Corrigé succinct de l'examen final de théorie de Galois du lundi 26 mai 2014

Exercice 1 a) Si P a une racine $x \in \mathbb{Q}$, alors $x \in \mathbb{Z}$ car $\mathbb{Z}$ est intégralement clos. Mais alors $x|1$ donc $x = \pm 1$. Or ± 1 ne sont pas racines. Donc P estt irréductible sur $\mathbb{Q}$.

b) Par exemple, $a = \sqrt[3]{\frac{-1+\sqrt{5}}{2}}, b = \sqrt[3]{\frac{-1-\sqrt{5}}{2}}$. $P(a+b) = a^3 + b^3 + 3(a+b)(ab+1) + 1 = 0$.

c) $\Delta_P = -4.3^3 - 27.1^2 = -5.3^3 < 0$. Donc P a une seule racine réelle et deux racines complexes conjuguées non réelles.

d) L'extension $\mathbb{Q}(a+b)/\mathbb{Q}$ n'est pas galoisienne car $|\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(a+b))| = 1 < 3 = [\mathbb{Q}(a+b) : \mathbb{Q}]$.

Exercice 2 a) Comme $\mathbb{Z}$ est intégralement clos, une racine x dans $\mathbb{Q}$ est dans $\mathbb{Z}$ et divise 3. Or $\pm 3, \pm 1$ ne sont pas racines. Donc P n'a pas de racines dans $\mathbb{Q}$.

b) $P = (X+1)(X^2+X+1)(X^3+X+1) \bmod 2$ qui est séparable donc G contient $c\tau$ où c est un 3-cycle et τ une transposition à supports disjoints. On a $(c\tau)^3 = \tau \in G$.

c) $P(5) = 0 \bmod 11$. Comme $P = (X-5)Q \bmod 11$ avec Q irréductible $\bmod 11$, d'après le théorème de Dedekind, G contient un 5-cycle.

d) Soit $H \leq S_6$ un sous-groupe transitif avec un 5-cycle c et une transposition t. On peut supposer $c = (23456)$; Si $t = (ij)$, il existe $s \in H$ tel que $s(i) = 1$. Alors $t' := sts^{-1}$ est de la forme $(1k)$ avec $k \in \{2,3,4,5,6\}$. Mais alors $\{c^n t' c^{-n} \, : \, n \in \mathbb{Z}\} = \{(1j) \, : \, j = 2, ..., 6\}$ engendre S_6 donc $H = S_6$.
G vérifie les hypothèses et donc $G \simeq S_6$ (G est transitif car P est irréductible).

Exercice 3 a) $X^4+9 = (X - e^{i\pi/4}\sqrt{3})(X - e^{i3\pi/4}\sqrt{3})(X + e^{i\pi/4}\sqrt{3})(X + e^{i3\pi/4}\sqrt{3}) = (X^2 - \sqrt{6}X + 3)(X^2 + \sqrt{6}X + 3)$. Comme aucun de ces facteurs n'est dans $\mathbb{Q}[X]$, P est irréductible sur $\mathbb{Q}$. Soit $x \in \mathbb{C}$ une racine de P. Les autres sont : $-x$, $3/x$ et $-3/x$. Donc $\mathbb{Q}(x)$ est bien le corps de décomposition sur $\mathbb{Q}$ de P $\mathbb{Q}(x)/\mathbb{Q}$ est galoisienne. Le groupe de Galois est d'ordre 4 donc isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Si $s \in \mathrm{Gal}(\mathbb{Q}(x)/\mathbb{Q})$, alors $s(x) = -x, 3/x$, ou $-3/x$. Donc $s = 1$ ou est d'ordre 2. Donc $\mathrm{Gal}(\mathbb{Q}(x)/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
Les sous-groupes propres de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ sont $\mathbb{Z}/2\mathbb{Z} \times 0$, $0 \times \mathbb{Z}/2\mathbb{Z}$ et $\mathrm{diag}(\mathbb{Z}/2\mathbb{Z})$. Les corps intermédiaires correspondants sont $\mathbb{Q}(i), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(i\sqrt{3})$.

b) Par Eisenstein, $Q := X^4 - 2$ est irréductible sur $\mathbb{Q}$. Le corps de décomposition est $K = \mathbb{Q}(\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}) = \mathbb{Q}(i, \sqrt[4]{2})$. Le groupe de Galois G de Q sur $\mathbb{Q}$ est donc d'ordre 8. C'est aussi un sous-groupe de S_4. C'est donc un $2-$Sylow de S_4 forcément isomorphe à D_4 le groupe diédral d'ordre 8. Soit r un élément de $G := \mathrm{Gal}_{\mathbb{Q}}(Q)$ d'ordre 4 et s un élément d'ordre 2 qui n'est pas r^2. Alors $G = \langle r, s\rangle$ avec : $r^4 = s^2 = 1$ et $srs = r^{-1}$. Les sous-groupes propres distingués sont $\langle r\rangle, \langle s, r^2\rangle, \langle sr, r^2\rangle, \langle r^2\rangle$,. Voici les corps intermédiaires correspondants : $\mathbb{Q}(i)$,$\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i\sqrt{2})$, $\mathbb{Q}(i, \sqrt{2})$ qui sont des extensions galoisiennes sur $\mathbb{Q}$.

Exercice 4 a) Comme $\mathbb{C}$ est algébriquement clos, comme K est de caractéristique nulle, $\mathbb{C}/K$ est normale et séparable donc galoisienne. $[\mathbb{C} : K]$ est un nombre premier donc le groupe de Galois est cyclique.

b) Soit $z := e^{2i\pi/p} \in K$. Le degré de z sur $\mathbb{Q}$ donc sur K est $\leq p-1$. Or, $[K(z) : K] | p = [\mathbb{C} : K]$ donc $[K(z) : K] = 1$ et $z \in K$. D'après Kummer cela suffit pour dire que $K = K(\alpha)$ pour un α tel que $\alpha^p \in K$.

c) $N(\alpha)^p = N(\alpha^p) = N(a) = a^d$. Or $N(\alpha) \in k$. Donc $a^d \in k^p$. Comme d est premier à p avec une relation de Bézout : $du + vp = 1$, on trouve $a = a^{du+pv} = (a^d)^u (a^v)^p \in k^p$. Donc si $X^p - a$ est réductible sur k, il existe un élément α racine de $X^p - a$ de degré $< p$ et donc $X^p - a$ a une racine dans k : contraposée : si $X^p - a$ n'a pas de racines, alors $X^p - a$ est irréductible sur k.

d) Si $X^p - a = (X-\alpha_1)...(X-\alpha_p)$, alors $X^{p^2} - a = \prod_i (X^p - \alpha_i)$. $N_{K(\alpha_1)/K}(\alpha_1) = (-1)^p(-a) = a$ car p est impair. Si $x^p = \alpha_1$, avec $x \in K(\alpha_1)$, alors $(\underbrace{N_{K(\alpha_1)/K}(x)}_{\in K})^p = N_{K(\alpha_1)/K}(\alpha_1) = a$ absurde car $a \notin K^p$. Donc $X^p - \alpha_1$ est irréductible sur $K(\alpha_1)$. Soit $x \in \mathbb{C}$ une racine $p$ième de α_1. On a $p = [\mathbb{C} : K] \geq [K(\alpha_1, x) : K] = [K(\alpha_1)(x) : K(\alpha_1)][K(\alpha_1) : K] = p^2$ absurde.

Exercice 5 a) L'application est un antimorphisme car $\varphi_{AB} = \varphi_B \circ \varphi_A$. Le noyau est l'ensemble des matrices $a\mathrm{Id}$, $a \in \mathbb{F}_p^\times$; donc $|G| = |\mathrm{GL}_2(\mathbb{F}_p)|/|\mathbb{F}_p^\times| = p^3 - p$.

b) $f := \frac{(X^{p^2}-X)^{p+1}}{(X^p-X)^{p^2+1}} \in \mathbb{F}_p(X)^G$ car $f(X+1) = f(X)$, $f(aX) = f(X)$, $a \in \mathbb{F}_p^\times$, $f(1/X) = f(X)$.

c) $P := \prod_{x \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p} (X-x) = (X^{p^2}-X)/(X^p-X) \in \mathbb{F}_p[X]$ et $f = (PQ)^{p+1}/Q^{p^2+1} = P^{p+1}/Q^{p^2-p}$.

d) Soit $a := P^{p+1}$ et $b := Q^{p^2-p}$. On a : $a, b \in \mathbb{F}_p[X]$, $\deg a = p^3 - p$ et $\deg b = p^3 - p^2$. Le polynôme $b(T)f - a(T) \in \mathbb{F}_p(f)[T]$ annule X et est de degré $\leq p^3 - p = \max\{\deg a, \deg b\}$. Donc $[\mathbb{F}_p(X) : \mathbb{F}_p(f)] \leq p^3 - p$. Or $\mathbb{F}_p(f) \leq \mathbb{F}_p(X)^G \leq \mathbb{F}_p(X)$ et $[\mathbb{F}_p(X) : \mathbb{F}_p(X)^G] = |G| = p^3 - p$. Donc $\mathbb{F}_p(f) = \mathbb{F}_p(X)^G$.