Correction du contrôle du mercredi 9 mars 2022 (CC1)

Exercice 1 a) Si $x \in A$, alors $F[x] \leq A$ donc $F[x]$ est de dimension finie. Soit $n \geq \dim F[x]$. En particulier les monômes $1, ..., x^n$ sont liés. Il existe donc $a_0, ..., a_n \in F$ non tous nuls tels que :

$$a_0 + ... + a_n x^n = 0$$

et le polynôme $a_0 + ... + a_n X^n \in F[X]$ est non nul et annule x.

b) Soit $k \leq A$ un corps. Si $x \in A$, alors $k[x]$ est un corps $\Leftrightarrow$ x est algébrique sur k. En effet, on a un isomorphisme d'anneaux :

$$k[x] \simeq k[X]/I_x$$

où I_x est l'idéal des polynômes à coefficients dans k annulateurs de x. Comme $k[x] \leq A$, l'anneau $k[x]$ est intègre donc l'idéal I_x est premier. Donc $k[x]$ est un corps $\Leftrightarrow$ l'idéal I_x est maximal$\Leftrightarrow$ l'idéal I_x est un idéal premier non nul $\Leftrightarrow$ x est algébrique sur k.

On en déduit que $F[\alpha_1]$ est un corps. Comme α_2 est algébrique sur F, c'est aussi algébrique sur $F[\alpha_1]$ donc $F[\alpha_1, \alpha_2] = F[\alpha_1][\alpha_2]$ est un corps. De même, $F[\alpha_1, \alpha_2, \alpha_3], ..., F[\alpha_1, ..., \alpha_n]$ sont des corps.

Par multiplicativité des degrés, on a

$$[F[\alpha_1, ..., \alpha_n] : F] =$$

$$[F[\alpha_1, ..., \alpha_n] : F[\alpha_1, ..., \alpha_{n-1}].[F[\alpha_1, ..., \alpha_{n-1}] : F[\alpha_1, ..., \alpha_{n-2}]]...$$

$$...[F[\alpha_1] : F] < \infty$$

Car pour tout i, α_i est algébrique sur F donc sur $F[\alpha_1, ..., \alpha_{i-1}]$.

c) Si x, y sont algébriques sur F, alors $\dim F[x, y]$ est finie.
En particulier, Si $z = x+y, xy, x-y$, ou $\frac{x}{y}$ (si $y \neq 0$), alors $F[z] \leq F[x, y]$ est de dimension finie aussi et z est algébrique sur F. Donc l'ensemble des éléments de A algébriques sur F est bien un sous-corps de A.

d) Si $\dim A < \infty$, alors tous les éléments de A sont algébriques sur F d'après a). Donc l'ensemble des éléments de A algébriques sur F est A et A est un corps d'après c).

Exercice 2 a) On a $x_1^2 = 1 + \sqrt{2} \Rightarrow (x_1^2 - 1)^2 = 2 \Rightarrow x_1^4 - 2x_1^2 - 1 = 0$. On peut donc prendre $P(X) = X^4 - 2X^2 - 1$.

b)

$$P(X+1) = (X+1)^4 - 2(X+1)^2 - 1 = X^4 + 4X^3 + 4X^2 - 2$$

D'après le critère d'Eisenstein avec le nombre premier 2, $P(X+1)$ est irréductible sur $\mathbb{Q}$. Or $X \mapsto X+1$ induit un automorphisme de l'algèbre $\mathbb{Q}[X]$ donc $P(X)$ aussi est irréductible sur $\mathbb{Q}$.
Or $P(x_1) = 0 \Rightarrow P$ est divisible par le polynôme minimal de x_1 sur $\mathbb{Q}$. Comme P est irééductible est unitaire, P est donc le polynôme minimal de x_1 sur $\mathbb{Q}$. Donc

$$[\mathbb{Q}(x_1) : \mathbb{Q}] = \deg P = 4 \ .$$

c) $\sqrt{2} = x_1^2 - 1 \in \mathbb{Q}(x_1) \Rightarrow \mathbb{Q}(\sqrt{2}) \leq \mathbb{Q}(x_1)$. L'inclusion est stricte car :

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 < 4 = [\mathbb{Q}(x_1) : \mathbb{Q}] \ .$$

d) On calcule :

$$P(\frac{i}{x_1}) = \frac{1}{x_1^4} + \frac{2}{x_1^2} - 1 = -\frac{P(x_1)}{x_1^4} = 0$$

de plus $P(-x) = P(x)$. On a donc 4 racines de P :

$$\pm x_1, \pm\frac{i}{x_1}$$

ce sont les seules car P est de degré 4.

e) On a

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(x_1)][\mathbb{Q}[x_1] : \mathbb{Q}] = 4[\mathbb{Q}(x_1)(i) : \mathbb{Q}(x_1)] \ .$$

Comme $i \notin \mathbb{R}$, $i \notin \mathbb{Q}(x_1)$ et $[\mathbb{Q}(x_1)(i) : \mathbb{Q}(x_1)] \geq 2$. Puisque $X^2 + 1$ annule i, $[\mathbb{Q}(x_1)(i) : \mathbb{Q}(x_1)] = 2 \Rightarrow [K : \mathbb{Q}] = 8$.
Or toujours grâce à la multiplicativité des degrés, on a :

$$[K : \mathbb{Q}(i)] = \frac{[K : \mathbb{Q}]}{[\mathbb{Q}(i) : \mathbb{Q}]} = 4 \ .$$

Comme $K = \mathbb{Q}(i)(x_1)$, le degré de x_1 sur $\mathbb{Q}(i)$ et 4 donc P est aussi le polynôme minimal de x_1 sur $\mathbb{Q}(i)$.

f) Soit $f \in \mathrm{Aut}K$. Alors f est $\mathbb{Q}-$linéaire et comme $K = \mathbb{Q}(i, x_1)$, f est uniquement déterminé par $f(i)$ et $f(x_1)$. Or $i^2 = -1 \Rightarrow f(i)^2 = -1 \Rightarrow f(i) = \pm i$. De même, $P(x_1) = 0 \Rightarrow P(f(x_1)) = 0$ car P est à coefiicients dans $\mathbb{Q}$ donc $f(x_1) = x_1, x_2, x_3$, ou x_4. Donc il y a au plus $2.4 = 8$ morphismes f possibles et $|\mathrm{Aut}K| \leq 8$.

g) Comme P est le polynôme minimal de x_1 sur $\mathbb{Q}(i)$, on a un isomorphisme d'anneaux

$$K = \mathbb{Q}(i)(x_1) \simeq \mathbb{Q}(i)[X]/(P) \ .$$

L'application $\mathbb{Q}(i)-$linéaire

$$\mathbb{Q}(i)[X] \to \mathbb{C}\, R(X) \mapsto R(x_2)$$

est

un morphisme d'anneaux dont le noyau contient (P) (car $P(x_2) = 0$) d'où un morphisme d'anneaux $\sigma : K =\simeq \mathbb{Q}(i)[X]/(P) \to \mathbb{C}$ tel que $\sigma(i) = i$ (car σ est $\mathbb{Q}(i)-$linéaire et $\sigma(x_1) = x_2$.

h) Comme σ est défini sur un corps, σ est injectif.
Comme $\sigma(x_1) = x_2 = \frac{i}{x_1} \in K$, $\sigma(K) = \mathbb{Q}(i)(\sigma(x_1)) \leq K$.
Comme K est un $\mathbb{Q}-$espace vectoriel de dimension finie 8, comme σ est un endomorphisme $\mathbb{Q}-$linéaire injectif, c'est aussi surjectif. Donc σ est un isomorphisme du corps K.

i) τ est un automorphisme du corps $\mathbb{C}$ et $\tau(K) = \tau(\mathbb{Q}(i, x_1)) = \mathbb{Q}(-i, x_1) = \mathbb{Q}(i, x_1) = K$. Donc τ induit par restriction un automorphisme de K.

j) On a $\sigma^2(x_1) = \sigma(\frac{i}{x_1}) = \frac{i}{\sigma(x_1)} = x_1$ et comme $\sigma^2(i) = i$, $\sigma^2 = \mathrm{Id}$. Comme $\sigma \neq \mathrm{Id}$, σ est d'ordre 2. Comme $\tau^2 = \mathrm{Id}$ et $\tau \neq \mathrm{Id}$ (car $\tau(x_2) = x_4 \neq x_2$), τ aussi est d'ordre 2.

Il y avait une erreur dans l'énoncé : $\tau\sigma\tau^{-1} \neq \sigma^{-1}$.

On peut néanmoins vérifier que $\sigma\tau(x_1) = x_2 \neq= -x_2 = \tau\sigma(x_1) \Rightarrow \sigma\tau \neq \tau\sigma$.

k) Le groupe $G' := \langle \sigma, \tau \rangle$ est un sous-groupe de $\mathrm{Aut}K$ donc d'ordre ≤ 8. Pour montrer l'égalité, il suffit de voir que $\sigma\tau$ est d'ordre 4 car $(\sigma\tau)^2(x_1) = \sigma\tau(\frac{i}{x_1}) = -x_1$ et $(\sigma\tau)^4(x_1) = x_1$; $(\sigma\tau)^4(i) = i$.

Donc G' est d'odre un multiple de 4. Donc G' est d'ordre 4 ou 8. L'ordre n'est pas 4 car les groupes d'ordre 4 sont abéliens et $\sigma\tau \neq \tau\sigma$. Donc G' est d'ordre 8 et $G' = G$.