

Exercice 1. (a) $E = \mathbb{F}_5(t)$ et $K = \mathbb{F}_5(t^5)$. Montrons que le polynôme $P(X) = X^5 - t^5 \in K[X]$ est irréductible. Supposons par l'absurde que P est réductible et s'écrit $\prod P_k$ avec les P_k irréductibles unitaires. Comme $P(X) = (X - t)^5$ dans $E[X]$, P est scindé sur E avec une seule racine t , donc P_k est scindé sur E avec pour seule racine t , donc P_k est le polynôme minimal de t pour tout k . Donc, si Q est le polynôme minimal de t sur K , alors $P = Q^m$ pour un $m \in \mathbb{N}^*$. Mais alors $5 = m \deg(Q)$ et 5 est premier. Comme $\deg(Q) = 1$ implique $t \in K$ - contradiction, on doit avoir $\deg(Q) = 5$, soit $Q = P$ et P est irréductible et c'est le polynôme minimal de t sur K . $P' = 0$, donc t est inséparable. L'extension est de degré 5 parce que $E = K(t)$ et donc E est isomorphe à $K[X]/(P)$ et P est de degré 5.

(b) On prend celle de (a) et on ajoute une extension E'/E avec $E' = \mathbb{F}_{25}(t)$, qui est de degré 2 parce qu'un générateur de \mathbb{F}_{25} sur \mathbb{F}_5 est aussi un générateur de E'/E . Alors E'/K est de degré 10, mais inséparable parce que t est toujours inséparable sur K .

(c) $\mathbb{Q}(\sqrt[5]{2})/\mathbb{Q}$ n'est pas normale. Elle est de degré 5 parce que $X^5 - 2$ est irréductible par Eisenstein, et elle ne contient pas les racines non réelles de ce polynôme, par exemple $e^{\frac{2\pi}{5}} \sqrt[5]{2}$.

(d) $\mathbb{F}_{32}/\mathbb{F}_2$, (\mathbb{F}_{32} est le corps de décomposition du polynôme $X^{32} - X \in \mathbb{F}_2[X]$).

Exercice 2. (a) Soit $x \in E$. Si x est réel, il est son propre conjugué. Si x est non réel, son polynôme minimal P_x sur \mathbb{Q} a aussi \bar{x} comme racine. Comme E/\mathbb{Q} est normale et contient une racine de P_x qui est irréductible elle contient toutes les racines de P_x , donc \bar{x} . Donc, si $x \in E$, alors $\bar{x} \in E$.

(b) Comme E est stable par conjugaison, si E n'est pas inclus dans \mathbb{R} alors $Gal(E/\mathbb{Q})$ a un élément d'ordre 2. Cela est impossible parce que E/\mathbb{Q} est galoisienne de degré 3 (séparable parce que la caractéristique est nulle) et donc $|Gal(E/\mathbb{Q})| = [E : \mathbb{Q}] = 3$.

(Oui, ça marche pour n impair quelconque à la place de 3.)

Exercice 3. (a) on trouve $k = 1, 2, 4$ par la formule de $\cos(3\theta)$.

(b) la relation $\cos(2\theta) = 2\cos^2(\theta) - 1$ montre que les trois racines s'obtiennent de la première $x_1 = 2\cos(\frac{2\pi}{9})$ par des relations polynômiales, autrement dit $E = \mathbb{Q}(x_1)$ et la dite dimension est donc 3.

(c) On suppose que $E = \mathbb{Q}(\alpha)$ où α est une racine troisième dans \mathbb{C} d'un nombre rationnel a . Comme $[E : \mathbb{Q}] = 3$, le polynôme minimal de α est de degré 3. C'est donc $X^3 - a$. Comme E est un corps de décomposition, E/\mathbb{Q} est normale. Mais E contient une racine de $X^3 - a$, à savoir α , et alors il doit contenir aussi $j\alpha$, donc j . Cela est impossible, parce que E est inclus dans \mathbb{R} .

(Moralité : si les extension quadratiques de \mathbb{Q} sont de la forme $\mathbb{Q}(\sqrt{x})$, il n'en est pas ainsi des extensions cubiques.)

Exercice 4. $\mathbb{Q}(i, j)$ est galoisienne, par la preuve de votre choix, par exemple finie de degré au plus 4 donc algébrique, séparable parce que la caractéristique est nulle, normale parce que c'est le corps de décomposition de $(X^2 + 1)(X^2 + X + 1)$ (ici il faut dire que \bar{j} est bien dedans! parce que c'est j^2).

Le cas de $\mathbb{Q}(i, \sqrt[3]{2})$: on a $j \notin \mathbb{Q}(i)$ puisque la partie imaginaire de j n'est pas rationnelle. Cela implique que $\mathbb{Q}(i, j)/\mathbb{Q}$ est de degré 4. Mais alors $\mathbb{Q}(i, j, \sqrt[3]{2})$ est de degré au moins 12, vu qu'elle contient $\mathbb{Q}(i, j)$ (degré 4) et $\mathbb{Q}(\sqrt[3]{2})$ (degré 3). Or, $\mathbb{Q}(i, \sqrt[3]{2})$ est une extension de degré 6 de \mathbb{Q} par le théorème de la base télescopique. Elle ne contient donc pas j . Elle n'est donc pas normale. En effet, elle contient une racine de $X^3 - 2$, mais si elle contenait une autre elle contiendrait j , (ou $j^2 = j^{-1}$ donc j).

La troisième, $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$, est incluse dans \mathbb{R} et n'est pas normale non plus : elle contient une racine de $X^3 - 2$ mais pas les autres qui ne sont pas réelles.

Exercice 5. Posons $E := \mathbb{Q}(\sqrt[4]{2}, i)$.

L'extension E/\mathbb{Q} est algébrique parce qu'engendrée par des éléments algébriques (et même finie parce qu'engendrée par un nombre fini d'éléments algébriques).

Soit $P(X) = X^4 - 2$, polynôme irréductible sur \mathbb{Q} par Eisenstein. Ses racines dans \mathbb{C} sont $\pm\sqrt[4]{2}$ et $\pm i\sqrt[4]{2}$. E est donc le corps de décomposition de P dans \mathbb{C} (que les racines appartiennent à E c'est immédiat, pour montrer qu'elles engendrent E il suffit de remarquer qu'une racine est $\sqrt[4]{2}$ et que i s'obtient comme quotient de deux racines). L'extension E/\mathbb{Q} est donc normale. Elle est séparable parce qu'on est en caractéristique nulle. Elle est donc galoisienne.

L'extension E/\mathbb{Q} est de degré 8 par le théorème de la base télescopique, parce que i n'appartient pas à $\mathbb{Q}(\sqrt[4]{2})$, et $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ parce que $X^4 - 2$ est irréductible sur \mathbb{Q} . Calculons son groupe de Galois G qui a 8 éléments.

On a $\mathbb{Q} \subset \mathbb{Q}(i) \subset E$. Le cours nous dit que $E/\mathbb{Q}(i)$ est galoisienne et son groupe de Galois H est un sous-groupe de G à quatre éléments. L'extension $E/\mathbb{Q}(i)$ est engendrée par $\sqrt[4]{2}$ (en particulier le polynôme $X^4 - 2$ est irréductible sur $\mathbb{Q}(i)$), donc le cours (extensions monogènes) nous dit que les quatre éléments de H sont définis en envoyant cet élément sur chaque autre racine de $X^4 - 2$. Remarquer qu'on peut calculer alors facilement l'image des autres racines que $\sqrt[4]{2}$ par un tel élément de H , parce qu'il s'agit d'un morphisme $\mathbb{Q}(i)$ -linéaire et il envoie donc i sur i . Soit $\sigma \in H$ défini par $\sqrt[4]{2} \mapsto i\sqrt[4]{2}$. On vérifie facilement que $\sigma^2 = -Id$. En effet, comme σ est $\mathbb{Q}(i)$ -linéaire, on a

$$\sigma^2(\sqrt[4]{2}) = \sigma(i\sqrt[4]{2}) = i\sigma(\sqrt[4]{2}) = ii\sqrt[4]{2} = -\sqrt[4]{2}.$$

Donc H contient cet élément σ qui au carré n'est pas l'identité. Donc $H = \langle \sigma \rangle \simeq \mathbb{Z}/4\mathbb{Z}$. Comme dans l'exercice 2 (a), E est stable par conjugaison et contient l'élément qui envoie i en $-i$ et stabilise $\sqrt[4]{2}$, qui n'est pas dans H . Cet élément c est d'ordre 2 et un calcul simple sur $\sqrt[4]{2}$ montre que $c\sigma c^{-1} = -\sigma = \sigma^{-1}$. On sait qu'alors G est le groupe diédral à 8 éléments. (Un groupe qui est engendré par deux éléments x et y tels que y est d'ordre n et x est d'ordre 2 et tels que $xyx^{-1} = y^{-1}$ est le groupe diédral à $2n$ éléments. Souvent c'est la définition, sinon c'est la caractérisation algébrique.)