EPFL - Automne 2020	Prof. Z. Patakfalvi
Structures Algébriques	**Exercices**
Série 3	2 Octobre 2020

Veuillez télécharger vos solutions aux exercices à rendre (Exercice 1) sur la page Moodle du cours avant le lundi 12 octobre, 18h.

---

1 Exercices à rendre

Exercise 1 (Applications de Cantor-Schröder-Bernstein)**.**
On rappelle (Définition 1.2.19.3) qu'un ensemble est **infini dénombrable** s'il a le même cardinal que $\mathbb{N}$.

1. Montrez que $\mathbb{Z}$ est infini dénombrable.

2. Montrez que $\mathbb{N}^n$ est infini dénombrable, pour n'importe quel entier $n \geq 1$.
   Indication : pensez à la factorisation en nombres premiers.

3. Montrez que $\mathbb{Q}$ est dénombrable.

4. Un nombre complexe $z \in \mathbb{C}$ est **algébrique** s'il existe un polynôme non-nul à coefficients rationnels $0 \neq p(t) \in \mathbb{Q}[t]$ tel que $p(z) = 0$. Montrez que l'ensemble des nombres algébriques est dénombrable.
   Indication : Commencez par montrer que l'ensemble $\mathbb{Q}[t]$ est dénombrable. Montrez ensuite que l'ensemble des nombres algébriques est la réunion d'ensembles finis indexés par $\mathbb{Q}[t]$. Concluez en montrant que la réunion d'une infinité dénombrable d'ensemble finis, est finie ou infini dénombrable.
   Vous pouvez utiliser sans preuve qu'un polynôme de degré n a au plus n solutions complexes.

2 Exercices supplémentaires

Exercise 2.
Soient $a \geq b \in \mathbb{N}^{>0}$. Prouvez que l'algorithme d'Euclide appliqué au couple $\{a, b\}$ se termine en un nombre d'étapes plus petit que $\min\{1 + 2\log_2 a, 2\log_2 b\}$.
Indication : montrez que le dividende de l'étape $i+1$ est plus petit que la moitié du dividende de l'étape $i-1$.

Exercise 3. 1. Montrez que $|2^{\mathbb{N}}| \neq |\mathbb{N}|$.
Indication : par l'absurde, supposons qu'il existe une bijection $\phi\colon \mathbb{N} \to 2^{\mathbb{N}}$. Considérez l'ensemble $\{n \in \mathbb{N} \mid n \notin \phi(n)\}$.

2. Montrez que $|2^{\mathbb{N}}| = |\mathbb{R}|$.
Indication : pensez au développement binaire.

3 Théorie des nombres sur $\mathbb{R}[t]$

Dans les trois exercices suivants, on généralise à l'ensemble $\mathbb{R}[t]$ les notions et les résultats du Chapitre 2 des notes de cours. La principale difficulté est de définir le pgcd. Une fois qu'elle est surmontée, la plupart des preuves du Chapitre 2 s'appliquent presque sans modifications.

On utilisera les définitions suivantes :

1. Un polynôme est dit **unitaire** si son coefficient dominant est égal à 1. En d'autres termes, $p(t) \in \mathbb{R}[t]$ est unitaire s'il s'écrit $p(t) = t^n + \sum_{i=0}^{n-1} a_i t^i$.
2. Un polynôme $p(t)$ **divise** un polynôme $q(t)$, ce que l'on note $p(t)|q(t)$, s'il existe $a(t) \in \mathbb{R}[t]$ tel que $q(t) = p(t)a(t)$.
3. Un polynôme $p(t)$ est dit **premier** si $\deg p(t) \geq 1$ et
$$\forall a(t), b(t) \in \mathbb{R}[t] : \quad p(t)|a(t)b(t) \Rightarrow p(t)|a(t) \text{ ou } p(t)|b(t).$$

Exercise 4 (Pgcd pour les polynômes)**.**
Dans cet exercice, on introduit le pgcd de deux polynômes.

1. Soit $\{0\} \neq I \subset \mathbb{R}[t]$ un sous-ensemble qui satisfait les deux propriétés suivantes :
$$\mathbb{R}[t] \cdot I \subseteq I \quad \text{et} \quad I + I \subseteq I. \tag{1}$$
Montrez qu'il existe un unique polynôme unitaire $p(t) \in \mathbb{R}[t]$ tel que
$$I_{p(t)} := \{a(t)p(t) \mid a(t) \in \mathbb{R}[t]\} = I.$$
Indication : considérez les polynômes non-nuls de degré minimal contenus dans I.

2. Prenons deux polynômes $a(t), b(t) \in \mathbb{R}[t]$. Montrez que l'ensemble
$$I_{a(t),b(t)} := \{p(t)a(t) + q(t)b(t) \mid p(t), q(t) \in \mathbb{R}[t]\}$$
satisfait aux deux conditions de (1) ci-dessus. En particulier il existe un polynôme unitaire $c(t) \in \mathbb{R}[t]$ tel que
$$I_{a(t),b(t)} = I_{c(t)}.$$
On appelle $\big(a(t), b(t)\big) := c(t)$ le **plus grand common diviseur** de $a(t)$ et $b(t)$.

3. Montrez qu'il existe une relation de Bézout :

$$\exists p(t), q(t) \in \mathbb{R}[t] : \quad p(t)a(t) + q(t)b(t) = \big(a(t), b(t)\big).$$

4. Supposons que $a(t), b(t)$ soient tous deux non-nuls. Montrez que si $p(t)$ divise $a(t)$ et $b(t)$, alors

$$\deg p(t) \leq \deg \big(a(t), b(t)\big),$$

avec égalité si et seulement si $p(t) = \alpha \cdot \big(a(t), b(t)\big)$ pour un certain $\alpha \in \mathbb{R}^*$. En particulier $\big(a(t), b(t)\big)$ mérite son appelation de plus grand diviseur commun.
Indication : considérer une relation de Bézout pour $a(t)$ et $b(t)$.

Exercise 5 (Algorithme d'Euclide pour les polynômes)**.**
Enoncez un algorithme qui, à partir de polynômes non-nuls $a(t), b(t) \in \mathbb{R}[t]$, calcule leur plus grand commun diviseur $\big(a(t), b(t)\big)$.
Indication : Inspirez-vous de l'algorithme d'Euclide (décrit dans Notation 2.1.3), puis prouvez l'équivalent du Théorème 2.1.6.

Exercise 6 (Théorème fondamental de l'arithmétique des polynômes)**.**
Dans cet exercice, on établit le théorème fondamental de l'arithmétique pour $\mathbb{R}[t]$. Prouvez le résultat suivant : pour tout $0 \neq a(t) \in \mathbb{R}[t]$, il existe des polynômes premiers unitaires $p_1(t), \ldots, p_r(t)$, uniquement déterminés à permutation près, ainsi qu'un nombre réel non-nul $\alpha \in \mathbb{R}^*$ tels que

$$a(t) = \alpha \prod_{i=1}^{r} p_i(t).$$

Indication : Définissez la notion de polynôme irréductible en vous inspirant de la Définition 2.2.1. Puis prouvez les équivalents des Propositions 2.2.3 et 2.2.4 pour les polynômes. Les preuves seront quasiment identiques.