1. On admet qu'il existe (à conjugaison près) sept sous-groupes transitifs de $\mathfrak{S}_7$: ce sont
– $C_7 = \mathbb{Z}/7\mathbb{Z}$ (groupe cyclique à sept éléments),
– $D_7 = (\mathbb{Z}/7\mathbb{Z}) \rtimes (\mathbb{Z}/2\mathbb{Z})$ (groupe diédral de l'heptagone),
– $G_{21} = (\mathbb{Z}/7\mathbb{Z}) \rtimes (\mathbb{Z}/3\mathbb{Z})$ (groupe métacyclique d'ordre 21, où $\mathbb{Z}/3\mathbb{Z}$ agit sur $\mathbb{Z}/7\mathbb{Z}$ par multiplication par 2, ou, ce qui revient au même, en le plongeant dans $(\mathbb{Z}/7\mathbb{Z})^\times \cong \mathbb{Z}/6\mathbb{Z}$),
– $G_{42} = (\mathbb{Z}/7\mathbb{Z}) \rtimes (\mathbb{Z}/6\mathbb{Z})$ (groupe métacyclique d'ordre 42, où $\mathbb{Z}/6\mathbb{Z}$ agit sur $\mathbb{Z}/7\mathbb{Z}$ par multiplication par 3, ou, ce qui revient au même, en identifiant $(\mathbb{Z}/7\mathbb{Z})^\times \cong \mathbb{Z}/6\mathbb{Z}$),
– $G_{168} = PSL_2(\mathbb{F}_7) \cong PSL_3(\mathbb{F}_2)$ (l'unique groupe simple à 168 éléments, opérant sur 7 objets comme $PSL_3(\mathbb{F}_2)$ opère sur $\mathbb{P}^2(\mathbb{F}_2)$),
– $\mathfrak{A}_7$ (le groupe alterné), et
– $\mathfrak{S}_7$ tout entier.

On considère le polynôme $p(t) = t^7 - 7t + 3$. Expérimentalement, modulo les 100 000 plus petits nombres premiers, il se factorise de la façon suivante :

Degrés	Fréquence
$1+3+3$	33.371%
7	28.537%
$1+2+4$	24.956%
$1+1+1+2+2$	12.562%
$1+1+1+1+1+1+1$	0.574%

Que peut-on en déduire sur le groupe de Galois du corps de décomposition de p, de façon certaine d'une part, et de façon heuristique d'autre part ?

En considérant le polynôme $r(t) = \prod_{i<j<k}(t - (\theta_i + \theta_j + \theta_k))$ où $\theta_1, \dots, \theta_7$ sont les sept racines de $p(t)$, expliquer (mais sans faire le calcul !) comment on pourrait prouver rigoureusement que le groupe de Galois est bien celui qu'on pense. (Indication : combien de fois transitivement opère-t-il sur $\{\theta_i\}$?)

2 (calcul général du groupe de Galois). Soit $p(t) = t^d + a_1 t^{d-1} + \cdots + a_d \in K[t]$ un polynôme (unitaire, de degré d) séparable à coefficients dans un corps K, et $\xi_1, \dots, \xi_d$ (de sorte que $p(t) = \prod_{i=1}^d (t - \xi_i)$) ses racines dans son corps de décomposition qu'on notera L. On définit la *résolvante de Kronecker* de p comme

$$s(t) = \prod_{\sigma \in \mathfrak{S}_d} \Big(t - \sum_{i=1}^d u_i \xi_{\sigma(i)} \Big) \in L[u_1, \dots, u_d, t]$$

(Imaginer que s est le polynôme en t dont les racines sont les combinaisons linéaires $\sum_i u_i \xi_{\sigma(i)}$ à coefficients des indéterminées u_i.) Montrer que s est, en fait, à coefficients dans K, et qu'il est invariant par $\mathfrak{S}_d$ (agissant par permutation sur les variables $u_1, \dots, u_d$). Soit h un facteur irréductible[1] quelconque de s dans $K[u_1, \dots, u_d, t]$ (on le prendra unitaire) : on considère le sous-groupe S_h de $\mathfrak{S}_d$ formé des permutations $\sigma \in \mathfrak{S}_d$ qui laissent h invariant. Montrer que S_h est conjugué, dans $\mathfrak{S}_d$, au groupe de Galois $G = \mathrm{Gal}(L/K)$ de p sur K vu comme un groupe de permutations sur $\{\xi_i\}$.

En admettant que la décomposition en facteurs premiers dans $\mathbb{Q}[u_1, \dots, u_d, t]$ est algorithmique, expliquer pourquoi ceci fournit un algorithme théorique permettant de calculer le groupe de Galois de n'importe quel polynôme sur $\mathbb{Q}$ (i.e., le problème du calcul du groupe de Galois est décidable), mais expliquer pourquoi cet algorithme est inutilisable en pratique.

Les exercices suivants demandent quelques connaissances en géométrie et/ou en analyse complexe.

([1]) On rappelle que les anneaux de polynômes sur un corps sont factoriels.

3 (extension icosaédrale). On rappelle que le groupe des isométries directes d'un icosaèdre régulier (ou, dualement, d'un dodécaèdre régulier) est le groupe alterné $\mathfrak{A}_5$ sur cinq éléments. En déduire qu'il existe une extension $\mathbb{C}(u) \subseteq \mathbb{C}(z)$, où u est une certaine fonction rationnelle en l'indéterminée z (et transcendante sur $\mathbb{C}$, c'est-à-dire que le corps $\mathbb{C}(u)$ qu'elle engendre est bien isomorphe au corps des fractions rationnelles complexes sur u vue comme une indéterminée) qui soit galoisienne de groupe de Galois $\mathfrak{A}_5$. Pour cela, on pourra voir les sommets de l'icosaèdre comme des points de la sphère de Riemann, et appliquer le lemme d'Artin et le théorème de Lüroth.

4 (problème de Galois inverse pour $\mathbb{C}(z)$). On se propose de démontrer que tout groupe fini est le groupe de Galois d'une extension (galoisienne finie) de $\mathbb{C}(z)$.

Soit G un groupe fini, d'ordre n, et $g_1 = 1, \dots, g_n$ ses éléments. On considère l'ensemble E des données $t = (t_1, \dots, t_n)$ suivantes : pour chaque $i \in \{1, \dots, n\}$, une fonction t_i *méromorphe* sur $\mathbb{C} \setminus [1; n]$ (où $[1; n]$ désigne l'intervalle fermé réel ayant ces bornes), à croissance au plus polynomiale à l'infini (c'est-à-dire $|t_i(z)| = O(|z|^k)$ pour un certain k lorsque $|z| \to +\infty$) ainsi qu'en tout point du bord (c'est-à-dire $|t_i(z - c)| = O(|z - c|^{-k})$ lorsque $z \to c$ avec $c \in [1; n]$), et vérifiant de plus la condition de compatibilité suivante : pour chaque triplet (i, j, k) tel que $g_i g_j = g_k$ dans G, la fonction t_i restreinte au demi-plan supérieur $\{z : \Im z > 0\}$ et la fonction t_k restreinte au demi-plan inférieur $\{z : \Im z < 0\}$ se prolongent en une fonction méromorphe commune sur un voisinage de $]j - 1; j[$ dans le plan complexe (lorsque $j = 1$, bien sûr, cette condition est automatique).

(a) Expliquer pourquoi E est un corps (l'addition et la multiplication étant données par les opérations terme à terme sur les t_i). On montrera notamment que si un quelconque des t_i associés à un $t \in E$ est nulle (ou simplement nulle sur un ouvert non vide) alors tous les t_i sont nuls.

(b) On plonge $\mathbb{C}(z)$ dans E en identifiant une fonction rationnelle $h \in \mathbb{C}(z)$ avec le n-uplet $(h, \dots, h)$ où chaque composante est la fonction h elle-même (vue comme une fonction méromorphe sur $\mathbb{C}$, donc *a fortiori* sur $\mathbb{C} \setminus [1; n]$). Expliquer pourquoi ce plongement est correct (définit bien un élément de E).

(c) On fait agir G sur E en posant $g \cdot (t_1, \dots, t_n) = (t'_1, \dots, t'_n)$, où $t'_i = t_{i'}$ si $g_{i'} = g g_i$: expliquer pourquoi cette action a un sens. Expliquer pourquoi le corps fixe de E par G est exactement $\mathbb{C}(z)$.

(d) On *admet*[2] le fait suivant : pour tout $i \in \{2, \dots, n\}$, il existe $t \in E$ tel que $t_i(0) \neq t_1(0)$. Montrer alors que E est bien une extension de $\mathbb{C}(z)$ galoisienne de groupe de Galois G.

Remarque : Le principe utilisé dans ce dernier exercice est de construire — sans le dire — un revêtement ramifié de la sphère de Riemann ayant $\{1, \dots, n\}$ pour points de ramification et groupe de Galois G, et le corps E est simplement le corps des fonctions méromorphes sur ce revêtement.

([2]) Il s'agit d'une conséquence du théorème de séparation de Riemann (sur toute surface de Riemann — compacte —, les fonctions méromorphes séparent les points). Reconnaissons que, dans ce cas, c'est un peu une pétition de principe, puisque toute la difficulté du résultat est cachée dans ce fait admis.