

Extensions de corps II : correction

Exercice 1.

1. Tous les éléments de K^a sont algébriques sur K et donc *a fortiori* algébriques sur L . L'extension K^a/L est donc algébrique. En outre, K^a est algébriquement clos. L'extension K^a/L est donc bien une clôture algébrique de L .
2. Montrons par récurrence sur d que tout élément de $K(\alpha_1, \dots, \alpha_d)$ s'écrit comme un polynôme (à coefficients dans K) en α_i , c'est-à-dire est dans la K -algèbre engendrée $K[\alpha_1, \dots, \alpha_d]$.

Si $d = 1$, $K[\alpha] \subset L$ est isomorphe à $K[X]/(\mu_K^\alpha)$ (α est nécessairement algébrique car L/K est finie). Mais les idéaux premiers non nuls de $K[X]$ (principal) sont maximaux, donc cette algèbre (intégrale car sous-algèbre d'un corps) est un corps. On a donc bien $K[\alpha] = K(\alpha)$.

Supposons maintenant le résultat démontré pour $1, \dots, d-1$ et soit $L = K(\alpha_1, \dots, \alpha_d) = M(\alpha_d)$, où $M = K(\alpha_1, \dots, \alpha_{d-1})$. Par hypothèse de récurrence, tout élément β de L est un polynôme (à coefficients dans M , lesquels sont des polynômes P_i (à coefficients dans K) en $\alpha_1, \dots, \alpha_{d-1}$) de α_d . On a donc une écriture

$$\beta = \sum_i P_i(\alpha_1, \dots, \alpha_{d-1}) \alpha_d^i = P(\alpha_1, \dots, \alpha_d),$$

où $P(X_1, \dots, X_d) = \sum_i P_i(X_1, \dots, X_{d-1}) X_d^i \in K[X]$.

3. Soit $\gamma \in L$; il est algébrique sur K par hypothèse. Puisque f est un morphisme de corps K -linéaire, on a $\mu_K^\gamma(f(\gamma)) = f(\mu_K^\gamma(\gamma)) = 0$. L'automorphisme f préserve donc la sous-extension $K \subset M_\gamma \subset L$ engendrée par les racines de μ_K^γ .
Pour tout $\gamma \in L$, on a donc vu que f induisait un morphisme $M_\gamma \rightarrow M_\gamma$, où M_γ/K est la sous-extension de L engendrée par les racines du μ_K^γ . Ce morphisme K -linéaire entre deux K -espaces vectoriels de dimension finie est injectif (c'est un morphisme de corps!), donc surjectif. Le morphisme f est donc bien bijectif, ce qui en fait un automorphisme K -linéaire de L .
4. Soit $\alpha_1, \dots, \alpha_d$ des éléments de L tels que $L = K(\alpha_1, \dots, \alpha_d)$. Si f est un automorphisme K -linéaire de L , on a forcément $\mu_K^{\alpha_i}(f(\alpha_i)) = f(\mu_K^{\alpha_i}(\alpha_i)) = 0$: l'automorphisme f envoie forcément α_i sur un élément de l'ensemble $V(\mu_K^{\alpha_i})$ des racines du polynôme minimal de α_i . Comme en outre $L = K(\alpha_1, \dots, \alpha_d)$, l'automorphisme est entièrement déterminé par ses valeurs en α_i . On a donc une injection

$$\begin{array}{ccc} \text{Aut}(L/K) & \rightarrow & \prod_{i=1}^d V(\mu_K^{\alpha_i}) \\ f & \mapsto & (f(\alpha_1), \dots, f(\alpha_d)) \end{array}$$

et $\text{Aut}(L/K)$ est fini.

Exercice 2.

1. Soit L/K une extension de degré 2 et $Q \in K[X]$ irréductible ayant une racine α dans L . Par un argument de dimension, $K(\alpha) = L$, qui est donc un corps de rupture de K . On a donc $\deg Q = 2$ et, comme Q est divisible par $X - \alpha$, il est bien scindé dans L .

Le critère d'Eisenstein montre que $X^4 - 2$ est irréductible sur $\mathbf{Z}$ et donc sur $\mathbf{Q}$. Il a bien une racine dans $\mathbf{Q}(\sqrt[4]{2})$, à savoir $\sqrt[4]{2}$. Il n'y est pourtant pas scindé : les racines de $X^4 - 2$ sont $\pm\sqrt[4]{2}$ et $\pm i\sqrt[4]{2}$, et ces dernières, non réelles, ne sont pas dans $\mathbf{Q}(\sqrt[4]{2})$. L'extension $\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}$ n'est donc pas normale.

L'extension $\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}$ est un corps de rupture de $X^4 - 2$: c'est une $\mathbf{Q}$ -algèbre isomorphe à $\mathbf{Q}[X]/(X^4 - 2)$. Les morphismes dans $\mathbf{C}$ sont donc uniquement déterminés par un élément $\alpha \in \mathbf{C}$ (l'image de $\sqrt[4]{2}$) tel que $\alpha^4 = 2$. Il y en a donc 4 dont 2 sont des isomorphismes de $\mathbf{Q}(\sqrt[4]{2})$ ($\sqrt[4]{2} \mapsto \pm\sqrt[4]{2}$) et 2 n'en sont pas ($\sqrt[4]{2} \mapsto \pm i\sqrt[4]{2}$, dont l'image n'est pas réelle). Les extensions $\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}(\sqrt{2})$ et $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$ sont de degré 2 (ce sont les corps de rupture de $X^2 - \sqrt{2} \in \mathbf{Q}(\sqrt{2})[X]$ et $X^2 - 2 \in \mathbf{Q}[X]$, respectivement) et donc normales ; pourtant, on a vu que $\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}$ ne l'était pas. Cela donne un exemple du type cherché.

2. (a) $L = K(\alpha_1, \dots, \alpha_d)$. D'après la deuxième question, tout élément de L , par exemple β , s'écrit $R(\alpha_1, \dots, \alpha_d)$ pour un certain $R \in K[X_1, \dots, X_n]$. Le polynôme

$$\tilde{S}(X, X_1, \dots, X_d) = \prod_{\sigma \in \mathfrak{S}_d} (X - R(X_{\sigma(1)}, \dots, X_{\sigma(d)})) \in K[X, X_1, \dots, X_d]$$

est symétrique en les X_i . Il s'écrit donc

$$\tilde{S}(X, X_1, \dots, X_d) = \sum_{i=0}^{d!} S_i(X_1, \dots, X_d) X^i,$$

où tous les $S_i(X_1, \dots, X_d) \in K[X_1, \dots, X_d]$ sont des polynômes symétriques. On peut les exprimer chacun en fonction des polynômes symétriques élémentaires

$$\Sigma_i^{(d)} = \Sigma_i^{(d)}(X_1, \dots, X_d) \in K[X_1, \dots, X_d],$$

ce qui donne

$$\tilde{S}(X, X_1, \dots, X_d) = \sum_{i=0}^{d!} P_i(\Sigma_1^{(d)}, \dots, \Sigma_d^{(d)}),$$

pour une certaine famille P_i d'éléments de $K[T_1, \dots, T_n]$. En spécialisant en $X_i = \alpha_i$, on obtient

$$S(X) = \sum_{i=0}^{d!} P_i(\Sigma_1^{(d)}(\alpha_1, \dots, \alpha_d), \dots, \Sigma_d^{(d)}(\alpha_1, \dots, \alpha_d)).$$

Mais les $\Sigma_i^{(d)}(\alpha_1, \dots, \alpha_d)$ sont, au signe près, les coefficients de P : ils sont donc dans K . On a bien obtenu $S \in K[X]$.

- (b) Puisque Q est irréductible, il est à une constante près le polynôme minimal de β : $\exists v \in K^\times : Q = v\mu_K^\beta$. Mais le polynôme $S \in K[X]$ annule également β . Il vient que Q divise S sur K et donc aussi sur L . Puisque S y est scindé, il doit en être autant de Q . On a bien vérifié que tout polynôme irréductible sur K et admettant une racine sur L y est scindé, c'est-à-dire que L/K est normale.

3. Commençons par démontrer que si $f : L \rightarrow K^a$ est un morphisme de corps K -linéaire, alors $f(L) \subset L$. Soit $\gamma \in L$; il est algébrique sur K par hypothèse. Puisque f est un morphisme de corps K -linéaire, on a $\mu_K^\gamma(f(\gamma)) = f(\mu_K^\gamma(\gamma)) = 0$. Mais μ_K^γ est irréductible sur K et admet une racine dans L . Par normalité, toutes ses racines, y compris $f(\gamma)$, sont donc dans L . On peut donc voir f comme un morphisme K -linéaire de L dans L , et la question 3 de l'exercice 1 entraîne que c'en est un automorphisme.

Exercice 3.

1. Soit $a \in S_K$ et $x \in K$ tel que $x^p - x = a$. Les éléments $(x + i)_{i \in \mathbf{F}_p}$ sont tous différents et tous vérifient $y^p - y = a$. On a donc

$$X^p - X - a = \prod_{i \in \mathbf{F}_p} (X - (x + i))$$

et le polynôme $X^p - X - a$ est scindé sur K .

2. Que le polynôme se scinde de cette façon dans un corps de rupture provient de la même preuve que précédemment. En particulier, pour ce polynôme, corps de décomposition et corps de rupture coïncident.

Soit L un corps de décomposition de $X^p - X - a$ et $x \in L$ une racine. Si ce polynôme n'était pas irréductible sur K , un facteur irréductible s'écrirait

$$\prod_{i \in I} (X - (x + i)),$$

pour un certain $I \subset \mathbf{F}_p$ de cardinal $d \notin \{0, p\}$. Mais le coefficient en X^{d-1} de ce polynôme est $-(dx + \sum_{i \in I} i)$: s'il était dans K , dx le serait aussi et, comme d est inversible modulo p , on aurait également $x \in K$, ce qui apporterait $x^p - x = a$ et une contradiction. Le polynôme $X^p - X - a$ est donc irréductible sur K .

Il reste à déterminer le groupe des automorphismes du corps de rupture L/K de ce polynôme. Fixons $\beta \in L$ une racine de $X^p - X - a$. L est le corps de rupture de $X^p - X - a$: les automorphismes de L sont donc déterminées par l'image de β , qui doit être une racine de $X^p - X - a$ (donc de la forme $\beta + i$ pour un certain élément $i \in \mathbf{F}_p$) et peut être n'importe laquelle. On a donc une bijection $\varphi : \text{Aut}(L/K) \rightarrow \mathbf{F}_p$ (ici, $\mathbf{F}_p$ est simplement le groupe additif) telle que f envoie β sur $\beta + \varphi(f)$. En outre, la composée $g \circ f$ envoie β sur $g(\beta + \varphi(f)) = g(\beta) + \varphi(f) = g(\beta) + \varphi(g) + \varphi(f)$, la première égalité étant justifiée par le fait que g est un morphisme de corps K -linéaire, donc en particulier $\mathbf{F}_p$ -linéaire. On a donc bien $\varphi(g \circ f) = \varphi(g) + \varphi(f)$, et φ est un isomorphisme de groupes $\text{Aut}(L/K) \rightarrow \mathbf{F}_p$.

Exercice 4. Soit L un corps de décomposition de $P(X) = X^{p^m} - a$ et $\beta \in L$ une racine. On a alors $P(X) = X^{p^m} - \beta^{p^m} = (X - \beta)^{p^m}$. Si le polynôme P était réductible, ses facteurs irréductibles seraient nécessairement de la forme $(X - \beta)^n$: il s'agit de montrer qu'aucun de ces polynômes n'est dans $K[X]$ pour $1 < n < p^m$. Écrivons $n = p^r s$, avec s non divisible par p . On a alors $P(X) = (X^{p^r} - \beta^{p^r})^s$. Le coefficient en $X^{p^r(s-1)}$ de ce polynôme est $-s\beta^{p^r}$. S'il était dans K , il en irait de même de β^{p^r} (car s est inversible modulo p). On aurait alors $a = \beta^{p^m} = (\beta^{p^r})^{p^{m-r}}$, qui serait une puissance p -ième d'un élément de K (car $m > r$), ce qui est exclu.

Exercice 5.

1. L'extension $\mathbf{Q}(\sqrt{p}, \sqrt{q})/\mathbf{Q}$ est le corps de décomposition de $(X^2 - p)(X^2 - q)$. À ce titre, elle est normale.
2. Comme on l'a vu précédemment, un automorphisme de $\mathbf{Q}(\sqrt{p}, \sqrt{q})$ doit envoyer $\sqrt{p}$ sur une racine de son polynôme minimal, à savoir $\pm\sqrt{p}$. De même, il doit envoyer $\sqrt{q}$ sur $\pm\sqrt{q}$. En outre, un automorphisme est entièrement déterminé par l'image de ces éléments. On a donc au plus quatre isomorphismes de $\mathbf{Q}(\sqrt{p}, \sqrt{q})/\mathbf{Q}$.

Ces quatre choix sont possibles : $\mathbf{Q}(\sqrt{p}, \sqrt{q})$ est le corps de rupture de $X^2 - p$ sur $\mathbf{Q}(\sqrt{q})$. Il y a donc deux morphismes $\mathbf{Q}(\sqrt{q})$ -linéaires $\mathbf{Q}(\sqrt{p}, q) \rightarrow \mathbf{C}$ envoyant $\sqrt{p}$ sur

$\pm\sqrt{p}$. Par normalité, ces morphismes sont des automorphismes de $\mathbf{Q}(\sqrt{p}, \sqrt{q})$. L'un des deux est l'identité et l'autre envoie $\sqrt{p}$ sur $-\sqrt{p}$ et fixe $\sqrt{q}$. On construit de même un automorphisme fixant $\sqrt{p}$ et envoyant $\sqrt{q}$ sur $-\sqrt{q}$. Leur composition envoie alors $\sqrt{p}$ et $\sqrt{q}$ sur leurs opposés.

Le groupe des automorphismes $\text{Aut}(\mathbf{Q}(\sqrt{p}, \sqrt{q})/\mathbf{Q})$ a donc exactement quatre éléments. Il est immédiat de voir qu'il est isomorphe à la *Viergruppe* de Klein $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

Exercice 6.

1. On a vu lors du premier exercice du TD 0 qu'un automorphisme de $\mathbf{C}$ envoyant $\mathbf{R}$ sur $\mathbf{R}$ était nécessairement l'identité ou la conjugaison complexe. Si f est un automorphisme sauvage, il existe donc $r \in \mathbf{R}$ tel que $f(r) \notin \mathbf{R}$. L'image $f(\mathbf{R})$ contient donc

$$f\left(\left\{ar + b \mid a, b \in \mathbf{Q}\right\}\right) = \left\{af(r) + b \mid a, b \in \mathbf{Q}\right\},$$

qui est dense dans $\mathbf{C}$ (1 et $f(r)$ forment une $\mathbf{R}$ -base de $\mathbf{C}$, et il suffit d'approcher les coefficients d'un élément de $\mathbf{C}$ dans cette base par des rationnels).

2. L'ensemble $\mathcal{F}$ contient (K, f) et est donc non vide.
3. Les axiomes d'ordre se vérifient immédiatement. Si $(K_\lambda, f_\lambda)_{\lambda \in \Lambda}$ est une famille totalement ordonnée, on pose $K = \bigcup_{\lambda \in \Lambda} K_\lambda$. Si $x \in K$, on pose $f(x) = f_\lambda(x)$ pour un $\lambda \in \Lambda$ tel que $x \in K_\lambda$. Puisque la famille est totalement ordonnée, cette fonction est bien définie. On a donc pour tout $\lambda \in \Lambda$, $(K_\lambda, f_\lambda) \prec (K, f)$: la famille a un majorant.

On peut alors appliquer le lemme de Zorn : $\mathcal{F}$ a un élément maximal, que rien n'empêche d'appeler $(\tilde{K}, \tilde{f})$.

4. Supposons α algébrique sur $\tilde{K}$. La clôture algébrique $\tilde{K}^a$ de $\tilde{K}$ est donc strictement plus grande que $\tilde{K}$. Le résultat suivant est une autre conséquence du lemme de Zorn. Pour répondre à la question, il suffit de l'appliquer au cas $F = G = \tilde{K}$.

Lemme. Soit $\varphi : F \rightarrow G$ un isomorphisme de corps. Alors φ s'étend en un isomorphisme $\tilde{\varphi} : F^a \rightarrow G^a$ entre les clôtures algébriques.

Si α est transcendant, on sait que l'évaluation $\varphi = \text{év}_\alpha : \tilde{K}(X) \rightarrow \tilde{K}(\alpha)$ est un isomorphisme de corps et de $\tilde{K}$ -algèbres. Or, tout automorphisme g de $\tilde{K}$ se prolonge en un unique isomorphisme g' de $\tilde{K}(X)$ envoyant X sur X . Cela permet d'étendre tout automorphisme de $\tilde{K}$, en particulier f , en un automorphisme de $\tilde{K}(\alpha)$.

5. La question précédente montre que l'existence de $\alpha \in \mathbf{C} \setminus \tilde{K}$ contredit la maximalité de $\tilde{K}$. L'hypothèse $\tilde{K} \subsetneq \mathbf{C}$ est donc absurde et $\tilde{K} = \mathbf{C}$: on a prolongé notre automorphisme en un automorphisme de $\mathbf{C}$!
6. On peut par exemple voir qu'il existe un (unique) $\mathbf{Q}$ -automorphisme de $\mathbf{Q}(\sqrt{2})$ envoyant $\sqrt{2}$ sur $-\sqrt{2}$.

Preuve du lemme. Soit $\mathcal{F}$ l'ensemble des isomorphismes $\psi : K \rightarrow L$, avec $K \subset F^a$ et $L \subset G^a$ qui prolongent $\varphi : F \rightarrow G$ (c'est-à-dire que $F \subset K$, $G \subset L$ et $\psi|_F = \varphi$). Cet ensemble est ordonné par la relation de prolongement $\prec$. Exactement comme précédemment, $\mathcal{F}$ est non vide et l'on montre que toute famille totalement ordonnée admet un majorant. D'après le lemme de Zorn, il existe donc un prolongement maximal $\tilde{\varphi} : \tilde{F} \rightarrow \tilde{G}$.

Si ce prolongement n'était pas un isomorphisme $F^a \rightarrow G^a$, l'un des deux corps en présence (et donc les deux, puisqu'ils sont isomorphes) ne serait pas algébriquement clos. Soit donc $P(X) = \sum_{i=1}^d p_i X^i \in \tilde{F}[X]$ un polynôme irréductible. Le polynôme « image » $\tilde{\varphi}_* P(X) = \sum_{i=1}^d \varphi(p_i) X^i$ serait alors un irréductible de $\tilde{G}[X]$.

Si $\alpha \in \tilde{F}^a$ est une racine de P , le corps $\tilde{F}(\alpha)$ est un corps de rupture de P : il est isomorphe à $\tilde{F}[X]/(P(X))$. Cela montre facilement qu'il existe un morphisme d'anneaux (et donc de corps) bien défini

$$\begin{array}{ccc} \tilde{F}(\alpha) & \rightarrow & \tilde{G}(\beta) \\ \hat{\varphi}: Q(\alpha) = \sum_{i=1}^r f_i \alpha^i \ (f_i \in \tilde{F}) & \mapsto & \varphi_* Q(\sum_{i=1}^r \varphi(f_i) \beta^i), \end{array}$$

où $\beta \in \tilde{G}^a$ est une racine de $\varphi_* P(X)$. On a donc prolongé l'isomorphisme $\tilde{\varphi} : \tilde{F} \rightarrow \tilde{G}$ en un isomorphisme $\hat{\varphi} : \tilde{F}(\alpha) \rightarrow \tilde{G}(\beta)$. Cela contredit la maximalité de $\tilde{\varphi}$ et constitue donc une contradiction.

On avait donc $\tilde{F} = F^a$ et $\tilde{G} = G^a$, ce qui démontre le lemme.