Correction Examen 2ème Session 2019/2020
MU4MA002 - Algèbre et théorie de Galois
Anna Cadoret

Exercice 1.

(1) (a) Soit $(M_1^\#, f_1^\#) \leq (M_2^\#, f_2^\#) \leq \cdots \leq (M_a^\#, f_a^\#) \leq \cdots$ une suite croissante d'éléments de $\mathcal{E}$. Comme $M' \subset M_1^\# \subset M_2^\# \subset \cdots \subset M$ sont des sous-A-modules de M contenant M', $M' \subset M^\# := \cup_{a\geq 1} M_a^\# \subset M$ est encore un sous-A-module de M contenant M'. Définissons $f^\# : M^\# \to N$ de la façon suivante. Pour tout $m \in M^\#$ et $a \geq 1$ tel que $m \in M_a^\#$ on pose $f^\#(m) = f_a^\#(m)$; la propriété que $a \leq b$ implique , $f_a^\# =, f_b^\#|_{M_a^\#}$ assure que cette définition ne dépend pas du choix de $a \geq 1$ tel que $m \in M_a^\#$. On a donc une application $f^\# : M^\# \to N$ bien définie, qui vérifie par construction $f^\#|_{M_a} = f_a^\#$. En particulier c'est un morphisme de A-modules. Cela montre que $(\mathcal{E}, \leq)$ est un ensemble ordonné inductif; il est aussi non-vide puisqu'il contient (M, f). Par le Lemme de Zorn, il existe $(M^\#, f^\#) \in \mathcal{E}$ tel que pour tout $(M^\flat, f^\flat) \in \mathcal{E}$, $(M^\flat, f^\flat) \leq (M^\#, f^\#)$. Si $M^\# = M$, on a gagné. Sinon, montrons qu'on a une contradiction. Fixons $m \in M \setminus M^\#$.

(b) Notons $\lambda : A \to M$ le morphisme de A-modules défini par $\lambda(a) = a \cdot m$. Soit $I := \{a \in A \mid am \in M^\#\}$. C'est un idéal de A car c'est l'image inverse du sous A-module $M^\# \subset M$ par $\lambda : A \to M$. Par définition $\lambda(I) \subset M^\#$ donc on dispose de l'application $g = f^\# \circ \lambda|_I^{M^\#} : I \to N$, qui est un morphisme de A-modules comme composé de morphismes de A-modules.

(c) Par hypothèse, il existe un morphisme de A-modules $g_0^\# : A \to N$ tel que $g_0^\#|_I = g$. Par propriété universelle de la somme directe, on dispose donc d'un morphisme de A-modules $f^\# \oplus g_0^\# : M^\# \oplus A \to N$, $m^\# \oplus a \mapsto f^\#(m^\#) + g_0^\#(a)$. Si on note $p : M^\# \oplus A \twoheadrightarrow M^\# + Am$, $m^\# \oplus a \mapsto m^\# + am$ le morphisme canonique, pour tout $m^\# \oplus a \in \ker(p)$ on a $m^\# = -am$ donc $a \in I$, ce qui implique $g_0^\#(am) = g^\#(am) = f^\#(am) = -f^\#(m^\#)$. Autrement dit, $\ker(p) \subset \ker(f^\# \oplus g_0^\#)$. Le morphisme $f^\# \oplus g_0^\# : M^\# \oplus A \to N$ passe donc au quotient en un morphisme $g^\# : M^\# \oplus A/\ker(p) = M^\# + Am \to N$. Par construction $g^\#|_{M^\#} = f^\#$. Par maximalité de $(M^\#, f^\#)$ on doit donc avoir $M^\# = M^\# + Am$ i.e. $m \in M^\#$.

(2) Utilisons le critère de la question (2). Pour tout idéal I de A et pour tout morphisme de A-modules $f : I \to K$ on veut construire un morphisme de A-modules $f^\# : A \to K$ tel que $f^\#|_I = f$. Si un tel $f^\# : A \to K$ existe, on a nécessairement pour tout $0 \neq a \in A$, $f^\#(a) = af^\#(1)$ ce qui se réécrit aussi $f^\#(1) = a^{-1}f^\#(a)$ puisque A est intègre. Or pour tout $0 \neq a, b \in I$ on a $af(b) - bf(a) = f(ab - ab) = 0$ i.e. $a^{-1}f(a) = b^{-1}f(b) = x$. On peut donc définir $f^\# : A \to K$ par $f^\#(a) = ax$, $a \in A$.

(3) Supposons que A est principal et que ce n'est pas un corps.

(a) A n'est jamais un A-module injectif car si $p \in A$ est premier on ne peut pas prolonger à A l'inverse $f : Ap \to A$ de l'isomorphisme de A-modules $- \cdot p : A \tilde{\to} Ap$, $a \mapsto ap$. En effet, si un tel prolongement $f^\# : A \to A$ existait, on devrait avoir $1 = f(p) = f^\#(p) = pf^\#(1) \in Ap$: contradiction.

(b) - N injectif $\Rightarrow$ N divisible: Pour tout $n \in N$, $0 \neq a \in A$ considérons l'inclusion canonique de A-modules $\iota : Aa \to A$ et le morphisme de A-modules $f : Aa \to N$ défini comme la composée de l'inverse de $A \tilde{\to} Aa$, $\alpha \mapsto \alpha a$ (ici on utilise qu'un anneau principal est intègre!) et de l'unique morphisme de A-modules $A \to N$, $1 \mapsto n$. Autrement dit, on a $f(\alpha a) = \alpha n$. Puisque N est injectif, il existe un morphisme de A-modules $f_\iota : A \to N$ tel que $f_\iota \circ \iota = f$. En particulier, $n = f(a) = f_\iota(a) = af_\iota(1)$ est divisible.

- N divisible $\Rightarrow$ N injectif: Utilisons encore le critère de la question (2). Pour tout idéal I de A et pour tout morphisme de A-modules $f : I \to N$ on veut construire un morphisme de A-modules $f^\# : A \to N$ tel que $f^\#\|_I = f$. Là encore, il suffit de déterminer l'image $f^\#(1)$ de 1. On peut supposer $0 \neq I$ (sinon $f^\# = 0$ convient). Comme A est principal, on a $I = Aa$ pour un certain $0 \neq a \in A$. Comme N est divisible, il existe $n^\# \in N$ tel que $an^\# = f(a)$. On vérifie immédiatement que le morphisme de A-modules $f^\# : A \to N$ défini par $f^\#(a) = an^\#$ convient.

(c) Par le théorème de structure des modules de type fini sur un anneau principal, un module de type fini sur A est de la forme $A^r \oplus A/Ad_1 \oplus \cdots A/Ad_s$ avec $d_1, \ldots, d_s \in A$ non nuls et non inversibles. Or on a déjà vu que A n'était jamais injectif. De même A/Ad_i n'est jamais injectif puisqu'il n'est pas divisible par d_i.

(d) Cela résulte immédiatement du fait qu'un quotient d'un A-module A-divisible est A-divisible.

(4) (a) Supposons d'abord que A est principal. Pour tout A-module M et pour tout $m \in M$, on a le morphisme de A-modules canonique $\iota_m : A \to M$, $a \to am$ donc, par propriété universelle de la somme directe, on a un morphisme de A-modules $p := \oplus_{m\in M}\iota_m : \oplus_{m\in M}A \to M$, qui est surjectif par construction. Consiérons l'inclusion canonique $\iota : \oplus_{m\in M}A \hookrightarrow \oplus_{m\in M}K$. On a $\ker(\oplus_{m\in M}A \overset{\iota}{\hookrightarrow} \oplus_{m\in M}K \twoheadrightarrow (\oplus_{m\in M}K)/\iota(\ker(p))) = \ker(p)$ donc le morphisme de A-modules $\oplus_{m\in M}A \overset{\iota}{\hookrightarrow} \oplus_{m\in M}K \twoheadrightarrow \oplus_{m\in M}/\iota(\ker(p))$ se factorise en un morphisme injectif de A-modules $M\tilde{\to}(\oplus_{m\in M}A)/\ker(p) \hookrightarrow (\oplus_{m\in M}K)/\iota(\ker(p))$. Puisqu'on a supposé A principal, par les questions (2) et (3) (d), $(\oplus_{m\in M}K)/\iota(\ker(p))$ est un A-module injectif.

(b) On ne suppose plus A principal. Soit C un $\mathbb{Z}$-module.

(i) Supposons C est un $\mathbb{Z}$-module injectif. Pour tout morphisme injectif de A-module $u : M' \to M$ et pour tout morphisme de A-module $f : M' \to Hom_{\mathbb{Z}}(A, C)$ on veut construire un morphisme de A-modules $f_u : M \to Hom_{\mathbb{Z}}(A, C)$ tel que $f_u \circ u = f$. Observons que $f : M' \to Hom_{\mathbb{Z}}(A, C)$ définit un morphisme de $\mathbb{Z}$-modules $\tilde{f} : M' \to C$, $m \mapsto f(m)(1)$. Comme C est un $\mathbb{Z}$-module injectif, il existe un morphisme de $\mathbb{Z}$-modules $\tilde{f}_u : M \to C$ tel que $\tilde{f}_u \circ u = \tilde{f}$. Définissons $f_u : M \to Hom_{\mathbb{Z}}(A, C)$ par $f_u(m) : A \to C$, $a \mapsto \tilde{f}_u(am)$. On a par construction pour tout $a \in A$ $f_u \circ u(m')(a) = \tilde{f}_u(au(m')) = \tilde{f}_u(u(am')) = \tilde{f}(am') = f(am)(1) = (a \cdot f)(1) = f(a)$ i.e. $f_u \circ u = f$. On a également pour tout $a \in A$, $\alpha, \beta \in A$ et $m, n \in M$ $f_u(\alpha m + \beta n)(a) = \tilde{f}_u(a(\alpha m + \beta n)) = \tilde{f}_u(a\alpha m + a\beta n) = \tilde{f}_u(a\alpha m) + \tilde{f}_u(a\beta n) = f_u(\alpha m)(a) + f_u(\beta m)(a) = (\alpha \cdot f_u(m) + \beta \cdot f_u(n)(a)$ i.e. $f_u : M \to Hom_{\mathbb{Z}}(A, C)$ est bien un morphisme de A-modules.

(ii) Soit M un A-module. Puisque $\mathbb{Z}$ est principal et en considérant M comme un $\mathbb{Z}$-module, il résulte de 5) (a) qu'il existe un $\mathbb{Z}$-module injectif C et un morphisme injectif de $\mathbb{Z}$-modules $u : M \hookrightarrow C$.

(iii) On vérifie immédiatement que $M \to Hom_{\mathbb{Z}}(A, C)$, $m \mapsto (a \mapsto u(am))$ est un morphisme injectif de A-modules et la conclusion résulte donc de (4) (b) (i).

Exercice 2.

(1) On considère l'application $\tilde{c} : K \times L \to \Omega$, $(x, y) \mapsto xy$. Elle est clairement k-biliniéaire donc se factorise en un morphisme de k-modules $c : K \otimes_k L \to \Omega$. Comme $K \otimes_k L$ est engendré comme k-modules par les éléments de la forme $x \otimes_k y$, $x \in K$, $y \in L$, l'image de c est le sous-k-module de Ω engendré par les éléments de la forme xy, $x \in K$, $y \in L$ i.e. c'est $K \cdot L$. Enfin $c : K \otimes_k L \to \Omega$ est bien un morphisme d'anneaux: par k-bilinéairté il suffit de vérifier que $c(x \otimes y \cdot x' \otimes y') = c(x \otimes y)c(x' \otimes y')$, $x, x' \in K$, $y, y' \in L$ ce qui résulte immédiatement de la construction.

(2) (a) Critère d'Eisenstein en $p = 2$.

(b) On étudie les variations de la fonction réelle $f : t \to t^n - 2$. Si n est pair, f' s'annule en $t = 0$, est < 0 si $t < 0$ et > 0 si $t > 0$ donc, comme $f(0) = -2 < 0$ et f tend vers $+\infty$ en $\pm\infty$, f a exactement deux racines réelles, $\pm\sqrt[n]{2}$. Si n est imppair, f' s'annule en $t = 0$, est > 0 si $t \neq 0$ donc, comme f tend vers $+\infty$ en $+\infty$ et $-\infty$ en $-\infty$, f a exactement une racines réelle, $\sqrt[n]{2}$. Si $n \geq 3$ et n est pair, dans $\mathbb{R}[T]$ on a $T^n - 2 = (T - \sqrt[n]{2})(T + \sqrt[n]{2})P(T)$ avec P sans racines réelles de degré $n - 2 \geq 2$ pair et si n est impair, dans $\mathbb{R}[T]$ on a $T^n - 2 = (T - \sqrt[n]{2})P(T)$ avec P sans racines réelles de degré $n - 1 \geq 2$ pair. Donc, dans les deux cas, les racines de P sont complexes conjuguées. Enfin les $\sqrt[n]{2}\zeta_n^k$, $k = 0, \ldots, n - 1$ sont n racines distinctes de $T^n - 2$ et comme $T^n - 2$ a au plus n racines, ce sont exactement les racines de $T^n - 2$.

(c) Par (2) (a), $[K_n : \mathbb{Q}] = n$. On a $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(\sqrt[12]{2}), \mathbb{Q}(\sqrt[8]{2})$ avec $[\mathbb{Q}(\sqrt[12]{2}) : \mathbb{Q}(\sqrt[4]{2})] = 12/4 = 3$, $[\mathbb{Q}(\sqrt[8]{2}) : \mathbb{Q}(\sqrt[4]{2})] = 8/4 = 2$. Donc

$$[\mathbb{Q}(\sqrt[12]{2}) \cdot \mathbb{Q}(\sqrt[8]{2}) : \mathbb{Q}(\sqrt[4]{2})] = 3[\mathbb{Q}(\sqrt[12]{2}) \cdot \mathbb{Q}(\sqrt[8]{2}) : \mathbb{Q}(\sqrt[12]{2})] = 2[\mathbb{Q}(\sqrt[12]{2}) \cdot \mathbb{Q}(\sqrt[8]{2}) : \mathbb{Q}(\sqrt[8]{2})].$$

En particulier, 3 divise $[\mathbb{Q}(\sqrt[12]{2}) \cdot \mathbb{Q}(\sqrt[8]{2}) : \mathbb{Q}(\sqrt[8]{2})]$. De plus $[\mathbb{Q}(\sqrt[12]{2}) \cdot \mathbb{Q}(\sqrt[8]{2}) : \mathbb{Q}(\sqrt[8]{2})]$ est le degré du polynôme minimal de $\sqrt[12]{2}$ sur $\mathbb{Q}(\sqrt[8]{2})$; il divise donc le degré du polynôme minimal de $\sqrt[12]{2}$ sur $\mathbb{Q}(\sqrt[4]{2})$, qui est $[\mathbb{Q}(\sqrt[12]{2}) \cdot \mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt[4]{2})] = 3$. Donc $[\mathbb{Q}(\sqrt[12]{2}) \cdot \mathbb{Q}(\sqrt[8]{2}) : \mathbb{Q}(\sqrt[4]{2})] = 6$

et $[\mathbb{Q}(\sqrt[12]{2})\cdot\mathbb{Q}(\sqrt[8]{2}):\mathbb{Q}]=6[\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}]=24$.
De même, $\mathbb{Q}(\sqrt{2})\subset\mathbb{Q}(\sqrt[12]{2}),\mathbb{Q}(\zeta_8\sqrt[8]{2})$ avec $[\mathbb{Q}(\sqrt[12]{2}):\mathbb{Q}(\sqrt{2})]=12/2=6$, $[\mathbb{Q}(\zeta_8\sqrt[8]{2}):\mathbb{Q}(\sqrt{2})]=8/2=4$. Donc $[\mathbb{Q}(\sqrt[12]{2})\cdot\mathbb{Q}(\zeta_8\sqrt[8]{2}):\mathbb{Q}(\sqrt{2})]=6[\mathbb{Q}(\sqrt[12]{2})\cdot\mathbb{Q}(\zeta_8\sqrt[8]{2}):\mathbb{Q}(\sqrt[12]{2})]$. De plus $[\mathbb{Q}(\sqrt[12]{2})\cdot\mathbb{Q}(\zeta_8\sqrt[8]{2}):\mathbb{Q}(\sqrt[12]{2})]$ est le degré du polynôme minimal de $\zeta_8^8\sqrt{2}$ sur $\mathbb{Q}(\sqrt[12]{2})$, lequel divise donc le polynôme minimal de $\zeta_8\sqrt[8]{2}$ sur $\mathbb{Q}(\sqrt{2})$ à savoir $T^4+\sqrt{2}$. Mais en fait, $T^4+\sqrt{2}$ est aussi irréductible sur dans $\mathbb{R}[T]$ (car ses facteurs irréductibles dans $\mathbb{C}[T]$ sont les $T-\zeta_4^k\zeta_8\sqrt[8]{2}$, $k=0,1,2,3$) donc a fortiori dans $\mathbb{Q}(\sqrt[12]{2})[T]$. On en déduit que $[\mathbb{Q}(\sqrt[12]{2})\cdot\mathbb{Q}(\zeta_8\sqrt[8]{2}):\mathbb{Q}(\sqrt[12]{2})]=4$ donc $[\mathbb{Q}(\sqrt[12]{2})\cdot\mathbb{Q}(\zeta_8\sqrt[8]{2}):\mathbb{Q}]=48$.
On a $K_{12}\tilde{\to}\mathbb{Q}(\sqrt[12]{2})\subset\mathbb{C}$ et $K_8\tilde{\to}\mathbb{Q}(\sqrt[8]{2}),\mathbb{Q}(\zeta_8\sqrt[8]{2})\subset\mathbb{C}$. On voit donc que deux $\mathbb{Q}$-plongements différents de K_8 dans $\mathbb{C}$ donne des extensions de $\mathbb{Q}$ différentes.

(3) Puisque par (1) (a) on sait que $c:K\otimes_k L\to K\cdot L$ est un morphisme de k-modules surjectifs, (b) $\Leftrightarrow$ (c). Par multiplicativité du degré on a aussi $[K\cdot L:k]=[K\cdot L:L][L:k]$ donc (c) $\Leftrightarrow$ (d). Clairement (b) $\Rightarrow$ (a). Inversement, si $K\otimes_k L$, son seul idéal strict est 0. Or comme $c:K\otimes_k L\to K\cdot L$ est un morphisme surjectif de k-algèbres, son noyau est idéal strict de $K\otimes_k L$. La propriété (a) ne fait pas intervenir les k-plongements $K\hookrightarrow\Omega$, $L\hookrightarrow\Omega$.

(4) On a $[K\cdot L:k]=[K\cdot L:L][L:k]=[K\cdot L:K][K:k]$. Comme $[K:k]$ et $[L:k]$ sont premiers entre eux, on en déduit que $[K:k][L:k]$ divise $[K\cdot L:k]$. Mais on a toujours $[K\cdot L:k]\leq[K:k][L:k]$ (par exemple par (1)). Donc $[K\cdot L:k]=[K:k][L:k]$ et on conclut par la caractérisation (3) (c).

(5) On peut remplacer k par $K\cap L$ dans la question (1). Donc $[K\cdot L:K\cap L]\leq[K:K\cap L][L:K\cap L]$. Mais si K/k, L/k sont linéairement indépendantes sur k, on a par (3) $[K:K\cap L][L:K\cap L][K\cap L:k]\geq[K\cdot L:K\cap L][K\cap L:k]=[K\cdot L:k]=[K:k][L:k]=[K:K\cap L][L:K\cap L][K\cap L:k]^2$ donc $[K\cap L:k]\leq 1$. Supposons de plus K/k galoisienne. Comme K/k est en particulier séparable, on peut écrire $K=k(\alpha)/k$. Notons $P\in k[T]$ le polynôme minimal de α sur k. Alors P est encore irréductible sur L. Sinon, on aurait $P=P_1P_2$ dans $L[T]$ avec P_1,P_2 de degré ≥ 2 et au moins l'un des coefficients - disons a_i - de P_i dans $L\setminus k$. Par contre, comme K/k est normale, et que les coefficients de P_i sont polynomiaux en les racines de P, ils sont dans K. Donc $a_i\in K\cap L=k$: contradiction.

(6) Ecrivons encore $K=k(\alpha)/k$ et notons P le polynôme minimal de α sur k; il est séparable puisque K/k est galoisienne. Alors comme $L[T]/P\tilde{\to}K[T]/P\otimes_k L\xrightarrow{c}K\cdot L$ est un corps, P est encore irréductible sur L. Par ailleurs, puisque K/k est normale, K - donc a fortiori $K\cdot L$ contient toutes les racines de P. Donc $K\cdot L/L$ est galoisienne comme corps de décomposition de P sur L. Comme K/k est normale, la restriction à K induit un morphisme canonique de groupes $Gal(K\cdot L|L)\to Gal(K|K\cap L)=Gal(K|k)$, qui est clairement injectif donc un isomorphisme puisque $|Gal(K\cdot L|L)|=[K\cdot L:L]=[K:k]=|Gal(K|k)|$ par (3) (d).

(7) Si K/k, L/k sont galoisiennes on a $K\cdot L/L$ séparable (car galoisienne par (6)) et L/k séparable (car galoisienne) donc $K\cdot L/k$ séparable. Par ailleurs, si on note $\overline{k}$ la clôture algébrique de k dans Ω, pour tout $\sigma\in Aut(\overline{k}|k)$ on a $\sigma(K)=K$ et $\sigma(L)=L$ puisque K/k et L/k sont normales. Mais par définition de $K\cdot L$, cela implique $\sigma(K\cdot L)=K\cdot L$. Donc $K\cdot L/k$ est aussi normale donc galoisienne. Les restrictions à K et à L induisent un morphisme canonique de groupes $Gal(K\cdot L|k)\to Gal(K|k)\times Gal(L|k)$, $\sigma\mapsto(\sigma|_K,\sigma|_L)$, qui est clairement injectif donc un isomorphisme puisque $|Gal(K\cdot L|k)|=[K\cdot L:k]=[K:k][L:k]=|Gal(K|k)||Gal(L|k)|=|Gal(K|k)\times Gal(L|k)|$ par (3) (c).

Exercice 3.

(1) Soit k une extension galoisienne de $\mathbb{Q}$. Supposons que k n'est pas totalement réelle i.e. qu'il existe un plongement $\rho:k\hookrightarrow\overline{\mathbb{Q}}$ tel que $\iota\circ\rho\neq\rho$. Comme $k/\mathbb{Q}$ est galoisienne, $Hom(k,\overline{\mathbb{Q}})=\rho\circ Gal(k|\mathbb{Q})=\{\rho\circ\sigma\mid\sigma\in Gal(k|\mathbb{Q})\}$. Or pour $\sigma\in Gal(k|\mathbb{Q})$ on a $\iota\circ\rho\circ\sigma=\rho\circ\sigma$ si et seulement si $\iota\circ\rho=\rho$ donc ι agit sans point fixe sur $Hom(k,\overline{\mathbb{Q}})$ i.e. k est totalement imaginaire.

(2) Comme $k/\mathbb{Q}$ est séparable (caractéristique 0) $[k:\mathbb{Q}]=|Hom(k,\overline{\mathbb{Q}})|$. Et comme $\langle\iota\rangle\simeq\mathbb{Z}/2$ agit sans point fixe sur $Hom(k,\overline{\mathbb{Q}})$, toute les orbites de $\langle\iota\rangle\simeq\mathbb{Z}/2$ opérant sur $Hom(k,\overline{\mathbb{Q}})$ sont de longueur 2 donc $|Hom(k,\overline{\mathbb{Q}})|=2|Hom(k,\overline{\mathbb{Q}})/\langle\iota\rangle|$ est paire.

(3) Il suffit d'exhiber un polynôme irréductible sur $\mathbb{Q}$ ayant au moins une racine réelle et une racine complexe non réelle. Par exemple l'extension $k=:\mathbb{Q}[T]/T^3-2$ de $\mathbb{Q}$ convient.

(4) On peut utiliser le fait qu'on a un morphisme surjectif canonique de $\mathbb{Q}$-algèbres $c:k_1\otimes_{\mathbb{Q}}k_2\twoheadrightarrow k_1\cdot k_2$ (cf. Exercice 2, (1)) qui induit une injection $f:=-\circ c:Hom(k_1\cdot k_2,\overline{\mathbb{Q}})\hookrightarrow Hom(k_1\otimes_k k_2,\overline{\mathbb{Q}})$, où $Hom(k_1\otimes_k k_2,\overline{\mathbb{Q}})$ désigne l'ensemble des morphismes de $\mathbb{Q}$-algèbres $k_1\otimes_k k_2\to\overline{\mathbb{Q}}$. Par ailleurs, les morphismes canoniques de $\mathbb{Q}$-algèbres $u_1:k_1\hookrightarrow k_1\otimes_{\mathbb{Q}}k_2$, $x_1\mapsto x_1\otimes 1$, $u_2:k_2\hookrightarrow k_1\otimes_{\mathbb{Q}}k_2$, $x_2\mapsto 1\otimes x_2$

induisent une injection $g := (- \circ u_1, - \circ u_2) : Hom(k_1 \otimes_k k_2, \overline{\mathbb{Q}}) \hookrightarrow Hom(k_1, \overline{\mathbb{Q}}) \times Hom(k_2, \overline{\mathbb{Q}})$. On obtient donc une injection $g \circ f : Hom(k_1 \cdot k_2, \overline{\mathbb{Q}}) \hookrightarrow Hom(k_1, \overline{\mathbb{Q}}) \times Hom(k_2, \overline{\mathbb{Q}})$. Par construction on a $g \circ f(\iota \cdot \rho) = \rho \cdot g \circ f(\rho)$ (où on fait agir $Aut(\overline{\mathbb{Q}}|Q)$ sur $Hom(k_1, \overline{\mathbb{Q}}) \times Hom(k_2, \overline{\mathbb{Q}})$ diagonalement) donc l'ensemble des points fixes de ι sur $Hom(k_1 \cdot k_2, \overline{\mathbb{Q}})$ est contenu dans l'ensemble des points fixes de ι sur $Hom(k_1, \overline{\mathbb{Q}}) \times Hom(k_2, \overline{\mathbb{Q}})$. Mais si k_1, k_2 sont totalement réelles (resp. totalement imaginaires), ι agit trivialement (resp. sans point fixe) sur $Hom(k_1, \overline{\mathbb{Q}}) \times Hom(k_2, \overline{\mathbb{Q}})$, d'où la conclusion. Soit T la propriété d'être totalement réel ou totalement imaginaire. Soit $k^T \subset k$ une sous-extension T de degré maximal sur $\mathbb{Q}$ et soit $k' \subset k$ une extension T quelconque. Comme $k^T \subset k' \cdot k^T$ et que $k' \cdot k^T$ est encore T, on a nécessairement $k^T = k' \cdot k^T$ par maximalité de $[k^T : \mathbb{Q}]$ i.e. $k' \subset k^T$.

(5) (i) $\Rightarrow$ (ii): Comme k/k^+ est séparable de degré 2, elle est galoisienne de groupe $\mathbb{Z}/2$. Notons $\iota_k \in Gal(k|k^+)$ l'élement non trivial. Comme $k^- = k$ on doit avoir $\iota \circ \rho \neq \rho$ pour tout $\rho \in Hom(k, \overline{\mathbb{Q}})$. Comme k^+ est totalement réelle, on doit avoir $\iota \circ \rho|_{k^+} = \rho|_{k^+}$ i.e. $\iota \in Aut(\overline{\mathbb{Q}}|\rho(k^+))$. Comme $\rho(k)/\rho(k^+)$ est de degré 2, elle est en particulier normale donc, $\iota(\rho(k)) = \rho(k)$. Notons encore $\rho : k \to \rho(k)$ et $\iota : \rho(k) \tilde{\to} \rho(k)$. On a par définition $\rho^{-1}\iota\rho \in Gal(k|k^+)$ non trivial donc, nécessairement $\rho^{-1}\iota\rho = \iota_k$.
(ii) $\Rightarrow$ (i): Puisque $\iota_k \neq Id$, on a $\iota \circ \rho = \rho \circ \iota_k \neq \rho$ pour tout $\rho \in Hom(k, \overline{\mathbb{Q}})$ donc $k^- = k$. La condition $\iota \circ \rho = \rho \circ \iota_k$ pour tout $\rho \in Hom(k, \overline{\mathbb{Q}})$ dit aussi que $k^{\iota_k} \subset k$ est totalement réelle. Donc $k^{\iota_k} \subset k^+$. Mais comme $k^+ \subsetneq k = k^-$ et $[k : k^{\iota_k}] = 2$, on doit forcément avoir $k^{\iota_k} = k^+$.

(6) Soit k un corps CM. Par définition k est totalement imaginaire donc ι agit sans point fixe sur $Hom(k, \overline{\mathbb{Q}})$. Comme ι est d'ordre 2, cela signifie que toutes les orbites de ι sur $Hom(k, \overline{\mathbb{Q}})$ sont de cardinal 2. Un type sur k est la donnée d'un sous-ensemble $\Phi \subset Hom(k, \overline{\mathbb{Q}})$ contenant exactement un représentant de chaque orbite de ι. Concrètementment cela signifie que $Hom(k, \overline{\mathbb{Q}})$ s'écrit comme réunion disjointe $Hom(k, \overline{\mathbb{Q}}) = \Phi \sqcup \iota\Phi$.

(a) Pour tout $\sigma \in Aut(\overline{\mathbb{Q}})$, on a $Hom(k, \overline{\mathbb{Q}}) = \sigma Hom(k, \overline{\mathbb{Q}}) = \sigma\Phi \sqcup \sigma\iota\Phi$. Par ailleurs, pour tout $\rho \in \Phi$ $\sigma \circ \iota \circ \rho = \sigma \circ \rho \circ \iota_k = (\sigma \circ \rho) \circ \iota_k = \iota \circ (\sigma \circ \rho)$ i.e. $\sigma\iota\Phi = \iota\sigma\Phi$

(b) Cours.

(c) (i) C'est le lemme de Dedekind. On rappelle l'argument. On se fixe une RDL *de longueur minimale* $\sum_{1 \leq i \leq r} \lambda_i \rho_i = 0$ avec $0 \neq \lambda_i \in \hat{k}$. Pour tout $x, y \in k$, on a $\sum_{1 \leq i \leq r} \lambda_i \rho_i(xy) = 0 = \sum_{1 \leq i \leq r} \lambda_i \rho_i(x)\rho_i(y)$ donc pour tout $x \in k$, $\sum_{1 \leq i \leq r} \lambda_i \rho_i(x)\rho_i = 0$. Comme $\rho_1 \neq \rho_2$, on peut choisir $0 \neq x$ tel que $\rho_1(x) \neq \rho_2(x)$. On a alors

$$0 = \sum_{1 \leq i \leq r} \lambda_i \rho_i(x)\rho_i - \rho_1(x) \sum_{1 \leq i \leq r} \lambda_i \rho_i = \sum_{2 \leq i \leq r} \lambda_i (\rho_i(x) - \rho_1(x))\rho_i,$$

qui est une RDL de longueur $< r$: contradiction.

(ii) Pour tout $\sigma \in S_\Phi$ on a $\sigma x_\Phi = \sum_{\rho \in \Phi} \sigma\rho(x) = \sum_{\rho \in \sigma\Phi} \rho(x) = x_\Phi$ par définition de S_Φ. Donc $k'_\Phi \subset k_\Phi$. Inversement, pour tout $\sigma \in Gal(\hat{k}|k'_\Phi)$ on a par définition $\sum_{\rho \in \Phi} \sigma\rho = \sum_{\rho \in \Phi} \rho$ donc par (2) (c) (i), $\sigma\Phi = \Phi$ i.e. $\sigma \in S_\Phi$. On en déduit, par la correspondance de Galois, $k_\Phi = \hat{k}^{S_\Phi} \subset \hat{k}^{Gal(\hat{k}|k'_\Phi)} = k'_\Phi$.

(iii) Notons $\hat{k}_\Phi/\mathbb{Q}$ la clôture galoisienne de $k_\Phi/\mathbb{Q}$ dans $\overline{\mathbb{Q}}$ et pour tout $\rho \in Hom(k_\Phi, \overline{\mathbb{Q}})$, notons $\hat{\rho} \in Hom(\hat{k}_\Phi, \overline{\mathbb{Q}}$ un porlongement de ρà $\hat{k}_\Phi$. On a $\iota\rho(x_\Phi) = \sum_{\varphi \in \Phi} \iota(\hat{\rho}\phi)(x) = \sum_{\varphi \in \Phi} (\hat{\rho}\phi)\iota_k(x) = \rho(\sum_{\varphi \in \Phi} (\phi\iota_k)(x)) = \rho((\iota_k x)_\Phi) \in \rho(k_\Phi)$. Donc comme les x_Φ, $x \in k$ engendrent k_Φ, on a bien $\iota\rho(k_\Phi) = \rho(k_\Phi)$. Par contre, on a également $\rho((\iota_k x)_\Phi) = \rho(x_{\iota\Phi})$ or, par (2) (c) (i), $\sum_{\phi \in \Phi} \phi \neq \sum_{\phi \in \Phi} \iota\phi$ (puisque $\Phi \cap \iota\Phi = \emptyset$!) donc il existe $x \in k$ tel que $x_\Phi \neq x_{\iota\Phi}$ donc $\rho(x_\Phi) \neq \rho(x_{\iota\Phi})(= \iota\rho(x_\Phi))$. Cela montre que $\iota\rho \neq \rho$. La condition (1) (e) (ii) est donc bien vérifiée.

anna.cadoret@imj-prg.fr
IMJ-PRG- Sorbonne Université.