TD 10 : corrigé

1. Critères pour montrer qu'un anneau est un corps

1. Soit A un anneau commutatif, intègre et fini. Soit $x \in \mathrm{A}$ non nul. L'application :

$$\mathrm{M}_x : \begin{array}{ccc} \mathrm{A} & \to & \mathrm{A} \\ y & \mapsto & xy \end{array}$$

est injective. En effet, si $\mathrm{M}_x(y) = \mathrm{M}_x(y')$, on a $xy = xy'$ et donc $x(y-y') = 0$, ce qui entraîne par intégrité que $y = y'$. Puisque A est fini, M_x est surjective et on peut trouver $y \in \mathrm{A}$ tel que $xy = 1$, ce qui prouve que x est inversible.

2. Tout d'abord, si I est un idéal non nul d'un corps K, on peut trouver un élément non nul $a \in \mathrm{I}$. Mais a est alors inversible et $\mathrm{I} = \mathrm{K}$. Les seuls idéaux de K sont donc (0) et K, et ils sont bien différents car l'anneau nul n'est pas un corps.

Réciproquement, supposons que A ait exactement deux idéaux : (0) et A. Soit alors $x \in \mathrm{A}$ non nul. L'idéal (x) étant alors non nul, on a $(x) = \mathrm{A}$, d'où l'existence d'un y tel que $1 = xy$, ce qui prouve l'inversibilité de x et que A est un corps.

Soit maintenant un morphisme de corps $\varphi : \mathrm{K} \to \mathrm{L}$. Le noyau $\ker\varphi$ est un idéal et, d'après ce qui précède, le morphisme est injectif ou nul. Ce dernier cas est exclu, car on doit avoir $\varphi(1_\mathrm{K}) = 1_\mathrm{L}$, différent de 0_L car L, qui est un corps, ne peut pas être l'anneau nul et donc φ est bien injectif.

3. Soit A un anneau dont tous les idéaux sont premiers. Déjà, comme l'idéal nul est premier, l'anneau $\mathrm{A} = \mathrm{A}/(0)$ est intègre. Soit alors un élément non nul $x \in \mathrm{A}$. Puisque l'idéal (x^2) est supposé premier, il découle de $x^2 \in (x^2)$ l'appartenance $x \in (x^2)$. On a donc un élément $a \in \mathrm{A}$ tel que $x = ax^2$, c'est-à-dire $x(1-ax) = 0$ et, par intégrité, $ax = 1$ ce qui démontre bien que x est inversible.

2. Groupes additif et multiplicatif

Il n'existe pas de tel corps K. Pour démontrer cela, cherchons à identifier les éléments d'ordre 2 dans les deux groupes.

Un élément $x \in \mathrm{K}$ d'ordre 2 dans $(\mathrm{K}, +)$ est un élément non nul tel que $x + x = 2x = 0$. Un tel élément n'existe qu'en caractéristique 2, où tous les x non nuls ont cette propriété.

Un élément $x \neq 0$ d'ordre 2 dans $(\mathrm{K}^\times, \cdot)$ est un élément différent de 1 tel que $x^2 = 1$. Puisque $(x^2 - 1) = (x+1)(x-1)$, il y a exactement un tel élément en caractéristique différente de 2 (l'élément -1) et il n'y en a aucun en caractéristique 2.

En résumé, si on note $\mathscr{O}_n(\mathrm{G})$ les éléments d'ordre n d'un groupe G, on a :

$$\mathscr{O}_2(\mathrm{K}, +) = \begin{cases} \mathrm{K}^\times & \text{si car K} = 2 \\ \varnothing & \text{sinon} \end{cases} \qquad \mathscr{O}_2(\mathrm{K}^\times, \cdot) = \begin{cases} \varnothing & \text{si car K} = 2 \\ \{-1\} & \text{sinon} \end{cases}$$

ce qui prouve que $(\mathrm{K}, +)$ et $(\mathrm{K}^\times, \cdot)$ ne peuvent pas être isomorphes.

3. Anneaux à quatre éléments

1. Dans le cours, le corps $\mathbb{F}_4$ a été défini comme le quotient $\mathbb{F}_2[X]/(X^2+X+1)$. Si on appelle $\omega \in \mathbb{F}_4$ l'image de X par ce morphisme, $\mathbb{F}_4$ est alors un $\mathbb{F}_2$-espace vectoriel de dimension 2 (le degré de X^2+X+1) et de base $(1,\omega)$, ce qui démontre :

$$\mathbb{F}_4 = \{0, 1, \omega, 1+\omega\}.$$

Par définition, ω vérifie $\omega^2 = \omega + 1$ (en se souvenant que l'on est en caractéristique 2 et qu'il n'y a donc pas lieu de se préoccuper de problèmes de signes). On obtient donc les tables d'addition et de multiplication :

$+$	0	1	ω	$1+\omega$
0	0	1	ω	$1+\omega$
1	1	0	$1+\omega$	ω
ω	ω	$1+\omega$	0	1
$1+\omega$	$1+\omega$	ω	1	0

$\times$	0	1	ω	$1+\omega$
0	0	0	0	0
1	0	1	ω	$1+\omega$
ω	0	ω	$1+\omega$	1
$1+\omega$	0	$1+\omega$	1	ω

2. Déjà, le corps $\mathbb{F}_4$ et l'anneau produit $\mathbb{F}_2 \times \mathbb{F}_2$ ont tous les deux la structure additive d'un $\mathbb{F}_2$-espace vectoriel. En particulier, leur groupe additif est isomorphe au groupe de Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ tandis que $\mathbb{Z}/4\mathbb{Z}$ a un groupe additif cyclique. Il suffit donc de montrer que $\mathbb{F}_4$ et $\mathbb{F}_2 \times \mathbb{F}_2$ ne sont pas isomorphes. Il suffit par exemple de constater que $(1,0)\cdot(0,1) = (0,0)$ et que donc $\mathbb{F}_2 \times \mathbb{F}_2$ n'est pas un anneau intègre.

3. Considérons l'anneau quotient $\mathbb{F}_2[X]/(X^2)$. Si on note ε l'image de X, on obtient facilement les tables d'addition et de multiplication :

$+$	0	1	ε	$1+\varepsilon$
0	0	1	ε	$1+\varepsilon$
1	1	0	$1+\varepsilon$	ε
ε	ε	$1+\varepsilon$	0	1
$1+\varepsilon$	$1+\varepsilon$	ε	1	0

$\times$	0	1	ε	$1+\varepsilon$
0	0	0	0	0
1	0	1	ε	$1+\varepsilon$
ε	0	ε	0	ε
$1+\varepsilon$	0	$1+\varepsilon$	ε	1

Le groupe additif de cet anneau est lui aussi isomorphe au groupe de Klein. Mais il possède une particularité : l'élément ε vérifie $\varepsilon^2 = 0$. Ainsi, il n'est pas intègre, mais d'une manière différente de $\mathbb{F}_2 \times \mathbb{F}_2$, qui n'a pas de tels éléments nilpotents. Notre anneau n'est donc isomorphe à aucun des trois précédents.

4. Ensembles de morphismes

- $\mathrm{Hom}(\mathbb{Q},\mathbb{C}) = \{\mathrm{inc} : \mathbb{Q} \to \mathbb{C}\}$:
  Soit $f \in \mathrm{Hom}(\mathbb{Q},\mathbb{C})$. On a nécessairement $f(1) = 1$ et donc, en appliquant par récurrence la propriété $f(a+b) = f(a)+f(b)$, on obtient que f coïncide avec l'inclusion $\mathrm{inc} : \mathbb{Q} \to \mathbb{C}$ sur $\mathbb{Z}$. Mais on doit alors avoir pour tout rationnel $\frac{a}{b} \in \mathbb{Q}$ l'égalité $f\left(\frac{a}{b}\right) = \frac{f(a)}{f(b)} = \frac{a}{b}$ ce qui prouve $f = \mathrm{inc}$.
- $\mathrm{Hom}(\mathbb{C},\mathbb{Q}) = \varnothing$:
  On a vu pendant le premier exercice que tout morphisme de corps doit être injectif. L'ensemble non dénombrable $\mathbb{C}$ ne pouvant s'injecter dans $\mathbb{Q}$, il n'y a donc ici aucun

morphisme de corps. (On peut aussi facilement vérifier que $\mathbb{Q}$ n'abrite aucun élément susceptible d'être l'image de i.)

– $\mathrm{Hom}(\mathbb{R},\mathbb{R}) = \{\mathrm{id}_{\mathbb{R}}\}$:
Les arguments de la première question montrent que si $f \in \mathrm{Hom}(\mathbb{R},\mathbb{R})$, la restriction de f à $\mathbb{Q}$ est l'identité. Or, un morphisme de corps $f : \mathbb{R} \to \mathbb{R}$ est nécessairement strictement croissant :

$$\begin{aligned} y > x &\Rightarrow \exists \varepsilon > 0 : y = x + \varepsilon \\ &\Rightarrow \exists \delta \in \mathbb{R}^\times : y = x + \delta^2 \\ &\Rightarrow \exists \delta \in \mathbb{R}^\times : f(y) = f(x + \delta^2) \\ &\Rightarrow \exists \delta \in \mathbb{R}^\times : f(y) = f(x) + f(\delta)^2 \\ &\Rightarrow f(y) > f(x). \end{aligned}$$

La fonction f est donc croissante et se restreint à l'identité sur $\mathbb{Q}$. En encadrant un réel x par deux suites de rationnels convergeant vers x, cela démontre que f est en fait l'identité.

– $\mathrm{Hom}(\mathrm{K},\mathrm{L}) = \varnothing$ si K et L n'ont pas la même caractéristique :
En effet, si $f : \mathrm{K} \to \mathrm{L}$ est un morphisme de corps, on a la suite d'équivalences (en se souvenant qu'un morphisme de corps est injectif) portant sur un entier $n \in \mathbb{Z}$:

$$n1_{\mathrm{K}} = 0_{\mathrm{K}} \Leftrightarrow f(n1_{\mathrm{K}}) = f(0_{\mathrm{K}}) \Leftrightarrow n1_{\mathrm{L}} = 0_{\mathrm{L}},$$

ce qui prouve que deux corps reliés par un morphisme ont la même caractéristique.

5. Algébriques et transcendants

1. Tous les axiomes des morphismes d'anneaux sont évidemment vérifiés par $\mathrm{év}_\alpha : \mathrm{K}[\mathrm{T}] \to \mathrm{L}$.
2. Le morphisme $\mathrm{év}_\alpha$ est injectif si et seulement si α n'est racine d'aucun polynôme non nul à coefficients dans K, ce qui est donc par définition équivalent à la négation de la propriété « α algébrique sur K. » Dans le cas où α est algébrique, le noyau $\ker \mathrm{év}_\alpha$ est un idéal de l'anneau principal $\mathrm{K}[\alpha]$ et est donc de la forme (P_α) pour un unique polynôme unitaire $\mathrm{P}_\alpha \in \mathrm{K}[\mathrm{T}]$.
3. Si α est algébrique, l'anneau $\mathrm{K}[\alpha] \simeq \mathrm{K}[\mathrm{T}]/(\mathrm{P}_\alpha)$ est un sous-anneau du corps L. Il est donc intègre, ce qui implique que l'idéal (P_α) est premier. Mais on a vu que dans un anneau principal, les idéaux premiers non nuls sont maximaux, donc le quotient $\mathrm{K}[\alpha] \simeq \mathrm{K}[\mathrm{T}]/(\mathrm{P}_\alpha)$ est un corps. Puisque tout corps contenant K et α doit naturellement contenir tout polynôme en α à coefficients dans K, c'est-à-dire tout $\mathrm{K}[\alpha]$, on a bien $\mathrm{K}[\alpha] = \mathrm{K}(\alpha)$.

Si en revanche α est transcendant, on a vu que $\mathrm{év}_\alpha$ était un morphisme injectif , et il réalise donc un isomorphisme entre $\mathrm{K}[\mathrm{T}]$ et $\mathrm{K}[\alpha]$. Puisque aucun polynôme à coefficients dans K ne s'annule en α, on peut étendre $\mathrm{év}_\alpha$ en

$$\overline{\mathrm{év}_\alpha} : \begin{array}{ccc} \mathrm{K}(\mathrm{T}) & \to & \mathrm{L} \\ \mathrm{R} = \dfrac{\mathrm{P}}{\mathrm{Q}} & \mapsto & \mathrm{R}(\alpha) = \dfrac{\mathrm{P}(\alpha)}{\mathrm{Q}(\alpha)} \end{array}.$$

C'est clairement un morphisme d'anneaux (et donc de corps) et son image est donc un corps isomorphe à $\mathrm{K}(\mathrm{T})$, d'après le théorème d'isomorphisme sur les morphismes d'anneaux et le

fait qu'un morphisme de corps est automatiquement injectif. Puisque tout corps contenant K et α doit contenir toutes ces fractions rationnelles, on a bien $\operatorname{im}\overline{\text{év}_\alpha} = \mathrm{K}(\alpha)$, ce qui démontre l'isomorphisme $\mathrm{K}(\mathrm{T}) \simeq \mathrm{K}(\alpha)$.

4. Commençons par un critère simple : si P est un polynôme irréductible et unitaire de K[T] admettant α comme racine, (P) est un idéal maximal contenu dans $\ker \text{év}_\alpha$, ce qui prouve $\ker \text{év}_\alpha = (\mathrm{P})$ et donc que P est le polynôme minimal de α. C'est comme cela que nous allons trouver les polynômes minimaux dans les exemples suivants (et c'est une des raisons pour lesquelles il est si important de savoir démontrer qu'un polynôme de $\mathbb{Q}[\mathrm{T}]$ est irréductible !) :

- $(\mathrm{L}/\mathrm{K} = \mathbb{C}/\mathbb{Q})$ Les trois éléments donnés sont algébriques sur $\mathbb{Q}$: i est annulé par T^2+1, $\sqrt[3]{2}$ par T^3-2 et $(1+i\sqrt{19})/2$ par $\mathrm{T}^2-\mathrm{T}+5$ (ce fait ayant déjà servi en TD). Pour montrer que ces polynômes sont bien les polynômes minimaux, il faut et il suffit de montrer leur irréductibilité. Ces polynômes sont tous de degré $\leqslant 3$. S'ils étaient réductibles, ils admettraient un facteur de degré 1, et donc une racine dans $\mathbb{Q}$. Mais on vérifie aisément que leurs racines dans $\mathbb{C}$ ne sont pas rationnelles.
- $(\mathrm{L}/\mathrm{K} = \mathbb{C}(\mathrm{X})/\mathbb{C})$. Les morphismes d'évaluation vus depuis le début sont :
$$\text{év}_\mathrm{X} : \begin{array}{ccc} \mathbb{C}[\mathrm{T}] & \to & \mathbb{C}(\mathrm{X}) \\ \mathrm{P}(\mathrm{T}) & \mapsto & \mathrm{P}(\mathrm{X}) \end{array} \qquad \text{et} \qquad \text{év}_{\mathrm{X}^2} : \begin{array}{ccc} \mathbb{C}[\mathrm{T}] & \to & \mathbb{C}(\mathrm{X}) \\ \mathrm{P}(\mathrm{T}) & \mapsto & \mathrm{P}(\mathrm{X}^2) \end{array}$$
qui sont clairement injectifs. Les éléments X et X^2 de $\mathbb{C}(\mathrm{X})$ sont donc transcendants sur $\mathbb{C}$.
- $(\mathrm{L}/\mathrm{K} = \mathbb{C}(\mathrm{X})/\mathbb{C}(\mathrm{X}^2)$ L'élément X^2 appartient au corps de base $\mathbb{C}(\mathrm{X}^2)$. Il est donc évidemment algébrique de polynôme minimal $\mathrm{T}-\mathrm{X}^2 \in \mathbb{C}(\mathrm{X}^2)[\mathrm{T}]$. L'élément X, quant à lui, n'est que la racine du précédent donc il est annulé par le polynôme $\mathrm{T}^2-\mathrm{X}^2 \in \mathbb{C}(\mathrm{X}^2)[\mathrm{T}]$. Ce polynôme est irréductible pour les mêmes raisons que plus haut : comme il est de degré 2, il serait scindé s'il était réductible, ce qui est impossible puisque $\mathrm{X} \notin \mathbb{C}(\mathrm{X}^2)$ (par exemple parce que toute fraction rationnelle $\mathrm{R} \in \mathbb{C}(\mathrm{X}^2)$ vérifie $\mathrm{R}(-\mathrm{X}) = \mathrm{R}(\mathrm{X})$, ce qui n'est pas vrai pour $\mathrm{R} = \mathrm{X}$.) Le polynôme $\mathrm{T}^2 - \mathrm{X}^2 \in \mathbb{C}(\mathrm{X}^2)[\mathrm{T}]$ est donc irréductible et c'est le polynôme minimal de $\mathrm{X} \in \mathbb{C}(\mathrm{X})$ sur $\mathbb{C}(\mathrm{X}^2)$.

5. Supposons que l'extension L/K soit de degré fini et soit $\alpha \in \mathrm{L}$. Puisque K[T] est de dimension finie sur K, le morphisme $\text{év}_\alpha : \mathrm{K}[\mathrm{T}] \to \mathrm{L}$ ne peut pas être injectif et α est algébrique sur L. L'extension L/K est donc algébrique.

6. Prenons $(l_i)_{i=1}^p$ une base du K-espace vectoriel L et $(m_j)_{j=1}^q$ une base du L-espace vectoriel M. On va démontrer que $(l_i m_j)_{\substack{1\leqslant i\leqslant p \\ 1\leqslant j\leqslant q}}$ est une base du K-espace vectoriel M.

Que ce soit une famille génératrice est aisé : un élément x de M s'écrit $x = \sum_{j=1}^{q} \lambda_j m_j$ avec $\lambda_j \in \mathrm{L}$ et on a pour chaque j une décomposition $\lambda_j = \sum_{i=1}^{p} \kappa_{ij} l_i$ (avec $\kappa_{ij} \in \mathrm{K}$) d'où :
$$x = \sum_{j=1}^{q} \sum_{i=1}^{p} \kappa_{ij} l_i m_j,$$
ce qui montre bien que la famille $(l_i m_j)_{\substack{1\leqslant i\leqslant p \\ 1\leqslant j\leqslant q}}$ engendre le K-espace vectoriel M.

Pour démontrer la liberté de cette famille, soit κ_{ij} une famille d'éléments de K telle que $\sum_{i=1}^{p} \sum_{j=1}^{q} \kappa_{ij} l_i m_j = 0$. On peut réécrire cela en une relation de liaison sur L entre les (m_j) :

$\sum_{j=1}^{q}\left(\sum_{i=1}^{p}\kappa_{ij}l_i\right)m_j = 0$ d'où, pour tout j, $\sum_{i=1}^{p}\kappa_{ij}l_i = 0$ et, par liberté de (l_i) sur K, les coefficients (κ_{ij}) sont tous nuls.

On a donc bien démontré que $(l_i m_j)_{\substack{1\leqslant i\leqslant p\\ 1\leqslant j\leqslant q}}$ est une base de M en tant que K-espace vectoriel, ce qui prouve l'égalité des dimensions

$$[\mathrm{M}:\mathrm{K}] = [\mathrm{M}:\mathrm{L}]\cdot[\mathrm{L}:\mathrm{K}].$$

7. Soit $\alpha\neq 0$ et β deux éléments de L algébriques sur K. On va démontrer que $\alpha+\beta$, $\alpha\beta$ et $1/\alpha$ appartiennent à des extensions de degré finies de K. Cela démontrera qu'ils sont algébriques sur K.

On a déjà vu que $\mathrm{K}[\alpha]$ était un corps. Il contient donc $1/\alpha$ qui est alors algébrique, puisqu'il appartient à une extension de degré fini de K.

Dans les cas restants, il est évident que $\mathrm{K}(\alpha+\beta)$ et $\mathrm{K}(\alpha\beta)$ sont inclus dans $\mathrm{K}(\alpha,\beta)$, le plus petit sous-corps de L contenant à la fois K, α et β. Il suffit donc de démontrer que ce corps $\mathrm{K}(\alpha,\beta)$ est de dimension finie sur K. Tout d'abord, β est algébrique sur $\mathrm{K}(\alpha)$: son polynôme minimal sur K reste un polynôme à coefficients dans $\mathrm{K}\subset\mathrm{K}(\alpha)$ qui annule α (même si, en passant de K à $\mathrm{K}(\alpha)$, il peut perdre son irréductibilité). $\mathrm{K}(\alpha)[\beta]$ est alors le corps $\mathrm{K}(\alpha)(\beta)$, qui est un autre nom de $\mathrm{K}(\alpha,\beta)$. D'après la formule de multiplicativité des degrés, $\mathrm{K}(\alpha,\beta)$ est alors une extension de degré fini de K et même, en notant $\deg_{\mathrm{K}}\alpha$ le *degré* de α sur K, c'est-à-dire le degré de l'extension $\mathrm{K}(\alpha)/\mathrm{K}$ ou, de manière équivalente, le degré du polynôme minimal de α sur K, on a :

$$[\mathrm{K}(\alpha,\beta):\mathrm{K}] = [\mathrm{K}(\alpha,\beta):\mathrm{K}(\alpha)]\cdot[\mathrm{K}(\alpha):\mathrm{K}] = \deg_{\mathrm{K}(\alpha)}\beta\cdot\deg_{\mathrm{K}}\alpha \leqslant \deg_{\mathrm{K}}\alpha\cdot\deg_{\mathrm{K}}\beta.$$

Ainsi, $\alpha+\beta$ et $\alpha\beta$ sont algébriques sur K, de degré $\leqslant \deg_{\mathrm{K}}\alpha\cdot\deg_{\mathrm{K}}\beta$.

8. D'après la question précédente, $\sqrt{3}+\sqrt{2}$ est algébrique. On en trouve facilement un polynôme annulateur :

$$(\sqrt{2}+\sqrt{3})^2 = 5+2\sqrt{6}$$
$$(\sqrt{2}+\sqrt{3})^4 = (5+2\sqrt{6})^2 = 49+20\sqrt{6} = 10\cdot(\sqrt{2}+\sqrt{3})^2 - 1$$

donc $\mathrm{T}^4-10\mathrm{T}^2+1$ annule $\sqrt{2}+\sqrt{3}$. On peut chercher à démontrer à la main qu'il est irréductible, mais, en suivant l'indication, nous allons démontrer que $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$.

Nous aurons alors progressé : puisque $\sqrt{3}\notin\mathbb{Q}(\sqrt{2})$ (si $\sqrt{3} = a+b\sqrt{2}$, avec $a,b\in\mathbb{Q}$, on obtient en élevant au carré et en identifiant les coefficients dans la base $(1,\sqrt{2})$ du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}(\sqrt{2})$: $3 = a^2+2b^2$ et $2ab = 0$, ce qui entraîne que soit $\sqrt{3}$ soit $\sqrt{3}/2$ est rationnel, contradiction), on a

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2})(\sqrt{3}):\mathbb{Q}(\sqrt{2})]\cdot[\mathbb{Q}(\sqrt{2}):\mathbb{Q}) = 4.$$

L'élément $\sqrt{2}+\sqrt{3}$ est alors de degré 4, et son polynôme minimal est bien $\mathrm{T}^4-10\mathrm{T}^2+1$.

Il est déjà évident que $\sqrt{2}+\sqrt{3}\in\mathbb{Q}(\sqrt{2},\sqrt{3})$, et donc que $\mathbb{Q}(\sqrt{2}+\sqrt{3})\subset\mathbb{Q}(\sqrt{2},\sqrt{3})$. Réciproquement, remarquons que $(\sqrt{3}-\sqrt{2})(\sqrt{3}+\sqrt{2}) = 3-2 = 1$. Ainsi, $\sqrt{3}-\sqrt{2} = (\sqrt{2}+\sqrt{3})^{-1}$ est un élément de $\mathbb{Q}(\sqrt{2}+\sqrt{3})$. Il en est alors de même de

$$\sqrt{2} = \frac{(\sqrt{3}+\sqrt{2})-(\sqrt{3}+\sqrt{2})^{-1}}{2} \qquad \text{et} \qquad \sqrt{3} = \frac{(\sqrt{3}+\sqrt{2})+(\sqrt{3}+\sqrt{2})^{-1}}{2}.$$

Ainsi, $\sqrt{2}$ et $\sqrt{3}$ appartiennent à $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ ce qui achève la preuve de l'égalité

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3}).$$

9. On a déjà vu que pour une extension L/K, l'ensemble des éléments de L algébriques sur K formait un sous-corps de L. L'ensemble $\overline{\mathbb{Q}}$ est donc un sous-corps de $\mathbb{C}$, et il est à ce titre de caractéristique nulle. Si on note V(P) l'ensemble des zéros d'un polynôme P, on a en outre

$$\overline{\mathbb{Q}} = \bigcup_{P \in \mathbb{Q}[X]\setminus\{0\}} V(P),$$

ce qui définit $\overline{\mathbb{Q}}$ comme une union dénombrable d'ensembles finis et prouve bien que $\overline{\mathbb{Q}}$ est dénombrable (ce qui démontre l'existence d'éléments de $\mathbb{C}$, ou de $\mathbb{R}$, transcendants sur $\mathbb{Q}$).

De manière semblable à ce que l'on a fait pour démontrer que les éléments algébriques forment un corps, on peut remarquer que si (α_i) est une famille finie d'algébriques, l'extension $\mathbb{Q}(\alpha_1,\ldots,\alpha_n)$, que l'on peut voir soit comme le plus petit sous-corps contenant $\mathbb{Q}$ et les α_i, soit à l'aide de la relation de récurrence $\mathbb{Q}(\alpha_1,\ldots,\alpha_i) = \mathbb{Q}(\alpha_1,\ldots,\alpha_{i+1})[\alpha_i]$ (en n'oubliant pas que si α_i est algébrique sur $\mathbb{Q}$, il l'est *a fortiori* sur $\mathbb{Q}(\alpha_1,\ldots,\alpha_{i+1})$), est une extension de degré finie de $\mathbb{Q}$.

Soit donc $P = a_0 + a_1X + \ldots + a_dX^d \in \overline{\mathbb{Q}}[X]$ et $\alpha \in \mathbb{C}$ une racine de P. Si on pose $K = \mathbb{Q}(a_1,\ldots,a_d)$, on peut voir P comme un polynôme de K[X] et donc α comme un élément algébrique sur K. Les extensions $K(\alpha)/K$ et $K/\mathbb{Q}$ étant alors de degré fini, il en est de même de $K(\alpha)/\mathbb{Q}$ donc α, vivant dans une extension de degré fini de $\mathbb{Q}$ est bien algébrique sur $\mathbb{Q}$. Le corps $\overline{\mathbb{Q}}$ est donc bien algébriquement clos.