Corrigé examen final Algèbre 2, mai 2023

Exercice 1. $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$, où $j = e^{\frac{2i\pi}{3}}$. Par le théorème de la base télescopique le degré est le produit de $[\mathbb{Q}(\sqrt[3]{2}, j) : \mathbb{Q}(\sqrt[3]{2})]$ et $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$. Le deuxième est égal à 3 parce que : $X^3 - 2 \in \mathbb{Q}[X]$ est unitaire, irréductible par Eisenstein et s'annule en $\sqrt[3]{2}$, c'est donc le polynôme minimal de $\sqrt[3]{2}$. Le premier est égal à 2 parce que j n'appartient pas à $\mathbb{R}$, donc $[\mathbb{Q}(\sqrt[3]{2}, j) : \mathbb{Q}(\sqrt[3]{2})] > 1$ et $X^2 + X + 1$ s'annule en j, donc $[\mathbb{Q}(\sqrt[3]{2}, j) : \mathbb{Q}(\sqrt[3]{2})] \leq 2$.

Exercice 2. Chaque élément x tel que $x \neq x^{-1}$ se simplifie avec son inverse dans le produit. Restent les éléments du corps qui vérifient $x = x^{-1}$, soit $x^2 = 1$, soit $(x-1)(x+1) = 0$. Donc 1 et -1 quand ils sont distincts, et alors le produit est -1. Quand $1 = -1$, le produit est cet élément, qui est -1.

Exercice 3. $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ est normale parce que $\mathbb{Q}(\sqrt{2})$ est le corps de décomposition de $X^2 - 2$ sur $\mathbb{Q}$. $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ est normale parce que $\mathbb{Q}(\sqrt[4]{2})$ est le corps de décomposition de $X^2 - \sqrt{2}$ sur $\mathbb{Q}(\sqrt{2})$. Mais $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ n'est pas normale, parce que $X^4 - 2 = (X^2 - \sqrt{2})(X^2 + \sqrt{2})$ est un polynôme à coefficients dans $\mathbb{Q}$, irréductible par Eisenstein, qui a une racine dans $\mathbb{Q}(\sqrt[4]{2})$, mais qui n'est pas scindé sur $\mathbb{Q}(\sqrt[4]{2})$ parce qu'il n'est même pas scindé sur $\mathbb{R}$, le polynôme $X^2 + \sqrt{2}$ n'ayant pas des racines réelles.

Exercice 4. L'application $f : \mathbb{F}^\times \to \mathbb{F}^\times$ définie par $f(x) = x^2$ est un morphisme de groupes. L'image est formée des éléments de $\mathbb{F}^\times$ qui sont des carrés. Par le théorème d'isomorphisme, le cardinal de l'image est le quotient de $q - 1$ par le cardinal du noyau. Or, le noyau est donné par $x^2 = 1$, soit $(x-1)(x+1) = 0$, et il est formé donc de 1 et -1. Or, $1 \neq -1$ parce que si $1 = -1$ alors $1 + 1 = 0$ et la caractéristique de $\mathbb{F}$ est 2, ce qui est impossible parce que q est une puissance de la caractéristique (ou parce que l'ordre de 1 dans $(\mathbb{F}, +)$ divise $|\mathbb{F}|$). Il y a donc $(q-1)/2$ carrés dans $\mathbb{F}^\times$. Il y a un de plus dans $\mathbb{F}$, parce que 0 est un carré.

Exercice 5. Supposons qu'il y a au moins une racine x. On a $x^p = 2$, donc $X^p - 2 = (X - x)^p$ et ce polynôme n'a pour racine que x.

Exercice 6. Par le théorème de plongement des extensions monogènes il existe un unique K-plongement f de $K(x)$ dans $\bar{K}$ tel que $f(x) = y$. Par le théorème de prolongement, parce que $\bar{K}/K(x)$ est algébrique et $\bar{K}$ est algébriquement clos, il existe un unique K-morphisme $\iota : \bar{K} \to \bar{K}$ qui prolonge f. Reste à montrer que ι est un isomorphisme, et on se rappelle d'un exercice de TD. Un morphisme de corps est injectif, donc ι est injectif. Il suffit de montrer que ι est surjectif. Soit $u \in \bar{K}$. Il est algébrique sur K et il a un polynôme minimal P_u sur K qui, lui, a n racines $x_1, x_2, ..., x_n$ dans $\bar{K}$. Comme ι est injectif et transforme toute racine de P_u en une racine de P_u, ι induit une application bijective de $\{x_1, x_2, ..., x_n\}$ dans lui-même. Donc u se trouve dans l'image de ι.

Pour la surjectivité, on peut aussi montrer que $K/\iota(K)$ est algébrique, tandis que $\iota(K)$ est algébriquement clos et n'a donc pas d'extension algébrique autre que lui-même.

Exercice 7. (a) Posons $E = K(x)$. Le polynôme minimal de x est de degré $[K(x) : K] = [E : K] = n$. Il est séparable, donc il a n racines dans $\bar{K}$. Il existe donc n K-plongements de $E = K(x)$ dans $\bar{K}$ par le théorème du plongement des extensions monogènes.

(b) Soit $x \in E \backslash K$. Si $K(x) = E$ c'est bon (point (a)). Sinon, on regarde $K(x)/K$ (de degré k) et $E/K(x)$ (de degré m) où $km = n$ et $k, m < n$. Par hypothèse de récurrence, il existe k K-plongements $f_1, f_2, .., f_k$ de $K(x)$ dans $\bar{K}$. Il suffit de montrer que pour chacun il existe m prolongements de ce plongement à E (dans l'autre sens, tout K-plongement de E dans $\bar{K}$ induit par restriction un K-plongement de $K(x)$). Notons que, si f_1 est le plongement qui est l'identité sur $K(x)$, alors il est $K(x)$-linéaire et l'hypothèse de récurrence montre qu'effectivement il existe m $K(x)$-morphismes de E dans $\bar{K}$, autrement dit qui prolongent f_1. Si $f : K(x) \to \bar{K}$ n'induit pas l'identité sur $K(x)$, alors l'image de x par f est un élément $y \neq x$ qui est une racine du polynôme minimal de x. On note $\iota : \bar{K} \to \bar{K}$ un K-isomorphisme qui transforme y en x comme dans l'exercice 6. Alors $\iota \circ f : K(x) \to \bar{K}$ induit l'identité sur $K(x)$ et admet donc exactement k prolongements distincts à E. En recomposant avec ι^{-1}, on obtient une bijection entre les prolongements de f à E et les prolongements de $f \circ \iota$ à E, d'où exactement k prolongements de f à E.

(c) Le fait que ce soit un sous-espace vectoriel se vérifie facilement. Le fait qu'il soit propre vient du fait que sinon on aurait $\sigma_i(x) = \sigma_j(x)$ pour tout x et donc $\sigma_i = \sigma_j$ (or, ils sont distincts).

(d) Puisque $K(x) \subset E$, il suffit de montrer que $[K(x) : K] \geq [E : K] = n$. Or, les $\sigma_i(x)$ étant tous distincts, les restrictions des σ_i à $K(x)$ sont distinctes, donc il y a au moins n K-plongements de $K(x)$ dans $\bar{K}$, donc par la question (a) on a $[K(x) : K] \geq n$.