Université Rennes 1, Année 2012-2013
Master 1 Math., Algèbre générale de base

Exercices sur les extensions de corps, chapitre 6
indications de correction

Question supplémentaire à l'exercice 6.4

(3) Illustrons ce qui précède avec le cas $n = 3$, en supposant toujours k de caractéristique $\neq 2$.

(a) Démontrer que

- si $\Delta(f)$ est un carré dans k, alors $G(K/k) \simeq \mathfrak{A}_3$ et, pour tout $1 \leqslant i \leqslant 3$, $K = k(\alpha_i)$.
- si $\Delta(f)$ n'est pas un carré dans k, alors $G(K/k) \simeq \mathfrak{S}_3$ et, pour tout $1 \leqslant i \leqslant 3$, $K = k(\alpha_i, \delta(f))$.

(b) Montrer que, pour $p, q \in k$, on a $\Delta(X^3 + pX + q) = -4p^3 - 27q^2$.

(c) Déterminer K et $G(K/k)$ pour $f = X^3-2$ sur $k = \mathbb{Q}$ et $k = \mathbb{Q}(i\sqrt{3})$ et pour $f = X^3+X^2-2X-1$ sur $\mathbb{Q}$.

Corrigé.

(3) (a) Supposons que $\Delta(f)$ est un carré dans k. Alors d'après la question 2. (b), on a $G(K/k) \subset \mathfrak{A}_3$. Par ailleurs $K \neq k$ donc $|G(K/k)| = [K : k] > 1$. Comme le seul sous-groupe non trivial de $\mathfrak{A}_3 \simeq \mathbb{Z}/3\mathbb{Z}$ est $\mathfrak{A}_3$ lui-même, on trouve $G(K/k) \simeq \mathfrak{A}_3$. Dans ce cas on a donc $[K : k] = |G(K/k)| = 3$. Pour $i \in \{1, 2, 3\}$ quelconque, le polynôme minimal de α_i est f qui est de degré 3, de sorte que $[k(\alpha_i) : k] = 3$. Il s'ensuit que $K = k(\alpha_i)$.

Supposons maintenant que $\Delta(f)$ n'est pas un carré dans k. D'après 2. (b), le groupe $G(K/k)$ n'est pas inclus dans $\mathfrak{A}_3$. Par ailleurs $[K : k] \geq [k(\alpha_1) : k] = 3$ donc $|G(K/k)| \geq 3$. Le seul sous-groupe de $\mathfrak{S}_3$ qui n'est pas inclus dans $\mathfrak{A}_3$ et qui est de cardinal ≥ 3 est $\mathfrak{S}_3$, donc $G(K/k) \simeq \mathfrak{S}_3$. Enfin, pour $i \in \{1, 2, 3\}$ quelconque, posons $k' = k(\alpha_i, \delta(f))$. Le corps k' est une extension de $k(\alpha_i)$ qui est de degré 3 sur k, donc $[k' : k]$ est multiple de 3. Par ailleurs k' est une extension de $k(\delta(f))$ qui est de degré 2 sur k, donc $[k' : k]$ est multiple de 2. Comme $[k' : k] \leq [K : k] = 6$, la seule possibilité est que $k' = K$.

(b) Dans les calculs qui vont suivre, il est utile (même si ce n'est pas nécessaire à strictement parler) d'avoir à l'esprit le théorème fondamental des fonctions symétriques (TFFS). (Les dénominations « polynôme symétrique » et « TFPS » sont plus appropriées, mais l'usage du mot « fonction » est aussi assez fréquent dans ce contexte.) Rappelons brièvement que les fonctions symétriques élémentaires en n variables $T_1, \dots, T_n$ sont les polynômes σ_i tels que

$$(X - T_1) \dots (X - T_n) = X^n - \sigma_1(T_1, \dots, T_n)X^{n-1} + \sigma_2(T_1, \dots, T_n)X^{n-2} + \dots + (-1)^n\sigma_n(T_1, \dots, T_n).$$

On les obtient simplement en développant le produit. Par définition même des σ_i, si un polynôme $X^n + a_1X^{n-1} + a_2X^{n-2} + \dots + a_n$ a pour racines $\alpha_1, \dots, \alpha_n$, alors on a $a_i = (-1)^i\sigma_(\alpha_1, \dots, \alpha_n)$ pour tout i. Ces égalités s'appellent les *relations coefficients-racines*. Le TFFS dit que tout polynôme en plusieurs variables $T_1, \dots, T_n$ qui est symétrique en les T_i (c'est-à-dire qui reste inchangé par toute permutation des T_i) peut s'exprimer comme un polynôme en $\sigma_1, \dots, \sigma_n$.

En adoptant des notations plus simples pour les racines, on a :

$$X^3 + pX + q = (X - \alpha)(X - \beta)(X - \gamma) = X^3 - (\alpha + \beta + \gamma)X^2 + (\alpha\beta + \alpha\gamma + \beta\gamma)X - \alpha\beta\gamma.$$

On en déduit que $\alpha+\beta+\gamma=0$, $\alpha\beta+\alpha\gamma+\beta\gamma=p$ et $\alpha\beta\gamma=-q$. On peut utiliser la première relation pour éliminer γ ; il est alors pratique d'introduire la somme $S=\alpha+\beta$ et le produit $P=\alpha\beta$. Les trois relations ci-dessus deviennent : $\gamma=-S$, $P-S^2=p$ et $PS=q$.

Passons au calcul de $\Delta(f)=((\alpha-\beta)(\alpha-\gamma)(\beta-\gamma))^2$. On a :

$$(\alpha-\beta)^2=(\alpha+\beta)^2-4\alpha\beta=S^2-4P.$$

et

$$\big((\alpha-\gamma)(\beta-\gamma)\big)^2=\big((\alpha+S)(\beta+S)\big)^2=(P+2S^2)^2.$$

(N.B. on choisit d'effectuer le calcul de $\Delta(f)$ en séparant les facteurs comme cela pour préserver la symétrie en α et β, cf le commentaire préliminaire sur le TFFS.) En faisant le produit, il vient $\Delta(f)=(S^2-4P)(P+2S^2)^2$.

Par ailleurs $-4p^3-27q^2=4(S^2-P)^3-27P^2S^2$. Or on voit facilement qu'on a l'égalité de polynômes en X :

$$(X-4P)(P+2X)^2=4(X-P)^3-27P^2X$$

et en faisant $X=S^2$ on trouve $\Delta(f)=-4p^3-27q^2$.

(c) On applique les résultats des questions précédentes...