Fiche 2 exercice 12 : Soient $K := \mathbb{Q}(t), K_1 := \mathbb{Q}(t^2), K_2 := \mathbb{Q}(t^2 - t)$.

On a $K = K_1(t)$. Or t est annulé par le polynôme $X^2 - t^2 \in K_1[X]$. Ce polynôme est de degré 2 donc t est de degré 1 ou 2 sur K_1. Il est clair que $t \notin K_1$ donc t est de degré 2 sur K_1 et $[K : K_1] := \dim_{K_1} K = 2$. De même, $[K : K_2] = 2$.

Montrons que $K_1 \cap K_2 = \mathbb{Q}$. Soit $f(t) \in K_1 \cap K_2$. Alors $f \in K_1 \Rightarrow f$ est une fraction rationnelle en t^2 donc $f(t) = f(-t)$. De plus, $f \in K_2 \Rightarrow f$ est une fraction rationnelle en $t^2 - t$ donc $f(1 - t) = f(t)$. On en déduit que $f(1 + t) = f(t)$. Mais alors, si $f \neq 0$, f n'a ni zéro ni pôle dans $\mathbb{C}$ (si z était un zéro ou un pôle, $1 + z, 2 + z, ...$ le seraient aussi ce qui ferait une infinité de pôles ou de zéros). On a donc que f est constante *i.e.* $f(t) \in \mathbb{Q}$.

Cet exercice donne un exemple d'extensions finies K/K_1 et K/K_2 telles que $K/(K_1 \cap K_2)$ n'est pas finie (en effet, $\mathbb{Q}(t)$ n'est pas de dimension finie sur $\mathbb{Q}$).

Fiche 3 exercice 1 :

Soit $\varphi : \mathbb{Q} \to \mathbb{C}$ un morphisme de corps. Alors, $\varphi(1) = 1$ et donc par récurrence :$\varphi(n) = n$ pour tout n entier ≥ 0. On en déduit que $\varphi(n) = n$ pour tout $n \in \mathbb{Z}$. Comme φ préserve le produit on a aussi pour tous entiers p, q, $q \neq 0$:

$$p = \varphi(p) = \varphi(p/q.q) = \varphi(p/q)q \Rightarrow \varphi(p/q) = p/q$$

donc φ laisse inchangés les rationnels.

Soit $\varphi : \mathbb{R} \to \mathbb{R}$ un automorphisme de corps. Alors, φ laisse fixes les rationnels. de plus $\varphi(x^2) = \varphi(x)^2$ pour tout $x \in \mathbb{R}$ donc φ envoie un réel positif sur un réel positif. On en déduit que φ est une fonction croissante $\mathbb{R} \to \mathbb{R}$.

Soit $x \in \mathbb{R}$. Pour tous rationnels r_1, r_2 tels que $r_1 < x < r_2$, on a donc $r_1 \leq \varphi(x) \leq r_2$. Comme $\mathbb{Q}$ est dense dans $\mathbb{R}$, on peut choisir r_1, r_2 arbitrairement proches de x donc : $\varphi(x) = x$.

Remarque : en revanche, il y a une infinité d'automorphismes $\mathbb{C} \to \mathbb{C}$. En effet, on peut pour des raisons de cardinal ($\mathbb{C}$ n'est pas dénombrable) trouver une infinité non dénombrable d'éléments x_i, $i \in I$, d'éléments de $\mathbb{C}$ algébriquement indépendants sur $\mathbb{Q}$. Alors, toute permutation des x_i définit un automorphisme du corps $\mathbb{Q}(x_i, i \in I)$. Mais tout automorphisme d'un sous-corps de $\mathbb{C}$ se prolonge en un automorphisme de $\mathbb{C}$, car $\mathbb{C}$ est algébriquement clos.

Les corps $\mathbb{Q}(i)$ et $\mathbb{Q}(j)$ ne sont pas isomorphes :

Les seuls morphismes de $\mathbb{Q}(i)$ dans $\mathbb{C}$ sont la restriction de l'identité et de la conjugaison complexe. Idem pour $\mathbb{Q}(j)$. Pourtant $\mathbb{Q}(i)$ n'est pas isomorphe à $\mathbb{Q}(j)$. En effet, par exemple, dans $\mathbb{Q}(i)^\times$ il existe un élément d'ordre 4 : i. En revanche dans $\mathbb{Q}(j)^\times$ il n'y a pas d'élément d'ordre 4 puisque les seuls éléments de $\mathbb{C}^\times$ d'ordre 4 sont $-i$ et i et $\pm i \notin \mathbb{Q}(j) = \mathbb{Q} \oplus \mathbb{Q}j$ (car $\sqrt{3}$ n'est pas rationnel).

Les plongements de $\mathbb{Q}(\sqrt[3]{2})$ dans $\mathbb{C}$:D'après le critère d'Eisenstein, le polynôme $X^3 - 2$ est irréductible sur $\mathbb{Z}$ donc sur $\mathbb{Q}$. Donc $X^3 - 2$ est le polynôme minimal de $\sqrt[3]{2}$ sur $\mathbb{Q}$. Ses racines dans $\mathbb{C}$ sont $\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}$. Donc les seuls morphismes de corps de $\mathbb{Q}(\sqrt[3]{2})$ dans $\mathbb{C}$ sont le morphisme qui envoie $\sqrt[3]{2}$ sur $\sqrt[3]{2}$ (c'est l'identité) celui qui envoie $\sqrt[3]{2}$ sur $j\sqrt[3]{2}$ et celui qui envoie $\sqrt[3]{2}$ sur $j^2\sqrt[3]{2}$.

fiche 2 exercice 2 :

a) Soit K une extension algébrique de $\mathbb{R}$. Si $K \neq \mathbb{R}$, montrons que $K \simeq \mathbb{C}$. Soit $x \in K \setminus \mathbb{R}$. Soit P le polyn ôme minimal de x sur $\mathbb{R}$. C'est un polynôme irréductible sur $\mathbb{R}$ car $\mathbb{R}[X]/(P) \simeq \mathbb{R}[x]$ qui est intègre. Soit $z \in \mathbb{C}$ une racine de P dans $\mathbb{C}$ (on admet que $\mathbb{C}$ est algébriquement clos). Alors $z \notin \mathbb{R}$ (car P est irréductible de degré > 1). On a donc $\mathbb{R}[z] = \mathbb{C}$. Or $\mathbb{R}[x] \simeq \mathbb{R}[X]/(P) \simeq \mathbb{R}[z] = \mathbb{C}$.

En particulier $\mathbb{R}[x]$ est algébriquement clos. Or K est une extension algébrique de $\mathbb{R}$ donc de $\mathbb{R}[x]$. Donc $K = \mathbb{R}[x] \simeq \mathbb{C}$ (en effet si $y \in K$, le polynôme minimal de y sur $\mathbb{R}[x]$ est scindé dans $\mathbb{R}[x]$ et irréductible donc de degré 1).

b) D'après le critère d'Eisenstein, pour tout n, le polynôme $X^n - 2$ est irréductible sur $\mathbb{Q}$. Donc l'extension $\mathbb{Q}(\sqrt[n]{2})/\mathbb{Q}$ est de degré n. Or, $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[n]{2}) \subseteq \overline{\mathbb{Q}}$. Donc pour tout n, $[\overline{\mathbb{Q}} : \mathbb{Q}] \geq [\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$ et $[\overline{\mathbb{Q}} : \mathbb{Q}]$ n'est pas fini.

Les corps finis

Exercice 4 fiche 3 :

Soit p un nombre premier. L'idéal $p\mathbb{Z}$ est premier non nul dans $\mathbb{Z}$ donc maximal (car $\mathbb{Z}$ est principal). Donc le quotient $\mathbb{Z}/p\mathbb{Z}$ est un corps que l'on note $\mathbb{F}_p$.

a) Soit P un polynôme irréductible sur $\mathbb{F}_p$ de degré n. Soit $K := \mathbb{F}_p[X]/(P)$. C'est un corps qui est une extension algébrique de $\mathbb{F}_p$ de degré (ou dimension) n. Donc K est de cardinal $|\mathbb{F}_p^n| = p^n$. Notons x la classe de X mod (P). Le polynôme P est le polynôme minimal (à multiplication par un scalaire non nul près pour le rendre unitaire) de x sur $\mathbb{F}_p$. Or, $K^\times$ est un groupe fini de cardinal $p^n - 1$. Mais alors, d'après le théorème de Lagrange, $z^{p^n-1} = 1$ pour tout $z \in K^\times$. En particulier, $x^{p^n} - x = 0$ *i.e.* le polynôme $X^{p^n} - X$ annule x. On en déduit (par définition du polynôme minimal) que $P | X^{p^n} - X$ sur $\mathbb{F}_p$.

Soit $\mathscr{I}_d$ l'ensemble des polynômes unitaires irréductibles sur $\mathbb{F}_p$ de degré d. Si $P \in \mathscr{I}_d$, alors $P | X^{p^d} - X$. Or, si $d|n$, $X^{p^d} - X | X^{p^n} - X$. En effet, $p^n - 1 = (p^d)^{n/d} - 1 = (p^d - 1)(1 + ... + p^{n/d-1})$ donc $p^d - 1 | p^n - 1$. On en déduit que :

$$\begin{aligned} X^{p^n} - X = X(X^{p^n-1} - 1) &= X((X^{p^d-1})^{\frac{p^n-1}{p^d-1}} - 1) \\ &= X(X^{p^d-1} - 1)(...) \\ &= (X^{p^d} - X)(...) \ . \end{aligned}$$

Donc, $\prod_{\substack{d|n \\ P\in\mathscr{I}_d}} P | X^{p^n} - X$.

Réciproquement, ...

Le polynôme $X^{p^n} - X$ est premier avec son polynôme dérivé qui est -1 (on est en carctéristique p). Donc dans la décomposition de $X^{p^n} - X$ en facteurs irréductibles dans $\mathbb{F}_p[X]$, chaque facteur irréductible apparaît une seule fois. Donc pour montrer que $X^{p^n} - X = \prod_{\substack{d|n \\ P\in\mathscr{I}_d}} P | X^{p^n} - X$, il suffit de montrer que si P est un facteur irréductible (disons unitaire) de $X^{p^n} - X$ dans $\mathbb{F}_p[X]$, alors P est de degré d qui divise n.

Soit P un tel facteur et notons d son degré. Soit $K := \mathbb{F}_p[X]/(P)$. Le corps K est de cardinal p^d. Donc, si on note $x := X \bmod (P)$, on a : $K = \mathbb{F}_p(x)$ et comme on est en caractéristique p, pour tout f polynôme à coefficients dans $\mathbb{F}_p$, on a : $f(x)^{p^n} = f(x^{p^n})$. or P divise $X^{p^n} - X$ donc $P(x) = 0 \Rightarrow x^{p^n} = x$. Donc pour tout $f(x) \in K$, on a : $f(x)^{p^n} = f(x)$. Donc $y^{p^n-1} = y$ pour tout $y \in K^\times$. Or, le groupe $K^\times$ est cyclique d'ordre p^d-1. Donc on a : $p^d-1|p^n-1$. Mais il est facile de voir que si r est le reste de la division euclidienne de n par d, alors $p^r - 1$ est le reste de la division euclidienne de $p^n - 1$ par $p^d - 1$. On a donc $p^r - 1 = 0$ et $r = 0$ *i.e.* $d|n$.

Fiche 3 exercice 5 : L'anneau $\mathbb{Z}[i]$ est principal. En effet, on pose $N(a + bi) := a^2 + b^2$ si $a, b \in \mathbb{Z}$. On voit que si $x, y \in \mathbb{Z}[i]$, alors si $y \neq 0$, il existe $z, r \in \mathbb{Z}[i]$ tel que $x = yz + r$ avec $N(r) < N(y)$ (c'est une sorte de division euclidienne, on dit que $\mathbb{Z}[i]$ est euclidien et cela entraîne que $\mathbb{Z}[i]$ est principal).

Si P est un idéal premier non nul de $\mathbb{Z}[i]$, alors P est maximal (car $\mathbb{Z}[i]$ est principal). Donc $\mathbb{Z}[i]/P$ est un corps. Si $x \in P$, alors $N(x) = x\overline{x} \in P \cap \mathbb{Z}$. Donc $P \cap \mathbb{Z}$ est un idéal premier non nul de $\mathbb{Z}$; notons p un nombre premier > 0 qui engendre $P \cap \mathbb{Z}$. On a donc :

$$\mathbb{Z}/p\mathbb{Z} \subseteq \mathbb{Z}[i]/P$$

et $\mathbb{Z}[i]/P = \mathbb{F}_p[\overline{i}]$ où $\overline{i}$ est la classe de i mod P. Mais $i^2 + 1 = 0$ donc $\overline{i}$ est de degré 1 ou 2 sur $\mathbb{F}_p$. Par conséquent, $\mathbb{Z}[i]/P$ est de cardinal p ou p^2.

Exemples : on voit facilement que 7 et $2 + i$ sont premiers dans $\mathbb{Z}[i]$ (en effet, si $uv = 7$, alors $N(u)N(v) = 49 \Rightarrow N(u) = 1, 7$ ou 49 (les seuls diviseurs entiers > 0 de 49) ; or, si $N(u) = 1$, u est inversible d'inverse $\overline{u}$, si $N(u) = 49$, v est inversible et le cas $N(u) = 7$ est impossible !).

Or $7\mathbb{Z}[i] \cap \mathbb{Z} = 7\mathbb{Z}$. Donc $\mathbb{Z}[i]/7\mathbb{Z}[i]$ est une extension de $\mathbb{F}_7$. Comme -1 n'a pas de racine carrée dans $\mathbb{F}_7$, $\mathbb{Z}[i]/7\mathbb{Z}[i]$ est un corps fini de cardinal 49.

Comme $2^2 = -1 \bmod 5$, comme $(2+i)\mathbb{Z}[i] \cap \mathbb{Z} = 5\mathbb{Z}$, on voit que $i \bmod (2+i) \in \mathbb{Z}/5\mathbb{Z}$ et que : $\mathbb{F}_5 \simeq \mathbb{Z}[i]/(2+i)$.