TD n°11 : Théorie de Galois, Résolubilité

Exercice 1. [Problème de Galois inverse]

1. Montrer que, pour tout groupe fini G, il existe une extension finie galoisienne de groupe de Galois G.
   Soit p un nombre premier impair, soit m un entier naturel non nul et soit $(n_1, \cdots, n_{p-2})$ un $(p-2)$-uplet d'entiers relatifs distincts. On pose $f = (X^2+m)\prod_{i=1}^{p-2}(X-n_i)$.
2. Montrer que pour tout réel ϵ de valeur absolue suffisamment petite, le polynôme $f+\epsilon \in \mathbf{R}[\mathbf{X}]$ admet $p-2$ racines réelles simples et 2 racines complexes conjuguées.
3. Pour ℓ un nombre premier, on pose $P_\ell = \ell^p f(X/\ell) + \ell$. Montrer que pour ℓ assez grand, le polynôme $P_\ell \in \mathbf{Q}[\mathbf{X}]$ est un polynôme unitaire irréductible, ayant $p-2$ racines réelles simples et 2 racines complexes conjuguées. Quel est le groupe de Galois de P_ℓ ?
4. Soit G un groupe fini. Montrer qu'il existe une extension finie galoisienne L/K de groupe de Galois G telle que K est une extension finie de $\mathbf{Q}$.

Exercice 2. Soient $p_1, \ldots, p_n$ des nombres premiers deux à deux distincts, et $K = \mathbf{Q}[\sqrt{p_1}, \ldots, \sqrt{p_n}]$.

1. Montrer que l'extension $K/\mathbf{Q}$ est galoisienne. On note $G = \mathrm{Gal}(K/\mathbf{Q})$.
2. Montrer que tout élément de G est d'ordre 2, et en déduire que G est un groupe abélien, isomorphe à $(\mathbf{Z}/2\mathbf{Z})^r$ pour un certain entier r.
3. Exprimer en fonction de r le nombre de sous-extensions de $K/\mathbf{Q}$ de degré 2.
4. Montrer que G est isomorphe à $(\mathbf{Z}/2\mathbf{Z})^n$.
5. Le réel $\sqrt{15}$ est-il dans $\mathbf{Q}(\sqrt{10}, \sqrt{42})$?

Exercice 3. [Un problème de résolubilité] Le polynôme $X^5 - 5X^2 + 1 \in \mathbf{Q}[X]$ est-il résoluble par radicaux ?

Exercice 4. [Groupes résolubles] Soient p, q, r trois nombres premiers distincts.

1. Montrer qu'un groupe d'ordre pq, pq^2 ou pqr est résoluble.
2. Montrer que les groupes suivants ne sont pas simples, et préciser dans quels cas on peut affirmer qu'ils sont résolubles :
   (a) un groupe d'ordre $p^\alpha q$ (où $p > q$) ;
   (b) un groupe d'ordre $p^\alpha q^\beta$ (où $p^\alpha < q+1$) ;
   (c) un groupe d'ordre $p^\alpha q$ (où p^α ne divise pas $(q-1)!$).
3. Montrer que tous les groupes d'ordre < 60 sont résolubles.

Exercice 5. [Un autre critère de résolubilité] On rappelle que, si G est un groupe, on note $D(G)$ le sous-groupe de G engendré par tous les commutateurs $[g,h] := ghg^{-1}h^{-1}$.

1. Rappeler pourquoi $D(G)$ est un sous-groupe distingué de G tel que le quotient $G/D(G)$ est un groupe abélien.
   Soit maintenant G un groupe fini. On définit par récurrence sur n la suite de sous-groupes $(D^n(G))_{n\geq 0}$ par $D^0(G) = G$ et $D^{n+1}(G) = D(D^n(G))$ pour $n \geq 0$.
2. Montrer que G est résoluble si et seulement si $D^n(G)$ est trivial pour n assez grand.
3. En déduire dans quels cas $\mathrm{SL}_n(\mathbf{F}_q)$ est résoluble.