Révisions : correction

Exercice 1.
Si M est un corps tel que $K \subseteq M \subseteq L$, le théorème de la base télescopique entraîne que

$$[L:K] = [L:M] \cdot [M:K].$$

La primalité de $[L : K]$ entraîne donc $[L : M] = 1$ (ce qui entraîne $M = L$) ou $[M : K] = 1$ (ce qui entraîne $M = K$).
Si $\alpha \in L \setminus K$, on a $K \subsetneq K(\alpha) \subseteq L$. D'après ce qui précède, on a $K(\alpha) = L$.

Exercice 2.
– (i) implique (iii) : on montre par récurrence sur $r \leq n$ que $K(\alpha_1, \ldots, \alpha_r)/K$ est une extension finie : Si α_1 est algébrique sur K, l'application surjective

$$\begin{array}{rcl} \text{év}_{\alpha_1} : K[X] & \to & K[\alpha] \\ P & \mapsto & P(\alpha_1) \end{array}$$

induit un isomorphisme $K[X]/(\mu_\alpha) \to K[\alpha]$. Cela démontre que $K[\alpha]$ est un corps et qu'il est de K-dimension finie. En particulier, $K(\alpha) = K[\alpha]$ est une extension finie de K.
Le point-clef pour faire marcher la récurrence est maintenant que α_r, algébrique sur K le reste *a fortiori* sur $K(\alpha_1, \ldots, \alpha_{r-1})$. L'extension $K(\alpha_1, \ldots, \alpha_r)/K(\alpha_1, \ldots, \alpha_{r-1})$ est donc finie. D'après le théorème de la base télescopique, on obtient donc que l'extension $K(\alpha_1, \ldots, \alpha_r)/K$ est finie.
– (iii) implique (ii) : soit $\alpha \in K(\alpha_1, \ldots, \alpha_n)$. L'application

$$\begin{array}{rcl} \text{év}_{\alpha} : K[X] & \to & K(\alpha_1, \ldots, \alpha_n) \\ P & \mapsto & P(\alpha) \end{array}$$

est K-linéaire. Si $\dim_K K(\alpha_1, \ldots, \alpha_n) < +\infty$, elle ne peut pas être injective, ce qui entraîne que α est algébrique sur K. L'extension $K(\alpha_1, \ldots, \alpha_n)/K$ est alors algébrique.
– (ii) implique (i) : par définition, si $K(\alpha_1, \ldots, \alpha_n)/K$ est une extension algébrique, tous les éléments de $K(\alpha_1, \ldots, \alpha_n)$, y compris les (α_i), sont algébriques sur K.
– (iii) implique (iv) : $K[\alpha_1, \ldots, \alpha_n]$ est un sous-K-espace vectoriel de $K(\alpha_1, \ldots, \alpha_n)$; si celui-ci est de dimension finie, il en est donc de même de celui-là.
– (iv) implique (i) : si $\dim_K K[\alpha_1, \ldots, \alpha_n] < +\infty$, la famille $(\alpha_i^k)_{k \in \mathbf{N}}$ est K-liée, ce qui entraîne que α_i est algébrique sur K.

Exercice 3.

1. On a vu en cours que $\mathbf{Q}(\zeta_n)$ est le corps de décomposition du polynôme irréductible $\Phi_n \in \mathbf{Q}[X]$, dont les racines sont les ζ_n^k, où k décrit l'ensemble des entiers de $\{1, \ldots, n\}$ premiers avec n : l'extension $\mathbf{Q}(\zeta_n)/\mathbf{Q}$ est donc normale, de degré $\deg \Phi_n = \varphi(n)$. Comme elle est de caractéristique nulle, elle est séparable (cf. TD 3, exercice 4). Comme ζ_n^k ne dépend que de la classe de k modulo n, on peut noter $\left(\zeta_n^k\right)_{k \in (\mathbf{Z}/n\mathbf{Z})^\times}$ ces racines.
   Par ailleurs, $\mathbf{Q}(\zeta_n)$ est un corps de rupture du polynôme irréductible Φ_n. Cela démontre que l'extension $\mathbf{Q}(\zeta_n)/\mathbf{Q}$ est de degré $\deg \Phi_n = \varphi(n)$. En outre, le cours affirme alors que les plongements de $\mathbf{Q}(\zeta_n)$ sont en bijection avec les racines de Φ_n, qui sont exactement les

$\left(\zeta_n^k\right)_{k\in(\mathbf{Z}/n\mathbf{Z})^\times}$. Plus précisément, pour chaque $k \in (\mathbf{Z}/n\mathbf{Z})^\times$, il existe un unique morphisme $\sigma_k : \mathbf{Q}(\zeta_n) \to \mathbf{C}$ envoyant ζ_n sur ζ_n^k.

Enfin, comme $\mathbf{Q}(\zeta_n)/\mathbf{Q}$ est normale, tous ces plongements sont en fait des automorphismes de $\mathbf{Q}(\zeta_n)$ et l'on a

$$\mathrm{Aut}_{\mathbf{Q}}\, \mathbf{Q}(\zeta_n) = \left\{ \sigma_k \,\middle|\, k \in (\mathbf{Z}/n\mathbf{Z})^\times \right\}.$$

2. Déjà, on peut remarquer que $\mathbf{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbf{Q}(\sqrt[6]{2})$. En effet, ce dernier contient évidemment $\left(\sqrt[6]{2}\right)^2 = \sqrt[3]{2}$ et $\left(\sqrt[6]{2}\right)^3 = \sqrt{2}$. Réciproquement, $\mathbf{Q}(\sqrt{2}, \sqrt[3]{2})$ contient $\sqrt{2}/\sqrt[3]{2} = \sqrt[6]{2}$.

   Cela montre que l'extension n'est pas normale : $\sqrt[6]{2}$ est annulé par le polynôme $\mathrm{X}^6 - 2$, qui est irréductible en vertu du critère d'Eisenstein. On a donc $\mu_{\sqrt[6]{2}} = \mathrm{X}^6 - 2$. Mais ce polynôme a des racines complexes qui ne sont pas dans $\mathbf{R}$, et *a fortiori* pas dans $\mathbf{Q}(\sqrt[6]{2})$, par exemple $\zeta_6 \sqrt[6]{2}$. En revanche, de caractéristique nulle, l'extension est bien séparable. Son degré est $[\mathbf{Q}(\sqrt[6]{2}) : \mathbf{Q}] = \deg \mu_{\sqrt[6]{2}} = 6$.

   Comme dans le point précédent, $\mathbf{Q}(\sqrt[6]{2})$ étant un corps de rupture de $\mathrm{X}^6 - 2$, les morphismes $\mathbf{Q}(\sqrt[6]{2})$ dans $\mathbf{C}$ sont en bijection avec les racines de $\mathrm{X}^6 - 2$, c'est-à-dire avec les $\left(\zeta_6^k \sqrt[6]{2}\right)_{k\in(\mathbf{Z}/6\mathbf{Z})}$. Parmi ceux-ci, seuls deux ont leur image dans $\mathbf{Q}(\sqrt[6]{2})$ (ou même dans $\mathbf{R}$) et sont donc des automorphismes : l'identité et

$$\begin{array}{rcl} \mathbf{Q}(\sqrt[6]{2}) = \mathbf{Q}(\sqrt[3]{2}, \sqrt{2}) = \left\{ \alpha + \beta\sqrt{2} \,\middle|\, \alpha, \beta \in \mathbf{Q}(\sqrt[3]{2}) \right\} & \to & \mathbf{Q}(\sqrt[3]{2}, \sqrt{2}) \\ \alpha + \beta\sqrt{2} & \mapsto & \alpha - \beta\sqrt{2}. \end{array}$$

3. On a vu (TD 3, exercice 4) qu'un corps de caractéristique p était parfait si et seulement si son morphisme de Frobenius $\mathrm{F} : x \mapsto x^p$ était bijectif, étant entendu qu'il est toujours injectif : comme $\mathrm{F}(x) - 1 = x^p - 1 = (x-1)^p$, on a bien $\ker \mathrm{F} = \{1\}$. En particulier, toute application injective d'un ensemble fini dans lui-même étant bijective, tout corps fini est parfait. L'extension $\mathbf{F}_9/\mathbf{F}_3$ est donc séparable.

   Comme $\mathbf{F}_9$ est le corps de décomposition du polynôme $\mathrm{X}^9 - \mathrm{X} \in \mathbf{F}_3[\mathrm{X}]$, l'extension est également normale. Un $\mathbf{F}_3$-espace vectoriel de dimension finie e a exactement 3^e éléments donc $[\mathbf{F}_9 : \mathbf{F}_3] = 2$. On a vu (TD 1, exercice 8) que toute extension quadratique d'un corps de caractéristique différente de 2 était le corps de rupture d'un polynôme $\mathrm{X}^2 - \alpha$, où α n'est pas un carré. Dans notre cas, $\mathbf{F}_9$ est donc un corps de rupture de $\mathrm{X}^2 + 1$. Si l'on note i une racine de -1 dans $\mathbf{F}_9$, on a simplement $\mathrm{X}^2 + 1 = (\mathrm{X} - i)(\mathrm{X} + i)$, avec $i \neq -i$. Le corps $\mathbf{F}_9$ a donc deux automorphismes, correspondant à $\alpha + \beta i \mapsto \alpha - \beta i$. Mais on connaît ces deux automorphismes ! En effet, le morphisme de Frobenius $\mathrm{F} : x \mapsto x^3$ continue à définir un automorphisme de $\mathbf{F}_9$ qui ne peut pas être l'identité (l'équation $x^3 = x$ ne saurait avoir plus de 3 racines). On a donc

$$\mathrm{Aut}_{\mathbf{F}_3}\, \mathbf{F}_9 = \{\mathrm{id}, \mathrm{F}\}.$$

4. Par construction, $\mathrm{F}(\alpha)$ est un corps de rupture du polynôme $\mathrm{X}^3 - t$, qui est irréductible dans $\mathbf{F}_3[t]$ (et donc dans $\mathbf{F}_3(t)$) en vertu du critère d'Eisenstein. Dans $\mathrm{F}(\alpha)$, ce polynôme se factorise sous la forme

$$\mathrm{X}^3 - t = \mathrm{X}^3 - \alpha^3 = (\mathrm{X} - \alpha)^3.$$

   Cela démontre du même coup que l'extension $\mathrm{F}(\alpha)/\mathrm{F}$ n'est pas séparable et qu'elle est normale, puisque $\mathrm{F}(\alpha)$ est bien le corps de décomposition de $\mathrm{X}^3 - t$. Corps de rupture de $\mathrm{X}^3 - t$, $\mathrm{F}(\alpha)$ est de F-dimension 3.

   Les morphismes de $\mathrm{F}(\alpha)$ dans une clôture algébrique Ω sont en bijection avec les racines de $\mathrm{X}^3 - t$: il n'y en a donc qu'un. En particulier,

$$\mathrm{Aut}_{\mathrm{F}}\, \mathrm{F}(\alpha) = \{\mathrm{id}\}.$$

Exercice 4.

On va démontrer les deux propriétés au cours de la même démonstration par récurrence. Les deux résultats sont vides si $n=0$.

Rappelons un des résultats de l'exercice 8 du TD 1 : soit $K(\sqrt{\alpha})/K$ une extension quadratique (avec K de caractéristique différente de 2). Cela revient à dire que α n'est pas un carré dans K. Alors si $\beta \in K$ est le carré d'un élément de $K(\sqrt{\alpha})$, β ou $\alpha\beta$ est le carré d'un élément de K.

En effet, si on écrit $x+y\sqrt{\alpha}$ $(x, y \in K)$ un élément de $K(\sqrt{\alpha})$ dont le carré est β, on a

$$(x+y\sqrt{\alpha})^2=\beta \Leftrightarrow x^2+\alpha y^2+2xy\sqrt{\alpha}=\beta \Leftrightarrow \begin{cases} x^2+\alpha y^2=\beta \\ 2xy=0. \end{cases}$$

Comme on est en caractéristique différente de 2, la deuxième équation entraîne que $y=0$ (auquel cas $\beta=x^2$ est bien le carré d'un élément de K) ou $x=0$ (auquel cas $\beta/\alpha=y^2$ est le carré d'un élément de K ; comme $\alpha\beta=\alpha^2\beta/\alpha$, cela est bien équivalent au fait que $\alpha\beta$ soit le carré d'un élément de K.)

Armé de ce résultat, nous pouvons faire marcher la récurrence. Supposons donc que les deux résultats aient été démontrés pour un entier n. Notons pour simplifier $K_n=\mathbf{Q}\left(\sqrt{p_1},\dots,\sqrt{p_n}\right)$.

L'élément $\sqrt{p_{n+1}}$ est évidemment racine du polynôme X^2-p_{n+1}. De degré 2, ce polynôme est irréductible sur K_n si et seulement s'il n'a pas de racine, c'est-à-dire si et seulement si p_{n+1} n'est pas le carré d'un élément de K_n. Mais, d'après l'hypothèse de récurrence, si p_{n+1} était un carré dans K_n, on pourrait trouver une partie $I \subseteq \{1,\dots,n\}$ telle que le nombre entier $\left(\prod_{i\in I} p_i\right)\cdot p_{n+1}$ soit le carré d'un rationnel, ce qui est exclu (la valuation p_{n+1}-adique de cet entier vaut 1). Le polynôme X^2-p_{n+1} est donc irréductible dans $K_n[X]$, ce qui entraîne que l'extension K_{n+1}/K_n est de degré 2 et donc, d'après l'hypothèse de récurrence et le théorème de la base télescopique,

$$[K_{n+1}:\mathbf{Q}]=[K_{n+1}:K_n]\cdot[K_n:\mathbf{Q}]=2\cdot 2^n=2^{n+1}.$$

Maintenant, d'après l'argument cité plus haut, $x\in K_n$ est le carré d'un élément de $K_{n+1}=K_n(\sqrt{p_{n+1}})$ si et seulement si x ou xp_{n+1} est le carré d'un élément de K_n. Si on suppose $x\in\mathbf{Q}$, l'hypothèse de récurrence entraîne que cela est équivalent à l'existence d'une partie $I\subseteq\{1,\dots,n\}$ telle que

$$x\prod_{i\in I} p_i \text{ ou } xp_{n+1}\prod_{i\in I} p_i \text{ soit le carré d'un nombre rationnel.}$$

Autrement dit, il existe une partie $J=I$ ou $I\sqcup\{n+1\}\subseteq\{1,\dots,n+1\}$ telle que

$$x\prod_{i\in J} p_i \text{ soit le carré d'un nombre rationnel,}$$

ce qui conclut la récurrence.

Notons que la preuve par récurrence de l'égalité $[K_n:\mathbf{Q}]$ entraîne même que la famille

$$\left\{\prod_{i\in I}\sqrt{p_i}\,\middle|\, I\subseteq\{1,\dots,n\}\right\}$$

forme une $\mathbf{Q}$-base de K_n. En particulier, pour tout n, la famille finie $(\sqrt{p_1},\dots,\sqrt{p_n})$ est $\mathbf{Q}$-libre, ce qui entraîne la $\mathbf{Q}$-liberté de la famille infinie $\left(\sqrt{p_i}\right)_{i\in\mathbf{N}}$.

La preuve du théorème de l'élément primitif vue en cours montre qu'un élément α d'une extension séparable L d'un corps K est primitif dès que

$$\forall i\neq j, \sigma_i(\alpha)\neq\sigma_j(\alpha),$$

où les (σ_i) sont les plongements $\mathrm{L} \to \overline{\mathrm{K}}$ de L dans une clôture algébrique $\overline{\mathrm{K}}$ du corps de base prolongeant l'inclusion $\mathrm{K} \to \overline{\mathrm{K}}$. Cela nous sera utile une fois que l'on aura démontré le résultat suivant.
Lemme. Les plongements de K_n dans $\mathbf{C}$ sont les

$$\begin{array}{rrcl} \sigma_{\mathrm{I}} : & \mathrm{K}_n & \to & \mathrm{K}_n \subseteq \mathbf{C} \\ & \sqrt{p_i} & \mapsto & \begin{cases} -\sqrt{p}_i & \text{si } i \in \mathrm{I} \\ \sqrt{p}_i & \text{si } i \notin \mathrm{I}, \end{cases} \end{array}$$

où I décrit l'ensemble des parties de $\{1, \ldots, n\}$ (en particulier, $\mathrm{I} = \varnothing$ correspond à l'inclusion $\mathrm{K}_n \to \mathbf{C}$.)
Cela conclut : si $\mathrm{I} \subseteq \{1, \ldots, n\}$,

$$\sigma_{\mathrm{I}}\left(\sum_{i=1}^{n} \sqrt{p_i}\right) = \sum_{i=1}^{n} \varepsilon_{\mathrm{I}}(i)\sqrt{p_i},$$

où $\varepsilon_{\mathrm{I}}(i) = -1$ si $i \in \mathrm{I}$ et 1 sinon. La famille $(\sqrt{p_i})_{i=1}^{n}$ étant libre, ces 2^n éléments sont effectivement tous distincts et $\sqrt{p_1} + \cdots + \sqrt{p_n}$ est bien un élément primitif de K_n.
Reste à montrer le lemme. Déjà, remarquons que $\mathrm{K}_n/\mathbf{Q}$ est une extension de degré 2^n. D'après le théorème de l'élément primitif, c'est le corps de rupture d'un polynôme irréductible de degré 2^n et les plongements dans $\mathbf{C}$ étant en bijection avec les racines de ce polynôme, il y en a exactement 2^n. Si on arrive à construire des plongements $\mathrm{K}_n \to \mathbf{C}$ qui vérifient les propriétés promises par le lemme, on aura donc trouvé tous les plongements.
Ensuite, remarquons que ces plongements sont en fait des automorphismes de K_n (qui sont d'ailleurs tous égaux à leur inverse). On peut notamment les composer. Il suffit donc de construire les $\sigma_{\{i\}}$ pour démontrer le lemme (si les $\sigma_{\{i\}}$ vérifient les propriétés énoncées par le lemme, on voit directement que $\sigma_{\{i_1,\ldots,i_p\}} = \sigma_{\{i_1\}} \circ \cdots \circ \sigma_{\{i_p\}}$ fait également ce que l'on attend de lui).
Pour cela, remarquons que $\mathrm{K}_n = \mathrm{K}_{n,i}(\sqrt{p_i})$, où

$$\mathrm{K}_{n,i} = \mathbf{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{i-1}}, \sqrt{p_{i+1}}, \ldots, \sqrt{p_n}).$$

L'extension $\mathrm{K}_n/\mathrm{K}_{n,i}$ est donc une extension quadratique, le corps de rupture du polynôme irréductible $\mathrm{X}^2 - p_i \in \mathrm{K}_{n,i}[\mathrm{X}]$. Il y a donc bien un plongement $\sigma_i : \mathrm{K}_n \to \mathbf{C}$ prolongeant l'inclusion $\mathrm{K}_{n,i} \to \mathbf{C}$ et envoyant $\sqrt{p_i}$ sur $-\sqrt{p_i}$. Ce plongement σ_i est bien le plongement $\sigma_{\{i\}}$ cherché et le lemme est démontré.
Notons au passage que l'on a démontré que l'extension $\mathbf{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})/\mathbf{Q}$ est normale et que ses automorphismes forment un groupe $\left\{\sigma_{\mathrm{I}} \,\middle|\, \mathrm{I} \subseteq \{1, \ldots, n\}\right\}$ isomorphe au groupe abélien produit $(\mathbf{Z}/2\mathbf{Z})^n$.

Exercice 5.
Nous sommes en caractéristique nulle : toutes les extensions sont séparables.
Pour comprendre plus efficacement les sous-extensions des extensions proposées, commençons par démontrer un résultat utilisant ce que l'on sait sur les extensions quadratiques.
Lemme. Soit E/F une extension de corps de caractéristique différente de 2. Alors les extensions intermédiaires E/L/F avec $[\mathrm{E} : \mathrm{L}] = 2$ sont exactement les

$$\mathrm{E}^{\sigma} = \left\{x \in \mathrm{E} \,\middle|\, \sigma(x) = x\right\},$$

où $\sigma : \mathrm{E} \to \mathrm{E}$ décrit l'ensemble des automorphismes F-linéaires $\sigma \neq \mathrm{id}_{\mathrm{E}}$ tels que $\sigma^2 = \mathrm{id}_{\mathrm{E}}$. (Pour simplifier, à partir de maintenant, on appellera F-*involution* un tel automorphisme).
Preuve. Soit L une telle extension intermédiaire. En particulier, E/L est une extension quadratique de caractéristique différente de 2. On sait qu'on peut donc l'écrire $\mathrm{E} = \mathrm{L}(\sqrt{\alpha})$, où $\alpha \in \mathrm{L}$ n'est pas un carré. En particulier, il y a deux plongements de E dans $\overline{\mathrm{L}}$ prolongeant l'inclusion de L dans $\overline{\mathrm{L}}$,

l'identité et un automorphisme L-linéaire de E envoyant $\sqrt{a}$ sur $-\sqrt{a}$. Puisque $\mathrm{L} \supseteq \mathrm{F}$, cet automorphisme est bien une F-involution σ et on a bien $\mathrm{E}^\sigma = \mathrm{L}$: si on écrit un élément de $\mathrm{E} = \mathrm{L}(\sqrt{a})$ dans la L-base $(1, \sqrt{a})$, on a

$$x + y\sqrt{a} \in \mathrm{E}^\sigma \Leftrightarrow x + y\sqrt{a} = x - y\sqrt{a} \Leftrightarrow 2y = 0.$$

Réciproquement, soit $\sigma : \mathrm{E} \to \mathrm{E}$ une F-involution. On veut démontrer que $\mathrm{E}/\mathrm{E}^\sigma$ est une extension quadratique (puisque σ est F-linéaire, il est clair que $\mathrm{E}^\sigma \supseteq \mathrm{F}$). Pour cela, remarquons que comme le polynôme minimal de E^σ est $\mathrm{X}^2 - 1$, on a une décomposition E^σ-linéaire en somme directe

$$\mathrm{E} = \mathrm{E}^\sigma \oplus \left\{ x \in \mathrm{E} \,\middle|\, \sigma(x) = -x \right\}.$$

Comme $\sigma \neq \mathrm{id}$, il existe un élément y non nul tel que $\sigma(y) = -y$. On vérifie alors directement que

$$\begin{array}{ccc} \left\{ x \in \mathrm{E} \,\middle|\, \sigma(x) = -x \right\} & \to & \mathrm{E}^\sigma \\ x & \mapsto & \dfrac{x}{y} \end{array}$$

est un isomorphisme E^σ-linéaire. On a donc bien $\dim_{\mathrm{E}^\sigma} \left\{ x \in \mathrm{E} \,\middle|\, \sigma(x) = -x \right\} = 1$, ce qui entraîne $[\mathrm{E} : \mathrm{E}^\sigma] = \dim_{\mathrm{E}^\sigma} \mathrm{E} = 2$.
Passons donc à l'étude dans le détail des trois extensions proposées.

1. Le cours sur les polynômes cyclotomiques montre que ζ_5 est un nombre algébrique de polynôme minimal $\Phi_5 = \mathrm{X}^4 + \mathrm{X}^3 + \mathrm{X}^2 + \mathrm{X} + 1 \in \mathbf{Q}[\mathrm{X}]$. Les racines de ce polynôme étant les $\left(\zeta_5^k\right)_{k=1}^4$, $\mathbf{Q}(\zeta_5)$ est à la fois un corps de rupture et de décomposition de $\mathbf{Q}(\zeta_5)$. En particulier, l'extension $\mathbf{Q}(\zeta_5)/\mathbf{Q}$ est normale et de degré 4.
   Il y a 4 plongements $(\sigma_i)_{i=1}^4$ de $\mathbf{Q}(\zeta_5)$ dans $\mathbf{C}$, déterminés par l'image de ζ_5 : $\sigma_i(\zeta_5) = \zeta_5^i$. Puisque l'extension est normale, ce sont tous des automorphismes de $\mathbf{Q}(\zeta_5)$ et

   $$\mathrm{Aut}_{\mathrm{Q}}(\mathbf{Q}(\zeta_5)) = \{\sigma_1 = \mathrm{id}_{\mathbf{Q}(\zeta_5)}, \sigma_2, \sigma_3, \sigma_4\}.$$

   Comme $\sigma_i(\sigma_j(\zeta_5)) = \sigma_i(\zeta_5^j) = \sigma_i(\zeta_5)^j = (\zeta_5^i)^j$, on a $\sigma_i \circ \sigma_j = \sigma_{ij}$, où l'indice ij est à entendre modulo 5. Le groupe $\mathrm{Aut}_{\mathbf{Q}}(\zeta_5)$ est donc isomorphe au groupe des inversibles $(\mathbf{Z}/5\mathbf{Z})^\times = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$. En particulier, c'est un groupe cyclique d'ordre 4.
   Puisque l'extension est de degré 4, ses seules extensions non triviales sont de degré 2. D'après le lemme, il s'agit des $\mathbf{Q}(\zeta_5)^\sigma$ où σ est un automorphisme d'ordre 2. Mais le groupe des automorphismes étant cyclique, il n'y a qu'un seul élément d'ordre 2. Puisque $4^2 = 16 \equiv 1 \pmod 5$, il s'agit de σ_4. Mais par ailleurs, on connaît une involution non triviale de $\mathbf{Q}(\zeta_5)$, c'est simplement la conjugaison complexe ! On a donc $\sigma_4(z) = \overline{z}$ (et, de fait, $\zeta_5^4 = \overline{\zeta}_5$) et la seule sous-extension intermédiaire non triviale est

   $$\mathbf{Q}(\zeta_5)^{\sigma_4} = \mathbf{Q}(\zeta_5)^{z \mapsto \overline{z}} = \mathbf{Q}(\zeta_5) \cap \mathbf{R}.$$

   Pour la déterminer plus précisément, il suffit d'exhiber un élément réel mais non rationnel de $\mathbf{Q}(\zeta_5)$.

   $$2\cos\left(\frac{2\pi}{5}\right) = \zeta_5 + \overline{\zeta}_5 = \zeta_5 + \zeta_5^4 = \frac{\sqrt{5} - 1}{2}$$

   fait l'affaire (voir TD 1, exercice 2 pour le calcul du cosinus). En résumé, voilà le diagramme des sous-extensions et des sous-groupes du groupe des automorphismes (qui se correspondent via la correspondance de Galois, énoncée en cours).

$$\begin{array}{ccc}
\mathbf{Q}(\zeta_5) & & \{\mathrm{id}\} \\
\Big| & & \Big| \\
\mathbf{Q}(\sqrt{5}) = \mathbf{Q}(\zeta_5)\cap\mathbf{R} & & \{\mathrm{id}=\sigma_1,\sigma_4\} = \{\mathrm{id}, z\mapsto\overline{z}\} \\
\Big| & & \Big| \\
\mathbf{Q} & & \{\mathrm{id}=\sigma_1,\sigma_2,\sigma_3,\sigma_4\} \simeq (\mathbf{Z}/5\mathbf{Z})^\times \simeq \mathbf{Z}/4\mathbf{Z}.
\end{array}$$

2. On voit directement que $\mathbf{Q}(\zeta_3, \sqrt[3]{2}) = \mathbf{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2})$ est le corps de décomposition de X^3-2. À ce titre $\mathbf{Q}(\zeta_3, \sqrt[3]{2})/\mathbf{Q}$ est une extension normale

   Puisque $\zeta_3 = \dfrac{-1}{2} + \dfrac{\sqrt{3}}{2}i$ est un algébrique de degré 2 et que $\sqrt[3]{2}$ est un algébrique de degré 3, le premier exercice du TD 1 montre que l'extension est de degré $2\cdot 3 = 6$.

   Si on écrit, grâce au théorème de l'élément primitif, $\mathbf{Q}(\zeta_3, \sqrt[3]{2}) = \mathbf{Q}(\alpha)$ où α est nécessairement de degré 6, on obtient qu'il y a six plongements de $\mathbf{Q}(\zeta_3, \sqrt[3]{2})$ dans $\mathbf{C}$, qui sont tous des automorphismes par normalité.

   Déjà, comme $\mathbf{Q}(\zeta_3, \sqrt[3]{2})/\mathbf{Q}(\sqrt[3]{2})$ est une extension quadratique, il existe une involution $s \in \mathrm{Aut}_{\mathbf{Q}}\,\mathbf{Q}(\zeta_3, \sqrt[3]{2})$ telle que $\mathbf{Q}(\zeta_3, \sqrt[3]{2})^s = \mathbf{Q}(\sqrt[3]{2})$. *A posteriori*, cette involution est simplement la conjugaison complexe.

   En outre, comme le polynôme X^3-2 reste irréductible sur $\mathbf{Q}(\zeta_3)$, il existe un automorphisme $t \in \mathrm{Aut}_{\mathbf{Q}(\zeta_3)}\,\mathbf{Q}(\zeta_3, \sqrt[3]{2}) \subseteq \mathrm{Aut}_{\mathbf{Q}}\,\mathbf{Q}(\zeta_3, \sqrt[3]{2})$ tel que $t(\sqrt[3]{2}) = \zeta_3\sqrt[3]{2}$ et $\mathrm{Aut}_{\mathbf{Q}(\zeta_3)}\,\mathbf{Q}(\zeta_3, \sqrt[3]{2}) = \{\mathrm{id}, t, t^2\}$.

   On vérifie alors que ts et t^2s sont deux automorphismes différents de ceux que nous venons de mentionner (par exemple en calculant l'image de $\sqrt[3]{2}$ et ζ_3 par ces automorphismes) et on a ainsi obtenu tous les automorphismes de $\mathbf{Q}(\zeta_3, \sqrt[3]{2})$.

   Le groupe ainsi obtenu est isomorphe au groupe symétrique $\mathfrak{S}(3)$. On peut le vérifier à la main assez facilement (par exemple en exhibant deux éléments qui ne commutent pas : $\mathfrak{S}(3)$ est le seul groupe d'ordre 6 non commutatif) mais il est plus frappant de remarquer que l'action de $\mathrm{Aut}_{\mathbf{Q}}\,\mathbf{Q}(\zeta_3, \sqrt[3]{2})$ sur les trois racines $r_1 = \sqrt[3]{2}$, $r_2 = \zeta_3\sqrt[3]{2}$ et $r_3 = \zeta_3^2\sqrt[3]{2}$ de X^3-2 réalise un isomorphisme.

Automorphisme σ	$\sigma(\zeta_3)$	$\sigma(\sqrt[3]{2})$	Action sur les racines de X^3-2
id	ζ_3	$\sqrt[3]{2}$	id
s	ζ_3^2	$\sqrt[3]{2}$	$(r_2\ r_3)$
t	ζ_3	$\zeta_3\sqrt[3]{2}$	$(r_1\ r_2\ r_3)$
ts	ζ_3^2	$\zeta_3\sqrt[3]{2}$	$(r_1\ r_2)$
t^2	ζ_3	$\zeta_3^2\sqrt[3]{2}$	$(r_1\ r_3\ r_2)$
t^2s	ζ_3^2	$\zeta_3^2\sqrt[3]{2}$	$(r_1\ r_3)$

   Le lemme que nous avons démontré nous assure maintenant qu'il y a trois sous-extensions de degré 3, obtenues comme points fixes des trois involutions s, ts et t^2s. Comme s est simplement la conjugaison complexe, on a immédiatement

$$\mathbf{Q}(\zeta_3, \sqrt[3]{2})^s = \mathbf{Q}(\zeta_3, \sqrt[3]{2}) \cap \mathbf{R} = \mathbf{Q}(\sqrt[3]{2}).$$

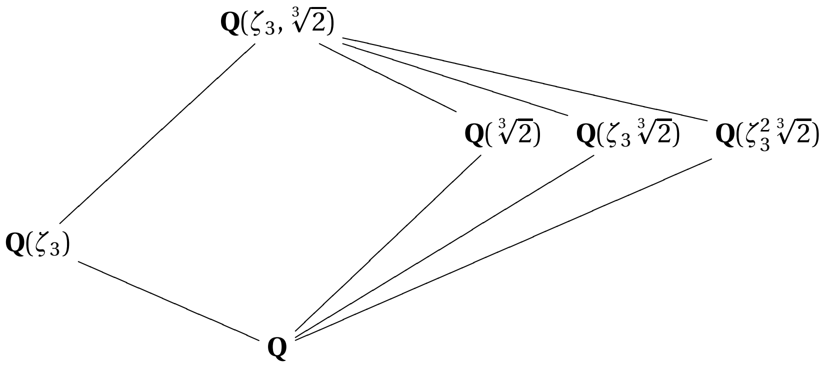
   En outre, puisque ts fixe $r_3 = \zeta_3^2\sqrt[3]{2}$ et que t^2s fixe $r_2 = \zeta_3\sqrt[3]{2}$, on a

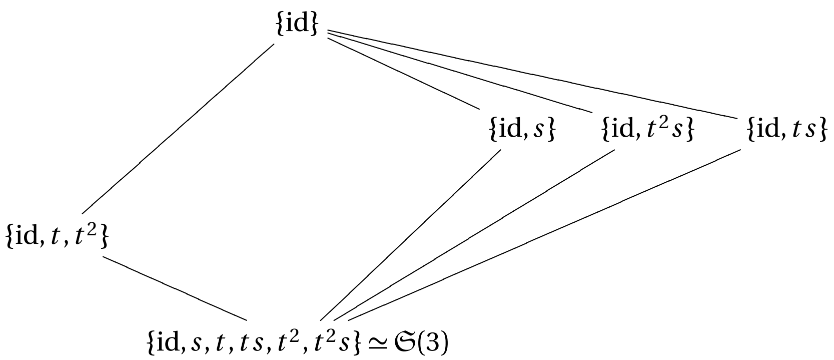
$$\mathbf{Q}(\zeta_3, \sqrt[3]{2})^{ts} = \mathbf{Q}(\zeta_3^2\sqrt[3]{2}) \text{ et } \mathbf{Q}(\zeta_3, \sqrt[3]{2})^{t^2s} = \mathbf{Q}(\zeta_3\sqrt[3]{2}).$$

Il nous faut cependant un argument *ad hoc* pour montrer que $\mathbf{Q}(\zeta_3) \subseteq \mathbf{Q}(\zeta_3, \sqrt[3]{2})$ est la seule sous-extension quadratique. Pour cela, remarquons que si K en était une autre, K ne contiendrait pas ζ_3. En particulier, son polynôme minimal ($X^2 + X + 1$, mais peu importe) resterait irréductible sur K. On aurait alors une extension $K(\zeta_3) \subseteq \mathbf{Q}(\zeta_3, \sqrt[3]{2})$ de degré

$$[K(\zeta_3) : \mathbf{Q}] = [K(\zeta_3) : K] \cdot [K : \mathbf{Q}] = 4,$$

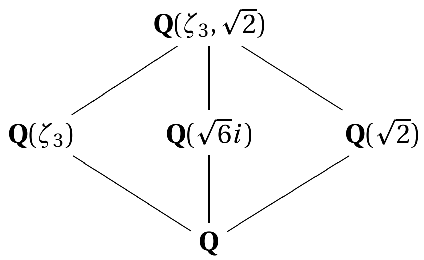
ce qui est impossible car $\mathbf{Q}(\zeta_3, \sqrt[3]{2})/\mathbf{Q}$ est de degré 6, qui n'est pas un multiple de 4.

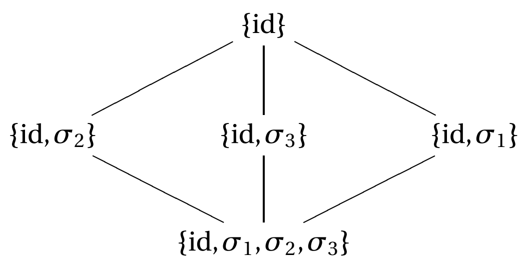




3. $\mathbf{Q}(\zeta_3, \sqrt{2}) = \mathbf{Q}(\sqrt{-3}, \sqrt{2})$ est une extension biquadratique de $\mathbf{Q}$. L'analyse qui a été faite de $\mathbf{Q}(\sqrt{p}, \sqrt{q})/\mathbf{Q}$ à l'exercice 7 du TD 4 peut être recopiée telle quelle (tout ce qui a été dit reste vrai pour deux entiers sans facteur carré différents). En résumé, les automorphismes forment un groupe d'ordre 4 isomorphe à $(\mathbf{Z}/2\mathbf{Z})^2$ et l'extension admet trois sous-extensions quadratiques.

Automorphisme σ	$\sigma(\zeta_3)$	$\sigma(\sqrt{2})$
id	ζ_3	$\sqrt{2}$
σ_1	ζ_3^2	$\sqrt{2}$
σ_2	ζ_3	$-\sqrt{2}$
$\sigma_3 = \sigma_1\sigma_2$	ζ_3^2	$-\sqrt{2}$





Exercice 6.
Soit F un corps de caractéristique p et L/F une extension non séparable. Par définition, cela signifie qu'il existe un polynôme $P \in F[X]$ irréductible tel que P ait une racine multiple dans L. En particulier, on doit avoir $P' = 0$ (comme P a une racine multiple $a \in L$, le polynôme $(X - a)$ divise à la fois P et P′ qui ne sont donc pas premiers entre eux ; mais comme P est irréductible sur F, le seul polynôme de F[X] de degré $< \deg P$ avec lequel P ne soit pas premier est le polynôme nul).
D'après l'exercice 4 du TD 3, il existe donc $Q \in F[X]$ tel que $P = Q(X^p)$. En particulier, le degré de P est un multiple de p. Une racine $a \in L$ de P a donc un degré $[F[a] : F] = \deg P$ multiple de p. En particulier, d'après le théorème de la base télescopique, $[L : F]$ est un multiple de p.
On a montré que le degré de toute extension inséparable est un multiple de la caractéristique. C'est la contraposée du résultat demandé par l'énoncé.

Exercice 7.
On va utiliser le résultat principal de l'exercice 4 du TD 4 : si L/K est une extension algébrique et que $A \subseteq K$ est un anneau dont K est le corps des fractions, alors $s \in L$ est entier sur A si et seulement si son polynôme minimal sur K est à coefficients dans l'anneau $A_K = \left\{ s \in K \,\middle|\, s \text{ est entier sur } A \right\}$.
En particulier, $s \in \mathbf{Q}(\sqrt{2}, i)$ est entier sur $\mathbf{Z}$ si et seulement si son polynôme minimal sur $\mathbf{Q}$ est dans $\mathbf{Z}[X]$. Mais ce critère n'est pas très pratique car le polynôme minimal de s est en général de degré 4.
Nous allons utiliser les extensions intermédiaires : un élément $s \in \mathbf{Q}(\sqrt{2}, i)$ est entier sur $\mathbf{Z}$ si et seulement s'il l'est sur $\mathbf{Z}[\sqrt{2}]$. En effet, $\mathbf{Z}[\sqrt{2}]$ est entier sur $\mathbf{Z}$ donc si s est entier sur $\mathbf{Z}[\sqrt{2}]$, il l'est sur $\mathbf{Z}$, la réciproque étant tautologique.
En cours, il a été démontré que $\mathbf{Z}[\sqrt{2}]$ est l'ensemble des éléments entiers sur $\mathbf{Z}$ de son corps des fractions $\mathbf{Q}(\sqrt{2})$. En particulier, c'est un anneau intégralement clos. Un élément $s \in \mathbf{Q}(\sqrt{2}, i)$ est donc entier sur $\mathbf{Z}$ si et seulement si son polynôme minimal sur $\mathbf{Q}(\sqrt{2})$ est à coefficients dans $\mathbf{Z}[\sqrt{2}]$.
Puisque $(1, \sqrt{2}, i, i\sqrt{2})$ est une $\mathbf{Q}$-base de $\mathbf{Q}(\sqrt{2}, i)$, on peut écrire l'élément $s \in \mathbf{Q}(\sqrt{2}, i)$ sous la forme

$$s = \left(x + y\sqrt{2}\right) + \left(z + w\sqrt{2}\right) i.$$

Son polynôme minimal sur $\mathbf{Q}(\sqrt{2})$ est

$$X^2 - 2(x+y\sqrt{2})X + (x+y\sqrt{2})^2 + (z+w\sqrt{2})^2 = X^2 - 2(x+y\sqrt{2})X + \left[(x^2+2y^2+z^2+2x^2) + 2(xy+zw)\sqrt{2}\right]$$

donc

$$\left(x + y\sqrt{2}\right) + \left(z + w\sqrt{2}\right) i \text{ est entier sur } \mathbf{Z} \text{ si et seulement si } \begin{cases} 2x, 2y \in \mathbf{Z} \\ x^2 + 2y^2 + z^2 + 2w^2 \in \mathbf{Z} \\ 2(xy + zw) \in \mathbf{Z}. \end{cases}$$

Ces équations entraînent que x, y, z et w sont des multiples (dans toute la suite, *multiple* veut dire *multiple entier*) de 1/2. En effet, les première et troisième conditions entraînent que zw est un multiple de 1/4. Mais w ne peut pas être de la forme $k/4$ avec k impair : cela entraînerait z entier d'après ce que l'on vient de dire et le 8 au dénominateur dans l'expression de $2w^2$ ne pourrait pas se simplifier (x^2, y^2 et z^2 étant alors tous des multiples de 1/4), provoquant une contradiction dans la deuxième condition. Pour la même raison, z ne peut pas être de la forme $k/4$ avec k impair et z comme w sont nécessairement des multiples de 1/2.
Autrement dit, l'ensemble des éléments de $\mathbf{Q}(\sqrt{2}, i)$ entiers sur $\mathbf{Z}$ est

$$\left\{ \frac{\left(\xi + \eta\sqrt{2}\right) + \left(\zeta + \omega\sqrt{2}\right) i}{2} \,\middle|\, \xi, \eta, \zeta, \omega \in \mathbf{Z}, \xi^2 + 2\eta^2 + \zeta^2 + 2\omega^2 \equiv 0 \pmod 4, \text{ et } \xi\eta + \zeta\omega \equiv 0 \pmod 2 \right\}.$$

La première congruence, réduite modulo 2, entraîne que $\xi + \zeta \equiv \xi^2 + \zeta^2 \equiv 0 \pmod 2$ donc $\xi \equiv \zeta \pmod 2$. En outre, on ne peut pas avoir ξ et ζ impairs, car la deuxième congruence impliquerait

alors $\eta + \omega \equiv 0 \pmod 2$ ou encore $\eta \equiv \omega \pmod 2$. Que ces nombres soient pairs ou impairs, on aurait alors $\xi^2 + 2\eta^2 + \zeta^2 + 2\omega^2 \equiv 2 \pmod 4$, contredisant la première congruence.
On a donc $\xi \equiv \zeta \equiv 0 \pmod 2$. La deuxième congruence est donc toujours satisfaite, et la première est équivalente à $2\eta^2 + 2\omega^2 \equiv 0 \pmod 4$, ce qui revient à demander $\eta \equiv \omega \pmod 2$.
Autrement dit, les entiers de $\mathbf{Q}(\sqrt{2}, i)$ sont les éléments de

$$\left\{ x + iz + \frac{\eta + i\omega}{2}\sqrt{2} \,\middle|\, x, \eta, z, \omega \in \mathbf{Z} \text{ et } \eta \equiv \omega \pmod 2 \right\} = \mathbf{Z}1 \oplus \mathbf{Z}i \oplus \mathbf{Z}\sqrt{2} \oplus \mathbf{Z}\left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i\right).$$

Remarque. On reconnaît $\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i = \zeta_8$. On peut d'ailleurs montrer que l'anneau que nous avons trouvé est égal à $\mathbf{Z}[\zeta_8]$: il suffit de constater que

$$i = \zeta_4 = \zeta_8^2 \text{ et } \sqrt{2} = \zeta_8 - i\zeta_8.$$

C'est d'ailleurs une conséquence d'un résultat plus général (et plus difficile) : l'ensemble des éléments de $\mathbf{Q}(\zeta_n)$ entiers sur $\mathbf{Z}$ est exactement l'anneau $\mathbf{Z}[\zeta_n]$. Ici, on aurait pu remarquer dès le début que $\mathbf{Q}(\sqrt{2}, i) = \mathbf{Q}(\zeta_8)$.

On détermine de la même façon l'anneau des entiers de $\mathbf{Q}(\sqrt{2}, \sqrt{3})$: un élément $s = (x + y\sqrt{3}) + (z + w\sqrt{3})\sqrt{2}$ est entier si et seulement si son polynôme minimal sur $\mathbf{Q}(\sqrt{2})$, à savoir

$$\mathrm{X}^2 - 2(x + y\sqrt{3})\mathrm{X} + \left[\left(x^2 + 3y^2 - 2z^2 - 6w^2\right) + 2\left(xy - 2zw\right)\sqrt{3}\right],$$

est à coefficients dans $\mathbf{Z}[\sqrt{3}]$. On a donc

$$s = \left(x + y\sqrt{3}\right) + \left(z + w\sqrt{3}\right)\sqrt{2} \text{ est entier sur } \mathbf{Z} \text{ si et seulement si } \begin{cases} 2x, 2y \in \mathbf{Z} \\ x^2 + 3y^2 - 2z^2 - 6w^2 \in \mathbf{Z} \\ 2(xy - 2zw) \in \mathbf{Z}. \end{cases}$$

On montre d'une façon comparable à l'exemple précédent que tous les coefficients en jeu sont des multiples de 1/2 et on analyse de la même façon les congruences modulo 2 et 4 que l'on obtient. Tout compte fait, on obtient comme ensemble d'entiers

$$\left\{ x + y\sqrt{3} + \frac{\zeta + \omega\sqrt{3}}{2}\sqrt{2} \,\middle|\, x, y, \zeta, \omega \in \mathbf{Z} \text{ et } \zeta \equiv \omega \pmod 2 \right\} = \mathbf{Z}1 \oplus \mathbf{Z}\sqrt{3} \oplus \mathbf{Z}\sqrt{2} \oplus \mathbf{Z}\frac{1 + \sqrt{3}}{2}\sqrt{2}.$$

Exercice 8.
Le nombre $3 + \sqrt{5}$ est un *nombre de Pisot* : c'est un nombre réel entier sur $\mathbf{Z}$ dont le polynôme minimal (ici, $\mathrm{X}^2 - 6\mathrm{X} + 4$) a pour autres racines des nombres complexes de module < 1 (ici, $3 - \sqrt{5}$).
Les puissances d'un nombre de Pisot se rapprochent exponentiellement rapidement des nombres entiers : la suite $u_n = (3 + \sqrt{5})^n + (3 - \sqrt{5})^n$ est la solution de l'équation de récurrence

$$u_{n+2} = 6u_{n+1} - 4u_n, \qquad u_0 = 2, u_1 = 6$$

et est donc entière pour tout $n \in \mathbf{N}$. Mais, comme $0 < 3 - \sqrt{5} < 1$, on a $\forall n \geq 1, u_n - 1 < (3 + \sqrt{5})^n < u_n$.
Cela implique

$$\forall n \in \mathbf{N}, \left\lfloor (3 + \sqrt{5})^n \right\rfloor = u_n - 1.$$

Ainsi, pour calculer ce que demande l'exercice, il suffit de calculer le résidu modulo 1 000 de la suite (u_n), c'est-à-dire la suite $(\overline{u}_n)$ définie par la même récurrence, mais interprétée dans $\mathbf{Z}/1\,000\mathbf{Z}$.

C'est évidemment beaucoup plus facile, car d'après le principe des tiroirs, la suite $(\overline{u}_n)$ est nécessairement périodique à partir d'un certain rang (inférieur à 1 000 000). Ce rang et la période sont aisément déterminables à l'aide d'un ordinateur. En particulier, on peut obtenir la valeur de $\overline{u}_n$ pour des valeurs démesurément grandes de n (pour peu qu'on sache quelle est le résidu de n modulo la période de la suite) pour lesquelles le calcul direct de u_n ou $(3+\sqrt{5})^n$ ne serait pas possible. Dans le cas donné par l'exercice, si je ne me suis pas trompé dans le programme, on obtient que

$$\forall n \geq 3, \overline{u}_n = \overline{u}_{100+n}.$$

En particulier, $\overline{u}_{10^{100}} = \overline{u}_{100} = \overline{752}$.
La partie entière de $(3+\sqrt{5})^{10^{100}}$ finit donc par les chiffres 751.