# Corrigé rapide examen 2008

**Ce corrigé donne uniquement des indications pour certaines réponses. Elles sont donc incomplètes.**

1. Comme $f$ est un polynôme unitaire de degré 3 et à coéfficients entiers, il est irréductible ssi il n'a pas de racine dans $\mathbb{Z}$. Supposons que $x$ est un entier et racine de $f$. Alors $x^3 = a(x-1)$. Donc si $p$ est un diviseur premie de $x-1$, alors $p$ divise $x^3$ donc $x$. On en déduit que $x-1$ est égal à $-1$, 0 ou 1, c'est-à-dire $x = 0, 1$ ou 2. On vérifie facilement que 0 et 1 sont impossibles et que 2 n'est possible que si $a = 8$. D'où le résultat.

   Si $a = 8$ alors $f = (X-2)(X^2+2X-4)$ et il est facile de voir que $X^2+2X-4$ n'a pas de racine dans $\mathbb{Z}$ donc c'est la factorisation recherchée.

2. (a) $g(X) = f(X^2)$ donc les racines de $f$ sont l'ensembles des racines carrées de $u$, $v$ et $w$. D'où le résultat.

   (b) Pour cette question on fait les calculs en utilisant les relations coefficients/racines de $f$.

   (c) On montre que $h$ est séparable en vérifiant que $h$ et $h'$ sont premier entre-eux (on peut utiliser l'algorithme d'euclide). On en déduit que $h$ a 4 racines distinctes.

   Rappelons que la notation $\sqrt{u}$ désigne l'une des deux racines carrées de $u$. Si on choisit l'autre, c'est-à-dire $-\sqrt{u}$ on déduit de la question pécédente que $x_2 = u\sqrt{v}\sqrt{w} - v\sqrt{w}\sqrt{u} - w\sqrt{u}\sqrt{v}$ est également racine de $h$. De même $x_3 = -u\sqrt{v}\sqrt{w} + v\sqrt{w}\sqrt{u} - w\sqrt{u}\sqrt{v}$ et $x_4 = -u\sqrt{v}\sqrt{w} - v\sqrt{w}\sqrt{u} + w\sqrt{u}\sqrt{v}$ sont racines de $h$. On vérifie en suite que $x$, $x_2$, $x_3$, $x_4$ sont 4 nombres disctincts (on utilise pour cela que $u$, $v$ et $w$ sont distincts car $f$ est séparable ; à vérifier également.)

   Donc $x$, $x_2$, $x_3$, $x_4$ sont les 4 racines de $h$. (Remarque : ces racines ne sont pas nécessairement toutes conjuguées sur $\mathbb{Q}$, voir le cas $a = 4$ dans la question 5.)

   Remarquons que $uvw = -a$. donc $\sqrt{-a} \in L$. Notons de plus que $2u\sqrt{v}\sqrt{w} = x + x_1$. De ceci, on déduit que $\sqrt{u} \in K(\sqrt{-a})$. De même pour $\sqrt{v}$ et $\sqrt{w}$ d'où le résultat.

   (d) D'après ce qui précède $u\sqrt{v}\sqrt{w} \in K$, donc $u = (u^2vw)/(uvw)$ également.

3. (a) $h \mod 3 = X^4 + X + 1 = (X-1)(X^3 + X^2 + X - 1)$ et $X^3 + X^2 + X - 1$ et n'a pas de racine dans $\mathbb{F}_3$. C'est donc la factorisation recherchée.

   (b) Du fait de la factorisation de $h \mod 3$, si $h$ est réductible sur $\mathbb{Q}$ alors $h$ a une racine. On étudie alors la tableau de variation de la fonction polynomiale associée à $h$ et on vérifie que cette fonction est strictement positive si $a \geq 7$. Si $a = 1$, les seules racines rationnelles possibles de $h$ sont $\pm 1$, $\pm 2$, $\pm 4$. On vérifie que ce ne sont pas des racines et on conclut.

   (c) Comme $h$ est irréductible et de degré 4, on a $|\mathrm{Gal}_{\mathbb{Q}}(h)|$ est divisible par 4. Par a) et van der Waerden,

   Par le critère de van der Waerden, $\mathrm{Gal}_{\mathbb{Q}}(h)$ conteint un 3-cycle. Donc $|\mathrm{Gal}_{\mathbb{Q}}(h)|$ est divisible par 12. Il est donc isomorphe à un sous-groupe d'indice 2 de $S_4$. D'où le résultat.

4. (a) $h \mod 3 = X^4 + X - 1$. Supposons que $x \in \mathbb{F}_9$ est racine de $h$. Alors $x^8 = 1$ et $x^4 + x - 1 = 0$. D'où $1 = (x^4)^2 = (x-1)^2 = x^2 + x + 1$. Alors $x^2 + x = 0$, donc $x = 0$ ou 1, ce qui est impossible. Si $X^4 + X - 1$ était réductible sur $\mathbb{F}_3$, il aurait un facteur de degré au plus 2 et donc une racine dans $\mathbb{F}_9$. Il est donc irréductible. On en déduit que $h$ est également irréductible sur $\mathbb{Q}$. Par van der Waerden, $\mathrm{Gal}_{\mathbb{Q}}(h)$ contient un 4-cycle.

   (b) Si $a \neq 8$, $f$ est irréductible. Comme $K$ contient $u, v, w$ les racines de $f$, on en déduit que $[K : \mathbb{Q}]$ est divisible par 3. Conclusion $|\mathrm{Gal}_{\mathbb{Q}}(h)|$ est divisible par 3 et 4 donc par 12. De plus il contient un 4-cycle, donc il ne peut être isomorphe à $A_4$. Il est donc isomorphe à $S_4$.

   (c) Si $a = 8$, on a $h \mod 13 = X^4 + 8X + 7 = (X+1)(X-2)(X^2 + X + 3)$ avec $X^2 + X + 3$ qui n'a pas de racine dans $\mathbb{F}_{13}$. C'est donc la factorisation recherchée. Par van der Waerden, $\mathrm{Gal}_{\mathbb{Q}}(h)$ contient une transposition. De plus il contient un 4-cycle. On en déduit qu'il est isomorphe à $S_4$ (A EXPLICITER).

5. Si $a = 4$, $h = (X-4)(X^3+4X^2+16X-64)$. On remarque que $X^3+4X^2+16X-64$ n'a pas de racine rationnelle,en étudiant la fonction polynomiale associée. Celle-ci est trictement croissante, et s'annule dan s'intervalle $]2,3[$. Donc $X^3+4X^2+16X-64$ n'a aps de racine dans $\mathbb{Z}$, et comme il est unitaire et degré 3, il suit qu'il est irréductible sur $\mathbb{Q}$. Cette décomposition montrer que $\mathrm{Gal}_{\mathbb{Q}}(h) = \mathrm{Gal}_{\mathbb{Q}}(X^3+4X^2+16X-64)$. Ce groupe est donc isomorphe à un sous-groupe de $S_3$ et d'ordre au moins 3. De plus $X^3+4X^2+16X-64$ a une seule racine réelle et deux racines complexes conjuguées, donc $\mathrm{Gal}_{\mathbb{Q}}(h)$ contient une transposition. Ce groupe est donc isomorphe à $S_3$.
6. (a) Pour le calcul du discriminant voir la fiche de TD 4. On a $\Delta = 4^6a^8(4a-27)$. D'où $-a\Delta \mod 3 = -a^2 \mod 3 = -1$. Donc $-a\Delta$ n'est pas un carré dans $\mathbb{Z}$ (ni dans $\mathbb{Q}$.
   (b) Supposons que $K \cap \mathbb{Q}(\sqrt{-a}) \neq \mathbb{Q}$. Alors comme $[\mathbb{Q}(\sqrt{-a}) : \mathbb{Q}] = 2$, on a $K \cap \mathbb{Q}(\sqrt{-a}) = \mathbb{Q}(\sqrt{-a})$ et $\mathrm{Gal}_{\mathbb{Q}(\sqrt{-a})}(h)$ est un sous-groupe d'indice 2 de $\mathrm{Gal}_{\mathbb{Q}}(h)$. Alors $\mathrm{Gal}_{\mathbb{Q}(\sqrt{-a})}(h)$ est donc isomorphe à $A_4$ ou $A_3$, et $\mathrm{Gal}_{\mathbb{Q}}(h)$ isomorphe à $S_4$ ou $S_3$. De ce fait $\Delta$ est alors un carré dans $\mathbb{Q}(\sqrt{-a})$, mais pas dans $\mathbb{Q}$. Comme $\Delta \in \mathbb{Q}$, on déduit facilement alors que $\Delta = (y\sqrt{-a})^2$ avec $y \in \mathbb{Q}$. Ceci contredit le fait que $-a\Delta$ n'est pas un carré dans $\mathbb{Q}$.
7. Rappelons que $L$ est le corps des racines de $g$. Donc $L$ est une extension galoisienne de $\mathbb{Q}$. D'autre part $K$ est une sous-extension galoisienne sur $\mathbb{Q}$. Par la correspondance de Galois, il suit que $H$ est un sous-groupe distingué de $G$.De même $H'$ est un sous-groupe distingué de $G$.
   Soit $\sigma \in H \cap H'$. Alors $\sigma$ fixe $K$ et $\sqrt{-a}$ donc fixe $K(\sqrt{-a}) = L$.
   Par 6b, $\sqrt{-a} \notin K$, donc $\sqrt{-a}$ et $-\sqrt{-a}$ sont conjugués au-dessus de $K$. Soit $\sigma \in G$. Comme $\sqrt{-a}$ et $-\sqrt{-a}$ sont conjugués au-dessus de $K$, il existe $\tau \in H$ tel que $\sigma(\sqrt{-a}) = \tau(\sqrt{-a})$. D'où $\tau^{-1}\sigma\tau^{-1} \in H'$ et $\sigma \in HH'$.
8. Les propriétés ci-dessus caractérisent le fait que $G$ est isomorphe au produit direct $H \times H'$ et de plus, on alors $H$ isomorphe à $G/H'$ et $H'$ isomorphe $G/H$. Par la correspondance de Galois, $G/H'$ est isomorphe à $\mathrm{Gal}(\mathbb{Q}(\sqrt{-a})/\mathbb{Q})$ qui est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ et $G/H$ est isomorphe à $\mathrm{Gal}(K/\mathbb{Q}) = \mathrm{Gal}_{\mathbb{Q}}(h)$. Pour conclure, il suffit de reprendre les questions précédentes, en utilisant le fait que dans le cas où $\mathrm{Gal}_{\mathbb{Q}}(h)$ est isomorphe à un sous-groupe de $S_4$, alors $\Delta$ est un carré dans $\mathbb{Q}$ si et seulement si $\mathrm{Gal}_{\mathbb{Q}}(h)$ est isomorphe à un sous-groupe de $A_4$.