EPFL - Printemps 2023	Prof. Zs. Patakfalvi
Anneaux et Corps	**Exercices**
Série 1	27 Février 2023

Les exercices indiqués par une étoile $\star$ sont optionnels.
Si vous le souhaitez, vous pouvez rendre votre solution de l'exercice bonus sur la page Moodle du cours avant le dimanche 12 mars, 18h.

Exercice 1.
Soit R un anneau. Lesquels des sous-ensembles suivants 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. $\left\{ \begin{pmatrix} a & b \\ b & a+b \end{pmatrix} \mid a, b \in \mathbb{Z}/2\mathbb{Z} \right\} \subset M_2(\mathbb{Z}/2\mathbb{Z})$.

Exercice 2.
Soit G un groupe fini non-trivial. Montrez que l'algèbre de groupe $\mathbb{Z}[G]$ contient des diviseurs de zéro.

Exercice 3.
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.

Exercice 4.
Montrez qu'il existe au plus 4 homomorphismes d'anneaux $\mathbb{Z}[S_3] \to \mathbb{Z}[\mathbb{Z}/2\mathbb{Z}]$.
Indication : si $f\colon \mathbb{Z}[S_3] \to \mathbb{Z}[\mathbb{Z}/2\mathbb{Z}]$ est un homomorphisme, étudiez les images possibles des éléments de S_3.
Montrez qu'il existe exactement 4 morphismes $\mathbb{Z}[S_3] \to \mathbb{Z}[\mathbb{Z}/2\mathbb{Z}]$.*

Exercice 5.
Soit $n \geq 1$ un entier et $(A, +, \cdot)$ un anneau tel que le groupe additif sous-jacent $(A, +)$ est isomorphe au groupe $(\mathbb{Z}/n\mathbb{Z}, +)$. Fixons un élément $a \in A$ qui génère le groupe cyclique $(A, +)$.

1. Montrez que A est un anneau commutatif.
2. Montrez que, connaissant l'élément $a^2 \in A$, il est possible de déterminer la valeur du produit $x \cdot y$ pour tous éléments $x, y \in A$.

3. Montrez que a est un élément inversible.

4. Montrez que $A \cong \mathbb{Z}/n\mathbb{Z}$ en tant qu'anneaux.

Exercice 6.
Soient A un anneau commutatif et $a \in A$. Montrez que l'application

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

est un isomorphisme d'anneaux.

Exercice 7.
Soit k un corps. Notons $M(k) \subset \{(a_{ij})_{i,j\in\mathbb{N}} \mid \forall i,j : a_{ij} \in k\}$ l'ensemble des matrices infinies à coefficients dans k qui vérifient la condition suivante : $(a_{ij}) \in M(k)$ si et seulement si le support de chaque colonne est fini, c'est-à-dire que pour tout $j_0 \in \mathbb{N}$ seulement un nombre fini de coefficients a_{ij_0} sont non-nuls.

1. Montrez que l'addition et la multiplication usuelle de matrices induit une structure d'anneau sur $M(k)$.

2. Exhibez un élément de $M(k)$ qui est inversible à gauche, mais pas à droite.

Exercice 8.
Prouvez les affirmations suivantes.

1. Un anneau intègre et fini est un corps.

2. Un anneau A dans lequel $a = a^2$ pour tout $a \in A$, est commutatif.

L'exercice suivant était un exercice bonus de l'année 2021.

Exercice 9 ($\star$).
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

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

Exercice bonus 1.
Considérons l'anneau suivant pour un corps quelconque k :

$$A = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a,b,c \in k \right\}.$$

1. Démontrez que si $I \neq A$ est un idéal (bilatère/à gauche/à droite) de A, alors I est contenu dans un des sous-ensembles suivants de A :

$$A_1 = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a,b \in k \right\}$$

   et

$$A_2 = \left\{ \begin{pmatrix} 0 & b \\ 0 & c \end{pmatrix} \mid b,c \in k \right\}.$$

2. Montrez que A_1 et A_2 sont des idéaux bilatères. Montrez que A_1 et A_2 avec l'addition et la multiplication héritée de l'anneau A ne sont pas des anneaux.

3. Listez tous les idéaux (bilatères/à gauche/à droite) de A.

EPFL - Printemps 2023	Prof. Zs. Patakfalvi
Anneaux et Corps	**Exercices**
Série 2	6 mars 2023

Les exercices indiqués par une étoile $\star$ sont optionnels.

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) $A = \mathbb{Q}$ et $B = \mathbb{Z}[i]$;

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

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

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

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

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

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

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

(n) $A = \mathbb{C}[S_3]$ et $B = \left\{ \sum_{g \in S_3} (-1)^{\operatorname{sgn}(g)} \lambda \cdot g \mid \lambda \in \mathbb{C} \right\}$;

(o) $A = \mathbb{C}[S_3]$ et $B = \left\{ \lambda \cdot \operatorname{Id} + \lambda\varepsilon(123) + \lambda\varepsilon^2(132) + \mu(12) + \mu\varepsilon(23) + \mu\varepsilon^2(13) \mid \lambda, \mu \in \mathbb{C} \right\}$, où ε est une racine cubique primitive d'unité;

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

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 $M_n(K)$.

Exercice 3.
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.

Exercice 4.
Montrer les isomorphismes suivants:

(a) $K[t]/(t-a) \cong K$ si K est un corps et $a \in K$.

(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 5.
Soit A un anneau intègre. Si $f, g \in A[t]$, alors $\deg(f \cdot g) = \deg(f) + \deg(g)$.

Exercice 6.
Montrer que $\mathbb{Z}[\varepsilon] \cong \mathbb{Z}[t]/(t^2+t+1)$, où ε est une racine cubique primitive de l'unité.

Exercice 7 ($\star$)**.**
Soit R un anneau commutatif. Déterminer $(R[t])^\times$.
Cet exercice peut être mieux compris grâce à la notion d'idéal premier qui sera vue dans quelques semaines. On reproposera ainsi cet exercice comme exercice optionnel dans la série 4.

Exercice 8 ($\star$)**.**
The goal of this exercise is to show that $\mathbb{Q}$ can be exhibited as the fraction field of many subrings other than $\mathbb{Z}$. We begin by giving the following definitions.

Definition 1 (Valuation Function)**.**
Let K be a field, a discrete valuation is a function $\nu : K \setminus 0 \to \mathbb{Z}$, such that

a) $\nu(x \cdot y) = \nu(x) + \nu(y)$

b) $\nu(x+y) \geq \min(\nu(x), \nu(y))$

We say that ν is non-trivial if it is not the constant 0 function.

Definition 2 (Valuation Ring)**.**
If ν is a discrete valuation function on the field K, then the valuation ring R_ν is the subset $\{x \in K | \nu(x) \geq 0\} \cup \{0\}$ of K.

Show that for a discrete valuation function ν on K we have:

1. $\nu(1) = 0$, $\nu(-1) = 0$.
2. R_ν is a subring of K.
3. K is the fraction field of R_ν.

From now on, $K = \mathbb{Q}$, that is the field of rational numbers. Show that

4. For every $x \in \mathbb{Z}$ we have $\nu(x) \geq 0$.
5. If $\nu(p) = 0$ for all primes p, then ν is trivial.
6. $\nu(p) \neq 0$ can happen for at most one (positive) prime p.
7. If $\nu(p) \neq 0$, then ν is given by $\nu(p^i a/b) = i \cdot c$, where a and b are prime to p and c is a fixed positive integer. Conversely, show that the above formula is a discrete valuation (called the p-adic valuation for $c = 1$, which we denote by ν_p).
8. Show that the valuation ring of ν_p is not equal to $\mathbb{Z} \subseteq \mathbb{Q}$.

Les exercices indiqués par une étoile $\star$ sont optionnels.
Si vous le souhaitez, vous pouvez rendre votre solution de l'exercice bonus sur la page Moodle du cours avant le dimanche 26 mars, 18h.

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.

Exercice 2.
Considérons l'homomorphisme

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

qui envoye un polynôme à coefficients dans $\mathbb{Z}$ au polynôme obtenu par réduction des coefficients mod p. Montrez que la préimage $\xi_p^{-1}(I)$ d'un idéal $I \in \mathbb{F}_p[t], I \neq 0, I \neq \mathbb{F}_p[t]$ n'est pas principal.

Exercice 3.
Cet exercice revoit des notions déjà connues dans le language des anneaux et des idéaux.
Soient m et n deux entiers naturels et (m) et (n) les deux idéaux principaux de $\mathbb{Z}$ correspondants.

1. **Identité de Bézout.** Soit d le pgdc de m et n. Montrer qu'il existe des entiers relatifs a, b tels que $am + bn = d$.
2. Identifier les idéaux $(m) \cdot (n)$, $(m) \cap (n)$ et $(m) + (n)$.

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 $\mathbb{Z}[i]/(i-2)$.

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 $\mathbb{Z}/250\mathbb{Z}$.)

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) $A/K \to \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$.

Exercice 7. 1. Montrer que $\mathbb{C}[x, y]/(x) \cong \mathbb{C}[y]$ (donner la forme explicite d'un isomorphisme).

2. Construire un homomorphisme d'anneaux $\mathbb{C}[x, y] \to \mathbb{C}[x] \times \mathbb{C}[y]$ dont le noyau est (xy).

3. Identifier l'image de cet homomorphisme et en conclure que $\mathbb{C}[x, y]/(xy)$ est isomorphe au sous-anneau de $\mathbb{C}[x] \times \mathbb{C}[y]$ formé des couples de polynômes $(p(x), q(y))$ tels que $p(0) = q(0)$.

Exercice 8 ($\star$).
Let $p \in \mathbb{N}$ be a prime number, ν_p be the p-adic valuation on $\mathbb{Q}$, and let R be the valuation ring of ν_p. (See, Exercice 8, Série 2)

1. Show that every $q \in \mathbb{Q} \setminus \{0\}$ with $\nu_p(q) = 0$ is an invertible element of R.

2. Show that (0) and (p^n) for $n \in \mathbb{N}$ is a complete list of ideals of R, and that all ideals in this list are different.

3. Show that $R/(p^n) \cong \mathbb{Z}/(p^n)$

4. Denote by R_p the valuation ring we obtain for different choices of p. Show that the different R_p's as well as $\mathbb{Z}$ are pairwise non-isomorphic rings (here we ask for isomorphism as abstract rings, so not as subrings of $\mathbb{Q}$).

Exercice bonus 2.
Définition. Un anneau commutatif A est dit *connexe* si pour tout $a, b \in A$ tel que

$$a + b = 1 \quad \text{et} \quad ab = 0$$

alors exactement l'un des deux éléments est nul.

1. Montrer qu'un anneau commutatif est connexe si et seulement si A possède exactement deux idempotents.

   On dit que $e \in A$ un idempotent est un *idempotent minimal* si eA est un anneau connexe non-nul avec l'addition et la multiplication venant de A avec e comme élément neutre. On pose

   $$\pi_0(A) = \{e \in A \mid e \text{ est un idempotent minimal}\}$$

   Remarquer que A est connexe si et seulement si $\pi_0(A) = \{1\}$. Remarquer qu'un anneau connexe est toujours non-nul.

2. Soit $(A_i)_{i=1}^n$ une collection finie d'anneaux connexes. Montrer que

   $$|\pi_0(\prod_{i=1}^n A_i)| = n.$$

3. Montrer que

   $$|\pi_0(\mathbb{Q}[\mathbb{Z}/4\mathbb{Z}])| = 3.$$

EPFL - Printemps 2023	Prof. Zs. Patakfalvi
Anneaux et Corps	**Exercices**
Série 4	20 mars 2023

Les exercices indiqués par une étoile $\star$ sont optionnels.

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.

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 $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$.

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.

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. Sous quelles conditions sur p a-t-on un isomorphisme d'anneaux $\mathbb{Z}[i]/(p) \cong \mathbb{F}_p \times \mathbb{F}_p$?
Indication : Si besoin, vous pouvez admettre l'existence d'une clôture algébrique de $\mathbb{F}_p$.

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

Exercice 6 ($\star$)**.**
Soit R un anneau commutatif. Déterminer $(R[t])^{\times}$.
On pourra se ramener au cas intègre en quotientant par des idéaux premiers de R.

Exercice 7 ($\star$ Introduction aux opérateurs différentiels)**.**
Soit A un anneau commutatif. Notons que s'il existe un homomorphisme d'anneaux injectif $K \hookrightarrow A$ où K est un corps, alors A a la structure d'un K-espace vectoriel. D'ailleurs, pour V un K-espace vectoriel,

$$\mathrm{End}_K(V) := \{\phi : V \to V \mid \phi \text{ est } K \text{ linéaire}\}$$

est un anneau, avec l'addition et la composition de fonctions comme opérations. On définit le **crochet de Lie** sur $\mathrm{End}_K(V)$ de la manière suivante :

$$\begin{array}{ccc} \mathrm{End}_K(V) \times \mathrm{End}_K(V) & \to & \mathrm{End}_K(V) \\ (\phi, \psi) & \mapsto & [\phi, \psi] := \phi \circ \psi - \psi \circ \phi \end{array}$$

Supposons maintenant que A est un anneau commutatif tel que $K \hookrightarrow A$ où K est un corps. Nous désignons par $m_a \in \mathrm{End}_K(A)$ la multiplication par un élément $a \in A$,

$$m_a : \begin{array}{ccc} A & \to & A \\ x & \mapsto & ax \end{array}.$$

Nous définissons les **opérateurs K-différentiels sur A de degré au plus n** inductivement par :

- $D_{\leq -1}(A) = \{m_0\}$,
- $D_{\leq 0}(A) = \{m_a \mid a \in A\}$,
- pour $n > 0$, posons $D_{\leq n}(A) = \{\psi \in \mathrm{End}_K(A) \mid [\psi, m_a] \in D_{\leq n-1}(A)\ \forall a \in A\}$.

Remarquez que $D_{\leq n}(A) \subseteq D_{\leq n+1}(A)$. On définit

$$D(A) := \bigcup_{n \geq -1} D_{\leq n}(A) \ \subset \mathrm{End}_K(A).$$

Montrer que $D(A)$ est un sous-anneau de $\mathrm{End}_K(A)$. On remarque que $K \ni \lambda \mapsto m_\lambda \in D_{\leq 0}(A)$ est le plongement de K dans $D(A)$ qui donne la structure d'espace vectoriel sur K.

A partir de maintenant, nous considérons le cas $A = K[x]$.

1. Montrer que le crochet de Lie

$$\begin{array}{ccc} D(K[x]) \times D(K[x]) & \to & D(K[x]) \\ (F, G) & \mapsto & [F, G] \end{array}$$

est K-bilinéaire.

2. Soit $\frac{\partial}{\partial x} \in \mathrm{End}_K(K[x])$ défini par $\frac{\partial}{\partial x}(x^i) = i \cdot x^{(i-1)}$ pour tout $i \in \mathbb{N}$. Montrez que $\left[\frac{\partial}{\partial x}, m_x\right] = m_1$.

3. Prenons $\frac{\partial}{\partial x}$ comme au-dessus. Montrez que $\left[\frac{\partial}{\partial x}, m_{x^j}\right] = j \cdot m_{x^{(j-1)}}$ pour $j \in \mathbb{N}$.

4. Prenons $\frac{\partial}{\partial x}$ comme au-dessus. Montrez que $\frac{\partial}{\partial x} \in D_{\leq 1}(K[x])$.

EPFL - Printemps 2023	Prof. Zs. Patakfalvi
Anneaux et Corps	**Exercices**
Série 5	27 mars 2023

Les exercices indiqués par une étoile $\star$ sont optionnels.
Si vous le souhaitez, vous pouvez rendre votre solution de l'exercice bonus sur la page Moodle du cours avant le dimanche 9 avril, 18h.

Exercice 1. (a) Soit k un corps. Trouver tous les idéaux de l'anneau quotient $k[t]\big/(t^2)$. 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.

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) Soit p est un nombre premier. Montrer que l'évaluation n'est pas injective lorsque $A = \mathbb{F}_p$. [Indication: Petit Théorème de Fermat.]

(c) Montrer que l'évaluation est injective pour $A = \mathbb{R}$.

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.

Exercice 4. (a) Montrer que $\mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}] \cong \mathbb{F}_p[x]/(x^p - 1)$.

(b) Montrez que $\mathrm{car}(\mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]) = p$. En particulier on a $\mathbb{F}_p \hookrightarrow \mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$

(c) Montrer que $\mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$ n'est pas un produit des 2 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 $N(a + b\sqrt{5}) = \pm 1$.
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?

Exercice 6.
Soit $d > 1$. On note $A = \mathbb{Z}[i\sqrt{d}]$. On note $N(a + i\sqrt{d}) = a^2 + db^2$.

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.

Exercice 7 ($\star$).
Soit $A = F[G]$, où F est un corps et G est un groupe.

(a) Montrer que $\sum_{g \in G} a_g g \in Z(A)$ si et seulement si $g \to a_g$ est constant sur les classes de conjugaison.

(b) Fixons $A = \mathbb{C}[S_3]$ et ε une racine primitive cubique d'unité. Soit

$$e_1 = \frac{1}{6} \sum_{g \in S_3} g,\ e_2 = \frac{1}{6} \sum_{g \in S_3} \operatorname{sgn}(g) g \text{ et } e_3 = f_1 + f_2 \in A,$$

où $f_1 = \frac{\operatorname{Id} + \varepsilon(123) + \varepsilon^2(132)}{3}$ et $f_2 = \frac{\operatorname{Id} + \varepsilon^2(123) + \varepsilon(132)}{3}$.
Montrer que $A \cong Ae_1 \times Ae_2 \times Ae_3$.

(c) Montrer que $Ae_1 \cong \mathbb{C}$ et $Ae_2 \cong \mathbb{C}$.

(d) Montrer que $Ae_3 \cong M_2(\mathbb{C})$.

Exercice bonus 3. Soit p un nombre premier. On dit qu'un anneau commutatif est de *caractéristique* p si le morphisme $\mathbb{Z} \to A$ envoie p sur zéro et donc factorise par $\mathbb{F}_p \to A$. **Dans cet exercice, on travaille uniquement avec des anneaux non-nuls commutatifs de caractéristique p.** On note $F : A \to A$ le *morphisme de Frobenius* $a \mapsto a^p$. Voir *Série 3, exercice 4.3.*

1. Montrer que le morphisme $\mathbb{F}_p \to A$ est injectif.
2. Montrer que $A^F := \{a \in A \mid F(a) = a\}$ est un sous-anneau.
3. Montrer que si $A = A^F$ alors $\operatorname{nil}(A) = 0$.
4. Montrer que si A est intègre et $A = A^F$, alors $\mathbb{F}_p \to A$ est un isomorphisme.
5. Montrer que si $A = A^F$, alors tout idéal premier est maximal.
6. Montrer que $\pi_0(A) = \pi_0(A^F)$. (Voir *exercice bonus 2.*)

EPFL - Printemps 2023	Prof. Zs. Patakfalvi
Anneaux et Corps	**Exercices**
Série 6	3 avril 2023

Les exercices indiqués par une étoile $\star$ sont optionnels.

Exercice 1.
Entiers de Gauss.

1. L'anneau $\mathbb{Z}[i]$ est euclidien avec $N(a+ib) = |a+ib|^2$. (Exemple 3.7.4.(3)) 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 quotient et reste 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. $\star$ Soit p un nombre premier. Montrer que les énoncés suivants sont équivalents.
   (a) Il existe $a, b \in \mathbb{Z}$ avec $p = a^2 + b^2$.
   (b) $p = 2$ ou alors $p \equiv 1 \mod 4$.

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?).

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 $\mathbb{Z}[i\sqrt{5}]$.

Exercice 4.
En s'inspirant de l'exemple 3.7.4.(3), montrer que $\mathbb{Z}[i\sqrt{2}]$ est Euclidien.

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 $\mathbb{R}[t]$. (Without proof, we note that irreducible polynomials of degree higher than 2 do not exist in $\mathbb{R}[t]$.)
2. Soit K un corps et $a \in K$. Montrer que $(t - a)$ est un idéal premier de $K[s, t]$, mais non maximal.

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 $1 \leq i \leq n$.

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).

Exercice 7.
Soit A un anneau intègre et soit $S \subseteq A$ multiplicativement clos, c'est a dire $1_A \in S$, et $\forall a, b \in S \Rightarrow a \cdot b \in S$. On définit $S^{-1}A := \{\frac{a}{b} \in \mathrm{Frac}(A) \mid b \in\}$.

1. Montrer que $S^{-1}A$ est un anneau (un sous-anneau de $\mathrm{Frac}(A)$).
2. Montrer que si $\mathfrak{p}$ est un idéal premier de A, alors $S := A \setminus \mathfrak{p}$ est multiplicativement clos. Dans ce cas, on dénote $A_{\mathfrak{p}} := S^{-1}A = \{\frac{a}{b} \in \mathrm{Frac}(A) \mid b \in S\}$, la localisation de A en $\mathfrak{p}$.
3. Considerons l'idéal premier (2) de $\mathbb{Z}$. Quels sont les idéaux maximaux et les ideaux premiers de $\mathbb{Z}_{(2)}$?
4. Soit $f \in A$. Le sous-ensemble $S := \{1, f, f^2, f^3 \ldots\}$ est multiplicativement clos. Dans ce cas, on dénote $A_f = S^{-1}A = \{\frac{a}{b} \in \mathrm{Frac}(A) \mid b \in S\}$. Quels sont les éléments irréductible de $\mathbb{Z}_2$?

EPFL - Printemps 2023	Prof. Zs. Patakfalvi
Anneaux et Corps	**Exercices**
Série 7	17 avril 2023

Les exercices indiqués par une étoile $\star$ sont optionnels.
Si vous le souhaitez, vous pouvez rendre votre solution de l'exercice bonus sur la page Moodle du cours avant le dimanche 30 avril, 18h.

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 $\mathbb{Z}[i]$.

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 $x \in [0,1]$.

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.

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 $a, b, n \in \mathbb{Z}$.

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.

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 $A \to A/I$.

Exercice 7.
1. Montrez que $x^2 + y^2$ est irréductible dans $\mathbb{Q}[x, y]$, mais pas dans $\mathbb{C}[x, y]$.
2. Montrez que $x^3 - (y^7 + 2y^5 + y^3)$ est irréductible dans $\mathbb{Q}[x, y]$.

Exercice 8.
Soit (B, σ) un anneau euclidien. Montrez que si $b \in B$ non-nul est tel que $\sigma(b) = 0$, alors $b \in B^\times$.

Exercice bonus 4. 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 le point 2. on considère (B, σ) un anneau euclidien quelconque qui n'est pas un corps.

2. Montrer qu'il existe un $b \in B$ non-nul et non inversible tel que
$$|B/(b)| \leq |B^\times| + 1.$$
3. 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.)

EPFL - Printemps 2023	Prof. Zs. Patakfalvi
Anneaux et Corps	**Exercices**
Série 8	24 avril 2023

Les exercices indiqués par une étoile $\star$ sont optionnels.

Exercice 1 (Échauffement).
Soit $\phi : A \to B$ un homomorphisme d'anneaux. Montrer que:

(a) Si $a \in A$ inversible, alors $\phi(a)$ est inversible.

(b) Si $a, b \in A$ tel que $a \sim b$, alors $\phi(a) \sim \phi(b)$.

(c) Si $a \in A$ irréductible, déterminer si $\phi(a)$ est irréductible ou non.

Exercice 2. (a) Soit A un anneau intègre. Si $a_1, \dots, a_n \in A$ 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 $\mathbb{F}_{11}[t0]$.

Exercice 3 (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 $\mathbb{Q}[x, y]$.

Exercice 4 (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.

EPFL - Printemps 2023	Prof. Zs. Patakfalvi
Anneaux et Corps	**Exercices**
Série 9	1 mai 2023

Les exercices indiqués par une étoile $\star$ sont optionnels.
Si vous le souhaitez, vous pouvez rendre votre solution de l'exercice bonus sur la page Moodle du cours avant le dimanche 14 mai, 18h.

Exercice 1.
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.

Exercice 2.
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?

Exercice 3.

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

Exercice 4.
Soit $K = \mathbb{Q}(\sqrt{3} + \sqrt{7})$. Montrez que $[K : \mathbb{Q}] = 4$.

Exercice 5.
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 $t^3 + t + [1]_2 \in \mathbb{F}_2[t]$.

Exercice 6.
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 $\mathbb{C}[x, y]$.

Exercice bonus 5. Soit $n \geq 1$ un entier. On dit qu'une racine n-ième de l'unité $\xi \in \mathbb{C}$ est primitive si n est le plus petit entier tel que $\xi^n = 1$. On pose,

$$\Phi_n(t) = \prod_{\substack{\xi \text{ racine} \\ \text{primitive} \\ n\text{-ième} \\ \text{de l'unité}}} (t - \xi) \in \mathbb{C}[t].$$

1. Montrer que $t^n - 1 = \prod_{d|n} \Phi_d(t)$ et que $\Phi_n(t) \in \mathbb{Z}[t]$.
2. Soit p un nombre premier et $n \geq 1$. En utilisant le critère d'Eisenstein et le changement de variable $t \mapsto t + 1$, montrer que $\Phi_{p^n}(t)$ est irréductible dans $\mathbb{Z}[t]$. (*c.f.* exemple 3.9.4.(2))
3. Soit $n \geq 1$ un entier et p un premier qui est premier avec n. On note ξ_n une racine primitive n-ième de l'unité. Soit $m(t) \in \mathbb{Q}[t]$ le polynôme minimal de ξ_n. Montrer que $m(t) \in \mathbb{Z}[t]$. Montrer que si ξ est une racine de $m(t)$, alors ξ^p est une racine de $m(t)$. En déduire que $m(t) = \Phi_n(t)$.

   Indication: on pourra montrer par l'absurde que si ξ^p n'est pas une racine de $m(t)$ alors $t^n - 1$ a une racine double modulo p, ce qui est absurde comme $(n, p) = 1$ (Voir Proposition 4.4.10).
4. Montrer qu'il existe une infinité de premiers p tel que $\Phi_n(t)$ a une racine dans $\mathbb{F}_p[t]$. En déduire qu'il existe une infinité de premiers p tel que $p \equiv 1 \mod n$.

   Indication: pour tout m suffisamment grand si un nombre premier p divise $\Phi_n(m!)$ alors $p > m$.

Exercice 7 ($\star$).
Calculer $\pi_0(\mathbb{Q}[\mathbb{Z}/n\mathbb{Z}])$.

EPFL - Printemps 2023	Prof. Zs. Patakfalvi
Anneaux et Corps	**Exercices**
Série 10	8 mai 2023

Exercice 1.
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 $K \subset F$.

Exercice 2.
Soit $n > 0$ un entier positif. Montrez que $\cos(2\pi/n)$ et $\sin(2\pi/n)$ sont des nombres algébriques sur $\mathbb{Q}$.

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

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 les mêmes, et ils sont les mêmes aussi que le sous-corps de $\mathbb{C}$ engendré par ξ et $\sqrt[n]{2}$.

Exercice 5.
1. Montrez qu'il existe que 2 polynômes irréductibles de degré 3 sur $\mathbb{F}_2$.
2. Soit f et g ces deux polynômes. Montrez que tous les deux f et g obtient 3 racines distinctes dans $K = \mathbb{F}_2[x]/(f)$.
3. Montrez que les corps de décomposition de ces 2 polynômes sont les mêmes, et il est isomorphe à $K = \mathbb{F}_2[x]/(f)$.

Exercice 6.
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'homomorphisme 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 $K(x,y)[\sqrt{xy}] \cong K(x,y)[\sqrt{x(x+y)}]$

EPFL - Printemps 2023	Prof. Zs. Patakfalvi
Anneaux et Corps	**Exercices**
Série 11 - Corps finis	15 mai 2023

Exercice 1.
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 $\mathbb{F}_{27}^{\times}$.

Exercice 2.
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.

Exercice 3 (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 3.4.17, 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
$$x^{p^d} - x = \prod_{\substack{h \text{ unitaire irréd.} \\ \text{dans } \mathbb{F}_p[x] \\ \deg h \text{ divise } d}} h.$$

Exercice 4 (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 3 et le Théorème fondamental des corps finis.

2. Montrez que

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

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.

Exercice 5.
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 injectives $\iota_j : K_j \to K_{j+1}$ pour chaque entier $j \geq 1$.

2. Fixons ι_j comme dans le point précédent. Montrez que la limite 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 4.2.21, 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.)

EPFL - Printemps 2023	Prof. Zs. Patakfalvi
Anneaux et Corps	**Exercices**
Série 12	22 mai 2023

Les exercices indiqués par une étoile $\star$ sont optionnels.

Exercice 1 (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.

Exercice 2 (Extension quadratique pour car$(k) = 2$.).
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.

(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.

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

Exercice 4.
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 $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{1+\sqrt{2}})$

Exercice 5.
Dans les cas suivants, calculez $G = \mathrm{Gal}(\mathbb{Q}(\alpha, \beta)/\mathbb{Q})$, et calculez le pôlynome minimal de $\alpha, \alpha+\beta, \alpha\cdot\beta$ et α^{-1}. Pour calculer les polynômes minimaux, on s'inspirera de l'exemple 4.6.12.

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

Exercice 6.
Let $f = x^3 + ax + 1 \in \mathbb{Q}[x]$ such that $a > 0$, $a \in \mathbb{Z}$.

1. Show that f is irreducible over $\mathbb{Q}$.
2. Show that f does not have 3 real roots in its splitting field (the splitting field (corps de décomposition) is isomorphic to the subfield of $\mathbb{C}$ generated by the complex roots of f, and hence it makes sense to talk about its element being real).

3. Let $K = \mathbb{Q}[x]/(f)$. Show that K is a degree 3 extension of $\mathbb{Q}$, which is not Galois.
4. Let L be the decomposition field of f over $\mathbb{Q}$. Show that $\mathrm{Gal}(L/Q) \cong S_3$

Exercice 7.
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.

Exercice 8 (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.

Exercice 9 ($\star$)**.**
Montrer que tous les groupes finis sont des groupes de Galois. *Indication: on pourra trouver un corps K_n où S_n agit fidèlement.*
Remarque. En utilisant des techniques de géométrie algébrique et de topologie algébrique on peut montrer que tout groupe fini est réalisé comme un groupe de Galois d'une extension de $\mathbb{C}(t)$.

1. Avec de la géométrie algébrique, on voit que les extensions finies de $\mathbb{C}(t)$ correspondent à des morphismes de *courbes algébriques* $X \to \mathbb{P}^1_{\mathbb{C}}$ tel que si ont enlève un nombre fini de points à $\mathbb{P}^1_{\mathbb{C}}$, le morphisme devient un revêtement au sens topologique.
2. $\mathbb{P}^1_{\mathbb{C}}$ privé d'un nombre fini de points est le plan complexe $\mathbb{C}$ privé d'un nombre fini de points. Par la topologie algébrique, on sait que $\pi_1(\mathbb{C} \setminus \{p_1, \ldots, p_n\}) \cong F_n$ le groupe libre sur n-générateurs. Dès lors par la théorie des revêtements, comme tout groupe fini G admet une surjection $F_n \to G$ pour un certain n, il existe un revêtement fini de $\mathbb{C} \setminus \{p_1, \ldots, p_n\}$ avec groupe de Galois égal à G.
3. En retournant à la géométrie algébrique, on obtient alors un morphisme de *courbes algébriques* $X \to \mathbb{P}^1_{\mathbb{C}}$ avec groupe de Galois G et donc une extension de $\mathbb{C}(t)$ avec groupe de Galois G.

Si ce genre de choses vous intrigue, le rédacteur vous encourage à suivre des cours de géométrie algébrique et de topologie algébrique, et/ou à faire des projets dans ces domaines.

Exercice 10 ($\star$)**.**
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

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