Corrigé du contrôle continu du lundi 29 mars 2021

Exercice 1 Soit k un corps. Soit $\overline{k}$ la clôture algébrique de k. Soit K le corps de décomposition de $X^n - 1$ sur k. On note G l'ensemble des racines de $X^n - 1$ dans $\overline{k}$.

a) L'extension K/k est toujours normale car K est un corps de décomposition sur k d'un polynôme.

L'extension K/k est toujours séparable. En effet K est engendré sur k par les racines de X^n-1. Or $(X^n-1)' = nX^{n-1}$. Donc si la caractéristique de k est nulle, les racines $z_1, ..., z_n$ de X^n-1 sont simples (car elles n'annulent pas X^{n-1}) donc $X^n - 1$ est séparable sur k. Donc $K = k(z_1, ..., z_n)$ est séparable sur k comme corps de décomposition sur k d'un polynôme séparable. Si k est de caractéristique $p > 0$. On peut écrire $n = p^\alpha n'$ où $\alpha \in \mathbb{N}$ et n' est premier à p. On a alors $X^n - 1 = X^{n'p^\alpha} - 1 = (X^{n\prime} - 1)^{p^\alpha}$ dans $k[X]$. Donc K est le corps de décomposition de $X^{n'} - 1$ sur k. Puisque $p \not| n'$ le polynôme $X^{n'} - 1$ et sa dérivée $n'X^{n'-1}$ sont premiers entre eux et les racines $z_1, ..., z_{n'}$ de $X^{n\prime} - 1$ dans $\overline{k}$ sont simples donc $X^{n'} - 1$ est séparable sur k. Donc l'extension K/k est séparable comme corps de décomposition d'un polynôme séparable sur k.

Une extension normale et séparable est galoisienne donc l'extension K/k est toujours galoisienne.

b) L'ensemble des racines de $X^n - 1$ est clairement un sous-groupe de K^*. C'est un sous-groupe fini de cardinal $\leq n$. En particulier, G est cyclique et il existe $g \in G$ d'ordre m. Comme $g^n = 1$, on a $m|n$.

On a $m = n$ si et seulement si les racines de $X^n - 1$ sont simples $\Leftrightarrow$ $X^n - 1$ et nX^{n-1} sont premiers entre eux $\Leftrightarrow n.1 \neq 0$ dans $k \Leftrightarrow p \not| n$ si p est la caractéristique de k.

c) Soit p la caractéristique de k. Si $p \neq n$, $m = n$, si $p|n$, alors $m = \frac{n}{p^\alpha}$ où p^α est la plus grande puissance de p qui divise n. En effet dans ce cas, $X^n - 1 = (X^{\frac{n}{p^\alpha}} - 1)^{p^\alpha}$ et les racines de $X^{\frac{n}{p^\alpha}} - 1$ sont simples et forment un ensemble de $\frac{n}{p^\alpha}$ éléments.

Exercice 2

Soit $P(X) = \frac{X^3}{3!} + \frac{X^2}{2} + X + 1 \in \mathbb{Q}[X]$.

a) $P = \frac{1}{6}(X^3+3X^2+6X+6)$. D'après le critère d'Eisenstein pour le nombre premier 3, $X^3 + 3X^2 + 6X + 6$ est irréductible sur $\mathbb{Q}$ car $3|6, 3$ et $3^2 \not| 6$. Donc P est irréductible sur $\mathbb{Q}$.

b) $P' = \frac{X^2}{2} + X + 1$. Donc si z était une racine au moins double de P, on aurait $P(z) = P'(z) = 0 \Rightarrow P(z) - P'(z) = \frac{z^3}{3!} = 0 \Rightarrow z = 0$ *absurde.* Donc les racines de P dans $\mathbb{C}$ sont simples.

c) Les racines de $P' = \frac{X^2}{2} + X + 1$ sont

$$-1 \pm \sqrt{1-2} = -1 \pm i \ .$$

d) On se ramène au calcul du discriminant d'un polynôme unitaire : $\Delta(P) = \Delta(6P) = (-1)^{\frac{3(3-1)}{2}} \text{Rés}_{3,2}(6P, (6P)')$.
Or $\text{Rés}_{3,2}(6P, (6P)') = (-1)^{3.2} 6^3 (6P)(-1-i)(6P(-1+i))$.
Or $P(-1-i) = \frac{(-1-i)^3}{6} + P'(-1-i) = \frac{(-1-i)^3}{6} = \frac{1-i}{3}$.
Donc $P(-1+i) = \frac{1+i}{3}$.
Ainsi, $\Delta(P) = -6^5 . \frac{2}{9} = -12^3$.

e) On a $\Delta(P) = (x_1-x_2)^2(x_2-x_3)^2(x_1-x_3)^2$. Si x_1, x_2, x_3 étaient réelles on aurait $\Delta(P) \geq 0$. Or $\Delta(P) < 0$. Donc P a au moins une racine complexe non réelle : x_2 par exemple. Comme P est réel, $\overline{x_2}$ est aussi une racine de P complexe non réelle. Comme P est de degré 3, P a au moins une racine réelle. Conclusion : P a une racine réelle et deux racines complexes conjuguées non réelles.

f) Il existe un morphisme de corps $\sigma : \mathbb{Q}(x_1) \to \mathbb{C}$ tel que $\sigma(x_1) = x_2$ car x_1, x_2 sont racines du polynôme P irréductible (sur $\mathbb{Q}$). Or $x_2 \notin \mathbb{Q}(x_1) \leq \mathbb{R}$ car x_2 est non réel. Donc $\mathbb{Q}(x_1)$ n'est pas galoisienne sur $\mathbb{Q}$.

g) Soit G le groupe de Galois de P sur $\mathbb{Q}$. Alors $|G| = [\mathbb{Q}(x_1, x_2, x_3) : \mathbb{Q}] = [\mathbb{Q}(x_1, x_2, x_3) : \mathbb{Q}(x_1)][\mathbb{Q}(x_1) : \mathbb{Q}]$. Or comme P est irréductible sur $\mathbb{Q}$, $P = \frac{1}{6}\pi_{x_1}$. Donc $[\mathbb{Q}(x_1) : \mathbb{Q}] = \deg \pi_{x_1} = \deg P = 3$. Comme x_2 est racine de $\frac{P}{X-x_1} \in \mathbb{Q}(x_1)[X]$, on a : $[\mathbb{Q}(x_1, x_2) : \mathbb{Q}(x_1)] \leq 2$. Puisque $x_2 \notin \mathbb{Q}(x_1)$, $[\mathbb{Q}(x_1, x_2) : \mathbb{Q}(x_1)] = 2$. Or $x_1 + x_2 + x_3 = -6\frac{1}{2} = -3$ ($-$ le coefficient de degré 2 de $6P$) donc $\mathbb{Q}(x_1, x_2, x_3) = \mathbb{Q}(x_1, x_2)$ et

$$|G| = [\mathbb{Q}(x_1, x_2, x_3) : \mathbb{Q}] = [\mathbb{Q}(x_1, x_2) : \mathbb{Q}] = [\mathbb{Q}(x_1, x_2) : \mathbb{Q}(x_1)][\mathbb{Q}(x_1) : \mathbb{Q}] = 6$$

.

h) Si $g \in G$, alors g est $\mathbb{Q}$ linéaire donc $P(x_i) = 0 \Rightarrow g(P(x_i)) = P(g(x_i)) = 0$ car P est à coefficients rationnels. Donc $g(x_i)$ est une racine de P et $g(x_i) \in \{x_1, x_2, x_3\}$. Donc g induit bien une permutation de l'ensemble $\{x_1, x_2, x_3\}$.

i) L'application $g \mapsto g\Big|_{\{x_1,x_2,x_3\}}$ est un morphisme de groupes. C'est injectif car g est entièrement déterminé par $g(x_1), g(x_2), g(x_3)$.

j) Donc $|G| \leq |\mathfrak{S}_{\{x_1,x_2,x_3\}}| = 6$. Or $|G| = 6$, donc le morphisme injectif de groupes $G \to \mathfrak{S}_{\{x_1,x_2,x_3\}}$ est bijectif. C'est un isomorphisme.

Exercice 3

a) Les polynômes de degré 2 sur $\mathbb{F}_2$ irréductibles sont ceux qui n'ont pas de racine. Donc $X^2 + X + 1$ est le seul polynôme de degré 2 sur $\mathbb{F}_2$.

b) Le polynôme $P = X^4 + X + 1$ n'a pas de racine dans $\mathbb{F}_2$. S'il était réductible, il serait le produit de deux polynômes irréductibles de degré 2. On aurait alors $P = (X^2 + X + 1)^2 = X^4 + X^2 + 1$ impossible !
Donc $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$.

c) Donc $X^4 + X + 1$ est le polynôme minimal de α sur $\mathbb{F}_2$.
Donc $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = 4$. Donc $\mathbb{F}_2(\alpha)$ est un $\mathbb{F}_2-$espace vectoriel de dimension 4. Donc comme groupe, $\mathbb{F}_2(\alpha) \simeq \mathbb{F}_2^4 \Rightarrow |\mathbb{F}_2(\alpha)| = 2^4 = 16$.

d) Comme $X^4 + X + 1$ est le polynôme minimal de α sur $\mathbb{F}_2$, le morphisme $\mathbb{F}_2[X]/(X^4 + X + 1) \to \mathbb{F}_2(\alpha)$, $X \mapsto \alpha$ est un isomorphisme. En particulier, la base $1, X, X^2, X^3$ de $\mathbb{F}_2[X]/(X^4+X+1)$ est envoyé sur $1, \alpha, \alpha^2, \alpha^3$, base de $K = \mathbb{F}_2(\alpha)$ comme $\mathbb{F}_2-$espace vectoriel.
On a :

$$\alpha^5 = \alpha.(\alpha^4) = \alpha.(-\alpha - 1) = -\alpha^2 - \alpha = \alpha^2 + \alpha \ .$$

Mais alors, $\alpha^5 \neq 1$. On a aussi $\alpha^3 \neq 1$. De plus :

$$\alpha^{15} = 1$$

car $\alpha \in K^*$ qui est un groupe d'ordre 15. Donc l'ordre de α dans K^* divise 15. Comme ce n'est ni 1, ni 3, ni 5, c'est 15.