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

Exercices sur les extensions de corps, chapitre 5
indications de correction

Exercice 5.2

1) Comme σ est un automorphisme de corps qui vaut l'identité sur k, c'est en particulier un automorphisme de k-espaces vectoriels. De plus, comme G est d'ordre n on a $\sigma^n = \mathrm{id}$ si bien que le polynôme $X^n - 1$ annule l'endomorphisme σ.

2) Soit m le degré du polynôme minimal m_σ. Alors aucune combinaison linéaire des endomorphismes $\mathrm{id}, \sigma, k \ldots, \sigma^{m-1}$ n'est nulle, donc ceux-ci sont linéairement indépendants dans l'anneau $\mathrm{End}_k(K)$ des endomorphismes du k-espace vectoriel K. En particulier $\mathrm{id}, \sigma, k \ldots, \sigma^{m-1}$ vus comme caractères sont linéairement indépendants. Ceci n'est pas possible si $m \geq n$, d'après l'indépendance linéaire des caractères. Donc $\deg(m_\sigma) \geq n$ et finalement $m_\sigma = X^n - 1$.

3) L'énoncé exact de la question est : *montrer qu'il existe* $\alpha \in K$ *tel que* $\{\omega(\alpha) | \omega \in \langle\sigma\rangle\}$ *est une* k*-base de* K. Montrons ceci ; c'est une question difficile. Notons $A = k[X]$ l'anneau des polynômes qui est principal. Les polynômes irréductibles unitaires forment un système de représentants des irréductibles de A (pour la relation d'association). Pour tout P irréductible unitaire et tout $F \in A$, notons $v_P(F)$ la multiplicité de P dans la décomposition en facteurs irréductibles de F. Notons $X^n - 1 = P_1^{d_1} \ldots P_r^{d_r}$ la décomposition de $X^n - 1$, avec $d_j = v_{P_j}(X^n - 1) \geq 1$. Soit $e_1, \ldots, e_n$ une k-base de K. Considérons les idéaux suivants de A :

- l'annulateur de K comme k-module :

$$I = \{F \in k[X], F(\sigma) \text{ est le } k\text{-endomorphisme nul de } K\}.$$

  On a $I = (X^n - 1)$ par définition du polynôme minimal ;

- l'annulateur de l'élément $e_j \in K$:

$$I_i = \{F \in k[X], [F(\sigma)](e_i) = 0\}.$$

  Notons F_i un générateur unitaire de I_i (rappelons que $A = k[X]$ est principal).

Il est facile de voir que $I = I_1 \cap \cdots \cap I_n$, ce qui signifie que $X^n - 1$ est le ppcm de $F_1, \ldots, F_n$. Pour j fixé, on a alors $d_j = v_{P_j}(X^n - 1) = \max\{v_{P_j}(F_1), \ldots, v_{P_j}(F_n)\}$. Soit $i = i(j) \in \{1, \ldots, n\}$ un entier tel que $d_j = v_{P_j}(F_i)$; on a donc $F_i = P_j^{d_j} G_i$ avec G_i premier avec P_j.

Il reste du travail, mais tout est en place pour montrer que l'élément $\varepsilon_i := [G_i(\sigma)](e_i)$ a pour idéal annulateur l'idéal engendré par $P_j^{d_j}$, et que l'élément $\alpha := \varepsilon_1 + \cdots + \varepsilon_n$ a pour idéal annulateur l'idéal engendré par le produit des $P_j^{d_j}$, c'est-à-dire $X^n - 1$.

Ceci implique que si on a une k-combinaison linéaire nulle $a_0\alpha + a_1\sigma(\alpha) + \cdots + a_{n-1}\sigma^{n-1}(\alpha) = 0$, alors le polynôme $P = a_0 + a_1 X + \cdots + a_{n-1}X^{n-1}$ annule α donc est multiple de $X^n - 1$.

Pour des raisons de degré, on a alors $P = 0$. En conséquence la famille $\{\alpha, \sigma(\alpha), \ldots, \sigma^{n-1}(\alpha)\}$ est k-libre. Comme elle possède $n = [K : k]$ éléments c'est une k-base de K.

4) Comme toute extension finie $k \subset K$ de corps finis est galoisienne de groupe de Galois cyclique, engendré par l'automorphisme de Frobenius de k noté $F_k : K \to K$, $x \mapsto x^q$ où $q = \mathrm{card}(k)$, ce qui précède s'applique.

Exercice 5.6

Dans cet exercice, on étudie le corps $K = \mathbb{Q}(\sqrt[8]{2}, i)$. Dans l'exemple qui suit le corollaire 5.6 du polycopié de cours, les automorphismes de $K/\mathbb{Q}$ sont décrits et il est affirmé en particulier que les conditions $\sigma(\sqrt[8]{2}) = \xi\sqrt[8]{2}$ et $\sigma(i) = i$ définissent un automorphisme de K, où $\xi = \exp(2i\pi/8)$. Cette affirmation est vraie mais nécessite une justification, car définir des automorphismes de corps ne peut pas se faire n'importe comment, juste en envoyant certaines racines de polynômes sur d'autres racines des mêmes polynômes. Dans le cas présent, le fait que l'on puisse définir un automorphisme σ comme indiqué ci-dessus peut se justifier en montrant que le polynôme $P = X^8 - 2$ est irréductible sur $\mathbb{Q}(i)[X]$.

$$\therefore$$

[Le paragraphe suivant peut être sauté en première lecture, surtout pour préparer les contrôles.]

Voici un exemple semblable, dans lequel l'affirmation semblable sera tout aussi plausible, mais sera *fausse*. Considérons le polynôme $P = X^4+16 \in \mathbb{Q}[X]$. Montrons qu'il est irréductible sur $\mathbb{Q}$. Il est facile de voir que ce polynôme est sans racine dans $\mathbb{Q}$. Maintenant observons que l'on a, dans $\mathbb{R}[X]$ ou dans $\mathbb{Q}(\sqrt{2})[X]$:

$$P = (X^2+4)^2 - 8X^2 = (X^2 + 2\sqrt{2}X + 4)(X^2 - 2\sqrt{2}X + 4)$$

Les deux facteurs sont à discriminant strictement négatif, donc sans racine dans $\mathbb{R}$, donc irréductibles sur $\mathbb{R}$ ou sur $\mathbb{Q}(\sqrt{2})$. Supposons maintenant que $P = QR$ est produit de deux polynômes de degré 2 dans $\mathbb{Q}[X]$. Alors cette décomposition reste valable dans $\mathbb{R}[X]$, et par unicité de la décomposition en facteurs irréductibles dans $\mathbb{R}[X]$ on voit que Q et R doivent être les polynômes $X^2 + 2\sqrt{2}X + 4$ et $X^2 - 2\sqrt{2}X + 4$. Comme ces derniers ne sont pas dans $\mathbb{Q}[X]$, on a une contradiction. Donc finalement P est irréductible sur $\mathbb{Q}$.

Notons $\alpha \in \mathbb{C}$ une racine de P et posons $K = \mathbb{Q}(\alpha, i)$ et $k_1 = \mathbb{Q}(i)$. Il est clair sur la forme de P que $i\alpha$ est aussi racine de P. Considérons l'automorphisme $\sigma : K \to K$ défini par $\sigma(\alpha) = i\alpha$ et $\sigma(i) = i$. Tout a l'air parfait, comme dans l'exercice 5.6... *mais σ n'existe pas.* Le problème est que P ne reste pas irréductible sur $k_1 = \mathbb{Q}(i)$: en effet,

$$P = (X^2 - 4i)(X^2 + 4i).$$

Comme α est racine de P, il est racine d'un des facteurs $Q^\varepsilon = X^2 + 4\varepsilon i$, avec $\varepsilon \in \{\pm 1\}$. S'il existe un $\sigma : K \to K$ défini par les conditions ci-dessus, alors σ vaut l'identité sur k_1 si bien que $\sigma(\alpha)$ est encore racine de Q^ε. Comme la somme des racines de Q^ε vaut 0, on voit qu'il n'est pas possible d'avoir $\sigma(\alpha) = i\alpha$. Contradiction.

La morale de cet exemple est que pour définir un automorphisme d'une extension finie K/k, si l'on ne veut pas risquer de dire des bêtises il vaut mieux être soigneux. La méthode la plus sûre est d'exprimer K comme composée d'extensions « monogènes » de la forme $k \subset k'$ où k' possède une représentation comme anneau quotient $k' \simeq k[X]/(P)$, puis d'utiliser la propriété universelle des anneaux quotients, comme nous l'avons fait de nombreuses fois.

$\therefore$

Revenons à l'exercice. Si l'on veut justifier le fait que σ est bien défini par les conditions $\sigma(\sqrt[8]{2}) = \xi\sqrt[8]{2}$ et $\sigma(i) = i$, une manière de procéder est de montrer que $X^8 - 2$ est irréductible dans $k_1[X]$, puis que $K \simeq k_1[X]/(X^8-2)$, et on utilise alors la propriété universelle de quotient. Pour montrer que $X^8 - 2$ est irréductible sur k_1, on peut faire comme ceci. On observe d'abord que par le critère d'Eisenstein, le polynôme $X^8 - 2$ est irréductible sur $\mathbb{Q}$, de sorte que c'est le polynôme minimal de α sur $\mathbb{Q}$ et donc $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ est de degré 8. Ensuite, il est facile de voir que $X^2 + 1$ est irréductible sur $\mathbb{Q}(\alpha)$, car il n'a pas de racine dans ce corps. Ainsi $[K : \mathbb{Q}(\alpha)] = 2$ et finalement $[K : \mathbb{Q}] = 16$. On en déduit que $[K : \mathbb{Q}(i)] = 8$. Alors α est de degré 8 sur $\mathbb{Q}(i)$, annulé par le polynôme $X^8 - 2$, donc ce polynôme est le polynôme minimal de α et il est irréductible. Passons aux trois groupes de Galois demandés.

1) Cas de $G(K/k_1)$. Notons $\alpha = \sqrt[8]{2}$ et $\xi = \exp(2i\pi/8)$. Étant donné que $\alpha^4 = \sqrt{2}$, on a $\xi = \frac{1+i}{\sqrt{2}} = \frac{1+i}{\alpha^4} \in K$. On vérifie que les conditions $\sigma(\alpha) = \xi\alpha$ et $\sigma(i) = i$ définissent bien un k_1-automorphisme $\sigma : K \to K$. Il est clair que σ est d'ordre 8. Par ailleurs, de la présentation $K \simeq k_1[X]/(X^8-2)$ on déduit que $[K : k_1] = 8$. Notons $H \subset G(K/k_1)$ le sous-groupe engendré par σ, il est cyclique d'ordre 8. Ainsi G est d'ordre au moins 8 car il contient H, et d'ordre au plus $[K : k_1] = 8$, donc finalement $G(K/k_1)$ est d'ordre 8, égal à H.

2) Cas de $G(K/k_2)$. Posons $\beta = \sqrt{2}$, on a donc $\alpha = \sqrt[4]{\beta}$. Considérons la composée d'extensions $k_2 \subset k_2(\alpha) \subset k_2(\alpha, i) = K$. Regardons d'abord $k_2 \subset k_2(\alpha)$. On peut voir de deux manières (au moins) que le polynôme $X^4 - \beta$ est irréductible sur k_2. Première manière : en utilisant le critère d'Eisenstein pour l'anneau $\mathbb{Z}[\sqrt{2}]$ qui est factoriel (en fait principal), et en montrant (c'est facile) que β est irréductible. Deuxième manière : directement, en utilisant l'automorphisme de conjugaison de $\mathbb{Q}(\sqrt{2})$ qui envoie $z = a + b\sqrt{2}$ sur $\overline{z} = a - b\sqrt{2}$: en effet, si $P = X^4 - \beta$ est un produit QR, alors en conjuguant on trouve $\overline{P} = X^4 - \beta = \overline{Q}\,\overline{R}$ donc $X^8 - 2 = P\overline{P} = (Q\overline{Q})\,(R\overline{R})$ avec $Q\overline{Q} \in \mathbb{Q}[X]$ et $R\overline{R} \in \mathbb{Q}[X]$, ce qui contredit le fait (facile) que $X^8 - 2$ est irréductible sur $\mathbb{Q}$. Regardons ensuite $k_2(\alpha) \subset k_2(\alpha, i)$. Celle-ci est plus simple, car $X^2 + 1$ n'a pas de racine dans $k_2(\alpha)$ (qui est inclus dans $\mathbb{R}$) donc est irréductible sur $k_2(\alpha)$. En conclusion $k_2(\alpha) \simeq k_2[X]/(X^4 - \beta)$, $K = k_2(\alpha, i) = k_2(\alpha)[Y]/(Y^2 + 1)$ et

$$K = k_2(\alpha, i) \simeq \frac{k_2[X, Y]}{(X^4 - \beta, Y^2 + 1)}.$$

À l'aide de ceci, on peut justifier que l'on définit bien des k_2-automorphismes u, v de K par les conditions : $u(\alpha) = i\alpha$, $u(i) = i$, et $v(\alpha) = \alpha$, $v(i) = -i$. On montre alors que u est d'ordre 4, v est d'ordre 2, ils engendrent un groupe d'ordre 8. Comme le degré $[K : k_2]$ est égal à 8, les automorphismes u et v engendrent $G(K/k_2)$. On n'a pas de mal à vérifier que ce groupe est le groupe diédral $\mathbb{D}_4$ à 8 éléments, en voyant qu'il est non abélien et (pour le distinguer du groupe des quaternions) soit qu'il possède au moins deux éléments d'ordre 2, soit que son centre est trivial.

3) Cas de $G(K/k_3)$. Posons $\gamma = \sqrt{-2} = i\beta = i\alpha^4$. Alors on vérifie que

$$K = k_3(i, \alpha) = \frac{k_3[X, Y]}{(X^2 + 1, Y^4 + \gamma X)}.$$

Rappelons que le groupe des quaternions Q_8, aussi noté $\mathbb{H}_8$, peut être décrit comme le groupe à 8 éléments notés $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ où la table de multiplication est celle de l'algèbre $\mathbb{H}$ des quaternions ; c'est donc le sous-groupe de $\mathbb{H}^\times$ formé des quaternions de norme 1 à coefficients dans $\mathbb{Z}$. On va définir des automorphismes I, J, K de K/k_3 (la notation est faite pour rappeler les i, j, k des quaternions, pour faciliter la preuve du fait que $G(K/k_3)$ est le groupe des quaternions). Notons tout d'abord que σ, τ définis comme ci-dessus par $\sigma(\alpha) = \xi\alpha$, $\sigma(i) = i$ et $\tau(\alpha) = \alpha$, $\tau(i) = -i$ ne fixent pas γ (vérification facile), donc ne définissent pas des k_3-automorphismes. On définit donc I par $I = \sigma^2$ c'est-à-dire $I(\alpha) = i\alpha$ et $I(i) = i$, et J par $J = \tau\sigma$ c'est-à-dire $J(\alpha) = \xi\alpha$ et $J(i) = -i$. On pose $K = IJ$, on vérifie que $I^2 = J^2 = K^2$ qui est égal à l'automorphisme que l'on note $[-1]$ (ici encore, pour rappeler les quaternions) et qui vérifie $[-1](\alpha) = -\alpha$ et $[-1](i) = i$. On observe ensuite que I est d'ordre 4 ; J n'appartient pas au sous-groupe d'ordre 4 engendré par I ; comme $[K : k_3] = 8$, le sous-groupe engendré par I et J est alors nécessairement d'ordre 8. On montre qu'il est non abélien et (pour le distinguer du groupe diédral) soit qu'il contient un seul élément d'ordre 2, soit que son centre est non trivial, contenant $[-1]$. On conclut que $G(K/k_3)$ est isomorphe au groupe de quaternions Q_8 aussi noté $\mathbb{H}_8$.