2+1) \quad \text{et} \quad g(x) = (x-2)(x^3+7),$$

et on prétend que x^2+1 et x^3+7 sont premiers entre eux. En fait, ceux deux polynômes sont primitifs et ne se décomposent pas dans $\mathbb{Q}[x]$ (car -1 n'as pas de racine carrée dans $\mathbb{Q}$, et -7 n'a pas de racine cubique dans $\mathbb{Q}$), donc en vertu de la Proposition 3.8.13 ils sont irréductibles dans $\mathbb{Z}[x]$. Ainsi $x-2$ est un pgdc de f et de g.

2. Les décompositions $f = (x-2)(x^2+1)$ et $g = (x-2)(x^3+7)$ sont encore valables après la réduction modulo p. Après cette réduction, le pgdc n'est plus égal à $x - [2]_p$ si et seulement si $x^2 + [1]_p$ et $x^3 + [7]_p$ ne sont plus premiers entre eux dans $\mathbb{F}_p[x]$.

   Notons qu'on peut écrire (en suivant la méthode de l'algorithme d'Euclide, même si $\mathbb{Z}[x]$ n'est pas euclidien) :

$$x^3 + 7 = x(x^2+1) + (-x+7), \quad x^2 + 1 = (-x-7)(-x+7) + 50$$

   et ces égalités sont encore valables modulo p. En fait, comme $\mathbb{F}_p[x]$ est un anneau euclidien dont la fonction euclidienne est donnée par le degré, la réduction modulo p de ces deux égalités donne les deux premiers pas de l'algorithme d'Euclide pour $x^3+[7]_p$ et $x^2+[1]_p$ (voir l'Exercice 1.1). Notons que le second reste est $[50]_p$. Si $[50]_p = 0$, alors l'algorithme est complet et

$$\text{pgdc}(x^2 + [1]_p, x^3 + [7]_p) = -x + [7]_p \quad \text{et ainsi} \quad \text{pgdc}(\bar{f}, \bar{g}) = (x - [2]_p)(-x + [7]_p).$$

   Si $[50]_p \neq 0$, alors il s'agit d'une unité dans $\mathbb{F}_p[x]$, et donc la prochaine étape de l'algorithme donne un reste nul. Ainsi le pgdc de $x^2 + [1]_p$ et de $x^3 + [7]_p$ est une unité, autrement dit ces deux polynômes sont encore premiers entre eux.

   Puisque $50 = 2 \cdot 5^2$, on a $[50]_p = 0$ si et seulement si $p \in \{2,5\}$. Ainsi :

   (a) Si $p \notin \{2,5\}$, alors $\text{pgdc}(\bar{f}, \bar{g}) = x - [2]_p$.
   (b) Si $p = 2$, alors $\text{pgdc}(\bar{f}, \bar{g}) = x(x + [1]_2)$.
   (c) Si $p = 5$, alors $\text{pgdc}(\bar{f}, \bar{g}) = (x - [2]_5)(-x + [2]_5)$.

Exercice 4. 1. Montrons d'abord que $\mathbb{Q}[i\sqrt{d}]$ est un corps. Puisque $(i\sqrt{d})^2 \in \mathbb{Q}$, on voit que

$$\mathbb{Q}[i\sqrt{d}] = \{a + bi\sqrt{d} \mid a, b \in \mathbb{Q}\}.$$

   Les inverses de ces éléments existent dans $\mathbb{C}$, où ils sont donnés par

$$(a + bi\sqrt{d})^{-1} = \frac{a - bi\sqrt{d}}{|a + bi\sqrt{d}|^2}, \quad \text{où } |a + bi\sqrt{d}|^2 = a^2 + b^2 d \in \mathbb{Q}.$$

Le côté droit appartient aussi à $\mathbb{Q}[i\sqrt{d}]$, on en déduit donc qu'il s'agit d'un corps.

On a l' inclusion évidente $\mathbb{Z}[i\sqrt{d}] \subset \mathbb{Q}[i\sqrt{d}]$. Pour chaque $a + bi\sqrt{d} \in \mathbb{Q}[i\sqrt{d}]$, on peut écrire

$$a + bi\sqrt{d} = \frac{a'}{n} + \frac{b'}{n} i\sqrt{d}$$

où n est le plus petit dénominateur commun de a et b, et $a', b' \in \mathbb{Z}$. Ainsi $\mathbb{Q}[i\sqrt{d}]$ est un corps de fractions pour $\mathbb{Z}[i\sqrt{d}]$.

2. Montrons que $x^3 - 2i$ est irréductible dans $\mathbb{Z}[i][x]$. Puisque le coefficient dominant est une unité, ce polynôme est primitif. En vertu du lemme de Gauss (Proposition 3.8.13) et du premier point, il est irréductible dans $\mathbb{Z}[i][x]$ si et seulement si il est irréductible dans $\mathbb{Q}[i][x]$. Si $x^3 - 2i$ se décompose dans $\mathbb{Q}[i][x]$, l'un des facteurs doit être un polynôme linéaire. Donc $x^3 - 2i$ est irréductible dans $\mathbb{Q}[i][x]$ si et seulement si il n'a pas de racines dans $\mathbb{Q}[i]$.

   Supposons que $2i$ possède une racine cubique dans $\mathbb{Q}[i]$. On peut écrire cette racine $\frac{a+bi}{n}$, avec $n \in \mathbb{N}$ et $a, b \in \mathbb{Z}$. On a alors

$$n^3 2i = (a + bi)^3$$

   et en prenant les modules au carré, on obtient

$$4n^6 = (a^2 + b^2)^3.$$

   C'est une égalité entre deux entiers, on peut donc compter les puissances de 2 dans chaque membre et s'apercevoir qu'elles n'ont pas le même reste modulo 3. C'est une contradiction. Ainsi $2i$ n'a pas de racine cubique dans $\mathbb{Q}[i]$.

   On a donc montré que $x^3 - 2i$ est irréductible dans $\mathbb{Z}[i\sqrt{d}][x]$.

   Remarque : Le critère d'Eisenstein ne peut être invoqué pour résoudre l'exercice. En effet la décomposition en facteurs irréductibles de $2i$ est

$$2i = (1 + i)^2,$$

   où $1 + i$ est irréductible en vertu de la Proposition 3.4.8

Exercice 5. 1. Notons $A = k[t^2, t^3]$. Puisque $A \subset k[t]$, on a

$$A^\times \subseteq (k[t])^\times = k^\times$$

   et l'inclusion inverse étant claire, on obtient $A^\times = k^\times$. On prétend ensuite que t^2 et t^3 sont irréductibles dans A :

   (a) Si on peut écrire $t^2 = fg$ dans A, alors cette décomposition est aussi valable dans $k[t]$. Donc soit f ou g est une unité dans $k[t]$ et donc dans A, soit $\deg f = 1 = \deg g$. Or A ne contient aucun polynôme linéaire en t (observez que $A = k + t^2 \cdot k[t] + t^3 \cdot k[t]$, et que les éléments de $t^2 \cdot k[t]$ et de $t^3 \cdot k[t]$ n'ont pas de termes d'ordre 1). On voit donc que t^2 est irréductible dans A.

   (b) Pour t^3, on procède de la même manière : les seules décompositions non-triviales dans $k[t]$ sont données par $t^3 = t \cdot t \cdot t = t \cdot t^2$, mais $t \notin A$.

   On peut ainsi affirmer que

$$(t^2)^3 = (t^3)^2 \quad \text{dans } A,$$

   et que t^2 et t^3 sont des éléments irréductibles non associés de A, puisqu'il n'existe pas de constante $\lambda \in k^\times$ telle que $\lambda t^2 = t^3$. Cela montre que A n'est pas factoriel.

2. On montre de la même manière que $k[t^2, t^5]$ et $k[t^3, t^7]$ ne sont pas factoriels.

3. On prétend que $k[x,y]/(x^2-y^3)$ est isomorphe à $k[t^2,t^3]$. En effet, considérons l'homomorphisme d'évaluation k-linéaire

$$\varphi\colon k[x,y] \to k[t^2,t^3], \quad x \mapsto t^3,\ y \mapsto t^2.$$

Alors φ est surjective et $k[x,y]/\ker\varphi \cong k[t^2,t^3]$. On prétend que $\ker\varphi = (x^2-y^3)$. L'inclusion $\supseteq$ est claire. Pour montrer l'inclusion inverse, prenons $f \in \ker\varphi$ et faisons l'observation suivante : il existe un polynôme $g \in k[x,y]$ tel que $\deg_x[f-(x^2-y^3)\cdot g] < 2$. En effet, puisque $f-(x^2-y^3)\cdot g \in \ker\varphi$, cela se montre aisément par induction sur $\deg_x$ pour les éléments de $\ker\varphi$. Si nous montrons que $f-(x^2-y^3)\cdot g \in (x^2-y^3)$, nous aurons établi l'inclusion désirée. Nous pouvons donc supposer que $\deg_x f < 2$, et nous allons en fait montrer que $f=0$.

Si $\deg_x f = 0$, alors $f = \sum_i a_i y^i$ et $\varphi(f) = \sum_i a_i t^{2i}$. Il est alors clair que $\varphi(f)=0$ si et seulement si $f=0$.

Si $\deg_x f = 1$, alors on peut écrire

$$f = \sum_i a_i y^i + \sum_j b_j x y^j$$

et ainsi

$$\varphi(f) = \sum_i a_i t^{2i} + \sum_j b_j t^{3+2j}.$$

Les puissances de t dans la première somme sont paires, celles dans la seconde sont impaires : il n'y a donc pas de simplifications possibles entre ces deux sommes, et on en déduit que $\varphi(f)=0$ si et seulement si $f=0$.

On a donc montré que $k[x,y]/(x^2-y^3) \cong k[t^2,t^3]$, ce qui conclut.

Pour démontrer l'inclusion $\ker(\varphi) \subseteq (x^2+y^3)$ on mentionne le lemme suivant qui peut être utile.

Lemme. *Soit A un anneau factoriel, B un anneau intègre et $A \to B$ un morphisme injectif d'anneau. Soit $b \in B$ tel que $\ker(ev_b)$ est non-nul. Alors $\ker(ev_b)$ est principal, généré par un élément irréductible. Plus encore, si $p(t)$ est irréductible et $p(t) \in \ker(ev_b)$, alors $\ker(ev_b) = (p(t))$.*

Preuve. On montre qu'il ne peut exister au plus qu'un unique élément irréductible (modulo la relation d'être associé) dans $\ker(ev_b)$. Si deux éléments irréductibles non-associés $p(t)$ et $q(t)$ sont dans $\ker(ev_b)$ alors on aurait un élément non-nul $a \in A$ et $m(t), g(t) \in A[t]$ tel que

$$p(t)m(t) + q(t)g(t) = a$$

en utilisant que $p(t)$ et $q(t)$ seraient premiers entre eux dans l'anneau $\mathrm{Frac}(A)[t]$. En utilisant que $A \to B$ est injectif et en évaluant en b on obtient $a=0$, une contradiction.

Si on décompose un élément non-nul du noyau en produit d'irréductibles, comme B est intègre, on voit qu'au moins un des facteurs irréductibles est dans $\ker(ev_b)$. Ainsi on a montré l'existence d'un élément irréductible dans le noyau. Comme c'est en fait le seul (modulo la relation d'être associé) on voit qu'en fait $\ker(ev_b) = (p(t))$. □

Ainsi en appliquant le lemme pour $A = k[y]$ et $B = k[t^2,t^3]$ et $y \mapsto t^2$, on voit qu'il suffit de démontrer que x^2+y^3 est irréductible. Cela peut se montrer exactement comme en 7.2.

Exercice 6. 1. Rappelons que

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \cdot \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} ax & ay+bz \\ 0 & cz \end{pmatrix}$$

de quoi il s'ensuit immédiatement que la fonction

$$A \to \mathbb{Z} \times \mathbb{Q}, \quad \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto (a, c)$$

est un homomorphisme surjectif dont le noyau est I.

Montrons maintenant que l'anneau commutatif $\mathbb{Z}\times\mathbb{Q}$ est Noethérien. Soit $I \subset \mathbb{Z}\times\mathbb{Q}$ un idéal. Il est facile de vérifier que l'intersection $I' := I\cap(\{0\}\times\mathbb{Q})$ est un idéal de $\mathbb{Q}$ via l'identification évidente $\mathbb{Q} = \{0\} \times \mathbb{Q}$. Puisque $\mathbb{Q}$ est un corps, on a $I' = \{(0,0)\}$ ou $I' = \{0\} \times \mathbb{Q}$.

(a) Supposons que $I' = \{(0,0)\}$. Alors tous les éléments de I sont de la forme $(x, 0)$. En effet, si $(x, y) \in I$, alors $(0, 1) \cdot (x, y) \in I$ et donc $(0, y) \in I'$, d'où $y = 0$.
Dans ce cas, I s'identifie à un idéal de $\mathbb{Z}$ via l'identification évidente $\mathbb{Z} = \mathbb{Z} \times \{0\}$. L'anneau $\mathbb{Z}$ est principal puisqu'il est Euclidien (Proposition 3.3.3), donc on en déduit que I est généré par un élément de la forme $(n, 0)$.

(b) Supposons que $I' = \{0\} \times \mathbb{Q}$. Alors on prétend que $I = I'' \times \mathbb{Q}$ pour un idéal I'' de $\mathbb{Z}$. En effet, soit $(x, y) \in I$. Puisque $(0, z) \in I'$ pour tout $z \in \mathbb{Q}$, on voit que $(x, y) + (0, z) = (x, y + z) \in I$ pour tout $z \in \mathbb{Q}$. Puisque la translation par y dans $\mathbb{Q}$ est bijective, on en déduit que $(x, z) \in I$ pour tout $z \in \mathbb{Q}$. Cela prouve qu'on peut écrire $I = I'' \times \mathbb{Q}$ pour un certain sous-ensemble $I'' \subset \mathbb{Z}$. Puisque I est un idéal, on vérifie aisément que I'' doit être un idéal de $\mathbb{Z}$. Si $I'' = (n)$, alors I est généré par $(n, 1)$.

On a montré que tous les idéaux de $\mathbb{Z} \times \mathbb{Q}$ étaient finiment générés (en fait, ils sont tous principaux), ce qui montre que cet anneau produit est Noethérien (et même principal).

2. Soit J un idéal à droite qui contient un élément de la forme

$$\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}, \quad 0 \neq b \in \mathbb{Q}.$$

Le calcul au début du point précédent montre alors que J contient tous les éléments de la forme

$$\begin{pmatrix} 0 & bz \\ 0 & 0 \end{pmatrix}, \quad z \in \mathbb{Q}$$

et il s'ensuit que $J \supseteq I$. Cela montre que I est minimal comme idéal à droite.

Notons que I n'est pas minimal comme idéal à gauche, puisqu'il contient strictement le sous-idéal à gauche

$$\left\{ \begin{pmatrix} 0 & n \\ 0 & 0 \end{pmatrix} \mid n \in \mathbb{Z} \right\}.$$

3. Montrons finalement que A est Noethérien à droite. Soit

$$J_1 \subseteq J_2 \subseteq \ldots$$

une suite croissante d'idéaux à droite. Alors chaque $J_k \cap I$ est un sous-idéal à droite de I. Par le point précédent, pour chaque k on a soit $J_k \cap I = I$, soit $J_k \cap I = 0$. Puisque la suite est croissante, ces intersections sont toujours les mêmes pour k assez grand. Quitte à oublier les premiers idéaux, on peut donc supposer que $J_k \cap I = 0$ pour *tous* les k, ou que $J_k \cap I = I$ pour *tous* les k.

Considérons l'application quotient $\pi\colon A \to A/I$. Puisque π est surjective, les ensembles images $\pi(J_k)$ sont tous des idéaux (à droite) de A/I (la vérification est aisée), et on obtient une suite croissante d'idéaux

$$\pi(J_1) \subseteq \pi(J_2) \subseteq \ldots$$

dans A/I. Nous avons montré dans le premier point que A/I est Noethérien : donc $\pi(J_k) = \pi(J_{k+1})$ pour tous les k assez grands.

On prétend que $\pi(J_k) = \pi(J_{k+1})$ entraîne $J_k = J_{k+1}$. Si ce n'est pas le cas, on peut trouver $x \in J_{k+1} \setminus J_k$. Puisque $\pi(x) \in \pi(J_{k+1}) = \pi(J_k)$, il existe $x' \in J_k$ tel que $x - x' \in \ker \pi = I$.

(a) Si $J_{k+1} \cap I = 0$, puisque $x - x' \in J_{k+1} \cap I$ on obtient $x = x' \in J_k$, contradiction.

(b) Si $J_{k+1} \cap I = I$, alors par notre simplification initiale on a aussi $J_k \cap I = I$ et donc $I \subseteq J_k$. Alors $x - x' \in J_k$ et ainsi $x = x' + (x - x') \in J_k$, contradiction.

Ainsi $J_k = J_{k+1}$ pour tous les k assez grands, ce qui montre que la chaîne d'idéaux se stabilise. Ainsi A est Noethérien à droite.

Exercice 7. 1. On a $x^2+y^2 = (x+iy)(x-iy)$ dans $\mathbb{C}[x,y]$, donc le polynôme n'est pas irréductible dans $\mathbb{C}[x,y]$.

Montrons qu'il est irréductible dans $\mathbb{Q}[x,y]$. Posons $A := \mathbb{Q}[x]$, c'est un anneau factoriel en vertu des Corollaires 3.3.5 et 3.7.2. On a $\mathbb{Q}[x,y] = A[y]$, et $x^2+y^2 \in A[y]$ est primitif puisque son coefficient dominant est une unité. Donc par la Proposition 3.8.13, x^2+y^2 est irréductible dans $A[y]$ si et seulement si il est irréductible dans $\mathrm{Frac}(A)[y]$.

On a

$$\mathrm{Frac}(A) = \mathbb{Q}(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in \mathbb{Q}[x], g(x) \neq 0 \right\}.$$

Puisque $\deg_y(y^2 + x^2) = 2$ et que les polynômes constants non-nuls de $\mathrm{Frac}(A)[y]$ sont des unités, le polynôme $y^2 + x^2 \in A[y]$ se scinde dans $\mathrm{Frac}(A)[y]$ si et seulement si $y^2 + x^2$ (vu comme un polynôme en y) admet une racine dans $\mathrm{Frac}(A) = \mathbb{Q}(x)$, autrement dit si et seulement si il existe $f(x), g(x) \in \mathbb{Q}[x]$ tels que

$$\left(\frac{f(x)}{g(x)}\right)^2 = -x^2.$$

Cela impliquerait que

$$f(x)^2 = -x^2 g(x)^2 \quad \text{dans } \mathbb{Q}[x].$$

Regardons le coefficient dominant de chaque côté : celui de $f(x)^2$ est positif (il s'agit du carré du coefficient dominant de $f(x)$), celui de $-x^2g(x)^2$ est négatif (il s'agit de l'opposé du carré du coefficient dominant de $g(x)$), c'est une contradiction.

Donc $y^2 + x^2 \in \mathrm{Frac}(A)[y]$ est irréductible, et ainsi $y^2 + x^2 \in \mathbb{Q}[x,y]$ est irréductible.

2. Montrons que $x^3-(y^7+2y^5+y^3)$ est irréductible dans $\mathbb{Q}[x,y]$. Comme dans le point précédent (en échangeant les rôles de x et y), il suffit de montrer qu'il n'existe pas de polynômes $f(y), g(y) \in \mathbb{Q}[y]$ tels que

$$\left(\frac{f(y)}{g(y)}\right)^3 = y^7 + 2y^5 + y^3 \quad \text{dans } \mathbb{Q}(y).$$

Cela impliquerait que

$$f(y)^3 = (y^7 + 2y^5 + y^3) g(y)^3 \quad \text{dans } \mathbb{Q}[y].$$

Regardons le degré de chaque côté : celui de gauche est un multiple de 3, tandis que celui de droite vaut 1 modulo 3. C'est une contradiction, et on en déduit que $x^3 - (y^7 + 2y^5 + y^3)$ est irréductible dans $\mathbb{Q}[x,y]$.

Remarque : le critère d'Eisenstein ne peut être appliqué dans aucun des deux cas (remarquons que le décomposition de $y^7 + 2y^5 + y^3$ en facteurs premiers est $(y^2+1)^2y^3$).

Exercice 8.
Comme b est supposé non-nul, on peut diviser 1 par b pour obtenir

$$1 = bq + r,$$

avec $\sigma(r) < 0$ ou $r = 0$. Cela force $r = 0$.

Exercice 1. (a) Let $\phi : A \to B$ be a ring homomorphism and let $a \in A^\times$. Then, there exists $b \in A^\times$ such that $ab = 1$. Then:

$$1 = \phi(1) = \phi(ab) = \phi(a)\phi(b).$$

Hence $\phi(a)$ is an invertible element of B with inverse $\phi(b)$.

(b) Let $a, b \in A$ such that $a \sim b$. Then there exists $u \in A^\times$ such that $a = ub$ and we have:

$$\phi(a) = \phi(ub) = \phi(u)\phi(b).$$

Now by point (a) we have that $\phi(u) \in B^\times$ and we conclude that $\phi(a) \sim \phi(b)$.

(c) Counterexample: Consider the ring homomorphism: $\xi_2 : \mathbb{Z}[x] \to \mathbb{F}_2[x]$ (Example 1.4.36). Now $x^2 + 4x + 2 \in \mathbb{Z}[x]$ is irreducible (one shows this using Eisenstein with $p = 2$), but $\xi_2(x^2 + 4x + 2) = x^2$ and $x^2 \in \mathbb{F}_2[x]$ is reducible.

Exercice 2. (a) Voir corrigé du bonus 3.

(b) Par le théorème des restes chinois

$$\mathbb{Z}/pq\mathbb{Z} = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}.$$

Ainsi $(1,0)$, $(0,1)$, $(0,0)$ et $(1,1)$ sont des racines. Comme les polynômes en jeu sont moniques, on peut voir avec le degré que le produit des $(t - a_i)$ ne peut diviser $t^2 - t$.

(c) As $f|g$ in $\mathbb{Q}[t]$, there exists $h \in \mathbb{Q}[t]$ such that $g(t) = f(t)h(t)$. Now, as $h \in \mathbb{Q}[t|$, we can write $h(t) = c \cdot h_1(t)$, where $h_1(t) \in \mathbb{Z}[t]$ is primitive and $c \in \mathbb{Q}$. Then:

$$g(t) = c \cdot f(t)h_1(t).$$

By Lemma 3.8.9, we have that $f(t)h_1(t)$ is primitive and, since $g(t)$ is also primitive, we use Lemma 3.8.11 to determine that $c \in \mathbb{Z}^\times$, i.e. $c = \pm 1$. Then

$$g(t) = \pm f(t)h_1(t) \text{ in } \mathbb{Z}[t], \text{ therefore } f|g \text{ in } \mathbb{Z}[t].$$

(d) The roots of $x^4 + 1$ over $\mathbb{C}$ are $e^{i(\frac{\pi}{4} + \frac{k\pi}{2})}$, where $0 \leq k \leq 3$, and we have:

$$x^4 + 1 = \prod_{k=0}^{3} (x - e^{i(\frac{\pi}{4} + \frac{k\pi}{2})}).$$

We group the conjugate complex roots and obtain the decomposition over $\mathbb{R}[x]$

$$x^4 + 1 = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1).$$

By Example 3.9.2 (4), it follows $x^4 + 1$ does not admit roots in $\mathbb{Q}$, as it does not admit roots in $\mathbb{R}$. If $x^4 + 1 = f(x)g(x)$, where $f(x), g(x) \in \mathbb{Q}[x]$ are polynomials of degree 2, then $f(x) = (x - a_1)(x - a_2)$ and $g(x) = (x - a_3)(x - a_4)$, where $a_1, a_2, a_3, a_4 \in \{e^{i(\frac{\pi}{4} + \frac{k\pi}{2})} | \, 0 \leq k \leq 3\}$ are distinct. One checks that for every choice of a_i a_j the polynomial $(x - a_i)(x - a_j)$ does

not have coefficients in $\mathbb{Q}$. We conclude that x^4+1 is irreducible in $\mathbb{Q}[x]$. Lastly, we note that, as it is primitive., by Lemma 3.8.13, it is also irreducible in $\mathbb{Z}[x]$.

In $\mathbb{F}_2[x]$ we have $x^4+[1]_2=(x+[1]_2)^4$.

The squares in $\mathbb{F}_{11}$ are $[0]_{11},[1]_{11},[3]_{11},[4]_{11},[5]_{11}$ and $[9]_{11}$ and we deduce that $x^4+[1]_{11}$ does not admit roots in $\mathbb{F}_{11}$. Assume that $x^4+[1]_{11}$ admits a decomposition into a product of two polynomials of degree 2. As $\mathbb{F}_{11}$ is a field, we can assume that these polynomials are unitary. We have:

$$x^4+[1]_{11}=(x^2+ax+b)(x^2+cx+d)=x^4+(a+c)x^3+(b+ac+d)x^2+(bc+ad)x+bd$$

and so $d=b^{-1}$ and $c=-a$. We substitute and obtain:

$$x^4+[1]_{11}=x^4+(b-a^2+b^{-1})x^2+a(b^{-1}-b)x+[1]_{11}$$

and so $a(b^{-1}-b)=0$.

- if $a=0$, then $b-a^2+b^{-1}=b+b^{-1}=0$, which is impossible as $[-1]_{11}$ is not a square in $\mathbb{F}_{11}$.
- if $b=b^{-1}$, then $b^2=[1]_{11}$ and so $b\in\{[1]_{11},[10]_{11}\}$.
  - If $b=[1]_{11}$, then $b-a^2+b^{-1}=[2]_{11}-a^2=0$, which is impossible as $[2]_{11}$ is not a square in $\mathbb{F}_{11}$.
  - If $b=[10]_{11}$, then $b-a^2+b^{-1}=[9]_{11}-a^2=0$ and so $a\in\{[3]_{11},[8]_{11}\}$.

We conclude that

$$x^4+[1]_{11}=(x^2+[3]_{11}\cdot x+[10]_{11})(x^2+[8]_{11}\cdot x+[10]_{11}) \text{ in } \mathbb{F}_{11}[x].$$

Since $x^8-1=(x^4+1)(x^4-1)$ it suffices to factor x^4-1:

- in $\mathbb{C}[x]$ we have: $x^4-1=(x+i)(x-i)(x+1)(x-1)$.
- in $\mathbb{R}[x]$, $\mathbb{Q}[x]$ and $\mathbb{Z}[x]$ we have: $x^4-1=(x^2+1)(x+1)(x-1)$.
- in $\mathbb{F}_2[x]$ we have: $x^4-[1]_2=x^4+[1]_2=(x+[1]_2)^4$.
- in $\mathbb{F}_{11}[x]$ we have: $x^4-[1]_{11}=(x^2+[1]_{11})(x+[1]_{11})(x+[10]_{11})$, where we have seen earlier that $x^2+[1]_{11}$ is irreducible.

Exercice 3. (a) We write $\frac{2}{9}x^5+\frac{5}{3}x^4+x^3+\frac{1}{3}=\frac{1}{9}(2x^5+15x^4+9x^3+3)\in\mathbb{Q}[x]$.

Now $\frac{1}{9}\in\mathbb{Q}[x]^\times$, as $\frac{1}{9}\in\mathbb{Q}^\times$. Therefore $\frac{2}{9}x^5+\frac{5}{3}x^4+x^3+\frac{1}{3}$ is irreducible in $\mathbb{Q}[x]$ if and only if $2x^5+15x^4+9x^3+3$ is. As $\gcd(2,15,9,3)=1$, we have that $2x^5+15x^4+9x^3+3$ is primitive, hence it is irreducible in $\mathbb{Q}[x]$ if and only if it is irreducible in $\mathbb{Z}[x]$ (Lemma 3.8.13). Using Eisenstein for $p=3$, where $3\in\mathbb{Z}$ is irreducible, we deduce that $2x^5+15x^4+9x^3+3$ is irreducible in $\mathbb{Z}[x]$.

(b) Let $f(x)=x^4+[2]_5\in\mathbb{F}_5[x]$. Note that for all $a\in\mathbb{F}_5$ we have $a^2\in\{[0]_5,[1]_5,[4]_5\}$. Therefore f does not admit roots in $\mathbb{F}_5$. We will now show that f is not a product of two polynomials of degree 2. As $\mathbb{F}_5$ is a field, we can assume that these polynomials are unitary and so assume there exist $a,b,c,d\in\mathbb{F}_5$ such that

$$f(x)=x^4+[2]_5=(x^2+ax+b)(x^2+cx+d)=x^4+(a+c)x^3+(b+ac+d)x^2+(bc+ad)x+bd.$$

Then $c=-a$ and $d=[2]_5b^{-1}$ and substituting in the above gives:

$$x^4+[2]_5=x^4+(b-a^2+[2]_5\cdot b^{-1})x^2+(-ab+[2]_5\cdot ab^{-1})x+[2]_5.$$

Thus $-ab+[2]_5\cdot ab^{-1}=a(-b+[2]_5\cdot b^{-1})=0$ and

- if $a = 0$, then $b^2 = -[2]_5$, a contradiction.
- if $-b + [2]_5 b^{-1} = 0$, then $b^2 = [2]_5$, a contradiction.

We conclude that f is irreducible in $\mathbb{F}_5[x]$.

Lastly, let $x^4+15x^3+7 \in \mathbb{Q}[x]$. As the dominant coefficient is 1, this polynomial is primitive, hence it is irreducible in $\mathbb{Q}[x]$ if and only if it is irreducible in $\mathbb{Z}[x]$ (Lemma 3.8.13). Let $\phi_5 : \mathbb{Z} \to \mathbb{F}_5$ be the quotient homomorphism and let $\pi_5 : \mathbb{Z}[x] \to \mathbb{F}_5[x]$ be its induced homomorphism. We have that:

$$\pi_5(x^4 + 15x^3 + 7) = x^4 + [2]_5$$

and, as $x^4+[2]_5$ is irreducible in $\mathbb{F}_5[x]$, we use Proposition 3.9.1 to conclude that x^4+15x^3+7 is irreducible in $\mathbb{Z}[x]$.

(c) First we note that $x^2+y^2+1 \in \mathbb{R}[x,y]$ is primitive as its dominant coefficient is 1. Secondly, $y^2+1 \in \mathbb{R}[y]$ is irreducible. We now apply Eisenstein with $p = y^2+1$ to conclude that x^2+y^2+1 is irreducible in $\mathbb{R}[x,y]$.

(d) We have $x^2 + y^2 + [1]_2 = (x + y + [1]_2)^2$ in $\mathbb{F}_2[x,y]$.

(e) The evaluation homomorphism $\mathrm{ev}_0 : \mathbb{Q}[y] \to \mathbb{Q}$, $\mathrm{ev}_0(y) = 0$, induces the homomorphism $\xi : \mathbb{Q}[y][x] \to \mathbb{Q}[x]$ with $\xi(y) = 0$ and $\xi(x) = x$. We have that:

$$\xi(y^4 + x^3 + x^2y^2 + xy + 2x^2 - x + 1) = x^3 + 2x^2 - x + 1$$

and, by Proposition 3.9.1, $y^4 + x^3 + x^2y^2 + xy + 2x^2 - x + 1$ is irreducible in $\mathbb{Q}[x,y]$ if x^3+2x^2-x+1 is irreducible in $\mathbb{Q}[x]$. Now $\deg(x^3+2x^2-x+1) = 3$ and thus x^3+2x^2-x+1 is irreducible in $\mathbb{Q}[x]$ if and only if it does not admit roots in $\mathbb{Q}$. Assume $\frac{p}{r} \in \mathbb{Q}$, where $p, r \in \mathbb{Z}$ and $\gcd(p,r) = 1$, is a root of $x^3 + 2x^2 - x + 1$. Then

$$\left(\frac{p}{r}\right)^3 + 2\left(\frac{p}{r}\right)^2 - \left(\frac{p}{r}\right) + 1 = 0.$$

As $\gcd(p,r) = 1$, it follows that $p|1$, $r|1$ and so $\frac{p}{r} \in \{-1, 1\}$. One checks that neither -1, nor 1 is a root of $x^3 + 2x^2 - x + 1$ and thus $x^3 + 2x^2 - x + 1$ is irreducible in $\mathbb{Q}[x]$.

(f) We have $4x^3 + 120x^2 + 8x - 12 = 4(x^3 + 30x^2 + 2x - 3) \in \mathbb{Q}[x]$. Now $4 \in \mathbb{Q}[x]^\times$ and so $4x^3 + 120x^2 + 8x - 12$ is irreducible in $\mathbb{Q}[x]$ if and only if $x^3 + 30x^2 + 2x - 3$ is. As $\deg(x^3+30x^2+2x-3) = 3$ it follows that x^3+30x^2+2x-3 is irreducible in $\mathbb{Q}[x]$ if and only if it does not admit roots in $\mathbb{Q}$. Assume there exist $\frac{p}{r} \in \mathbb{Q}$, where $p, r \in \mathbb{Z}$ and $\gcd(p,r) = 1$, such that:

$$\left(\frac{p}{r}\right)^3 + 30\left(\frac{p}{r}\right)^2 + 2\left(\frac{p}{r}\right) - 3 = 0.$$

As $\gcd(p,r) = 1$, it follows that $p|3$ and $r|1$. Therefore $\frac{p}{r} \in \{-3, -1, 1, 3\}$. One checks that none of the elements in $\{-3, -1, 1, 3\}$ is a root of $x^3 + 30x^2 + 2x - 3$. We conclude that $x^3 + 30x^2 + 2x - 3$ is irreducible in $\mathbb{Q}[x]$. .

(g) As the polynomial t^6+t^3+1 is primitive, it follows that it is irreducible in $\mathbb{Q}[t]$ if and only if it is irreducible in $\mathbb{Z}[x]$ (Lemma 3.8.13). We consider the quotient homomorphism $\phi_2 : \mathbb{Z} \to \mathbb{F}_2$ and its induced homomorphism $\pi_2 : \mathbb{Z}[t] \to \mathbb{F}_2[t]$ under which

$$\pi_2(t^6 + t^3 + 1) = t^6 + t^3 + [1]_2.$$

By Proposition 3.9.1, $t^6 + t^3 + 1$ is irreducible in $\mathbb{Z}[t]$ if $t^6 + t^3 + [1]_2$ is irreducible in $\mathbb{F}_2[t]$.

Now, one checks that $t^6+t^3+[1]_2$ does not admit roots in $\mathbb{F}_2[t]$. Secondly, the only irreducible polynomial of degree 2 in $\mathbb{F}_2[t]$ is $t^2 + t + [1]_2$ and one checks that this does not divide

$t^6 + t^3 + [1]_2$. Lastly, we assume that $t^6 + t^3 + [1]_2$ is a product of two polynomials of degree 3. As $\mathbb{F}_2$ is a field, we can assume that these polynomials are unitary and we have:

$$\begin{aligned} t^6 + t^3 + [1]_2 &= (t^3 + a_2t^2 + a_1t + a_0)(t^3 + b_2t^2 + b_1t + b_0) \\ &= t^6 + (a_2 + b_2)t^5 + (a_1 + a_2b_2 + b_1)t^4 + (a_0 + a_1b_2 + a_2b_1 + b_0)t^3 + \\ &\quad + (a_0b_2 + a_1b_1 + a_2b_0)t^2 + (a_0b_1 + a_1b_0)t + a_0b_0. \end{aligned}$$

Then $a_0 = b_0 = [1]_2$, $a_2 = b_2$ and

$$\begin{cases} a_0b_1 + a_1b_0 = [0]_2 \\ a_0b_2 + a_1b_1 + a_2b_0 = [0]_2 \\ a_0 + a_1b_2 + a_2b_1 + b_0 = [1]_2 \\ a_1 + a_2b_2 + b_1 = [0]_2 \end{cases} \rightarrow \begin{cases} b_1 + a_1 = [0]_2 \\ a_1b_1 = [0]_2 \\ b_2(a_1 + b_1) = [1]_2 \\ a_2b_2 = [0]_2 \end{cases} \rightarrow [1]_2 = [0]_2.$$

We conclude that $t^6 + t^3 + [1]_2$ is irreducible in $\mathbb{F}_2[t]$.

(h) We first note that the ring $\mathbb{Q}[x]$ is factorial, as $\mathbb{Q}$ is (Theorem 3.8.1), and that $x \in \mathbb{Q}[x]$ is irreducible. Secondly the polynomial $y^4 + xy^3 + xy^2 + x^2y + 3x^2 - 2x \in \mathbb{Q}[x, y]$ is primitive, as its dominant coefficient is 1. We now apply Eisenstein with $p = x$ to conclude that $y^4 + xy^3 + xy^2 + x^2y + 3x^2 - 2x$ is irreducible in $\mathbb{Q}[x, y]$.

Exercice 4.
Let $f(t) = t^4 + 4t^3 + 3t^2 + 7t - 4 \in \mathbb{Z}[t]$.

(a) We have $\pi_2(f(t)) = t^4 + t^2 + t = t(t^3 + t + [1]_2) \in \mathbb{F}_2[t]$. Moreover, we remark that $t^3 + t + [1]_2$ is irreducible in $\mathbb{F}_2[t]$, as it does not admit roots in $\mathbb{F}_2$.

(b) We have $\pi_3(f(t)) = t^4 + t^3 + t - [1]_3 = (t^2 + [1]_3)(t^2 + t - [1]_3) \in \mathbb{F}_3[t]$.

(c) Assume that $f(t)$ is reducible in $\mathbb{Z}[t]$. Then either $f(t) = (t - a)g(t)$, where $a \in \mathbb{Z}$ and $g(t) \in \mathbb{Z}[t]$ is a polynomial of degree 3, or $f(t) = f_1(t)f_2(t)$, where $f_1(t), f_2(t) \in \mathbb{Z}[t]$ are two polynomials of degree 2.

In the first case, $a|4$ but none of the elements of $\{\pm 1, \pm 2, \pm 4\}$ are roots of f. Hence, we only need to consider the case when $f(t) = f_1(t)f_2(t)$, where $\deg(f_1(t)) = \deg(f_2(t)) = 2$, and we have:

$$\pi_2(f(t)) = \pi_2(f_1(t)f_2(t)) = \pi_2(f_1(t))\pi_2(f_2(t).$$

Now, as $\deg(\pi_2(f(t))) = 4$ and as $\deg(\pi_2(f_1(t))) = \deg(\pi_2(f_2(t))) \leq 2$, it follows that $\deg(\pi_2(f_1(t))) = 2$ and $\deg(\pi_2(f_2(t))) = 2$.

On the other hand, we have $\pi_2(f(t)) = t^4 + t^2 + t = t(t^3 + t + [1]_2)$, where $t^3 + t + [1]_2 \in \mathbb{F}_2[t]$ is irreducible. We have arrived at a contradiction. We conclude that $f(t) \in \mathbb{Z}[t]$ is irreducible.

Exercice 1. 1. Let L' denote the field extension of K of degree 1. This means that L' is a field that contains K, and that has a K- vector space structure such that the dimension of L' as a K-vector space is 1.The K-subspace of L' generated by 1 is equal to K, and equal to L' as well, due to the dimension of L' over K being 1. Hence K and L' coincide.

2. We take any $\alpha \in L \setminus K$. Then we have the following field extensions, $K \subseteq K(\alpha) \subseteq L$. From this, it follows using Proposition 4.2.15 that

$$\underbrace{[L:K]}_{=2} = [L:K(\alpha)] \cdot [K(\alpha):K].$$

Since we take $\alpha \notin K$, it holds that $K \neq K(\alpha)$, and hence by the first point, $[K(\alpha):K] \neq 1$. From this, it follows using the equation above that $[K(\alpha):K] = 2$. But that means that $[L:K(\alpha)] = 1$, from which it follows by the first point that $L = K(\alpha)$.

3. Since $L = K(\alpha)$, and $[L:K] = 2$, it holds that $\{1, \alpha\}$ forms a K-linear basis of $K(\alpha)$. This means in particular that α^2 is a K-linear combination of 1 and α. There exists $a, b \in K$ such that $\alpha^2 = b \cdot 1 + a \cdot \alpha \Leftrightarrow \alpha^2 - a\alpha - b = 0$. We define d to be $d = a^2 + 4b$, the discriminant of the quadratic equation. We now show that d is a square in $K(\alpha)$. We do so by multiplying the quadratic equation by 4 (note that the characteristic of K is not equal to 2), and completing the square, to find:

$$4\alpha^2 - 4a\alpha - 4b = 0 \Leftrightarrow (2\alpha - a)^2 - a^2 - 4b = 0 \Leftrightarrow (2\alpha - a)^2 = a^2 + 4b = d.$$

Hence d is a square in $K(\alpha)$, and we let $\delta = 2\alpha - a \in K(\alpha) \setminus K$, with $\delta^2 = d$. By the second part of this exercise, it holds that $L = K(\delta) = K(\sqrt{d})$.

Let us give an alternative proof that illuminates the role of the discriminant. Since the characteristic of K is different from 2, the well-known theory of quadratic equations with coefficients in $\mathbb{C}$ can be carried over verbatim to K to obtain the following: if $p(x) = ax^2 + bx + c \in K[x]$ is a degree 2 polynomial, then the roots ξ_1, ξ_2 of $p(x)$ in any extension F of K can be written

$$\xi_1 = \frac{-2b + \sqrt{\Delta(p)}}{2a}, \quad \xi_2 = \frac{-2b - \sqrt{\Delta(p)}}{2a}$$

where $\Delta(p) = b^2 - 4ac$ and $\sqrt{\Delta(p)} \in F$ denotes a square root of $\Delta(p)$. Now observe that:

(a) $K(\xi_i) = K(\xi_1, \xi_2)$ for any $i = 1, 2$. We can write in $K(\xi_1)[x]$ that

$$p(x) = (x - \xi_1)q(x)$$

where necessarily $\deg q(x) = 1$. Thus $q(x) = x - \xi_2$, and so $\xi_2 \in K(\xi_1)$. Hence $K(\xi_1) = K(\xi_1, \xi_2)$, and by exchanging the roles of ξ_1 and ξ_2 we also obtain $K(\xi_2) = K(\xi_1, \xi_2)$.

(b) $K(\xi_1, \xi_2) = K\left(\sqrt{\Delta(p)}\right)$. Indeed $\sqrt{\Delta(p)} = 2a(\xi_1 - \xi_2)$ so the inclusion $\supseteq$ holds. Also it follows from the formulae for ξ_1 and ξ_2 that $\subseteq$ holds.

So we obtain that $K(\xi_1) = K(\xi_2) = K(\xi_1, \xi_2) = K\left(\sqrt{\Delta(p)}\right)$ as subfields of F. Taking $F = L$ and $p(x) = m_{\alpha,K}$, we obtain an alternative proof of the exercise.

4. From the definition of δ, it immediately follows that $\{1, \delta\}$ forms a K-linear basis of $K(\delta)$ as a K-vector space. By definition, $[K(\delta):K]$ is the dimension of $K(\delta)$ as a K-vector space, which is 2.

Exercice 2. 1. There are two options for $\mathbb{Q}(\sqrt{a})$. If a is a square in $\mathbb{Q}$, then it holds that $\sqrt{a}$ is contained in $\mathbb{Q}$, and hence $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}$, and so $[\mathbb{Q}(\sqrt{a}) : \mathbb{Q}] = 1$. If a is no square, then $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{a})$, and the degree of this field extension is equal to 2, since the polynomial $x^2 - a$ is zero for $\sqrt{a}$, and the polynomial is irreducible (since a is no square). The same holds for $\mathbb{Q}(\sqrt{b})$. We now use the fact (seen in Linear Algebra) that any two vector spaces over the same field are isomorphic if and only if they are of the same dimension. In our case, both $\mathbb{Q}(\sqrt{a})$ and $\mathbb{Q}(\sqrt{b})$ can be of dimension 1 or 2 over $\mathbb{Q}$, depending on whether or not a resp. b is a square. We conclude that $\mathbb{Q}(\sqrt{a})$ is of the same dimension over $\mathbb{Q}$ as $\mathbb{Q}(\sqrt{b})$, and hence isomorphic, if and only if both a and b are simultaneously squares in $\mathbb{Q}$, or both are simultaneously not squares.

2. We now assume that $\mathbb{Q}(\sqrt{a})$ and $\mathbb{Q}(\sqrt{b})$ are isomorphic as fields. We claim that this holds if and only if they are equal as subfields of $\mathbb{C}$. This means that there exists $c \in \mathbb{Q}$ such that $\sqrt{a} = c\sqrt{b}$.

   First, we assume that $\sqrt{a} = c\sqrt{b}$. Then, $\sqrt{a}$ and $\sqrt{b}$ generate the same field extension of $\mathbb{Q}$, and hence clearly the two fields are isomorphic.

   Secondly, assume that the fields $\mathbb{Q}(\sqrt{a})$ and $\mathbb{Q}(\sqrt{b})$ are isomorphic. Denote the isomorphism $\varphi : \mathbb{Q}(\sqrt{a}) \to \mathbb{Q}(\sqrt{b})$. We note that from $\varphi(1) = 1$, it follows that φ acts as the identity on $\mathbb{Z}$, and furthermore on $\mathbb{Q}$. On one hand, we have that $\varphi(\sqrt{a}) = u + \sqrt{b}v$ for some $u, v \in \mathbb{Q}$. On the other hand, with $a \in \mathbb{Q}$, it holds that

$$a = \varphi(a) = \varphi(\sqrt{a}^2) = \varphi(\sqrt{a})^2 = (u + \sqrt{b}v)^2 = (u^2 + bv^2) + \sqrt{b}(2uv).$$

   We now distinguish between two cases.

   - If $\sqrt{b} \in \mathbb{Q}$, then $\varphi(\sqrt{a}) \in \mathbb{Q}$, and hence $\sqrt{a} \in \mathbb{Q}$. (If $\sqrt{a}$ was not contained in $\mathbb{Q}$, then φ would be an isomorphism from $\mathbb{Q}(\sqrt{a}) \neq \mathbb{Q}$ to $\mathbb{Q}$. This is a contradiction to φ being injective.) Then,

$$\sqrt{a} = \frac{\sqrt{a}}{\sqrt{b}} \cdot \sqrt{b},$$

     and $\sqrt{a} = c\sqrt{b}$ with $c := \frac{\sqrt{a}}{\sqrt{b}} \in \mathbb{Q}$.

   - If $\sqrt{b} \notin \mathbb{Q}$, then

$$a = (u^2 + bv^2) + \sqrt{b}(2uv),$$

     with $\sqrt{b} \notin \mathbb{Q}$. Since $a \in \mathbb{Q}$, it follows that $2uv = 0$, and hence either $u = 0$ or $v = 0$. If $u = 0$, then $a = bv^2 \Rightarrow \sqrt{a} = \sqrt{b}v$, and hence the property is satisfied. If $v = 0$, then $\varphi(\sqrt{a}) = u \in \mathbb{Q}$. It then follows that the image of φ is contained in $\mathbb{Q}$, which means that φ can not be an isomorphism. Hence this case does not occur.

Exercice 3. 1. We have the following field extensions,

$$K \subset K(\alpha^2) \subset K(\alpha) \subset L.$$

   By proposition 4.2.15, it follows that

$$[L : K] = [L : K(\alpha)] \cdot [K(\alpha) : K(\alpha^2)] \cdot [K(\alpha^2) : K].$$

   Since the degree of the field extension L over K is odd, it follows that the degrees on the right hand side of the equality above are odd as well. We now look at the extension $K(\alpha)$ over $K(\alpha^2)$. The degree of this extension is at most 2, since the polynomial $x^2 - \alpha^2 \in K(\alpha^2)[x]$ vanishes at α. But since the degree needs to be odd, it follows that it is 1. Hence $K(\alpha) = K(\alpha^2)$.

2. We first show that $\sqrt{p} \notin \mathbb{Q}(\sqrt{q})$. If $\sqrt{p}$ is contained in $\mathbb{Q}(\sqrt{q})$, then there are $r, s \in \mathbb{Q}$ such that $\sqrt{p} = r + s\sqrt{q}$. From this, it follows that

$$p = (r + s\sqrt{q})^2 = (r^2 + s^2 q) + (2rs)\sqrt{q}.$$

Using the fact that $p \in \mathbb{Q}$, we compare the right hand side and left hand side, and note that $2rs = 0$. If $r = 0$, then $p = s^2 q$ which is a contradiction with p, q prime and distinct.

If $s = 0$, then $\sqrt{p} = r \Rightarrow p = r^2$, which is a contradiction to p prime.

It follows that $\sqrt{p} \notin \mathbb{Q}(\sqrt{q})$. The same argument, with the roles of p and q reversed shows that $\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$.

We now compute the degree of the field extension $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ over $\mathbb{Q}$. We have the following extensions of fields,

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\sqrt{p}, \sqrt{q}).$$

From proposition 4.2.15 it follows that

$$[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}(\sqrt{p})] \cdot [\mathbb{Q}(\sqrt{p}) : \mathbb{Q}].$$

We calculate both degrees on the right hand side separately. Firstly, $[\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 2$. This holds because $\sqrt{p} \notin \mathbb{Q}$. The polynomial $x^2 - p \in \mathbb{Q}[x]$ vanishes at $\sqrt{p}$, and combining Gauss III with Eisenstein for the prime p, it follows that the polynomial is irreducible over $\mathbb{Q}$. Hence it is the minimal polynomial, and the degree is 2.

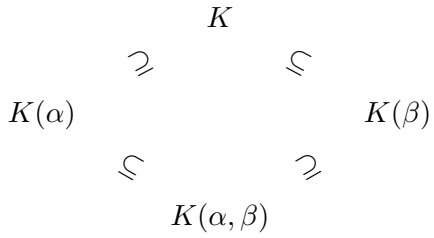
Secondly, $[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}(\sqrt{p})] = 2$. This holds because $\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$. Therefore, the degree of the extension is not equal to 1. Furthermore, the degree of the extension is at most 2, since $\sqrt{q}^2 = q \in \mathbb{Q}$, and hence $\sqrt{q}^2 \in \mathbb{Q}(\sqrt{p})$. Combining these restrictions, the degree of the extension is equal to 2, and hence the product of the two extensions is 4, meaning that $[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}] = 4$.

3. We have the following extension of fields, $K \subset K(\alpha) \subset K(\alpha, \beta)$. Using proposition 4.2.15, it follows that

$$[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\alpha)] \cdot [K(\alpha) : K].$$

From this, it follows that $m = [K(\alpha) : K]$ divides $[K(\alpha, \beta) : K]$. The same argument for the extension of fields $K \subset K(\beta) \subset K(\alpha, \beta)$ shows that n divides $[K(\alpha, \beta) : K]$. Using the fact that m and n are coprime, it follows that mn divides $[K(\alpha, \beta) : K]$. This means that the degree of the field extension is a multiple of mn. We show that it is equal to mn by considering the first field extension again, $K \subset K(\alpha) \subset K(\alpha, \beta)$. Since $[K(\beta) : K] = n$, it holds in particular that the degree of the field extension $K(\alpha, \beta)$ over $K(\alpha)$ is at most n. Hence $[K(\alpha, \beta) : K]$ is at most nm. On the other hand, as we have seen above, it is at least mn, from which we conclude that it is exactly mn.

The two field extensions are illustrated below.



Exercice 4.

It holds that $\mathbb{Q}(\sqrt{3} + \sqrt{7}) \subseteq \mathbb{Q}(\sqrt{3}, \sqrt{7})$. We show that indeed it holds that $\mathbb{Q}(\sqrt{3} + \sqrt{7}) =$

$\mathbb{Q}(\sqrt{3},\sqrt{7})$. For this, it is enough to show that $\sqrt{3} \in \mathbb{Q}(\sqrt{3}+\sqrt{7})$ and $\sqrt{7} \in \mathbb{Q}(\sqrt{3}+\sqrt{7})$. We denote $K = \mathbb{Q}(\sqrt{3}+\sqrt{7})$. It holds that $(\sqrt{3}+\sqrt{7})^3 = 24\sqrt{3}+16\sqrt{7} \in K$. With this, and using that $-16\sqrt{3}-16\sqrt{7} \in K$, it follows that their sum is contained in K as well,

$$(24\sqrt{3}+16\sqrt{7})+(-16\sqrt{3}-16\sqrt{7}) = 8\sqrt{3}.$$

Now using that $\frac{1}{8} \in K$, and $8\sqrt{3} \in K$ we deduce that their product $\sqrt{3} \in K$. From $\sqrt{3} \in K$, it immediately follows that $\sqrt{7} \in K$ as well, since $\sqrt{7} = (\sqrt{3}+\sqrt{7})-\sqrt{3}$. This shows that indeed $K = \mathbb{Q}(\sqrt{3},\sqrt{7})$.

The degree of the field extension $[\mathbb{Q}(\sqrt{3},\sqrt{7}):\mathbb{Q}]$ is by definition the dimension of $\mathbb{Q}(\sqrt{3},\sqrt{7})$ as a $\mathbb{Q}$-vector space. Using exercise 3.2, it follows that the degree is 4. $\{1,\sqrt{3},\sqrt{7},\sqrt{3}\sqrt{7}\}$ forms a basis of this vector space.

Exercice 5. 1. If $p = 2$, then $e^{2i\pi/2} = -1$, which is contained in $\mathbb{R}$, and hence $\mathbb{R}(e^{2i\pi/p}) = \mathbb{R}$. From this, it follows that the degree of the extension is equal to 1.

For $p \neq 2$, it holds that $e^{2i\pi/p}$ is a complex number, and not contained in $\mathbb{R}$. By example 4.2.14 (a), we know that $[\mathbb{C}:\mathbb{R}] = 2$. Using exercise 1.2, it follows that $\mathbb{R}(e^{2i\pi/p}) = \mathbb{C}$, and hence $[\mathbb{R}(e^{2i\pi/p}):\mathbb{R}] = [\mathbb{C}:\mathbb{R}] = 2$.

2. By definition, α vanishes over $t^{42}+t^{41}+\cdots+t^2+t+1$. Furthermore, using the fact that 43 is prime, and Example 3.9.4(b), it follows that $t^{42}+t^{41}+\cdots+t^2+t+1$ is irreducible over $\mathbb{Q}$. Hence we get that $m_{\alpha,\mathbb{Q}} = t^{42}+t^{41}+\cdots+t^2+t+1$, and so $[\mathbb{Q}(\alpha):\mathbb{Q}] = 42$.

3. We follow the same steps as example 4.2.16(a). First, we note that we have the following field extensions, $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[5]{13}) \subseteq \mathbb{Q}(\sqrt[5]{13},i)$. We can calculate the degree of the extension $\mathbb{Q}(\sqrt[5]{13},i)$ over $\mathbb{Q}$ using proposition 4.2.15. It holds that

$$[\mathbb{Q}(\sqrt[5]{13},i):\mathbb{Q}] = [\mathbb{Q}(\sqrt[5]{13},i):\mathbb{Q}(\sqrt[5]{13})]\cdot[\mathbb{Q}(\sqrt[5]{13}):\mathbb{Q}].$$

First, we calculate $[\mathbb{Q}(\sqrt[5]{13}):\mathbb{Q}]$. The polynomial x^5-13 vanishes at $\sqrt[5]{13}$. Furthermore, the polynomial is irreducible over $\mathbb{Q}$: By Gauss III, it is equivalent to showing that the polynomial is irreducible over $\mathbb{Z}$. We can apply Eisensteins criterion with $p = 13$, form which irreducibility over $\mathbb{Z}$ follow. Therefore, $m_{\sqrt[5]{13},\mathbb{Q}} = x^5-13$, and the degree of the field extension is 5.

Secondly, we calculate $[\mathbb{Q}(\sqrt[5]{13},i):\mathbb{Q}(\sqrt[5]{13})]$. Since $\mathbb{Q} \subseteq \mathbb{R}$, and $\sqrt[5]{13} \in \mathbb{R}$, it follows that $\mathbb{Q}(\sqrt[5]{13}) \subseteq \mathbb{R}$. Hence $i \notin \mathbb{Q}(\sqrt[5]{13})$. Using that i is a root of x^2+1, we get that the degree of i over $\mathbb{Q}(\sqrt[5]{13})$ is 2, and hence $[\mathbb{Q}(\sqrt[5]{13},i):\mathbb{Q}(\sqrt[5]{13})] = 2$.

By the formula above, it follows that

$$[\mathbb{Q}(\sqrt[5]{13},i):\mathbb{Q}] = [\mathbb{Q}(\sqrt[5]{13},i):\mathbb{Q}(\sqrt[5]{13})]\cdot[\mathbb{Q}(\sqrt[5]{13}):\mathbb{Q}] = 2\cdot 5 = 10.$$

4. There are two possibilities. The first possibility is that α is the root $\alpha = [1]_3$. In that case, $\mathbb{F}_3(\alpha) = \mathbb{F}_3$, and hence $[\mathbb{F}_3(\alpha):\mathbb{F}_3] = 1$. We can therefore write the polynomial $t^4-t^3-t^2-t-[1]_3 = (t-[1]_3)(t^3-t+[1]_3)$. If $\alpha \neq [1]_3$, then α is a root of the polynomial $t^3-t+[1]_3$. But this polynomial is irreducible over $\mathbb{F}_3$, since neither $[0]_3,[1]_3$ or $[2]_3$ is a root of $t^3-t+[1]_3$. We conclude with the fact that $m_{\alpha,\mathbb{F}_3} = t^3-t+[1]_3$, and hence $[\mathbb{F}_3(\alpha):\mathbb{F}_3] = 3$.

5. We note that $(3+\sqrt{5})^2 = 14+6\sqrt{5} \Rightarrow 3+\sqrt{5} = \sqrt{14+6\sqrt{5}}$. Therefore, $\mathbb{Q}(\sqrt{14+6\sqrt{5}},\sqrt{3}) = \mathbb{Q}(3+\sqrt{5},\sqrt{3}) = \mathbb{Q}(\sqrt{5},\sqrt{3})$. It follows that $[\mathbb{Q}(\sqrt{5},\sqrt{3}):\mathbb{Q}] = 4$. $\{1,\sqrt{3},\sqrt{5},\sqrt{3}\sqrt{5}\}$ forms a basis of $\mathbb{Q}(\sqrt{5},\sqrt{3})$ as a $\mathbb{Q}$-vector space.

6. We calculate the degree of the extension using proposition 4.2.15 for the extension $\mathbb{Q} \subseteq \mathbb{Q}((\sqrt[6]{7})^2) \subseteq \mathbb{Q}(\sqrt[6]{7})$, from which it follows that

$$[\mathbb{Q}(\sqrt[6]{7}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[6]{7}) : \mathbb{Q}((\sqrt[6]{7})^2)] \cdot [\mathbb{Q}((\sqrt[6]{7})^2) : \mathbb{Q}].$$

We first calculate $[\mathbb{Q}(\sqrt[6]{7}) : \mathbb{Q}]$. The polynomial $x^6 - 7 \in \mathbb{Q}[x]$ is zero for $\sqrt[6]{7}$. Furthermore, by Gauss III, it is irreducible if it is irreducible over $\mathbb{Z}$. Applying Eisenstein with $p = 7$, this holds. Hence $m_{\sqrt[6]{7},\mathbb{Q}} = x^6 - 7$, and the degree of the field extension is 6.

Secondly, we calculate $[\mathbb{Q}((\sqrt[6]{7})^2) : \mathbb{Q}]$. It holds that $(\sqrt[6]{7})^2 = \sqrt[3]{7}$. The polynomial $x^3 - 7 \in \mathbb{Q}[x]$ is zero for $\sqrt[3]{7}$. Furthermore, by Gauss III, it is irreducible if it is irreducible over $\mathbb{Z}$. Applying Eisenstein with $p = 7$, this holds. Hence $m_{\sqrt[3]{7},\mathbb{Q}} = x^3 - 7$, and the degree of the field extension is 3.

Using the formula above, we get that $[\mathbb{Q}(\sqrt[6]{7}) : \mathbb{Q}((\sqrt[6]{7})^2)] = 2$.

7. We apply the same technique as in the exercise above, noting that we have an extension as follows, $\mathbb{F}_2 \subseteq \mathbb{F}_2(\alpha^2) \subseteq \mathbb{F}_2(\alpha)$, and hence

$$[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = [\mathbb{F}_2(\alpha) : \mathbb{F}_2(\alpha^2)] \cdot [\mathbb{F}_2(\alpha^2) : \mathbb{F}_2].$$

On the left hand side, the degree is equal to 3, since $m_{\alpha,\mathbb{F}_2} = t^3 + t + [1]_2$. Hence on the right hand side, one of the factors is 1, and the other one is three. We note that $[\mathbb{F}_2(\alpha^2) : \mathbb{F}_2]$ can not be 1, since $\alpha^2 \notin \mathbb{F}_2$. If α^2 was contained in $\mathbb{F}_2$, then the polynomial $t^2 - \alpha^2 \in \mathbb{F}_2[t]$ vanishes at α, which contradicts the fact that $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = 3$. Therefore, $[\mathbb{F}_2(\alpha^2) : \mathbb{F}_2] = 3$, and so $[\mathbb{F}_2(\alpha) : \mathbb{F}_2(\alpha^2)] = 1$.

Exercice 6. 1. We show that the minimal polynomial $m_{\beta,K} = x^7 - y \in K[x]$. It holds that the polynomial vanishes at β, since

$$\beta^7 - y = \left(\frac{\alpha^3}{y^2}\right)^7 - y = \frac{(\alpha^7)^3}{y^{14}} - y \overset{*}{=} \frac{(y^5)^3}{y^{14}} - y = y - y = 0,$$

where in the equation $*$, we use the fact that α is a root of f in L, and hence $\alpha^7 = y^5$. Furthermore, the polynomial is irreducible in $K[x]$: We use Gauss III to deduce that f is irreducible in $K[x] = (\mathbb{C}(y))[x]$ if and only if f is irreducible in $(\mathbb{C}[y])[x]$. Since y is irreducible in $\mathbb{C}[y]$, we may use Eisenstein with $p = y$ to deduce that $x^7 - y$ is irreducible in $(\mathbb{C}[y])[x]$, and hence in $K[x]$. This proves that the minimal polynomial $m_{\beta,K} = x^7 - y \in K[x]$. We conclude that $[K(\beta) : K] = 7$.

2. To show that $K(\alpha) = K(\beta)$, we show that $K(\alpha) \subseteq K(\beta)$ and $K(\beta) \subseteq K(\alpha)$.

We note that

$$\beta^5 = \left(\frac{\alpha^3}{y^2}\right)^5 = \frac{\alpha^{15}}{(y^5)^2} = \frac{\alpha^{15}}{(\alpha^7)^2} = \alpha.$$

From this, it follows that $\alpha = \beta^5 \in K(\beta)$, and hence $K(\alpha) \subseteq K(\beta)$. On the other hand, $\beta = \frac{\alpha^3}{y^2} \in K(\alpha)$, and hence $K(\beta) \subseteq K(\alpha)$.

3. We first remark that by Gauss III, f is irreducible in $\mathbb{C}[x, y] = (\mathbb{C}[y])[y]$ if and only if f is irreducible in $(\mathbb{C}(y))[x] = K[x]$. By the first and second part of this exercise, it holds that $[K(\alpha) : K] = 7$. From this, it follows that the degree of the minimal polynomial $m_{\alpha,K}$ is 7. Now since α is a root of $x^7 - y^5 \in K[x]$, it follows that $x^7 - y^5 \mid m_{\alpha,K}$. Since both polynomials are of degree 7, it follows that $m_{\alpha,K} \sim x^7 - y^5$, and from $m_{\alpha,K}$ being irreducible in $K[x]$ it follows that $x^7 - y^5$ is irreducible in $K[x]$ as well. Applying Gauss III, with $x^7 - y^5$ being primitive, it follows that $x^7 - y^5$ is irreducible in $\mathbb{C}[x, y]$.

Exercice 7.
Par le point 3 de l'exercice bonus, pour tout $k \geq 1$, le polynôme $\Phi_k(t)$ est irréductible. En particulier

$$t^n - 1 = \prod_{d|n} \Phi_d(t)$$

est une décomposition en irréductibles dans $\mathbb{Q}[t]$. Dès lors,

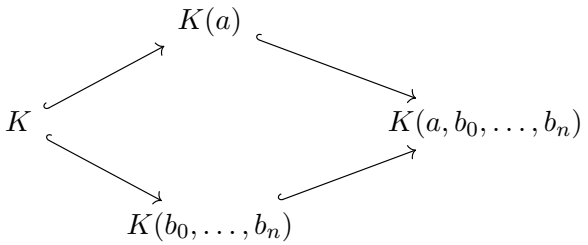
$$\mathbb{Q}[\mathbb{Z}/n\mathbb{Z}] \cong \mathbb{Q}[t]/(t^n - 1) \cong \prod_{d|n} \mathbb{Q}(\xi_d).$$

On a désigné par ξ_d une racine primitive d-ième de l'unité. Si $\mu(n)$ désigne le nombre de diviseurs de n, on obtient alors

$$\pi_0(\mathbb{Q}[\mathbb{Z}/n\mathbb{Z}]) = \mu(n).$$

Exercice 1.
Soient $K \subset L \subset F$ comme dans l'énoncé. Pour montrer que F est algébrique sur K, il suffit de montrer que chaque $a \in F$ est algébrique sur K. Puisque a est algébrique sur L, il existe $b_0, \dots, b_n \in L$ tels que $m_{a,L}(t) = \sum_{i=0}^{n} b_i t^i$. En particulier, a est algébrique sur le sous-corps $K(b_0, \dots, b_n)$.

Nous allons comparer les deux chaînes d'extensions suivantes :



On prétend que les degrés

$$[K(a, b_0, \dots, b_n) : K(b_0, \dots, b_n)] \quad \text{et} \quad [K(b_0, \dots, b_n) : K]$$

sont finis. C'est le cas du premier par construction (cf la Proposition 4.2.7 et le Corollaire 4.2.13). Pour le second, par la formule de multiplication des degrés on se réduit à montrer que chaque

$$[K(b_0, \dots, b_{i+1}) : K(b_0, \dots, b_i)]$$

est fini. C'est le cas par le Corollaire 4.2.13, puisque b_{i+1} est algébrique sur K, donc a fortiori sur $K(b_0, \dots, b_i)$. On peut ainsi appliquer la Proposition 4.2.15 pour obtenir

$$[K(a, b_0, \dots, b_n) : K] = [K(a, b_0, \dots, b_n) : K(b_0, \dots, b_n)] \cdot [K(b_0, \dots, b_n) : K] < \infty.$$

On en déduit que l'extension intermédiaire $K \subset K(a) \subset K(a, b_0, \dots, b_n)$ est de degré fini sur K (il s'agit simplement d'algèbre linéaire : un sous-espace vectoriel d'un espace de dimension finie, est également de dimension finie). Donc a est algébrique sur K par le Corollaire 4.2.13.

Exercice 2.
Comme

$$\cos(2\pi/n) = \frac{e^{2\pi i/n} + e^{-2\pi i/n}}{2} \quad \sin(2\pi/n) = \frac{e^{2\pi i/n} - e^{-2\pi i/n}}{2i}$$

on voit que $\cos(2\pi/n), \sin(2\pi/n) \in \mathbb{Q}(\xi_n, i)$ si ξ_n désigne une racine primitive n-ième de l'unité, ce qui conclut.

On peut aussi tirer partie des polynômes de Chebyshev $\{T_n(x)\}_n$, qui ont la propriété que

$$\cos(n\theta) = T_n(\cos(\theta)) \quad \forall \theta \in \mathbb{R}\ n \geq 0.$$

Les polynômes $T_n(x)$ sont définis par la relation de récurrence

$$T_0(x) = 1, \quad T_1(x) = x, \quad T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x).$$

et il s'ensuit que les coefficients de $T_n(x)$ sont rationnels (et même entiers) pour tous les n.

On voit ainsi que $\cos(\theta)$ est algébrique sur $\mathbb{Q}(\cos(n\theta))$ pour tout $n \geq 1$. En prenant $\theta = 2\pi/m$ et $n = m$, on obtient ainsi que $\cos(2\pi/n)$ est algébrique sur $\mathbb{Q}(\cos(2\pi)) = \mathbb{Q}$.

Pour finir, la relation bien connue $\cos^2(\theta) + \sin^2(\theta) = 1$ entraîne que $\sin(2\pi/n)$ est algébrique sur $\mathbb{Q}(\cos(2\pi/n))$, et donc sur $\mathbb{Q}$ par l'Exercice 1.

Exercice 3.
Dans $\mathbb{Q}(x)$ on a la relation $x^3 - sx + 2 = 0$, ce qui montre que x est une racine du polynôme $t^3 - st + 2 \in \mathbb{Q}(s)[t]$. Ainsi $\mathbb{Q}(x) = \mathbb{Q}(s, x)$ est une extension algébrique de $\mathbb{Q}(s)$. On prétend que $\mathbb{Q}(s)$ est une extension transcendante de $\mathbb{Q}$. Si ce n'était pas le cas, alors par l'Exercice 1 l'extension $\mathbb{Q} \subset \mathbb{Q}(x)$ serait également algébrique, ce qui est absurde. Donc $[\mathbb{Q}(s) : \mathbb{Q}] = \infty$.

Calculons ensuite le degré de $\mathbb{Q}(x)$ sur $\mathbb{Q}(s)$. On prétend que $t^3 - st + 2$ est irréductible dans $\mathbb{Q}(s)[t]$, et il s'ensuivra que $[\mathbb{Q}(x) : \mathbb{Q}(s)] = 3$. Si ce polynôme n'est pas irréductible, puisqu'il est de degré 3 il doit admettre une racine dans $\mathbb{Q}(s)$. Puisque s est transcendant sur $\mathbb{Q}$, on peut traiter s comme une variable indépendante et oublier qu'elle a été définie en fonction de x. Supposons donc qu'il existe $p(s), q(s) \in \mathbb{Q}[s]$ tels que

$$\frac{p^3}{q^3} - s\frac{p}{q} + 2 = 0.$$

On obtient donc

$$p\left[p^2 - sq^2\right] = -2q^3 \quad \text{dans } \mathbb{Q}[s].$$

Distinguons deux cas :

1. p est un polynôme constant, qu'on peut sans perte de généralité prendre égal à 1. Dans ce cas $1 - sq^2 = -2q^3$. Le terme constant de $1 - sq^2$ vaut 1, tandis que celui de $-2q^3$ vaut $-2b^3$ où b est le coefficient constant de q. Donc $b \in \mathbb{Q}$ est une racine cubique de $-1/2$, ce qui est impossible. Donc p ne peut être constant.

2. p n'est pas constant. Puisque p divise le membre de gauche, il doit aussi diviser $-2q^3$, et donc q^3. En particulier p et q ne sont pas premiers entre eux. Or on peut sans perte de généralité les supposer premiers entre eux, on a donc une contradiction.

On obtient ainsi que $t^3 - st + 2$ est irréductible dans $\mathbb{Q}(s)$, ce qui conclut.

Voici une autre méthode pour montrer que $t^3 - st + 2 \in \mathbb{Q}(s)[t]$ est irréductible. Par le lemme de Gauss III, il suffit de montrer que ce polynôme est irréductible dans $\mathbb{Q}[s][t]$. Par la Proposition 3.9.1, il suffit de montrer que la réduction modulo s, à savoir $t^3 + 2 \in \mathbb{Q}[t]$, est irréducible. Par Gauss III encore, il suffit de montrer que $t^3+2 \in \mathbb{Z}[t]$ est irréductible, et cela se vérifie en appliquant le critère d'Eisenstein.

Exercice 4.
Note that the complex roots of $x^2 - 2$ are of the form $e^{\frac{2\pi ik}{n}}\sqrt{2}$ for $0 \leq k < n$. Moreover, note that $x^{2n} - 3x^n + 2$ can be factorized as $x^{2n} - 3x^n + 2 = (x^n - 2)(x^n - 1)$. One can conclude for Lemma 4.3.3 point (1) that the splitting fields are the same and they are given by $\mathbb{Q}(\xi, \sqrt[n]{2})$.

Exercice 5. 1. : These two polynomials are $x^3 + x + 1$ and $x^3 + x^2 + 1$, because we know that a degree 3 polynomial is irreducible if and only if it does not have a root. If we plug in 0, this means that we have to have a constant term, and if we plug in 1, this means that there has to be an odd number of terms. These two conditions together leave only the above two polynomials.

2. In both cases if α denotes the class of x in the quotient, then α^2 and α^4 are also roots of f.* This follows from $f(\alpha^2) = f(\alpha)^2 = 0$ and $f(\alpha^4) = f(\alpha)^4 = 0$. Note that they are indeed diffferent elements because they are represented by the classes of the polynominals x, x^2 and $x^2 + x$ and $x^3 + x$ respectively in the cases $f = x^3 + x + 1$ and $f = x^3 + x^2 + 1$.

   Remarque. C'est un fait général qui suit du fait que tous les corps finis sont des corps de décomposition que si $f(x) \in \mathbb{F}_q[x]$ est irréductible, alors il scinde sur $\mathbb{F}_q[x]/f(x)$ et les racines dans le quotient sont données par les classes x^{q^i} pour $i = 0, \deg(f) - 1$.

*This is also well understood using Galois theory.

3. Note that f and g are irreducible and that K is a field such that $L = \mathbb{F}_2[x]/f \cong \mathbb{F}_2(\alpha)$, where α is a roots of f. Since L is a extension of degree 3 of $K = \mathbb{F}_2[x]$, it is a finite field. Then by theorem 4.4.17, L is a splitting field of $x^8 - x$ over K. To see that it is also the splitting field of g, we know from the previous point that K contains all the roots of g and is an extension of degree 3. Using this one can conclude that K satisfies the definition of being the splitting field of g.

Exercice 6. 1. Use the following isomorphisms to define $\eta : K(\alpha) \to K'(\alpha')$

$$K(\alpha) \cong K[x]/(m_{\alpha,K}) \cong K'[x]/(\xi(m_{\alpha,K})) \cong K'[x]/(m_{\alpha',K'}) \cong K'(\alpha')$$

This shows that $L \cong L'$, and moreover by the universal property of polynomial rings and of fraction fields we have that η is the unique extension of ϕ such that $\eta(\alpha) = \alpha'$.

2. Use point (1) with the automorphism $K(x) \to K(x)$ given by $x \mapsto x + 1$. This isomorphism is induced by the universal property of polynomial rings and of fraction fields, and also that it is an isomorphism because it has an inverse given by $x \mapsto x - 1$

3. Use point (1) with the automorphism $K(x, y) \to K(x, y)$ given by $x \mapsto x$ and $y \mapsto x + y$, here the inverse is $x \mapsto x$ and $y \mapsto y - x$.

Exercice 1.
We note that $\mathbb{F}_{27}^\times \cong \mathbb{Z}/26\mathbb{Z}$, see Theorem 4.4.17 (7). Let $\alpha \in \mathbb{F}_{27}^\times$. Then $\mathrm{ord}(\alpha) \in \{1, 2, 13, 26\}$. As $\alpha \neq 1, -1$, it follows that $\mathrm{ord}(\alpha) \in \{13, 26\}$. If $\mathrm{ord}(\alpha) = 13$, then $(-\alpha)^{13} = -1$ and so $\mathrm{ord}(-\alpha) = 26$.

Exercice 2. 1. Par le Corollaire 4.4.22, $\mathbb{F}_{p^r}$ contient un et un seul sous-corps isomorphe à $\mathbb{F}_{p^n}$ pour n divisant r. Si $\mathbb{F}_{p^s}$ est l'un d'eux, alors les corps intermédiaires de l'extension $\mathbb{F}_{p^s} \subset \mathbb{F}_{p^r}$ sont les $\mathbb{F}_{p^n}$ où s divise n et n divise r.

2. Les sous-corps de $\mathbb{F}_{16}$, en vertu du premier point, sont $\mathbb{F}_2$ et $\mathbb{F}_4$, et ils forment une chaîne. Donc $\mathbb{F}_2(a) = \mathbb{F}_{16}$ si et seulement si $a \notin \mathbb{F}_4$. Par le Théorème 4.2.17 on a

$$\mathbb{F}_{16}^\times \cong \mathbb{Z}/15\mathbb{Z}, \quad \mathbb{F}_4^\times \cong \mathbb{Z}/3\mathbb{Z}$$

et $\mathbb{F}_4^\times \subset \mathbb{F}_{16}^\times$ est un sous-groupe. Un élément $0 \neq a \in \mathbb{F}_{16}$ vérifie $\mathbb{F}_2(a) = \mathbb{F}_{16}$ si et seulement si son image dans $\mathbb{F}_{16}^\times$ n'est pas contenue dans ce sous-groupe. D'un autre côté, il y a $\varphi(15) = 8$ éléments qui génèrent $\mathbb{F}_{16}^\times$, où φ est la fonction de comptage d'Euler. Remarquons aussi qu'un élément contenu dans le sous-groupe $\mathbb{F}_4^\times$ ne saurait générer le groupe $\mathbb{F}_{16}^\times$. Il y a ainsi

$$|\mathbb{F}_{16}^\times| - |\mathbb{F}_4^\times| - \varphi(15) = 15 - 3 - 8 = 4$$

éléments $0 \neq a \in \mathbb{F}_{16}$ tels que $\mathbb{F}_2(a) = \mathbb{F}_{16}$ et $\langle a \rangle \neq \mathbb{F}_{16}^\times$.

3. L'argument est semblable à celui du point précédent. Les sous-corps de $\mathbb{F}_{p^4}$ sont $\mathbb{F}_p \subset \mathbb{F}_{p^2}$, et on a $\mathbb{F}_p(a) = \mathbb{F}_{p^4}$ si et seulement si $a \notin \mathbb{F}_{p^2}$. Par le Théorème 4.2.17 on a

$$\mathbb{F}_{p^4}^\times \cong \mathbb{Z}/(p^4-1)\mathbb{Z}, \quad \mathbb{F}_{p^2} \cong \mathbb{Z}/(p^2-1)\mathbb{Z}.$$

Notons $E := \{0 \neq a \in \mathbb{F}_{16} \mid \langle a \rangle = \mathbb{F}_{16}^\times\}$. Alors $|E| = \varphi(p^4-1)$. Remarquons aussi que E et $\mathbb{F}_{p^2}^\times$ sont des sous-ensembles disjoints de $\mathbb{F}_{p^4}^\times$. Ainsi

$$\begin{aligned} |\{0 \neq a \in \mathbb{F}_{p^4} \mid \mathbb{F}_p(a) = \mathbb{F}_{p^4} \text{ et } \langle a \rangle \neq \mathbb{F}_{p^4}^\times\}| &= |\mathbb{Z}/(p^4-1)\mathbb{Z} \setminus (E \sqcup \mathbb{F}_{p^2}^\times)| \\ &= p^4 - 1 - (p^2-1) - \varphi(p^4-1) \\ &= p^4 - p^2 - \varphi(p^4-1). \end{aligned}$$

Exercice 3. 1. Notons $q := \mathrm{pgdc}(f, x^{p^d} - x)$. Comme f est irréductible, on a $q = 1$ ou $q = f$. On va montrer que $q = 1$ n'est pas possible. Puisque f est irréductible de degré d, le quotient $\mathbb{F}_p[t]/(f(t))$ est un corps de degré d sur $\mathbb{F}_p$. En particulier il contient p^d éléments. Par le Théorème 3.4.17, on obtient un isomorphisme

$$\phi \colon \mathbb{F}_p[t]/(f(t)) \cong \mathbb{F}_{p^d}$$

qui se restreint à l'égalité sur $\mathbb{F}_p$ (puisqu'il envoie 1 vers 1). Ainsi l'isomorphisme

$$\Phi \colon \big(\mathbb{F}_p[t]/(f)\big)[x] \cong \mathbb{F}_{p^d}[x]$$

induit par ϕ fait commuter le diagramme

$$\begin{array}{ccc} \big(\mathbb{F}_p[t]/(f)\big)[x] & \xrightarrow{\quad\Phi\quad} & \mathbb{F}_{p^d}[x] \\ & \nwarrow \quad \nearrow & \\ & \mathbb{F}_p[x] & \end{array}$$

On en conclut que l'extension $\mathbb{F}_p \subset \mathbb{F}_{p^d}$ contient une racine de $\Phi(f) = f \in \mathbb{F}_p[x]$. Notons $\alpha \in \mathbb{F}_{p^d}$ cette racine. Par le Théorème 4.2.17 à nouveau, α est aussi une racine de $x^{p^d} - x \in \mathbb{F}_p[x]$. Donc $x - \alpha$ divise à la fois f et $x^{p^d} - x$ dans $\mathbb{F}_{p^d}[x]$. Cela implique que $(f, x^{p^d} - x) \subseteq (x - \alpha)$ dans l'anneau $\mathbb{F}_{p^d}[x]$.

Si $q = 1$, alors par Bézout il existerait $a, b \in \mathbb{F}_p[x]$ tels que $af + b(x^{p^d} - x) = 1$. Cette relation serait encore vraie dans le plus gros anneau $\mathbb{F}_{p^d}[x]$. Or on vient d'établir que $(f, x^{p^d} - x) \subseteq (x - \alpha)$ dans $\mathbb{F}_{p^d}[x]$, c'est donc une contradiction. Ainsi $q = f$, d'où f divise $x^{p^d} - x$.

2. Le Théorème 4.2.17 nous indique que $x^{p^d} - x$ se scinde sur $\mathbb{F}_{p^d}$. Or f divise $x^{p^d} - x$, donc (par unicité de la décomposition en facteurs premiers) le polynôme f se scinde sur $\mathbb{F}_{p^d}$.

3. Puisque f se scinde sur $\mathbb{F}_{p^d}$ et divise $x^{p^d} - x$ dans $\mathbb{F}_{p^d}[x]$, il suffit de montrer que $x^{p^d} - x$ n'a pas de racines multiples dans $\mathbb{F}_{p^d}$. Or le Théorème 4.2.17 implique que

$$x^{p^d} - x \quad \text{est divisible par} \prod_{\alpha \in \mathbb{F}_{p^d}} (x - \alpha) \quad \text{dans } \mathbb{F}_{p^d}[x].$$

En comparant les degrés et les coefficients dominants, on voit qu'il y a en fait égalité entre ces deux polynômes. Donc $x^{p^d} - x$ n'a pas de racine multiple.

4. Par le second point, f et g se scindent sur $\mathbb{F}_{p^d}$. S'ils ont une racine β en commun dans $\mathbb{F}_{p^d}$, alors l'idéal $(f, g) \subseteq (x - \beta)$ n'est pas égal à $\mathbb{F}_{p^d}[x]$. Mais si $\text{pgdc}(f, g) = 1$ dans $\mathbb{F}_p[x]$, alors par Bézout on obtient comme dans le premier point que $(f, g) = \mathbb{F}_{p^d}[x]$. Donc $\text{pgdc}(f, g) \neq 1$. Comme f et g sont irréductibles, on en déduit que $f = g$ modulo une unité (c'est-à-dire modulo multiplication par un scalaire de $\mathbb{F}_p^\times$).

5. Le premier point montre que $x^{p^d} - x$ est divisible par tous les polynômes irréductibles de degré d. La preuve du Corollaire 4.4.22 montre que $x^{p^s} - x$ divise $x^{p^d} - x$ pour tous les s divisant d. Donc

$$\prod_{\substack{h \text{ unitaire irréd.} \\ \text{dans } \mathbb{F}_p[x] \\ \deg h \text{ divise } d}} h \quad \text{divise} \quad x^{p^d} - x.$$

Il reste à montrer qu'il n'existe pas d'autre polynôme irréductible divisant $x^{p^d} - x$. Soit g un polynôme irréductible dont le degré ne divise pas d. Si g divise $x^{p^d} - x$, alors g se scinde sur $\mathbb{F}_{p^d}$, et donc $\mathbb{F}_p[x]/(g)$ s'identifie à un sous-corps de $\mathbb{F}_{p^d}$, c'est-à-dire à un $\mathbb{F}_{p^s}$ où s divise d. Mais dans ce cas

$$\deg g = [\mathbb{F}_p[x]/(g) : \mathbb{F}_p] = [\mathbb{F}_{p^s} : \mathbb{F}_p] = s$$

divise d, ce qui est une contradiction. On a donc l'égalité désirée.

Exercice 4.
Cette solution est adaptée de l'article *Counting Irreducible Polynomials over Finite Fields Using the Inclusion-Exclusion Principle* de S.K.Chebolu et J. Minác, dans *Math. Mag.* **84** (2011) 369-371.

1. On a vu dans l'Exercice 3 que tout polynôme f irréductible de degré d se scinde sur $\mathbb{F}_{p^d}$. On a vu dans le même exercice que f n'a pas de racines doubles, et que deux polynômes unitaires irréductibles de même degré n'ont pas de racines en commun. Si $f_1, \ldots, f_{N_d}$ sont les polynômes unitaires irréductibles de degré d et $R_{f_i} \subset \mathbb{F}_{p^d}$ les ensembles de racines, on a donc montré que
$$|R_{f_i}| = d \quad \text{et} \quad R_{f_i} \cap R_{f_j} = \emptyset \text{ si } i \neq j.$$
Ainsi on obtient
$$dN_d = |R_{f_1} \sqcup \cdots \sqcup R_{f_{N_d}}|.$$
Il reste à déterminer quels éléments de $\mathbb{F}_{p^d}$ sont des racines de polynômes irréductibles de degré d. Remarquons que si $a \in \mathbb{F}_{p^d}$ est une racine de f_i, alors
$$\mathbb{F}_p(a) \cong \mathbb{F}_p[t]/(f_i(t))$$
et en prenant les degrés sur $\mathbb{F}_p$ on obtient $[\mathbb{F}_p(a) : \mathbb{F}_p] = d$. Donc $\mathbb{F}_p(a) = \mathbb{F}_{p^d}$. Ainsi si a est une racine de f_i, il n'appartient à aucun sous-corps strict $L \subsetneq \mathbb{F}_{p^d}$. Inversément, supposons que $a \in \mathbb{F}_{p^d}$ n'appartienne à aucun sous-corps strict. Par le Théorème 4.2.17, a est racine de $x^{p^d} - x \in \mathbb{F}_p[x]$, donc de l'un de ses facteurs irréductibles de degré e. Alors $[\mathbb{F}_p(a) : \mathbb{F}] = e$, et si $e < d$ on obtient $\mathbb{F}_p(a) \subsetneq \mathbb{F}_{p^d}$, ce qui est une contradiction avec le choix de de a. En définitive nous avons montré que
$$R_{f_1} \sqcup \cdots \sqcup R_{f_{N_d}} = \mathbb{F}_{p^d} \setminus \bigcup_{L \subsetneq \mathbb{F}_{p^d}} L$$
où L parcourt les sous-corps stricts de $\mathbb{F}_{p^d}$.

2. Le problème pour tirer une formule générale du point précédent est que les sous-corps L ne sont pas tous inclus les uns dans les autres, et que leurs intersections sont non-triviales. Pour les petites valeurs de d, il est cependant facile passer en revue les sous-corps et leurs intersections. Nous utilisons sans plus y faire référence le Corollaire 4.4.22.

   (a) $d = 2$. Le seul sous-corps strict de $\mathbb{F}_{p^2}$ est $\mathbb{F}_p$. Donc
   $$N_2 = \frac{p^2 - p}{2}.$$

   (b) $d = 3$. Le seul sous-corps strict de $\mathbb{F}_{p^3}$ est $\mathbb{F}_p$. Donc
   $$N_3 = \frac{p^3 - p}{3}.$$

   (c) $d = 4$. Les sous-corps stricts de $\mathbb{F}_{p^4}$ sont $\mathbb{F}_p \subset \mathbb{F}_{p^2}$. Donc
   $$N_4 = \frac{p^4 - p^2}{4}.$$

   (d) $d = 5$. Le seul sous-corps strict de $\mathbb{F}_{p^5}$ est $\mathbb{F}_p$. Donc
   $$N_5 = \frac{p^5 - p}{5}.$$

   (e) $d = 6$. Le premier cas non-trivial. Les sous-corps stricts sont
   $$\mathbb{F}_{p^2} \supset \mathbb{F}_p \subset \mathbb{F}_{p^3}.$$
   Ainsi
   $$|\mathbb{F}_{p^6} \setminus (\mathbb{F}_{p^2} \cup \mathbb{F}_{p^3})| = |\mathbb{F}_{p^6}| - |\mathbb{F}_{p^2}| - |\mathbb{F}_{p^3}| + |\mathbb{F}_{p^2} \cap \mathbb{F}_{p^3}|.$$

L'intersection $\mathbb{F}_{p^2} \cap \mathbb{F}_{p^3}$ est un corps fini de caractéristique p, donc un corps de la forme $\mathbb{F}_{p^s}$ où s divise à la fois 2 et 3. Donc $s = 1$ et le cardinal de l'intersection vaut p. Il s'ensuit que

$$N_6 = \frac{p^6 - p^3 - p^2 + p}{6}.$$

3. Observez que le Corollaire 4.4.22 permet d'écrire explicitement le réseau de sous-corps de n'importe quel corps fini. Puisque $\mathbb{F}_{p^{d/n}} \cap \mathbb{F}_{p^{d/m}}$ est un sous-corps à la fois de $\mathbb{F}_{p^{d/n}}$, de $\mathbb{F}_{p^{d/m}}$ et de $\mathbb{F}_{p^d}$, on utilise le Corollaire 4.4.22 pour indentifier cette intersection. Elle est donnée par $\mathbb{F}_{p^s}$, où s est le plus grand entier qui divise à la fois d/n et d/m. Puisque n et m sont premiers entre eux, en considérant la décomposition de d en facteurs premiers on voit que $s = d/nm$.

4. Passons au cas général. Dans la formule établie au premier point, on peut évidemment prendre l'union sur l'ensemble des sous-corps stricts L qui sont maximaux. Par le Corollaire 4.4.22, ces sous-corps sont donnés par

$$F_j := \mathbb{F}_{p^{d/s_j}} \quad \text{avec } d = \prod_{j=1}^{n} s_j^{i_j} \text{ la décomposition en nombres premiers.}$$

Ecrivons $F_{j_1 \dots j_r} := F_{i_1} \cap \cdots \cap F_{j_r}$. En utilisant le point précédent par induction sur t, on voit que $|F_{j_1 \dots j_t}| = p^{d/s_{j_1} \cdots s_{j_t}}$. La formule d'inclusion-exclusion nous donne alors

$$\begin{aligned} dN_d &= |\mathbb{F}_{p^d}| - \left| \bigcup_{j=1}^{n} F_j \right| \\ &= p^d - \sum_{t=1}^{n} (-1)^{t+1} \sum_{j_1 < \cdots < j_t} |F_{j_1 \dots j_t}| \\ &= p^d - \sum_{t=1}^{n} (-1)^{t+1} \sum_{j_1 < \cdots < j_t} p^{d/s_{j_1} \cdots s_{j_t}} \\ &= \sum_{t=0}^{n} (-1)^{t} \sum_{j_1 < \cdots < j_t} p^{d/s_{j_1} \cdots s_{j_t}} \end{aligned}$$

où on pose $p^{d/s_{j_1} \cdots s_{j_t}} = p^d$ pour $t = 0$. Considérons maintenant un entier r divisant d. On a

$$r = \prod_{j=1}^{n} s_j^{k_j} \quad \text{avec } 0 \le k_j \le i_j, \quad \text{donc} \quad \frac{d}{r} = \prod_{j=1}^{n} s_j^{i_j - k_j}.$$

Par la définition de la fonction de Möbius, on obtient

$$\mu\left(\frac{d}{r}\right) = \begin{cases} 0 & \text{si } k_j \le i_j - 2 \text{ pour au moins un } j, \\ 1 & \text{si } \forall j: \ k_j \ge i_j - 1 \text{ avec inégalité pour un nombre pair de } j, \\ -1 & \text{si } \forall j: \ k_j \ge i_j - 1 \text{ avec inégalité pour un nombre impair de } j. \end{cases}$$

Il s'ensuit que

$$\sum_{t=0}^{n} (-1)^t \sum_{j_1 < \cdots < j_t} p^{d/s_{j_1} \cdots s_{j_t}} = \sum_{r \mid d} \mu\left(\frac{d}{r}\right) p^r$$

ce qui conclut l'exercice.

Exercice 5. 1. By corollary 4.4.22 we know that for every j K_{j+1} contains a subfield isomorphic to K_j. We can then considered the induced inclusion homomorphism $\iota_j : K_j \to K_{j+1}$ for every $j \ge 1$.

2. Recall that if $K_0 \overset{\iota_0}{\hookrightarrow} K_1 \overset{\iota_1}{\hookrightarrow} K_2 \overset{\iota_2}{\hookrightarrow} \dots$ is an infinite sequence of fields with injectiv homomorphisms between each K_j and K_{j+1}. Then the direct limit is given by

$$\varinjlim_i K_i = \bigsqcup_{i\in\mathbb{N}} K_i \Big/ \begin{array}{l} - \ x \equiv \iota_{s-1} \circ \dots \circ \iota_r(x) \text{ et } \iota_{s-1} \circ \dots \circ \iota_r(x) \equiv x \text{ pour chaque entier } s > r, \text{ et } x \in K_r \\ - \ x \equiv x \text{ pour chaque } x \in K_r \end{array}$$

is a field with sum given by $[x] + [y]$ and product given by $[x] \cdot [y]$ for $x \in K_r$ and $y \in K_s$ are defined as follows: if $s > r$, then $[x] = [\iota_{s-1} \circ \dots \circ \iota_r(x)]$ which means that we can suppose $s = r$, and thus we define

(a) $[x] + [y] = [x + y]$

(b) $[x] \cdot [y] = [x \cdot y]$

It is clear that the unit and zero element are given by the inclusion of each the zero and unit element in each field. And since each K_i is a field the sum and multiplication defined as above endow the direct limit with a ring structure. It is also not difficult to see that each element $[x] \in \bigsqcup_{i\in\mathbb{N}} K_i$ has an inverse, since $x \in K_n$ for some $n \in \mathbb{N}$

Moreover the inclusion $K_0 \hookrightarrow \bigsqcup_{i\in\mathbb{N}} K_i$ gives us an embedding $K_0 \hookrightarrow \varinjlim_i K_i$.

3. Note that $\mathbb{F}_p \subset K$. Moreover each extension $K_j \subset K_{j+1}$ is a finite extension therefore it is an algebraic extension. Thus we have that each K_j is algebraic over $\mathbb{F}_p$. We then have that K is algebraic over $\mathbb{F}_p$ because each of its element lives in one of the K_j.

4. Let g be a polynomial in $K[t]$. Since g has a finite sum of coefficients, then there exists $n \in \mathbb{N}$ such that $g \in K_n[t]$. Let α be a root of g, then $K_n \subset K_n(\alpha)$ is a finite extension of degree r, for some $r \in \mathbb{N}$. Therefore $K_n(\alpha)$ is a field with p^{rn} elements. Hence $K_n(\alpha)$ is also a finite field containing F_p. Then we have that $K_n(\alpha) = K_{rn}$. So the root α is also an element of K since $\alpha \in K_{rn} \subset K$. Thus K is the algebraic closure of $\mathbb{F}_p$.

Exercice 1. (a) As $\alpha \notin K^p$ it follows that for all $\beta \in K$ we have $\beta^p \neq \alpha$ and thus $x^p - \alpha \in K[x]$ does not admit roots in K. Let F be a decomposition field of $x^p - \alpha$ over K and let $\beta \in F$ be a root of this polynomial. We have that:

$$x^p - \alpha = x^p - \beta^p = (x - \beta)^p \text{ in } F[x].$$

Let $m_{\beta,K}(x) \in K[x]$ denote the minimal polynomial of β over K. As β is a root of $x^p - \alpha$, it follows that $m_{\beta,K}(x) | x^p - \alpha = (x - \beta)^p$. Therefore there exists some i, $1 \leq i \leq p$, such that $m_{\beta,K}(x) = (x - \beta)^i$. Now, as $m_{\beta,K}(x) \in K[x]$ we have that:

$$(x - \beta)^i = \sum_{j=0}^{i} (-1)^j \binom{i}{j} x^{i-j} \beta^j = x^i - i\beta x^{i-1} + \cdots + (-1)^i \beta^i \in K[x].$$

It follows that $-i\beta = 0$ and so $i = p$. Therefore $m_{\beta,K}(x) = (x-\beta)^p = x^p - \alpha$ and we conclude that $x^p - \alpha \in K[x]$ is irreducible.

(b) To show that L is a field, we will show that the polynomial $y^2 - x(x-1)(x+1) \in (\mathbb{F}_p(x))[y]$ is irreducible. As $y^2 - x(x-1)(x+1)$ is a unitary polynomial, it is primitive and so, by Gauss III, it is irreducible in $(\mathbb{F}_p(x))[y]$ if and only if it is irreducible in $(\mathbb{F}_p[x])[y]$. Now, $x \in \mathbb{F}_p[x]$ is irreducible and we use Eisenstein with "$p = x$" (here p denotes the irreducible in Eisenstein criterion) to deduce that $y^2 - x(x-1)(x+1)$ is irreducible in $(\mathbb{F}_p[x])[y]$.

(c) By Proposition 4.5.7, as $\text{char}(L) = p$, we have that L is perfect if and only if $L^p = L$. We will show that $x \notin L^p$.

Assume by contradiction that $x \in L^p$. Then, there exists $f \in L$ such that $x = f^p$. It follows that $f \in L$ is a root of the polynomial $t^p - x \in \mathbb{F}_p(x)[t]$. As $x \in \mathbb{F}_p(x)$ is not a p^{th} power, see Exercice 3, it follows that the polynomial $t^p - x$ is irreducible in $(\mathbb{F}_p(x))[t]$, see item (a). This shows that $m_{f,\mathbb{F}_p(x)}(t) \sim t^p - x \in (\mathbb{F}_p(x))[t]$.

Consider the chain of extensions:

$$\mathbb{F}_p(x) \subseteq (\mathbb{F}_p(x))(f) \subseteq L$$

and we have $[(\mathbb{F}_p(x))(f) : \mathbb{F}_p(x)] | [L : \mathbb{F}_p(x)]$. But $[L : \mathbb{F}_p(x)] = 2$ and $[(\mathbb{F}_p(x))(f) : \mathbb{F}_p(x)] = p$, where $p \neq 2$. We have arrived at a contradiction.

(d) We have that $L = (\mathbb{F}_2(x))[y]/(y^2 + x(x+1)^2)$. Note that the polynomial $y^2 + x(x+1)^2 \in (\mathbb{F}_2(x))[y]$ admits $\sqrt{x}(x+1)$ as a double root and so it is irreducible in $(\mathbb{F}_2(x))[y]$. Now, by Proposition 4.2.25, it follows that $L = (\mathbb{F}_2(x))(\sqrt{x}(x+1)) = (\mathbb{F}_2(x))(\sqrt{x}) = \mathbb{F}_2(\sqrt{x})$. For the last equality, note that $\mathbb{F}_2(\sqrt{x}) \subseteq (\mathbb{F}_2(x))(\sqrt{x})$ and, as $\mathbb{F}_2(x) \subseteq \mathbb{F}_2(\sqrt{x})$, we have $(\mathbb{F}_2(x))(\sqrt{x}) \subseteq (\mathbb{F}_2(\sqrt{x}))(\sqrt{x}) = \mathbb{F}_2(\sqrt{x})$.

As $\text{char}(L) = 2$, it follows that L is perfect if and only if $L^2 = L$, see Proposition 4.5.7. But

$$\begin{aligned} L^2 &= \{f(\sqrt{x})^2 |\ f(\sqrt{x}) \in L\} = \left\{ \left(\frac{f_1(\sqrt{x})}{f_2(\sqrt{x})} \right)^2 |\ f_1(\sqrt{x}), f_2(\sqrt{x}) \in \mathbb{F}_2[\sqrt{x}],\ f_2(\sqrt{x}) \neq 0 \right\} \\ &= \left\{ \frac{f_1(x)}{f_2(x)} |\ f_1(x), f_2(x) \in \mathbb{F}_2[x],\ f_2(x) \neq 0 \right\} = \mathbb{F}_2(x) \end{aligned}$$

and clearly $\sqrt{x} \notin L^2$.

Exercice 2(a)(i) Let $\alpha \in L\backslash K$. As $\alpha^2 \in K$, it follows that α is a root of the polynomial $x^2+\alpha^2 \in K[x]$ and thus $[K(\alpha):K] \leq 2$. On the other hand, we have that $[K(\alpha):K] \geq 2$, as $\alpha \notin K$, and we conclude that $[K(\alpha):K]=2$ and $K(\alpha)=L$.

(ii) The polynomial $x^2+\alpha^2 \in K[x]$, where $\alpha \in L\backslash K$, admits α as a double root, hence it is irreducible in $K[x]$. Now, as this is a unitary irreducible polynomial of degree 2 and as $\alpha \notin K$, it follows that $m_{\alpha,K}(x)=x^2+\alpha^2$ and so we conclude that $\alpha \in L\backslash K$ is inseparable.

(b)(i) Let $\alpha \in L\backslash K$ be such that $\alpha^2 \notin K$. First, we have that $[K(\alpha):K] \geq 2$ and, as $K(\alpha) \subseteq L$, it follows that $[K(\alpha):K] \leq [L:K]=2$, and so $[K(\alpha):K]=2$, hence $K(\alpha)=L$.

Secondly, as $\alpha^2 \in K(\alpha)$ and $\alpha^2 \notin K$, there exist $a,b \in K$, $a \neq 0$, such that $\alpha^2 = a\alpha + b$. Then:

$$\left(\frac{\alpha}{a}\right)^2 = \left(\frac{\alpha}{a}\right) + \frac{b}{a^2}.$$

Set $\beta = \frac{\alpha}{a} \in K(\alpha)$ and $c = \frac{b}{a^2} \in K$. We have that $K(\alpha) = K(\frac{\alpha}{a}) = K(\beta)$ and so $L = K(\beta)$. Moreover, β is a root of the unitary polynomial $x^2+x+c \in K[x]$ and, as $[K(\beta):K]=2$, we conclude that $m_{\beta,K}(x) = x^2+x+c$.

(ii) Note that a polynomial of the form x^2+x+c is always separable as the derivative is $1 \neq 0$. So, β is automatically separable. Now $\beta+1 \in K(\beta)$ is a root of $m_{\beta,K}(x)$, as $(\beta+1)^2+(\beta+1)+c = \beta^2+\beta+c = 0$, and we conclude that $\tau : K(\beta) \to K(\beta)$ given by $\tau(\beta) = \beta+1$ is an automorphism of $K(\beta)$. Then, by Proposition 4.6.3.4 we have that $|\operatorname{Gal}(K(\beta)/K)| = 2$.

(iii) Note that $K(\beta)^{\langle\tau\rangle} = K$ by theorem 4.6.13. If $\gamma \in L \setminus K$ then $\tau(\gamma) \neq \gamma$ and by proposition 4.6.3.(3), we get that the minimal polynomial of γ is $(t-\gamma)(t-\tau(\gamma))$. Therefore $K \subset L$ is separable.

Exercice 3.
We use the same techniques as in Example 4.6.5, and denote $G = \operatorname{Gal}(K/\mathbb{Q}) = \operatorname{Aut}_{\mathbb{Q}}(K)$.

- Let $K = \mathbb{Q}(i)$. The irreducible polynomial $x^2+1 \in \mathbb{Q}[x]$ has two distinct roots in $\mathbb{Q}(i)$, and they are i and $-i$. From Prop 4.6.3(1), it follows that every element in G sends i to i or to $-i$. By Prop 4.6.3(2), there is at most one element in G for each possibility. By Prop 4.6.3(4), it holds that $|\operatorname{Gal}(K/\mathbb{Q})| = [\mathbb{Q}(i):\mathbb{Q}] = 2$, hence $\operatorname{Gal}(K/\mathbb{Q}) = \{\mathrm{id}_{\mathbb{Q}(i)}, \sigma\} \cong \mathbb{Z}/2\mathbb{Z}$, where (the identity sends i to i, and) σ sends i to $-i$. As σ is $\mathbb{Q}$-linear, we have that $\sigma(a+ib) = a-ib$, the conjugation.

- Let $K = \mathbb{Q}(\sqrt{7})$. Using the same steps as above, considering the irreducible polynomial $x^2-7 \in \mathbb{Q}[x]$, we get that $\operatorname{Gal}(K/\mathbb{Q}) = \{\mathrm{id}_{\mathbb{Q}(\sqrt{7})}, \sigma\} \cong \mathbb{Z}/2\mathbb{Z}$, where (the identity sends $\sqrt{7}$ to $\sqrt{7}$, and) σ sends $\sqrt{7}$ to $-\sqrt{7}$. As σ is $\mathbb{Q}$-linear, we have that $\sigma(a+\sqrt{7}b) = a-\sqrt{7}b$.

- Let $K = \mathbb{Q}(\sqrt[3]{2})$. The irreducible polynomial $x^3-2 \in \mathbb{Q}[x]$ has only one root in $\mathbb{Q}(\sqrt[3]{2})$. As by Prop 4.6.3(1), every root of this polynomial gets sent to a root of the same polynomial by an element in G, and for each such possibility there is at most one element in G by Prop 4.6.3(2), we conclude that $G = \{\mathrm{id}_{\mathbb{Q}(\sqrt[3]{2})}\}$ is trivial.

- Let $K = \mathbb{Q}(\omega^2)$, where $\omega = e^{2i\pi/3}$. The irreducible polynomial $x^2+x+1 \in \mathbb{Q}[x]$ has two roots in $\mathbb{Q}(\omega)$, which are ω and ω^2. As for the first and second example, it follows that G is cyclic of order two, consisting of the identity and σ, which sends ω to ω^2. We have in fact $K = \mathbb{Q}(i\sqrt{3})$, and one can argue as in the first two points.

Exercice 4.
We have the following extension tower:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{1+\sqrt{2}}).$$

The extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ is Galois, as $\mathbb{Q}$ is a perfect field and $\mathbb{Q}(\sqrt{2})$ is the decomposition field of the polynomial $x^2 - 2 \in \mathbb{Q}[x]$, see Theorem 4.6.15. Similarly, the extension $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{1+\sqrt{2}})$ is Galois, as $\mathbb{Q}(\sqrt{2})$ is perfect and $\mathbb{Q}(\sqrt{1+\sqrt{2}})$ is the decomposition field of the polynomial $x^2 - 1 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})[x]$.

We now consider the extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{1+\sqrt{2}})$. We note that this extension is of degree 4. We also note by devellopping

$$(x^2 - (1+\sqrt{2}))(x^2 - (1-\sqrt{2}))$$

that $\sqrt{1+\sqrt{2}}$ is a root of the polynomial $x^4 - 2x^2 - 1 \in \mathbb{Q}[x]$, hence $m_{\sqrt{1+\sqrt{2}},\mathbb{Q}}(x) = x^4 - 2x^2 - 1$ by the degree because $[\mathbb{Q}(\sqrt{1+\sqrt{2}}) : \mathbb{Q}] = 4$. Moreover, the other roots of $x^4 - 2x^2 - 1$ are $-\sqrt{1+\sqrt{2}}$ and $\pm\sqrt{1-\sqrt{2}}$. Now, we remark that $\mathbb{Q}(\sqrt{1+\sqrt{2}}) \subseteq \mathbb{R}$, therefore $\pm\sqrt{1-\sqrt{2}} \notin \mathbb{Q}(\sqrt{1+\sqrt{2}})$. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{1+\sqrt{2}})/\mathbb{Q})$. Then $\sigma(\sqrt{1}+\sqrt{2}) \in \mathbb{Q}(\sqrt{1+\sqrt{2}})$ is a root of $m_{\sqrt{1+\sqrt{2}},\mathbb{Q}}(x)$ and thus $\sigma(\sqrt{1+\sqrt{2}}) = \pm\sqrt{1+\sqrt{2}}$, see Proposition 4.6.3 (c). It follows that $|\mathrm{Gal}(\mathbb{Q}(\sqrt{1+\sqrt{2}})/\mathbb{Q})| = 2$ and we conclude, using Corollary 4.6.13, that the extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{1+\sqrt{2}})$ is not Galois.

Exercice 5.
In the following solutions, we use the same technique to find the minimal polynomials as in Example 4.6.11. With Proposition 4.6.10, it holds that for an element $z \in \mathbb{Q}(\alpha, \beta)$, the minimal polynomial is $m_{z,\mathbb{Q}} = \prod_{z'}(x - z')$, where z' is a Galois conjugate of z.

1. As in Example 4.6.4 (3), we see that $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The elements in G are the identity, σ, with $\sigma(\sqrt{3}) = \sqrt{3}$ and $\sigma(\sqrt{7}) = -\sqrt{7}$, τ with $\tau(\sqrt{3}) = -\sqrt{3}$ and $\tau(\sqrt{7}) = \sqrt{7}$, and $\tau\sigma$, with $\tau\sigma(\sqrt{3}) = -\sqrt{3}$ and $\tau\sigma(\sqrt{7}) = -\sqrt{7}$.

   The elements $\{1, \sqrt{3}, \sqrt{7}, \sqrt{3}\sqrt{7}\}$ form a basis of $\mathbb{Q}(\sqrt{3}, \sqrt{7})$ over $\mathbb{Q}$. Now let $z \in \mathbb{Q}(\alpha, \beta)$, with $z = a + b\sqrt{3} + c\sqrt{7} + d\sqrt{3}\sqrt{7}$. The conjugates of z are

   $$z, \quad a + b\sqrt{3} - c\sqrt{7} - d\sqrt{3}\sqrt{7}, \quad a - b\sqrt{3} + c\sqrt{7} - d\sqrt{3}\sqrt{7}, \quad a - b\sqrt{3} - c\sqrt{7} + d\sqrt{3}\sqrt{7}.$$

   As noted above, the minimal polynomial is

   $$m_{z,\mathbb{Q}} = (x-z)(x-(a+b\sqrt{3}-c\sqrt{7}-d\sqrt{3}\sqrt{7}))(x-(a-b\sqrt{3}+c\sqrt{7}-d\sqrt{3}\sqrt{7}))(x-(a-b\sqrt{3}-c\sqrt{7}+d\sqrt{3}\sqrt{7})),$$

   if all factors are different. Hence the minimal polynomials of the elements $\sqrt{3}, \sqrt{3}+\sqrt{7}, \sqrt{3}\cdot\sqrt{7}, \sqrt{3}^{-1}$ are

   $$\begin{aligned}
   m_{\sqrt{3},\mathbb{Q}} &= x^2 - 3 \\
   m_{\sqrt{3}+\sqrt{7},\mathbb{Q}} &= (x - \sqrt{3} - \sqrt{7})(x - \sqrt{3} + \sqrt{7})(x + \sqrt{3} - \sqrt{7})(x + \sqrt{3} + \sqrt{7}) \\
   m_{\sqrt{3}\cdot\sqrt{7},\mathbb{Q}} &= (x - \sqrt{3}\sqrt{7})(x + \sqrt{3}\sqrt{7}) \\
   m_{\sqrt{3}^{-1},\mathbb{Q}} &= x^2 - \frac{1}{3}.
   \end{aligned}$$

2. We note that since $\beta = -1 \in \mathbb{Q}$, it holds that $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha)$. α is a root of the polynomial $x^3 + 1$. The other two roots are -1, and $e^{-2i\pi/3} = \overline{\alpha}$. Since one of the roots is contained in $\mathbb{Q}$, over which every element of the Galois group acts as the identity we get by Prop 4.6.3 (1) that every element of the Galois group G either sends α to α, or to $\overline{\alpha}$. By (b), there exists at most one element for each possibility. Hence $|G| \leq 2$. There are exactly two automorphisms, one being the identity, and the other acting on α by sending α to $\overline{\alpha}$. Therefore, $G \cong \mathbb{Z}/2\mathbb{Z}$.

   Again, we calculate the minimal polynomial of an element $z = (a + b\alpha) \in \mathbb{Q}(\alpha)$ as above. Its

minimal polynomial is $m_{z,\mathbb{Q}} = (x - a - b\alpha)(x - a - b\overline{\alpha})$, if the factors are different. We get

$$\begin{aligned} m_{\alpha,\mathbb{Q}} &= (x-\alpha)(x-\overline{\alpha}) = x^2 - x + 1 \\ m_{\alpha+\beta,\mathbb{Q}} &= x^2 + x + 1 \\ m_{\alpha\cdot\beta,\mathbb{Q}} &= x^2 + x + 1 \\ m_{\alpha^{-1},\mathbb{Q}} &= x^2 - x + 1 \end{aligned}$$

3. Let $\alpha = e^{(\pi i/3)}$ and $\beta = i$. Since $\alpha = \cos(\pi/3) + i\sin(\pi/3) = \frac{1}{2} + \frac{1}{2}i\sqrt{3}$, it follows that $\alpha \in \mathbb{Q}(i\sqrt{3})$, and $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(i\sqrt{3})$. With $i\sqrt{3} = 2\alpha - 1$, it follows that $i\sqrt{3} \in \mathbb{Q}(\alpha)$, and $\mathbb{Q}(i\sqrt{3}) \subseteq \mathbb{Q}(\alpha)$. With this, it follows that $\mathbb{Q}(\alpha) = \mathbb{Q}(i\sqrt{3})$. Furthermore, $\mathbb{Q}(\alpha,\beta) = \mathbb{Q}(i\sqrt{3}, i) = \mathbb{Q}(\sqrt{3}, i)$. As in Example 4.6.4 (c), we see that $\mathrm{Gal}(\mathbb{Q}(\sqrt{3},i)/\mathbb{Q})$ contains 4 elements, the identity, σ, τ and $\sigma\tau$, where $\sigma(i) = i, \sigma(\sqrt{3}) = -\sqrt{3}, \tau(i) = -i, \tau(\sqrt{3}) = \sqrt{3}$ and $\sigma\tau(i) = -i, \sigma\tau(\sqrt{3}) = -\sqrt{3}$, and that $\mathrm{Gal}(\mathbb{Q}(\sqrt{3},i)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. On the elements α and β, those four elements act as follows:

$$\sigma(\alpha) = e^{-(i\pi/3)}, \sigma(\beta) = \beta, \quad \tau(\alpha) = e^{-(i\pi/3)}, \sigma(\beta) = -\beta, \quad \sigma\tau(\alpha) = \alpha, \sigma\tau(\beta) = -\beta.$$

As for the first example, we remark that the elements $\{1, i, \sqrt{3}, i\sqrt{3}\}$ form a basis of $\mathbb{Q}(\sqrt{3}, i)$ over $\mathbb{Q}$. Let $z \in \mathbb{Q}(\sqrt{3}, i)$ with $z = a + bi + c\sqrt{3} + d\sqrt{3}i$. Then, as stated above, the minimal polynomial of z is of the following form, if all factors are different

$$\begin{aligned} m_{z,\mathbb{Q}} &= (x-z)(x-\sigma(z))(x-\tau(z))(x-\sigma\tau(z)) \\ &= (x-z)(x-(a+bi-c\sqrt{3}-d\sqrt{3}i))(x-(a-bi+c\sqrt{3}-d\sqrt{3}i))(x-(a-bi-c\sqrt{3}+d\sqrt{3}i)). \end{aligned}$$

We note that the element α is of the form $\alpha = \frac{1}{2} + \frac{1}{2}(i\sqrt{3})$ in the basis $\{1, i, \sqrt{3}, i\sqrt{3}\}$. Then, the minimal polynomials are of the form

$$\begin{aligned} m_{\alpha,\mathbb{Q}} &= (x-(0.5+0.5i\sqrt{3}))(x-(0.5-0.5i\sqrt{3})) = (x-\alpha)(x-e^{(-i\pi/3)}) \\ m_{\alpha+\beta,\mathbb{Q}} &= (x-(0.5+i+0.5i\sqrt{3}))(x-(0.5+i-0.5\sqrt{3}i))(x-(0.5-i-0.5\sqrt{3}i))(x-(0.5-i+0.5\sqrt{3}i)) \\ m_{\alpha\cdot\beta,\mathbb{Q}} &= (x-(0.5i-0.5\sqrt{3}))(x-(0.5i+0.5\sqrt{3}))(x-(-0.5i-0.5\sqrt{3}))(x-(-0.5i+0.5\sqrt{3})) \\ m_{\alpha^{-1},\mathbb{Q}} &= m_{e^{(-i\pi/3)},\mathbb{Q}} = m_{0.5-0.5i\sqrt{3},\mathbb{Q}} = (x-(0.5-0.5i\sqrt{3}))(x-(0.5+0.5i\sqrt{3})) \end{aligned}$$

4. Let $\alpha = e^{(i\pi/6)}$ and $\beta = i$. We first calculate $G = \mathrm{Gal}(\mathbb{Q}(\alpha,\beta)/\mathbb{Q})$. We remark that $\beta = \alpha^3$, and hence $\mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\alpha)$. Furthermore, α is a root of the polynomial $x^6 + 1$, which decomposes as $x^6 + 1 = (x^2+1)(x^4 - x^2 + 1)$. The polynomial $x^2 + 1$ has two complex roots $\pm i$. The polynomial $x^4 - x^2 + 1$ has four complex roots $\alpha, \alpha^5, \alpha^7, \alpha^{11}$. Furthermore, this polynomial is irreducible over $\mathbb{Q}$.

Hence the minimal polynomial of α is $m_{\alpha,\mathbb{Q}} = x^4 - x^2 + 1$. Since by adjoining α to $\mathbb{Q}$, all roots of $m_{\alpha,\mathbb{Q}}$ are adjoined as well, we remark that $\mathbb{Q}(\alpha)$ is the splitting field of the polynomial $x^4 - x^2 + 1$ over $\mathbb{Q}$. By Proposition 4.6.3 (4), we get that $|G| = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg m_{\alpha,\mathbb{Q}} = 4$. The elements in G are the identity, τ, σ, η, where the root α gets sent to a root of $x^4 - x^2 + 1$ by every element of G. We let $\tau(\alpha) = \alpha^5, \sigma(\alpha) = \alpha^7, \eta(\alpha) = \alpha^{11}$.

The minimal polynomials are calculated as stated above by observing the action of the ele-

ments id, τ, σ, η. It follows that

$$m_{\alpha,\mathbb{Q}} = (x-\alpha)(x-\tau(\alpha))(x-\sigma(\alpha))(x-\eta(\alpha)) = (x-\alpha)(x-\alpha^5)(x-\alpha^7)(x-\alpha^{11}) = x^4 - x^2 + 1$$

$$m_{\alpha+\beta,\mathbb{Q}} = m_{\alpha+\alpha^3,\mathbb{Q}} = (x-(\alpha+\alpha^3))(x-\tau(\alpha+\alpha^3))(x-\sigma(\alpha+\alpha^3))(x-\eta(\alpha+\alpha^3))$$
$$= (x-(\alpha+\alpha^3))(x-(\alpha^5+\alpha^3))(x-(\alpha^7+\alpha^9))(x-(\alpha^{11}+\alpha^9)) = x^4 + 3x^2 + 9$$

$$m_{\alpha\cdot\beta,\mathbb{Q}} = m_{\alpha^4,\mathbb{Q}} = m_{-0.5+0.5i\sqrt{3},\mathbb{Q}} = (x-\alpha^4)(x-\tau(\alpha^4))(x-\sigma(\alpha^4))(x-\eta(\alpha^4))$$
$$= (x-\alpha^4)(x-\alpha^8)\cancel{(x-\alpha^4)(x-\alpha^8)} = x^2 + x + 1$$

$$m_{\alpha^{-1},\mathbb{Q}} = m_{\alpha^{11},\mathbb{Q}} = (x-\alpha^{11})(x-\tau(\alpha^{11}))(x-\sigma(\alpha^{11}))(x-\eta(\alpha^{11}))$$
$$= (x-\alpha^{11})(x-\alpha^7)(x-\alpha^7)(x-\alpha) = x^4 - x^2 + 1$$

Exercice 6. 1. As $\deg f = 3$ one just has to verify that f does not have a root over $\mathbb{Q}$. So, we need to show that if a and b are non-zero relatively prime integers, then

$$(a/b)^3 + (a/b) + 1 \neq 0,$$

or equivalently

$$a^3 + ab^2 + b^3 \neq 0.$$

Suppose the contrary. Then b divides a^3 and a divides b^3. Using the relative prime assumption we obtain both a and b are plus-minus 1, but one cannot add together three numbers, each plus or minus 1 to get 0.

2. Let α, β and γ be the three roots of f in its splitting field. Assume that they are all real. Then we have

$$f = (x-\alpha)(x-\beta)(x-\gamma)$$

and hence

$$\alpha + \beta + \gamma = 0$$

and

$$\alpha\beta + \alpha\gamma + \beta\gamma = a$$

From the first equation we have $\gamma = -\alpha - \beta$. Plugging this into the left side of the second equation yields

$$\alpha\beta + \alpha(-\alpha-\beta) + \beta(-\alpha-\beta) = -\alpha^2 - \beta^2 - \alpha\beta = -\frac{1}{2}(\alpha+\beta)^2 - \frac{\alpha^2}{2} - \frac{\beta^2}{2} \leq 0$$

However, we assumed that $a > 0$. This is a contradiction.

3. As $\deg f = 3$, and complex roots of a real polynomial come in complex conjugate pairs, f has to have a real root. Let this real root be α. Then, $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ is a degree 3 extension and additionally $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$. Hence, the other two roots of f, say β and γ, cannot be contained in $\mathbb{Q}(\alpha)$. So, every element $g \in \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ can send α only to α. However, as α generated $\mathbb{Q}(\alpha)$ this means that $g = \mathrm{id}$.

4. Let α, β and γ be as in the previous point. Then both β and γ are roots of $h = \frac{f}{x-\alpha} \in \mathbb{Q}(\alpha)[x]$. As this polynomial has degree 2, and β and γ are not in $\mathbb{Q}[x]$, $h = m_{\beta,\mathbb{Q}(\alpha)} = m_{\gamma,\mathbb{Q}(\alpha)}$. So, $\mathbb{Q}(\alpha,\beta,\gamma)$ has degree 2 over $\mathbb{Q}(\alpha)$. So, by the multiplicativity of the degrees of field extensions, $L = \mathbb{Q}(\alpha,\beta,\gamma)$ has degree 6 over $\mathbb{Q}$. Let G be the Galois group of L over $\mathbb{Q}$. Then, G acts faithfully on α, β and γ, which yields an embedding $G \hookrightarrow S_3$. As both have 6 elements, this is in fact an isomorphism.

Exercice 7. 1. Let β be a root of f. It holds that $\beta^p - \beta + \alpha = 0$. Let $\gamma \in \mathbb{F}_p \subseteq K$. Then, using Fermat's little theorem, which states that $\gamma^p = \gamma$ modulo p, it holds that over a field of characteristic p, we have

$$(\beta+\gamma)^p - (\beta+\gamma) + \alpha = \beta^p + \gamma^p - \beta - \gamma + \alpha = \beta^p + \gamma - \beta - \gamma + \alpha = \beta^p - \beta + \alpha = 0.$$

Hence all $\beta + \gamma$, where $\gamma \in \mathbb{F}_p$ are roots of f. We get p distinct roots, and as $\mathbb{F}_p \subseteq K$, by adjoining β to K, all roots are contained in $K(\beta)$ and hence $L = K(\beta)$.

Moreover, we have that $m_{\beta,K} = f$. Let $m_{\beta,K} = \prod_{\gamma\in I}(x-(\beta+\gamma)$ in $L[x]$ with $I \subset \mathbb{F}_p[x]$. Then the coefficients in front of $x^{|I|-1}$ are exactly $-\sum_{\gamma\in I(\beta+\gamma)} = |I|\beta + \sum_{\gamma\in I}\gamma$. If we suppose that $|I| < p$, one contradicts the fact that $\beta \notin K$. Therefore $m_{\beta,K} = f$.

We use Proposition 4.6.3 and get the following: by (a), G acts on the roots of f. By (b), since $L = K(\beta)$, there is at most one element in G that sends the root β to the root $\beta + \gamma$, for $\gamma \in \mathbb{F}_p$. Therefore, $|G| \leq p$. There are indeed p elements in G, which are of the form σ_γ, with $\sigma_\gamma(\beta) = \beta + \gamma$ for all $k \in \mathbb{F}_p$. We get p automorphisms, and hence $G \cong \mathbb{Z}/p\mathbb{Z}$.

2. The fact that f is irreducible over K follows from Prop 4.6.3 (d), which states that $|G| = [L : K]$, where $L = K(\beta)$ is the splitting field of f. By the previous point, $|G| = p$, and hence $[K(\beta) : K] = \deg m_{\beta,K} = p$. Since β is a root of f, and since its minimal polynomial is of degree p, it follows that $f \sim m_{\beta,K}$, and hence, f is irreducible over K.

3. Let $\frac{g}{h} \in \mathbb{F}_p(t)$ a root of $x^p - x + t$. Then, $g, h \in \mathbb{F}_p[t], h \neq 0$ and it holds that

$$\left(\frac{g}{h}\right)^p - \left(\frac{g}{h}\right) + t = 0 \Leftrightarrow g^p - gh^{p-1} + th^p = 0.$$

Denote the degree of g by d_g, and the degree of h by d_h. Then, the degree of the following polynomials are

$$\deg(g^p) = pd_g, \quad \deg(gh^{p-1}) = d_g + (p-1)d_h, \quad \deg(th^p) = 1 + pd_h.$$

In order for the sum $g^p - gh^{p-1} + th^p$ to be zero, the degrees of each of the summands needs to be canceled out.

If $d_h \geq d_g$, then the degree of th^p, being $1+pd_h$, is strictly bigger than pd_g and $d_g+(p-1)d_h$ and hence th^p can't be canceled out, and the sum of polynomials can only be zero if $h = 0$, but this is a contradiction to the choice of g, h.

On the other hand, if $d_g > d_h$, then nothing can cancel out g^p, which one sees by a degree comparison, and hence the sum $g^p - gh^{p-1} + th^p$ can only be zero if $g = 0$ and $h = 0$, which is a contradiction.

4. Let u be a root of $f : u^p - u + t = 0 \Leftarrow u^p - u = -t$, and hence $\mathbb{F}(t) \subseteq \mathbb{F}_p(u)$. With u being transcendental over $\mathbb{F}_p$, it follows that the splitting field is $\mathbb{F}_p(u)$. We remark that by the second part of the exercise, all roots are of the form $u + \gamma$, where $\gamma \in \mathbb{F}_p$, and hence all roots are contained in $\mathbb{F}_p(u)$.

Exercice 8 (Galois correspondence)**.** 1. Let $L = \mathbb{Q}(\sqrt{7})$. We have that $[L : \mathbb{Q}] = 2$, as $\sqrt{7} \notin \mathbb{Q}$ is a root of the irreducible polynomial $x^2 - 7 \in \mathbb{Q}[x]$. Now, $\mathbb{Q}$ is a perfect field and L is the splitting field of $x^2 - 7 \in \mathbb{Q}[x]$ over $\mathbb{Q}$, hence the extension $\mathbb{Q} \subseteq L$ is Galois. By Proposition

4.6.3(d), it follows that $|\operatorname{Gal}(L/\mathbb{Q})| = 2$ and so $\operatorname{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$. The only subgroups of $\operatorname{Gal}(L/\mathbb{Q})$ are $\operatorname{Gal}(L/\mathbb{Q})$ and $\{\mathrm{Id}_L\}$, therefore the only sub-extensions of L are $\mathbb{Q} = L^{\operatorname{Gal}(L/\mathbb{Q})}$ and $L = L^{\{\mathrm{Id}_L\}}$.

2. Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. We have seen in Series 9, Exercise 5.2 that $[L : \mathbb{Q}] = 4$. Now, $\mathbb{Q}$ is a perfect field and L is the decomposition field of $(x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$ over $\mathbb{Q}$, hence the extension $\mathbb{Q} \subseteq L$ is Galois. By Proposition 4.6.3(d), it follows that $|\operatorname{Gal}(L/\mathbb{Q})| = 4$. Now, let $\sigma, \tau \in \operatorname{Gal}(L/\mathbb{Q})$ be such that $\sigma(\sqrt{2}) = -\sqrt{2}$ and $\sigma(\sqrt{3}) = \sqrt{3}$, respectively $\tau(\sqrt{2}) = \sqrt{2}$ and $\tau(\sqrt{3}) = -\sqrt{3}$. We see that $\sigma^2 = \tau^2 = \mathrm{Id}_L$ and that $\sigma\tau = \tau\sigma$. Therefore $\operatorname{Gal}(L/\mathbb{Q}) =< \sigma, \tau >\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Now, $\operatorname{Gal}(L/\mathbb{Q})$ admits 3 non-trivial proper subgroups: $< \sigma >$, $< \tau >$ and $< \sigma\tau >$, each isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Let H be one of these subgroups. By applying Theorem 4.6.18, we determine that $L^H \subseteq L$ is Galois and $[L : L^H] = |H| = 2$. Therefore, $[L^H : \mathbb{Q}] = 2$. One checks that $\mathbb{Q}(\sqrt{3}) \subseteq L^{<\sigma>}$, as $\sigma(\sqrt{3}) = \sqrt{3}$, and, similarly, that $\mathbb{Q}(\sqrt{2}) \subseteq L^{<\tau>}$ and $\mathbb{Q}(\sqrt{6}) \subseteq L^{<\sigma\tau>}$, respectively. We conclude that

$$L^{<\sigma>} = \mathbb{Q}(\sqrt{3}),\ L^{<\tau>} = \mathbb{Q}(\sqrt{2}) \text{ and } L^{<\sigma\tau>} = \mathbb{Q}(\sqrt{6}).$$

3. Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ and consider the extension chain:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq L$$

We have that $[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt{2}, \sqrt{3})][\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 8$, as $\sqrt{5} \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a root of the polynomial $x^2 - 5 \in \mathbb{Q}(\sqrt{2}, \sqrt{3})[x]$. Now, $\mathbb{Q}$ is a perfect field and L is the splitting field of $(x^2 - 2)(x^2 - 3)(x^2 - 5) \in \mathbb{Q}[x]$ over $\mathbb{Q}$, hence the extension $\mathbb{Q} \subseteq L$ is Galois. By Proposition 4.6.3(d), it follows that $|\operatorname{Gal}(L/\mathbb{Q})| = 8$. Let $\sigma_1, \sigma_2, \sigma_3 \in \operatorname{Gal}(L/\mathbb{Q})$ be such that:

$$\sigma_1(\sqrt{2}) = -\sqrt{2},\ \sigma_1(\sqrt{3}) = \sqrt{3} \text{ and } \sigma_1(\sqrt{5}) = \sqrt{5}$$

$$\sigma_2(\sqrt{2}) = \sqrt{2},\ \sigma_2(\sqrt{3}) = -\sqrt{3} \text{ and } \sigma_2(\sqrt{5}) = \sqrt{5}$$

$$\sigma_3(\sqrt{2}) = \sqrt{2},\ \sigma_3(\sqrt{3}) = \sqrt{3} \text{ and } \sigma_3(\sqrt{5}) = -\sqrt{5}$$

One shows that $\sigma_i^2 = \mathrm{Id}_L$ for all $i = 1, 2, 3$ and that $\sigma_i\sigma_j = \sigma_j\sigma_i$ for all $i \neq j$, therefore determining that $\operatorname{Gal}(L/\mathbb{Q}) =< \sigma_1, \sigma_2, \sigma_3 >\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. We first consider the subgroups of order 2 of $\operatorname{Gal}(L/\mathbb{Q})$. There are 7 of them and each of these is cyclic and generated by an element of $\operatorname{Gal}(L/\mathbb{Q})$. Let H be one of these subgroups. We apply Theorem 4.6.18 to determine that $L^H \subseteq L$ is Galois with $[L : L^H] = |H| = 2$. Therefore we have $[L^H : \mathbb{Q}] = 4$.

Let $H =< \sigma_1 >$. One checks that $\mathbb{Q}(\sqrt{3}, \sqrt{5}) \subseteq L^H$, as $\sigma_1(\sqrt{3}) = \sqrt{3}$ and $\sigma_1(\sqrt{5}) = \sqrt{5}$. Therefore, $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}, \sqrt{5}) \subseteq L^H$, where $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 4$ and $[L^H : \mathbb{Q}] = 4$. We conclude that $L^H = \mathbb{Q}(\sqrt{3}, \sqrt{5})$. Similarly, one shows that:

$$L^{<\sigma_2>} = \mathbb{Q}(\sqrt{2}, \sqrt{5}),\ L^{<\sigma_3>} = \mathbb{Q}(\sqrt{2}, \sqrt{3}),\ L^{<\sigma_1\sigma_2>} = \mathbb{Q}(\sqrt{6}, \sqrt{5})$$

$$L^{<\sigma_1\sigma_3>} = \mathbb{Q}(\sqrt{3}, \sqrt{10}),\ L^{<\sigma_2\sigma_3>} = \mathbb{Q}(\sqrt{2}, \sqrt{15}),\ L^{<\sigma_1\sigma_2\sigma_3>} = \mathbb{Q}(\sqrt{6}, \sqrt{10}, \sqrt{15}) = \mathbb{Q}(\sqrt{6}, \sqrt{10})$$

We now consider the subgroups of order 4 of $\operatorname{Gal}(L/\mathbb{Q})$. Again, there are 7 of them and each of these is generated by two distinct elements of order 2 of $\operatorname{Gal}(L/\mathbb{Q})$ and is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Let H be one of these subgroups. We apply Theorem 4.6.18 to determine that $L^H \subseteq L$ is Galois with $[L : L^H] = |H| = 4$. Therefore we have $[L^H : \mathbb{Q}] = 2$. One shows that:

$$L^{<\sigma_1,\sigma_2>} = \mathbb{Q}(\sqrt{5}),\ L^{<\sigma_1,\sigma_3>} = \mathbb{Q}(\sqrt{3}),\ L^{<\sigma_1,\sigma_2\sigma_3>} = \mathbb{Q}(\sqrt{15}),\ L^{<\sigma_2,\sigma_3>} = \mathbb{Q}(\sqrt{2})$$

$$L^{<\sigma_2,\sigma_1\sigma_3>} = \mathbb{Q}(\sqrt{10}),\ L^{<\sigma_3,\sigma_1\sigma_2>} = \mathbb{Q}(\sqrt{6}),\ L^{<\sigma_1\sigma_2,\sigma_1\sigma_3>} = \mathbb{Q}(\sqrt{30}).$$

4. First, we note that the extension $\mathbb{Q} \subseteq E$ is Galois, as $\mathbb{Q}$ is a perfect field and E is the splitting field of the polynomial $t^4 - 2t^2 - 1 \in \mathbb{Q}[t]$ over $\mathbb{Q}$. By Proposition 4.6.3(d), it follows that $|\operatorname{Gal}(E/\mathbb{Q})| = [E : \mathbb{Q}]$. We see that $t^4-2t^2-1 = (t^2-1-\sqrt{2})(t^2-1+\sqrt{2}) = (t-\sqrt{1+\sqrt{2}})(t+\sqrt{1+\sqrt{2}})(t-\sqrt{1-\sqrt{2}})(t+\sqrt{1-\sqrt{2}})$. Therefore $E = \mathbb{Q}(\sqrt{1+\sqrt{2}}, \sqrt{1-\sqrt{2}})$. Now, we have that $i = \sqrt{1+\sqrt{2}} \cdot \sqrt{1-\sqrt{2}} \in E$ and thus $\mathbb{Q}(\sqrt{1+\sqrt{2}}, i) \subseteq E$. Conversely, we have $\sqrt{1-\sqrt{2}} = i \cdot (\sqrt{1+\sqrt{2}})^{-1} \in \mathbb{Q}(\sqrt{1+\sqrt{2}}, i)$ and we deduce that $E = \mathbb{Q}(\sqrt{1+\sqrt{2}}, i)$. We now consider the extension chain:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{1+\sqrt{2}}) \subseteq E.$$

Since $\sqrt{1+\sqrt{2}}$ is a root of $t^4 - 2t^2 - 1 \in \mathbb{Q}[t]$, it follows that $[\mathbb{Q}(\sqrt{1+\sqrt{2}}) : \mathbb{Q}] \leq 4$. We have already seen that the polynomial $t^4 - 2t^2 - 1$ does not admit roots in $\mathbb{Q}$. We now assume that there exist $a, b, c, d \in \mathbb{Q}$ such that:

$$t^4 - 2t^2 - 1 = (t^2 + at + b)(t^2 + ct + d).$$

Then $\begin{cases} a + c = 0 \\ b + ac + d = -2 \\ ad + bc = 0 \\ bd = -1 \end{cases}$ and so $c = -a$, $d = -\frac{1}{b}$ and $-a(\frac{1}{b} + b) = 0$.

- If $a = 0$, then $c = 0$ and $b + d = -2$. Keeping in mind that $d = -\frac{1}{b}$, it follows that $(b+1)^2 = 2$, hence $\sqrt{2} \in \mathbb{Q}$, which is a contradiction.
- If $\frac{1}{b} + b = 0$, then $b^2 + 1 = 0$ and so $i \in \mathbb{Q}$, which is a contradiction.

We have thus shown that $t^4-2t^2-1 \in \mathbb{Q}[t]$ is irreducible and therefore $[\mathbb{Q}(\sqrt{1+\sqrt{2}}) : \mathbb{Q}] = 4$. We remark that $\mathbb{Q}(\sqrt{1+\sqrt{2}}) \subseteq \mathbb{R}$ and so $[E : \mathbb{Q}(\sqrt{1+\sqrt{2}})] = 2$, as $i \notin \mathbb{Q}(\sqrt{1+\sqrt{2}})$ is a root of $t^2 + 1 \in \mathbb{Q}(\sqrt{1+\sqrt{2}})[t]$. In conclusion, $[E : \mathbb{Q}] = 8$, hence $|\operatorname{Gal}(E/\mathbb{Q})| = 8$.

Let $\sigma, \tau \in \operatorname{Gal}(E/\mathbb{Q})$ be such that $\sigma(\sqrt{1+\sqrt{2}}) = \sqrt{1-\sqrt{2}}$ and $\sigma(i) = -i$, respectively $\tau(\sqrt{1+\sqrt{2}}) = \sqrt{1+\sqrt{2}}$ and $\tau(i) = -i$. One checks that:

$$\sigma^2(\sqrt{1+\sqrt{2}}) = -\sqrt{1+\sqrt{2}},\ \sigma^2(i) = i$$

$$\sigma^3(\sqrt{1+\sqrt{2}}) = -\sqrt{1-\sqrt{2}},\ \sigma^3(i) = -i$$

$$\sigma^4(\sqrt{1+\sqrt{2}}) = \sqrt{1+\sqrt{2}},\ \sigma^4(i) = i$$

and thus deduces that $\sigma^4 = \tau^2 = \mathrm{Id}_E$. Now $< \sigma >$ is a subgroup of order 4 in $\operatorname{Gal}(E/\mathbb{Q})$ and $\tau \notin < \sigma >$. We deduce that $\operatorname{Gal}(E/\mathbb{Q}) =< \sigma, \tau >$ and, moreover, as $\sigma\tau \neq \tau\sigma$, $\operatorname{Gal}(E/\mathbb{Q})$ is non-commutative. Lastly, $\operatorname{Gal}(E/\mathbb{Q})$ admits two elements of order 2: σ^2 and τ, and we conclude that $\operatorname{Gal}(E/\mathbb{Q}) \cong D_8$.

We now determine the subgroups of $\operatorname{Gal}(E/\mathbb{Q})$. There are 5 elements of order 2 in $\operatorname{Gal}(E/\mathbb{Q})$: τ,σ^2, $\tau\sigma^2$, $\tau\sigma$ and $\sigma\tau$, each generating a cyclic group of order 2. Let H be one of these subgroups. By applying Theorem 4.6.18, we determine that $E^H \subseteq E$ is Galois and $[E : E^H] = |H| = 2$. Therefore, $[E^H : \mathbb{Q}] = 4$. One checks that:

$$\tau\sigma^2(\sqrt{1+\sqrt{2}}) = \tau(-\sqrt{1+\sqrt{2}}) = -\sqrt{1+\sqrt{2}} \text{ and } \tau\sigma^2(i) = -i$$

$$\tau\sigma(\sqrt{1+\sqrt{2}}) = \tau(\sqrt{1-\sqrt{2}}) = \tau(i(\sqrt{1+\sqrt{2}})^{-1}) = -\sqrt{1-\sqrt{2}} \text{ and } \tau\sigma(i) = i$$

$$\sigma\tau(\sqrt{1+\sqrt{2}}) = \sigma(\sqrt{1+\sqrt{2}}) = \sqrt{1-\sqrt{2}} \text{ and } \sigma\tau(i) = i$$

and therefore

$$\tau\sigma^2(\sqrt{2}) = \tau\sigma^2((\sqrt{1+\sqrt{2}})^2 - 1) = (\tau\sigma^2((\sqrt{1+\sqrt{2}}))^2 - 1 = (-\sqrt{1+\sqrt{2}})^2 - 1 = \sqrt{2}$$

$$\begin{aligned}\tau\sigma(\sqrt{1+\sqrt{2}} - \sqrt{1-\sqrt{2}}) &= \tau\sigma(\sqrt{1+\sqrt{2}}) - \tau\sigma(i(\sqrt{1+\sqrt{2}})^{-1}) = -\sqrt{1-\sqrt{2}} - \tau(-i(\sqrt{1-\sqrt{2}})^{-1}) \\ &= -\sqrt{1-\sqrt{2}} - \tau(-\sqrt{1+\sqrt{2}}) = \sqrt{1+\sqrt{2}} - \sqrt{1-\sqrt{2}}\end{aligned}$$

$$\begin{aligned}\sigma\tau(\sqrt{1+\sqrt{2}} + \sqrt{1-\sqrt{2}}) &= \sqrt{1-\sqrt{2}} + \sigma\tau(i(\sqrt{1+\sqrt{2}})^{-1}) = \sqrt{1-\sqrt{2}} + \sigma(-i(\sqrt{1+\sqrt{2}})^{-1}) \\ &= \sqrt{1-\sqrt{2}} + i(\sqrt{1-\sqrt{2}})^{-1} = \sqrt{1-\sqrt{2}} + \sqrt{1+\sqrt{2}}\end{aligned}$$

The corresponding sub-extensions are

$$E^{<\tau>} = \mathbb{Q}(\sqrt{1+\sqrt{2}}),\ E^{<\sigma^2>} = \mathbb{Q}(\sqrt{1-\sqrt{2}}),\ E^{<\tau\sigma^2>} = \mathbb{Q}(\sqrt{2}, i)$$

$$E^{<\tau\sigma>} = \mathbb{Q}(\sqrt{1+\sqrt{2}} - \sqrt{1-\sqrt{2}}) \text{ and } E^{<\sigma\tau>} = \mathbb{Q}(\sqrt{1+\sqrt{2}} + \sqrt{1-\sqrt{2}}).$$

Lastly, $\mathrm{Gal}(E/\mathbb{Q})$ admits 3 subgroups of order 4, one of which is cyclic, $< \sigma >$, and the other two are isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $< \tau, \sigma^2 >$ and $< \tau\sigma, \sigma^2 >$.Let H be one of these subgroups. By applying Theorem 4.6.18, we determine that $E^H \subseteq E$ is Galois and $[E : E^H] = |H| = 4$. Therefore, $[E^H : \mathbb{Q}] = 2$. One checks that:

$$\sigma(i\sqrt{2}) = -i\sigma(\sqrt{2}) = -i\sigma((\sqrt{1+\sqrt{2}})^2 - 1) = -i(\sqrt{1-\sqrt{2}})^2 - 1) = i\sqrt{2}$$

$$\begin{cases}\tau(\sqrt{2}) = \tau(\sqrt{1+\sqrt{2}})^2 - 1)(= \sqrt{1+\sqrt{2}})^2 - 1 = \sqrt{2} \\ \sigma^2(\sqrt{2}) = \sigma^2((\sqrt{1+\sqrt{2}})^2 - 1) = (-\sqrt{1+\sqrt{2}})^2 - 1 = \sqrt{2}\end{cases}$$

$$\tau\sigma(i) = \tau(-i) = i \text{ and } \sigma^2(i) = i$$

The corresponding sub-extensions are:

$$E^{<\sigma>} = \mathbb{Q}(i\sqrt{2}),\ E^{<\tau,\sigma^2>} = \mathbb{Q}(\sqrt{2}) \text{ and } E^{<\tau\sigma,\sigma^2>} = \mathbb{Q}(i).$$

Exercice 9.
Let G be a finite group and let $|G| = n$. By Cayley's Theorem, we know that we can embed G as a subgroup of S_n.

Now, consider the ring $F = \mathbb{Q}[x_1, \ldots, x_n]$ and for each $\sigma \in G$ define:

$$\phi_\sigma : F \to F \text{ by } \phi_\sigma(x_i) = x_{\sigma(i)} \text{ for all} 1 \leq i \leq n.$$

One shows that ϕ_σ is a ring homomorphism for all $\sigma \in G$. Moreover, we have that $\phi_\sigma \circ \phi_{\sigma^{-1}} = \phi_{\sigma^{-1}} \circ \phi_\sigma = \mathrm{Id}_F$, hence ϕ_σ is invertible for all $\sigma \in G$ with inverse $\phi_\sigma^{-1} = \phi_{\sigma^{-1}}$.

Let $E = \mathbb{Q}(x_1, \ldots, x_n)$ be the field of fractions of F. Then $\phi_\sigma : F \to E$ is an injective ring homomorhism, as it is the composition of two injective ring homomorphisms.We now apply the universal property of the fraction field, to determine that:

$$\phi_\sigma : E \to E,\ \text{where } \phi_\sigma(x_i) = x_{\sigma(i)} \text{ for all } 1 \leq i \leq n$$

is a field homomorphism. Now, one checks that, in fact, ϕ_σ is a $\mathbb{Q}$-automorphism of E.

Let $H = \{\phi_\sigma |\ \sigma \in G\}$ be a subset of $\mathrm{Aut}_\mathbb{Q}(E)$. Since $\phi_{\sigma_1} \circ \phi_{\sigma_2} = \phi_{\sigma_1\sigma_2}$ for all $\sigma_1, \sigma_2 \in G$, it follows that H is a subgroup of $\mathrm{Aut}_\mathbb{Q}(E)$. Moreover, we have that $H \cong G$, hence H is a finite group. We now apply Theorem 4.6.12 to E and H to deduce that $[E : E^H] = |H| = |\mathrm{Gal}(E/E^H)|$, hence $E^H \subseteq E$ is Galois, see Corollary 4.6.13. We conclude that $\mathrm{Gal}(E/E^H) = H \cong G$.

Remarque. En utilisant des techniques de géométrie algébrique et de topologie algébrique on peut montrer que tout groupe fini est réalisé comme un groupe de Galois d'une extension de $\mathbb{C}(t)$.

1. Avec de la géométrie algébrique, on voit que les extensions finies de $\mathbb{C}(t)$ correspondent à des morphismes de *courbes algébriques* $X \to \mathbb{P}^1_{\mathbb{C}}$ tel que si ont enlève un nombre fini de points à $\mathbb{P}^1_{\mathbb{C}}$, le morphisme devient un revêtement au sens topologique.

2. $\mathbb{P}^1_{\mathbb{C}}$ privé d'un nombre fini de points est le plan complexe $\mathbb{C}$ privé d'un nombre fini de points. Par la topologie algébrique, on sait que $\pi_1(\mathbb{C} \setminus \{p_1, \ldots, p_n\}) \cong F_n$ le groupe libre sur n-générateurs. On sait également par la théorie des revêtements, comme tout groupe fini G admet une surjection $F_n \to G$ pour un certain n, qu'il existe un revêtement fini de $\mathbb{C} \setminus \{p_1, \ldots, p_n\}$ avec groupe de Galois égal à G.

3. En retournant à la géométrie algébrique, on obtient alors un morphisme de *courbes algébriques* $X \to \mathbb{P}^1_{\mathbb{C}}$ avec groupe de Galois G et donc une extension de $\mathbb{C}(t)$ avec groupe de Galois G.

Si ce genre de choses vous intrigue, le rédacteur vous encourage à suivre des cours de géométrie algébrique et de topologie algébrique, et/ou à faire des projets dans ces domaines.

Exercice 10.
Remarquons que

$$\left(X^n - \left(\frac{\sqrt{t}+1}{\sqrt{t}-1}\right)\right)\left(X^n - \left(\frac{\sqrt{t}-1}{\sqrt{t}+1}\right)\right) = X^{2n} - 2\left(\frac{t+1}{t-1}\right)X^n + 1.$$

Notons que $\mathbb{C}(\sqrt{t}) \to \mathbb{C}(\sqrt{t})$ qui envoie $\sqrt{t} \mapsto \frac{\sqrt{t}+1}{\sqrt{t}-1}$ et $\sqrt{t} \mapsto \frac{\sqrt{t}-1}{\sqrt{t}+1}$ sont des automorphismes. Comme $X^n - \sqrt{t}$ est irréductible par Einsenstein, il suit que les deux polynômes en facteur ci-dessus sont irréductibles. On voit alors que l'extension

$$\mathbb{C}(t) \subset \mathbb{C}(\sqrt{t}) \subset \mathbb{C}\left(\sqrt[n]{\frac{\sqrt{t}+1}{\sqrt{t}-1}}\right)$$

est de degré $2n$. Notons $x := \sqrt[n]{\frac{\sqrt{t}+1}{\sqrt{t}-1}}$. Les racines de $X^{2n} - 2\left(\frac{t+1}{t-1}\right)X^n + 1$ sont

$$x, \xi_n x, \ldots, \xi_n^{n-1} x, \frac{1}{x}, \xi_n \frac{1}{x}, \ldots, \xi_n^{n-1}\frac{1}{x},$$

où ξ_n est une racine primitive n-ième de l'unité. Dès lors $\mathbb{C}\left(\sqrt[n]{\frac{\sqrt{t}+1}{\sqrt{t}-1}}\right)$ est le corps de décomposition $X^{2n} - 2\left(\frac{t+1}{t-1}\right)X^n + 1$.

Notons $\sigma \in \mathrm{Gal}(L_n/\mathbb{C}(t))$ l'automorphisme tel que $\sigma(x) = \xi_n x$ pour ξ_n. Notons τ pour l'automorphisme tel que $\tau(x) = \frac{1}{x}$. Comme les racines de $X^{2n} - 2\left(\frac{t+1}{t-1}\right)X^n + 1$ sont de la forme $x^\epsilon \xi_n^j$ pour $\epsilon = 1, -1$ et $j = 0, \ldots, n-1$, on voit que tout élément du groupe de Galois est de la forme $\tau^\epsilon \sigma^j$. Comme $\sigma^n = \mathrm{id}$, $\tau^2 = \mathrm{id}$ et $\tau\sigma\tau\sigma = \mathrm{id}$ on a dès lors un morphisme surjectif

$$D_{2n} \to \mathrm{Gal}(L_n/\mathbb{C}(t))$$

qui est un isomorphisme par cardinalité.