Corrigé de la Feuille d'exercices 7

Exercice 1.

(i) Soit $x \in K$ non réel. Alors $K = \mathbf{R}[x]$. Soit $\pi_x(X) \in \mathbf{R}[X]$ le polynôme minimal de x sur $\mathbf{R}$. Il est irréductible de degré 2, et donc de la forme

$$\pi_x(X) = (X-a)^2 + b$$

avec $a, b \in \mathbf{R}$ et $b > 0$. Alors

$$K \simeq \mathbf{R}[X]/((X-a)^2+b) \simeq \mathbf{R}[Y]/(Y^2+b) \simeq \mathbf{R}[Z]/(Z^2+1) \simeq \mathbf{C}.$$

(ii) Soit $x \in K$ non réel et π_x sont polynôme minimal sur $\mathbf{R}$. Alors $[\mathbf{R}[x] : \mathbf{R}] = \deg(\pi_x)$ divise $[K : \mathbf{R}]$, donc $\deg(\pi_x)$ est impair. D'après le théorème des valeurs intermédiaires, un polynôme réel de degré impair a au moins une racine réelle. Comme π_x est irréductible, il est de degré 1. Donc $\pi_x(X) = X - x$ et $x \in \mathbf{R}$, contradiction.

(iii) Supposons que K est une extension de $\mathbf{C}$ de degré 2. Soit $x \in K$ qui n'est pas dans $\mathbf{C}$. Soit π_x le polynôme minimal de x sur $\mathbf{C}$. Comme $K = \mathbf{C}[x]$, on a $deg(\pi_x) = 2$. Or on connait explicitement les racines d'un polynôme complexe de degré 2, et elles sont complexes. Donc π_x ne peut pas être irréductible sur $\mathbf{C}$, contradiction.

(iv) Soit $G = Gal(K/\mathbf{R})$. C'est un groupe fini, écrivons $|G| = 2^\alpha m$ avec m impair. D'après le théorème de Sylow, on a un sous-groupe P de G d'ordre 2^α. Le théorème de Galois s'applique ($\mathbf{R}$ est parfait), et on obtient une sous-extension $\mathbf{R} \subset K_1 \subset K$ telle que $[K_1 : \mathbf{R}] = |G|/|P| = m$ impair, K/K_1 est galoisienne et $Gal(K/K_1) = P$. On travaille à présent dans cette extension (K_1 est parfait comme extension finie d'un corps parfait). On a une suite de sous-groupes distingués dans P

$$P_1 \subset P_2 \subset \cdots P_\alpha = P$$

avec $|P_i| = 2^i$. Le théorème de Galois s'applique, et on obtient une tour de sous-extensions

$$K_1 \subset K_2 \subset \cdots \subset K_{\alpha+1} = K$$

avec $Gal(K/K_i) = P_{\alpha+1-i}$ pour $1 \leq i \leq \alpha$. En particulier, $[K_{i+1} : K_i] = 2$ pour $1 \leq i \leq \alpha$.

(v) Soit k une extension finie de $\mathbf{R}$. Alors on a une extension galoisienne finie $K/\mathbf{R}$ telle que $k \subset K$. On construit une tour comme dans la question précédent. Alors $K_1 = \mathbf{R}$ d'après (ii). Si $n = 1$, $K = \mathbf{R}$. Si $n \geq 2$, $K_2 \simeq \mathbf{C}$ d'après (i). D'après (iii), $n \geq 2$. Donc $K = \mathbf{R}$ ou $K \simeq \mathbf{C}$, ce qui permet de conclure.

Exercice 2.

(i) On a $f([x,y]) = [f(x), f(y)]$ pour tous $x, y \in G$. Donc $f(D(G)) \subset D(G')$.

Si f est une surjection, pour $X, Y \in G'$ on a $x, y \in G$ tels que $X = f(x)$ et $Y = f(y)$. Donc

$$f([x,y]) = [X,Y] \in Im(f).$$

D'où l'égalité.

(ii) Supposons que G est résoluble. Soit $n \geq 1$ tel que $D^n(G) = \{e\}$. Alors $D^n(H) \subset D^n(G) = \{e\}$ donc H est résoluble. De plus $D^n(K)$ est l'image de $D^n(G)$ dans K, donc $D^n(K)$ est trivial et K est résoluble.

Réciproquement, soient $n, m \geq 0$ tels que $D^n(K)$ et $D^m(H)$ sont triviaux. Alors l'image de $D^m(G)$ dans K est $\{e\}$, donc $D^m(G) \subset H$. Ainsi

$$D^{n+m}(G) \subset D^m(H) = \{e\}$$

et G est résoluble.

(iii) Soit $g \in G$ et $\phi_g : G \to G$ défini par $\phi_g(h) = ghg^{-1}$. Alors ϕ_g est un morphisme de groupe, donc $\phi_g(D(G)) \subset D(G)$. Donc $D(G)$ est distingué dans G.

Les assertions suivantes sont équivalentes :

$D(G) \subset H$.

pour $x, y \in G$, $xyx^{-1}y^{-1} \in H$.

pour $x, y \in G$, xy, yx ont même image dans G/H.

G/H est abélien.

(iv) Si G est résoluble, soit n tel que $D^n(G) = \{e\}$. Alors il suffit de poser $G_i = D^{n-i}(G)$.

Réciproquement, si on a une telle suite, on a $D(G_{i+1}) \subset G_i$. Donc par récurrence, $D^i(G) \subset G_{n-i}$ et donc $D^n(G) \subset G_0 = \{e\}$.

(v) On suppose que G est fini.

Comme un groupe cyclique est abélien, l'existence de la suite implique la résolubilité de G comme ci-dessus. On considére une suite comme dans la question précédent. Il suffit donc de montrer que pour $H' \subset H$ deux groupes finis tels que H' est distingué dans H et $D(H) \subset H'$, on a une suite

$$H_0 = H' \subset H_1 \subset \cdots \subset H_N = H$$

telle que H_i est distingué dans H_{i+1} et H_{i+1}/H_i est cyclique. On raisonne par récurrence sur $|H|/|H_0|$. Si $|H| = |H_0|$, c'est clair. En général, soit $x \in H$ qui n'est pas dans H' et soit H_1 le sous-groupe de H engendré par H' et x. Alors H' est distingué dans H_1 et H_1/H' est cyclique engendré par l'image de x. De plus, pour $g \in H$ et $h \in H_1$, on a

$$ghg^{-1}h^{-1} \in H' \subset H_1,$$

et donc

$$ghg^{-1} \in hH_1 \subset H_1.$$

Donc H_1 est distingué dans H, et $D(G) \subset H_1$. On conclut en utilisant l'hypothèse de récurrence pour $H_1 \subset H$.

Exercice 3.

(i) On utilise le (v) de l'exercice précédent avec $G = Gal(K/k)$ fini résoluble. On obtient une suite

$$G_0 = \{e\} \subset G_1 \subset \cdots \subset G_n = G.$$

Comme k est parfait, le théorème de Galois s'applique, et on obtient une tour d'extensions

$$K_0 = k \subset K_1 \subset \cdots \subset K_n = K,$$

avec $Gal(K_{i+1}/K_i) = G_{n-i}/G_{n-i-1}$ cyclique pour $0 \leq i \leq n$. On peut alors appliquer le théorème de Kummer à chaque extension K_{i+1}/K_i (la preuve du théorème de Kummer nécessite seulement que les racines $[K_{i+1} : K_i]$-ième de l'unité soient dans K_i, ce qui est satisfait car $[K_{i+1} : K_i]$ divise $[K : k]$). Chaque $K_{i+1}.K_i$ est donc radicale, et K/k est radicale.

(ii) Les conjugués d'un élément de K sur $k[x]$ sont des conjugués sur k, et sont donc dans K car K/k est galoisienne. De plus, $x \in k[x]$. Donc on a une extension galoisienne.

Maintenant pour $\sigma \in Gal(K[x]/k[x])$, soit $\Psi(\sigma)$ la restriction à K. C'est notamment un morphisme de k-algèbre. Comme K/k est galoisienne, $\Psi(\sigma)$ est à valeur dans K. On obtient donc un morphisme de groupe

$$\Psi : Gal(K[x]/k[x]) \to Gal(K/k).$$

Il est injectif car un élément de $Gal(K[x]/k[x])$ est uniquement déterminé par l'image des éléments de K. Comme $Gal(K/k)$ est résoluble, $Gal(K[x]/k[x])$ l'est également.

(iii) On considère $x_1, \cdots, x_N$ les racines $[K : k]$-ième de l'unité de Ω. On considère l'extension

$$K[x_1, \cdots, x_N]/k[x_1, \cdots, x_N].$$

En appliquant N fois le résultat de (ii), on obtient que c'est une extension galoisienne finie de groupe de Galois résoluble. D'après (i), c'est une extension radicale. De plus, $k[x_1, \cdots, x_N]/k$ est clairement radicale. Donc $K[x_1, \cdots, x_N]/k$ est radicale. Comme

$$k \subset K \subset K[x_1, \cdots, x_N],$$

K est résoluble par radicaux.