DM n°2

Exercice 1. 1. Si $a_i^{m_i} \in K$ et $x = \sum_{i=1}^{l} a_i$, alors les a_i sont algébriques sur K, donc x aussi, donc si tout élément de L est exprimable directement par radicaux sur K alors L est algébrique de K.

2. Si L/K est un extension quadratique de caractéristique différente de 2, alors d'après la classification des extensions quadratiques (TD7 Exercice 4), il existe $\alpha \in L \setminus K$ tel que $L = K(\alpha)$ et $\alpha^2 \in K$. Donc tout élément de L est de la forme $a + b\alpha$ avec $a, b \in K$, donc est exprimable directement par radicaux sur K.

3. (a) On a $\zeta_n^n = 1$, donc ζ_n est algébrique sur $\mathbb{Q}$, et tout élément de $\mathbb{Q}(\zeta_n)$ est un polynôme en ζ_n. Or les puissances de ζ_n sont exprimable directement par radicaux sur $\mathbb{Q}$, donc par additivité, tout élément de $\mathbb{Q}(\zeta_n)$ est exprimable directement par radicaux sur $\mathbb{Q}$.

   (b) L'extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est séparable car elle est de caractéristique 0. D'autre part, le corps $\mathbb{Q}(\zeta_n)$ est le corps de décomposition du polynôme $X^n - 1 \in \mathbb{Q}[X]$, car le polynôme est scindé et l'extension est engendré par les racines. Donc l'extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est normale, donc galoisienne.

   (c) On veut définir un automorphisme de $\mathbb{Q}(\zeta_n)$ qui envoie ζ_n sur ζ_n^a. L'unicité d'un tel automorphisme vient du fait que l'extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est monogène, et il reste à montrer l'existence. Il n'est pas difficile de voir que $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_n^a)$, et pour pouvoir définir le morphisme, il nous reste à montrer que les deux nombres ζ_n et ζ_n^a ont le même polynôme minimal sur $\mathbb{Q}$. Quitte à itérer l'argument, on peut supposer que $a = p$ est un nombre premier ne divisant pas n.

   Soit P (respectivement Q) le polynôme minimal (unitaire) de ζ_n (respectivement ζ_n^a) sur $\mathbb{Q}$. On sait que P et Q divisent $X^n - 1$ dans $\mathbb{Q}[X]$, donc par le lemme de Gauss, ces deux polynômes sont dans $\mathbb{Z}[X]$. Supposons par l'absurde que $P \neq Q$. Et alors P et Q sont premiers entre eux, et on peut écrire $X^n - 1 = PQR$ dans $\mathbb{Z}[X]$. En réduisant modulo p, on obtient

   $$X^n - 1 = \bar{P}\bar{Q}\bar{R} \tag{1}$$

   dans $\mathbb{F}_p[X]$. Comme p est premier avec n, on sait que le polynôme $X^n - 1$ est séparable dans $\mathbb{F}_p[X]$, donc $\bar{P}$ et $\bar{Q}$ sont premiers entre eux. Comme P et Q sont unitaires, leurs réductions modulo p sont non constantes. D'autre part, comme ζ_n^p est une racine de Q, on sait que $P(X)|Q(X^p)$ dans $\mathbb{Q}[X]$. Ecrivons $Q(X^p) = P(X)S(X)$, comme P et Q sont unitaires, par le lemme de Gauss, on sait que $S(X) \in \mathbb{Z}[X]$. En réduisant modulo p et en utilisant le fait que $\bar{Q}(X^p) = (\bar{Q}(X))^p$ dans $\mathbb{F}_p[X]$, on obtient

   $$(\bar{Q}(X))^p = \bar{P}(X)\bar{S}(X) \tag{2}$$

   dans $\mathbb{F}_p[X]$. Donc tout facteur irréductible de $\bar{P}(X)$ divise $\bar{Q}(X)$, contradiction.

   Finalement, le morphisme σ_a est obtenu par la composition

   $$\mathbb{Q}(\zeta_n) \simeq \mathbb{Q}[X]/(P) \simeq \mathbb{Q}(\zeta_n^a),$$

   qui envoir ζ_n sur ζ_n^a.

   (d) Comme $\sigma_a(\zeta_n) = \zeta_n^a$, par la question précédente on obtient $\sigma_b \circ \sigma_a = \sigma_{ab}$, et on en déduit que l'application $a \mapsto \sigma_a$ est un morphisme de groupes, qui est injectif par définition. Pour la surjectivité, soit $\sigma \in Aut(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Comme l'extension est monogène, σ est entièrement déterminér par $\sigma(\zeta_n)$. Comme $\zeta_n^n = 1$, $\sigma(\zeta_n)$ est une racine n-ième de l'unité, et comme ζ_n est d'ordre n dans $(\mathbb{Q}(\zeta_n))^*$, $\sigma(\zeta_n)$ aussi, donc $\sigma(\zeta_n) = \zeta_n^a$ avec a premier avec n, d'où la surjectivité.

4. (a) Par hypothèse, pour tout $x, y \in L$, on a

$$c_1\chi_1(xy) + \cdots + c_m\chi_m(xy) = 0,$$

autrement dit

$$c_1\chi_1(x)\chi_1(y) + \cdots + c_m\chi_m(x)\chi_m(y) = 0,$$

et

$$c_1\chi_1(x)\chi_m(y) + \cdots + c_m\chi_m(x)\chi_m(y) = 0.$$

En comparant les deux formules précédentes, on obtient, pour tout $x \in L$,

$$c_1(\chi_1(y) - \chi_m(y))\chi_1(x) + \cdots + c_{m-1}(\chi_1(y) - \chi_m(y))\chi_{m-1}(x) = 0.$$

Comme les $m-1$ premiers automorphismes sont L-linéairement indépendants, on sait que pour tout $y \in L$, $c_1(\chi_1(y) - \chi_m(y)) = 0$. Comme les morphismes χ_1 et χ_m sont distincts, il existe $y_0 \in L$ tel que $\chi_1(y_0) \neq \chi_m(y_0)$, ce qui implique que $c_1 = 0$.

(b) Montrons le résultat par récurrence sur le nombre d'automorphismes n. Pour $n = 1$, le résultat est clair. Supposons que tous $n-1$ automorphismes sont L-linéairement indépendants. Soient n automorphismes de corps distincts $\chi_i : L \to L$, $i = 1, \cdots, n$. Supposons qu'il existe une combinaison linéaire $c_1\chi_1 + \cdots + c_m\chi_m$ à coefficients dans L qui est identiquement nulle. On sait que les $n-1$ premiers sont L-linéairement indépendants par hypothèse de récurrence, donc par la question précédente on a $c_1 = 0$, donc $c_2\chi_2 + \cdots + c_m\chi_m = 0$. Or les $n-1$ derniers sont aussi L-linéairement indépendants par hypothèse de récurrence, donc $c_2 = \cdots = c_m = 0$, ce qui achève la récurrence.

5. (a) Par un calcul direct on obtient

$$\prod_{k=0}^{n-1} \sigma^k(\beta) = \prod_{k=0}^{n-1} \frac{\sigma^k(\alpha)}{\sigma^{k+1}(\alpha)} = \frac{\alpha}{\sigma^n(\alpha)} = 1.$$

(b) Soit $\beta \in L$ tel que

$$\prod_{k=0}^{n-1} \sigma^k(\beta) = 1.$$

Pour tout $\theta \in L$, posons

$$\alpha = \sum_{k=0}^{n-1} \left(\prod_{r=0}^{k} \sigma^r(\beta) \right) \sigma^k(\theta).$$

Montrons qu'alors on a $\alpha = \beta\sigma(\alpha)$. En effet, on a

$$\begin{aligned} \beta\sigma(\alpha) &= \beta \sum_{k=0}^{n-1} \left(\prod_{r=1}^{k+1} \sigma^{r+1}(\beta) \right) \sigma^{k+1}(\theta) \\ &= \sum_{k=1}^{n} \left(\prod_{r=0}^{k} \sigma^r(\beta) \right) \sigma^k(\theta). \end{aligned}$$

En comparant ce dernier avec l'expression de α, on voit que pour montrer que les deux coïncident, il suffit de montrer que

$$\beta\theta = \left(\prod_{r=0}^{n} \sigma^r(\beta) \right) \sigma^n(\theta),$$

ce qui est vrai car $\sigma^n = Id_L$ et $\prod_{k=0}^{n-1} \sigma^k(\beta) = 1$ par hypothèse.
Pour écrire $\beta = \alpha/\sigma(\alpha)$, il suffit alors de trouver θ tel que $\sigma(\alpha) \neq 0$. Par la question 4), comme les automorphismes $Id_L, \sigma, \sigma^2 \cdots \sigma^{n-1}$ sont distincts, ils sont L-linéairement indépendants, et comme l'application $\theta \mapsto \sigma(\alpha)$ est un combinaison linéaire de ces automorphismes, on en déduit qu'il existe $\theta \in L$ tel que $\sigma(\alpha) \neq 0$.

(c) Soit $\beta = \zeta_n^{-1}$. Comme σ laisse fixe les éléments de $K = \mathbb{Q}(\zeta_n)$, β vérifie bien $\prod_{k=0}^{n-1} \sigma^k(\beta) = 1$. Par la question précédente, il existe $\alpha \in L \setminus \{0\}$ tel que

$$\sigma(\alpha) = \zeta_n \alpha.$$

Montrons qu'un tel α convient. On a d'abord $\sigma(\alpha^n) = (\zeta_n \alpha)^n = \alpha^n$, donc α^n est un point fixe de σ. Or l'extension L/K est galoisienne, et $Aut(L/K)$ est engendré par σ, donc l'ensemble des points fixes de σ est exactement les éléments de K, donc $\alpha^n \in K$ et α est exprimable directement par radicaux sur K.

Il nous reste à montrer que $L = K(\alpha)$. On propose deux preuves ici :

i. Par hypothèse σ est annulé par le polynôme $X^n - 1$, lequel est scindé à racines simples sur $K = \mathbb{Q}(\zeta_n)$. On voit σ comme un endomorphisme du K-espace vectoriel L, et l'algèbre linéaire nous donne une décomposition

$$L = \oplus_{k=0}^{n-1} L_k$$

de L en sous-K-espaces vectoriels, où L_k est le sous-espace propre associè à la valeur propre ζ_n^k. Donc tout $y \in L$ s'écrit de manière unique comme $y = y_0 + \cdots + y_{n-1}$, où $\sigma(y_k) = \zeta_n^k y_k$. On a alors $\sigma(\alpha^{-k} y_k) = \alpha^{-k} y_k$, donc $\alpha^{-k} y_k \in K$ par ce qui précède. Donc $y_k \in K(\alpha)$, et on en déduit que $L = K(\alpha)$.

ii. Plus généralement, si L/K est une extension galoisienne, pour tout $\alpha \in L$ posons

$$C(\alpha) = \{\sigma(\alpha) | \sigma \in Aut(L/K)\}$$

l'orbite de α sous l'action de $Aut(L/K)$. Montrons que si le cardinal de $C(\alpha)$ coïncide avec le degré $n = [L : K]$, alors on a $L = K(\alpha)$. En effet, tout élément de $Aut(L/K)$ laisse stable P, le polynôme minimal de α sur K, donc envoie α sur une racine de P ; comme $C(\alpha)$ possède n éléments distincts, P possède au moins n racines, donc son degré est au moins n. Donc l'extension $K(\alpha)/K$ est de degré au moins n, et on en déduit que $L = K(\alpha)$.

On applique le résultat précédent ici : $C(\alpha) = \{\zeta_n^k \alpha | k = 0, \cdots, n-1\}$ est de cardinal $n = [L : K]$, donc $L = K(\alpha)$.