Feuille 1 : Produit tensoriel, localisations, modules des différentielles

Dans tout la suite, on notera A un anneau commutatif, E, E' et F des A-modules.

Exercice 1 Soit $f : E \to E'$ un morphisme injectif de A-modules. Montrer sur un exemple que l'homomorphisme $f \otimes 1 : E \otimes F \to E' \otimes F$ n'est pas injectif en général.

Exercice 2 On suppose E et F libres de bases respectives $(e_i)_{i\in I}$ et $(f_j)_{j\in J}$. Montrer que $E \otimes F$ est libre et donner une base de $E \otimes F$.

Exercice 3

1. Si I est un idéal de A, montrer l'isomorphisme $E \otimes_A A/I \simeq E/EI$ défini par $x \otimes (a + I) \mapsto xa + EI$. (On pourra par exemple introduire la suite exacte canonique $0 \to I \to A \to A/I \to 0$).
2. En déduire une forme plus simple pour $A/I \otimes A/J$ où I et J sont deux idéaux de A.
3. Montrer directement que $A/I \otimes A/J = A/(I + J)$ en étudiant l'annulateur de $\pi_I(1) \otimes \pi_J(1)$ dans $A/I \otimes A/J$.

Exercice 4 (Calculs de produits tensoriels sur $\mathbb{Z}$) On introduit les $\mathbb{Z}$-modules suivants : $\mathbb{Z}^r$ avec $r \in \mathbb{N}$, $\mathbb{Z}/n\mathbb{Z}$ avec $n \in \mathbb{N}^*$, $\mathbb{Q}$, $\mathbb{Q}/\mathbb{Z}$, et $\mathbb{Z}^{(\mathbb{N})}$.

1. Calculer le produit tensoriel (sur $\mathbb{Z}$) de $\mathbb{Z}^r$ avec chacun des autres termes (y compris avec $\mathbb{Z}^{r'}$ pour $r' \in \mathbb{N}$).
2. Calculer le produit tensoriel de $\mathbb{Z}^{(\mathbb{N})}$ avec chacun des autres termes.
3. Calculer le produit tensoriel de $\mathbb{Z}/n\mathbb{Z}$ avec chacun des autres termes (y compris avec $\mathbb{Z}/m\mathbb{Z}$).
4. Montrer que si G est un groupe abélien fini, on a $G \otimes_{\mathbb{Z}} \mathbb{Q} = 0$.
5. En admettant que $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} = 0$, montrer que $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = 0$.

Exercice 5 Soit B une A-algèbre et $f \in A[X]$.

1. Montrer que $B \otimes_A A[X]/(f(X)) = B[X]/(f(X))$.
2. Montrer que $A[X] \otimes_A A[Y] = A[X, Y]$.
3. Déterminer $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ (ceci fourni un exemple de produit tensoriel de deux extensions qui n'est pas une extension).
4. Soient $K = k[\alpha]/k$ une extension finie séparable de corps et Ω une extension quelconque de k. Montrer que $K \otimes_k \Omega$ est produit d'extensions séparables de Ω
$$K \otimes_k \Omega = \Pi_{i=1}^r \Omega_i.$$
5. Est-ce encore vrai si l'extension K/k n'est pas séparable ? (Considérer un élément convenable de la forme $\alpha \otimes 1 - 1 \otimes \alpha$ dans le produit $K \otimes_k K$).

Exercice 6 (Localisation) Soient A un anneau commutatif et M et N deux A-modules. On note $S_{\mathfrak{p}} = A \backslash \mathfrak{p}$ pour tout idéal premier $\mathfrak{p}$ de A. On note $M_{\mathfrak{p}}$ le module défini comme l'ensemble des "fractions" $\frac{m}{s}$ avec $m \in M$ et $s \in S_{\mathfrak{p}}$, deux telles fractions $\frac{m}{s}$ et $\frac{m'}{s'}$ étant identifiées si et seulement si
$$\exists s'' \in S_{\mathfrak{p}} \quad s''(s'm - sm') = 0.$$
Ceci s'applique en particulier à A (non nécessairement intègre) et défini $A_{\mathfrak{p}}$. On a des applications naturelles
$$A \to A_{\mathfrak{p}} \; a \mapsto \frac{a}{1}, \quad \text{et} \quad M \to M_{\mathfrak{p}} \; m \mapsto \frac{m}{1}.$$
La multiplication $\frac{a}{s} \cdot \frac{a'}{s'}$ définie une structure d'anneau sur $A_{\mathfrak{p}}$. De même $M_{\mathfrak{p}}$ est naturellement muni d'une structure de $A_{\mathfrak{p}}$-module.

On suppose donné un morphisme $\varphi : M \to N$ de A-modules. Pour tout $\mathfrak{p}$ premier, on note $\varphi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ le morphisme de $A_{\mathfrak{p}}$-modules déduit de φ par $\varphi_{\mathfrak{p}}(\frac{m}{s}) = \frac{\varphi(m)}{s}$.

Montrer que φ est injective (respectivement surjective) si et seulement si pour tout premier $\mathfrak{p}$, le morphisme $\varphi_{\mathfrak{p}}$ est injectif (respectivement surjectif).

Exercice 7 Soient $\mathfrak{p}$ un idéal maximal de A et $\mathfrak{q} = \mathfrak{p}A_{\mathfrak{p}}$ où $A_{\mathfrak{p}}$ est le localisé de A suivant l'ensemble multiplicatif $S_{\mathfrak{p}} = A - \mathfrak{p}$. Montrer que l'application

$$A/\mathfrak{p}^m \to A_{\mathfrak{p}}/\mathfrak{q}^m, \;\; a + \mathfrak{p}^m \mapsto a + \mathfrak{q}^m$$

est un isomorphisme. Pour l'injectivité on montrera que l'anneau quotient $A/\mathfrak{p}^m$ est local.

Exercice 8 (Foncteurs représentables)

1. Soient A un anneau commutatif et E, F deux A-modules. On note B le foncteur covariant de Mod_A (catégorie des A-modules) dans Ens (catégorie des ensembles) donné par

   $$B(G) = \mathrm{Bil}(E \times F, G).$$

   Montrer que B est représentable ; par quel A-module ?
2. Soit X un ensemble et $\mathcal{R}$ une relation déquivalence sur X. Montrer que le foncteur covariant de Ens dans Ens qui à Z associe l'ensemble des applications $f : X \to Z$ telles que $(x\mathcal{R}y \Rightarrow f(x) = f(y))$ est représentable ; par quel objet ?
3. Soient A un anneau commutatif, E un A-module et $(x_i)_{i\in I}$ une famille d'éléments de E. On note Φ le foncteur covariant de Mod_A dans Ens donné par

   $$\Phi(G) = \{f : E \to G \text{ linéaire} \mid \forall i \in I, \quad f(x_i) = 0\}.$$

   Montrer que Φ est représentable ; par quel module ?
4. Soit E un espace vectoriel normé. On note $Banach$ la catégorie des espace de Banach et Ψ le foncteur covariant de $Banach$ dans Ens donné par

   $$\Psi(F) = \{f : E \to F \mid f \text{ linéaire continue}\}.$$

   Montrer que Ψ est représentable ; par quel objet ?
5. Soient X un espace topologique et Y un sous-ensemble de X. On note Top la catégorie des espaces topologiques et Ψ le foncteur contravariant de Top dans Ens donné par

   $$\Psi(T) = \{f : T \to X \text{ continue} \mid f(T) \subset Y\}.$$

   Montrer que Ψ est représentable ; par quel objet ?

Feuille 2 : Valuations et complétion

Dans toute cette feuille, si l'on ne précise rien, p est un nombre premier.

.

Exercice 1 (clôture intégrale et localisation)

1. On rappelle tout d'abord deux définitions : soit A un anneau intègre inclus dans un corps L. On dit que $x \in L$ est *entier sur* A si l'une des deux conditions équivalentes (preuve !) est vérifiée :
   (i) Il existe $P \in A[X]$ unitaire de degré ≥ 1 tel que $P(x) = 0$,
   (ii) Il existe un A-module $M \subset L$, de type fini, non-nul, tel que $xM \subset M$.
   L'anneau A est dit *intégralement clos* si tout élement de $\mathrm{Frac}(A)$ qui est entier sur A est en fait dans A.
2. Soient $A \subset B$ deux anneaux intègres, avec B entier sur A. Soit $S \subset A$ un ensemble multiplicatif contenant 1 et pas 0. Montrer que $S^{-1}B$ est entier sur $S^{-1}A$ et que si A est intégralement clos alors $S^{-1}A$ aussi.

Exercice 2 (Formule du produit sur $k(X)$)

Soient k un corps et $K = k(X)$.

1. Montrer qu'il y a bijection entre l'ensemble des valuations v de K (normalisées telles que $v(K^*) = \mathbb{Z}$), triviales sur k, telles que $v(X) \geq 0$ et l'ensemble des polynômes irréductibles unitaires de $k[X]$ (*i.e.* l'ensemble des idéaux maximaux de $k[X]$). On note $v_{\mathfrak{p}}$ la valuation qui correspond à l'idéal $\mathfrak{p}$.
2. Si v est une valuation de K, triviale sur k, telle que $v(X) < 0$, montrer que
$$\forall h \in k[X], \quad v(h) = -\deg h.$$
   On note v_∞ l'unique telle valuation.
3. Montrer que pour tout $h \in K^*$, on a
$$v_\infty(h) + \sum_{\mathfrak{p}} [k[X]/\mathfrak{p} : k]\, v_{\mathfrak{p}}(h) = 0.$$

Exercice 3 (Approximation faible)

Soit K un corps de nombres (*i.e.* une extension finie de $\mathbb{Q}$) et soient $\sigma_i : K \hookrightarrow \mathbb{R}$, m plongements de corps, deux à deux distincts. Soient ε_i pour $1 \leq i \leq m$ des signes, *i.e.* des éléments de $\{-1, 1\}$. Montrer qu'il existe $a \in K^*$ tel que
$$\forall i \in \{1, \ldots, m\}, \quad \mathrm{sign}(\sigma_i(a)) = \varepsilon_i.$$

Exercice 4 (Calculs)

1. Calculer la limite de $\frac{n!}{n!+1}$ dans $\mathbb{R}$ et dans $\mathbb{Q}_p$ pour tout premier p.
2. On ordonne les nombres premiers par ordre croissant et on forme ainsi la suite $(p_n)_{n\geq 1}$ où p_n est le n-ieme nombre premier. On note $p_\infty := \infty$. Pour tout entier $n \geq 1$, soient $a_n \in \mathbb{Z}_{p_n}$ des entiers p_n-adiques et $a_\infty = 0$. Montrer qu'il existe une suite de rationnels $(x_n)_{n\geq 1}$ avec $x_n \in \mathbb{Q}$ telle que
$$\forall i \in \mathbb{N}^* \cup \{\infty\}, \quad \lim_{n\to+\infty} |x_n - a_{p_i}|_{p_i} = 0.$$
   On pourra par exemple écrire $x_n = \frac{u_n}{v_n}$ et poser $v_n = 2^n f(n) + 1$ avec $f(n) = (\prod_{i=1}^n p_i)^n$.

Exercice 5 ($\mathbb{Q}$ n'est pas complet)

1. **(Théorème de Baire)** Soit E un espace topologique. On suppose que E est localement compact, ou que E est muni d'une distance d qui en fait un espace métrique complet. Montrer que toute intersection dénombrable $\bigcap_{n\geq 1} V_n$ d'ouverts denses dans E est dense dans E (on pourra construire une suite d'ouverts non vides (B_n) telle que $\overline{B}_{n+1} \subset V_n \cap B_n$).
2. Soit $(K, |\cdot|)$ un corps valué (*i.e.* muni d'une valeur absolue *ultramétrique*) complet, avec $|\cdot|$ une valeur absolue non-triviale. Montrer que K est indénombrable (on pourra utiliser le théorème de Baire).
3. En déduire que $\mathbb{Q}$ muni de la valeur absolue p-adique n'est pas complet.

Exercice 6 ($\mathbb{Q}_p$ n'est pas algébriquement clos)
Montrer que le complété, $\mathbb{Q}_p$, de $\mathbb{Q}$ pour la valeur absolue p-adique, n'est pas algébriquement clos (on considerera un polynôme convenable de degré 2 de $\mathbb{Z}_p[X]$).

Exercice 7 Soient U un ouvert non-vide de $\mathbb{Z}_p$. Montrer que U n'est pas connexe.

Exercice 8 (Développement de Hensel)
Soient K un corps complet pour une valuation discrète, d'anneau A, d'idéal maximal $\mathfrak{p}$, de corps de fractions $k := A/\mathfrak{p}$. Soit π une uniformisante de $\mathfrak{p}$ (*i.e.* un élément π de A tel que $v(\pi) = 1$) et soit S un système de représentants de k dans A. Montrer que tout élément de $a \in A$ s'écrit de façon unique comme une série convergente

$$a = \sum_{n=0}^{\infty} s_n \pi^n \quad \text{avec} \quad s_n \in S.$$

Exercice 9 (Description de $\mathbb{Q}_p/\mathbb{Z}_p$)
On rappelle que tout $x \in \mathbb{Q}_p$ admet le développement de Hensel suivant

$$x = \sum_{i\in\mathbb{Z}} x_i p^i \quad \text{avec} \quad x_i \in \{0, \ldots, p-1\} \quad \text{et } x_i = 0 \text{ pour tout } i \ll 0.$$

On note

$$[x] := \sum_{i\geq 0} x_i p^i \quad \text{sa partie entière, et} \quad < x >:= \sum_{i<0} x_i p^i \quad \text{sa partie fractionnaire.}$$

1. Supposant l'existence et l'unicité du développement de Hensel sur $\mathbb{Z}_p$ acquis, le démontrer pour $\mathbb{Q}_p$.
2. Montrer que $\mathbb{Q}_p/\mathbb{Z}_p$ est un groupe topologique discret.
3. Montrer que l'application $\tau : \mathbb{Q}_p \to \mathbb{C}^*$, $x \mapsto \exp(2i\pi < x >)$ est bien définie et est un morphisme de groupes.
4. À quoi est isomorphe le groupe $\mathbb{Q}_p/\mathbb{Z}_p$?

Exercice 10 (Compacité)

1. Soit K un corps valué ultramétrique de valuation discrète, complet, d'anneau de valuation A. Soit $\mathfrak{m}$ l'idéal maximal de A. Montrer que A est compact si et seulement si $A/\mathfrak{m}$ est fini.
2. En déduire que si K un corps valué ultramétrique de valuation discrète, complet, d'anneau de valuation A, d'idéal maximal $\mathfrak{p}$, d'uniformisante π et de corps résiduel fini, alors pour tout entier $n \geq 0$, les ensembles $\mathfrak{p}^n$, $1 + \mathfrak{p}^n$, $A^\times \pi$ sont compacts.

Feuille 3 :

Dans toute cette feuille, si l'on ne précise rien, p est un nombre premier.

.

Exercice 1 Soit $K = \mathbb{Q}(S)$ le corps engendré par $S = \{\sqrt{p} \mid p \text{ premier }\}$.

1. Montrer que $K/\mathbb{Q}$ est galoisien. Déterminer son groupe de Galois et l'écrire comme une limite projective.
2. Soit V un $\mathbb{F}_2$-espace-vectoriel de dimension infinie. Montrer que : pour tout entier $n \geq 0$, il existe un sous-espace vectoriel $V_n \subset V$ de codimension n.
3. Déduire de ce qui précède qu'il existe dans $\mathrm{Gal}(K/\mathbb{Q})$ des sous-groupes non-ouverts d'indice 2^n pour tout entier $n \geq 0$.
4. En déduire l'existence dans $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ de sous-groupes distingués non-ouverts d'indice 2^n pour tout entier $n \geq 0$.

Exercice 2 (Extensions cyclotomiques I) Soient $K/\mathbb{Q}$ un corps de nombres et $\mathcal{O}_K$ la clôture intégrale de $\mathbb{Z}$ dans K, *i.e.* l'anneau des entiers de $\mathcal{O}_K$. C'est un anneau de Dedekind. Soient L une extension finie séparable de degré n d'un corps de nombres K et B la clôture intégrale de $\mathcal{O}_K$ dans L. Soient $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$ et $\mathfrak{p}B = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_g^{e_g}$ sa décomposition en idéaux premiers dans B. Soit $f_i = [B/\mathcal{P}_i : \mathcal{O}_K/\mathfrak{p}]$, $1 \leq i \leq g$ le degré d'inertie. On rappelle que

$$\sum_{i=1}^{g} e_i f_i = n.$$

On note $r \geq 1$, p premier, ζ une racine primitive p^r-ième de l'unité, $K = \mathbb{Q}[\zeta]$ et $\mathcal{O}_K$ son anneau d'entiers.

1. Montrer que K est une extension normale et que l'on a un morphisme injectif du groupe de Galois G_K vers le groupe $(\mathbb{Z}/p^r\mathbb{Z})^\times$ des inversibles de $\mathbb{Z}/p^r\mathbb{Z}$. Montrer également que $\mathbb{Z}[\zeta] \subset \mathcal{O}_K$ et que $[\mathbb{Q}[\zeta] : \mathbb{Q}] \leq \varphi(p^r) = p^{r-1}(p-1)$.
2. On appelle *polynôme cyclotomique* Φ_{p^r} le polynôme $\prod_{\zeta \in \mu_{p^r} \text{primitive}} (X - \zeta)$. Montrer que
$$\Phi_{p^r} = \prod_{[i] \in (\mathbb{Z}/p^r\mathbb{Z})^\times} (X - \zeta^i) = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1}.$$
3. Soit ξ une autre racine primitive p^r-ième de l'unité. Montrer que $\frac{1-\zeta}{1-\xi}$ est une unité de $\mathcal{O}_K$ (*i.e.* est inversible dans $\mathcal{O}_K$).
4. Soit $\pi = 1 - \zeta$. En calculant $\Phi_{p^r}(1)$, montrer l'égalité d'idéaux dans $\mathcal{O}_K$, $(p) = (\pi)^{\varphi(p^r)}$. En déduire que le corps $\mathbb{Q}[\zeta]$ est de degré $\varphi(p^r)$ sur $\mathbb{Q}$ et que l'élément π est premier dans $\mathcal{O}_K$. Quels sont les premiers ramifiés dans $K/\mathbb{Q}$? Donner le degré résiduel f et l'indice de ramification e.

Exercice 3 (Extension $\mathbb{Q}^{\mathbf{ab}}/\mathbb{Q}$) Dans la suite on utilisera librement que si $n \in \mathbb{N}$, et si ζ_n est une racine primitive n-ieme de 1, alors $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$. On rappelle également le *théorème de Kronecker-Weber* : "si $K/\mathbb{Q}$ est une extension finie abélienne, alors il existe $n \geq 1$ tel que $K \subset \mathbb{Q}(\zeta_n)$." On note $\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}$ l'extension abélienne maximale de $\mathbb{Q}$.

Montrer que cette extension est galoisienne et décrire explicitement son groupe de Galois.

Exercice 4 Soit G un groupe topologique compact et $\{N_i \mid i \in I\}$ une famille de sous-groupes distingués, fermés d'indice fini dans G telle que

$$\bigcap_{i \in I} N_i = \{1\}.$$

On a alors G est un groupe profini, homéomorphe à la limite projective des G/N_i.

Exercice 5
1. Montrer que si H est un sous-groupe fermé de $\mathbb{Z}_p$ alors il existe $i \in \mathbb{N}$ tel que $p^i\mathbb{Z}_p = H$.
2. Montrer que $p\mathbb{Z}_p$ est l'unique sous groupe fermé maximal de $\mathbb{Z}_p$.
3. Montrer que si $\alpha : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ est un morphisme surjectif, et si H est un sous-groupe fermé tel que $\alpha(H) = \alpha(\mathbb{Z}_p)$, alors $H = \mathbb{Z}_p$.

Exercice 6 Prouver que $\widehat{\mathbb{Z}}$ est homéomorphe à $\prod_{p \text{ premier}} \mathbb{Z}_p$. Soit S un sous-ensemble non-vide de l'ensemble des nombres premiers. Donner un énoncé analogue avec la limite projective $\mathbb{Z}_S$ des $\mathbb{Z}/n\mathbb{Z}$ quand n décrit l'ensemble

$$\{n \in \mathbb{N} \mid \text{ les diviseurs premiers de } p \text{ sont dans } S\}.$$

Exercice 7 (Extensions quadratiques)
Soit K une extension quadratique de $\mathbb{Q}$. On note $\mathcal{O}$ la clôture intégrale de $\mathbb{Z}$ dans K :

$$\mathcal{O} = \{x \in K, x \text{ solution d'un polynôme unitaire à coefficients dans } \mathbb{Z}\}.$$

1. Montrer que K est de la forme $\mathbb{Q}(\sqrt{\Delta})$ avec $\Delta \in \mathbb{Z} - \{0, 1\}$ sans facteur carré.
2. Pour $z = x + y\sqrt{\Delta} \in \mathbb{Q}(\sqrt{\Delta})$, $\bar{z} = x - y\sqrt{\Delta}$. Montrer que

$$z \in \mathcal{O} \text{ si et seulement si } \begin{cases} N_{K/\mathbb{Q}}(z) = N(z) := z\bar{z} \in \mathbb{Z} \\ \mathrm{T}_{K/\mathbb{Q}}(z) = T(z) := z + \bar{z} \in \mathbb{Z} \end{cases}$$

3. En déduire $\mathcal{O}$.

Feuille 3 : Lemme de Hensel, discriminant

Exercice 1 Soit K un corps ultramétrique complet de valeur absolue $|\cdot|$. On note R son anneau de valuation. Soit $f = \sum_{i=0}^{n} a_i X^i \in K[X]$ de degré $n \geq 0$ tel que $a_0 a_n \neq 0$.

1. Si f est irréductible, montrer que
$$\max_{0 \leq i \leq n} |a_i| = \max\{|a_0|, |a_n|\}.$$
2. En déduire que si f est irréductible, unitaire, tel que $a_0 \in R$, alors $f \in R[X]$.

Exercice 2 (Lemme de Hensel, variante)
Soit K un corps ultramétrique complet de valeur absolue $|\cdot|$. On note R son anneau de valuation. Soient $f \in R[X]$ et $\alpha_0 \in R$ tel que $|f(\alpha_0)| < |f'(\alpha_0)|^2$. Pour $i \geq 0$, on introduit la suite
$$\alpha_{i+1} = \alpha_i - \frac{f(\alpha_i)}{f'(\alpha_i)} \quad \text{et on pose} \quad c := \frac{|f(\alpha_0)|}{|f'(\alpha_0)|^2}.$$
1. Montrer que pour tout $i \geq 0$, on a
$$\left| \frac{f(\alpha_i)}{f'(\alpha_i)^2} \right| < c^{2^i}.$$
2. En déduire que la suite (α_i) converge dans R vers une racine α de f, et que de plus, on a
$$|\alpha - \alpha_0| \leq c < 1.$$
3. En déduire que si $|f'(\alpha_0)| = 1$ et $|f(\alpha_0)| < 1$, alors f admet une racine α dans R.

Exercice 3 (Extensions quadratiques de $\mathbb{Q}_2$)
1. Soient K un corps de caractéristique différente de 2 et $\alpha, \beta \in K - K^2$. Montrer que
$$K[\sqrt{\alpha}] = K[\sqrt{\beta}] \iff \exists x \in K^* \ \ \alpha = x^2 \beta.$$
2. Soit $x = 2^n u$ un élément de $\mathbb{Q}_2^*$ avec $n \in \mathbb{Z}$ et $u \in \mathbb{Z}_2^\times$ une unité 2-adique. Montrer que $x \in \mathbb{Q}_2^{*2}$ si et seulement si n est pair et $u = 1 \mod 8\mathbb{Z}_2$.
3. En déduire les extensions quadratiques de $\mathbb{Q}_2$.

Exercice 4 (Autres applications de Hensel)
1. Soient ℓ, p deux nombres premiers. Montrer que le corps $\mathbb{Q}_\ell$ est isomorphe au corps $\mathbb{Q}_p$ si et seulement si $\ell = p$.
2. Soit $u \in \mathbb{Q}_p^*$. Montrer que
$$u \in \mathbb{Z}_p^\times \iff \text{il existe une infinité d'entiers } n \text{ tels que } u^{p-1} \in \mathbb{Q}_p^{*n}.$$
3. En déduire que si φ est un endomorphisme de corps de $\mathbb{Q}_p$ alors en notant v_p la valuation p-adique, on a : $\forall x \in \mathbb{Q}_p$, $v_p(\varphi(x)) = v_p(x)$.
4. En déduire que le seul endomorphisme de corps de $\mathbb{Q}_p$ est l'identité.

Exercice 5 Soit A l'algèbre des polynômes de $\mathbb{C}[t]$ dont le coefficient de degré 1 est nul. Montrer que A est une algèbre intègre de type fini sur $\mathbb{C}$. Détermniner son corps des fractions et sa clotûre intégrale.

Exercice 6 (Norme et Trace)
Soient $A \subset B$ des anneaux intègres avec B un A-module libre de rang n. L'élément $\beta \in B$ définit par multiplication une application linéaire $B \to B,\ x \mapsto \beta x$. Le déterminant (resp. la trace) de cette application linéaire est noté $\mathrm{Nm}_{B/A}\beta$ (resp. $\mathrm{Tr}_{B/A}\beta$).

1. Observer que $\mathrm{Nm}_{B/A}\beta\beta' = \mathrm{Nm}_{B/A}\beta \mathrm{Nm}_{B/A}\beta'$.
2. Soient L/K une extension galoisienne de corps de degré n et $y \in L$. Soient $f(X)$ le polynôme minimal de y sur K et $y_1 = y, y_2, \ldots, y_m$ les racines de $f(X)$. Montrer que
$$\mathrm{Tr}_{L/K}\, y = r(y_1 + \cdots + y_m), \quad \mathrm{Nm}_{L/K}\, y = (y_1 \cdots y_m)^r$$
où $r = [L : K[y]] = n/m$ (on pourra commencer par traiter le cas $r = 1$).
3. En déduire que si L/K est séparable de degré n et si $\{\sigma_1, \ldots, \sigma_n\}$ sont les différents K-plongements de L dans une clôture algébrique de L/K, alors, on a
$$\forall y \in L, \quad \mathrm{Tr}_{L/K}\, y = \sum_{i=1}^{n} \sigma_i(y) \quad \text{et} \quad \mathrm{Nm}_{L/K}(y) = \prod_{i=1}^{n} \sigma_i(y).$$

Exercice 7 (Discriminant)
Soient $A \subset B$ des anneaux avec B libre de rang m comme A-module. Soit $\{\beta_1, \ldots, \beta_m\}$ des éléments de B. Le *discriminant de la famille* $\{\beta_1, \ldots, \beta_m\}$ est
$$\mathrm{disc}(\{\beta_1, \ldots, \beta_m\}) := \det(\mathrm{Tr}_{B/A}(\beta_i\beta_j)).$$

1. Montrer que si l'on pose $\mathrm{disc}(B/A) := \mathrm{disc}(\{\text{base de } B/A\})$ on obtient un élément bien défini de $A/(A^\times)^2$.
   Dans le cas particulier où $A = \mathbb{Z}$ et B l'anneau d'entiers $\mathcal{O}_K$ d'un corps de nombres K, le discriminant $\mathrm{disc}(B/\mathbb{Z})$ est un élément bien défini de $\mathbb{Z}$, que l'on appelle *discriminant absolu de* $K/\mathbb{Q}$ et que l'on note $d_{K/\mathbb{Q}}$ ou $d_{\mathcal{O}_K/\mathbb{Z}}$ ou même d_K.
2. Supposons $A = \mathbb{Z}$. Soit N le sous-A-module de B engendré par $\{\gamma_1, \ldots, \gamma_m\}$. Montrer que si le module N est d'indice fini dans B alors
$$\mathrm{disc}(\{\gamma_1, \ldots, \gamma_m\}) = (B : N)^2 \,\mathrm{disc}(B/\mathbb{Z})$$
3. Soit $K = \mathbb{Q}[\alpha]$ un corps de nombres de degré n avec α un entier algébrique (justifier...). Montrer que si $d = \mathrm{disc}(1, x, \ldots, x^{n-1})$ on a
$$\mathbb{Z}[x] \subset \mathcal{O}_K \subset \frac{1}{d}\mathbb{Z}[x].$$

4. Soit $K = \mathbb{Q}[\alpha]$ un corps de nombres de degré n avec α un entier algébrique. Montrer que si $\mathrm{disc}(\{1, \alpha, \ldots, \alpha^{n-1}\})$ est sans facteur carré, alors

$$\mathcal{O}_K = \mathbb{Z}[\alpha] \quad \text{et} \quad d_K = \mathrm{disc}(\{1, \alpha, \ldots, \alpha^{n-1}\}).$$

5. Soit L/K une extension finie séparable de degré n. Soit $\sigma_1, \ldots, \sigma_n$ les K-homomorphismes distincts de L dans une clôture algébrique de L. Alors pour toute base $\beta_1, \ldots, \beta_n$ de L sur K, montrer que

$$\mathrm{disc}(\beta_1, \ldots, \beta_n) = \det(\sigma_i \beta_j)^2.$$

6. Soit $L = K[\beta]$ et $f(X)$ le polynôme minimal de β sur K. Supposons que $f(X)$ se factorise sous la forme $f(X) = \Pi(X - \beta_i)$ sur une clotûre algébrique de L. Montrer que

$$\mathrm{disc}(1, \beta, \ldots, \beta^{n-1}) = \prod_{i<j} (\beta_i - \beta_j)^2 = (-1)^{n(n-1)/2} \, \mathrm{Nm}_{L/K}(f'(\beta)).$$

   Ce nombre est appelé le *discriminant de* f et noté $\mathrm{disc}(f)$. On pourrait également le définir comme le résultant de f et f'.

Exercice 8 (Applications)
Soient k un corps, $a, b \in k$, $n \in \mathbb{N}\backslash\{0, 1\}$ et $P = X^n + aX + b$. On suppose que P est irréductible et **séparable**.

1. Montrer que

$$\mathrm{disc}(P) = (-1)^{\frac{n(n-1)}{2}} \left(n^n b^{n-1} + (-1)^{n+1}(n-1)^{n-1} a^n\right).$$

2. Cas particulier où $n = 2$ et $n = 3$.
3. On suppose $n = 3$. Soit x une racine de P dans une clôture algébrique $\overline{k}$ de k et K le corps de décomposition de $k(x)$ dans $\overline{k}$. Montrer que le groupe de Galois $\mathrm{Gal}(K/k)$ est soit isomorphe au groupe symétrique S_3 soit au groupe alterné A_3 et que

$$k(x) = K \iff [K : k] = 3 \iff \mathrm{disc}(P) \text{ est un carré dans } k.$$

4. Déterminer l'anneau des entiers de $\mathbb{Q}[x]$ où x est une racine du polynôme $X^3 - X - 1$ et le groupe de Galois de son corps de décomposition.
5. Calculer le discriminant d'une extension quadratique de $\mathbb{Q}$.

Feuille 5 :

Exercice 1 (Extensions cyclotomiques) On note $r \geq 1$, p premier, ζ une racine primitive p^r-ième de l'unité, $K = \mathbb{Q}[\zeta]$ et $\mathcal{O}_K$ son anneau d'entiers.

1. Montrer que K est une extension normale et que l'on a un morphisme injectif du groupe de Galois G_K vers le groupe $(\mathbb{Z}/p^r\mathbb{Z})^\times$ des inversibles de $\mathbb{Z}/p^r$. Montrer également que $\mathbb{Z}[\zeta] \subset \mathcal{O}_K$ et que $[\mathbb{Q}[\zeta] : \mathbb{Q}] \leq \varphi(p^r) = p^{r-1}(p-1)$.
2. On appelle *polynôme cyclotomique* Φ_{p^r} le polynôme $\prod_{\zeta \in \mu_{p^r} \text{primitive}} (X - \zeta)$. Montrer que
$$\Phi_{p^r} = \prod_{[i] \in (\mathbb{Z}/p^r\mathbb{Z})^\times} (X - \zeta^i) = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1}.$$
3. Soit ξ une autre racine primitive p^r-ième de l'unité. Montrer que $\frac{1-\zeta}{1-\xi}$ est une unité de $\mathcal{O}_K$ (*i.e.* est inversible dans $\mathcal{O}_K$).
4. Soit $\pi = 1 - \zeta$. En calculant $\Phi_{p^r}(1)$, montrer l'égalité d'idéaux dans $\mathcal{O}_K$, $(p) = (\pi)^{\varphi(p^r)}$. En déduire que le corps $\mathbb{Q}[\zeta]$ est de degré $\varphi(p^r)$ sur $\mathbb{Q}$ et que l'élément π est premier dans $\mathcal{O}_K$. Quels sont les premiers ramifiés dans $K/\mathbb{Q}$? Donner le degré résiduel f et l'indice de ramification e.
5. Calculer la valeur absolue du discriminant $|\operatorname{disc}(\mathbb{Z}[\zeta] : \mathbb{Z})| = \operatorname{Nm}_{K/\mathbb{Q}}(\Phi'_{p^r}(\zeta))$ (on pourra commencer par $r = 1$ avant de traiter le cas général). En déduire que $\operatorname{disc}(\mathcal{O}_k/\mathbb{Z})$ est une puissance de p et que $p^M \mathcal{O}_K \subset \mathbb{Z}[\zeta]$ pour tout entier M suffisamment divisible.
6. Montrer que $\mathbb{Z}[\zeta] + \pi^m \mathcal{O}_K = \mathcal{O}_K$ pour $m \geq 1$. En déduire que l'anneau des entiers de $\mathbb{Q}[\zeta]$ est $\mathbb{Z}[\zeta]$ et que le discriminant de $\mathcal{O}_K$ sur $\mathbb{Z}$ est de valeur absolue $p^{p^{r-1}(pr-r-1)}$.
7. Soit $p \neq 2$. On définit le symbole quadratique pour $n \in \mathbb{Z}$, par 0 si $(n, p) \neq 1$; et si $(n, p) = 1$ on pose
$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{si } n \text{ est un carré} \mod p \\ -1 & \text{sinon} \end{cases}$$
Soit ζ une racine primitive p-ième de l'unité et $S = \sum_{v=0}^{p-1} \left(\frac{v}{p}\right) \zeta^v$. Montrer que $S^2 = \left(\frac{-1}{p}\right) p$. En déduire que toute extension quadratique de $\mathbb{Q}$ est contenue dans une extension cyclotomique.

Exercice 2 (Norme numérique) Soient K un corps de nombres et $\mathcal{O}_K$ son anneau d'entiers. Soit $\mathfrak{a}$ un idéal non nul de $\mathcal{O}_K$. L'indice de $\mathfrak{a}$ dans $\mathcal{O}_K$ est fini et on note la *norme numérique* N :
$$\mathrm{N}(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a}).$$
Pour tout idéal $\mathfrak{p}$ premier de $\mathcal{O}_K$ au dessus d'un premier p, on pose $N_{K/\mathbb{Q}}(\mathfrak{p}) := p^{f(\mathfrak{p}/p)}$. On prolonge ceci multiplicativement aux idéaux fractionnaires de $\mathcal{O}_K$.

1. Soit $\mathcal{O}_K$ l'anneau des entiers d'un corps de nombres K. Soit $\mathfrak{a}$ un idéal dans $\mathcal{O}_K$, montrer que $N_{K/\mathbb{Q}}(\mathfrak{a}) = \mathrm{N}(\mathfrak{a})$; en déduire $\mathrm{N}(\mathfrak{ab}) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b})$.

2. En déduire (*cf.* Samuel p.62) que pour tout entier $x \in \mathcal{O}_K$, on a $N_{K/\mathbb{Q}}(x) = \pm \mathrm{N}_{K/\mathbb{Q}}(x\mathcal{O}_K)\mathbb{Z}$.
3. Soient $\mathfrak{b} \subset \mathfrak{a}$ des idéaux fractionnaires de K. Montrer que $(\mathfrak{a} : \mathfrak{b}) = \mathrm{N}(\mathfrak{a}^{-1}\mathfrak{b})$.
4. Montrer que $\alpha \in K$ est une unité si et seulement si $\alpha \in \mathcal{O}_K$ et $N_{K/\mathbb{Q}}(\alpha) = \pm 1$.
5. Soit $\alpha \in K$. Si $N_{K/\mathbb{Q}}(\alpha) = \pm 1$, α est-il forcément une unité dans K ?

Exercice 3 (Clôture algébrique de $\mathbb{Q}_p$) Notons $\overline{\mathbb{Q}}_p$ une clôture algébrique de $\mathbb{Q}_p$. Supposons par l'absurde que $\overline{\mathbb{Q}}_p$ est complet et posons $\alpha = \sum_{n=1}^{\infty} \zeta_{n'} p^n$ avec $n' = \begin{cases} n & \text{si } (n,p) = 1 \\ 1 & \text{sinon} \end{cases}$ où ζ_m est une racine primitive m-ieme de l'unité. Posons $K = \mathbb{Q}_p(\alpha)$.

1. Montrer que $\forall m \in \mathrm{N}$, $\zeta_{m'} \in \mathcal{O}_K$.
2. En déduire que $\overline{\mathbb{Q}}_p$ n'est pas complet.

Exercice 4 (Lemme de Krasner) Soit K un corps complet pour une valuation non-archimédienne. Soit α, β deux éléments d'une clôture algébrique $\overline{K}$ de K avec α séparable sur $K(\beta)$. On dit que α *appartient à* β si pour tout conjugé $\sigma\alpha \neq \alpha$ de α,

$$|\beta - \alpha| < |\sigma\alpha - \alpha|$$

(où $|\cdot|$ désigne l'unique extension de la valeur absolue de K).

1. Montrer que si α appartient à β alors $K(\alpha) \subset K(\beta)$.
2. Si $f = \sum_{i=0}^{n} a_i X^i \in K[X]$, on pose $|f| := \max_{0 \leq i \leq n} |a_i|$. Soient f et g deux éléments de $K[X]$ unitaires, de même degré n. On suppose que f est irréductible sur K et séparable. Montrer que si $|f - g|$ est suffisamment petite, alors g est aussi irréductible. De plus dans ce cas, si α est une racine de f dans $\overline{K}$ montrer qu'il existe une racine β de g dans $\overline{K}$ telle que $K(\alpha) = K(\beta)$.

Exercice 5 (Extensions totalement ramifiées) Soit K un corps de caractéristique nulle, valué ultramétrique de valuation discrète, complet, d'anneau de valuation A, d'idéal maximal $\mathfrak{p}$, d'uniformisante π et de corps résiduel fini (ceci est notamment vérifiée par $\mathbb{Q}_p$). Montrer qu'il n'y a, à isomorphisme près, qu'un nombre fini d'extensions de K totalement ramifiées de degré fixé.

Exercice 6 (Applications de Krasner)

1. Soient $\overline{\mathbb{Q}}_p$ une clôture algébrique de $\mathbb{Q}_p$ et $\mathbb{C}_p$ la complétion de $\overline{\mathbb{Q}}_p$. Montrer que $\mathbb{C}_p$ est algébriquement clos.
2. Soit K une extension finie de $\mathbb{Q}_p$. Montrer qu'il existe une extension finie L de $\mathbb{Q}$ contenue dans K telle que $[L : \mathbb{Q}] = [K : \mathbb{Q}_p]$ et $L\mathbb{Q}_p = K$.

Feuille 6

Exercice 1 (Borne de Minkowski et ramification) Soient K une extension de degré n de $\mathbb{Q}$, d_K le discriminant de $K/\mathbb{Q}$, $2s$ le nombre de plongements complexes non réels de K. On rappelle le résultat suivant appelé *borne de Minkowski* : il existe un ensemble de représentants du groupe des classes de K composé d'idéaux entiers $\mathfrak{a}$ de K tels que

$$\mathrm{N}(\mathfrak{a}) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s |d_K|^{1/2}$$

1. Trouver le nombre de classes des corps suivants : $K = \mathbb{Q}[i]$, $\mathbb{Q}[\sqrt{-5}]$.
2. Soient $x = (11)^{1/3}$ et $K = \mathbb{Q}(x)$. Notons $\mathcal{O}_K$ l'anneau des entiers de K, U_K son groupe d'unités et C_K son groupe des classes d'idéaux.
   Montrer[1] que $\mathcal{O}_K = \mathbb{Z}[x]$. Montrer que C_K est engendré par au plus deux éléments (on pourra étudier la décomposition en premiers de $2\mathcal{O}_K, \ldots, 13\mathcal{O}_K$). En considérant l'idéal $\mathfrak{p}_2 = (2, x-1)$, montrer que $x^2 - 5$ est dans $\mathfrak{p}_2^2$ et de norme 4. En déduire que $|C_K| \leq 2$.
3. Montrer[2] qu'il n'existe pas d'extension non ramifiée de $\mathbb{Q}$.

Exercice 2 (Nombre de classes de $\mathbb{Q}[\zeta_{23}]$)

1. Décrire le groupe de Galois $\mathrm{Gal}(\mathbb{Q}[\zeta_{23}]/\mathbb{Q})$. En déduire l'unique extension quadratique K de $\mathbb{Q}$ contenue dans K.
2. On admet que le nombre de classes de K vaut 3. En déduire que le nombre de classes de $\mathbb{Q}[\zeta_{23}]$ est strictement supérieur à 1 (on pourra étudier l'idéal $2\mathcal{O}_K$).

[1] On rappelle le résultat suivant :

Théorème 0.1 Si A est un anneau de valuation discrète (DVR), d'idéal maximal $\mathfrak{p}$, de corps résiduel k ; si $f \in A[X]$ est de degré $n \geq 1$ et est d'Eisenstein pour $\mathfrak{p}$, alors, l'anneau $B := A[X]/(f)$ est DVR, d'idéal maximal engendré par x (image de X dans B), de corps résiduel k.

[2] Ceci n'est en général plus vrai pour des corps autres que $\mathbb{Q}$: c'est la notion de corps de classes de Hilbert.

Feuille 7

Exercice 1 Soit K un corps complet pour une valuation discrète d'uniformisante π. Un polynôme $f(X) \in K[X]$ est dit *polynôme d'Eisenstein* si

$$f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n$$

avec $|a_0| = 1, |a_i| < 1, |a_n| = |\pi|$.

1. Soit L une extension finie de K. Montrer que L/K est totalement ramifiée si et seulement si $L = K[\alpha]$ avec α racine d'un polynôme d'Eisenstein.
2. Supposons que L/K est totalement ramifiée. Soit A et B les anneaux de valuations discrètes de K et L. Soit Π un élément premier dans B. Montrer que $B = A[\Pi]$.

Exercice 2 Le groupe topologique $\mathbb{A}_{\mathbb{Q}}^{\times}$

1. En considérant les adèles x_p valant p à la place $\mathbb{Q}_p$ et 1 à toutes les autres places, montrer que $\mathbb{A}_{\mathbb{Q}}^{\times}$ muni de la restriction de la topologie de $\mathbb{A}_{\mathbb{Q}}$ n'est pas un groupe topologique.
2. Soient K un corps de nombres et $i : \mathbb{A}_K^{\times} \hookrightarrow \mathbb{A}_K \times \mathbb{A}_K$, $x \mapsto (x, x^{-1})$. On munit $i(\mathbb{A}_K^{\times})$ de la topologie restreinte de celle sur $\mathbb{A}_K \times \mathbb{A}_K$ et on met sur $\mathbb{A}_K^{\times}$ la topologie telle que i est un homéomorphisme sur son image. Montrer que muni de cette topologie, le groupe $\mathbb{A}_K^{\times}$ est un groupe topologique et que l'application $j : \mathbb{A}_K^{\times} \hookrightarrow \mathbb{A}_K$ est continue.
3. En voyant $\mathbb{A}_K^{\times}$ comme le produit restreint des $K_v^{\times}$ relativement aux $\mathcal{O}_{K_v}^{\times}$ et en mettant sur $\mathbb{A}_K^{\times}$ la topologie limite inductive qui en découle, montrer que cette topologie est la même que la précédente.

Exercice 3 Soit K un corps de nombres et $\mathbb{I}_K$ le groupe des idèles sur K. En considérant l'application volume

$$\mathrm{vol} : \mathbb{I}_K \to \mathbb{R}_+^*, \quad (x_v) \mapsto \prod_v |x_v|_v,$$

montrer que $\mathbb{I}_K/K^*$ n'est pas compact.

Exercice 4 ($\mathbb{I}_K^1/K^*$ compact $\Rightarrow$ $\mathrm{Cl}(\mathcal{O}_K)$ fini) Soit K un corps de nombres. On rappelle que l'on a un morphisme de groupes entres les idèles de K et les idéaux fractionnaires de K :

$$\varphi : \mathbb{I}_K \to \mathrm{Div}(\mathcal{O}_K), \quad x = (x_v) \mapsto \prod_{v \nmid \infty} \mathfrak{p}_v^{\mathrm{val}(x_v)}.$$

Montrer que si l'on munit $\mathrm{Div}(\mathcal{O}_K)$ de la topologie discrète, ce morphisme est continu et que $\varphi_{|\mathbb{I}_K^1}$ est surjectif. En déduire la finitude du groupe des classes $\mathrm{Cl}(\mathcal{O}_K)$.

Exercice 5 ($\mathbb{I}_K^1/K^*$ compact $\Rightarrow$ Théorème des unités) Soient K un corps de nombres et S un ensemble fini de places, contenant les places à l'infini. On note

$$H_S = \{x \in K \mid \ \forall v \notin S \ \ |x|_v = 1\}$$

le *groupe des S-unités*.

1. Vérifier que H_S est un sous-groupe de K^*.
2. Soient $0 < c \leq C < +\infty$. Montrer que l'ensemble des S-unités x vérifiant $c \leq |x|_v \leq C$ pour tout $v \in S$ est fini.
3. Notons $\mu_\infty(K)$ le groupe des racines de l'unités dans K. Déduire de la question précédente que si $x \in K$, on a

$$|x|_v = 1 \ \ \forall v \iff x \in \mu_\infty(K).$$

4. On suppose désormais que $S = S_\infty$ est l'ensemble des places archimédiennes de K. On note $J_S = \{x \in \mathbb{I}_K \mid \ \forall v \notin S \ |x_v|_v = 1\}$ et on pose $J_S^1 = J_S \cap \mathbb{I}_K^1$. On introduit également le plongement logarithmique

$$\lambda : J_S \to (\mathbb{R})^s, \quad \alpha \mapsto (\log |\alpha_i|_i)_{1 \leq i \leq s} \quad \text{avec } s = \mathrm{Card}(S).$$

   Montrer que λ est surjective, continue. Montrer que $\ker(\lambda_{|H_S})$ est cyclique et que $\lambda(H_S)$ est discret.
5. Considérant $\lambda(J_S^1)$ montrer que $\lambda(H_S)$ est libre de rang $s - 1$.

Feuille 5 : Frobenius et début de courbes elliptiques

Exercice 1 (Rappels sur le groupe de décomposition et sur Frobenius) Dans la suite on considère une extension E/F galoisienne de corps de nombres, de degré n, de groupe de Galois G. Soit $\mathfrak{p}$ un idéal maximal de $\mathcal{O}_F$. Le groupe G agit sur les idéaux maximaux $\mathfrak{P}$ de $\mathcal{O}_E$ au-dessus de $\mathfrak{p}$.

1. Montrer que cette action est transitive (on raisonnera par l'absurde en appliquant le lemme Chinois aux idéaux $\mathfrak{P}' \notin \omega(\mathfrak{P})$ et $\sigma(\mathfrak{P})$ pour tout $\sigma \in G$).
2. Fixons désormais un idéal $\mathfrak{P}$ au-dessus de $\mathfrak{p}$. On rappelle que le *groupe de décomposition* de $\mathfrak{P}/\mathfrak{p}$, noté $D(\mathfrak{P}/\mathfrak{p})$, est le stabilisateur de $\mathfrak{P}$ dans G. Rappeler pourquoi (en notant e l'indice de ramification et f le degré résiduel)
$$|D(\mathfrak{P}/\mathfrak{p})| = ef \quad \text{et} \quad \forall \sigma \in G, \quad D(\sigma\mathfrak{P}/\mathfrak{p}) = \sigma D(\mathfrak{P}/\mathfrak{p})\sigma^{-1}.$$
On note $I(\mathfrak{P}/\mathfrak{p})$ le noyau du morphisme naturel φ de $D(\mathfrak{P}/\mathfrak{p})$ vers $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$: c'est le *groupe d'inertie*.
3. Vérifier que $I(\sigma\mathfrak{P}/\mathfrak{p}) = \sigma I(\mathfrak{P}/\mathfrak{p})\sigma^{-1}$.
4. On rappelle (cours) que φ est un morphisme surjectif. En déduire que,
$$|I(\mathfrak{P}/\mathfrak{p})| = e,$$
et donc que si $\mathfrak{p}$ est non-ramifié dans E/F, alors φ est un isomorphisme.
5. On suppose désormais que $\mathfrak{p}$ est non-ramifié dans E/F. On note $\mathrm{Frob}_{\mathfrak{P}}(E/F)$ ou $(\mathfrak{P}, E/F)$ l'unique élément de $D(\mathfrak{P}/\mathfrak{p})$ dont l'image par φ est l'automorphisme de Frobenius pour $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$: on appelle cet automorphisme l'*automorphisme de Frobenius de* $\mathfrak{P}/\mathfrak{p}$. Autrement dit, c'est l'unique $\sigma \in G$ vérifiant :
$$\sigma \in D(\mathfrak{P}/\mathfrak{p}) \ \text{ et } \ \forall x \in \mathcal{O}_E, \ \sigma(x) = x^{|\mathbb{F}_{\mathfrak{p}}|} \mod \mathfrak{P}.$$
Quel est l'ordre de $\mathrm{Frob}_{\mathfrak{P}}(E/F)$? Vérifier que
$$\forall \sigma \in G, \quad (\sigma\mathfrak{P}, E/F) = \sigma(\mathfrak{P}, E/F)\sigma^{-1}.$$
[Notons que si E/F est abélien, ceci montre que $(\mathfrak{P}, E/F)$ est indépendant du choix de $\mathfrak{P}$ au-dessus de $\mathfrak{p}$: on le note dans ce cas $(\mathfrak{p}, E/F)$ (ou $\mathrm{Frob}_{\mathfrak{p}}(E/F)$ ou même $\mathrm{Frob}_{\mathfrak{p}}$ si le contexte est clair).]
6. Caractériser le fait que $\mathfrak{p}$ est totalement décomposé en terme des Frobenius $\mathrm{Frob}_{\mathfrak{P}}$.
7. Si K est une extension intermédiaire : $F \subset K \subset E$, et si $\mathfrak{p}_K := \mathfrak{P} \cap \mathcal{O}_K$, montrer que
$$\mathrm{Frob}_{\mathfrak{P}/\mathfrak{p}_K} = \left(\mathrm{Frob}_{\mathfrak{P}/\mathfrak{p}}\right)^{f(\mathfrak{p}_K/\mathfrak{p})}.$$

Exercice 2 (Loi de réciprocité quadratique via Frobenius) Soit $\Delta \in \mathbb{Z} - \{0, 1\}$ sans facteur carré. On note $K = \mathbb{Q}(\sqrt{\Delta})$ l'extension quadratique d'anneau d'entiers $\mathcal{O}_K$. On rappelle que
$$O_K = \begin{cases} \mathbb{Z}\left[\sqrt{\Delta}\right] \text{ si } \Delta = 2, 3 \mod 4 \text{ et dans ce cas } d_K = 4\Delta. \\ \mathbb{Z}\left[\frac{1+\sqrt{\Delta}}{2}\right] \text{ si } \Delta = 1 \mod 4 \text{ et dans ce cas } d_K = \Delta. \end{cases}$$

Dans la suite on fixe un nombre premier p impair, ne divisant pas Δ (i.e. non-ramifié). Soit par ailleurs ζ une racine primitive p-ième de l'unité et $F = \mathbb{Q}(\zeta)$.

1. En étudiant l'anneau $\mathcal{O}_K/p\mathcal{O}_K$, montrer que p est totalement décomposé dans $\mathcal{O}_K$ si et seulement si $\left(\frac{\Delta}{p}\right) = 1$.
2. En déduire la valeur du Frobenius $\mathrm{Frob}_p(K/\mathbb{Q}) \in \mathrm{Gal}(K/\mathbb{Q})$.
3. Montrer que F contient une unique extension quadratique K de $\mathbb{Q}$. Déterminer Δ tel que $F = \mathbb{Q}(\sqrt{\Delta})$.
4. Soit q un nombre premier impair distinct de p.
5. Calculer $(q, F/\mathbb{Q})$ et en déduire $(q, K/\mathbb{Q})_{|F}$.
6. En déduire[1] la loi de réciprocité quadratique :

$$\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{p}{q}\right).$$

Exercice 3 Soit $E/\mathbb{C}$ une courbe elliptique, de réseau associé Λ. On note ω_1, ω_2 des générateurs de Λ. On rappelle que l'anneau des endomorphismes de E est isomorphe à $\mathcal{R} := \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subset \Lambda\}$. Par ailleurs si $K/\mathbb{Q}$ est un corps de nombres, on dit que $\mathcal{R}$ est un *ordre de* K si c'est un sous-anneau de K, qui est un $\mathbb{Z}$-module de type fini et tel que $\mathcal{R} \otimes \mathbb{Q} = K$. Montrer que

1. Soit $\mathrm{End}(E) = \mathbb{Z}$;
2. Soit $K := \mathbb{Q}(\omega_1/\omega_2)$ est une extension quadratique imaginaire de $\mathbb{Q}$ et $\mathrm{End}(E)$ est isomorphe à un ordre de K.

Exercice 4 Soit K un corps de caractéristique 0 et ℓ un nombre premier. Pour tout entier $n \geq 1$ on note $\mu_{\ell^n} \subset \overline{K}^*$ le groupe des racines ℓ^n-ieme de 1. L'application $x \mapsto x^\ell$ permet de définir la limite projective (justifier) des μ_{ℓ^n} : on note $T_\ell(\mu)$ cette limite projective (c'est le module de Tate de μ).

1. Décrire $T_\ell(\mu)$ en tant que groupe abstrait.
2. Montrer que l'on a une représentation ℓ-adique naturelle (le *caractère cyclotomique*) de $\mathrm{Gal}(\overline{K}/K)$ vers $\mathrm{Aut}(T_\ell(\mu)) \simeq \mathbb{Z}_\ell^\times$.

Exercice 5 Soit K un corps de caractéristique nulle et ℓ un nombre premier. Montrer que la donnée des accouplements

$$\forall n \geq 1, \quad e_{\ell^n} : E[\ell^n] \times E[\ell^n] \to \mu_{\ell^n}$$

donne naissance à un accouplement de Weil ℓ-adique au niveau des modules de Tate.

Exercice 6 Soient E/K une courbe elliptique sur un corps K de caractéristique 0, et $n \geq 1$.

1. En utilisant le formalisme de l'accouplement de Weil, montrer qu'il existe des points $P, Q \in E[n]$ tels que $e_n(P, Q)$ est une racine primitive n-ieme de l'unité.
2. En déduire que si K est tel que $E[n] \subset E(K)$ alors $\mu_n \subset K^\times$.

Exercice 7 Montrer que le groupe $E(\mathbb{R})$ des points $\mathbb{R}$-rationnels d'une courbe elliptique n'est pas de type fini (alors que l'on sait par un théorème de Mordell que $E(K)$ est de type fini si K est un corps de nombres).

[1] On rappelle que -1 est un carré dans $\mathbb{F}_p$ si et seulement si $p = 1 \mod 4$.

Feuille 8

Exercice 1 (Rappels sur le groupe de décomposition et sur Frobenius) Dans la suite on considère une extension E/F galoisienne de corps de nombres, de degré n, de groupe de Galois G. Soit $\mathfrak{p}$ un idéal maximal de $\mathcal{O}_F$. Le groupe G agit transitivement sur les idéaux maximaux $\mathfrak{P}$ de $\mathcal{O}_E$ au-dessus de $\mathfrak{p}$. On fixe désormais un idéal $\mathfrak{P}$ au-dessus de $\mathfrak{p}$.

1. On rappelle que le *groupe de décomposition* de $\mathfrak{P}/\mathfrak{p}$, noté $D(\mathfrak{P}/\mathfrak{p})$, est le stabilisateur de $\mathfrak{P}$ dans G. Montrer que (en notant e l'indice de ramification et f le degré résiduel)
$$|D(\mathfrak{P}/\mathfrak{p})| = ef \quad \text{et} \quad \forall \sigma \in G, \quad D(\sigma\mathfrak{P}/\mathfrak{p}) = \sigma D(\mathfrak{P}/\mathfrak{p})\sigma^{-1}.$$
On note $I(\mathfrak{P}/\mathfrak{p})$ le noyau du morphisme naturel φ de $D(\mathfrak{P}/\mathfrak{p})$ vers le groupe de Galois des corps résiduels $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$: c'est le *groupe d'inertie*.
2. Vérifier que $I(\sigma\mathfrak{P}/\mathfrak{p}) = \sigma I(\mathfrak{P}/\mathfrak{p})\sigma^{-1}$.
3. On rappelle (théorème non-trivial de cours) que φ est un morphisme surjectif. En déduire que,
$$|I(\mathfrak{P}/\mathfrak{p})| = e,$$
et que, $\mathfrak{p}$ est non-ramifié dans E/F si et seulement si φ est un isomorphisme.
4. On suppose désormais que $\mathfrak{p}$ est non-ramifié dans E/F. On note $\mathrm{Frob}_{\mathfrak{P}}(E/F)$ ou $(\mathfrak{P}, E/F)$ l'unique élément de $D(\mathfrak{P}/\mathfrak{p})$ dont l'image par φ est l'automorphisme de Frobenius pour $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$: on appelle cet automorphisme l'*automorphisme de Frobenius de* $\mathfrak{P}/\mathfrak{p}$. Autrement dit, c'est l'unique $\sigma \in G$ vérifiant :
$$\sigma \in D(\mathfrak{P}/\mathfrak{p}) \ \text{ et } \ \forall x \in \mathcal{O}_E, \ \sigma(x) = x^{|\mathbb{F}_{\mathfrak{p}}|} \mod \mathfrak{P}.$$
Quel est l'ordre de $\mathrm{Frob}_{\mathfrak{P}}(E/F)$? Vérifier que
$$\forall \sigma \in G, \quad (\sigma\mathfrak{P}, E/F) = \sigma(\mathfrak{P}, E/F)\sigma^{-1}.$$
[Notons que si E/F est abélien, ceci montre que $(\mathfrak{P}, E/F)$ est indépendant du choix de $\mathfrak{P}$ au-dessus de $\mathfrak{p}$: on le note dans ce cas $(\mathfrak{p}, E/F)$ (ou $\mathrm{Frob}_{\mathfrak{p}}(E/F)$ ou même $\mathrm{Frob}_{\mathfrak{p}}$ si le contexte est clair).]
5. Caractériser le fait que $\mathfrak{p}$ est totalement décomposé en terme des Frobenius $\mathrm{Frob}_{\mathfrak{P}}$.
6. Si K est une extension intermédiaire : $F \subset K \subset E$, et si $\mathfrak{p}_K := \mathfrak{P} \cap \mathcal{O}_K$, calculer $\mathrm{Frob}_{\mathfrak{P}/\mathfrak{p}_K}$ en fonction de $\mathrm{Frob}_{\mathfrak{P}/\mathfrak{p}}$.

Exercice 2 (Loi de réciprocité quadratique via Frobenius) Soit $\Delta \in \mathbb{Z} - \{0, 1\}$ sans facteur carré. On note $K = \mathbb{Q}(\sqrt{\Delta})$ l'extension quadratique d'anneau d'entiers $\mathcal{O}_K$. On rappelle que
$$\mathcal{O}_K = \begin{cases} \mathbb{Z}\left[\sqrt{\Delta}\right] & \text{si } \Delta = 2, 3 \mod 4 \text{ et dans ce cas } d_K = 4\Delta. \\ \mathbb{Z}\left[\frac{1+\sqrt{\Delta}}{2}\right] & \text{si } \Delta = 1 \mod 4 \text{ et dans ce cas } d_K = \Delta. \end{cases}$$
Dans la suite on fixe un nombre premier p impair, ne divisant pas Δ. Soit par ailleurs ζ une racine primitive p-ième de l'unité et $F = \mathbb{Q}(\zeta)$. On rappelle qu'en étudiant l'anneau $\mathcal{O}_K/p\mathcal{O}_K$, on montre que p est totalement décomposé dans $\mathcal{O}_K$ si et seulement si $\left(\frac{\Delta}{p}\right) = 1$.

1. Calculer le Frobenius $\mathrm{Frob}_p(K/\mathbb{Q}) \in \mathrm{Gal}(K/\mathbb{Q})$.
2. Montrer que F contient une unique extension quadratique K de $\mathbb{Q}$. Déterminer Δ tel que $F = \mathbb{Q}(\sqrt{\Delta})$.
3. Soit q un nombre premier impair distinct de p. Calculer $(q, F/\mathbb{Q})$ et en déduire $(q, F/\mathbb{Q})_{|K}$.
4. En déduire[1] la loi de réciprocité quadratique :

$$\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{p}{q}\right).$$

Exercice 3 Corps résiduel (du complété) de la clôture algébrique d'un corps ultramétrique)

1. Soit K un corps ultramétrique algébriquement clos. Montrer que sont corps résiduel k_K est algébriquement clos.
2. Montrer que si K est un corps ultramétrique, de clôture algébrique $\overline{K}$, alors $k_{\overline{K}} = \overline{k_K}$.
3. Montrer que si K est ultramétrique et algébriquement clos, de complété $\widehat{K}$, alors $k_K = k_{\widehat{K}}$.

Exercice 4 1. Montrer que $\mathbb{Q}_p$ n'a pas de sous-groupe discret non nul.
2. Donner une famille infinie d'exemples de sous-groupes discrets de $\mathbb{Q}_p^*$.

Exercice 5 (Ax-Sen-Tate) Dans la suite on note $\mathrm{G}_{\mathbb{Q}_p}$ le groupe de Galois absolu de $\overline{\mathbb{Q}_p}$ sur $\mathbb{Q}_p$ et v la valuation p-adique normalisée par $v(p) = 1$.

1. Soit $\sigma \in \mathrm{G}_{\mathbb{Q}_p}$. Montrer que l'on peut étendre continuement σ sur $\mathbb{C}_p$.
2. On veut montrer dans la suite que $\mathbb{Q}_p = C_p^{\mathrm{G}_{\mathbb{Q}_p}}$. On commence pour cela par admettre la proposition suivante (due à Ax) : " il existe $C > 0$ telle que

$$\forall x \in \overline{\mathbb{Q}}_p, \quad \exists a \in \mathbb{Q}_p, \quad v(x-a) \geq \inf_{\sigma \in \mathrm{G}_{\mathbb{Q}_p}} v(\sigma(x) - x) - C. \ \text{"}$$

   Montrer comment en déduire le résultat.
3. Dans la suite on veut prouver la proposition précédente.
4. Soit $P = X^n + a_{n-1}X^{n-1} = \ldots + a_0 \in \overline{\mathbb{Q}}_p[X]$ unitaire de degré n tel que toutes ses racines vérifient $v(\alpha) \geq u$ (pour un certain rationnel u).
   (a) Vérifier que $v(a_{n-i}) \geq iu$ pour tout i.
   (b) Soit $q = p^k$ un diviseur de n. Montrer que la dérivée q-ieme, $P^{(q)}$ de P admet une racine β telle que

$$v(\beta) \geq u - \frac{1}{n-q} v\left(\frac{n!}{q!(n-q)!}\right).$$

   (c) Si $n = p^k d$ avec $d \wedge k = 1$ et $d > 0$, montrer que la dérivée q-ieme, $P^{(q)}$ de P admet une racine β telle que $v(\beta) \geq u$.

[1] On rappelle que -1 est un carré dans $\mathbb{F}_p$ si et seulement si $p = 1 \mod 4$.

(d) Si $n = p^{k+1}$, montrer que la dérivée q-ieme, $P^{(q)}$ de P admet une racine β telle que $v(\beta) \geq u - \frac{1}{p^{k+1}-p^k}$.

5. Si $x \in \overline{\mathbb{Q}}_p$ est de degré n sur $\mathbb{Q}_p$ et si $\ell(n)$ est le plus grand entier ℓ tel que $p^\ell \leq n$, montrer qu'il existe $a \in \mathbb{Q}_p$ tel que (en notant $\Delta(x) := \inf_{\sigma \in \mathrm{G}_{\mathbb{Q}_p}} v(\sigma(x) - x)$)

$$v(x-a) \geq \Delta(x) - \sum_{i=1}^{\ell(n)} \frac{1}{p^i - p^{i-1}}.$$

6. Conclure.

Soit K un corps parfait. Soit V un $\overline{K}$-espace vectoriel. On dit que $\mathrm{Gal}(\overline{K}/K)$ (noté également G_K) *agit continument* sur V si pour tout $v \in V$ le stablisateur $\{\sigma \in G_K \mid v^\sigma = v\}$ est fermé d'indice fini dans G_K. (Ceci équivaut à dire que l'action $G_K \times V \to V$ est continue pour la topologie discrète sur V).

Exercice 6 (Action de Galois)

1. Montrer que G_K agit continument sur $\overline{K}$ pour son action naturelle.
2. Soit V un $\overline{K}$-espace vectoriel tel que G_K agit continument et de manière compatible à son action sur $\overline{K}$. Posons

$$V_K := V^{G_K} = \{v \in V \mid \forall \sigma \in G_K,\ v^\sigma = v\}.$$

Fixons $v \in V$.

(a) Montrer qu'il existe une extension galoisienne L/K finie telle que v est fixé par G_L.

(b) Montrer que v peut s'écrire comme une combinaison linéaire à coefficients dans $\overline{K}$ d'éléments de V_K (on pourra considérer la matrice $(\sigma_i \alpha_j)$ où $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Gal}(L/K)$ et où les α_j forment une base de L/K).

(c) En déduire que $V \simeq V_K \otimes_K \overline{K}$.

3. Que dire dans le cas de $\mathbb{C}_p$ et de $G_{\mathbb{Q}_p}$?

Feuille 9

Dans toute la suite F est un corps de nombres. On note $\mathbb{A}_F$ l'anneau des adèles, $\mathbb{I}_F$ le groupe des idèles. Pour toute partie finie S contenant l'ensemble S_∞ des places à l'infini, on pose

$$\mathbb{I}_F^S := \prod_{v\in S} F_v^\times \times \prod_{v\notin S} \mathcal{O}_{F_v}^\times, \text{ et } \mathbb{I}_F^\infty := \mathbb{I}_F^{S_\infty}.$$

Exercice 1 1. Montrer que F est discret dans $\mathbb{A}_F$.

2. Montrer que $F^\times$ est discret dans $\mathbb{I}_F$.

Exercice 2 1. Montrer que le groupe des classes, $\mathrm{Cl}(\mathcal{O}_F)$ est isomorphe au quotient $\mathbb{I}_F/\mathbb{I}_F^\infty F^\times$.

2. Si S est une partie finie contenant S_∞ telle que les $\mathfrak{p}_v$, $v \in S - S_\infty$, engendrent le groupe des classes. Montrer que

$$\mathbb{I}_F = \mathbb{I}_F^S \cdot \mathbb{F}^\times.$$

3. Montrer que $\mathbb{I}_\mathbb{Q}$ est le produit direct de $\mathbb{Q}^*$ (plongé diagonalement) par $\mathbb{R}_+^\times \times \prod_p \mathbb{Z}_p^\times$.
4. Interpréter les inversibles de $\mathbb{Z}/n\mathbb{Z}$ comme un quotient de $\mathbb{I}_\mathbb{Q}/\mathbb{Q}^\times$.

Exercice 3 (Composante neutre de $\mathbb{I}_K$) Soit K un corps de nombres admettant r_1 plongements réels et r_2 paires de plongements complexes. Soient $\mathbb{I}_K$ le groupe des idèles de K et H sa composante connexe de l'identité. Montrer que H est contenu dans tous les sous groupes ouverts de $\mathbb{I}_K$. En déduire que $H = (\mathbb{C}^\times)^{r_2} \times (\mathbb{R}_+^\times)^{r_1}$.

Exercice 4 (Groupe des classes d'idèles) Soient p premier, $V = \Pi_{i\in\mathrm{N}}\mathbb{F}_p$ un produit dénombrable de copies de $\mathbb{F}_p$ et $W = \oplus_{i\in\mathrm{N}}\mathbb{F}_p \subset V$.

1. Construire un sous-groupe $W \subset W' \subset V$ propre d'indice fini dans V. Montrer qu'il n'est pas ouvert.
2. Montrer que pour tout nombre premier p, le groupe $\mathbb{Z}_p^\times$ admet un sous-groupe ouvert d'indice 2 (distinguer les cas $p = 2$ et p impair).
3. En déduire l'existence d'un sous-groupe d'indice fini du groupe des classes d'idèles $C_\mathbb{Q} = I_\mathbb{Q}/\mathbb{Q}^*$ qui n'est pas ouvert.

M2R Université de Paris-Sud
2008-2009 séance du 12 janvier 2008

Sur le théorème de Chebotarev

Exercice 1 Pour $h \in \mathbb{Z}[X]$, on définit

$$\mathrm{Spl}_1(h) := \{p \text{ premier } \mid \text{ il existe } n \in \mathbb{Z}, p \,|\, h(n)\}\,.$$

Pour K un corps de nombres, on définit

$$\mathrm{Spl}_1(K) := \{p \text{ premier } \mid \text{ il existe } \mathfrak{p}|p \text{ idéal premier dans } K \text{ avec } f(\mathfrak{p}|p) = 1\}\,.$$

1. Soit K un corps de nombres. Montrer que la densité analytique des premiers $\mathfrak{p}$ de $\mathcal{O}_K$ tels que $f(\mathfrak{p}/p) \geq 2$ est nulle.
2. Calculer $\mathrm{Spl}_1(T^2+1)$ et $\mathrm{Spl}_1(\mathbb{Q}(i))$.
3. Montrer plus généralement que si h est irréductible sur $\mathbb{Q}$ et si x est une racine de h dans une clôture algébrique, les ensembles $\mathrm{Spl}_1(h)$ et $\mathrm{Spl}_1(\mathbb{Q}(x))$ coincident à un nombre fini d'exceptions près.
4. Soit $m \in \mathbb{N}^*$ impair et K un corps de nombres. On définit

   $$S_1(m,K) := \{b \bmod m \,|\, p = b \bmod m \text{ pour une infinité de } p \in \mathrm{Spl}_1(K)\}\,.$$

   Montrer que

   $$S_1(m,K) = \{b \bmod m \,|\, b = q \bmod m,\ q \in \mathrm{Spl}_1(K) \text{ et } q \text{ non ramifié dans } K(\zeta_m)\}\,.$$

5. Montrer que $S_1(m,K)$ est l'image de $\mathrm{Gal}(K(\zeta_m)/K) \to \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. En déduire que pour tout corps de nombre K, $S_1(m,K)$ est un sous-groupe de $(\mathbb{Z}/m\mathbb{Z})^*$.
6. Un polynôme $h(T)$ est dit euclidien pour $a \mod m$ où $(a,m) = 1$ si presque tous les diviseurs premiers de tous les $h(n)$ satisfont $p \equiv a \mod m$ ou $p \equiv 1 \mod m$ et si une infinité d'entre eux satisfont $p \equiv a \mod m$. Montrer que s'il existe un polynôme euclidien pour $a \mod m$ alors $a^2 \equiv 1 \mod m$. (Murty 1988[1]).

Exercice 2 Si L/K est une extension finie de corps de nombres, on note $\mathcal{P}(L/K)$ l'ensemble des places finies v de K non ramifiées dans L/K telles qu'il existe une place w de L au-dessus de v de degré 1, *i.e.* telle que $f(w|v) = 1$.

[1]Schur avait montré la réciproque en 1912

1. Soit L/K une extension finie de corps de nombres. Soit N une extension galoisienne finie de K contenant L ; on note G le groupe de Galois de N sur K, H celui de N sur L. Soit v une place finie de K non ramifiée dans N/K et $\sigma \in G$ un Frobenius en v, *i.e.* l'automorphisme de Frobenius correspondant à une place de N au-dessus de v. Interpréter, en termes de H et de la classe de conjugaison de σ, le fait qu'il existe une place w de L au-dessus de v telle que $f(w/v) = 1$.
2. Soit L/K une extension finie de corps de nombres. Montrer que $\mathcal{P}(L/K)$ a une densité, qui est $\geq 1/[L : K]$, avec égalité si et seulement si L/K est galoisienne. Montrer que L/K est galoisienne si et seulement si tout élément de $\mathcal{P}(L/K)$ est totalement décomposé dans L (on rappelle qu'un premier $\mathfrak{p}$ de K est totalement décomposé dans L/K si et seulement si il est totalement décomposé de la cloture galoisienne de L/K).
3. Soit L/K une extension finie de corps de nombres et soit M une extension finie galoisienne de K. Montrer que les deux conditions suivantes sont équivalentes :
   (a) M/K est (isomorphe à) une sous-extension de L/K
   (b) $\mathcal{P}(L/K) - (\mathcal{P}(M/K) \cap \mathcal{P}(L/K))$ est de densité nulle (*i.e*, à un ensemble de densité nulle près, $\mathcal{P}(L/K)$ est inclus dans $\mathcal{P}(M/K)$).

Exercice 3 Soit $n \in \mathbb{Z}$.

1. Montrer que n est un carré dans $\mathbb{Z}$ si et seulement si pour tout p premier suffisamment grand, n est un carré modulo p.
2. Plus généralement soit ℓ un nombre premier. Montrer que n est une puissance ℓ-ème dans $\mathbb{Z}$ si et seulement si pour tout p premier suffisamment grand, n est une puissance ℓ-ème modulo p.
3. En utilisant la question 1 de l'exercice 2 de la feuille précédente montrer plus généralement que si K est un corps de nombres et si $f \in K[X]$ est irréductible et tel que pour un ensemble de $\mathfrak{p}$ premiers de K de densité 1, la réduction $f \mod \mathfrak{p}$ admet une racine dans $\mathcal{O}_K/\mathfrak{p}$, alors f admet une racine sur K et est donc de degré 1 (on pourra montrer et utiliser le fait que si H est un sous-groupe strict d'un groupe fini G alors la réunion des conjugués de H est différente de G).