Exercice 1.
Soit R un anneau. Parmi les sous-ensembles suivants, lesquels sont-ils des sous-anneaux ?

1. $\{A \in M_n(R) \mid a_{ij} = 0 \text{ si } i > j\} \subset M_n(R)$.
2. $\{A \in M_n(R) \mid a_{ij} = 0 \text{ si } i \leq j\} \subset M_n(R)$.
3. $\{A \in M_n(R) \mid a_{ij} = 0 \text{ si } i \neq j\} \subset M_n(R)$.
4. $\{a + bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$.
5. $\{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\} \subset \mathbb{R}$.
6. $\left\{\begin{pmatrix} a & b \\ a & b \end{pmatrix} \mid a, b \in \mathbb{Z}\right\} \subset M_2(\mathbb{Z})$.
7. $\left\{\begin{pmatrix} a & b \\ b & a+b \end{pmatrix} \mid a, b \in \mathbb{Z}/2\mathbb{Z}\right\} \subset M_2(\mathbb{Z}/2\mathbb{Z})$.

Solution. 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.
Dans chacun des cas suivants, déterminez l'ensemble des homomorphismes d'anneaux $A \to B$.

1. $A = \mathbb{Z}$ et $B = \mathbb{Z}$.
2. $A = \mathbb{Z}$ et $B = \mathbb{Z}/n\mathbb{Z}$ où $n \in \mathbb{N}$.
3. $A = \mathbb{Z}/n\mathbb{Z}$ et $B = \mathbb{Z}$ où $n \in \mathbb{N}$.
4. $A = \mathbb{Z}/m\mathbb{Z}$ et $B = \mathbb{Z}/n\mathbb{Z}$ où $m, n \in \mathbb{N}$.
5. $A = \mathbb{Q}$ et $B = \mathbb{R}$.
6. $A = \mathbb{R}$ et $B = \mathbb{R}$.
7. $A = \mathbb{R}$ et $B = \mathbb{Q}$.
8. $A = \mathbb{R}[t]$ et $B = \mathbb{R}$.
9. $A = \mathbb{R}$ et $B = \mathbb{R}[t]$.

Indication : Pour le point 6, montrez qu'un homomorphisme $f\colon \mathbb{R} \to \mathbb{R}$ envoie les réels positifs vers les réels positifs, et déduisez que f préserve l'ordre usuel sur les réels.

Solution.

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 $n \cdot f([1]) = n \cdot 1 = n \neq 0$ 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 3.
Soient A un anneau commutatif et $a \in A$. Montrer que l'application

$$f\colon A[t] \to A[t], \quad p(t) \mapsto p(t+a)$$

est un isomorphisme d'anneaux.

Solution.
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 4.
Soit G un groupe fini non-trivial. Considérons l'anneau $\mathbb{Z}[G]$.

1. Supposons que $g \in G$ soit non-trivial et que $g^2 = e$. Montrez que $1-g$ et $1+g$ sont des diviseurs de zéro.

2. Plus généralement, montrez que si $g \in G$ est non-trivial, alors $1-g$ est un diviseur de zéro.

Solution.
Notons G multiplicativement, et les éléments de $\mathbb{Z}[G]$ comme des sommes $\sum_{g\in G} a(g)e_g$ où $a(g) \in \mathbb{Z}$. Nous noterons ϵ l'élément neutre de G (donc en particulier $\epsilon = 1$ dans $\mathbb{Z}[G]$).

1. On a que $(1-e_g)(1+e_g) = 1 - e_g + e_g - e_{g^2} = 1 - e_\epsilon = 0$, alors que vu que $g \neq \epsilon$, ni $1-e_g$ ni $1+e_g$ ne sont triviaux.

2. 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 $e_\epsilon + e_g + \cdots + e_{g^{n-1}}$ ne sont égaux à zéro.

Exercice 5.
Montrez qu'il existe au plus 4 homomorphismes d'anneaux $\mathbb{Z}[S_3] \to \mathbb{Z} \times \mathbb{Z}$.
Indication : si $f\colon \mathbb{Z}[S_3] \to \mathbb{Z} \times \mathbb{Z}$ est un homomorphisme, étudiez les images possibles des éléments de S_3.
($\star$) Montrez qu'il existe exactement 4 morphismes $\mathbb{Z}[S_3] \to \mathbb{Z} \times \mathbb{Z}$.

Solution.

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

$$f(e_{(123)})^3 = (1,1).$$

On peut écrire $f(e_{(123)}) = (n,m)$ pour certains $n, m \in \mathbb{Z}$, et donc il faut que $n^3 = m^3 = 1$. Ainsi, on a que

$$f(e_{(123)}) = (1,1).$$

Faisons le même raisonemment pour $e_{(12)}$. Si $f(e_{(12)}) = (a,b)$, alors on obtient que $a^2 = b^2 = 1$, et ainsi (a,b) vaut $(1,1), (1,-1), (-1,1)$ ou $(-1,-1)$.

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 $(a,b) \in \{(1,1),(-1,1),(1,-1),(-1,-1)\}$ et les 3-cycles ainsi que l'élément neutre sur $(1,1)$ se prolonge en unique morphisme. Pour démontrer cela on peut passer par l'argument suivant, qui met en situation ce "prolongement".

L'idée est la suivante: de manière similare au cas des polynômes, la donnée d'un morphisme $R[G] \to S$ pour S un anneau commutatif est *exactement* la même chose que la donnée d'un morphism d'anneaux $R \to S$ et celle d'un morphisme de groupes $G \to (S^\times, \cdot)$. Expliquons cela un peu plus.

Si l'on a un morphisme d'anneaux $f\colon R[G] \to S$, alors on peut précomposer par l'injection canonique $R \to R[G]$ pour obtenir un morphisme d'anneaux $R \to S$. De plus, les éléments de G sont nécessairement envoyés sur des unités de S. En effet, $f(e_g)f(e_{g^{-1}}) = f(e_g e_{g^{-1}}) = f(1) = 1$. Ainsi, on voit que l'on obtient un morphisme de groupes $G \to (S^\times, \cdot)$ donné par $g \mapsto f(e_g)$.

Voyons l'autre sens de la bijection. Si l'on a un morphisme d'anneaux $\theta\colon R \to S$ et un morphisme de groupes $\phi\colon G \to (S^\times, \cdot)$, alors on peut définir $f\colon R[G] \to S$ par

$$f\left(\sum_{g\in G} a(g)e_g\right) = \sum_{g\in G} \theta(a(g))\phi(g) \in S.$$

En utilisant la commutativité de S, on peut montrer que cela est bien un morphisme d'anneaux.

Revenons maintenant à notre cas. On veut comprendre les morphismes d'anneaux $\mathbb{Z}[S_3] \to \mathbb{Z}\times\mathbb{Z}$. Par ce que l'on a dit précédemment, il suffit donc de comprendre les morphismes d'anneaux $\mathbb{Z} \to \mathbb{Z}\times\mathbb{Z}$ et les morphismes de groupes $S_3 \to (\mathbb{Z}\times\mathbb{Z})^\times$.

Pour les morphismes d'anneaux, vu que 1 doit être préservé (et donc ici envoyé sur $(1,1)$), on en déduit par la compatibilité avec l'addition que pour tout $n \in \mathbb{Z}$, son image est obligatoirement $(n,n) \in \mathbb{Z}\times\mathbb{Z}$. Ainsi, il y a bien un unique morphisme d'anneaux $\mathbb{Z} \to \mathbb{Z}\times\mathbb{Z}$ (notez que cet argument montre que pour *tout* anneau R, il y a un unique morphisme $\mathbb{Z} \to R$).

Etudions maintenant les morphisme de groupes $S_3 \to (\mathbb{Z}\times\mathbb{Z})^\times$. Vu que $(\mathbb{Z}\times\mathbb{Z})^\times = \mathbb{Z}^\times \times \mathbb{Z}^\times$ et que $\mathbb{Z}^\times = \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$, on en déduit qu'un morphisme de groupes $S_3 \to (\mathbb{Z}\times\mathbb{Z})^\times$ est la même chose que deux morphismes de groups $S_3 \to \mathbb{Z}/2\mathbb{Z}$.

Nous allons montrer qu'il n'y a en fait que 2 tels morphismes (et donc bien quatre morphismes $\mathbb{Z}[S_3] \to \mathbb{Z}\times\mathbb{Z}$ par notre discussion précédente). Donnons deux preuves:

- Vu que $\mathbb{Z}/2\mathbb{Z}$ est abélien, un morphisme $S_3 \to \mathbb{Z}/2\mathbb{Z}$ doit nécessairement contenir $[S_3, S_3] = \langle(123)\rangle$ dans son noyau. Ainsi, il se factorise automatiquement par $S_3/\langle(123)\rangle \cong \mathbb{Z}/2\mathbb{Z}$, et il suffit donc d'étudier les morphismes $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$. Il n'y a que deux tels morphismes: le morphisme trivial et l'identité.

- Vu que $(123) \in S_3$ est d'ordre 3, l'ordre de son image doit diviser 3. Etant donné que $\mathbb{Z}/2\mathbb{Z}$ n'a aucun élément d'ordre 3, on obtient que le noyau d'un morphisme $g\colon S_3 \to \mathbb{Z}/2\mathbb{Z}$ doit contenir (123). Ainsi, il se factorise par $S_3/\langle(123)\rangle \cong \mathbb{Z}/2\mathbb{Z}$. On conclut comme juste au-dessus.

Exercice 6.
Soit K un corps et $R \subset K$ un sous-anneau.

1. Montrer que R est intègre.
2. Montrer que si pour tout élément de $k \in K$ il existe $r \in R$ non-nul tel que $rk \in R$, alors l'application naturelle $\mathrm{Frac}(R) \to K$ est un isomorphisme.
3. Les inclusions suivantes sont-elles l'inclusion d'un anneau dans son corps des fractions ?
   (a) $\mathbb{Z}[i] \subset \mathbb{Q}[i]$
   (b) $\mathbb{Z}[t] \subset \mathbb{Q}[t]$
   (c) $R[x,y] \subset K(x,y)$ si $K = \mathrm{Frac}(R)$.

Solution.

1. Si $a, b \in R$ satisfont que $ab = 0$, alors c'est aussi vrai dans K (qui est un corps, donc certainement intègre). Du coup, a ou b doivent être nuls.
2. Nommons cette application θ, et montrons tout d'abord qu'elle est injective. Vu que $\ker(\theta)$ est un idéal de K, on a que soit $\ker(\theta) = \mathrm{Frac}(R)$ ou $\ker(\theta) = 0$. Dans le deuxième cas on est bon, et le premier cas est absurde.

   Si l'on s'évite de parler d'idéaux (c'est le thème de la prochaine série), alors on peut raisonner ainsi: supposons qu'il existe $s \in \mathrm{Frac}(R)^\times$ tel que $\theta(s) = 0$. Alors $1 = \theta(1) = \theta(ss^{-1}) = \theta(s)\theta(s^{-1}) = 0$, et donc on a une contradiction.

   Montrons maintenant la surjectivité: soit $k \in K$, et par hypothèse soit $0 \neq r \in R$ tq $rk \in R$. On a alors que
   $$r\theta\left(\frac{rk}{r}\right) = \theta\left(\frac{rk}{1}\right) = rk,$$
   et donc en divisant par $r \in R \subseteq K$ des deux cotés, on obtient que
   $$\theta\left(\frac{rk}{r}\right) = k.$$
3. (a) C'est le cas. On a vu en cours que $\mathbb{Q}[i]$ est en corps. Maintenant, si $s = \frac{a}{b} + \frac{c}{d}i$, alors $(bd)s \in \mathbb{Z}[i]$.
   (b) Non, car $\mathbb{Q}[t]$ n'est pas un corps (t n'a pas d'inverse).
   (c) C'est le cas. Montrons-le en deux temps. Disons qu'une inclusion d'anneaux intègres $A \subseteq B$ satisfait $(\star)$ si pour tout $b \in B$, alors il existe $a \in A$ non-nul tel que $ab \in A$. Notez que si $A \subseteq B$ et $B \subseteq C$ satisfont $(\star)$, alors $A \subseteq C$ le satisfait aussi.

   Par le point précédent, il suffit de montrer que $R[x,y] \subseteq K(x,y)$ satisfait $(\star)$, et donc que les deux inclusions $R[x,y] \subseteq K[x,y]$ et $K[x,y] \subseteq K(x,y)$ satisfont $(\star)$. Pour la première inclusion, si $f = \sum_{i,j} \frac{r_{ij}}{s_{ij}} x^i y^j \in K[x,y]$ est non-nul, et $s := \prod_{i,j} s_{i,j}$ (il y a un nombre fini de tels éléments par définition d'un polynôme), alors $sf \in R[x,y]$.

   Pour la deuxième inclusion, c'est en fait immédiat parce que $K(x,y)$ est par définition le corps des fractions de $K[x,y]$.

Exercice 7 $(\star)$**.**
Soit k un corps. Considérons l'anneau des séries formelles $k[[t]]$.

1. Montrez que $f(t) = \sum_{i=0}^{\infty} a_i t^i$ est un élément inversible de $k[[t]]$ si et seulement si $a_0 \neq 0$. *Indication : Construisez les inverses algorithmiquement. Le cas de $f(t) = 1 - t$ est instructif pour comprendre la preuve générale.*

2. Montrer que le corps des fractions de $k[[t]]$ est donné par les séries de Laurent

$$k((t)) := \left\{ \sum_{i=n}^{\infty} a_i t^i \mid a_i \in k, n \in \mathbb{Z} \right\}.$$

Solution.

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

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

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

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

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

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

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

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

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

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

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

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

Solutions.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Solution.

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

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

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

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

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

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

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

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

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

Exercice 3.
Soit R un anneau commutatif.

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

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

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

Solution.

(a) Donnons deux preuves de ce fait:

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

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

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

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

(b) Soit $f\colon R[t] \to R[\mathbb{Z}/n\mathbb{Z}]$ le morphisme évaluant t en $e_{[1]}$. Comme avant, on calcule que $(t^n - 1) \subseteq \ker(f)$ (c'était l'inclusion facile), et donc que on obtient un morphisme $\overline{f}\colon R[t]/(t^n - 1) \to R[\mathbb{Z}/n\mathbb{Z}]$. Trouvons un inverse explicite.
Comme expliqué dans la preuve de l'exercice 5 de la série 1.1, trouver un morphisme $R[\mathbb{Z}/n\mathbb{Z}] \to R[t]/(t^n - 1)$ est équivalent à trouver un morphisme d'anneaux $R \to R[t]/(t^n - 1)$ et un morphisme de groupes $\mathbb{Z}/n\mathbb{Z} \to (R[t]/(t^n - 1))^\times$. Dans notre cas, on prend la composition $R \to R[t] \to R[t]/(t^n - 1)$, et le morphisme de groupes défini par envoyer $[1] \in \mathbb{Z}/n\mathbb{Z}$ sur $[t] \in (R[t]/(t^n - 1))^\times$ (notez que cela a du sens, car $[t]$ est inversible et d'ordre n dans cet anneau, vu que $[t]^n = [1]$). Ainsi, on a un morphisme d'anneaux explicite $g\colon R[\mathbb{Z}/n\mathbb{Z}] \to R[t]/(t^n - 1)$, qui "fixe" R et envoie $e_{[1]}$ sur t.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Solution.

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

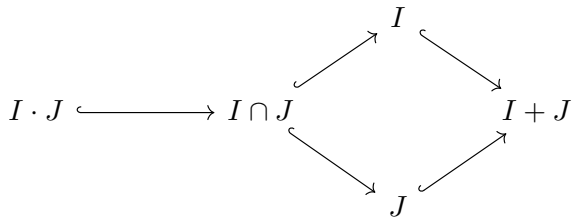
(b) Proposition 2.4.7;

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

(d) Proposition 2.4.7.

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

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



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

$$xyg = y^2 h,$$

et donc

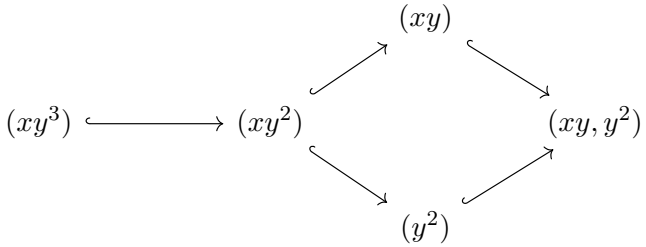
$$y(xg - yh) = 0.$$

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

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

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

Il faut donc montrer que chaque inclusion



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

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

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

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

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

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

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

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

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

Solution.

(a) Example 2.4.10;

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

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

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

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

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

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

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

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

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

Solution.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

EPFL - Printemps 2025	Prof. Zs. Patakfalvi
Anneaux et Corps	**Exercices**
Solutions 2	

Exercice 1.
Dans chacun des cas suivants, déterminer si l'affirmation suivante est vraie ou fausse. Justifier la réponse par un raisonnement ou un contre-exemple.

1. L'image d'un idéal bilatère par un homomorphisme d'anneaux est encore un idéal bilatère.
2. La préimage d'un idéal bilatère par un homomorphisme d'anneaux est encore un idéal bilatère.

Solution.

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 *2.4.32* in the notes.

Exercice 2.
Considérons l'homomorphisme

$$\begin{array}{rccc} \xi_p: & \mathbb{Z}[t] & \to & \mathbb{F}_p[t] \\ & \sum_{i=0}^n a_i t^i & \mapsto & \sum_{i=0}^n [a_i] t^i \end{array}$$

qui envoie un polynôme à coefficients dans $\mathbb{Z}$ au polynôme obtenu par réduction des coefficients mod p. Soit $f(t)$ un polynôme dans $\mathbb{F}_p[t]$ et $g(t)$ une pré-image par ξ_p. Montrez que la pré-image de l'idéal $((f(t)))$ est $(p, g(t))$.

Solution. Nous allons procéder de deux manières différentes.

1. Non-explicite: Cet homomorphisme est surjectif de noyau (p). Comme la pré-image de $(f(t))$ et $(p, g(t))$ contiennent les deux (p), on sait par le théorème de correpondance qu'il suffit de montrer que leur image via $\mathbb{Z}[t] \to \mathbb{F}_p[t]$ sont les mêmes. Comme elles sont les deux $(f(t))$ par construction, on est bon.
2. Explicite: tout d'abord, vu que p et $g(t)$ sont dans $\xi_p^{-1}((f(t))$, alors automatiquement

$$(p, g(t)) \subseteq \xi_p^{-1}((f(t)).$$

Soit maintenant $h \in \xi_p^{-1}((f(t))$, et écrivons $\xi_p(h(t)) = \lambda(t)f(t)$, avec $\lambda(t) \in \mathbb{F}_p[t]$. Soit de plus $\mu(t)$ tel que $\xi_p(\mu(t)) = \lambda(t)$. Alors on obtient que

$$\xi_p(\mu(t)g(t)) = \lambda(t)f(t) = \xi_p(h(t)),$$

te donc que $\mu(t)g(t) - h(t) \in \ker(\xi_p) = (p)$. Ainsi, il exists $w(t)$ tel que

$$h(t) = \mu(t)g(t) - pw(t) \in (p, g(t)),$$

et donc on a bel et bien que

$$\xi_p^{-1}((f(t))) \subseteq (p, g(t)).$$

Exercice 3.
Prouvez les affirmations suivantes.

1. Un anneau intègre avec un nombre fini d'éléments est un corps.
2. Soit K un corps et A un anneau commutatif.
   (a) Soit $K \to A$ un morphisme d'anneau. Montrez que multiplier par l'image des éléments de K fait de A un K-espace vectoriel avec son addition qui vient de la structure d'anneau de A.
   (b) Si maintenant A est intègre et de dimension finie en tant qu'espace vectoriel avec la structure ci-dessus, montrez que A est un corps.

Solution. Dans les deux cas on utilise l'argument suivant: la multiplication par un élément non-nul est injective (par intégrité), et donc dans nos cas surjective. Cette déduction est valide dans le premier cas car une fonction injective d'un ensemble fini vers lui même est injective si et seulement si surjective, et c'est aussi vrai pour les endomorphismes K-linéaires de K-espaces vectoriels de dimension finie.

Exercice 4.
Soit $f\colon A \to B$ un homomorphisme d'anneaux.

1. Montrer que $\mathrm{car}(B)$ divise $\mathrm{car}(A)$, mais qu'en général $\mathrm{car}(B) \neq \mathrm{car}(A)$.
2. Montrer que si f est injectif alors $\mathrm{car}(B) = \mathrm{car}(A)$.
3. Montrer que si A est commutatif et $\mathrm{car}(A) = p$, un nombre premier, alors l'application $F\colon A \to A$ définie par $F(a) = a^p$ est un homomorphisme d'anneaux.
4. Calculer la caractéristique de l'anneau $\mathbb{Z}[i]/(i-2)$.

Solution. Let $\iota_A : \mathbb{Z} \to A$ be the unique ring homomorphism with source $\mathbb{Z}$. By definition, $\mathrm{car}(A) = n$, 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 $\mathrm{car}(B)$. Therefore, $m \big| n$, and so $\mathrm{car}(B) \big| \mathrm{car}(A)$.

   In general, $\mathrm{car}(B) \neq \mathrm{car}(A)$, 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.
Soit $A = \mathbb{Z}/250\mathbb{Z}$.

1. Trouver tous les diviseurs de zéro et tous les éléments inversibles de A.
2. Trouver tous les idéaux de A qui contiennent l'élément $[50]_{250}$. (Ce qu'on veut dire par cette notation c'est l'image de 50 dans $\mathbb{Z}/250\mathbb{Z}$.)

Solution. 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 theorem described in *Propositon 2.4.39*, 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 $a, b, c \in \mathbb{Z}$. Montrez 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) $A/K \to \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$.

Solution. 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

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

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.
Soit R un anneau commutatif.

1. Montrer que $R[x, y]/(x) \cong R[y]$ (donner la forme explicite d'un isomorphisme).
2. Construire un homomorphisme d'anneaux $R[x, y] \to R[x] \times R[y]$ dont le noyau est (xy).
3. Identifier l'image de cet homomorphisme et en conclure que $R[x, y]/(xy)$ est isomorphe au sous-anneau de $R[x] \times R[y]$ formé des couples de polynômes $(p(x), q(y))$ tels que $p(0) = q(0)$.

Solution.

1. We use the universal property of polynomial rings, applied to the identity on $R[y]$. to obtain a ring homomorphism $ev_0 : R[y][x] \to R[y]$ s.t. $id_{R[y]} = \iota \circ ev_0$, where ι denotes the inclusion $\iota : R[y] \to R[y][x]$. ev_0 acts by sending a polynomial $p(x, y) \in R[y][x] \cong R[x, y]$ to $p(0, y) \in R[y]$. One easily verifies that ev_0 is surjective, as the identity on $R[y]$ is surjective. The kernel of ev_0 consists of all polynomials $p(x, y) \in R[x, y]$ 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 $R[y] \cong R[x, y]/(x)$.

2. As above, consider the two evaluations

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

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

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

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

$$(xy) \subset (x) \cap (y)$$

   holds immediately – as for the other inclusion, say $xf = yg$ for $f, g \in R[x, y]$ *i.e* an element of $(x) \cap (y)$. Note that $ev_{0,y}(xf) = xf(0, y) = 0$. As x is not a divisor of zero in $R[x]$, we conclude that $f(0, y) = 0$. Therefore $f \in (y)$, showing that $xf \in (xy)$.

3. We note that for a polynomial $p(x, y) \in R[x, y]$ 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 $p(x) \in R[x]$ and $q(y) \in R[y]$. Consider the pair $(a + xp(x), a + yq(y)) \in R[x] \times R[y]$ with $a \in R$. 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.

EPFL - Printemps 2025 | Prof. Zs. Patakfalvi
Anneaux et Corps | **Exercices**
Solutions 3

Exercice 1.
Dans chacun des cas suivants, déterminer si l'idéal proposé est premier ou maximal.

(a) $(0) \subset \mathbb{Z}$.
(b) $(t) \subset \mathbb{Z}[t]$.
(c) $(t) \subset \mathbb{R}[t]$.
(d) $(101) \subset \mathbb{Z}[t]$.
(e) $(42) \subset \mathbb{Z}[t]$.
(f) $(t^2-2) \subset \mathbb{Z}[t]$.
(g) $(t^2-2) \subset \mathbb{R}[t]$.
(h) $(t+5, 10) \subset \mathbb{Z}[t]$.
(i) $(t+5, 11) \subset \mathbb{Z}[t]$.
(j) $(t^2+1, 2) \subset \mathbb{Z}[t]$.

Indication : Pour prouver qu'un idéal bilatère $I \subset A$ est premier, il suffit de montrer que le quotient A/I est intègre.

Solution.

1. $(0) \subset \mathbb{Z}$ est premier car $\mathbb{Z}$ est intègre, 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 2.4.19 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. Discuter les systèmes suivants : $\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 7 \pmod{12} \end{cases}$ et $\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 8 \pmod{12} \end{cases}$

2. Montrer que $\mathbb{Z}/36\mathbb{Z}$ n'est pas isomorphe à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$.

Solution.

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. Soit $f\colon A \twoheadrightarrow B$ un homomorphisme d'anneaux surjectif tel que $\ker f = (a_1, \ldots, a_m)$ pour certains $a_1 \ldots, a_m \in A$. Soit aussi $I = (b_1, \ldots, b_n) \subseteq B$ un idéal à gauche. Si $c_1, \ldots, c_n \in A$ sont tels que $f(c_i) = b_i$ pour chaque i, montrez que $f^{-1}(I) = (a_1, \ldots, a_m, c_1, \ldots, c_n)$.

2. Soit k un corps, $a, b \in k$ et considérons les homomorphismes d'anneaux k-linéaires

$$\mathrm{ev}_b\colon k[x,y] \to k[x],\ x \mapsto x,\ y \mapsto b \qquad \text{et} \qquad \mathrm{ev}_a\colon k[x] \to k,\ x \mapsto a$$

   et

$$\xi := \mathrm{ev}_a \circ \mathrm{ev}_b\colon k[x,y] \longrightarrow k.$$

   Montrez que $\ker \xi = (x - a, y - b)$ et que $\ker \xi$ est un idéal maximal de $k[x,y]$.

   On peut en fait montrer que si k est algébriquement clos, alors tous les idéaux maximaux de $k[x,y]$ sont de cette forme. C'est une conséquence du Nullstellensatz d'Hilbert.

Solution.

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'Exercice 6.a) de la série 1.2 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 2.5.5, on obtient que $\ker \xi$ est un idéal maximal.

Exercice 4.
Dans cet exercice, nous étudions les anneaux $\mathbb{Z}[i]/(p)$ pour p un nombre premier. Nous écrirons $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

1. Montrez que $\mathbb{Z}[i]/(p) \cong \mathbb{F}_p[t]/(t^2+1)$.
   Indication : Combinez l'exemple 2.4.19 et le quotient en deux temps.
2. Pour $p = 5$, montrez que $\mathbb{Z}[i]/(5) \cong \mathbb{F}_5 \times \mathbb{F}_5$.
   Indication : Le théorème des restes chinois peut être utile.
3. ($\star$) Plus généralement montrez que $\mathbb{Z}[i]/(p) \cong \mathbb{F}_p \times \mathbb{F}_p$ si et seulement si $p \equiv 1 \mod 4$.
   Indication : Montrez que l'hypothèse est équivalente à l'existence de deux racines carrés disctintes de -1 dans $\mathbb{F}_p$. Pour une direction, on utilisera que $\mathbb{F}_p^\times$ est un groupe cyclique. [*]

Solution.

1. On sait par l'Exemple 2.4.19 que le morphisme $\mathbb{Z}[x] \to \mathbb{Z}[i]$ donné par l'évaluation en i induit un isomorphisme $\theta\colon \mathbb{Z}[x]/(x^2+1) \to \mathbb{Z}[i]$. De plus, $p + (x^2+1)$ est envoyé sur p par cet isomorphisme, et donc on en déduit un isomorphisme

$$(\mathbb{Z}[x]/(x^2+1))/(p + (x^2+1)) \cong \mathbb{Z}[i]/(p).$$

   Par le théorème du quotient en deux temps appliqué deux fois, on a que

$$(\mathbb{Z}[x]/(x^2+1))/(p + (x^2+1)) \cong \mathbb{Z}[x]/(p, x^2+1) \cong (\mathbb{Z}[x]/(p))/(x^2+1+(p)).$$

   De plus, il est immédiat que le morphisme $\mathbb{Z}[x] \to \mathbb{F}_p[x]$ induit par la réduction modulo p et envoyant x sur x est surjectif, de noyau $(p) \subseteq \mathbb{Z}[x]$. Il induit donc un isomorphisme $\mathbb{Z}[x]/(p) \cong \mathbb{F}_p[x]$. Comme ce morphisme envoit $x^2+1+(p)$ sur x^2+1, on a donc un isomorphisme induit

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

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 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

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

$*$. Voici une preuve de ce fait. Si ce groupe n'était pas cyclique, par la classification des groupes abéliens de type fini, il existerait $n < p-1$ tel que $x^n = 1$ pour tout $x \in \mathbb{F}_p^\times$. Mais alors $t^n - 1$ aurait $p-1$ racines dans $\mathbb{F}_p$ ce qui est absurde.

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. Montrons tout d'abord que 4 divise $p-1$ (i.e. $p \equiv 1 \mod 4$) si et seulement si -1 possède deux racines distinctes modulo p.

   Tout d'abord, aucun des deux côtés de l'équivalence n'est satisfait si $p = 2$, donc supposons que $p \neq 2$. Dans ce cas, il suffit de montrer que 4 divise $p-1$ si et seulement si -1 est un carré modulo p (si $a \in \mathbb{F}_p$ satisfait $a^2 = -1$, alors $-a$ aussi et vu que $p \neq 2$, il y a automatiquement deux racines carrés de -1).

   Supposons tout d'abord qu' il existe $a \in \mathbb{F}_p$ tel que $a^2 = -1$. Vu que $p \neq 2$, a est donc un élément d'ordre 4 dans le groupe multiplicatif $(\mathbb{F}_p^\times, \cdot)$, qui est d'ordre $p-1$. Ainsi, 4 divise $p-1$ par le théorème de Lagrange.
   Si 4 divise $p-1$, alors comme $(\mathbb{F}_p^\times, \times)$ est cyclique, de générateur disons α, on voit que $\alpha^{\frac{p-1}{4}}$ est d'ordre 4.
   Maintenant montrons que $\mathbb{Z}[i]/(p) \cong \mathbb{F}_p \times \mathbb{F}_p$ si et seulement si -1 possède deux racines distinctes modulo p.
   Si -1 possède deux racines distinctes dans $\mathbb{F}_p$, disons α_1, α_2, alors $t^2+1 = (t-\alpha_1)(t-\alpha_2)$ et donc comme $\alpha_1 \neq \alpha_2$ on peut utiliser le théorème des restes chinois pour obtenir que

$$\mathbb{Z}[i]/(p) \cong \mathbb{F}_p[t]/(t^2+1) = \mathbb{F}_p[t]/(t-\alpha_1)(t-\alpha_2) \cong \mathbb{F}_p \times \mathbb{F}_p.$$

   Réciproquement si

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

   notons (α_1, α_2) l'image de t par cet isomorphisme. Comme $t^2 = -1$ dans l'anneau de gauche, on voit que $\alpha_1^2 = \alpha_2^2 = -1$. Il reste à démontrer que $\alpha_1 \neq \alpha_2$. Supposons par l'absurde que ce soit le cas, et que ces éléments soient égaux à un $\lambda \in \mathbb{F}_p$. Mais alors $t - \lambda$ serait dans le noyau de la composition

$$\mathbb{F}[t] \to \mathbb{F}_p[t]/(t^2+1) \cong \mathbb{F}_p \times \mathbb{F}_p$$

   et donc inclus dans (t^2+1) comme le deuxième morphisme est un isomorphisme. Mais cela est absurde car un polynôme de degré 2 ne peut diviser un polynôme de degré 1.

Exercice 5.
Soient A et B deux anneaux commutatifs. Quels sont les idéaux de $A \times B$? Quels sont les idéaux premiers de $A \times B$?

Solution. 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.
Soit A un anneau commutatif.

1. Montrez que si $\mathfrak{m}$ est maximal et est composé uniquement d'éléments nilpotents, alors c'est l'unique idéal maximal de A. La réciproque est-elle vraie ?
2. Montrez que $A \setminus A^\times$ est un idéal si et seulement si A a un unique idéal maximal.

Solution.

1. Notons que $\mathfrak{m} \subset \mathrm{nil}(A)$ par hypothèse implique en fait $\mathfrak{m} = \mathrm{nil}(A)$ par maximalité. Maintenant si $\mathfrak{m}'$ est un autre idéal maximal, on a $\mathrm{nil}(A) \subset \mathfrak{m}'$ Mais alors on a encore égalité par maximalité, ce qui conclut. La réciproque est fausse, considérez $\mathbb{Z}_{(p)}$ (c.f. l'exercice 1 de la série 1.2).
2. 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 $\mathfrak{m} = A \setminus A^\times$.

   Réciproquement si A a un unique idéal maximal $\mathfrak{m}$, alors $A \setminus \mathfrak{m} = A^\times$. En effet $\supset$ suit, sinon il y a un élément inversible dans $\mathfrak{m}$, ce qui contredirait le caractère propre de $\mathfrak{m}$. Pour l'autre inclusion prenons $x \in A \setminus \mathfrak{m}$. Par l'absurde supposons que x ne soit pas inversible. Alors (x) est un idéal propre est donc inclus dans un idéal maximal. Mais par hypothèse on a alors $(x) \subset \mathfrak{m}$ ce qui est absurde.

Exercice 7 $(\star)$**.**
Soit R un anneau commutatif. Déterminer $(R[t])^\times$.
On pourra se ramener au cas intègre en quotientant par des idéaux premiers de R.

Solution.

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,

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

†. 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.

EPFL - Printemps 2025	Prof. Zs. Patakfalvi
Anneaux et Corps	**Exercices**
Solutions 4	

Exercice 1. (a) Soit k un corps. Trouver tous les idéaux de l'anneau quotient $k[t]/(t^2)$. Déterminer lesquels sont premiers et lesquels sont maximaux.

(b) Soit $I \subset M \subset A$ deux idéaux d'un anneau A et soit $\pi : A \to A/I$ l'homomorphisme quotient. Montrer que l'idéal $\pi(M)$ est maximal dans A/I si et seulement si M est maximal dans A.

Solution.

(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).

Un autre argument: (t) dans le quotient est un idéal maximal nilpotent. C'est alors l'unique idéal *premier*. Dans l'exercice 6 de la série 3, on montre que c'est l'unique idéal maximal. Mais l'exact même argument fonctionne également pour montrer que c'est l'unique idéal premier.

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

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

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

Exercice 2 (Fonctions polynomiales.)**.**
Soit A un anneau commutatif et $\mathcal{F}(A)$ l'anneau des fonctions $\varphi\colon A \to A$ où la somme et le produit sont définis dans l'ensemble d'arrivée (par exemple $(\varphi \cdot \phi)(a) = \varphi(a) \cdot \phi(a)$). On considère l'évaluation comme application $\mathrm{ev}\colon A[t] \to \mathcal{F}(A)$. L'évaluation d'un polynôme f est donc la fonction polynomiale $\mathrm{ev}(f)$ définie par $\mathrm{ev}(f)(a) = \mathrm{ev}_a(f) = f(a)$.

(a) Montrer que l'évaluation est un homomorphisme d'anneaux.

(b) Montrer que si A est fini, alors l'évaluation n'est pas injective.

(c) Montrer que si A est intègre et infini, alors l'évaluation est injective.

Solution.

(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) Consider the polynomial $f(t) = \prod_{a\in A}(t-a)$. Then $f \neq 0 \in A[t]$, but $f(a) = 0$ for all $a \in A$.

(c) Supposons que A est intègre et infini. Soit f dans le noyau. Alors f s'annule en tous les $a \in A$. Prenons une suite infinie d'éléments distincts $a_1, \ldots, a_n, \ldots$. Notons que $(t-a_1) \mid f$. Donc

$$f = g(t-a_1).$$

Donc $f(a_2) = g(a_2)(a_2 - a_1)$. Comme $a_2 \neq a_1$ et A est intègre, on a $g(a_2) = 0$. Alors $(t-a_2) \mid g$. Par récurence, on voit que $(t-a_n) \mid f$ pour tout n. Ainsi on voit que forcément $f = 0$, sans quoi le degré de ce polynôme ne serait pas borné.

Exercice 3.
Soit A un anneau commutatif. On note $\mathrm{nil}(A)$ pour les éléments nilpotents de A. Soit k un corps.

1. Déterminer $\mathrm{nil}(A)$, où $A = {k[x,y]}\Big/{(x^2y^3)}$.
2. Écrire $\mathrm{nil}(A)$ comme l'intersection d'idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$, $\mathrm{nil}(A) = \cap_{i=1}^m \mathfrak{p}_i$, pour m minimal.
3. Déterminer les premiers minimaux de A.

Solution.

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.

Exercice 4.
Montrer que $\mathbb{F}_p[x]/(x^p - 1)$ n'est pas isomorphe à un produit de deux anneaux non-nuls.

Solution.

Notons que $(t^p - 1) = (t^p + (-1)^p) = (t-1)^p$.* Dès lors

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

Première solution.

Notez que l'évaluation $\mathbb{F}_p[t] \xrightarrow{t\mapsto 1} \mathbb{F}_p$ passe au quotient

$$A \xrightarrow{t\mapsto 1} \mathbb{F}_p$$

car $(t-1)^p$ est envoyé su zéro. Prenons maintenant un idempotent $e \in A$, c'est à dire que $e^2 = e$. Notez que si $f(t)$ est un lift de e dans $\mathbb{F}_p[t]$, on peut écrire

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

par division euclidienne.

Notez que que comme $(t-1)^p = 0$ et que $(-)^p$ est un morphisme en caractéristique p on peut dès lors écrire

$$e = \lambda + n$$

pour $\lambda \in \mathbb{F}_p$ et $n \in A$ tel que $n^p = 0$. Comme $e^p = e$ on obtient

$$\lambda + n = \lambda^p + n^p = \lambda$$

car $n^p = 0$ et $\lambda^p\lambda$ comme $\lambda \in \mathbb{F}_p$. On en déduit que $n = 0$. Comme dès lors on sait aussi que $\lambda^2 = \lambda$, on voit que $\lambda = 0, 1$ ce qui conclut que les seuls idempotents sont $0, 1$ et donc que A n'est pas un produit d'anneaux non-nuls.

Deuxième solution.

Rappelons que selon l'exercice 6 de la série 3, si $A \setminus A^\times$ est un idéal, alors c'est l'unique idéal maximal de A.

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

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

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.

Exercice 5.
L'anneau $\mathbb{Z}[\sqrt{5}]$.

1. Montrer que la norme $N\colon \mathbb{Z}[\sqrt{5}] \to \mathbb{Z}$ définie par $N(a + b\sqrt{5}) = a^2 - 5b^2$ est une fonction multiplicative (donc que $N(xy) = N(x)N(y)$ – noter que si l'on définit $\overline{a + b\sqrt{5}} = a - b\sqrt{5}$, alors $N(x) = x\overline{x}$) et que $a + b\sqrt{5}$ est inversible si et seulement si $N(a + b\sqrt{5}) = \pm 1$.

*Cet argument marche aussi en caractéristique 2 car dès lors $1 = -1$.

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

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

2. Montrer que $9+4\sqrt{5}$ est inversible et en déduire que $(\mathbb{Z}[\sqrt{5}])^\times$ est infini.

3. Montrer qu'il n'existe aucun élément de norme 2 ou -2, si bien que tout élément de norme 4 est irréductible.

4. Trouver deux décompositions de 4 en produit d'irréductibles dans $\mathbb{Z}[\sqrt{5}]$.

5. L'idéal $(3+\sqrt{5})$ est-il premier?

Solution.

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.
Soit $d > 1$. On note $A = \mathbb{Z}[i\sqrt{d}]$. On note $N(a+bi\sqrt{d}) = a^2 + db^2$.

1. Lister les éléments $x \in A$ tel que $N(x) \leq d+1$.

2. Montrer que $i\sqrt{d}$, $1+i\sqrt{d}$ et $1-i\sqrt{d}$ sont irréductibles.

3. Si $d+1$ n'est pas premier *dans* $\mathbb{Z}$, alors A n'est pas factoriel.

4. Si $q = d+1$ est premier *dans* $\mathbb{Z}$ alors celui-ci admet une factorisation unique en irréductibles dans A.

Solution.

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.

EPFL - Printemps 2025 | Prof. Zs. Patakfalvi
Anneaux et Corps | **Exercices**
Solutions 5

Exercice 1.
Entiers de Gauss.

1. Comme vu en cours, l'anneau $\mathbb{Z}[i]$ est euclidien avec $N(a+ib) = |a+ib|^2$. Pour $a, b \in \mathbb{Z}[i], a \neq 0$ on appelle une égalité de la forme $b = aq + r$, avec $q, r \in \mathbb{Z}[i]$ et $N(r) < N(a)$ une division avec reste. Effectuer la division avec reste de $5 + 5i$ par $4 + 2i$ et montrer que les quotients et restes de la division dans $\mathbb{Z}[i]$ ne sont pas uniques.

2. Les entiers de Gauss $2, 3$ et 5 sont-ils irréductibles dans $\mathbb{Z}[i]$? Et $2i$ et $2 - 3i$?

3. Montrer que le quotient $\mathbb{Z}[i]/(3)$ est un corps de cardinalité 9.

4. Soit p un nombre premier. Montrer que les énoncés suivants sont équivalents.

   (a) L'entier p n'est pas irréductible dans $\mathbb{Z}[i]$.
   (b) Il existe $a, b \in \mathbb{Z}$ avec $p = a^2 + b^2$.
   (c) ($\star$) $p = 2$ ou alors $p \equiv 1 \mod 4$.

Solution.

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 $9 = N(xy) = N(x)N(y)$, so both $N(x)$ and $N(y)$ divide 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 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 3.7.4, from which it follows that $\mathbb{Z}[i]$ is principal. The Proposition 3.6.3 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. - On montre que $(a) \implies (b)$. Vu que p n'est pas irréductible, on peut écrire $p = xy$ avec x et y non-inversibles (en donc pas de norme 1). On a alors que $p^2 = N(p) = N(x)N(y)$ et donc $N(x), N(y) \in \{1, p, p^2\}$. Vu que $N(x)$ et $N(y)$ ne valent pas 1, ils ne peuvent pas valoir p^2 non plus, et donc $N(x) = N(y) = p$. Si l'on écrit $x = a+bi$, alors $p = a^2+b^2$.
   - On montre que $(b) \implies (a)$. Si $p = a^2+b^2$, alors $p = (a+bi)(a-bi)$. Vu que $a \pm bi$ n'est pas inversible (sa norme vaut p), on en déduit que p n'est pas irreductible dans $\mathbb{Z}[i]$.
   - On montre que $(a) \implies (c)$. Supposons $p \neq 2$, et montrons que 4 divise $p-1$. Vu que p n'est pas irréductible dans $\mathbb{Z}[i]$, l'ideal (p) ne peut pas être intègre. Ainsi,

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

     n'est pas intègre, et donc en particulier t^2+1 n'est pas premier dans $\mathbb{F}_p[t]$ (et donc pas irreductible, vu que $\mathbb{F}_p[t]$ est factoriel). Ainsi, il existe une race $a \in \mathbb{F}_p$ de t^2+1, et donc $a^4 = 1$. Comme $p \neq 2$, on a que $a^2 \neq 1$, et donc a est d'ordre 4 dans le groupe multiplicatif $\mathbb{F}_p^\times$, qui est d'ordre $p-1$. Par le théorpme de Lagrange, on en déduit que 4 divise $p-1$.
   - On montre que $(c) \implies (a)$. Par le même argument que précédemment, il suffit de montrer que t^2+1 n'est pas irréductible dans $\mathbb{F}_[t]$ (et donc que t^2+1 admet une racine dans $\mathbb{F}_p$). Si $p = 2$, c'est immédiat ($1^2+1 = 2 = 0$). Supposons donc que 4 divise $p-1$. Vu que $\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$, il existe un élément a d'ordre 4 dans $\mathbb{F}_p^\times$. Vu que $a^2 \neq 1$, on a forcément que $a^2 = -1$, et donc a et bel et bien une racine de t^2+1.

Exercice 2.
Entiers d'Eisenstein. Soit $\omega = e^{\frac{2\pi i}{3}}$ et $\mathbb{Z}[\omega]$ l'anneau des entiers d'Eisenstein.

1. Montrer que $N(a+b\omega) = a^2-ab+b^2$ coïncide avec le module au carré dans le plan complexe de $a+b\omega$.

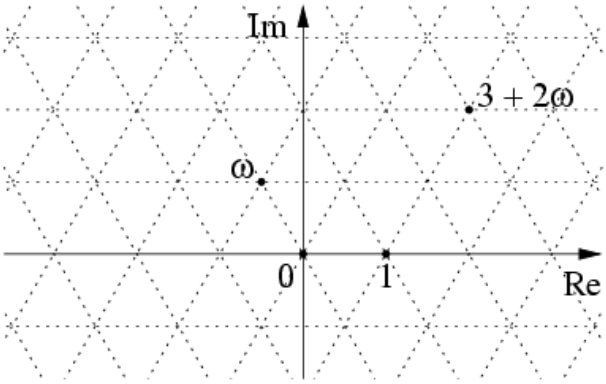
2. Montrer que $N(a+b\omega) = a^2-ab+b^2$ munit $\mathbb{Z}[\omega]$ d'une fonction euclidienne. On pourra par exemple montrer que le point milieu d'une maille du réseau $(a+b\omega)$ se trouve à une distance strictement plus petite que $\sqrt{N(a+b\omega)}$ de chacun des quatre sommets de cette maille.

3. Trouver les éléments inversibles de $\mathbb{Z}[\omega]$ (quelle est leur norme?).

Solution.

1. On the 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 de 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.
L'anneau $\mathbb{Z}[i\sqrt{5}]$.

1. Montrer que le polynôme $3 + 2t + 2t^2$ est irréductible sur $\mathbb{Z}[i\sqrt{5}]$, mais pas sur le corps des fractions de $\mathbb{Z}[i\sqrt{5}]$

2. **Généralisation.** Soient a, b, c, d des éléments irréductibles non associés d'un anneau commutatif et intègre A tels que $ab = cd$. Calculer $(a + ct)(b + ct)$ et conclure que le polynôme $d + (a + b)t + ct^2$ est irréductible sur A, mais pas sur son corps des fractions K.

3. Montrer que la norme n'est pas une fonction euclidienne sur $\mathbb{Z}[i\sqrt{5}]$.

Solution.

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 Euclidian by Proposition 3.7.1 (hence factorial by Theorem 3.7.7) it holds that every irreducible element is prime by Theorem 3.5.1. Again, since this ring is factorial, if 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. Dividing $-2 + i\sqrt{5}$ by $1 + i\sqrt{5}$ with rest and calculating the norm of the rest, we see that 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.
En s'inspirant de l'exemple 3.7.4.(3), montrer que $\mathbb{Z}[i\sqrt{2}]$ est Euclidien.

Solution.
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.
Idéaux dans un anneau de polynômes.

1. Décrire tous les idéaux premiers et tous les idéaux maximaux de $\mathbb{C}[t]$ et de $\mathbb{R}[t]$.

Pour $\mathbb{R}[t]$, montrez d'abord en utilisant que $\mathbb{C}$ est algébriquement clos et que les racines d'un polynôme réel sont closes par conjugaison, qu'un polynôme de $\mathbb{R}[t]$ se décompose toujours comme produits de polynômes dans $\mathbb{R}[t]$ de degré au plus 2.*

2. Soit K un corps et $a \in K$. Montrer que $(t-a)$ est un idéal premier de $K[s,t]$, mais non maximal. Ainsi $K[s,t]$ est un anneau factoriel mais pas principal.

3. Montrer que l'anneau quotient $\mathbb{C}[s,t]/(s-t^2)$ est principal

4. **Polynôme d'interpolation de Lagrange.** Soit K un corps, $a_1, \ldots, a_n$ des éléments de K distincts et $b_1, \ldots, b_n \in K$. Montrer qu'il existe un polynôme $f \in K[t]$ de degré au plus $n-1$ tel que $f(a_i) = b_i$ pour tout $1 \leq i \leq n$.

Solution.

For any field K, we know that by Propositions 3.7.1 and 3.7.6, $K[t]$ is a principal ideal domain (often denoted PID). By Proposition 3.6.3, the following are equivalent for an element q in a PID:

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

1. For $\mathbb{C}[t]$, we know by Example 3.2.10.(3) 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 $(ct+d)$.

   Pour $\mathbb{R}[t]$: considérons les racines complexes d'un polynôme réel $f(t)$. On les sépare en deux groupes

   (a) les racines dans $\mathbb{R}$
   (b) les racines dans $\mathbb{C} \setminus \mathbb{R}$.

   Comme $\overline{f}(t) = f(t)$ car le polynôme est réel, on voit que les racines du deuxième groupe viennent forcément par paires de conjugués, car si $\lambda \in \mathbb{C} \setminus \mathbb{R}$ est dans ce deuxième groupe, alors $\overline{\lambda} \neq \lambda$ l'est aussi. Mais notons également que $(t-\lambda)(t-\overline{\lambda}) \in \mathbb{R}[t]$, car $\lambda + \overline{\lambda}, \lambda\overline{\lambda} \in \mathbb{R}$. Ainsi on voit que tout polynôme réel se décompose comme produit de polynôme réels de degré au plus 2.

   Dès lors, on conlut que les polynômes irréductibles de $\mathbb{R}[t]$ sont

   (a) Les polynômes de degré 1,
   (b) Les polynômes de degré 2 sans racines.

   En effet tout les polynômes de degré 1 sont irréductibles et un polynôme de degré 2 l'est si et seulement si il n'a pas de racine. En effet s'il n'était pas irréductible il devrait être divisé par un polynôme de degré 1 est donc avoir une racine.

   Attention ce dernier argument ne marche pas pour les polyômes de plus haut degré. Par exemple $(t^2+1)^2$ n'a pas de racine dans $\mathbb{R}$ mais n'est pas irréductible dans $\mathbb{R}[t]$.

2. By example 2.4.10.(1), we know that $K[s,t]/(t-a) \cong K[s]$, which is a domain but not a field. Hence, $(t-a)$ is prime but not maximal.

*En effet si $f(t)$ est à coefficient réels, alors $\overline{f}(t) = f(t)$ et donc si $f(t) = \prod(t-\lambda_i)$ dans $\mathbb{C}[t]$ alors on voit que l'ensemble des racines est stable par conjugaison.

3. As above, $\mathbb{C}[s,t]/(s-t^2) \cong \mathbb{C}[t]$, which is a PID.

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.
Trouver tous les idéaux de $\mathbb{Z}[i]$ qui contiennent l'idéal (5) et tous les idéaux de $\mathbb{Z}[i]$ qui contiennent l'idéal (2).

Solution.

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.
L'objectif de cet exercice est de trouver toutes les paires $(x,y) \in \mathbb{Z}^2$ telles que $x^2+2 = y^3$. Nous allons procéder ainsi.

Fixons $x, y \in \mathbb{Z}$ tel que $x^2+2 = y^3$.

1. Montrer que 2 ne divise pas x.

2. Montrer que $\text{pgdc}(x+i\sqrt{2}, x-i\sqrt{2}) = 1$ dans l'anneau $\mathbb{Z}[i\sqrt{2}]$.

3. Montrer qu'il existe $z \in \mathbb{Z}[i\sqrt{2}]$ tel que $x+i\sqrt{2} = \pm z^3$.

4. Trouver toutes les solutions de l'équation $x^2+2 = y^3$ à valeur dans $\mathbb{Z}$.

Solution.

1. Si 2 divise x, alors 2 divise y^3, et donc 2 divise y. Posons $x = 2x_0$ et $y = 2y_0$. On a alors que
$$4x_0^2 + 2 = 8y_0^3,$$
ce qui est impossible (4 divise $4x_0^2$ et $8y_0^3$, mais pas 2).

2. Supposons que ce n'est pas le cas, et soit $d \in \mathbb{Z}[i\sqrt{2}]$ un élément irréductible tel que d divise à la fois $x + i\sqrt{2}$ et $x - i\sqrt{2}$. L'élément d divise alors
$$(x + i\sqrt{2}) - (x - i\sqrt{2}) = 2i\sqrt{2} = -(i\sqrt{2})^3.$$
Montrons que $i\sqrt{2}$ est irréductible, et soient donc $a, b \in \mathbb{Z}[i\sqrt{2}]$ tels que $ab = i\sqrt{2}$. On a alors que $N(a)N(b) = N(i\sqrt{2}) = 2$, qui est un nombre premier. Ainsi, $N(a)$ ou $N(b)$ doit valoir 1, i.e. a ou b est inversible. Ainsi, $i\sqrt{2}$ est bel et bien irréductible.

   Comme d divise $(i\sqrt{2})^3$ et que $i\sqrt{2}$ est irréductible, on a nécéssairement que $d = i\sqrt{2}$. En effet, vu que $\mathbb{Z}[i\sqrt{2}]$ est Euclidien par l'exercice 4, on sait par le cours que cet anneau est factoriel, et donc que la décomposition en facteurs irréductibles est unique.

   On a donc prouvé que d est associé à $i\sqrt{2}$, et par hypothèse celui-ci divise $x + i\sqrt{2}$. Ainsi, $i\sqrt{2}$ divise x, et donc $2 = N(i\sqrt{2})$ divise $N(x) = x^2$ (dans $\mathbb{Z}$). Comme 2 est premier dans $\mathbb{Z}$, on en déduit que 2 divise x, ce qui contredit le premier point.

3. Posons $a := x + i\sqrt{2}$ et $b = x - i\sqrt{2}$. On a par hypothèse que $ab = y^3$. Soit p un diviseur premier de y. Comme a et b sont premiers entre eux, p ne peut pas diviser a et b à la fois. Comme y^3 est un produit d'éléments premiers élevés au cube, on en déduit que c'est aussi le cas de a et b par l'unicité de la décomposition en facteurs premiers. En particulier, a est un cube à unité près.

   Or, les seuls éléments inversibles de $\mathbb{Z}[i\sqrt{2}]$ sont ± 1. En effet, ces éléments sont certainement inversibles, et dans l'autre sens si $u \in \mathbb{Z}[i\sqrt{2}]^\times$, alors $N(u) \in \mathbb{Z}^\times = \{\pm 1\}$, ce qui force $u = \pm 1$.

   Ainsi, $a = \pm z^3$ pour un certain $z \in \mathbb{Z}[i\sqrt{2}]$.

4. Remarquons que 1 et -1 sont aussi des cubes, et du coup il existe $w \in \mathbb{Z}[i\sqrt{2}]$ tel que $x + i\sqrt{2} = w^3$. Ecrivons $w = e + fi\sqrt{2}$. Alors on a
$$x + i\sqrt{2} = (e + fi\sqrt{2})^3 = (e^3 - 6ef^2) + (3e^2f - 2f^3)i\sqrt{2},$$
et donc
$$\begin{cases} x = e^3 - 6ef^2; \\ 1 = 3e^2f - 2f^3. \end{cases}$$
La deuxième équation montre que f divise 1, i.e. $f = \pm 1$. Ainsi, on a
$$1 = \pm(3e^2 - 2).$$
Si $f = -1$, on en déduirait que $3e^2 = -1$, ce qui est impossible car 3 ne divise par -1. Ainsi, $f = 1$ et donc
$$3e^2 = 3,$$
i.e. $e = \pm 1$.

   On a donc
$$x = e^3 - 6ef^2 = \pm 5.$$
Cela implique que $y^3 = 27$, et donc $y = 2$. Ainsi, les solutions de l'équation $x^2 + 2 = y^3$ dans $\mathbb{Z}^2$ sont
$$\{(5, 3), (-5, 3)\}.$$

EPFL - Printemps 2025	Prof. Zs. Patakfalvi
Anneaux et Corps	**Exercices**
Solutions 6	

Exercice 1. 1. Soit A un anneau Euclidien. Prouvez que l'algorithme d'Euclide peut être adapté pour calculer les pgdc dans A.

2. Effectuez la division avec reste de $27-23i$ par $8+i$ dans $\mathbb{Z}[i]$, et montrez que ces deux entiers de Gauss sont premiers entre eux.

3. Calculez un pgdc de $11+3i$ et de $1+8i$ dans $\mathbb{Z}[i]$. Ce pgdc est-il unique ?

4. Écrivez les idéaux $(11+3i)$ et de $(1+8i)$ comme un produit d'idéaux premiers de $\mathbb{Z}[i]$.

Solution.

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 $\dfrac{193}{65}-\dfrac{211}{65}i$. 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 $\dfrac{1 + 8i}{2 - 4i} = \dfrac{(1 + 8i)(2 + 4i)}{20} = \dfrac{-3 + 2i}{2}$ 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 $\mathbb{Z}[i]$

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

   Notez que la décomposition de 2 en termes de multiplication d'idéaux est

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

   Notons que comme les éléments dans les décompositions 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 $1 + 8i$. En effet,

$$(2i - 3)(1 - 2i) = (-3 + 4) + i(6 + 2) = 1 + 8i.$$

   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 $1 - 2i$ on conclut que

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

Exercice 2.
Notons $\mathcal{C} := C^0([0, 1]; \mathbb{R})$ l'anneau des fonctions réelles continues sur l'intervalle $[0, 1]$ (muni des opérations d'addition et de multiplication de fonctions).

1. Pour $x \in [0, 1]$, écrivons $I_x := \{f \in \mathcal{C} \mid f(x) = 0\}$. Montrez que I_x est un idéal maximal.
2. Pour $x \neq y$, montrez que $I_x \cap I_y$ n'est pas un idéal premier.
3. Soit $I \subset \mathcal{C}$ un idéal. Supposons que I n'est contenu dans aucun des I_x. Montrez que $I = \mathcal{C}$. *Indication : la propriété de Heine–Borel sera utile.*

4. Montrez que tout idéal maximal de $\mathcal{C}$ est égal à I_x pour un certain $x \in [0,1]$.

Solution.

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, cela s'appelle la "Gelfand-Kolomogorov duality".

Exercice 3.
Considérons les polynômes $f = x^3 - 2x^2 + x - 2$ et $g = x^4 - 2x^3 + 7x - 14$ dans $\mathbb{Z}[x]$.

1. Montrez que le pgdc de f et de g dans $\mathbb{Z}[x]$ vaut $x-2$ en écrivant $f = (x-2)f_0$ et $g = (x-2)g_0$ dans $\mathbb{Z}[x]$.

2. Pour un premier p, notons $\bar{f}$ et $\bar{g}$ la réduction de f et g dans $\mathbb{F}_p[x]$. Calculez le pgdc de $\bar{f}$ et de $\bar{g}$ pour chaque p.
Indication : Remarquez que les étapes de l'algorithme d'Euclide définissables dans $\mathbb{Z}[x]$ sont des étapes de l'algorithme d'Euclide dans $\mathbb{F}_p[x]$ après réduction modulo p.

Solution.

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, ces 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 $\mathbb{Q}$), et donc ils sont irréductibles en vertu du lemme de Gauss III. 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
$$\operatorname{pgdc}(x^2 + [1]_p, x^3 + [7]_p) = -x + [7]_p \quad \text{et ainsi} \quad \operatorname{pgdc}(\bar{f}, \bar{g}) = (x - [2]_p)(-x + [7]_p).$$
   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 $\operatorname{pgdc}(\bar{f}, \bar{g}) = x - [2]_p$.
   (b) Si $p = 2$, alors $\operatorname{pgdc}(\bar{f}, \bar{g}) = x(x + [1]_2)$.
   (c) Si $p = 5$, alors $\operatorname{pgdc}(\bar{f}, \bar{g}) = (x - [2]_5)(-x + [2]_5)$.

Exercice 4. 1. Soit $d > 0$ un entier positif. Montrez que $\mathbb{Q}[i\sqrt{d}]$ est un corps de fractions de $\mathbb{Z}[i\sqrt{d}]$.

2. Montrez que $x^3 - 2i$ est irréductible dans $(\mathbb{Z}[i])[x]$.
Indication : Utilisez le lemme de Gauss, et gardez en tête qu'un élément de $\mathbb{Q}[i]$ peut s'écrire comme $\frac{a+bi}{n}$ avec $a, b, n \in \mathbb{Z}$.

Solution.

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 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 $\mathbb{Z}[i][x]$.

   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, comme il est de norme 2.

Exercice 5.
Soit k un corps.

1. Montrez que le sous-anneau $k[t^2, t^3] \subset k[t]$ n'est pas factoriel.
2. De même, montrez que $k[t^2, t^5]$ et $k[t^3, t^7]$ ne sont pas factoriels.
3. Montrez que $k[x, y]/(x^2 - y^3)$ n'est pas factoriel.
   Indication : Montrez que cet anneau est isomorphe à l'un des anneaux considérés précédemment.

Solution.

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.

On aurait aussi pu montrer montrer l'inclusion $\ker(\varphi) \subseteq (x^2+y^3)$ en utilisant le lemme suivant :

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.
Considérons l'anneau de matrices

$$A := \left\{ \begin{pmatrix} n & x \\ 0 & y \end{pmatrix} \mid n \in \mathbb{Z},\ x, y \in \mathbb{Q} \right\}$$

ainsi que le sous-ensemble

$$I := \left\{ \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} \mid x \in \mathbb{Q} \right\} \subset A.$$

1. Montrez que I est un idéal bilatère, que $A/I \cong \mathbb{Z} \times \mathbb{Q}$ et que A/I est Noethérien.
2. Montrez que I est un idéal à droite minimal (c'est-à-dire qu'il n'existe pas d'idéal à droite J tel que $0 \subsetneq J \subsetneq I$).
3. Montrez que A est Noethérien à droite.
   Indication : Etant donnée une chaîne croissante d'idéaux, considérez son image par l'application quotient $A \to A/I$.

Solution.

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, 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

$$J_1 \subseteq J_2 \subseteq \dots$$

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

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

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 ($\star$).
Soit $A = \mathbb{Z}[i\sqrt{d}]$ pour un $d \geq 1$. Pour un $a+bi\sqrt{d} \in \mathbb{Z}[i\sqrt{d}]$ on pose la norme $N(a+bi\sqrt{d}) = a^2+db^2$

1. Soit $x \in A$ non-nul. Montrer que

$$|A/(x)| = N(x).$$

(C'est à dire que la cardinalité du quotient est égale à la norme de x.)

Remarquer que A est un groupe abélien libre de rang 2 et que le quotient $A/(x)$ est égal au quotient de A par l'image de l'application linéaire $\cdot x : A \to A$, et utiliser la forme normale de Smith pour conclure.

Dans les points 2. et 3., on considère (B, σ) un anneau euclidien quelconque qui n'est pas un corps.

2. Montrer que si $b \in B$ est non-nul tel que $\sigma(b) = 0$, alors b est inversible.

3. Montrer qu'il existe un $b \in B$ non-nul et non inversible tel que

$$|B/(b)| \leq |B^\times| + 1.$$

4. Montrer que si $d > 3$, alors A n'est pas Euclidien. (Il ne s'agit pas de montrer que N n'est pas une fonction Euclidienne pour A, mais qu'il n'en existe aucune.)

Solution.

1. Prenons $x = a + bi\sqrt{d} \in A$ non-nul. On prend $(1, i\sqrt{d})$ comme $\mathbb{Z}$-base de A. Dès-lors il suit que la matrice de $\cdot x$ dans cette base est

$$\begin{pmatrix} a & -db \\ b & a \end{pmatrix}.$$

Le déterminant de cette matrice qui est égal $a^2 + bd^2 = N(x)$. Par la forme normale de Smith, il existe des automorphismes de groupes abéliens $f, g : A \to A$ tel que $f \circ (\cdot x) \circ g$ est sous forme diagonale dans la base $(1, i\sqrt{d})$. Soit donc $\alpha_1, \alpha_2 \in \mathbb{Z}$ tel que la matrice soit de forme,

$$\begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix}.$$

avec donc $|\alpha_1\alpha_2| = N(x)$. Ainsi on peut identifier $A/(x)$ *en tant que groupe abélien* à

$$\mathbb{Z}/\alpha_1\mathbb{Z} \oplus \mathbb{Z}/\alpha_2\mathbb{Z}$$

ce qui conclut. (Noter que comme le déterminant est non nul α_1 et α_2 sont aussi non-nuls, et donc ces groupes sont finis, de cardinal $|\alpha_1\alpha_2|$.)

2. 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 $r = 0$.

3. Soit b non-inversible de norme minimale (on a $\sigma(b) > 0$, car sinon b serait inversible par le point précédent). Soit $a \in B$, et soient $q, r \in B$ tels que

$$a = bq + r.$$

Par hypothèse sur b, on a $\sigma(r) = 0$, et donc r est inversible ou nul par le point précédent. Comme $a \equiv r$ modulo b, on conclut la preuve.

4. Supposons par l'absurde que A soit Euclidien. Soit dès lors un élément $x = a + bi\sqrt{d} \in A$ comme au point précédent. Avec la norme multiplicative $N : A \to \mathbb{N}$, on voit que les seuls inversibles de A sont 1 et -1. Dès lors, une combinaison deux deux points précédents donne,

$$1 < a^2 + b^2 d \leq 3.$$

Comme $d > 3$ on voit que $b = 0$. Comme 2 et 3 ne sont pas des carrés d'entiers, on aboutit à une contradiction.

Exercice 1. (a) Soit A un anneau intègre. Si $a_1, \ldots, a_n \in A$ sont des racines distinctes de $f(x) \in A[x]$, montrer que $\prod_{i=1}^{n}(x - a_i)$ divise $f(x)$.

(b) Soient p et q deux nombres premiers distincts dans $\mathbb{Z}$. Montrer que le polynôme $t^2 - t$ de $(\mathbb{Z}/pq\mathbb{Z})[t]$ possède quatre racines distinctes $a_1, a_2, a_3, a_4 \in \mathbb{Z}/pq\mathbb{Z}$, mais que $(t - a_1)(t - a_2)(t - a_3)(t - a_4)$ ne divise pas $t^2 - t$.

(c) Soient $f, g \in \mathbb{Z}[t]$ des polynômes primitifs. Montrer que si f divise g dans $\mathbb{Q}[t]$, alors f divise g dans $\mathbb{Z}[t]$.

(d) Décomposer les polynômes $t^4 + 1$ et $t^8 - 1$ en facteurs irréductibles dans les anneaux $\mathbb{C}[t]$, $\mathbb{R}[t]$, $\mathbb{Q}[t]$, $\mathbb{Z}[t]$, $\mathbb{F}_2[t]$ et $\mathbb{F}_7[t]$.

Solution.

(a) On mène la division euclidienne de $f(x)$ par $x - a_1$ pour obtenir un $f_1(x) \in A[x]$ tel que

$$f(x) = (x - a_1)f_1(x) + a$$

pour $a \in A$. En évaluant en a_1, on obtient que $a = 0$. *Maintenant, on utilise de manière cruciale que A est intègre* pour voir que pour $i \geq 2$ on a $f_1(a_i) = 0$. En effet en évaluant en a_i on a

$$0 = (a_i - a_1)f_1(a_i),$$

et donc comme $a_1 \neq a_i$ et que A est intègre, on voit que $f_1(a_i) = 0$. Ainsi, on peut continuer par récurence sur $2 \leq i \leq p + 1$ obtenir par le même procédé que

$$f(x) = (x - a_1) \cdots (x - a_n)g(x)$$

pour un $g(x) \in A[x]$.

(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 $\mathbb{F}_7$ are $[0]_7, [1]_7, [2]_7, [4]_7$ and $[9]_7$ and we deduce that $x^4+[1]_7$ does not admit roots in $\mathbb{F}_7$. But it can still be possible that $x^4+[1]_7$ admits a decomposition into a product of two polynomials of degree 2. It is the case: indeed, as

$$([3]_7)^2 = [2]_7$$

we see from the above decomposition that

$$x^4+1 = (x^2+[3]_7x+1)((x^2-[3]_7x+1)).$$

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 $\mathbb{F}_7[x]$ we have: $x^4-[1]_7 = (x^2+[1]_7)(x-[1]_7)(x+[1]_7)$, where we have seen earlier that $x^2+[1]_7$ is irreducible.

Exercice 2 (Polynômes irréductibles I). (a) Montrer que $\frac{2}{9}x^5+\frac{5}{3}x^4+x^3+\frac{1}{3}$ est un polynôme irréductible de $\mathbb{Q}[x]$.

(b) Montrer que $x^4+[2]_5$ est un polynôme irréductible de $\mathbb{F}_5[x]$ et conclure que x^4+15x^3+7 est un polynôme irréductible de $\mathbb{Q}[x]$.

(c) Montrer que x^2+y^2+1 est un polynôme irréductible de $\mathbb{R}[x,y]$.

(d) Montrer que $x^2+y^2+[1]_2$ n'est pas un polynôme irréductible de $\mathbb{F}_2[x,y]$.

(e) Montrer que $y^4+x^3+x^2y^2+xy+2x^2-x+1$ est un polynôme irréductible de $\mathbb{Q}[x,y]$.

(f) Montrer que $4x^3+120x^2+8x-12$ est un polynôme irréductible de $\mathbb{Q}[x]$.

(g) Montrer que t^6+t^3+1 est un polynôme irréductible de $\mathbb{Q}[t]$.

(h) Montrer que $y^4+xy^3+xy^2+x^2y+3x^2-2x$ est un polynôme irréductible de $\mathbb{Q}[x,y]$.

Solution.

(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 $d = [2]_5 b^{-1}$ 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

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

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 3 (Polynômes irréductibles II).
Soit $f(t) = t^4 + 4t^3 + 3t^2 + 7t - 4$ dans $\mathbb{Z}[t]$.

(a) Montrer que $\pi_2(f)$, la réduction modulo 2, n'est pas irréductible.

(b) Montrer que $\pi_3(f)$, la réduction modulo 3, n'est pas irréductible.

(c) Utiliser les décompositions des parties précédentes pour conclure néanmoins que f est irréductible.

Solution.
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 4.
Soit K un corps et L une extension quadratique, i.e. $[L : K] = 2$.

1. Montrez que toute extension de K de degré 1 est égale à K.
2. Montrez qu'il existe un élément $\alpha \in L$ tel que $L = K(\alpha)$.
3. Soit K de caractéristique différente de 2. Montrez qu'il existe un élément $\delta \in L$ avec $\delta^2 = d \in K$ tel que $L = K(\delta) = K(\sqrt{d})$.
4. Soit M une extension de K et $\delta \in M \setminus K$ un élément avec $\delta^2 \in K$. Montrez que $K(\delta)$ est une extension quadratique de K.

Solution.

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 5.
Soient $a, b \in \mathbb{Z}$.

1. Quand est-ce que les corps $\mathbb{Q}(\sqrt{a})$ et $\mathbb{Q}(\sqrt{b})$ sont isomorphes en tant que $\mathbb{Q}$-espaces vectoriels?
2. Quand est-ce que les corps $\mathbb{Q}(\sqrt{a})$ et $\mathbb{Q}(\sqrt{b})$ sont isomorphes en tant que corps?

Solution.

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 6. 1. Soit L une extension de K avec $[L : K]$ impair. Montrer que $K(\alpha) = K(\alpha^2)$ pour tout $\alpha \in L \setminus K$.

2. Soient $p, q \in \mathbb{Z}$ deux nombres premiers distincts. Montrez que $\sqrt{p} \notin \mathbb{Q}(\sqrt{q})$ et $\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$. Calculez $[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}]$.

3. Soit L une extension de K et soient $\alpha, \beta \in L$ des éléments tels que $[K(\alpha) : K] = m$ et $[K(\beta) : K] = n$ sont premiers entre eux. Montrer que $[K(\alpha, \beta) : K] = mn$.

Solution.

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.

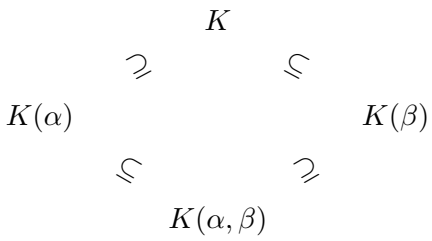
Secondly, $[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}(\sqrt{p})] = 2$. This holds because $\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$. Therefore, the degree of the extension is not equal to 1. Furthermore, the degree of the extension is at most 2, since $\sqrt{q}^2 = q \in \mathbb{Q}$, and hence $\sqrt{q}^2 \in \mathbb{Q}(\sqrt{p})$. 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 1.
Soit $K = \mathbb{Q}(\sqrt{3}+\sqrt{7})$. Montrez que $[K : \mathbb{Q}] = 4$.

Solution. 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 2.
Dans tous les cas suivants, calculez le degré de l'extension.

1. $[\mathbb{R}(e^{2i\pi/p}) : \mathbb{R}]$ pour p un nombre premier;
2. $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ pour α une racine de $t^{42}+t^{41}+\cdots+t^2+t+1$;
3. $[\mathbb{Q}(i, \sqrt[5]{13}) : \mathbb{Q}]$;
4. $[\mathbb{F}_3(\alpha) : \mathbb{F}_3]$ où α est une racine de $t^4-t^3-t^2-t-[1]_3 \in \mathbb{F}_3[t]$ (disons que α vit dans le corps de décomposition de ce polynôme sur $\mathbb{F}_3$ pour fixer les idées) La réponse peut changer en fonction de la racine considérée.
5. $[\mathbb{Q}(\sqrt{14+6\sqrt{5}}, \sqrt{3}) : \mathbb{Q}]$ (on pourra calculer $(3+\sqrt{5})^2$ pour commencer);
6. $[\mathbb{Q}(\sqrt[6]{7}) : \mathbb{Q}((\sqrt[6]{7})^2)\,]$;
7. $[\mathbb{F}_2(\alpha) : \mathbb{F}_2(\alpha^2)\,]$ où α est une racine de $t^3+t+[1]_2 \in \mathbb{F}_2[t]$.

Solution.

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 3. 1. Considérons la situation suivante:

- $\phi : K \to K'$ est un isomorphisme des corps,
- $K \subseteq L$ et $K' \subseteq L'$ sont deux extensions de corps
- $L = K(\alpha)$ et $L' = K'(\alpha')$ avec α et α' algébriques sur K et K' respectivement
- si $\xi : K[x] \to K'[x]$ est l'isomorphisme induit par ϕ, alors $\xi(m_{\alpha,K}) = m_{\alpha',K'}$

Démontrez qu'il existe une extension unique de ϕ à un isomorphisme $\eta : L \to L'$ tel que $\eta(\alpha) = \alpha'$

2. Démontrez que $K(x)[\sqrt{x+1}] \cong K(x)[\sqrt{x+2}]$
3. Démontrez que $K(x,y)[\sqrt{xy}] \cong K(x,y)[\sqrt{x(x+y)}]$

Solution.

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 $L \cong L'$, so we have proven the existence of η. The uniqueness follows from the fact L is generated by K and α by definition, so knowing the image of K and that of α entirely determines the image of L.

2. Consider the ϕ: $K(x) \to K(x)$ 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 $x \mapsto x-1$.

Let $K = K' = K(x)$, $L = K(x)(\sqrt{x+1})$ and $L' = K(x)[\sqrt{x+2}]$. Then ϕ sends the minimal polynomial of $\sqrt{x+1}$ to that of $\sqrt{x+2}$, so by (1) we deduce that $L \cong L'$.

3. Use point (1) and the same idea as in (2) 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 4.
Soit $\xi = e^{\frac{2\pi i}{n}}$ pour un entier $n > 2$. Démontrez que les corps de décomposition de $x^n - 2$ et de $x^{2n} - 3x^n + 2$ sur $\mathbb{Q}$ sont isomorphes entre eux, et aussi isomorphes à

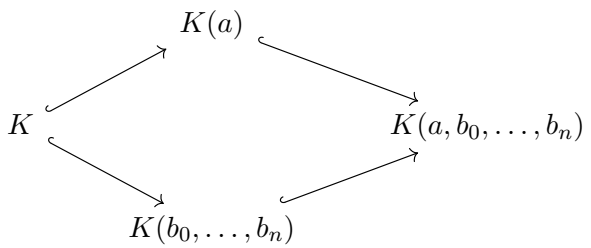
$$\mathbb{Q}(\xi, \sqrt[n]{2}) \subseteq \mathbb{C}.$$

Solution. 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 Corollary 4.3.5 that the splitting fields are the same and they are given by $\mathbb{Q}(\xi, \sqrt[n]{2})$.

Exercice 5.
Soient $K \subset L \subset F$ des extensions de corps. Si $K \subset L$ et $L \subset F$ sont algébriques, montrez qu'il en est de même pour $K \subset F$.

Solution. 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 $b_0, \ldots, b_n \in L$ tels que $m_{a,L}(t) = \sum_{i=0}^{n} b_i t^i$. En particulier, a est algébrique sur le sous-corps $K(b_0, \ldots, b_n)$.

Nous allons comparer les deux chaînes d'extensions suivantes :



On prétend que les degrés

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

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

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

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

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

On en déduit que l'extension intermédiaire $K \subset K(a) \subset K(a, b_0, \ldots, b_n)$ 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 6.
Soit $\mathbb{Q}(x)$ le corps de fractions de l'anneau polynomial $\mathbb{Q}[x]$, et considérons

$$s := \frac{x^3 + 2}{x} \in \mathbb{Q}(x).$$

On a les extensions successives $\mathbb{Q} \subset \mathbb{Q}(s) \subset \mathbb{Q}(x)$.

1. Montrez que $\mathbb{Q}(x)$ est une extension algébrique de $\mathbb{Q}(s)$.
2. Calculez $[\mathbb{Q}(s) : \mathbb{Q}]$ et $[\mathbb{Q}(x) : \mathbb{Q}(s)]$.

Solution. 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 $[\mathbb{Q}(x) : \mathbb{Q}(s)] = 3$.

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.

Voici une autre méthode pour montrer que ce polynôme est irréductible. 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.

Exercice 7.
Soit $f = x^7 - y^5 \in \mathbb{C}[x, y]$. Le but de cet exercice est de démontrer que f est irréductible dans $\mathbb{C}[x, y]$. Soit $K = \mathbb{C}(y)$ et L le corps de décomposition de f sur K. Soit α une racine de f dans L, et $\beta = \frac{\alpha^3}{y^2}$.

1. Montrez que $[K(\beta) : K] = 7$. *Indication: Trouvez un polynôme sur K dont β est une racine.*
2. Montrez que $K(\beta) = K(\alpha)$.
3. Déduisez que f est irréductible dans $\mathbb{C}[x, y]$.

Solution.

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 $m_{\alpha,K} | x^7 - y^5$. 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 1.
Soit $n > 0$ un entier positif. Montrez que $\cos(2\pi/n)$ et $\sin(2\pi/n)$ sont des nombres algébriques sur $\mathbb{Q}$.

Solution.
Comme (formules de partie réelles et imaginaires d'un nombre complexe)

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

on voit que $\cos(2\pi/n), \sin(2\pi/n) \in \mathbb{Q}(i, e^{2\pi i/n})$, ce qui conclut.

Exercice 2.
Soit $\alpha \in \mathbb{F}_{27}^\times$ un élément différent de 1 et -1. Montrer que soit α, soit $-\alpha$, est un générateur du groupe cyclique $\mathbb{F}_{27}^\times$.

Solution.
Comme $26 = 13 * 2$ l'ordre multiplicatif d'un élément est $1, 2, 13$ ou 26. Comme $\alpha \neq 1, -1$ et que ces éléments sont les seuls d'ordre 1 et 2 respectivement, l'ordre de α est 13 ou 26. Si α est d'ordre 26, c'est un générateur. S'il est d'ordre 13, alors $(-\alpha)^{13} = -1$. Il suit que $-\alpha$ est d'ordre 26.

Exercice 3.
Fixons un nombre premier p.

1. Pour $r > 0$, énumérez les sous-corps de $\mathbb{F}_{p^r}$. Si s divise r, énumérez les corps intermédiaires $\mathbb{F}_{p^s} \subseteq L \subseteq \mathbb{F}_{p^r}$.

2. Montrez que l'ensemble $\{0 \neq a \in \mathbb{F}_{16} \mid \mathbb{F}_2(a) = \mathbb{F}_{16} \text{ et } \langle a \rangle \neq \mathbb{F}_{16}^\times\}$ possède 4 éléments. Ici $\langle a \rangle$ désigne le sous-groupe de $\mathbb{F}_{16}^\times$ généré par l'élément $a \neq 0$.
Indication : Etudiez la structure du groupe $\mathbb{F}_{16}^\times$.

3. Plus généralement, montrez que l'ensemble $\{0 \neq a \in \mathbb{F}_{p^4} \mid \mathbb{F}_p(a) = \mathbb{F}_{p^4} \text{ et } \langle a \rangle \neq \mathbb{F}_{p^4}^\times\}$ possède $p^4 - p^2 - \varphi(p^4 - 1)$ éléments, où φ est la fonction de comptage d'Euler.

Solution.

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

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

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 4 (Corps de décomposition sur $\mathbb{F}_p$)**.**
Fixons un nombre premier $p > 0$ et un polynôme $f(x) \in \mathbb{F}_p[x]$ irréductible de degré d.

1. Montrez que f divise $x^{p^d} - x$ dans $\mathbb{F}_p[x]$.
   Indication : A l'aide du Théorème fondamental des corps finis, montrez que $\mathbb{F}_{p^d}$ contient une racine de f.

2. Montrez que $f(x)$ se scinde sur $\mathbb{F}_{p^d}$.

3. Montrez que f n'a pas de racines multiples.

4. Soit $g \in \mathbb{F}_p[x]$ un polynôme irréductible de degré d qui n'est pas associé à f. Montrez que f et g n'ont pas de racines en commun.

5. Montrez que
$$x^{p^d} - x = \prod_{\substack{h \text{ unitaire irréd.} \\ \text{dans } \mathbb{F}_p[x] \\ \deg h \text{ divise } d}} h.$$

Solution.

1. Comme $\mathbb{F}_p[x]/(f)$ est un corps de cardinal p^d, on sait qu'il est isomorphe à $\mathbb{F}_{p^d}$ par le théorème de classification des corps finis. Mais alors, il suit que f a une racine $\alpha \in \mathbb{F}_{p^d}$. Dès lors, on peut supposer quitte à rendre $f(x)$ unitaire que $m_\alpha(x) = f(x)$ car $f(x)$ est supposé irréductible. Mais comme $\alpha^{p^d} = \alpha$ car $\alpha \in \mathbb{F}_{p^d}$, on obtient donc $f(x) = m_\alpha(x) \mid x^{p^d} - x$, concluant.

2. Le Théorème fondamental des corps finis 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 fondamental des corps finis 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. Si par l'absurde α est une racine commune, alors $m_\alpha(x)$ divise tant bien f que g. Par suite, comme ces polynômes sont supposés irréductibles, on voit que ceux-ci sont associés.

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 5.
Soit $f(t) \in \mathbb{F}_p[t]$ un polynôme de degré n. Montrez que $f(t)$ est irréductible si et seulement si $f(t)$ n'a pas de racines dans $\mathbb{F}_{p^k}$ pour tout $1 \leq k \leq \lfloor \frac{n}{2} \rfloor$.

Une application de ce principe permet de montrer que $t^4 + 2 \in \mathbb{F}_5[t]$ est irréductible (voir Série 7.2.(b)). En effet, montrez qu'une racine α de ce polynôme a pour ordre multiplicatif* 16, mais que cela n'est pas possible pour des éléments de $\mathbb{F}_{25}$.

Solution.
Si $f(t)$ n'est pas irréductible alors il existe $g(t)$ irréductible de degré $k \leq \lfloor n/2 \rfloor$ qui divise $f(t)$. Or, $g(t)$ a une racine sur $\mathbb{F}_{p^k}$ car

$$\mathbb{F}_p[t]/(g(t)) \cong \mathbb{F}_{p^k}.$$

Réciproquement si $f(t)$ a une racine α dans $\mathbb{F}_{p^k}$ pour $k \leq \lfloor n/2 \rfloor < n$, alors $m_\alpha(t)$ le polynôme minimal de α divise f, mais $m_\alpha(t)$ est degré inférieur ou égal à k car $\mathbb{F}_p(\alpha) \subset \mathbb{F}_{p^k}$. Ainsi on a trouvé un polynôme non-constant de degré strictement inférieur à n divisant f, ce qui montre que f n'est pas irréductible.

Une racine de $t^4 + 2$ dans $\mathbb{F}_5[t]$ satisfait $\alpha^4 = 3$. Cependant, l'ordre multiplicatif de 3 dans $\mathbb{F}_5$ est 4, donc il suit que l'ordre multiplicatif de de α est 16. Mais comme 16 ne divise pas 24, on voit que α ne peut être un élément de $\mathbb{F}_{25}$.

Exercice 6 (Polynômes irréductibles sur $\mathbb{F}_p$)**.**
Fixons un nombre premier $p > 0$. Nous allons calculer le nombre N_d de polynômes irréductibles unitaires d'un degré fixé sur $\mathbb{F}_p$. (Rappelons qu'un polynôme est unitaire si son coefficient dominant vaut 1).

1. Montrez que

$$d \cdot N_d = \left| \mathbb{F}_{p^d} \setminus \bigcup_{L \subsetneq \mathbb{F}_{p^d}} L \right|$$

où L parcourt l'ensemble des sous-corps strictement inclus dans $\mathbb{F}_{p^d}$.
Indication : Utilisez les résultats de l'Exercice 4 et le Théorème fondamental des corps finis.

2. Montrez que

$$N_2 = \frac{p^2 - p}{2}, \quad N_3 = \frac{p^3 - p}{3}, \quad N_4 = \frac{p^4 - p^2}{4}, \quad N_5 = \frac{p^5 - p}{5}, \quad N_6 = \frac{p^6 - p^3 - p^2 + p}{6}.$$

*Plus petit entier n tel que $\alpha^n = 1$.

Pour établir une formule générale, il sera utile d'introduire la **fonction de Möbius**. Il s'agit de la fonction

$$\mu\colon \mathbb{N}_{>0} \longrightarrow \{-1, 0, 1\}$$

définie par

$$\mu(n) = \begin{cases} 0 & \text{si } n \text{ est divisible par } p^2 \text{ pour un premier } p, \\ 1 & \text{si } n = 1 \text{ ou si } n \text{ est le produit d'un nombre pair de premiers distincts,} \\ -1 & \text{si } n \text{ est le produit d'un nombre impair de premiers distincts.} \end{cases}$$

Ceci étant, passons au cas général :

3. Si n, m divisent d et sont premiers entre eux, montrez que $\mathbb{F}_{p^{d/n}} \cap \mathbb{F}_{p^{d/m}} = \mathbb{F}_{p^{d/nm}}$ dans $\mathbb{F}_{p^d}$.

4. Montrez que
$$N_d = \frac{1}{d} \sum_{r|d} \mu\left(\frac{d}{r}\right) p^r.$$

   Indication : Soit $d = s_1^{i_1} \cdots s_n^{i_n}$ la décomposition en produit de nombres premiers. Montrez d'abord que
$$dN_d = \left| \mathbb{F}_{p^d} \setminus \bigcup_{j=1}^{n} \mathbb{F}_{p^{d/s_j}} \right|$$
   puis développez le terme de droite grâce à la formule d'inclusion-exclusion.

Solution. 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

$$\begin{aligned} dN_d &= \left|\mathbb{F}_{p^d}\right| - \left|\bigcup_{j=1}^{n} F_j\right| \\ &= p^d - \sum_{t=1}^{n} (-1)^{t+1} \sum_{j_1 < \cdots < j_t} |F_{j_1 \dots j_t}| \\ &= p^d - \sum_{t=1}^{n} (-1)^{t+1} \sum_{j_1 < \cdots < j_t} p^{d/s_{j_1} \cdots s_{j_t}} \\ &= \sum_{t=0}^{n} (-1)^{t} \sum_{j_1 < \cdots < j_t} p^{d/s_{j_1} \cdots s_{j_t}} \end{aligned}$$

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.

EPFL - Printemps 2025	Prof. Zs. Patakfalvi
Anneaux et Corps	**Exercices**
Solutions 10	

Exercice 1. 1. Montrez que $1, \sqrt[3]{2}, \sqrt[3]{4}$ est une $\mathbb{Q}$ base de $\mathbb{Q}(\sqrt[3]{2})$.

2. Écrivez la matrice de la multiplication par

$$1 + \sqrt[3]{2} + \sqrt[3]{4},$$

vue comme application linéaire $\mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2})$. Calculez le polynôme caractéristique de cette matrice et déduisez en le polynôme minimal de l'élément ci-dessus.

Solution. Le premier point suit par exemple de l'isomorphisme $\mathbb{Q}[t]/(t^3-2) \cong \mathbb{Q}(\sqrt[3]{2})$ par $t \mapsto \sqrt[3]{2}$. Dans la description par quotient, on voit que l'image de $1, t, t^2$ forme une $\mathbb{Q}$-base.

Pour le deuxième point, la matrice est

$$\begin{pmatrix} 1 & 2 & 2 \\ 1 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix}.$$

Le polynôme caractéristique de cette matrice est

$$X^3 - 3X^2 - 3X - 1.$$

Par Cayley-Hamilton l'endomorphisme de multiplication par $1 + \sqrt[3]{2} + \sqrt[3]{4}$ est annulé par ce polynôme. En évaluant en 1 cet endormophisme, on conclut que $1 + \sqrt[3]{2} + \sqrt[3]{4}$ est un zéro de ce polynôme. Comme $1 + \sqrt[3]{2} + \sqrt[3]{4} \notin \mathbb{Q}$ on a forcément que $\mathbb{Q}(1 + \sqrt[3]{2} + \sqrt[3]{4}) = \mathbb{Q}(\sqrt[3]{2})$ car comme $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ il n'y a pas de sous-extensions propres car le degré d'une sous-extension propre diviserait 3. Ainsi le degré du polynôme minimal de $1 + \sqrt[3]{2} + \sqrt[3]{4}$ est 3, ce qui conclut.

Exercice 2.
Décrivez le groupe $\mathrm{Gal}(K/\mathbb{Q})$ dans les cas suivants: $K = \mathbb{Q}(i), \mathbb{Q}(\sqrt{7}), \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\xi)$ où $\xi = e^{2i\pi/3}$.

Solution.

Pour toutes les extensions sauf $\mathbb{Q}(\sqrt[3]{2})$, on est dans un cas de forme $\mathbb{Q}(\alpha)$ avec le polynôme minimal de α de degré 2. Notons α' l'autre racine et $m(t) \in \mathbb{Q}[t]$ le polynôme minimal. En utilisant l'exercice 4 de la Série 7, on voit que $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha')$. Dès lors

$$\mathbb{Q}(\alpha) \xleftarrow{\mathrm{ev}_\alpha} \mathbb{Q}[t]/(m(t)) \xrightarrow{\mathrm{ev}_{\alpha'}} \mathbb{Q}(\alpha')$$

est un automorpshime non trivial, comme il envoie $\alpha \mapsto \alpha'$. Par le dernier point de la Proposition 4.6.4 on déduit que $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ est cyclique d'ordre 2.

En plongeant $\mathbb{Q}(\sqrt[3]{2})$ dans le corps de décomposition de $x^3 - 2$ on voit qu'un automorphisme doit envoyer $\sqrt[3]{2}$ sur une autre racine de $x^3 - 2$. Mais comme la seule racine de $x^3 - 2$ contenue dans $\mathbb{Q}(\sqrt[3]{2})$ est $\sqrt[3]{2}$ on conclut que $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ est réduit à l'identité.

Exercice 3.
Soit $\xi = e^{\frac{2\pi i}{3}}$. Considérons

$$\mathbb{Q}(\xi, \sqrt[3]{2}) \subseteq \mathbb{C},$$

un corps de décomposition de $x^3 - 2$. (Voir série 8, exercice 4).

On attire l'attention sur le point (3) de la Proposition 4.6.4. Que le groupe $\mathrm{Gal}(L/K)$ *agit transitivement sur les racines d'un polynôme minimal est un théorème* d'existence. *En effet étant donné des racines* α_1, α_2 *d'un polynôme minimal, la transitivité signifie qu'il existe* $\phi \in \mathrm{Gal}(L/K)$ *tel que* $\phi(\alpha_1) = \alpha_2$.

1. Montrez qu'il existe $\phi \in \mathrm{Gal}(\mathbb{Q}(\xi, \sqrt[3]{2})/\mathbb{Q})$ tel que $\phi(\xi) = \xi$ et $\phi(\sqrt[3]{2}) = \xi\sqrt[3]{2}$. Quel est l'ordre de ϕ ?

2. Montrez qu'il existe $\psi \in \mathrm{Gal}(\mathbb{Q}(\xi, \sqrt[3]{2})/\mathbb{Q})$ avec $\psi(\xi\sqrt[3]{2}) = \xi^2\sqrt[3]{2}$ et $\psi(\sqrt[3]{2}) = \sqrt[3]{2}$. Quel est l'ordre de ψ ?

3. En utilisant l'action de $\mathrm{Gal}(\mathbb{Q}(\xi, \sqrt[3]{2})$ sur les racines de $x^3 - 2$ et la Proposition 4.6.4 du cours, déduisez que $\mathrm{Gal}(\mathbb{Q}(\xi, \sqrt[3]{2}) \cong S_3$.

4. Raisonnez similairement pour calculer les groupes de Galois des extensions $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ et $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

Solution.

1. On considère l'extension
$$\mathbb{Q}(\xi) \subset \mathbb{Q}(\xi, \sqrt[3]{2}).$$
Comme $\mathbb{Q}(\xi, \sqrt[3]{2})$ est le corps de décomposition de $x^3 - 2 \in \mathbb{Q}(\xi)[x]$, on peut appliquer le point (3) de la Proposition 4.6.4 pour avoir l'existence d'un $\phi \in \mathrm{Gal}(\mathbb{Q}(\xi, \sqrt[3]{2})/\mathbb{Q}(xi))$ tel que $\phi(\sqrt[3]{2}) = \xi\sqrt[3]{2}$.

   Explicitement, on peut construire cet automorphisme de la manière suivante.

   On étend l'identité sur $\mathbb{Q}(\xi)$ en utilisant les évaluations
$$\mathbb{Q}(\xi, \sqrt[3]{2}) \xleftarrow{\mathrm{ev}_{\sqrt[3]{2}}} \mathbb{Q}(\xi)[t]/(t^3 - 2)) \xrightarrow{\mathrm{ev}_{\xi\sqrt[3]{2}}} \mathbb{Q}(\xi, \sqrt[3]{2})$$
   le polynôme $t^3 - 2$ étant irréductible dans $\mathbb{Q}(\xi)$ car il n'a pas de racines. En effet toute racine de ce polynôme est de degré 3 sur $\mathbb{Q}$ et ne peut donc être contenue dans $\mathbb{Q}(\xi)$ qui est une extension de degré 2.

2. Comme $\mathbb{Q}(\xi, \sqrt[3]{2})$ est le corps de décomposition de $x^2 + x + 1 \in \mathbb{Q}(\sqrt[3]{2})[x]$, on peut appliquer le point (3) de la Proposition 4.6.4 pour avoir l'existence d'un $\psi \in \mathrm{Gal}(\mathbb{Q}(\xi, \sqrt[3]{2})/\mathbb{Q}(\sqrt[3]{2}))$ tel que $\psi(\xi) = \xi^2$ et $\psi(\xi\sqrt[3]{2}) = \xi^2\sqrt[3]{2}$.

   Solution commune aux points 1. et 2. On sait comme $\mathbb{Q}(\xi, \sqrt[3]{2})$ est un corps de décomposition d'un polynôme séparable, qu'elle est Galoisienne et donc que
$$|\mathrm{Gal}(\mathbb{Q}(\xi, \sqrt[3]{2})/\mathbb{Q})| = 6.$$
   Aussi, on sait que si $\phi \in \mathrm{Gal}(\mathbb{Q}(\xi, \sqrt[3]{2})$ alors forcément
$$\phi(\xi) = \xi, \xi^2 \quad \phi(\sqrt[3]{2}) = \sqrt[3]{2}, \xi\sqrt[3]{2}, \xi^2\sqrt[3]{2}.$$
   Comme on dénombre 6 possibilités d'automorphismes, elles sont forcément toutes réalisées. Cela démontre les points 1. et 2. simultanément.

3. Par le point (2) de la Proposition mentionnée on a un morphisme injectif $\mathrm{Gal}(\mathbb{Q}(\xi, \sqrt[3]{2})/\mathbb{Q}) \to S_3$. Mais par le quatrième point, on sait que $\mathrm{Gal}(\mathbb{Q}(\xi, \sqrt[3]{2})$ a $[\mathbb{Q}(\xi, \sqrt[3]{2}) \colon \mathbb{Q}] = 6$ éléments ce qui conclut.

4. Commençons par remarquer que les éléments de $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q})$ doivent envoyer $\sqrt{i} \mapsto \pm\sqrt{i}$ pour $i = 2, 3, 5$. En effet par le point 1 de la Proposition 4.6.4 les racines de (t^2-2) et (t^2-3) et $(t^2 - 5)$ sont respectivement permutées. Ainsi, on voit qu'on au plus 4 (respectivement 8) automorphismes entièrement déterminés par $\sqrt{2} \mapsto \pm\sqrt{2}$ et $\sqrt{3} \mapsto \pm\sqrt{3}$ et $(\sqrt{5} \mapsto \pm\sqrt{5})$.

   Mais par le quatrième point de la Proposition 4.6.4, on sait que la taille des groupes de Galois sont égaux au degré de ces extensions. En effet les extensions considérées sont respectivement les corps de décomposition des polynômes séparables
$$(t^2 - 2)(t^2 - 3) \quad \text{et} \quad (t^2 - 2)(t^2 - 3)(t^2 - 5).$$

Dès lors on sait que $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$ a 4 éléments et que $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q})$ a 8 éléments. En effet on peut calculer le degré de ces extensions en utilisant les extensions successives de degré 2

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2},\sqrt{3}) \subset \mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}).$$

Ainsi, on conclut que les 4 (respectivement 8) automorphismes sont donc entièrement déterminés par $\sqrt{2} \mapsto \pm\sqrt{2}$ et $\sqrt{3} \mapsto \pm\sqrt{3}$ et ($\sqrt{5} \mapsto \pm\sqrt{5}$). Notons τ_i pour l'automorphisme qui envoie $\sqrt{i} \mapsto -\sqrt{i}$ et fixe $\sqrt{j}$ si $j \neq i$ pour $i,j = 2,3,5$. Ces automorphismes génèrent les groupes de Galois considérés et commutent deux à deux. Ainsi on voit que ces groupes de Galois sont abéliens. Notons C_2 pour un groupe d'ordre 2; on conclut maintenant que les morphismes

$$C_2 \oplus C_2 \to \mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) \quad \text{et} \quad C_2 \oplus C_2 \oplus C_2 \to \mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q})$$

définis en utilisant la propriété universelle de la somme directe de groupe abéliens en envoyant les générateurs des copies de C_2 sur les τ_i sont des isomorphismes.

Exercice 4.
Soit K un corps et L un corps de décomposition généré par des éléments séparables. En utilisant la Proposition 4.6.4 du cours montrez que si $\alpha \in L$ alors si l'orbite de α par l'action $\mathrm{Gal}(L/K)$ est de taille $[L:K]$ on a $L = K(\alpha)$.

Calculez des éléments primitifs pour chacune des extensions apparaissant dans l'exercice 3 en utilisant ce principe.

Solution.

Montrons l'affirmation. Premièrement, si on suppose que l'orbite de α est de taille $[L\colon K]$ alors tous les éléments de l'orbite sont de racines de $m_\alpha(t)$ par le premier point de la Proposition 4.6.4. Ainsi le degré de $m_\alpha(t)$ est au moins $[L\colon K]$. Mais comme il est également au plus $[L\colon K]$, on conclut qu'il est de degré $[L\colon K]$. On conclut alors $K(\alpha) = L$ par égalité des degrés.

Maintenant on en déduit que

$$\xi + \sqrt[3]{2} \quad \text{et} \quad \sqrt{2}+\sqrt{3} \quad \text{et} \quad \sqrt{2}+\sqrt{3}+\sqrt{6}$$

sont des éléments primitifs des extensions de l'exercice 3.

Exercice 5 (Corps imparfaits)**.** (a) Soit K un corps de caractéristique $p > 0$ et soit $\alpha \in K \backslash K^p$. Montrer que $x^p - \alpha \in K[x]$ est irréductible.

Soit $L = (\mathbb{F}_p(x))[y]/(y^2 - x(x-1)(x+1))$.

(b) Montrer que L est un corps.

(c) Si $p \neq 2$, montrer que L n'est pas parfait.

(d) Si $p = 2$, montrer que L n'est pas parfait.

Solution.

(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 $\mathrm{char}(L) = p$, 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, we see this using from example the degree of polynomials, 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 $\mathrm{char}(L) = 2$, 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 6.
Soit $p > 0$ un nombre premier, posons $L = \mathbb{F}_p(x, y)$ et $K = \mathbb{F}_p(x^p, y^p) \subseteq L$.

1. Calculer le degré de l'extension $K \subseteq L$.
2. Calculer $\mathrm{Gal}(L/K)$.
3. Montrer que cette extension ne peut pas être générée par un seul élément.
4. Montrer que pour tout $\gamma \neq \gamma' \in K$, on a que $K(x+\gamma y) \neq K(x+\gamma' y)$. En déduire qu'il existe une infinité de sous-extensions $K \subseteq F \subseteq L$ différentes.

Solution.

1. Soit $F = \mathbb{F}_p(x, y^p)$. Calculons les degrés des extensions $K \subseteq F$ et $F \subseteq L$. Nous calculerons uniquement le degré de $K \subseteq F$, car l'autre calcul est identique.

   Montrons que le polynôme $f(t) = t^p - x^p \in K[t] = \mathbb{F}_p(x^p, y^p)[t]$ est irréductible. Si on pouvait écrire $f(t) = g(t)h(t)$ avec $g, h \in K[t]$, alors on a aussi l'égalité

$$t^p - x^p = f(t) = g(t)h(t)$$

dans $\mathbb{F}_p(x,y)$!

Or, on peut écrire $t^p - x^p = (t-x)^p$ dans $\mathbb{F}_p(x,y)[t]$ (on ne pouvait pas le faire dans $K[t]$, vu que $x \notin K$). Cela implique qu'à unité près, on a $g(t) = (t-x)^a$ et $h(t) = (t-x)^b$ avec $a+b=p$. Le coefficient constant de $(t-x)^a$ est x^a, et vu que $g(t) \in K[t]$, cela force $x^a \in K$. Le seul cas ou c'est possible est que $a=0$ ou $a=p$, i.e. $g(t) = f(t)$ ou est constant (à unité près). On a donc montré que $f(t)$ était irréductible de degré p, et donc

$$[F:K] = p.$$

Le même calcul montre que $[L:F] = p$, et donc

$$[L:K] = [L:F][F:K] = p^2.$$

2. Soit $\sigma \in \mathrm{Gal}(L/K)$, et soit $\alpha \in L$. Notons que $\alpha^p \in K$. En effet, c'est le cas pour x et y, et vu que ces deux éléments génèrent L/K et que la puissance p est un morphisme d'anneaux (on est en caractéristique p), c'est aussi le cas de tout $\alpha \in L$.

   On a donc
   $$\alpha^p = \sigma(\alpha^p) = \sigma(\alpha)^p,$$
   ou la première égalité vient que $\alpha^p \in K$ et $\sigma|_K = id_K$.

   On a donc
   $$(\sigma(\alpha) - \alpha)^p = \sigma(\alpha)^p - \alpha^p = 0,$$
   donc on a forcément que $\sigma(\alpha) = \alpha$. On a donc montré que $\sigma = id$, et donc
   $$\mathrm{Gal}(L/K) = \{id\}.$$

3. Supposons que L/K soit générée par un élément, disons β. Vu que $\beta^p \in K$ (cf plus haut), on déduit que β satisfait l'équation algébrique $t^p - \beta^p \in K[t]$. Soit m le polynôme minimal de β sur K. Alors automatiquement m divise $t^p - \beta^p$, et on a donc
   $$p^2 = [L:K] = [K(\beta):K] = \deg(m) \leq \deg(t^p - \beta^p) = p,$$
   ce qui est une contradiction.

4. Pour tout $\gamma \in K$, considérons l'extension intermédiaire
   $$F_\gamma := K(x + \gamma y) \subseteq L.$$
   Montrons que pour $\gamma \neq \gamma'$, on a $F_\gamma \neq F_{\gamma'}$. Cela conclura la preuve, car K est infini.

   Soient $\gamma \neq \gamma' \in K$, et supposons par l'absurde que $F_\gamma = F_{\gamma'}$. Notons F ce corps. Alors par construction, on a que
   $$\begin{cases} x + \gamma y \in F \\ x + \gamma' y \in F. \end{cases}$$
   On peut alors sousraire et obtenir que
   $$(\gamma - \gamma')y \in F.$$
   Comme $\gamma \neq \gamma'$ et que K est un corps, on peut diviser et déduire que
   $$y \in F.$$
   Or si $x + \gamma y \in F$ et $y \in F$, on a donc que $x \in F$. Vu que $x, y \in F$, on déduit alors que $F = L$. Or, F est généré par un élément, ce qui contredit le point précédent.

Remarque. Le théorème principal de la théorie de Galois montre en particulier que si $K \subseteq L$ est une extension Galoisienne, alors il y a un nombre fini de sous-extensions $K \subseteq F \subseteq L$. L'exercice ci-dessus montre que cette conséquence est fausse dans le cas inséparable. Le troisième point montre aussi que le théorème de l'élément primitif est faux dans le cas inséparable.

Exercice 1.
Dans les cas suivants, montrez que $\mathbb{Q}(\alpha,\beta)$ est le corps de décomposition d'un polynôme, puis calculez $G = \mathrm{Gal}(\mathbb{Q}(\alpha,\beta)/\mathbb{Q})$, et calculez le polynôme minimal de $\alpha, \alpha+\beta, \alpha\cdot\beta$ et α^{-1}. Pour calculer les polynômes minimaux, on calculera l'orbite de ces éléments par G.

1. $\alpha = \sqrt{3}, \beta = \sqrt{7}$
2. $\alpha = e^{(i\pi/3)}, \beta = -1$
3. $\alpha = e^{(i\pi/3)}, \beta = i$
4. $\alpha = e^{(i\pi/6)}, \beta = i$.

Solution. Throughout, we write $K = \mathbb{Q}(\alpha,\beta)$.

In the following solutions, we use the same technique to find the minimal polynomials as in Example 4.6.15. With Proposition 4.6.14, 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 Exercise 3.4 of sheet 10, 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

   $$m_{\sqrt{3},\mathbb{Q}} = x^2 - 3$$
   $$m_{\sqrt{3}+\sqrt{7},\mathbb{Q}} = (x-(\sqrt{3}+\sqrt{7})(x+(\sqrt{3}+\sqrt{7}))(x-(\sqrt{3}-\sqrt{7}))(x+(\sqrt{3}-\sqrt{7})) =$$
   $$(x^2-(10+2\sqrt{21}))(x^2-(10-2\sqrt{21})) = x^4 - 20x^2 + 16$$

   $$m_{\sqrt{3}\cdot\sqrt{7},\mathbb{Q}} = (x-\sqrt{3}\sqrt{7})(x+\sqrt{3}\sqrt{7}) = x^2 - 21$$
   $$m_{\sqrt{3}^{-1},\mathbb{Q}} = x^2 - \frac{1}{3}.$$

2. We note that since $\beta = -1 \in \mathbb{Q}$, it holds that $K = \mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\alpha)$. Now, α is a root of the polynomial $x^3+1 = (x+1)(x^2-x+1)$. Since $\alpha \neq -1$, we deduce that α is a root of $f = x^2 - x + 1$. Note that this polynomial is irreducible (otherwise $\alpha \in \mathbb{Q}$, which is not correct). Since f has degree 2 and K has one root, it automatically has the other root of f (in fact, this other root is $\overline{\alpha} = 1/\alpha = e^{-i\pi/3}$). Thus, it is indeed the splitting field of f over $\mathbb{Q}$. Since f is a separable polynomial, we know by Proposition 4.6.5.(4) that G has order 2 (hence $G \cong \mathbb{Z}/2\mathbb{Z}$). Since a non-trivial element in G has no other choice but to send α to $\overline{\alpha}$ (the other root of f) and fix $\mathbb{Q}$, we deduce that $G = \langle\tau\rangle$, where $\tau(\alpha) = \overline{\alpha}$ (in fact, τ is the

complex conjugation here). Indeed, if τ defined as above was not a field automorphism, then we would obtain that $|G| < 2$, a contradiction with our previous discussion.

Let us compute minimal polynomials. We will shortcut a bit compared to the previous exercise, although one could have done the exact same computations! We already computed the minimal polynomial of α: it is $f = x^2 - x + 1$. Since $1/\alpha$ is the other root of f, it also has f as its minimal polynomial.

Since $\alpha^3 = -1$, $(-\alpha)^3 = 1$, so $-\alpha$ is a root of $x^3 - 1 = (x-1)(x^2+x+1)$. As before, we deduce that the minimal polynomial of $-\alpha$ is $x^2 + x + 1$.

Finally, since $\alpha^2 = \alpha - 1$, we deduce that $(\alpha - 1)^3 = 1$. Thus, we conclude as above that the minimal polynomial of $\alpha - 1$ is $x^2 + x + 1$.

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 4.6.7 (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

$$\begin{aligned} m_{z,\mathbb{Q}} &= (x-z)(x-\sigma(z))(x-\tau(z))(x-\sigma\tau(z)) \\ &= (x-z)(x-(a+bi-c\sqrt{3}-d\sqrt{3}i))(x-(a-bi+c\sqrt{3}-d\sqrt{3}i))(x-(a-bi-c\sqrt{3}+d\sqrt{3}i)). \end{aligned}$$

This leads for example that

$$m_{\alpha+\beta,\mathbb{Q}} = x^4 - 2x^3 + 5x^2 - 4x + 1.$$

Let us compute the other minimal polynomials in an easier way. We already computed $m_{\alpha,\mathbb{Q}} = m_{1/\alpha,\mathbb{Q}} = x^2 - x + 1$ in the previous point. Note that $\alpha\beta = ie^{i\pi/3}$, which is annihilated by $x^6 + 1 = (x^2+1)(x^4 - x^2 + 1)$. Since it is not killed by $x^2 + 1$, we deduce that it is killed by $x^4 - x^2 + 1$. Since the minimal polynomial of $\alpha\beta$ has degree 4 (c.f. the expression above, since $\alpha\beta$, $\sigma(\alpha\beta)$, $\tau(\alpha\beta)$ and $\sigma\tau(\alpha\beta)$ are all different), we deduce that its minimal polynomial is actually $x^4 - x^2 + 1$.

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 elements id, τ, σ, η. It follows that

$$m_{\alpha,\mathbb{Q}} = (x-\alpha)(x-\tau(\alpha))(x-\sigma(\alpha))(x-\eta(\alpha)) = (x-\alpha)(x-\alpha^5)(x-\alpha^7)(x-\alpha^{11}) = x^4 - x^2 + 1$$

$$m_{\alpha+\beta,\mathbb{Q}} = m_{\alpha+\alpha^3,\mathbb{Q}} = (x-(\alpha+\alpha^3))(x-\tau(\alpha+\alpha^3))(x-\sigma(\alpha+\alpha^3))(x-\eta(\alpha+\alpha^3))$$
$$= (x-(\alpha+\alpha^3))(x-(\alpha^5+\alpha^3))(x-(\alpha^7+\alpha^9))(x-(\alpha^{11}+\alpha^9)) = x^4 + 3x^2 + 9$$

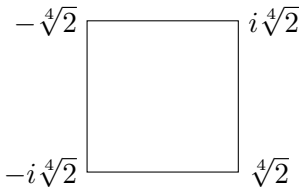
$$m_{\alpha\cdot\beta,\mathbb{Q}} = m_{\alpha^4,\mathbb{Q}} = m_{-0.5+0.5i\sqrt{3},\mathbb{Q}} = (x-\alpha^4)(x-\tau(\alpha^4))(x-\sigma(\alpha^4))(x-\eta(\alpha^4))$$
$$= (x-\alpha^4)(x-\alpha^8)\cancel{(x-\alpha^4)(x-\alpha^8)} = x^2 + x + 1$$

$$m_{\alpha^{-1},\mathbb{Q}} = m_{\alpha^{11},\mathbb{Q}} = (x-\alpha^{11})(x-\tau(\alpha^{11}))(x-\sigma(\alpha^{11}))(x-\eta(\alpha^{11}))$$
$$= (x-\alpha^{11})(x-\alpha^7)(x-\alpha^7)(x-\alpha) = x^4 - x^2 + 1$$

Exercice 2. 1. Montrez que $K = \mathbb{Q}(i, \sqrt[4]{2})$ est le corps de décomposition de $x^4 - 2 \in \mathbb{Q}[x]$.

2. Montrez qu'il existe $r, s \in \mathrm{Gal}(K/\mathbb{Q})$ tel que
   (a) $r(\sqrt[4]{2}) = i\sqrt[4]{2}$ et $r(i) = i$,
   (b) $s(\sqrt[4]{2}) = -\sqrt[4]{2}$ et $s(i) = -i$.

3. Déduire que si l'on nomme les sommets d'un carré selon les racines de $x^4 - 2$ comme ci-dessous



   le groupe $\mathrm{Gal}(K, \mathbb{Q})$ est isomorphe au groupe D_8 des symétries du carré.

4. Donner un élément $\alpha \in K$ avec $\mathbb{Q}(\alpha) = K$.

5. Pour tous les éléments suivants de K

$$3 + \sqrt{2}, \quad i + \sqrt{2}, \quad 1 + \sqrt[4]{2} \quad 1 + i\sqrt[4]{2}, \quad \sqrt[4]{2}(1+i) \quad \sqrt[4]{2}(1-i)$$

   déterminer,
   (a) l'orbite de ces éléments par $\mathrm{Gal}(K/\mathbb{Q})$,
   (b) leur polynôme minimal,
   (c) le stabilisateur de ces éléments dans $\mathrm{Gal}(K/\mathbb{Q})$.*

Solution.

1. Les racines de $x^4 - 2$ sont $\pm\sqrt[4]{2}$ et $\pm i\sqrt[4]{2}$, et l'extension de $\mathbb{Q}$ générée par ces éléments est bel et bien K.

*C'est à dire si α est un tel élément, $\mathrm{Gal}(K/\mathbb{Q}(\alpha))$.

2. Montrons d'abord que $[K:\mathbb{Q}]=8$. Comme x^4-2 est irréductible sur $\mathbb{Z}[x]$ par Eisenstein et primitif, il est aussi irréductible sur $\mathbb{Q}[x]$ par les lemmes de Gauss. Ainsi, $[\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}]=4$. Comme $i\notin\mathbb{Q}(\sqrt[4]{2})$, on en déduit que le polynôme minimal de i sur $\mathbb{Q}(\sqrt[4]{2})$ est x^2+1, et donc $[\mathbb{Q}(i,\sqrt[4]{2}):\mathbb{Q}(\sqrt[4]{2})]=2$. On en déduit donc que $[\mathbb{Q}(i,\sqrt[4]{2}):\mathbb{Q}]=8$ par multiplicativité des degrés.

   Vu que $8=[K:\mathbb{Q}]=[K:\mathbb{Q}(i)][\mathbb{Q}(i):\mathbb{Q}]$, on en déduit que $[K:\mathbb{Q}(i)]=4$. Ainsi, x^4-2 est nécessairement le polynôme minimal de $\sqrt[4]{2}$ sur $\mathbb{Q}(i)$ (sinon cette extension serait de degré <4). Par la proposition 4.6.5.(3), le groupe de Galois de $K/\mathbb{Q}(i)$ agit transitivement sur les racines de x^4-2, donc on obtient l'existence de r comme dans (a).

   Montrons maintenant l'existence de s. Notez que $r^2(\sqrt[4]{2})=-\sqrt[4]{2}$ et $r^2(i)=i$. Ainsi, si l'on considère s comme la composée de r^2 et de la conjugaison complexe habituelle, alors $s(\sqrt[4]{2})=-\sqrt[4]{2}$ et $s(i)=-i$.

3. Par le point précédent, cette extension est un corps de décomposition. Vu qu'elle est séparable ($\mathbb{Q}$ est parfait, car de caractéristique zéro), on en déduit par la Proposition 4.6.5 que $|\operatorname{Gal}(K/\mathbb{Q})|=8$. Montrons que $\langle r,s\rangle=\operatorname{Gal}(K/\mathbb{Q})$. Vu que r est d'ordre 4 et que s n'est pas une puissance de r (tout ceci de vérifie à la main), on obtient que $\langle r,s\rangle$ contient au moins 5 éléments. Comme son ordre doit diviser 8, on en déduit que

$$\langle r,s\rangle=\operatorname{Gal}(K/\mathbb{Q}).$$

   Nous allons conclure de deux manières différentes:

   (a) Par la géométrie: notez que r et s agissent par isométries sur le carré de la donnée (r est une rotation d'un quart de tour dans le sens anti-horaire, et s est la symmétrie d'axe d'en bas à gauche vers en haut à droite). Cette action est nécessairement fidèle, car ces quatre sommets génèrent K sur $\mathbb{Q}$.
   Ainsi, $\langle r,s\rangle$ agit fidèlement par isométries sur ce carré. Comme le groupe d'isométries du carré est D_8 (donc d'ordre 8), on a une injection $\langle r,s\rangle\hookrightarrow D_8$ est un isomorphisme. Comme $\operatorname{Gal}(K/\mathbb{Q})=\langle r,s\rangle$ est d'ordre 8, on conclut que $\operatorname{Gal}(K/\mathbb{Q})\cong D_8$.

   (b) Par la théorie des groupes: on calcule à la main que $r^4=id, s^2=id$ et $(rs)^2=id$. Comme D_8 a comme présentation $\langle\sigma,\tau|\sigma^4=1\ \tau^2=1\ (\sigma\tau)^2=1\rangle$, on obtient par définition l'existence d'un morphisme surjectif $D_8\to\langle r,s,\rangle=\operatorname{Gal}(K/\mathbb{Q})$ envoyant σ sur r et τ sur s. Comme ces deux groupes sont d'ordre 8, on conclut que notre morphisme est un isomorphisme.

4. Comme on l'a vu au point précédent, on a que $\operatorname{Gal}(K/\mathbb{Q})=\langle r,s\rangle=\{1,r,r^2,r^3,s,sr,sr^2,sr^3\}$. Prenons $\alpha=\sqrt[4]{2}+i$. Vu qu'une $\mathbb{Q}$-base de K est donnée par $\{1,i,\sqrt[4]{2},\sqrt{2},(\sqrt[4]{2})^3,i\sqrt[4]{2},i\sqrt{2},i(\sqrt[4]{2})^3\}$, un calcul direct montre que cet élément n'est fixé par aucun $g\neq id$ de $\operatorname{Gal}(K/\mathbb{Q})$, donc c'est bien un élément primitif.

5. - $3+\sqrt{2}$: Comme 3 est forcément fixé et que $\sqrt{2}$ ne peut être qu'envoyé sur $\pm\sqrt{2}$ (les racines de $x^2-2\in\mathbb{Q}[x]$), on déduit que l'orbite de $3+\sqrt{2}$ est incluse dans $\{3\pm\sqrt{2}\}$. Vu que $r(3+\sqrt{2})=3-\sqrt{2}$, on conclut que l'orbite de $3+\sqrt{2}$ est bien $\{3+\sqrt{2},3-\sqrt{2}\}$. Par la proposition 4.6.14, on a que son polynôme minimal est

$$(x-(3+\sqrt{2}))(x-(3-\sqrt{2}))=x^2-6x+7.$$

     On voit par un calcul direct que r^2 et s fixent $3+\sqrt{2}$, donc $\operatorname{Gal}(K/\mathbb{Q}(3+\sqrt{2}))$ contient $\{id,r^2,s,sr^2\}$. Vu que $|\operatorname{Gal}(K:\mathbb{Q})/\operatorname{Gal}(K:\mathbb{Q}(3+\sqrt{2}))|$ est égale à la taille de l'orbite de $3+\sqrt{2}$ (qui vaut 2), on déduit que $\operatorname{Gal}(K/\mathbb{Q}(3+\sqrt{2}))$ a taille 4, donc

$$\operatorname{Gal}(K/\mathbb{Q}(3+\sqrt{2}))=\{id,r^2,s,sr^2\}.$$

- $i+\sqrt{2}$: Nous avons déjà vu par le passé que $\mathbb{Q}(i+\sqrt{2}) = \mathbb{Q}(i,\sqrt{2})$, donc il génère une extension d'ordre 4. L'orbite de $i+\sqrt{2}$ est donc de taille 4 par la proposition 4.6.5. Comme i est forcément envoyé sur $\pm i$ et $\sqrt{2}$ sur $\pm\sqrt{2}$, on a au plus 4 éléments dans l'orbite : $\pm\sqrt{2} \pm i$.

  Comme on en a exactement 4, on en déduit que l'orbite est exactement ces quatre éléments ci-dessus. Comme vu en cours, le polynôme minimal est alors

  $$(x-(i+\sqrt{2}))(x+(i+\sqrt{2}))(x-(i-\sqrt{2}))(x+(i-\sqrt{2})) = (x^2-(1+2i\sqrt{2}))(x^2-(1-2i\sqrt{2})) = x^4-2x^2+9.$$

  Le même argument montre que le stabilisateur est d'ordre 2. Comme r^2 stabilise cet élément, on en déduit que le stabilisateur est exactement $\{id, r^2\}$.
- On a que $\mathbb{Q}(1+\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2})$ est un extension de degré 4 sur $\mathbb{Q}$, donc l'orbite est de taille 4. Comme l'orbite de $1+\sqrt[4]{2}$ par $\langle r\rangle$ est $\{1+\sqrt[4]{2}, 1+i\sqrt[4]{2}, 1-\sqrt[4]{2}, 1-i\sqrt[4]{2}\}$, on a trouvé notre orbite.

  Notez de $(x-1)^4-2$ annule cet élément. Vu que ce polynôme est de degré $4 = [\mathbb{Q}(1+\sqrt[4]{2}) : \mathbb{Q}]$, c'est forcément le polynôme minimal.

  Finalement, on sait comme avant que le stabilisateur est d'ordre 2. Comme sr^2 stabilise cet élément, on en déduit que le stabilisateur est exactement $\{1, sr^2\}$.
- Remarquez que $1+i\sqrt[4]{2}$ est dans l'orbite de $1+\sqrt[4]{2}$, donc ces éléments ont la même orbite, et donc le même polynôme minimal

  Quant au stabilisateur, celui-ci sera conjugué, précisément par un élément du groupe de Galois qui envoie $1+\sqrt[4]{2}$ sur $1+i\sqrt[4]{2}$ – r est un tel élément. On déduit que le stabilisateur est $\{id, s\}$. Cela se voyait aussi directement comme s fixait $1+i\sqrt[4]{2}$.
- L'orbite de $\sqrt[4]{2}(1+i)$ par $\langle r\rangle$ est exactement

  $$\{\sqrt[4]{2}(1+i), i\sqrt[4]{2}(1+i), -\sqrt[4]{2}(1+i), -i\sqrt[4]{2}(1+i)\}.$$

  Vu que la taille de l'orbite divise la taille du groupe de Galois (i.e. 8), on aurait que si l'orbite était plus grande que l'ensemble ci-dessus, alors le stabilisateur serait trivial. Or, sr^3 est dans ce stabilisateur, et donc l'orbite est exactement de taille 4 (et est donnée ci-dessus), et le stabilisateur est exactement $\{id, sr^3\}$.

  On pourrait trouver le polyôme minimal en faisant un calcul fastidieux, mais trouvons-le plutôt à la main. on a que

  $$(\sqrt[4]{2}(1+i))^4 = 2(1+i)^4 = -8,$$

  donc c'est une racine de x^4+8. Vu que l'extension générée est de degré 4, c'est donc le polynôme minimal.
- Comme $\sqrt[4]{2}(1-i) = -i\sqrt[4]{2}(1+i)$ est dans l'orbite de $\sqrt[4]{2}(1+i)$, on conclut qu'ils ont la même orbite, et donc le même polynôme minimal.

  Quant au stabilisateur, il est conjugé au précédent et donc c'est $\{id, sr\}$.

Exercice 3.
Soit $f = x^3+ax+1 \in \mathbb{Q}[x]$ avec $a > 0$, $a \in \mathbb{Z}$.

1. Montrer que f est irréductible sur $\mathbb{Q}$.
2. Montrer que f a une racine réelle, mais pas trois.
3. Soit $K = \mathbb{Q}[x]/(f)$. Montrer que $K/\mathbb{Q}$ est une extension de degré 3 qui n'est pas Galoisienne.
4. Soit L le corps de décomposition de f sur $\mathbb{Q}$. Montrer que $\mathrm{Gal}(L/Q) \cong S_3$.

Solution.

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 b and c are non-zero relatively prime integers, then

$$(b/c)^3 + (ab/c) + 1 \neq 0,$$

or equivalently

$$b^3 + abc^2 + c^3 \neq 0.$$

Suppose the contrary. Then c divides b^3 and b divides c^3. Using the relative prime assumption we obtain both b and c are plus-minus 1, so that a root has to be 1 or -1 but one sees as $a > 0$ that

$$1 + a + 1 \neq 0 \quad \text{and} \quad -1 - a + 1 \neq 0.$$

2. Since $f(x)$ tends to $-\infty$ as x goes to $-\infty$ and goes to $+\infty$ as x goes to $+\infty$, we deduce by the mean value theorem that f has at least one real root. Now, let α, β and γ be the three roots of f in its splitting field, and 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.

Once we know that not all roots are real, here is a slick way to deduce that f must have a real root. As $\deg f = 3$, and complex roots of a real polynomial come in complex conjugate pairs, f has to have a real root.

3. Let α denote the unique real root. 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 4.
Soit K un corps de caractéristique $p > 0$, et $\alpha \neq 0 \in K$ tel que le pôlynome $f(x) = x^p - x + \alpha \in K[x]$ n'a pas de racines dans K. Soit L le corps de decomposition de f, et $G = \mathrm{Gal}(L/K)$.

1. Montrez que $G \cong \mathbb{Z}/p\mathbb{Z}$. *Indication: Si β est une racine de f, alors $\beta + \gamma$ l'est aussi, pour tout $\gamma \in \mathbb{F}_p$.*

2. Montrez que le pôlynome f est irréductible sur K.

3. Considérons $K = \mathbb{F}_p(t)$. Montrez que le pôlynome $f(x) = x^p - x + t \in K[x]$ n'a pas de racines dans K.

4. Soit K et f comme dans le point précédent. Donnez le corps de décomposition de f sur K.

Solution.

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 5.
Soit $K \subseteq L \subseteq E$ une extension algébrique tel que $K \subseteq L$ et $L \subseteq E$ sont Galois. Montrer que $K \subseteq E$ n'est pas forcément Galois.
Indication. Envisager les extensions $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{1+\sqrt{2}})$ ou $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$.

Solution. 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 $\pm\sqrt{1-\sqrt{2}} \notin \mathbb{Q}(\sqrt{1+\sqrt{2}})$.

It follows that the extension is not Galois: indeed in a Galois extension L/K for $\alpha \in L$ the polynominal $m_{\alpha,K}$ has all its roots in L, these roots being the orbit of the element α by the Galois group. But this was just shown no to be the case for $\sqrt{1+\sqrt{2}}$.

A similar argument works also for

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2}).$$

Exercice 1 (Correspondance de Galois)**.**
Dans chacun des cas suivantes déterminer le groupe de Galois de l'extension donnée, déterminer tous ses sous-groupes et tous les sous-corps de points fixes correspondants.

1. $\mathbb{Q} \subset \mathbb{Q}(\sqrt{7})$.
2. $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
3. $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.
4. $\mathbb{Q} \subset E$ où E est le corps de décomposition de $t^4 - 2t^2 - 1 \in \mathbb{Q}[t]$.

Indication. Ce corps de décomposition est de degré 8 et on montrera qu'il s'agit de $\mathbb{Q}(\sqrt{1+\sqrt{2}}, i)$. On explicitera alors un automorphisme d'ordre 2 et un autre d'ordre 4 qui ne commutent pas entre eux, si bien que le groupe de Galois est le groupe dihédral d'ordre 8.

Solution.

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 4.6.5(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 3.4 of sheet 10 that $[L : \mathbb{Q}] = 4$, that Galois group is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$ and that it is generated by σ and τ, where $\sigma(\sqrt{2}) = -\sqrt{2}$ and $\sigma(\sqrt{3}) = \sqrt{3}$, respectively $\tau(\sqrt{2}) = \sqrt{2}$ and $\tau(\sqrt{3}) = -\sqrt{3}$.

   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. We therefore need to determine $L^H \subseteq L$. By the main theorem of Galois theory, we know that $[L : L^H] = |H| = 2$. 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. As in the previous point, we already computed that $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}$ is Galois, with Galois group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$. It is generated by $\sigma_1, \sigma_2, \sigma_3 \in \operatorname{Gal}(L/\mathbb{Q})$ with:

$$\sigma_1(\sqrt{2}) = -\sqrt{2},\ \sigma_1(\sqrt{3}) = \sqrt{3} \text{ and } \sigma_1(\sqrt{5}) = \sqrt{5}$$
$$\sigma_2(\sqrt{2}) = \sqrt{2},\ \sigma_2(\sqrt{3}) = -\sqrt{3} \text{ and } \sigma_2(\sqrt{5}) = \sqrt{5}$$
$$\sigma_3(\sqrt{2}) = \sqrt{2},\ \sigma_3(\sqrt{3}) = \sqrt{3} \text{ and } \sigma_3(\sqrt{5}) = -\sqrt{5}$$

   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. Then by the main theorem of Galois theory, $L^H \subseteq L$ is Galois with $[L : L^H] = |H| = 2$, so $[L^H : \mathbb{Q}] = 4$.

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 $\mathrm{Gal}(L/\mathbb{Q})$. Again, there are 7 of them and each of these is generated by two distinct elements of order 2 of $\mathrm{Gal}(L/\mathbb{Q})$ and is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Let H be one of these subgroups. As above, $L^H \subseteq L$ 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 $\mathbb{Q}$. It follows that $|\mathrm{Gal}(E/\mathbb{Q})| = [E : \mathbb{Q}]$. 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 can make a choice of complex square root sucht that 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:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{\sqrt{1+\sqrt{2}}}) \subseteq E.$$

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 $|\mathrm{Gal}(E/\mathbb{Q})| = 8$.

Since $E/\mathbb{Q}(\sqrt{1+\sqrt{2}})$ has degree 2 and is Galois, there exists $\tau \in \mathrm{Gal}(E/\mathbb{Q})$ such that $\tau(\sqrt{1+\sqrt{2}}) = \sqrt{1+\sqrt{2}}$ and $\tau(i) = -i$.

Note that $t^4 - 2t^2 - 1$ is a degree 4 polynomial in $\mathbb{Q}(i)$ annihilating $\sqrt{1+\sqrt{2}}$. Since the associated extension $E/\mathbb{Q}(i)$ has degree 4, we deduce that $t^4 - 2t^2 - 1$ is irreducible over $\mathbb{Q}(i)$.

By the course, we know that there exists $\sigma' \in \mathrm{Gal}(E/\mathbb{Q}(i))$ sending $\alpha := \sqrt{1+\sqrt{2}}$ to $\sqrt{1-\sqrt{2}}$. Set $\sigma = \sigma'\tau$. Recall that $\sqrt{1-\sqrt{2}} = i\alpha^{-1}$. Therefore we can write the four roots of

$$t^4 - 2t^2 - 1$$

as

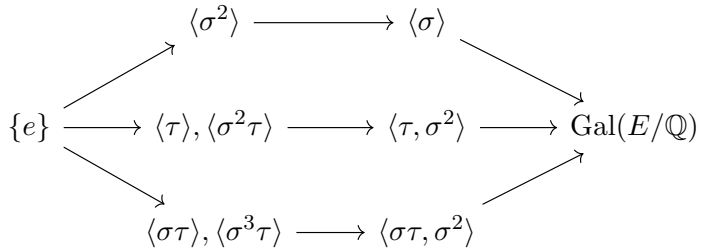
$$\alpha, \quad -\alpha, \quad i\alpha^{-1}, \quad -i\alpha^{-1}.$$

One checks that:

$$\sigma^2(\alpha) = -\alpha, \ \sigma^2(i) = i$$

which implie that σ^2 is of order 2, and therefore that σ is of order 4. Also, as $\sigma\tau(\alpha) = i\alpha^{-1}$ and $\tau\sigma(\alpha) = -i\alpha^{-1}$, we conclude that $\mathrm{Gal}(E/\mathbb{Q})$ is a non-commutative group of order 8. Also as $\sigma^2(i) = i$ and $\tau(i) = -i$, we see that there is two elements of order 2, which implies $\mathrm{Gal}(E/\mathbb{Q}) \cong D_8$.

Subgroups of $\mathrm{Gal}(E/\mathbb{Q})$, arranged by conjugacy classes, are



Recall also that the index of subgroup coresond to the degree of the corresponding fixed extension. To deduce what are the corresponding extensions, notice also that

$$1 + \sigma(\sqrt{2}) = \sigma(1 + \sqrt{2}) = \sigma(\alpha^2) = (i\alpha^{-1})^2 = -\frac{-1}{1+\sqrt{2}} = 1 - \sqrt{2},$$

impliyng that $\sigma(\sqrt{2}) = -\sqrt{2}$. As $\tau(\alpha) = \alpha$, we also get $\tau(\sqrt{2}) = \sqrt{2}$. As a consequence we get,

$$E^{<\sigma>} = \mathbb{Q}(i\sqrt{2}), \ E^{<\tau,\sigma^2>} = \mathbb{Q}(\sqrt{2}) \text{ and } E^{<\tau\sigma,\sigma^2>} = \mathbb{Q}(i).$$

Now as for the degree four extensions corresponding to subgroups of order 2; we can first deduce that

$$E^{\langle\sigma^2\rangle} = \mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(i + \sqrt{2}).$$

has $\mathbb{Q}(i, \sqrt{2})$ is Galois of order 4 and by the correspondence there is only one sub Galois extension of order 4.

Now, we deduce from the above calculations and from the fact that if H is a subgroup, then $\sigma(E^H) = E^{\sigma H \sigma^{-1}}$, we get

$$E^{<\tau>} = \mathbb{Q}(\sqrt{1+\sqrt{2}}) \quad E^{<\sigma^2\tau>} = \mathbb{Q}(\sqrt{1-\sqrt{2}}).$$

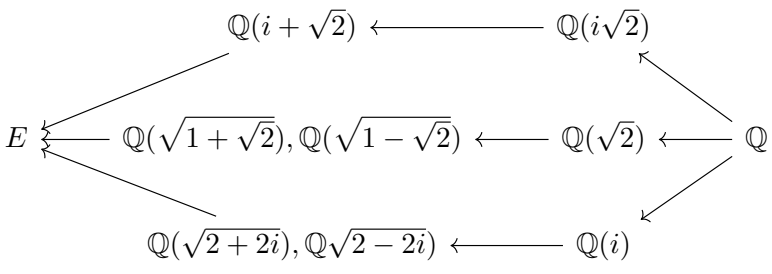
Also, note that squaring we deduce that,

$$\sqrt{1+\sqrt{2}} + \sqrt{1-\sqrt{2}} = \sqrt{2+2i} \quad \sqrt{1+\sqrt{2}} - \sqrt{1-\sqrt{2}} = \sqrt{2-2i}.$$

And therefore, we see that

$$E^{<\sigma\tau>} = \mathbb{Q}(\sqrt{2+2i}) \text{ and } E^{<\sigma^3\tau>} = \mathbb{Q}(\sqrt{2-2i}).$$

All in all, we get the following subfields, mirroring the subgroup diagram above.



Exercice 2.
Soit $K \subseteq L = K(\alpha)$ une extension simple de degré 2 de corps de caractéristique différente de 2.

1. Soit $m_{\alpha,K} = x^2 + bx + c$, où $b, c \in K$. Démontrez que la formule quadratique est valide ici. Cela veut dire les deux racines de $m_{\alpha,K}$ sont $\frac{-b+\sqrt{b^2-4c}}{2}$ et $\frac{-b-\sqrt{b^2-4c}}{2}$, où $\beta = \sqrt{b^2-4c} \in L$ est un quelconque élément tel que $\beta^2 = b^2 - 4c$. Cela inclut l'affirmation que tel β n'existe pas dans K. Concluez que L est une extension par une racine (deuxième) d'un élément adéquat de K.

2. Démontrez que $K \subseteq L$ est $\mathbb{Z}/2\mathbb{Z}$-galoisienne .

3. Soit $\mathbb{Q} = K \subseteq L$ une extension de corps $\mathbb{Z}/4\mathbb{Z}$-galoisienne. Démontrez que il existe des entiers rationnels a, $b \neq 0$ et d tel que $L = \mathbb{Q}\Big(\sqrt{a+b\sqrt{d}}\Big)$ et $\sqrt{d} \notin \mathbb{Q}$, $\sqrt{a+b\sqrt{d}} \notin \mathbb{Q}(\sqrt{d})$.

4. Considérons a, $b \neq 0$, $d \in \mathbb{Q}$ tel que $\sqrt{d} \notin \mathbb{Q}$ et $\alpha = \sqrt{a+b\sqrt{d}} \notin \mathbb{Q}\big(\sqrt{d}\big)$. Démontrez que l'extension $K = \mathbb{Q} \subseteq L = \mathbb{Q}(\alpha)$ est $\mathbb{Z}/4\mathbb{Z}$-galoisienne si et seulement si $\sqrt{a-b\sqrt{d}} \in L$ et $\lambda = a^2 - b^2 d$ n'est pas un carré dans $\mathbb{Q}$.

5. Montrez que $\mathbb{Q} \subseteq \mathbb{Q}\big(\sqrt{2+\sqrt{2}}\big)$ est $\mathbb{Z}/4\mathbb{Z}$-galoisienne.

Solution.

1. Comme 2 est inversible, on peut écrire

$$x^2 + bx + c = 0 \iff x^2 + 2\frac{b}{2}x + \frac{b^2}{4} = \frac{b^2}{4} - c$$

c'est à dire

$$(2x+b)^2 = b^2 - 4c.$$

Ainsi, $\beta = 2\alpha + b$ est une racine carrée de $\frac{b^2}{4} - c$. Notons que $L = K(\alpha) = K(\beta)$. Comme $K \neq L$, on a que $\beta \neq\in K$. Cet élément est une racine carrée d'un élément de K. On voit par calcul direct que $\frac{-b+\beta}{2}$ et $\frac{-b-\beta}{2}$ sont les racines du polynôme minimal.

2. On construit un automorphisme de Galois de L sur K par

$$L = K(\beta) \xleftarrow{\mathrm{ev}_\beta} K[t]/(t^2 - \beta^2) \xrightarrow{\mathrm{ev}_{-\beta}} K(\beta) = L.$$

Comme il envoie $\beta \mapsto -\beta$, il n'est pas l'identité. Comme $|\operatorname{Gal}(L \mid K)| \leq 2$ on a égalité et donc que cette extension est Galoisienne.

3. Soit H l'unique sous-groupe d'ordre 2 dans le groupe de galois $G = \operatorname{Gal}(L \mid K)$. Soit $M = L^H$. Ce corps est de degré 2 sur $\mathbb{Q}$ par la correspondance de Galois. Soit donc $d \in \mathbb{Q}$ avec $M = \mathbb{Q}(\sqrt{d})$. Comme $M \subset L$ est de degré 2 par multiplicativité des degré, il existe un élément $a + b\sqrt{d} \in M$ tel que $L = M(\sqrt{a+b\sqrt{d}})$.

Montrons que $b \neq 0$. Si $b = 0$, alors $\sqrt{a} \notin \mathbb{Q}(\sqrt{d})$. Mais alors $L = \mathbb{Q}(\sqrt{a}, \sqrt{d})$ qui a groupe de Galois isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. En effet, un élément σ du groupe de Galois doit envoyer $\sqrt{a}$ sur $\pm\sqrt{a}$ et $\sqrt{d}$ sur $\pm\sqrt{d}$, ce qui force $\sigma^2 = id$. Ainsi, le groupe de Galois serait un groupe d'ordre 2 ou tous les éléments sont d'ordre au plus 2, i.e. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Dès lors, notons que $\sqrt{d} \in \mathbb{Q}(\sqrt{a+b\sqrt{d}})$, ce qui permet de conclure que $L = \mathbb{Q}(\sqrt{a+b\sqrt{d}})$.

4. Soit $\alpha = \sqrt{a+b\sqrt{d}}$ et $\beta = \sqrt{a-b\sqrt{d}}$. Notons que $\mathbb{Q}(\sqrt{d})$ est une extension intermédiaire Galoisienne de degré 2 sur $\mathbb{Q}$. Supposons l'extension Galoisienne. Soit $\phi \in \operatorname{Gal}(L \mid K)$ une extension de l'automorphisme de $\mathbb{Q}(\sqrt{d})$ qui envoie $\sqrt{d} \mapsto -\sqrt{d}$ à L par le théorème 4.3.4. On voit alors que $\phi(\alpha) \in L$ est une racine carrée de $a - b\sqrt{d}$. En particulier cet élément

appartient à L. A l'inverse, si $\sqrt{a-b\sqrt{d}} \in L$, alors L contient toutes les racines du polynôme minimal de $\sqrt{a+b\sqrt{d}}$, donc $L/\mathbb{Q}$ est Galoisienne par le théorème 4.6.17.

Ainsi, il suffit de montrer que a^2-b^2d n'est pas un carré si et seulement si $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$. Notons que $(\alpha\beta)^2 = a^2 - b^2d$.

Supposons tout d'abord que $a^2 - b^2d$ est un carré, et soit $\psi \in \mathrm{Gal}(L/\mathbb{Q})$. Alors $\psi(\alpha) \in \{\pm\alpha, \pm\beta\}$. Si $\psi(\alpha) = \alpha$ ou $-\alpha$, alors $\psi^2(\alpha) = \alpha$ et donc ψ est d'ordre 2. Comme $(\alpha\beta)^2 = a^2 - b^2d$, on a que $\alpha\beta \in \mathbb{Q}$ et donc vu que

$$\frac{1}{\alpha} = \frac{\beta}{\alpha\beta},$$

on a

$$\psi(\alpha) = \psi(\alpha\beta/\beta) = \alpha\beta\psi(1/\beta) = \alpha\beta\psi(\beta)^{-1}.$$

Ainsi, si $\psi(\alpha) = \beta$ ou $-\beta$, on en déduit aussi que $\psi^2(\alpha) = \alpha$, et donc $\psi^2 = id$.

Ainsi, on a dans tous les cas que $\psi^2 = id$, et donc le groupe de Galois $\mathrm{Gal}(L/\mathbb{Q})$ est 2-torsion. Il ne peut donc pas être isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

Supposons maintenant que $a^2 - b^2d$ n'est pas un carré. Alors $\mathbb{Q}(\alpha\beta)$ est une sous-extension de degré 2 sur $\mathbb{Q}$. On alors deux extensions ϕ_1, ϕ_2 de l'automorphisme de Galois non-trivial $\phi\colon \mathbb{Q}(\alpha\beta) \to \mathbb{Q}(\alpha\beta)$ qui envoie $\alpha\beta \mapsto -\alpha\beta$. Ces deux extensions sont déterminées par leur valeur sur α. Par exemple, $\phi_1(\alpha) = \beta$ et alors forcément $\phi_1(\beta) = -\alpha$. Ainsi, il est clair que ϕ_1 est d'ordre 4.

5. C'est immédiat par le point précédent.

Exercice 3.
Montrer que tous les groupes finis sont des groupes de Galois. *Indication: il suffit de prouver le cas du groupe S_n! Pour ce cas en particuler, pensez à permuter les variables de $\mathbb{C}(x_1, \ldots, x_n)$.*

Solution. 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 $\pi_1(\mathbb{C} \setminus \{p_1, \dots, p_n\}) \cong F_n$ 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 $\mathbb{C} \setminus \{p_1, \dots, p_n\}$ 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 4.
Soit $n \geq 1$. Calculez le groupe de Galois $\mathrm{Gal}(L_n/\mathbb{C}(t))$ où est L_n est le corps de décomposition de

$$f = X^{2n} - 2\left(\frac{t+1}{t-1}\right)X^n + 1,$$

de la manière suivante:

1. Montrez qu'il existe des automorphismes $\mathbb{C}(\sqrt{t}) \to \mathbb{C}(\sqrt{t})$ envoyant $\sqrt{t}$ sur $\frac{\sqrt{t}-1}{\sqrt{t}+1}$ et $\frac{\sqrt{t}+1}{\sqrt{t}-1}$.

2. Déduisez que les polynômes $X^n - \frac{\sqrt{t}-1}{\sqrt{t}+1}$ et $X^n + \frac{\sqrt{t}-1}{\sqrt{t}+1}$ sont irréductibles sur $\mathbb{C}(\sqrt{t})$, et que f est irréductible sur $\mathbb{C}(t)$.

3. Montrez que
$$L_n = \mathbb{C}(t)\left(\sqrt[n]{\frac{\sqrt{t}+1}{\sqrt{t}-1}}\right).$$

4. Posons $\xi_n = e^{\frac{2i\pi}{n}}$ et
$$x = \sqrt[n]{\frac{\sqrt{t}+1}{\sqrt{t}-1}}.$$
Montrez qu'il existe $r, s \in \mathrm{Gal}(L_n/\mathbb{C}(t))$ tel que $r(x) = \xi_n x$ et $s(x) = \frac{1}{x}$.

5. Déduire que $\mathrm{Gal}(L_n/\mathbb{C}(t)) \cong D_{2n}$.

Solution.

1. Posons $z = \sqrt{t}$, et considérons le morphisme $\mathbb{C}[z] \to \mathbb{C}(z)$ donné en envoyant z sur $\frac{z-1}{z+1}$ (et fixant $\mathbb{C}$). Montrons que ce morphisme est injectif pour le faire passer au corps des fractions.

   Cela peut certainement se faire à la main, mais voici une petite astuce. Considésons I le noyau de ce morphisme, et supposons que $I \neq 0$. Comme $\mathbb{C}(z)$ est en particulier intègre, ce noyau I est premier, et donc maximal vu que $\mathbb{C}[z]$ est principal. Comme $\mathbb{C}$ est algébriquement clos, alors $I = (z-a)$ pour un certain $a \in \mathbb{C}$. Or, on voit à la main que $z - a$ n'est jamais dans le noyau, donc ce morphisme est bien injectif.

   Ainsi, par la propriété universelle du corps des fractions, il existe un morphisme $\phi\colon \mathbb{C}(z) \to \mathbb{C}(z)$ envoyant z sur $\frac{z-1}{z+1}$. Le même argument montre qu'il existe un morphisme $\psi\colon \mathbb{C}(z) \to \mathbb{C}(z)$ envoyant z sur $\frac{z+1}{z-1}$. Il nous reste à montrer que ϕ et ψ sont des automorphismes. Ces morphismes sont certainment injectifs (tout morphisme de corps est injectif). De plus, $\phi \circ \psi$

envoie z sur $-z$, qui est un automorphisme. En particulier, ϕ est forcément surjectif,et donc aussi automorphisme.

Similairement, $\psi \circ \phi$ envoie z sur $\frac{1}{z}$, qui est aussi un isomorphisme. Le même argument qu'avant montre donc que ψ est aussi un automorphisme.

2. Comme $X^n \pm \sqrt{t}$ est irréductible sur $\mathbb{C}[\sqrt{t}][X]$ par le critère d'Eisenstein, on déduit par le lemme de Gauss que ce polynôme est aussi irreductible sur $\mathbb{C}(t)[X]$. Comme l'image d'un polynôme irréductible par un automorphisme est encore irréductible, on en déduit que les polynômes $X^n - \left(\frac{\sqrt{t}+1}{\sqrt{t}-1}\right)$ et $X^n - \left(\frac{\sqrt{t}-1}{\sqrt{t}+1}\right)$ sont aussi irréductibles sur $\mathbb{C}(\sqrt{t})[X]$.

   Montrons maintenant que f est irréductible sur $\mathbb{C}(t)$, donc écrivons $f = gh$ avec $\deg(g), \deg(h) > 1$. Vu que

$$\left(X^n - \left(\frac{\sqrt{t}+1}{\sqrt{t}-1}\right)\right)\left(X^n - \left(\frac{\sqrt{t}-1}{\sqrt{t}+1}\right)\right) = X^{2n} - 2\left(\frac{t+1}{t-1}\right)X^n + 1 = f,$$

   on sait par l'unicité de la décomposition en facteurs irréductibles dans $\mathbb{C}(\sqrt{t})[X]$ que g et h doivent être un des facteurs ci-dessus. Or, aucun de ces facteurs n'est à coefficients dans $\mathbb{C}(t)$ (notez que p.ex. $\frac{\sqrt{t}-1}{\sqrt{t}+1} = \frac{t+1-2\sqrt{t}}{t-1}$), donc on a une contradiction.

3. Comme $\mathbb{C}$ contient toutes les racines n'emes de l'unité, la décomposition de f ci-dessus montre que

$$L_n = \mathbb{C}(t)\left(\sqrt[n]{\frac{\sqrt{t}+1}{\sqrt{t}-1}}, \sqrt[n]{\frac{\sqrt{t}-1}{\sqrt{t}+1}}\right)$$

   (notez que le calcul du point précédent montre que $L_n \ni \sqrt{t}$).

   Posons $x = \sqrt[n]{\frac{\sqrt{t}+1}{\sqrt{t}-1}}$ et $y = \sqrt[n]{\frac{\sqrt{t}-1}{\sqrt{t}+1}}$. Vu que $y = 1/x$, on en déduit que

$$L_n = \mathbb{C}(t)\left(\sqrt[n]{\frac{\sqrt{t}+1}{\sqrt{t}-1}}, \sqrt[n]{\frac{\sqrt{t}-1}{\sqrt{t}+1}}\right).$$

4. Vu que $\xi_n x$ et $1/x$ sont aussi des racines de f (rappelez-vous que $y = 1/x$ et de la décomposition de f) et que L_n est générée par une seule racine de f, on sait par la proposition 4.6.5 l'existence de tels s et r.

5. Notez que r est d'ordre n et s est d'ordre 2. Comme s n'est pas une puissance de r, on sait que $\langle r, s\rangle$ est d'ordre $> n$. D'un autre côté, $|\operatorname{Gal}(L_n/\mathbb{C}(t))| = [L_n : \mathbb{C}(t)] = 2n$, vu que L_n est généré par un élément dont le polynôme minimal f est de degré $2n$. Ainsi, on en déduit que $\langle r, s\rangle = \operatorname{Gal}(L_n/\mathbb{C}(t))$.

   Remarquez que $(rs)^2 = id$. Vu que la présentation du groupe D_{2n} est $\langle \sigma, \tau | \sigma^n = 1\ \tau^2 = 1\ (\sigma\tau)^2 = 1\rangle$, on sait qu'il existe un morphisme surjectif $D_{2n} \to \langle r, s\rangle = \operatorname{Gal}(L_n/\mathbb{C}(t))$ envoyant σ sur r et τ sur s. Comme ces deux groupes sont d'ordre $2n$, cette surjection est automatiquement un automorphisme.

EPFL - Printemps 2025	Prof. Zs. Patakfalvi
Anneaux et Corps	**Exercices**
Solutions 13	

Les exercices marqués d'une étoile ($\star$) sont optionnels.

Exercice 1 (Correspondance de Galois)**.**
Calculez les groupes de Galois $\mathrm{Gal}(E/\mathbb{Q})$ puis exprimez tous les sous-corps intermédiaires avec leur sous-groupe correspondant ainsi que des éléments primitifs* et polynôme minimaux pour ceux-ci des extensions Galoisiennes E de $\mathbb{Q}$ donnés par

1. le corps de décomposition de x^3-2 dans $\mathbb{C}$,
2. le corps de décomposition de x^4-2 dans $\mathbb{C}$.

Utilisez ce que vous savez déjà grâce aux exercices *Série 10 exercice 3* et *Série 11 exercice 2.*

Solution.

1. On a déjà calculé que $E=\mathbb{Q}(\xi,\sqrt[3]{2})$ et que $\mathrm{Gal}(E/\mathbb{Q})\cong S_3$. Notons r un élément d'ordre 3 et s un élément d'ordre 2 de sorte que $\langle r,s\rangle=\mathrm{Gal}(E/\mathbb{Q})$, avec

   (a) $r(\xi)=\xi$, $r(\sqrt[3]{2})=\xi\sqrt[3]{2}$.
   (b) $s(\sqrt[3]{2})=\sqrt[3]{2}$, $s(\xi)=\xi^2$.

   Les sous-groupes de $\mathrm{Gal}(E/\mathbb{Q})$ sont les suivants (regroupés par classe de conjugaison, avec leur ordre en titre de colonne)

   1 2 3 6

   $$\{e\} \longrightarrow <s>,<sr>,<sr^2> \longrightarrow \mathrm{Gal}(E/\mathbb{Q}), \quad <r> \nearrow \searrow \mathrm{Gal}(E/\mathbb{Q})$$

   Comme ξ est de degré 2, on voit que $\mathbb{Q}(\xi)$ est le sous-corps fixé par $<r>$. Comme $\sqrt[3]{2}$ est de degré 3, on voit que $\mathbb{Q}(\sqrt[3]{2})$ est le sous-corps fixé par $<s>$.

   Notons également que $sr=rsr^{-1}$ et que $sr^2=r^2sr^{-2}$. Ainsi comme les conjugués correspondent à l'image par l'élément de l'extension on obtient que les sous-corps fixés par $<sr>$ et $<sr^2>$ sont respectivement $\mathbb{Q}(\xi\sqrt[3]{2})$ et $\mathbb{Q}(\xi^2\sqrt[3]{2})$. On résume cela en imitant en miroir le tableau des sous-groupes ci-dessus, le nombre de la colonne correspondant maintenant au degré.

   6 3 2 1

   $$\mathbb{Q}(\xi,\sqrt[3]{2}) \longrightarrow \mathbb{Q}(\sqrt[3]{2}),\mathbb{Q}(\xi\sqrt[3]{2}),\mathbb{Q}(\xi^2\sqrt[3]{2}) \longrightarrow \mathbb{Q}, \quad \mathbb{Q}(\xi) \nearrow \searrow \mathbb{Q}$$

   En ce qui est des éléments primitifs, ils sont tous déjà donnés sauf $\xi+\sqrt[3]{2}$ pour l'extension E. Les polynômes minimaux de ξ et $\sqrt[3]{2}$ et leurs conjugués sont x^2+x+1 et x^3+2 respectivement. Quant à $\xi+\sqrt[3]{2}$ – on pourrait multiplier les $x-\alpha$ où α sont tous les conjugés de l'élément.

*C'est à dire des générateurs sur $\mathbb{Q}$ de ces extensions intermédiaires.

C'est un peu fastidieux, alors on écrit la matrice de multiplication par cet élément dans la base de E suivante

$$1, \xi, \sqrt[3]{2}, \xi\sqrt[3]{3}, \sqrt[3]{4}, \xi\sqrt[3]{4}$$

c'est à dire (on utilise $\xi^2 = -1 - \xi$)

$$\begin{pmatrix} 0 & -1 & 0 & 0 & 2 & 0 \\ 1 & -1 & 0 & 0 & 0 & 2 \\ 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 1 & -1 \end{pmatrix}$$

puis on calcule le polynôme caractéristique de cette matrice pour conclure que le polynôme suivant

$$x^6 + 3x^5 + 6x^4 + 3x^3 + 9x + 9$$

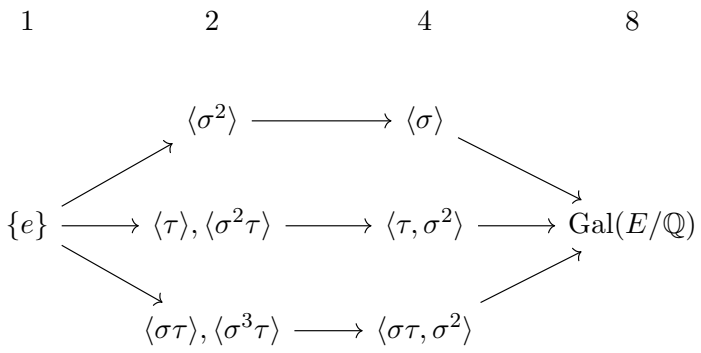
annule $\xi + \sqrt[3]{2}$ – comme il est de degré 6, c'est le polynôme minimal.

2. On a déjà calculé que $E = \mathbb{Q}(i, \sqrt[4]{2})$ et que $\mathrm{Gal}(E/\mathbb{Q}) \cong D_8$. Notons σ un élément d'ordre 4 et τ un élément d'ordre 2

   (a) $\sigma(i) = i$, $\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$.
   (b) $\tau(i) = -i$, $\tau(\sqrt[4]{2}) = -\sqrt[4]{2}$.

   Notons que $\tau(-\sqrt[4]{2}) = \sqrt[4]{2}$ et $i\sqrt[4]{2}$ et $-i\sqrt[4]{2}$ sont fixés par τ. Notons aussi que $\sigma(\sqrt{2}) = -\sqrt{2}$.

   Les sous-groupes de $\mathrm{Gal}(E/\mathbb{Q})$ sont les suivants (regroupés par classe de conjugaison, avec leur ordre en titre de colonne)



   Notons que $\sqrt{2}$ est fixée par σ^2 et τ et que $i\sqrt{2}$ est fixée par σ^2 et $\sigma\tau$, et que i est fixée par σ, on a en comparant les degrés sur $\mathbb{Q}$ que

$$E^{<\sigma>} = \mathbb{Q}(i) \quad E^{\langle\tau,\sigma^2\rangle} = \mathbb{Q}(\sqrt{2}) \quad E^{\langle\sigma\tau,\sigma^2\rangle} = \mathbb{Q}(i\sqrt{2}).$$

   Comme $\mathbb{Q}(i, \sqrt{2})$ est une sous-Galois extension de de degré 4 on conclut qu'elle corresponds au seul sous-groupe normal d'ordre 2, c'est à dire

$$E^{<\sigma^2>} = \mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(i + \sqrt{2}).$$

   Comme $i\sqrt[4]{2}$ est fixée par τ et qu'il a degré 4, et que $\sigma^2\tau = \sigma\tau\sigma^{-1}$, on obtient que

$$E^{<\tau>} = \mathbb{Q}(i\sqrt[4]{2}) \qquad E^{<\sigma^2\tau>} = E^{\sigma<\tau>\sigma^{-1}} = \sigma(E^{<\tau>}) = \mathbb{Q}(-\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}).$$

Notons que $\sqrt[4]{2}(1-i) = \sqrt[4]{2} - i\sqrt[4]{2}$ is est fixée par $\sigma\tau$ et de degré 4 car on peut calculer son orbite par le groupe de Galois explicitement et qu'elle est de taille 4, on obtient en comparant les degrés

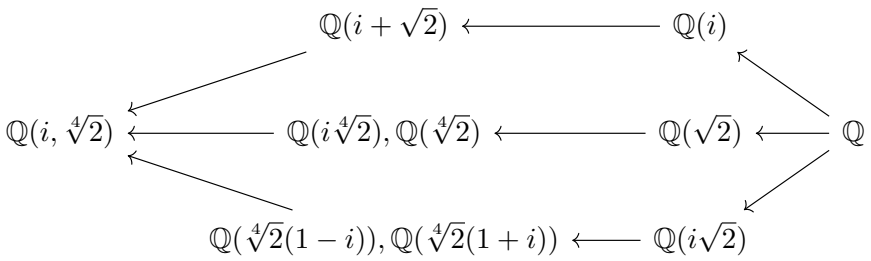
$$E^{<\sigma\tau>} = \mathbb{Q}(\sqrt[4]{2}(1-i)).$$

Maintenant en utilisant le même argument que ci-dessus on obtient finalement

$$E^{<\sigma^3\tau>} = \mathbb{Q}(\sqrt[4]{2}(1+i)).$$

On résume la correspondance obtenue en imitant en miroir le diagramme des sous-groupes ci-dessus.

8 4 2 1



En ce qui est des polynômes minimaux des éléments primitifs apparaissant ci-dessus,

(a) Les polynômes minimaux de $i, \sqrt{2}, i\sqrt{2}$ sont respectivement x^2+1, x^2-2 et x^2+2.

(b) Le polynôme minimal de $i+\sqrt{2}$ est

$$x^4 - 2x^2 + 9$$

voir la solution de l'exercice 2 de la série 11.

(c) Le polynôme minimal de $i\sqrt[4]{2}$ et $\sqrt[4]{2}$ est

$$x^4 - 2.$$

(d) Le polynôme minimal de $\sqrt[4]{2}(1-i)$ et $\sqrt[4]{2}(1+i)$ est

$$x^4 + 8.$$

Pour conclure on calcule le polynôme minimal de l'élément primitif de $i+\sqrt[4]{2}$. Pour cela on calcule le produit des $x-\alpha$ où les α sont les conjugués de $i+\sqrt[4]{2}$. On regroupe deux par deux ceux ci $i+i^k\sqrt[4]{2}$ et $-i+i^k\sqrt[4]{2}$ pour $k=0,1,2,3$. On commence par multiplier les polynômes en regroupant par paire comme ci-dessus pour obtenir les quatres polynômes de degré 2

$$x^2 + 2\sqrt[4]{2}x + \sqrt{2}, \quad x^2 - 2\sqrt[4]{2}x + \sqrt{2}, \quad x^2 + 2i\sqrt[4]{2}x - \sqrt{2}, \quad x^2 - 2i\sqrt[4]{2}x - \sqrt{2}.$$

Puis un multipliant les deux premiers puis les deux suivants, on obtient respectivement

$$x^4 - 2\sqrt{2}x^2 + 2, \quad x^4 + 2\sqrt{2}x^2 + 2.$$

Et finalement en multipliant ces deux derniers polynômes,

$$x^8 - 4x^4 + 4.$$

Exercice 2.
Fixons un entier $n > 0$. Soit K un corps de caractéristique soit 0 soit positive et première avec n.

1. Démontrez que $x^n - 1 \in K[x]$ n'admet pas de racine multiples dans son corps de décomposition sur K.

   Autrement dit il y a n racines distinctes qui sont des n-ième racines de l'unité dans les extensions de K.

   Supposons à a partir de maintenant que K contient toutes les racines n-ièmes de l'unité.

2. ($\star$) Considérons une $\mathbb{Z}/n\mathbb{Z}$-galoisienne extension $K \subseteq L$. Démontrez, que $L = K\left(\sqrt[n]{a}\right)$ pour un $a \in K$ adéquat, où $\sqrt[n]{a}$ dénote un élément dont le n-ième puissance égale à a.

   Indice: considérons un générateur ϕ du groupe de Galois en tant qu'application K-linéaire sur L. Démontrez que le polynôme minimal de ϕ en tant qu'application K linéaire est $x^n - 1$. Utilisez la décomposition en espaces propres pour trouver un vecteur propre $\alpha \in L$ avec valeur propre une n-ième racine primitive de l'unité. Démontrez après que n est l'entier minimal tel que $\alpha^n \in K$.

3. Supposons maintenant $n = p$ premier. Démontrez que si $\sqrt[p]{a}$ est une racine fixée de $a \in K \setminus K^p$ (dans un corps de décomposition adéquat), alors $L = K(\sqrt[p]{a})$ est $\mathbb{Z}/p\mathbb{Z}$ galoisienne.

   Indice: Soit ξ un p-ième racine primitve d'unité, et soit $\alpha = \sqrt[p]{a}$. Dans Lemme 4.9.1 des notes de cours on a démontré que toute les racines de $m_{\alpha,K}$ sont de forme de $\xi^j\alpha$, et que $K \subseteq L$ est galoisienne avec $\mathrm{Gal}(K/L)$ abélien. Notons aussi que puisque $a \notin K^p$, l'extension $K \subseteq L$ est non-triviale. Prenons donc un élément non-neutre $\phi \in \mathrm{Gal}(K/L)$. Démontrez que le plus petit entier $s > 0$ tel que $\phi^s(\alpha) = \alpha$ est $s = p$.

   Comme corollaire, déduisez que si $a \in K \setminus K^p$ alors le polynôme $x^p - a$ est irréductible dans $K[x]$. Donnez un contre-exemple à cet énoncé si p n'est pas premier.

4. Soit p un entier premier et soit $n > 0$ un entier positif arbitraire. Démontrez que $\mathbb{Q} \subseteq \mathbb{Q}\left(e^{\frac{2\pi i}{p^n}}\right)$ est $(\mathbb{Z}/p^n\mathbb{Z})^\times$-Galoisienne.

   Indice: Pour $n = 1$, en utilisant comme vu en cours que $x^{p-1} + x^{p-2} + \cdots + 1$ est irréductible montrez que $\mathbb{Q}(e^{\frac{2\pi i}{p}})$ est une extension de degré $p - 1$. Ensuite, utilisez le point précédent par induction pour conclure que l'extension $\mathbb{Q} \subseteq \mathbb{Q}\left(e^{\frac{2\pi i}{p^n}}\right)$ est de degré $|\,(\mathbb{Z}/p^n\mathbb{Z})^\times\,|$. Ensuite, montrez que si ϕ est dans le groupe Galois et $\xi = e^{\frac{2\pi i}{p}}$, alors $\phi(\xi) = \xi^k$ pour un $k \in \mathbb{Z}$ avec $(k, p) = 1$, ce qui donnera lieu en réduisant k modulo p^n à une injection du groupe Galois dans $(\mathbb{Z}/p^n\mathbb{Z})^\times$, ce qui permettra de conclure.

Solution.

1. Si il y avait une racine multiple de $f(x) = x^n - 1$, alors on saurait par le cours que $f(x)$ et $f'(x)$ ne serait pas premiers entre eux. Or, $f'(x) = nx^{n-1}$, qui est premier avec $f(x)$.

2. Soit ϕ un générateur de $\mathrm{Gal}(L/K) \cong \mathbb{Z}/n\mathbb{Z}$.

   Notons tout d'abord que comme $\phi^n = id$ par hypothèse, le polynôme minimal de ϕ en tant application K-linéaire divise $x^n - 1$.

   Donnons deux preuves que ϕ admet une racine primitive n-ième de l'unité comme valeur propre.

   Preuve 1. Le polynôme minimal de ϕ est ainsi scindé est à racine simples, donc l'application ϕ est diagonalisable.[†]

[†]On rappelle le *lemme des noyaux* (voir fin de corrigé pour un rappel d'une preuve) qui dit que si $\phi\colon V \to V$ est un endomorphisme d'un K-espace vectoriel, $f(x) = \prod_i g_i(x)$ est une décomposition en irréductibles dans $K[t]$ et que $f(\phi) = 0$ alors $V = \bigoplus_i \ker(g_i(\phi))$. Si f est scindé à racines simples $f = \prod_i (x - \lambda_i)$, alors ϕ restreint au sous-espace correspondant est la multiplication par λ_i, ce qui démontre que ϕ est diagonalisable.

Il suffit de montrer que $x^n - 1$ est le polynôme minimal de l'application linéaire ϕ pour montrer qu"il existe une racine primitive n-ième de l'unité comme valeur propre. Pour cela, il suffit alors de montrer que tout espace propre est de dimension 1. En effet, on aura dès-lors nécessairement n valeurs propres distinctes, et donc que le degré du polynôme minimal est égal à n.

Montrons que tout espace propre est de dimension 1. Soit ξ une valeur propre, qui est nécessairement une racine de l'unité en tant que racine de $x^n - 1$. Notons d son ordre multiplicatif. Soit x un vecteur propre associé à la valeur propre ξ. On note alors que x^i est un vecteur propre associé à la valeur propre ξ^i car $\phi(x^i) = \phi(x)^i = \xi^i x^i$. Cela nous permet de déduire que

$$1, x, x^2, \ldots, x^{d-1}$$

est une base de vecteurs propres à valeurs propres distinctes du sous-espace stable par ϕ qu'est l'extension intermédiaire $K(x)$. En effet x^d étant associé à la valeur propre 1, x^d est fixé par ϕ et donc on a $x^d \in K$ et donc que $[K(x)\colon K] \leq d$. Dès-lors le fait que les valeurs propres des éléments ci-dessus soient distinctes implique leur indépendance linéaire et donc que la liste forme une base de $K(x)$ sur K. Soit x' un autre vecteur propre associé à la valeur propre ξ. Par la correspondance de Galois, il existe une *unique* sous-extension de degré d sur K, car il existe un unique sous-groupe d'ordre n/d dans $\mathbb{Z}/n\mathbb{Z}$. Cela implique donc que $K(x) = K(x')$. Mais alors il suit que x' est colinéaire à x en comparant les valeurs propres, montrant par suite notre assertion que tous les espaces propres sont 1-dimensionnels. □

Preuve 2. Supposons tout d'abord que $n = p^j$ pour un certain $j > 0$ et p premier. Soit $f(t)$ le polynôme minimal de l'application linéraire ϕ (et donc comme noté ci-dessus, $f(t)$ divise $t^{p^j} - 1$). Si par contradiction ϕ n'admettait pas de valeur propre étant une racine primitive p^j'ème de l'unité, alors ϕ devrait automatiquement diviser $t^{p^{j-1}} - 1$, vu que

$$t^{p^j} - 1 = (t^{p^{j-1}} - 1) \prod_{\alpha} (t - \alpha),$$

ou le produit se fait sur les racine primitives p^j'ème de l'unité α.

Comme le polynôme minimal annule ϕ, on aurait que $\phi^{p^{j-1}} = id$, ce qui contredit l'hypothèse sur l'ordre de ϕ. Ainsi, on est bon dans ce cas.

Soit maintenant n général, et écrivons $n = p_1^{j_1} \ldots p_s^{j_s}$. Pour tout $1 \leq r \leq s$, on sait par le théorème fondamental de la théorie de Galois qu'il existe une (unique) sous-extension Galoisienne F_r de L de groupe de Galois $\mathbb{Z}/p_j^{r_j}\mathbb{Z}$ (la sous-extension est Galoisienne, car on est dans un groupe abélien, donc tous les sous-groupes sont normaux). Comme F_r/K est Galoisienne, on sait par le cours que ϕ fixe F_r. De plus, la restriction de ϕ à F_r correspond à une surjection $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/p_r^{j_r}\mathbb{Z}$, donc l'image de ϕ doit être une générateur de $\mathrm{Gal}(F_r/K)$. En particulier, $\phi|_{F_r}$ est d'ordre $p_j^{j_r}$. Ainsi, on sait par le cas précédent que $\phi|_{F_r}$ admet un vecteur propre $a_r \in F_r$ de valeur propre λ_r une racine primitive $p_r^{j_r}$ de l'unité.

Il est direct de vérifier que $a_1 \ldots a_s$ est alors aussi un vecteur propre, de valeur propre une racine primitive n-ième de l'unité. □

Soit alors x un vecteur propre associé à une racine *primitive* n-ième de l'unité. On voit alors en suivant le même raisonnement que dans la première preuve que $L = K(x)$ avec une base de vecteurs propre pour ϕ

$$1, x, x^2, \ldots, x^{n-1}$$

et que $a = x^n$ satisfait à l'énoncé.

3. Notons que L est Galoisienne car le polynôme minimal du générateur de l'extension est scindé et séparable. Il suffit de montrer que l'ordre de l'extension est p car la seule classe d'isomorphisme de groupe d'ordre p est celle de $\mathbb{Z}/p\mathbb{Z}$. Soit ϕ non trivial dans le groupe de

Galois. Notons que $\phi(\alpha) = \xi\alpha$ pour ξ une racine primitive p-ième de l'unité car ϕ permute les racines du polynôme minimal. Mais alors $\phi^s(\alpha) = \xi^s\alpha$ et donc le premier minimal tel que $\phi^s(\alpha) = \alpha$ est p, ce qui démontre l'assertion.

Démontrons le corollaire. Nous voyons par ci-dessus que $K(\sqrt[p]{a})$ est de degré p sur K. Comme $x^p - a$ annule le générateur de cette extension, il en suit que c'est le polynôme minimal de ce dernier, concluant. Un contre exemple pour n pas premier: Dans $K = \mathbb{Q}(i, \sqrt{2})$, il n'y a pas de racine quatrième de 2 (voir. premier exercice) et

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

qui n'est donc pas irréductible.

4. Comme $x^{p-1} + \cdots + x + 1$ est irréductible par un exemple du cours, on voit que

$$\mathbb{Q} \subset \mathbb{Q}(e^{\frac{2\pi i}{p}})$$

est de degré $p-1$. Maintenant, par le point précédent, on voit que $\mathbb{Q}\left(e^{\frac{2\pi i}{p^j}}\right) \subseteq \mathbb{Q}\left(e^{\frac{2\pi i}{p^{j+1}}}\right)$ pour $1 \leq j \leq n-1$ sont de degré p. Dès lors, on voit que

$$\mathbb{Q} \subset \mathbb{Q}(e^{\frac{2\pi i}{p^n}})$$

est de degré $p^n - p^{n-1} = p^{n-1}(p-1) = |\,(\mathbb{Z}/p^n\mathbb{Z})^\times\,|$. Notons G le groupe de Galois et prenons $\phi \in G$. Notons $j(\phi) \in \mathbb{Z}$ un entier tel que $\phi(e^{\frac{2\pi i}{p^n}}) = e^{\frac{2\pi i j(\phi)}{p^n}}$. Notons que $(j(\phi), p) = 1$ car cette dernière racine est nécessairement primitive, en tant qu'image par un automorphisme d'une racine primitive. Ainsi, on voit que $G \to (\mathbb{Z}/p^n\mathbb{Z})^\times$ qui envoie $\phi \mapsto \phi(j) \mod n$ est un morphisme de groupe bien défini. Comme un automorphisme est entièrement déterminé par sa valeur en $e^{\frac{2\pi i}{p^n}}$, on conclut que ce morphisme est injectif, et donc un isomorphisme par cardinalité.

Preuve du lemme des noyaux. Dans le point 2 de l'exercice ci-dessus on fait appel à un petit lemme d'algèbre linéaire qui suit du résultat suivant. *Soit $\phi\colon V \to V$ un endomorphisme d'un K-espace vectoriel et $f, g \in K[t]$ deux polynômes tels que $(f, g) = 1$. Alors*

$$\ker(fg(\phi)) = \ker(f(\phi)) \oplus \ker(g(\phi)).$$

Preuve. On rappelle que $f(\phi)$ désigne l'image par f du morphisme $\mathrm{ev}_\phi\colon K[t] \to End(V)$. Soit $a, b \in K[t]$ avec $1 = af + bg$, donc $\mathrm{id} = af(\phi) + bg(\phi)$. Si $fg(\phi)(v) = 0$, alors $f(\phi)bg(\phi)(v) = fbg(\phi)(v) = 0$ et $g(\phi)af(\phi)(v) = gaf(\phi)(v) = 0$. Il suit que $bg(\phi)$ et $af(\phi)$ sont les deux projecteurs désirés sur $\ker(fg(\phi))$.

Exercice 3. 1. Démontrez que $\mathbb{Q}\left(e^{\frac{2\pi i}{9}} + e^{-\frac{2\pi i}{9}}\right)$ est $\mathbb{Z}/3\mathbb{Z}$-galoisisenne.

Indice: considérez l'extension $\mathbb{Q}\left(e^{\frac{2\pi i}{9}}\right)$.

2. Plus généralement, démontrez que pour chaque entier premier p, il existe une extension $\mathbb{Q} \subseteq L$ tel que $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/p\mathbb{Z}$.

Indice: Pour $p \geq 3$ considérez l'extension $\mathbb{Q} \subseteq \mathbb{Q}\left(e^{\frac{2\pi i}{p^2}}\right)$, et appliquez le théorème fondamental de la théorie de Galois.

Solution.

1. Soit $\alpha := e^{2i\pi/p}$ (et donc $\alpha^{-1} = e^{-2i\pi/9}$).

   Par le point 4 de l'exercice précédent, on sait que l'extension $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ est $(\mathbb{Z}/9\mathbb{Z})^\times$-Galoisienne. De plus, $(\mathbb{Z}/9\mathbb{Z})^\times \cong \mathbb{Z}/6\mathbb{Z}$ (ce groups multiplicatif est généré par 2), et donc il existe un unique élément d'ordre 2.

   De plus, la conjugaison complexe σ agit sur $\mathbb{Q}(\alpha)$, vu que $\sigma(\alpha) = \overline{\alpha} = \alpha^{-1}$. Ainsi, $\sigma \in \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ et correspond donc a cet unique élément d'ordre 2 (et son élément correspondant dans $\mathbb{Z}/6\mathbb{Z}$ est nécessairement 3). Comme le sous-groupe $H\langle\sigma\rangle \subseteq \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ est normal, on sait par le théorème fondamental que l'extension $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)^H$ est Galoisienne, de groupe de Galois

   $$\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})/H \cong (\mathbb{Z}/6\mathbb{Z})/\langle 3\rangle \cong \mathbb{Z}/3\mathbb{Z}.$$

   Il suffit donc de montrer que $\mathbb{Q}(\alpha)^H = \mathbb{Q}(\alpha + \alpha^{-1})$. L'inclusion $\mathbb{Q}(\alpha + \alpha^{-1}) \subseteq \mathbb{Q}(\alpha)^H$ est immédiate, car $\alpha + \alpha^{-1}$ est fixé par σ. Comme $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)^H$ est de degré 3, il suffit de montrer que $\mathbb{Q} \subseteq \mathbb{Q}(\alpha + \alpha^{-1})$ est aussi de degré 3. Or, on a que

   $$3 = [\mathbb{Q}(\alpha)^H : \mathbb{Q}] = [\mathbb{Q}(\alpha)^H : \mathbb{Q}(\alpha + \alpha^{-1})][\mathbb{Q}(\alpha + \alpha^{-1}) : \mathbb{Q}]$$

   donc si par contradiction $\mathbb{Q}(\alpha + \alpha^{-1}) \neq \mathbb{Q}(\alpha)^H$, alors automatiquement $\mathbb{Q} = \mathbb{Q}(\alpha + \alpha^{-1})$, en d'autres termes que $\alpha + \alpha^{-1} = \mathbb{Q}$.

   Montrons que ce n'est pas le cas. On a que

   $$(\alpha + \alpha^{-1}) = e^{2i\pi/3} + e^{-2i\pi/3} + 3(\alpha + \alpha^{-1}) = -1 + 3(\alpha + \alpha^{-1})$$

   donc $\alpha + \alpha^{-1}$ est une racine de $f(x) = x^3 - 3x + 1$. Il suffit donc de montrer que $f(x) \in \mathbb{Q}[x]$ est irréductible. Par Gauss et réduction modulo 2, il suffit de montrer que $x^3 + x + 1 \in \mathbb{F}_2[x]$ est irréductible. Or, c'est immédiat car ce polynôme est de degré 3 et n'a pas de racines.

2. Pour $p = 2$, on a déjà vu par exemple que $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ était Galoisienne de degré 2. Supposons maintenant $p \geq 3$, et posons $\alpha = e^{2i\pi/p^2}$. Alors par l'exercice précédent, $\mathbb{Q}(\alpha)/\mathbb{Q}$ est Galoisien de groupe de Galois $(\mathbb{Z}/p^2\mathbb{Z})^\times$. Ce groupe est abélien d'ordre $\varphi(p^2) = p(p-1)$, donc par le théorème structural des groupe abéliens, on sait que l'on a

   $$(\mathbb{Z}/p^2\mathbb{Z})^\times \cong \mathbb{Z}/p\mathbb{Z} \times H$$

   pour H un groupe abélien d'ordre $p - 1$. Ce groupe est automatiquement normal (car tout est abélien ici), et donc par le théorème fondamental de la théorie de Galois, $\mathbb{Q}(\alpha)^H/\mathbb{Q}$ est Galoisienne de groupe de Galois

   $$(\mathbb{Z}/p\mathbb{Z} \times H)/H \cong \mathbb{Z}/p\mathbb{Z}.$$

Exercice 4.
Soit K un corps, et soit $K \subseteq M = K(\alpha)$ et $K \subseteq N = K(\beta)$ des extensions galoisiennes de K.

1. Démontrez que $K \subseteq L = K(\alpha, \beta)$ est aussi galoisienne.

Supposons à partir de maintenant que $M \cap N = K$ en tant que sous-corps de L.

2. Démontrez que $\mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K) \times \mathrm{Gal}(N/K)$ qui est la restriction sur chaque composante est un isomorphisme.

3. Démontrez que pour chaque entiers premiers distincts p et q, il existe une extension $\mathbb{Q} \subseteq L$ galoisienne tel que $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/pq\mathbb{Z}$.

Solution.

1. On sait par le cours qu'une extension est Galoisienne si et seulement si c'est un corps de décomposition d'un polynôme séparable. Ainsi les polynômes $m_{\alpha,K}$ et $m_{\beta,K}$ sont séparables et se scindent sur $K(\alpha)$ et $K(\beta)$ respectivement. Ainsi, le polynôme $m_{\alpha,K}m_{\beta,K}$ est aussi séparable et se scinde sur $K(\alpha,\beta)$. Comme $K(\alpha,\beta)$ est généré par les racines de $m_{\alpha,K}m_{\beta,K}$ (il est généré par α et β), c'est bien un corps de décomposition de $m_{\alpha,K}m_{\beta,K}$. Par le même fait rappelé plus haut, $K(\alpha,\beta)$ est Galoisien sur K.

2. Comme M/K est Galoisienne, on sait que pour tout $\sigma \in \mathrm{Gal}(L/K)$, $\sigma(M) = M$. Ainsi, σ se restricte en un élément $\sigma|_M \in \mathrm{Gal}(M/K)$, et on a donc un morphisme de groupes $\mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$. En faisant la même chose pour N, on en déduit un morphisme de groupes

$$\begin{aligned} \mathrm{Gal}(L/K) &\xrightarrow{\quad\phi\quad} \mathrm{Gal}(M/K) \times \mathrm{Gal}(N/K) \\ \sigma &\longmapsto (\sigma|_M, \sigma|_N) \end{aligned}$$

   Ce morphisme est automatiquement injectif, car si $\sigma \in \mathrm{Gal}(L/K)$ se restreint à l'identité sur M et sur N, alors il fixe α et β. Come $L = K(\alpha,\beta)$, on doit avoir $\sigma = id$.

   De plus, $|\mathrm{Gal}(L/K)| = [L:K]$ et

$$|\mathrm{Gal}(M/K) \times \mathrm{Gal}(N/K)| = |\mathrm{Gal}(M/K) \cdot |\mathrm{Gal}(N/K)| = [M:K][N:K].$$

   Supposons que l'on a prouvé que $[L:M] = [N:K]$. Alors

$$[M:K][N:K] = [M:K][L:M] = [L:K].$$

   Ainsi, ϕ est un morphisme injectif entre groupes finis ayant le même cardinal. C'est donc automatiquement un isomorphisme, ce qui conclut la preuve.

   Montrons maintenant que $[L:M] = [N:K]$ (c'est ici ou on utilisera que $M \cap N = K$!). Comme $L = M(\beta)$, il est équivalent de montrer que $\deg(m_{\beta,M}) = \deg(m_{\beta,K})$. Comme $m_{\beta,M}$ divise $m_{\beta,K}$, ce qu'il faut réellement montrer est que $m_{\beta,M} = m_{\beta,K}$.

   Comme $m_{\beta,K}$ sur scinde sur N, on a que

$$m_{\beta,K}(t) = \prod_i (t - \beta_i) \in N[t],$$

   où le produit se fait sur les racines de $m_{\beta,K}$. Ainsi, en voyant $m_{\beta,M}(t)$ comme un élément de $L[t]$, on a nécessairement que

$$m_{\beta,M}(t) = c\prod_j (t - \beta_j)$$

   où $c \in L$ et les β_j sont certaines racines de $m_{\beta,K}$. Comme $m_{\beta,M}$ est unitaire, $c = 1$ et donc comme tous les β_j sont dans N, on en déduit que $m_{\beta,M}(t) \in N[t]$. Ainsi $m_{\beta,M}(t) \in M[t] \cap N[t] = K[t]$, et comme il s'annule en β, il est divisible par $m_{\alpha,K}(t)$. Cela conclut donc la preuve.

3. Par l'exercice précédent, on sait qu'il existe des extensions $\mathbb{Q} \subseteq M \subseteq \mathbb{C}$ et $\mathbb{Q} \subseteq N \subseteq \mathbb{C}$, de groupes de Galois sur $\mathbb{Q}$ valant $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z}$ respectivement.

   Montrons que $M \cap N = \mathbb{Q}$. Par les extensions $\mathbb{Q} \subseteq M \cap N \subseteq N$ et le fait que $[N:\mathbb{Q}]$ est un nombre premier, on a que soit $M \cap N = \mathbb{Q}$, soit $M \cap N = N$. En faisant le même raisonnement pour M, on en déduit que soit $M = M \cap N = N$, soit $M \cap N = \mathbb{Q}$. Le premier cas est impossible, car $p \neq q$.

   Par le théorème de l'élément primitif, on peut écrire $M = \mathbb{Q}(\alpha)$ et $N = \mathbb{Q}(\beta)$, donc par les deux points précédents, $L = \mathbb{Q}(\alpha,\beta)$ est Galoisienne sur $\mathbb{Q}$, de groupe de Galois

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

Exercice 5.
Soit $K \subseteq L$ une extension Q_8-galoisienne (où Q_8 est le groupe des quaternions), et soit $f \in K[x]$ un polynôme irréductible tel que L est un corps de décomposition de f. Démontrez que $\deg f = 8$.

Solution.

Supposons par l'absurde que $d := \deg(f) < 8$, et soit $\alpha \in L$ une racine de f. Alors $[K(\alpha) : K] = d < 8$, donc il suffit de montrer que $K(\alpha) = L$ pour obtenir une contradiction.

Comme tous les sous-groupes de Q_8 sont normaux (nous vous laissons le soin de faire ce calcul), l'extension $K(\alpha)/K$ est Galoisienne par le théorème fondamental de la théorie de Galois. On sait que dans une extension Galoisienne, tout les polynômes minimaux des éléments scindent, les racines de ces polynômes étant formant des orbites sous le groupe de Galois. O<n en déduit que $m_{\alpha,K} = f$ se scinde sur $K(\alpha)$. Comme L est le corps de décomposition de L, on a donc forcément que $L = K(\alpha)$, ce qui donne une contradiction.

EPFL - Printemps 2025	Prof. Zs. Patakfalvi
Anneaux et Corps	**Exercices**
Solutions 14	

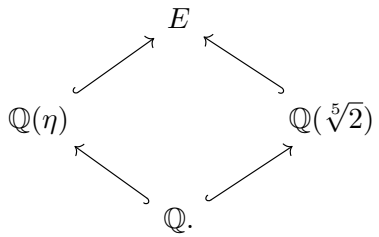
Les exercices marqués d'une étoile ($\star$) sont optionnels.

Exercice 1 (Correspondance de Galois)**.**
Soit $f = x^5 - 2 \in \mathbb{Q}[x]$, et soit E le corps de décomposition de f sur $\mathbb{Q}$.

1. Montrez que $[E : \mathbb{Q}] = 20$.
2. Montrez qu'il existe un morphisme de groupes $f\colon \mathbb{Z}/4\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/5\mathbb{Z})$ tel que
$$\mathrm{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z} \rtimes_f \mathbb{Z}/4\mathbb{Z},$$
et identifiez explicitement f.
3. *Un peu de théorie des groupes.*
   (a) Comme $\mathbb{Z}/5\mathbb{Z} \times 0$ est normal dans $\mathbb{Z}/5\mathbb{Z} \rtimes_f \mathbb{Z}/4\mathbb{Z}$, déduisez comme c'est un 5-Sylow qu'il y a un unique sous-groupe d'ordre 5 dans $\mathrm{Gal}(E/\mathbb{Q})$, qu'on note H_5.
   (b) Soit H un sous-groupe d'ordre 10. Montrez que $H_5 \subset H$. En prenant le quotient par H_5 et en utilisant le théorème de correspondance, déduisez que $\mathrm{Gal}(E/\mathbb{Q})$ a un unique sous-groupe d'ordre 10, qu'on note H_{10}, que celui-ci est normal et isomorphe à D_{10}.
   (c) On rappelle que si $H, K \subset G$ sont des sous-groupes normaux d'un groupe avec $H \cap K = \{e\}$, alors HK est un sous-groupe de G isomorphe au produit direct $H \times K$. En utilisant cela, montrez qu'il n'existe pas de sous-groupes normaux d'ordre 4 et 2 dans $\mathrm{Gal}(E/\mathbb{Q})$.
4. Listez toutes les sous-extensions Galoisiennes sur $\mathbb{Q}$ de E et donnez des éléments primitifs pour ces extensions.

Solution. Soit $\eta = e^{2i\pi/5}$.

1. On peut poser $E = \mathbb{Q}(\sqrt[5]{2}, \eta)$, et on a ainsi un diagramme d'extensions



   Vu que $[\mathbb{Q}(\eta) : \mathbb{Q}] = 4$ (c.f. exercice 4 de la série 13), on a que 4 divise $[E, \mathbb{Q}]$. Similairement, vu que $[\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}] = 5$ (le polynôme $x^5 - 2$ est irréductible par Gauss et Eisenstein), on a que 5 divise $[E : \mathbb{Q}]$.

   D'un autre côté, $[E : \mathbb{Q}] = [E : \mathbb{Q}(\eta)][\mathbb{Q}(\eta) : \mathbb{Q}] = [E : \mathbb{Q}(\eta)]4$. Vu que $[E : \mathbb{Q}(\eta)] = [\mathbb{Q}(\eta)(\sqrt[5]{2}) : \mathbb{Q}(\eta)] \leq 5$ ($m_{\sqrt[5]{2}, \mathbb{Q}(\eta)}$ divise $x^5 - 2$), on a que $[E : \mathbb{Q}] \leq 20$. On a donc égalité.

2. Comme $E/\mathbb{Q}$ est Galoisienne, on sait que $E/\mathbb{Q}(\eta)$ est aussi Galoisienne (et elle est de degré 5 par le point précédent).

   Ainsi, $x^5 - 2$ est bien le polynôme irréductible de $\sqrt[5]{2}$ sur $\mathbb{Q}(\eta)$ (il a le bon degré), et donc vu que $\sqrt[5]{2}$ et $\eta\sqrt[5]{2}$ sont des racines, on sait alors qu'il existe $\sigma \in \mathrm{Gal}(E/\mathbb{Q}(\eta)) \subseteq \mathrm{Gal}(E/\mathbb{Q})$ envoyant $\sqrt[5]{2}$ sur $\eta\sqrt[5]{2}$. Vu que σ est automatiquement d'ordre 5, on en déduit que
$$\mathrm{Gal}(E/\mathbb{Q}(\eta)) = \langle\sigma\rangle \cong \mathbb{Z}/5\mathbb{Z}.$$

Le même argument qu'avant montre que $x^4+x^3+x^2+x+1 = \frac{x^5-1}{x-1}$ est le polynôme minimal de η sur $\mathbb{Q}(\sqrt[5]{2})$. Vu que η et η^2 sont des racines de ce polynômes, il existe $\tau \in \mathrm{Gal}(E/\mathbb{Q}(\sqrt[5]{2}))$ envoyant η sur η^2. Vu que η est une racine primitive 5eme de l'unité, on en déduit que τ est d'ordre 4. Comme

$$[E : \mathbb{Q}(\sqrt[5]{2})] = 4,$$

on en déduit que

$$\mathrm{Gal}(E/\mathbb{Q}(\sqrt[5]{2})) = \langle \tau \rangle \cong \mathbb{Z}/4\mathbb{Z}.$$

Soit $H := \langle \sigma \rangle$ et $K = \langle \tau \rangle$. Vu que $H \cap K = \{id\}$ (son ordre divise 4 et 5), et que H est normal dans $\mathrm{Gal}(E/\mathbb{Q})$ (l'extension associée, i.e. $\mathbb{Q}(\eta)$, est le corps de décomposition de $x^4+x^3+x^2+x+1$), on en déduit que $HK = \mathrm{Gal}(E/\mathbb{Q})$ et que

$$\mathrm{Gal}(E/\mathbb{Q}) \cong H \rtimes_\phi K,$$

où le morphisme associé $K \to \mathrm{Aut}(H)$ est donné par la conjugaison.

Vu que $\tau\sigma\tau^{-1} = \sigma^2$ (cela se calcule explicitement en étudiant leur action sur les racines de x^5-2), on en déduit qu'à travers les isomorphismes $H \cong \mathbb{Z}/5\mathbb{Z}$ et $K \cong \mathbb{Z}/4\mathbb{Z}$ donnés auparavant, le morphisme $f\colon \mathbb{Z}/4\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/5\mathbb{Z})$ envoie 1 (i.e. τ) sur le morphisme $\mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$ donné par $(\cdot 2)$, vu qu'il envoie le générateur σ sur σ^2. On a donc

$$\mathrm{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z} \rtimes_f \mathbb{Z}/4\mathbb{Z}$$

avec f explicité juste avant.

3. (a) Comme tous les 5-Sylow sont conjugés, et que l'un d'entre eux est normal, on conclut.
   (b) Un groupe d'ordre 10 possède un élément d'ordre 5 car 5 est premier (en utilisant le "théorème de Cayley"). Comme H_5 est le seul-sous groupe d'ordre 5, il suit que $H_5 \subset H$. Comme $\mathrm{Gal}(E/\mathbb{Q})/H_5 \cong \mathbb{Z}/4\mathbb{Z}$ et que ce dernier a un unique sous-groupe normal d'ordre 2, on déduit que H_{10} est l'unique sous-groupe normal d'ordre 10 de $\mathrm{Gal}(E/\mathbb{Q})$. Notons que comme H_{10} est d'indice 2, tout carré de $\mathrm{Gal}(E/\mathbb{Q})$ est dans H_{10}. Dès lors, $\langle \sigma, \tau^2 \rangle \subset H_{10}$. Mais on sait aussi que

   $$\sigma^5 = (\tau^2)^2 = e \quad \sigma\tau^2\sigma^{-1} = \tau^{-2}.$$

   On reconnaît alors la présentation de D_{10}, ce qui conclut.
   (c) S'il y avait un sous-groupe normal d'ordre 4, disons K_4, alors $\mathrm{Gal}(E/\mathbb{Q}) \cong H \times K$, et serait donc abélien, une contradiction. Similairement, s'il y avait un sous-groupe normal d'ordre 2, disons K_2, alors $H_{10} \cong H \times K_2$, et serait donc abélien, une contradiction.

4. Par le point précédent, comme les sous-groupes de $\mathrm{Gal}(E/\mathbb{Q})$ sont d'ordre 2,4,5, ou 10, on conclut que $\mathrm{Gal}(E/\mathbb{Q})$ a exactement quatres sous-groupes normaux

   $$\{e\}, \quad H_5, \quad H_{10}, \quad \mathrm{Gal}(E/\mathbb{Q}).$$

   On calcule donc des éléments primitifs pour les extensions correspondantes des trois premiers sous-groupes, le quatrième correspondant à $\mathbb{Q}$.

   (a) Le sous-groupe fixé par $H_5 = \langle \sigma \rangle$ est d'ordre 4. Par construction on a $\sigma(\eta) = \eta$ et cet élément est d'ordre 4 comme expliqué plus haut. On conclut donc que

   $$E^{H_5} = \mathbb{Q}(\eta).$$

   (b) Le sous-corps fixé par $H_{10} = \langle \sigma, \tau^2 \rangle$ est de degré 2. De plus on sait que c'est une sous-extension de $E^{H_5} = \mathbb{Q}(\eta)$ – en effet $H_5 \subset H_{10}$. Notons que comme $1, \eta, \eta^2, \eta^3, \eta^4$ est une base de $\mathbb{Q}(\eta)$, on voit que $\eta + \eta^4 = \eta + \eta^{-1}$ n'est pas dans $\mathbb{Q}$. Dès lors on conclut que

   $$E^{H_{10}} = \mathbb{Q}(\eta + \eta^{-1}).$$

Exercice 2.
Soit K un corps de caractéristique différente de 2, soit f un polynôme irréductible séparable sur K, et soient $\alpha_1, \ldots, \alpha_n$ les racines de f dans un corps de décomposition. Le *discriminant* de f est par définition

$$\Delta := \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

Montrez que $\Delta \in K$, et que les conditions suivantes sont équivalentes :

- Δ est un carré dans K;
- le morphisme naturel $\mathrm{Gal}(E/K) \to S_n$ défini par l'action sur les racines de f se factorise dans le groupe alterné A_n.

Indice: $\delta = \prod_{i<j}(\alpha_i - \alpha_j)$ est une racine carrée de Δ.

Solution. Soit E un corps de décomposition de f sur K. Comme f est irréductible et séparable, on sait par le cours que K/E est Galoisienne. Soit $\sigma \in \mathrm{Gal}(L/K)$, et montrons que $\sigma(\Delta) = \Delta$. Un calcul rapide montre que

$$\prod_{i<j}(\alpha_i - \alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j}(\alpha_i - \alpha_j),$$

et vu que σ permute les racines, on voit donc que $\sigma(\Delta) = \Delta$. On a donc montré que $\Delta \in L^{\mathrm{Gal}(L/K)} = K$.

Montrons maintenant l'équivalent de l'exercice. Notez que vu que $\delta^2 = \Delta$ et que les seules racines carrées de Δ sont $\pm\delta$, on a que Δ est un carré dans K si et seulement si $\delta \in K$. Comme L/K est Galoisienne, on en Δ est un carré dans K si et seulement si pour tout $\sigma \in \mathrm{Gal}(L/K)$, $\sigma(\delta) = \delta$.

Considérons ϕ: $\mathrm{Gal}(L/K) \to S_n$ le morphisme correspondant à l'action sur les racines de f. On montre à la main que

$$\sigma(\delta) = \sigma\left(\prod_{i<j}(\alpha_i - \alpha_j)\right) = (-1)^{\mathrm{sgn}(\phi(\sigma))} \prod_{i<j}(\alpha_i - \alpha_j) = (-1)^{\mathrm{sgn}(\phi(\sigma))}\delta,$$

donc vu qu'on est en caractéristique différent de 2 et que $\delta \neq 0$ (f est séparable), on en déduit que $\sigma(\delta) = \delta$ si et seulement si $\mathrm{sgn}(\phi(\sigma)) = 1$, i.e. $\phi(\sigma) \in A_n$.

Exercice 3.
Soit $f = x^3 + ax + b \in \mathbb{Q}[x]$ un polynôme irréductible de discriminant Δ (c.f. l'exercice précédent).

1. Montrez qu'on a deux cas:
   - Si Δ n'est pas un carré dans $\mathbb{Q}$, alors $\mathrm{Gal}(E/\mathbb{Q}) \cong S_3$;
   - Si Δ est un carré dans $\mathbb{Q}$, alors $\mathrm{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$.
2. Montrez que $\Delta = -(4a^3 + 27b^2)$.

   Indice: Soient $\alpha_1, \alpha_2, \alpha_3$ les racines de f dans un corps de décomposition. Montrez que $\Delta = -f'(\alpha_1)f'(\alpha_2)f'(\alpha_3)$, et écrivez $x^3 + ax + b = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ pour trouver des relations entre les α_i qui permettent de faire le calcul. Pour vous entraîner, vous pouvez essayer de faire le calcul pour un polynôme de degré 2 sans utiliser les formules pour les solutions (vous devriez trouver le determinant habituel!).
3. Trouvez deux extensions Galoisiennes K_1, K_2 de $\mathbb{Q}$ réelles (i.e. $K_1, K_2 \subseteq \mathbb{R}$) telles que $\mathrm{Gal}(K_1/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$ et $\mathrm{Gal}(K_2/\mathbb{Q}) \cong S_3$.

Solution.

1. Si Δ n'est pas un carré, alors on sait par l'exercice précédent que l'image de l'inclusion $\mathrm{Gal}(E/\mathbb{Q}) \to S_3$ n'est pas dans A_3. Comme

$$|\mathrm{Gal}(E/\mathbb{Q})| = [E:\mathbb{Q}] \geq 3,$$

et que A_3 est l'unique sous-group d'ordre 3 de S_3, on en déduit que l'injection $\mathrm{Gal}(E/\mathbb{Q}) \to S_3$ est automatiquement surjective.

De même, si Δ est un carré, alors l'image de l'injection $\mathrm{Gal}(E/\mathbb{Q}) \to S_3$ est incluse dans $A_3 \cong \mathbb{Z}/3\mathbb{Z}$. Vu que $|\mathrm{Gal}(E/\mathbb{Q})| \geq 3$, cette injection est automatiquement surjective.

2. En utilisant que $f(x) = x^3 + ax + b = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$, on a que

$$\begin{cases} -\alpha_1\alpha_2\alpha_3 = b \\ \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = a \\ \alpha_1 + \alpha_2 + \alpha_3 = 0. \end{cases}$$

Calculons maintenant Δ. On a $f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$, et donc $f'(x) = (x-\alpha_1)(x-\alpha_2) + (x-\alpha_1)(x-\alpha_3) + (x-\alpha_2)(x-\alpha_3)$. Ainsi,

$$f'(\alpha_1)f'(\alpha_2)f'(\alpha_3) = (\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_1)(\alpha_2-\alpha_3)(\alpha_3-\alpha_2)(\alpha_3-\alpha_1) = -\Delta,$$

donc on a bien l'égalité énoncée dans l'indice.

Comme $f'(x) = 3x^2 + 1$, on a que

$$\begin{aligned} -\Delta &= (3\alpha_1^2 + a)(3\alpha_2^2 + a)(3\alpha_3^2 + a) \\ &= 27(\alpha_1\alpha_2\alpha_3)^2 + 3a^2(\alpha_1^2 + \alpha_2^2 + \alpha_3^2) + 9a(\alpha_1^2\alpha_2^2 + \alpha_1^2\alpha_3^2 + \alpha_2^2\alpha_3^2) + a^3. \end{aligned}$$

Par la première équation, $(\alpha_1\alpha_2\alpha_3)^2 = b^2$. Par les 2e et 3e équations, on a que

$$0 = (\alpha_1 + \alpha_2 + \alpha_3)^2 = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + 2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + 2a,$$

et donc

$$\alpha_1^2 + \alpha_2^2 + \alpha_3^2 = -2a.$$

Enfin, on a que

$$\begin{aligned} a^2 &= (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)^2 \\ &= \alpha_1^2\alpha_2^2 + \alpha_1^2\alpha_3^2 + \alpha_2^2\alpha_3^2 + \alpha_1\alpha_2\alpha_3(\alpha_1 + \alpha_2 + \alpha_3) \\ &= \alpha_1^2\alpha_2^2 + \alpha_1^2\alpha_3^2 + \alpha_2^2\alpha_3^2. \end{aligned}$$

Ainsi, on en déduit que

$$\begin{aligned} -\Delta &= (3\alpha_1^2 + a)(3\alpha_2^2 + a)(3\alpha_3^2 + a) \\ &= 27(\alpha_1\alpha_2\alpha_3)^2 + 3a^2(\alpha_1^2 + \alpha_2^2 + \alpha_3^2) + 9a(\alpha_1^2\alpha_2^2 + \alpha_1^2\alpha_3^2 + \alpha_2^2\alpha_3^2) + a^3 \\ &= 27b^2 - 6a^3 + 9a^3 + a^3 = 27b^2 + 4a^3. \end{aligned}$$

3. Pour trouver K_1 (resp. K_2), il faut trouver un polynôme $f = x^3 + ax + b$ irréductible sur $\mathbb{Q}$, ayant trois racines réelles, tel que Δ est un carré (resp. n'est pas un carré). En effet, le premier point conclura en prenant un corps de décomposition de f dans $\mathbb{R}$.

Pour trouver un tel polynôme ayant trois racines réelles, on utilise une technique ancestrale : WolphramAlpha.

En jouant un peu, on se rend compte que $f = x^3 - 3x - 1$ a bien trois racines réelles. Montrons qu'il est irréductible. Par Gauss, il suffit de montrer que c'est vrai sur $\mathbb{Z}$, et par un lemme de cours il suffit de le montrer sur $\mathbb{F}_2$. Comme ce polynôme est d'ordre 3 et n'a pas de racine sur $\mathbb{F}_2$, il est donc bien irréductible. On a par le point précédent que $\Delta = -(4 \cdot (-3)^3 + 27) = 3 \cdot 27 = 3^4$, qui est bien un carré. On a donc trouvé une extension réelle $\mathbb{Z}/3\mathbb{Z}$–Galoisienne.

En jouant encore plus, on se rend compte que $f = x^3 - 4x - 1$ a aussi trois racines réelles. Par le même argument que juste avant, cela est une conséquence du fait qu'il n'ait pas de racine sur $\mathbb{F}_3$. Comme $\Delta = -(4 \cdot (-4)^3 + 27) = 4^4 - 27 = 229$ est premier, il ne peut pas être un carré, et donc on a trouvé une extension réelle S_3–Galoisienne.

Exercice 4.
Soit $L = K(a)$ une extension simple, et soit A la matrice de l'application K-linéaire $(\cdot a)\colon L \to L$ par rapport à une base quelconque de L. Soit aussi $E \supseteq L$ un corps de décomposition de $m_{a,K}$.

1. Montrez que le polynôme caractéristique $\phi(x) = \det(x\,\mathrm{id} - A)$ de A est égal au polynôme minimal $m_{a,K}$.
2. Montrez que si a est séparable, alors A est diagonalisable dans E.
3. ($\star$) Montrez que si a est purement inséparable, alors A a un seul bloc de Jordan dans E.
4. Montrez que $\det(A) = (-1)^{[L:K]} m_{a,K}(0)$.
5. Montrez que si L/K est Galois, alors $\det(A) = \prod_{g \in G} g(a)$ où $G = \mathrm{Gal}(L/K)$ au signe près.
6. Calculez ce polynôme minimal pour L le corps de décomposition de $x^3 - 2$ sur $\mathbb{Q}$, et $a = \sqrt[3]{2} + e^{2\pi i/3}$.

Solution.

1. Le polynôme caractéristique de A est un polynôme qui annule a par Cayley-Hamilton. Mais il est de degré $[K(a)\colon K]$. Comme le coefficient dominant du polynôme caractéristique avec la coefficient choisie est 1, on conclut.
2. Notons A_E pour la matrice multiplication par a vue comme application K-linéaire sur E. Notons qu'on peut identifier le polynôme minimal de A_E en tant qu'application linéaire (le polynôme avec coefficient dominant 1 de plus petit degré qui annule ϕ_E) au polynôme minimal de $m_{a,K}$. Comme on suppose $m_{a,K}$ séparable et E étant son corps de décomposition, on en déduit que le polynôme minimal en tant qu'application linéaire de ϕ_E est scindé à racines simples, ce qui conclut comme en exercice 2 de la série 13.
3. Notons p la caractéristique finie du corps et q la puissance de p minimale telle que $a^q \in K$. Rappelons que dans ce cas la seule racine du polynôme minimal de a^q est a et que ce polynôme minimal est $x^q - a$. On en déduit qu'au signe près le polynôme caractéristique de de A est $x^q - a$. Mais notons que la seule valeur propre sur $K(a)$ de A est a – ce qui conclut.
4. Suit de l'identification du polynôme caractéristique $\det(x\,\mathrm{id} - A) = \phi(x) = m_{a,K}(X)$.
5. On rappelle que dans ce cas, les racines de $m_{a,K}$ sont les conjugués $(g(a))_{g \in \mathrm{Gal}(L|K)}$. Mais alors comme,
$$m_{a,K}(0) = (-1)^{\deg(m_{a,K})} \prod_{g \in \mathrm{Gal}(L|K)} g(a)$$
on conclut par le point précédent et $\deg(m_{a,K}) = [L\colon K]$.

6. Notons $\xi = e^{2\pi i/3}$. La matrice de multiplication par $\xi + \sqrt[2]{2}$ élément dans la base de L suivante

$$1, \xi, \sqrt[3]{2}, \xi\sqrt[3]{3}, \sqrt[3]{4}, \xi\sqrt[3]{4}$$

est (on utilise $\xi^2 = -1 - \xi$)

$$\begin{pmatrix} 0 & -1 & 0 & 0 & 2 & 0 \\ 1 & -1 & 0 & 0 & 0 & 2 \\ 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 1 & -1 \end{pmatrix}$$

puis on calcule le polynôme caractéristique de cette matrice pour conclure que le polynôme suivant

$$x^6 + 3x^5 + 6x^4 + 3x^3 + 9x + 9$$

Exercice 5 ($\star$)**.**
Montrez que si $K \subseteq L$ et $L \subseteq E$ sont deux extensions séparables (pas nécessairement finies), alors $K \subseteq E$ est aussi séparable.

Solution.
Prenons $\alpha \in E$. Le but est de montrer que α est séparable sur K.
Considérons

$$m_{\alpha,L}(t) = t^{r+1} + \sum_{i=0}^{r} a_i t^i \in L[t]$$

le polynôme minimal de de α sur L. Celui-ci est est séparable par hypothèse. Considérons F le corps de décomposition de $\prod_{i=1}^{r} m_{a_i,K}(t) \in K[t]$. Cette extension $K \subset F$ est Galoisienne sur K étant généré par les racines des $m_{a_i,K}$ qui sont des polynômes séparables sur K comme $K \subset L$ est supposée séparable. Maintenant considérons l'orbite de Galois $\{m_1 = m_{\alpha,L}(t), m_2, \ldots, m_k\}$ de $m_{\alpha,L}(t)$ par $\mathrm{Gal}(F/K)$.* Remarquons que comme la séparabilité d'un polynôme $p(t)$ est équivalente à $\gcd(p(t), p'(t)) = 1$ et que cette condition est stable par automorphisme, on voit que tout les m_i sont séparables. Posons maintenant le polynôme

$$f := \prod_{i=1}^{k} m_i(t).$$

Notons deux choses,

- ce polynôme f est à coefficient dans K car on voit que ce polynôme est stable par l'action de $\mathrm{Gal}(F/K)$,
- ce polynôme est séparable. En effet c'est un produit de polynôme irréductibles séparables distincts de $F[t]$.

Mais comme $f(\alpha) = 0$, on conclut.

Exercice 6 (Extension quadratique pour $\mathrm{car}(k) = 2$) ($\star$)**.**
Soit K un corps de caractéristique 2 et soit $K \subseteq L$ une extension de degré 2.

(a) Supposons que pour tous $\alpha \in L \backslash K$ nous avons que $\alpha^2 \in K$. Montrer que:

(i) $L = K(\alpha)$, où $\alpha \in L \backslash K$.

(ii) tout $\alpha \in L \backslash K$ est inséparable.

*Cela signifie qu'on voit $m_{\alpha,L}(t)$ dans $F[t]$ et qu'on étend un automorphisme $\sigma \in \mathrm{Gal}(F/K)$ à $F[t]$ en envoyant $t \mapsto t$ et en définissant par σ sur les coefficients des polynômes.

(b) Supposons qu'il existe $\alpha \in L\backslash K$ tel que $\alpha^2 \notin K$. Montrer que:

(i) $L = K(\beta)$, où $\beta \in L\backslash K$ est tel que $m_{\beta,K}(x) = x^2 + x + c \in K[x]$.

(ii) $\tau : K(\beta) \to K(\beta)$ donné par $\tau|_K = \mathrm{Id}_K$ et $\tau(\beta) = \beta + 1$ est un automorphisme de $K(\beta)$. Conclure que $\mathrm{Gal}(K(\beta)/K) \cong \mathbb{Z}/2\mathbb{Z}$.

(iii) tout $\alpha \in L\backslash K$ est séparable, c'est à dire que $K \subset L$ est une extension séparable.

Solution.

(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 $|\mathrm{Gal}(K(\beta)/K)| = 2$.

(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 7 $(\star)$**.**
Si K est un corps dénombrable, montrez que $\overline{K}$ est également dénombrable.

Solution. Let K be a countable field and consider the polynomial ring $K[x]$. For all $i \geq 0$ define the subsets $K^i[x] \subseteq K[x]$ with $K^i[x] = \{f \in K[x] | \deg(f) = i\}$. We remark that $K[x] = \bigcup_{i \geq 0} K^i[x]$ and that $K^i[x] \cong K^i$, hence $|K^i[x]| = i \cdot |K| = |K|$, for all $i \geq 0$. It follows that $|K[x]| = \aleph_0 \cdot |K| = \aleph_0$ and so $K[x]$ is also countable.

We define the map $\phi : \overline{K} \to K[x]$ by $\phi(\alpha) = m_{\alpha,K}$. Now the subset $\phi(\overline{K})$ of $K[x]$ contains all polynomials of the form $x - \alpha$, where $\alpha \in K$, hence $\phi(\overline{K})$ is also countable. Lastly, for any $m_{\alpha,K} \in \phi(\overline{K})$ we have that the preimage $\phi^{-1}(m_{\alpha,K})$ is non-empty and finite, as $\alpha \in \phi^{-1}(m_{\alpha,K})$ and $m_{\alpha,K}$ admits a finite number of roots. We conclude that $\overline{K}$ has the same cardinality as $\phi(\overline{K})$, hence it is countable.

Exercice 8 $(\star)$**.**
Fixons un entier premier p. Soit $n_j = p^{m_j}$ où $m_j = \prod_{i=1}^{j} i$ pour chaque entier $j \geq 1$, et soit $K_j = \mathbb{F}_{n_j}$.

1. Démontrez que les K_j peuvent être mis dans un système direct. Autrement dit, il existe des homomorphismes injectifs $\iota_j : K_j \to K_{j+1}$ pour chaque entier $j \geq 1$.

2. Fixons ι_j comme dans le point précédent. Montrez que la colimite directe K, comme définie dans le Lemme 4.8.7, est un corps, et de plus il existe un plongement $\mathbb{F}_p \to K$

3. Démontrez que K est algébrique sur $\mathbb{F}_p$

4. Démontrez que chaque polynôme $f \in \mathbb{F}_p$ scinde sur K. (Autrement dit K est la clôture algébrique de $\mathbb{F}_p$, et on le dénote d'habitude par $\overline{\mathbb{F}}_p$. Dans une manière similaire, le corps de nombres algébriques $\mathbb{C}_{alg,\mathbb{Q}}$, en utilisant la notation du Cor 4.2.22, est la clôture algébrique de $\mathbb{Q}$. Aussi, $\mathbb{C}$ est la clôture algébrique de $\mathbb{R}$. On étudiera plus des clotûre algébriques à la fin du semestre.)

Solution.

1. We know that for every j teh field K_{j+1} contains a subfield isomorphic to K_j because by construction $m_j \mid m_{j+1}$. We can then considered the induced inclusion homomorphism $\iota_j : K_j \to K_{j+1}$ for every $j \geq 1$.

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 colimit is given by

$$\varinjlim_i K_i = \bigsqcup_{i\in\mathbb{N}} K_i \Big/ \begin{array}{l} \text{- } x \equiv \iota_{s-1} \circ \dots \circ \iota_r(x) \text{ et } \iota_{s-1} \circ \dots \circ \iota_r(x) \equiv x \text{ pour chaque entier } \\ \quad s > r, \text{ et } x \in K_r \\ \text{- } x \equiv x \text{ pour chaque } x \in K_r \end{array}$$

   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 colimit 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 9 ($\star$). 1. Si $K \subseteq L$ est une extension purement inséparable, alors $\mathrm{Gal}(L/K) = \{\mathrm{Id}_L\}$.

2. Soit $K \subseteq L$ une extension finie tel que

$$[L_{insep,K} : K] |\mathrm{Gal}(L/K)| = [L : K].$$

   Montrer que L est séparable sur $L_{insep,K}$.

Solution.

1. As $K \subseteq L$ is a purely inseparable extension, it follows that $\alpha \in L \backslash K$ is purely inseparable over K, thus there exists $n \geq 1$ such that $\alpha^{p^n} \in K$. We fix such an $\alpha \in L \backslash K$ and we let $\sigma \in \mathrm{Gal}(L/K)$. It suffices to show that $\sigma(\alpha) = \alpha$.

   The element $\alpha \in L/K$ is the unique p^nth root of α^{p^n}, see Exercise 2.(a) of Series 11. Therefore, it suffices to show that $(\sigma(\alpha))^{p^n} = \alpha^{p^n}$. We have:

   $$(\sigma(\alpha))^{p^n} = \sigma(\alpha^{p^n}) = \alpha^{p^n}.$$

   We conclude that $\mathrm{Gal}(L/K) = \{\mathrm{Id}_L\}$.

2. First, we will show that $L_{insep,K} \subseteq L^{\mathrm{Gal}(L/K)}$. For this, let $\alpha \in L_{insep,K}$ and let $\sigma \in \mathrm{Gal}(L/K)$. As $\alpha \in L_{insep,K}$, there exists $n \in \mathbb{Z}_{\geq 0}$ such that $\alpha^{p^n} \in K$. Then:

   $$\sigma(\alpha)^{p^n} = \sigma(\alpha^{p^n}) = \alpha^{p^n} \in K$$

   and it follows that $\sigma(\alpha) \in L_{insep,K}$. Hence the restriction $\sigma|_{L_{insep,K}}$ is a K-automorphism of $L_{insep,K}$ and thus $\sigma|_{L_{insep,K}} = \mathrm{Id}_{L_{insep,K}}$, see item 1. Therefore $\sigma(\alpha) = \sigma|_{L_{insep,K}}(\alpha) = \alpha$ for all $\alpha \in L_{insep,K}$ and thus $L_{insep,K} \subseteq L^{\mathrm{Gal}(L/K)}$.

   We now consider the extension tower:

   $$K \subseteq L_{insep,K} \subseteq L^{\mathrm{Gal}(L/K)} \subseteq L.$$

   We have that $[L : K] = [L : L_{insep,K}][L_{insep,K} : K]$, hence $[L : L_{insep,K}] = |\mathrm{Gal}(L/K)|$.On the other hand, we have $[L : L^{\mathrm{Gal}(L/K)}] = |\mathrm{Gal}(L/K)|$, see Theorem 4.6.12, and we deduce that $[L^{\mathrm{Gal}(L/K)} : L_{insep,K}] = 1$, hence $L^{\mathrm{Gal}(L/K)} = L_{insep,K}$. Lastly, the extension $L^{\mathrm{Gal}(L/K)} \subseteq L$ is separable, see Proposition 4.6.10, and we conclude that $L_{insep,K} \subseteq L$ is separable.