# Examen
26/01/18, durée 4h

Les documents sont interdits.

Dans cet examen, si $K$ est un corps de nombres ou un corps local, on notera $\mathcal{O}_K$ son anneau des entiers.

**Exercice 1.** Les questions suivantes n'ont besoin que de brèves justifications.

1. Soit $\alpha$ une racine complexe du polynôme $X^2 - X + 3$, et soit $K = \mathbb{Q}(\alpha)$. Quels sont les nombres premiers ramifiés dans $K$ ?
2. Comment calculeriez-vous le nombre de classe ou le groupe de classe d'un corps de nombres explicite [1] ?
3. Rappeler la définition de la fonction $\zeta$ de Dedekind d'un corps de nombres. Que dire (qualitativement) de son comportement en 1 ?
4. Rappeler la définition de la fonction $L$ de Dirichlet associée à un caractère de $(\mathbb{Z}/N\mathbb{Z})^*$. Rappeler la définition des fonctions $L$ d'Artin (on pourra exclure un certain nombre de premiers). Y a-t-il un lien entre les deux notions ?
5. Que dire du comportement des fonctions $L$ d'Artin en 1 ? Comment le prouve-t-on (donner une idée brève) ? Donner un exemple d'application.
6. Soit $K$ un corps local. Rappeler la définition d'une extension finie, modérément ramifiée de $K$. Comment décrire ces extensions ?
7. Soit $K$ un corps local. Donner une famille d'algèbres simples centrales qui engendrent le groupe de Brauer de $K$.

# Problème 1

Soit $K$ un corps de nombre, et soit $L$ une extension finie galoisienne de $K$, de groupe de Galois $G$. Soit $H$ un sous-groupe de $G$, et soit $E = L^H$ le sous-corps de $L$ fixe par $H$.

1. Rappeler l'énoncé du théorème de Cebotarev pour l'extension $L/K$. Donner en particulier la densité analytique de l'ensemble $D(L/K)$ des idéaux premiers de $\mathcal{O}_K$ totalement décomposés dans $L$.
2. Montrer que si $L \subset M$, alors $D(M/K) \subset D(L/K)$.
3. Soit $M$ une autre extension finie galoisienne de $K$. Soit $C$ une clôture algébrique de $K$ contenant $L$ et $M$, et soit $LM$ le sous-corps de $K$ engendré par $L$ et $M$ dans $C$. Montrer que l'extension $LM/K$ est finie galoisienne.
4. Montrer que s'il existe un ensemble fini $S$ de l'ensemble des premiers de $\mathcal{O}_K$ tel que $D(M/K) \subset D(L/K) \cup S$, alors $D(LM/K)$ et $D(M/K)$ ne diffèrent que d'un ensemble fini.

[1] Il s'agit d'une question ouverte, donnez simplement quelques méthodes que vous connaissez.

5. Que déduire de la question précédente, en utilisant le théorème de Cebotarev ?
6. En utilisant la question précédente, montrer que si $P$ est un polynôme unitaire dans $\mathcal{O}_K[X]$ tel que pour presque tout premier $\mathfrak{p}$ de $\mathcal{O}_K$, la réduction de $P$ modulo $\mathfrak{p}$ est un produit de polynômes de degré 1, alors $P$ est produit de termes de degré 1.
7. Soit $D'(E/K)$ l'ensemble des premiers $\mathfrak{p}$ de $\mathcal{O}_K$ tels qu'il existe un premier $\mathfrak{q}$ dans $\mathcal{O}_E$ au-dessus de $\mathfrak{p}$ avec $e_{\mathfrak{q}/\mathfrak{p}} = f_{\mathfrak{q}/\mathfrak{p}} = 1$. Soit $\mathfrak{p}$ un premier non nul de $\mathcal{O}_K$, soit $\mathfrak{P}$ un idéal premier de $\mathcal{O}_L$ au-dessus de $\mathfrak{p}$, et soit $D_{\mathfrak{P}} \subset G$ le sous-groupe de décomposition de $\mathfrak{P}$. Montrer que $\mathfrak{p} \in D'(E/K)$ si et seulement il existe un conjugué de $D_{\mathfrak{P}}$ dans $G$ qui est inclus dans $H$.
8. Que dire de la densité analytique de $D'(E/K)$ ?
9. Soit $H'$ un sous-groupe de $G$, et soit $E' = L^{H'}$. Montrer que $E$ et $E'$ sont isomorphes comme extensions de $K$ si et seulement si $H$ et $H'$ sont conjugués dans $G$.
10. Avec les notations précédentes, supposons que $G = \mathfrak{S}_6$ est le groupe symétrique sur 6 éléments,
$$H = \{1, (12)(34), (13)(24), (14)(23)\}$$
et
$$H' = \{1, (12)(34), (12)(56), (34)(56)\}.$$
Montrer que $E$ et $E'$ ne sont pas isomorphes, mais que $D'(E/K) = D'(E'/K)$.

# Problème 2

Soit $p$ un nombre premier impair.

**Partie 1.**

1. Montrer que la fonction
$$\mathbb{Z} \to \mathbb{Z}_p, x \mapsto (1+p)^x$$
s'étend par continuité en une fonction continue $f : \mathbb{Z}_p \to \mathbb{Z}_p$, et donner une série formelle représentant $f$.
2. Montrer que l'adhérence du sous-groupe de $(\mathbb{Z}_p^*, \times)$ engendré par $1+p$ est $1 + p\mathbb{Z}_p$. En déduire l'image de $f$.
3. Donner un inverse de $f : \mathbb{Z}_p \to 1+p\mathbb{Z}_p$, et en déduire que $f$ est un isomorphisme de groupes topologiques de $\mathbb{Z}_p$ sur $1 + p\mathbb{Z}_p$.
4. Montrer que le groupe $\mathbb{Q}_p^*$ est isomorphe au groupe
$$\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p.$$

5. En utilisant l'application de réciprocité d'Artin, montrer qu'il n'existe pas d'extension galoisienne de $\mathbb{Q}_p$ de groupe $(\mathbb{Z}/p\mathbb{Z})^3$.

**Partie 2.**

1. Soit $N = p^s - 1$, où $s$ est un entier strictement positif. Soit $\zeta_N$ une racine primitive $N$-ième de l'unité dans une clôture algébrique de $\mathbb{Q}_p$. Montrer que l'extension $\mathbb{Q}_p(\zeta_N)/\mathbb{Q}_p$ est galoisienne. Calculer son groupe de Galois et le groupe de Galois de l'extension résiduelle.
2. Même question avec $N = p$. On pourra calculer le polynôme minimal de $\zeta_N - 1$.
3. Même question avec $N = p^t$. On pourra calculer le polynôme minimal de $\zeta_N^{p^{t-1}} - 1$.
4. Soit $K$ une extension cyclique de $\mathbb{Q}_p$ de degré une puissance de $p$. Montrer que le groupe de Galois de $K(\zeta_N)$ sur $\mathbb{Q}$, pour $N$ de la forme $(p^{p^s} - 1)p^t$ avec $s, t > 0$, a un quotient de la forme $(\mathbb{Z}/p\mathbb{Z})^3$ dès que $K$ n'est pas inclus dans $\mathbb{Q}(\zeta_N)$.
5. Montrer que si $K$ est une extension abélienne de $\mathbb{Q}_p$ de degré une puissance de $p$, alors $K$ est inclus dans une extension cyclotomique.