Université de Paris-Sud
2006-2007

Feuille 1

1. Extensions quadratiques

Soit K une extension quadratique de $\mathbb{Q}$. On note $\mathcal{O}$ la clôture intégrale de $\mathbb{Z}$ dans K :

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

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

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

1.2 En déduire $\mathcal{O}$.

2. 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

$$\forall y \in L, \quad \mathrm{Tr}_{L/K}\, y = \sum_{i=1}^{n} \sigma_i(y) \quad \text{et} \quad \mathrm{Nm}_{L/K}(y) = \prod_{i=1}^{n} \sigma_i(y).$$

3. 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

$$\operatorname{disc}(\{\gamma_1, \ldots, \gamma_m\}) = (B : N)^2 \operatorname{disc}(B/\mathbb{Z})$$

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

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

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

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

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

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

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

4. Application

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

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

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 $\operatorname{Gal}(K/k)$ est soit isomorphe au groupe symétrique S_3 soit au groupe alterné A_3 et que

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

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 $\mathbb{Q}$.

5. Extensions cyclotomiques

1. 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 $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ sa décomposition en idéaux premiers dans B. Soit $f_i = [B/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$, $1 \leq i \leq g$ le degré d'inertie. On rappelle que

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

   Dans la suite 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.

2. Montrer que K est une extension normale et que l'on a un morphsime 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 $[\mathbb{Q}[\zeta] : \mathbb{Q}] \leq \varphi(p^r) = p^{r-1}(p-1)$.
3. On appelle *polynôme cyclotomique* Φ_{p^r} le polynôme $\prod_{\zeta \in \mu_{p^r} \text{primitive}} (X - \zeta)$. Montrer que

$$\Phi_{p^r} = \prod_{[i] \in (\mathbb{Z}/p^r\mathbb{Z})^\times} (X - \zeta^i) = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1}.$$

4. 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 $\mathcal{O}_K$).
5. 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 $\mathcal{O}_K$.
6. Calculer la valeur absolue du discriminant $|\operatorname{disc}(\mathbb{Z}[\zeta] : \mathbb{Z})| = \operatorname{Nm}(\Phi'_{p^r}(\zeta))$ (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.
7. 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 $p^{p^{r-1}(pr-r-1)}$.
8. Soient K, L des extensions finies de $\mathbb{Q}$ vérifiant

$$[KL : \mathbb{Q}] = [K : \mathbb{Q}][L : \mathbb{Q}].$$

   Soit $d = pgcd(d_{K/\mathbb{Z}}, d_{L/\mathbb{Z}})$. Montrer que

$$\mathcal{O}_{KL} \subset d^{-1} \mathcal{O}_K \cdot \mathcal{O}_L$$

   (Considérer $\{\alpha_1, \ldots, \alpha_m\}$ (resp. $\{\beta_1, \ldots, \beta_n\}$) une base intégrale de K sur $\mathbb{Q}$ (resp. de L sur $\mathbb{Q}$). Soit $\gamma \in \mathcal{O}_{KL}$. On pourra écrire $\gamma = \sum \frac{a_{i,j}}{r} \alpha_i \beta_j$ avec r minimal et montrer que r divise d).
9. sous les hypothèses précédentes et si $d = 1$, montrer que

$$d_{KL/\mathbb{Z}} = d_{K/\mathbb{Z}}^{[L:\mathbb{Q}]} d_{L/\mathbb{Z}}^{[K:\mathbb{Q}]}.$$

   En déduire que

$$|\operatorname{disc}(\mathbb{Z}[\zeta_n]/\mathbb{Z})| = \frac{n^{\varphi(n)}}{\Pi_{p|n} p^{\varphi(n)/(p-1)}}.$$

10. 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

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{si } n \text{ est un carré} \quad \mod p \\ -1 & \text{sinon} \end{cases}$$

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.

M2R Université de Paris-Sud
2006-2007

Feuille 2 : Norme, différente et nombre de classes et compléments

0. 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

$$\exists s'' \in S_{\mathfrak{p}} \quad s''\left(s'm - sm'\right) = 0.$$

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).

1. La différente. (voir par exemple *Corps locaux*, Serre, chap. III § 6 ; ou *Algebraic Number Theory*, Lang, chap. III).

Soient A un anneau de Dedekind, K son corps des fractions, L une extension finie séparable de K, B la fermeture intégrale de A dans L, $\mathrm{Tr} = \mathrm{Tr}_{L/K}$ la trace de L sur K. Si Λ un sous-groupe additif de L, on note Λ^0 l'ensemble de $x \in L$ tels que $\mathrm{Tr}(x\Lambda) \subset A$.

1. Si Λ est le A-sous-module de L engendré par une base de L sur K, montrer que Λ^0 est le A-sous-module engendré par la base duale (relativement à la trace).
2. Si $\mathfrak{a}$ est un idéal fractionnaire[1] de B, montrer qu'il en est de même de $\mathfrak{a}^0$. Montrer que $B \subset B^0$ et $\mathfrak{a}^0 = B^0\mathfrak{a}^{-1}$.

On rappelle que la *différente* $\mathcal{D}_{B/A}$ *de* B *sur* A est par définition l'idéal $(B^0)^{-1}$ de B.

3. On suppose que $L = K(\alpha)$ est de degré n sur K, de polynôme minimal f sur K. En notant f' sa dérivée et
$$\frac{f(X)}{X-\alpha} = \sum_{i=0}^{n-1} b_i X^i$$
montrer que la base duale de $\{1, \alpha, \ldots, \alpha^{n-1}\}$ est
$$\left\{\frac{b_0}{f'(\alpha)}, \ldots, \frac{b_{n-1}}{f'(\alpha)}\right\}.$$
(On pourra considérer les polynômes $g_r = \sum \frac{f(X)}{X-\alpha_i}\frac{\alpha_i^r}{P'(\alpha_i)} - X^r$ où les α_i sont les différentes racines de f dans une clôture algébrique de K.)

[1] *i.e.* un B-module inclus dans K tel qu'il existe $b \in B\backslash\{0\}$ tel que $b\mathfrak{a} \subset B$.

4. En supposant[2] que $B = A[\alpha]$ et f le polynôme minimal de α sur A. Déduire de ce qui précède que $\mathcal{D}_{B/A} = f'(\alpha)B$.
5. Si S est un ensemble multiplicatif de A ne contenant pas 0 et $\mathfrak{b}$ un idéal fractionnaire de A, montrer que

$$S^{-1}\mathfrak{b}^{-1} = (S^{-1}\mathfrak{b})^{-1} \text{ puis que } \mathcal{D}_{S^{-1}B/S^{-1}A} = S^{-1}\mathcal{D}_{B/A}.$$

On rappelle que l'*idéal discriminant de* B/A, noté $d_{B/A}$, est par définition l'idéal de A engendré par les $\mathrm{disc}\{b_1, \ldots, b_n\}$ où $\{b_i\}_{i=1}^n$ décrit les bases de L/K telles que $b_i \in B$ pour tout i.

6. Si $S \subset A\backslash\{0\}$ est un ensemble multiplicatif, vérifier que l'on a $S^{-1}d_{B/A} = d_{S^{-1}B/S^{-1}A}$.
7. On suppose, dans cette question uniquement, que A est de valuation discrète. Soit $\mathfrak{b}$ un idéal fractionnaire de B, $\mathfrak{b} = (\beta)$ avec $\beta \in L$. Montrer que

$$\mathrm{disc}_{L/K}(\mathfrak{b}) = N_{L/K}(\beta)^2 d_{B/A}.$$

8. Soit $d_{B/A}$ le discriminant de B sur A. Montrer que

$$d_{B/A} = N_{L/K}(\mathcal{D}_{B/A}).$$

9. Si M est une extension finie séparable de L et C la fermeture intégrale de B dans M. Montrer que $\mathcal{D}_{C/A} = \mathcal{D}_{C/B} \cdot (\mathcal{D}_{B/A} \cdot C)$.

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* $\mathbf{N}$:

$$\mathbf{N}(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a}).$$

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 $N_{K/\mathbb{Q}}(\mathfrak{a}) = \mathbf{N}(\mathfrak{a})$; en déduire $\mathbf{N}(\mathfrak{ab}) = \mathbf{N}(\mathfrak{a})\mathbf{N}(\mathfrak{b})$.
2. En déduire (*cf.* Samuel p.62) que pour tout entier $x \in \mathcal{O}_K$, on a $N_{K/\mathbb{Q}}(x) = N_{K/\mathbb{Q}}(x\mathcal{O}_K)\mathbb{Z}$.
3. Soient $\mathfrak{b} \subset \mathfrak{a}$ des idéaux fractionnaires de K. Montrer que $(\mathfrak{a} : \mathfrak{b}) = \mathbf{N}(\mathfrak{a}^{-1}\mathfrak{b})$.
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 ?

3. Application de la borne de Minkowski.

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. D'après la 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

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

[2] ce qui n'est pas toujours vrai comme l'a notamment montré Dedekind avec l'exemple de l'extension $\mathbb{Q}(x)/\mathbb{Q}$ où x est une racine de $X^3 + X^2 - 2X + 8$, cf. Milne *Algebraic Number Theory*, Example 2.37., p.32.

1. Trouver le nombre de classes des corps suivants :
   (a) $K = \mathbb{Q}[i]$, $\mathbb{Q}[\sqrt{-5}]$.
   (b) K une extension cubique de $\mathbb{Q}$ de discriminant $-1 \geq d_K \geq -49$.
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.
   (a) Déterminer $\mathcal{O}_K$. Montrer que $|C_K| \leq 2$.
   (b) Soit $y = (x-2)^3/3$. Montrer qu'il existe $\varepsilon \in U_K$ tel que $U_K = \{\pm 1\} \times \varepsilon^{\mathbb{Z}}$. Prouver que $y = \pm\varepsilon^l$ avec l impair.
   (c) Soit P l'idéal engendré par 2 et x. Montrer que P n'est pas principal. En déduire $|C_K|$.
3. Calculer le nombre de classes des corps suivants :
   (a) K un corps de rupture sur $\mathbb{Q}$ de $X^3 + 10X + 1$.
   (b) K un corps de rupture sur $\mathbb{Q}$ de $X^3 - 3X + 1$.
4. Montrer[3] qu'il n'existe pas d'extension non ramifiée de $\mathbb{Q}$.

4. 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 $2\mathcal{O}_K$).

5. Loi de réciprocité quadratique. (Voir Samuel §5.5)

Soient p un nombre premier impair et d un entier premier à p. Le symbole de Legendre est défini par

$$\left(\frac{d}{p}\right) = \begin{cases} 1 & \text{si } d \text{ est un carré modulo } p, \\ -1 & \text{sinon.} \end{cases}$$

1. Montrer le critère d'Euler
$$\left(\frac{d}{p}\right) \equiv d^{(p-1)/2} \mod p.$$
En déduire $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.
2. Soit ω une racine primitive p-ième de l'unité dans une extension convenable de $\mathbb{F}_q$.
   (a) Pour $x \in \mathbb{F}_p^*$, donner un sens aux notations ω^x et $\left(\frac{x}{p}\right)$.
   (b) Pour $a \in \mathbb{F}_p^*$, on appelle *somme de Gauss* le nombre
$$\tau(a) = \sum_{x \in \mathbb{F}_p^*} \left(\frac{x}{p}\right) \omega^{xa}.$$
   Montrer que $\tau(a) = \left(\frac{a}{p}\right)\tau(1)$ et $\tau(1)^q = \tau(q)$.
   (c) Calculer $\tau(1)^2$.

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

(d) En déduire la loi de réciprocité quadratique

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

3. Montrer que $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

6. Loi de réciprocité quadratique.

Soient p un nombre premier impair, ζ une racine primitive p-ième de l'unité et $K = \mathbb{Q}(\zeta)$.

1. Montrer que K contient une unique extension quadratique F de $\mathbb{Q}$. Déterminer d tel que $F = \mathbb{Q}(\sqrt{d})$.
2. Soit q un nombre premier impair distinct de p. Calculer $(q, K/\mathbb{Q})$ et $(q, K/\mathbb{Q})_{|F}$.
3. En déduire

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

7. Localisation.

Soient A un anneau, $\mathbf{p}$ un idéal maximal de A et $\mathbf{q} = A_{\mathbf{p}}$.

1. Montrer que l'application

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

est un isomorphisme.

2. Écrire explicitement cet isomorphisme pour $A = \mathbb{Z}$.

8. Produit tensoriel.

Soient $K = k[\alpha]/k$ une extension finie séparable de corps et Ω une extension quelconque de k.

1. Montrer que $K \otimes_k \Omega$ est produit d'extensions séparables de Ω :

$$K \otimes_k \Omega = \Pi_{i=1}^{r} \Omega_i.$$

2. Est-ce encore vrai si l'extension K/k n'est pas séparable ?

M2R Université de Paris-Sud
2006-2007

TD 3 : Compléments

1. Loi de réciprocité quadratique. (Voir Samuel §5.5)

Soient p un nombre premier impair et d un entier premier à p. Le symbole de Legendre est défini par

$$\left(\frac{d}{p}\right) = \begin{cases} 1 & \text{si } d \text{ est un carré modulo } p, \\ -1 & \text{sinon.} \end{cases}$$

1. Montrer le critère d'Euler

$$\left(\frac{d}{p}\right) \equiv d^{(p-1)/2} \mod p.$$

En déduire $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

2. Soit ω une racine primitive p-ième de l'unité dans une extension convenable de $\mathbb{F}_q$.
   (a) Pour $x \in \mathbb{F}_p^*$, donner un sens aux notations ω^x et $\left(\frac{x}{p}\right)$.
   (b) Pour $a \in \mathbb{F}_p^*$, on appelle *somme de Gauss* le nombre

$$\tau(a) = \sum_{x \in \mathbb{F}_p^*} \left(\frac{x}{p}\right) \omega^{xa}.$$

   Montrer que $\tau(a) = \left(\frac{a}{p}\right) \tau(1)$ et $\tau(1)^q = \tau(q)$.
   (c) Calculer $\tau(1)^2$.
   (d) En déduire la loi de réciprocité quadratique

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

3. Montrer que $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

2. Loi de réciprocité quadratique.

Soient p un nombre premier impair, ζ une racine primitive p-ième de l'unité et $K = \mathbb{Q}(\zeta)$.

1. Montrer que K contient une unique extension quadratique F de $\mathbb{Q}$. Déterminer d tel que $F = \mathbb{Q}(\sqrt{d})$.
2. Soit q un nombre premier impair distinct de p. Calculer $(q, K/\mathbb{Q})$ et $(q, K/\mathbb{Q})_{|F}$.
3. En déduire

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

3. Localisation.

Soient A un anneau, $\mathbf{p}$ un idéal maximal de A et $\mathbf{q} = A_{\mathbf{p}}$.

1. Montrer que l'application

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

est un isomorphisme.

2. Écrire explicitement cet isomorphisme pour $A = \mathbb{Z}$.

4. Produit tensoriel.

Soient $K = k[\alpha]/k$ une extension finie séparable de corps et Ω une extension quelconque de k.

1. Montrer que $K \otimes_k \Omega$ est produit d'extensions séparables de Ω :

$$K \otimes_k \Omega = \Pi_{i=1}^{r} \Omega_i.$$

2. Est-ce encore vrai si l'extension K/k n'est pas séparable ?

5. Représentations linéaires finies.

Écrire la table des caractéres du groupe des quaternions H_8.

6. Transformée de Fourier.

1. Calculer la transformée de Fourier de la fonction

$$f : \mathbb{R} \to \mathbb{C}, f(t) = e^{-\pi t^2}$$

2. Soit $f : \mathbb{R} \to \mathbb{C}$ de classe $\mathbb{C}^1$ et de transformée de Fourier convergente. Calculer la transformée de Fourier de la dérivée f'.

M2R Université de Paris-Sud
2006-2007

Feuille 3 : Dirichlet, Cebotarev et Formule analytique du nombre de classes

1. Théorème de Dirichlet

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. Calculer $\mathrm{Spl}_1(T^2+1)$ et $\mathrm{Spl}_1(\mathbb{Q}(i))$.
2. 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.
3. Soit $m \in \mathbb{N}^*$ impair et K un corps de nombres. On définit

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

   Montrer que

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

4. 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 $(\mathbb{Z}/m\mathbb{Z})^*$.
5. 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]).

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. 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 de degré 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.

[1] Schur avait montré la réciproque en 1912

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 $\mathcal{P}(M/K)$).

3. Formule analytique du nombre de classes. Soit $K = \mathbb{Q}(\sqrt{-d})$ un corps quadratique complexe, δ_K son discriminant, χ le caractère de Dirichlet primitif modulo $D = |\delta_K|$ associé à K :

$$\chi(p) = \begin{cases} \left(\frac{D}{p}\right) & \text{si } p \text{ premier impair,} \\ (-1)^{(d-1)/2} & \text{si } p = 2 \text{ et } d \equiv 1 \mod 4, \\ 0 & \text{si } p = 2 \text{ et } d \not\equiv 1 \mod 4. \end{cases}$$

On rappelle que dans le cas complexe $\chi(-1) = -1$. On rappelle également la formule analytique du nombres des classes (cas complexe)

$$h_K = \frac{w_k \sqrt{|\delta_k|}}{2\pi} L(1, \chi),$$

pour w_K le cardinal des racines de l'unité de K.

1. On pose $w = e^{\frac{2i\pi}{D}}$ et si $a \in \mathbb{Z}$, on introduit la somme de Gauss

$$g_a(\chi) = \sum_{k=1}^{D} \chi(k) w^{ak}.$$

   Si $(a, D) = 1$, montrer que $\chi(a) g_a(\chi) = g_1(\chi)$. Si $(a, D) \neq 1$, montrer que $g_a(\chi) = 0$.
2. Montrer que

$$L(1, \chi) = -\frac{g_1(\chi)}{D} \left(\sum_{(a,D)=1} \chi(a) \log(\sin(\frac{\pi a}{D})) - i \frac{\pi}{D} \sum_{(a,D)=1} \chi(a) a \right).$$

3. Montrer que $|g_1(\chi)| = \sqrt{D}$.
4. Montrer que $\sum_{(a,D)=1} \chi(a) \log(\sin(\frac{\pi a}{D})) = 0$.
5. Supposons D impair (i.e $\chi(2) \neq 0$). Posons $S = \sum_{0<a<D} a\chi(a)$. Montrer que

$$(2 - \chi(2))S = -D \sum_{0<a<\frac{D}{2}} \chi(a).$$

6. Montrer que la formule de la question 1.5 est encore vraie pour D pair.
7. En déduire que si K est un corps quadratique imaginaire,

$$h_K = \frac{w_K}{2(2 - \chi(2))} \Big| \sum_{0<a<D/2} \chi(a) \Big|.$$

8. Quel est le nombre de classes de $\mathbb{Q}(\sqrt{-23})$?
9. Quel est le nombre de classes de $\mathbb{Q}(\sqrt{-15})$?

M2R Université de Paris-Sud
2006-2007 séance 5 du 13 novembre 2006

Feuille 4 : Ramification, Chebotarev

Exercice 1 (Une famille infinie de corps cubiques K tels que $\forall x \in \mathcal{O}_K$, $\mathcal{O}_K \neq \mathbb{Z}[x]$)
Soient p un premier vérifiant $p = 1 \mod 3$ et ζ_p une racine primitive p-ième de l'unité.

1. Montrer que $\mathbb{Q}(\zeta_p)$ admet un unique sous-corps cubique F_p de degré 3 sur $\mathbb{Q}$. Montrer que $F_p/\mathbb{Q}$ est galoisien.
2. Soit $q \neq p$ premier. Montrer que q est totalement décomposé dans F_p si et seulement si q est un cube modulo p.
3. **(Hensel)** Montrer que si 2 est un cube modulo p, alors
$$\forall x \in \mathcal{O}_{F_p}, \quad \mathcal{O}_{F_p} \neq \mathbb{Z}[x].$$
4. Montrer que l'ensemble des $p = 1 \mod 3$ tels que 2 est un cube modulo p est infini.
5. Soit $p \geq 5$. Montrer que $p = 1 \mod 3$ si et seulement si $\exists x \in \mathbb{Z}/p\mathbb{Z}\backslash\{1\}$ tel que $x^3 = 1$. En déduire que la densité analytique des $p = 1 \mod 3$ tels que 2 est un cube modulo p est $\frac{1}{6}$.

Exercice 2 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).

Exercice 3 Soit L/K une extension galoisienne de corps de nombres. Soit $\mathfrak{p}$ un idéal maximal de $\mathcal{O}_K$. Montrer que $\mathfrak{p}\mathcal{O}_L$ est maximal si et seulement si $\mathfrak{p}$ est non ramifié et le groupe $\mathrm{Gal}(L/K)$ est cyclique engendré par $\mathrm{Frob}_{\mathfrak{p}}(L/K)$.

Exercice 4 Soit $f \in \mathbb{Z}[X]$ un polynôme unitaire et irréductible et soit K_f un corps de décomposition de f sur $\mathbb{Q}$. On note $\mathrm{Spl}(f) = \{p \in \mathbb{Z} \,|\, f \text{ est scindé modulo } p\}$.

1. Soit p et q deux nombres premiers impairs distincts avec $p \equiv 1 \mod 4$. Montrer l'équivalence des propriétés suivantes :
   i. $\left(\frac{p}{q}\right) = 1$
   ii. $X^2 - X + \frac{1-p}{4}$ a une racine $\mod q$

iii. q se décompose dans $\mathbb{Q}(\sqrt{p})$

iv. $\mathrm{Frob}_q\Big(\mathbb{Q}(\sqrt{p})/\mathbb{Q}\Big) = 1$

v. $\left(\frac{q}{p}\right) = 1$.

2. Soit p un nombre premier $p \equiv 1 \mod 4$, $f(X) = X^2 - p$ et $g(X) = X^p - 1$. Montrer que $K_f \subset K_g$.
3. Montrer que $q \in \mathrm{Spl}(g)$ si et seulement si $q \equiv 1 \mod p$. Montrer que $\mathrm{Spl}(g) \subset \mathrm{Spl}(f)$.
4. Soient f et g des polynômes irréductibles de $\mathbb{Z}[X]$ de corps de décomposition respectif K_f et K_g. Montrer que $K_g \subset K_f$ si et seulement si $\mathrm{Spl}(f) \subset^* \mathrm{Spl}(g)$, où $\subset^*$ signifie inclusion à un ensemble fini près (l'équivalence restant vrai avec $\subset^\times$ qui signifie à un ensemble de densité nulle près).

M2R Université de Paris-Sud
2006-2007 séances 6 et 7 des 20 et 27 novembre 2006

Feuille 5 : Corps locaux

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

Exercice 1 (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 2 (Complétion)

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 3 Soient U un ouvert de $\mathbb{Z}_p$. Montrer que U n'est pas connexe.

Exercice 4 (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 5 (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 que $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \simeq \mathbb{Z}/2Z \times (\mathbb{Z}/8\mathbb{Z})^\times \simeq (\mathbb{Z}/2\mathbb{Z})^3$.
4. En déduire les extensions quadratiques de $\mathbb{Q}_2$.

Exercice 6 (Autres applications de Hensel)

1. Soient ℓ, p deux nombres premiers. Montrer que $\mathbb{Q}_\ell \simeq \mathbb{Q}_p$ 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 7 (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 $\forall m \in \mathbb{N}$, $\zeta_{m'} \in \mathcal{O}_K$.
2. En déduire que $\overline{\mathbb{Q}}_p$ n'est pas complet.

Exercice 8 (Divers)

1. En considérant par exemple le polynôme $P = X^2 - p$ vérifier que $\mathbb{Q}_p$ n'est pas algébriquement clos.
2. Montrer que -1 est un carré dans $\mathbb{Q}_5$.
3. Montrer que l'équation $(X^2 - 2)(X^2 - 17)(X^2 - 34) = 0$ a des solutions dans tous les $\mathbb{Z}_p$ et dans $\mathbb{R}$ mais pas dans $\mathbb{Q}$.

Exercice 9 (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 10 (Extensions totalement ramifiées)

1. Soit K un corps valué ultramétrique de valuation discrète, complet, d'anneau d'entiers 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 d'entiers 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.
3. En déduire que sous les hypothèses précédentes et en supposant de plus que K est de caractéristique nulle (ceci étant notamment vérifiée par $\mathbb{Q}_p$) qu'il n'y a, à isomorphisme près, qu'un nombre fini d'extensions de K totalement ramifiées de degré fixé.

Exercice 11 (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 $L\mathbb{Q}_p = K$.

Exercice 12 (Polygone de Newton) Soit K un corps ultramétrique complet pour une valuation discrète. On étend sa valuation à la clôture algébrique de K : val :$\overline{K}^* \to \mathbb{Q}$. Pour

$$f(X) = \sum_{i=0}^{n} a_i X \quad a_i \in K \quad \text{et} \quad a_0 a_n \neq 0$$

on considère l'enveloppe convexe inférieure de l'ensemble des points $P_i := (i, \mathrm{val}(a_i))$ avec $i \in \{0, \ldots, n\}$, et on appelle *polygone de Newton de* f la chaine polygonale délimitant cette enveloppe convexe.

1. Comment est transformé le polygone de Newton quand on passe de f à $\frac{1}{a_n} f$?
2. (Cf. par exemple Neukirch *Algebraic Number Theory* p.145) Si le polygone de Newton de $f(X)$ a un segment de longueur n et de pente $-s$, montrer que f admet exactement n racines $\alpha_1, \ldots, \alpha_n \in \overline{K}$ telles que $\mathrm{val}(\alpha_i) = 0$ pour tout $i \in \{1, \ldots, n\}$.
3. Montrer que $f_i(X) := \prod_{\mathrm{val}(\alpha_i) = s_i} (X - \alpha_i)$ est à coefficients dans K.
4. Soit $K = \mathbb{Q}[\alpha]$ où α est une racine de $X^3 - X^2 - 2X - 8$. Montrer qu'il y a trois extensions de la valuations 2-adique dans K.

Exercice 13 (Classification des corps locaux) On dit que K est un *corps local* si c'est un corps muni d'une valeur absolue non triviale, localement compact pour la topologie de cette valeur absolue et non discret. L'objet de cet exercice est la démonstration du résultat suivant :

Théorème : Tout corps local est isomorphe à l'un des corps suivants :

1. $\mathbb{R}$ ou $\mathbb{C}$;
2. une extension finie de $\mathbb{Q}_p$;
3. le corps des fractions de $k[[T]]$ où $[k : \mathbb{F}_p] < \infty$.

Dans chacun de ces cas, la valeur absolue est équivalente à la valeur absolue "naturelle".

On note F un corps local et $|\cdot|$ sa valeur absolue.

1. Montrer que F n'est pas discret si et seulement si l'image de $|\cdot|$ est infinie.
2. On suppose F de caractéristique zéro. Montrer que F contient $\mathbb{R}$ ou $\mathbb{Q}_p$ et que la restriction de $|\cdot|$ est équivalente à la valeur absolue naturelle sur $\mathbb{R}$ ou $\mathbb{Q}_p$. Notons $F_0 \subset F$ ce sous-corps. (F_0 est dit *sous-corps premier topologique de F*).
3. On appelle *espace de Banach sur F_0* un espace vectoriel V sur F_0 muni d'une norme et complet pour la topologie induite par cette norme. Montrer que F muni de sa norme est un Banach sur F_0.
4. Conclure quand F est de caractéristique zéro (on pourra se rappeler du théorème de Riesz).
5. On suppose maintenant F de caractéristique $p > 0$. Donc F contient $\mathbb{F}_p$. Soit k la clôture algébrique de $\mathbb{F}_p$ dans F. Montrer que $|x| = 1$ pour tout $x \in k^*$. En déduire que k est discret dans F et fini.
6. On rappelle que la valuation sur F est ultramétrique. Soit k_F le corps résiduel. Montrer que l'application naturelle $k \to k_F$ est un isomorphisme.
7. Montrer que F contient un élément t transcendant sur $\mathbb{F}_p$ tel que $|t| < 1$, puis que F contient un sous-corps $F_0 \simeq \mathbb{F}_p((T))$ et que la valeur absolue de F restreinte à F_0 est équivalente à l'une des valeurs absolues naturelles sur F_0. En déduire que F est une extension finie de F_0 et que la valeur absolue sur F est discrète.
8. D'après la question précédente, F contient un élément s tel que $|s| = \varepsilon$, avec ε le générateur inférieur à 1 de $|F^*|$. Montrer alors que tout élément de F s'écrit de façon unique $x = \sum_{n \geq n_0} a_n s^n$ avec $a_n \in k$. En déduire que F est isomorphe à $k((T))$.

M2R Université de Paris-Sud
2006-2007 décembre 2006

Feuille 6 : Caractères, Adèles, Idèles

Exercice 1 Soit G le produit restreint de groupes localement compacts G_v relativement aux sous-groupes ouverts H_v. Si $y \in G$, on note $y_v \in G_v$ sa projection sur la v-eme composante et on plonge G_v dans G par $x \mapsto (\ldots, 1, 1, x, 1, 1, \ldots)$. Soit $\chi \in \widehat{G}$ un caractère.

1. Montrer que χ est trivial sur presque tous les H_v (*i.e.* tous sauf eventuellement un nombre fini).
2. En déduire que pour tout $y \in G$ on a

$$\chi(y_v) = 1 \text{ pour presque tout } v, \text{ et } \chi(y) = \prod_v \chi(y_v).$$

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 Y un sous-ensemble de $\mathbb{A}_{\mathbb{Q}}$. Montrer que Y est d'adhérence compacte si et seulement si $Y \subset K_\infty \prod_p K_p$ où les K_p (p premier ou ∞) sont des compacts de $\mathbb{Q}_p$ tels que $K_p = \mathbb{Z}_p$ pour tout p sauf un nombre fini.

Exercice 4 Caractères de $\mathbb{F}_q((X))$ Soient p premier et q une puissance non nulle de p. On note $\mathbb{F}_q$ un corps à q éléments. On note $K := \mathbb{F}_q((X))$ le corps des séries de Laurent sur $\mathbb{F}_q$ (*i.e.* les séries $\sum_{i \in \mathbb{Z}} a_i X^i$ avec $a_i \in \mathbb{F}_q$ et $a_i = 0$ si $i \ll 0$). C'est un corps valué pour la valuation $v(\sum a_i X^i) = \min\{i \mid a_i \neq 0\}$.

1. Déterminer les caractères de $\mathbb{F}_q$.
2. Soit $\psi_0 \in \widehat{\mathbb{F}_q}$ non trivial. Montrer que l'application $\psi : \sum_i q_i X^i \mapsto \psi_0(a_{-1})$ est un caractère unitaire de K.
3. Déterminer $\widehat{K}$.

Exercice 5 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 6 Soit K un corps de nombres de groupe d'idèles $\mathbb{I}_K$.

1. Montrer que $\mathbb{I}_K/\mathbb{I}_K^{S_\infty} \simeq \mathrm{Div}(\mathcal{O}_K)$.
2. En déduire que $\mathbb{I}_K = \mathbb{I}_K^S \cdot K^*$ si S est un ensemble de places de K assez grand.
3. Montrer que l'on a
$$\mathbb{I}_K \Big/ (\mathbb{I}_K^{S_\infty} \cdot K^*) \simeq \mathrm{Cl}(\mathcal{O}_K).$$

Exercice 7 Approximation Forte (exercice 1/3 de l'examen de janvier 2006) Soit F un corps de nombres, et soit v_0 une place de F. On désire prouver le *théorème d'approximation forte* : l'image de F dans le produit restreint des F_v pour $v \neq v_0$ est **dense**.

1. Prouver que pour toute place v infinie de F il existe des nombres réels $r_v > 0$ tels que tout adèle $x \in \mathbb{A}_F$ s'écrive $x = \alpha + z$ avec $\alpha \in F$ et $z \in \mathbb{A}_F$, $|z_v|_v \leq r_v$ pour v infinie, $|z_v|_v \leq 1$ pour v finie.

   Sur le groupe localement compact $\mathbb{A}_F$, choisissons une mesure de Haar dx. Cela donne une mesure de Haar $d\bar{x}$ sur $\mathbb{A}_F/F$, telle qu'on ait

   $$\int_{\mathbb{A}_F} f(x)dx = \int_{\mathbb{A}_F/F} \Big(\sum_{\xi \in F} f(\xi + x) \Big) d\bar{x}$$

   pour toute fonction mesurable positive (ou intégrable) $f : \mathbb{A}_F \to \mathbb{R}$.

2. Soit C une partie mesurable de $\mathbb{A}_F$ de volume (pour dx) strictement plus grand que celui de $\mathbb{A}_F/F$ (pour $d\bar{x}$). Prouver qu'il existe $\xi \in F^*$ tel que C rencontre $C + \xi$.
3. Soit S un ensemble fini de places de F ne contenant pas v_0. Pour $v \in S$, soit δ_v un nombre réel > 0. Prouver qu'il existe $\xi \in F^*$ tel que

   $$|\xi|_v \leq \delta_v \quad \text{pour} \quad v \in S, \quad \text{et} \quad |\xi|_v \leq 1 \quad \text{pour} \quad v \notin S, \ \ v \neq v_0.$$

4. Soit S un ensemble fini de places de F ne contenant pas v_0. Pour $v \in S$ soit $a_v \in F_v$. Soit ε un nombre réel strictement positif. Prouver qu'il existe $\xi \in F$ tel que

   $$|\xi - a_v|_v < \varepsilon, \quad \text{pour} \quad v \in S, \quad \text{et} \quad |\xi|_v \leq 1 \quad \text{pour} \quad v \notin S, \ \ v \neq v_0.$$

   (Indication : Appliquer 1.1 à $\lambda^{-1}a$ pour $\lambda \in F$ bien choisi et a l'adèle de composante a_v pour $v \in S$ et 0 ailleurs).
5. Prouver le théorème d'approximation forte.

M2R Université de Paris-Sud
2006-2007 décembre 2006

Feuille 7 : Caractères, Idèles, Fourier

Exercice 1 Montrer que pour la transformation de Fourier définie dans le cours (par $\widehat{f}(x) = \int_{\mathbb{R}} f(t)e^{2i\pi xt}dt$) la mesure de Lebesgue dx sur $\mathbb{R}$ est autoduale. On pourra considérer la fonction $t \mapsto \exp(|-t|)$.

Exercice 2 Faire l'exercice 1 de la feuille 2 sur la différente (notamment le lien avec le discriminant).

Exercice 3 Soient E/K une extension finie de corps de nombres de degré n. On note $\{u_1, \ldots, u_n\}$ une base de E/K. Montrer que l'application

$$\varphi : \prod_{j=1}^{n} \mathbb{A}_K \to \mathbb{A}_E, \qquad ((x_{v,j})_v)_j \mapsto \sum_{j=1}^{n} (x_{v,j})_v u_j$$

est un isomorphisme topologique.

Exercice 4 (Le solénoïde infini) Pour tout entiers $n, m \geq 1$ tels que m divise n, la suite d'applications naturelles

$$\mathbb{R}/n\mathbb{Z} \to \mathbb{R}/m\mathbb{Z}$$

permet de définir le groupe compact abélien, dit *solénoïde infini*, $S = \varprojlim \mathbb{R}/n\mathbb{Z}$. Par ailleurs on note $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$ où le produit porte sur tous les nombrs premiers.

1. Montrer pour tout entier $n \geq 1$ la variante suivante du théorème d'approximation faible : $\mathbb{A}_{\mathbb{Q}} = \mathbb{Q} + \mathbb{R} \times n\widehat{\mathbb{Z}}$.
2. Montrer que pour tout n, l'application

$$\mathbb{R}/n\mathbb{Z} \to \mathbb{A}_{\mathbb{Q}}/\left(\mathbb{Q} + n\widehat{\mathbb{Z}}\right), \quad x \mapsto (x \text{ à la place } \infty, 0 \text{ ailleurs})$$

   (où $n\widehat{\mathbb{Z}}$ est plongé dans $\mathbb{A}_{\mathbb{Q}}$ par $x \mapsto (0_\infty, x_2, \ldots, x_p \ldots)$) est un isomorphisme.
3. Montrer que le passage à la limite projective définit un isomorphisme

$$\mathbb{A}_{\mathbb{Q}}/\mathbb{Q} \to S.$$

Exercice 5 (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 $H = (\mathbb{C}^*)^{r_2} \times (\mathbb{R}^{+*})^{r_1}$.

Exercice 6 (Groupe des classes d'idèles) Soient p premier, $V = \Pi_{i\in\mathbb{N}}\mathbb{F}_p$ un produit dénombrable de copies de $\mathbb{F}_p$ et $W = \oplus_{i\in\mathbb{N}}\mathbb{F}_p \subset V$.

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.

Exercice 7 (Calculs d'intégrales sur $\mathbb{Q}_p$) Soit dx la mesure sur $\mathbb{Z}_p$ normalisée par $\int_{\mathbb{Z}_p} dx = 1$. Soit $s \neq 0$.

1. Calculer $\int_{\mathbb{Z}_p} |x|^s dx$.
2. Si φ est une fonction continue sur $\mathbb{Z}_p$, calculer $\int_{\mathbb{Z}_p} \varphi(x)dx$.
3. Soit "dg" une mesure de Haar sur $\mathbb{Q}_p$. Montrer que pour toute fonction continue φ sur $\mathbb{Q}_p$, on a
$$\int_{\mathbb{Q}_p} \varphi(g)dg = |\alpha|_p^{-1} \int_{\mathbb{Q}_p} \varphi(\alpha g)dg, \quad \alpha \in \mathbb{Q}_p^*.$$
4. Soit $e_p : \mathbb{Q}_p \to \mathbb{C}^*$ le caractère additif donné par $e_p(x) = e^{-2\pi iq}$ si $x \in q + \mathbb{Z}_p$ (q étant la partie fractionnaire dans $\mathbb{Z}[\frac{1}{p}]$ de x). Montrer que
$$\int_{x\in\mathbb{Q}_p, |x|=p^{-k}} e_p(x)dx = \begin{cases} \frac{p-1}{p}p^{-k} & k \geq 0 \\ -1 & k = -1 \\ 0 & \text{sinon} \end{cases}$$
5. Montrer que pour tout $s \in \mathbb{R}$, on a
$$\int_{\mathbb{Q}_p} e_p(x)|x|^s dx = \frac{1 - p^s}{1 - p^{-s-1}}$$

Exercice 8 ($\mathbb{I}_K^1/K^*$ 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 9 ($\mathbb{I}_K^1/K^*$ 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 $s-1$.

M2R Université de Paris-Sud
2006-2007 décembre 2006

Feuille 8 : Thèse de Tate et corps de classes

.

Exercice 1 (**Première partie de l'examen 2003-2004**) Soient k un corps de nombres, $\mathbb{A} = \mathbb{A}_k$ son anneau des adèles et $\mathbb{I}_k$ le groupe des idèles. Pour toute place finie v de k, on note f_v^0 la fonction caractéristique de $\mathcal{O}_v$ ($f_v^0 \in \mathcal{S}(k_v)$ espace de Schwartz-Bruhat de k_v). Rappelons que l'intégrale zéta de Tate est $Z(f,s) = \int_{\mathbb{I}_k} f(x)|x|^s d^\times x$ et notons $\zeta_k(s)$ la fonction zéta de Dedekind de k.

On pose $k = \mathbb{Q}$, $\mathbb{A} := \mathbb{A}_\mathbb{Q}$ et $\mathbb{I} = \mathbb{I}_\mathbb{Q}$. Soit $f = h \otimes f_f^0 \in \mathcal{S}(\mathbb{A})$ une fonction décomposée où $h \in \mathcal{S}(\mathbb{R})$ (l'espace de Schwartz usuel) et $f_f^0 = \otimes_p f_p^0$.

1. Pour $\sigma = \Re(s) \in]0,1[$, montrer l'équivalence suivante :
$$\Big(\forall h \in \mathcal{S}(\mathbb{R}),\ Z(f,s) = 0\ \Big) \Longleftrightarrow \zeta_\mathbb{Q}(s) = 0.$$
2. On montrera (ou on admettra, cf. la preuve de Tate de l'équation fonctionnelle globale) que l'on peut écrire
$$Z(f,s) = Z_+(f,s) + Z_+(\widehat{f}, 1-s) - \frac{\widehat{f}(0)}{1-s} - \frac{f(0)}{s},$$
où $Z_+(f,s) = \int_{|x|>1} f(x)|x|^s d^\times x$.
3. Montrer que
$$Z_+(f,s) = \int_\mathbb{R} h(x)\Big(|x|^{s-1} \sum_{1 \le n \le |x|} n^{-s}\Big) dx.$$
4. Soient $\sigma \in]0,1[$ et
$$H_s(x) = |x|^{s-1} \sum_{1 \le n \le |x|} n^{-s} - \frac{1}{1-s}, \quad x \in \mathbb{R}.$$
Montrer que $H_s(x) = O(|x|^{\sigma-1})$ pour $|x| \to +\infty$ (on utilisera la formule
$$\sum_{1 \le n \le X} \frac{1}{n^s} = \big[[x]x^{-s}\big]_1^X - \int_0^X [x] - sx^{-s-1} dx$$
où $[x]$ est la partie entière de x et $[f]_a^b = f(b) - f(a)$).
5. Si $0 < \sigma < 1$, montrer que
$$\zeta_\mathbb{Q}(s) = 0 \iff \int_\mathbb{R} h(x) H_s(x) dx = -\int_\mathbb{R} \widehat{h}(x) H_{1-s}(x) dx.$$

Exercice 2 (Corps de classes de Hilbert) Soient K un corps de nombres et L son corps de classes de Hilbert de K, c'est-à-dire, la plus grande extension abélienne non ramifiée de K (aux places finies **et** infinies).

1. On rappelle que l'application de réciprocité (dite *application d'Artin*) induit un isomorphisme $\mathrm{Gal}(L/K) \simeq Cl(\mathcal{O}_K)$, où $Cl(\mathcal{O}_K)$ désigne le groupe des classes d'idéaux de K. Soit $\wp$ un idéal premier de K. Montrer que $\wp$ est totalement décomposé dans L si et seulement si c'est un idéal principal.

2. Soit $n > 0$ un entier sans facteur carré et tel que $n \not\equiv 3 \mod 4$. Soit $K = \mathbb{Q}(\sqrt{-n})$ et L son corps de classes de Hilbert. Soit enfin p un nombre premier impair ne divisant pas n. Montrer qu'il existe $x, y \in \mathbb{Z}$ tels que $p = x^2 + ny^2$ si et seulement si $p\mathcal{O}_K = \wp\overline{\wp}, \wp \neq \overline{\wp}$ et $\wp$ est totalement décomposé dans L.
3. Montrer que l'extension $L/\mathbb{Q}$ est galoisienne. En déduire que $p = x^2+ny^2$ si et seulement si p est totalement décomposé dans L.
4. Soit $L = K\sqrt{u})$ une extension quadratique avec $u \in \mathcal{O}_K$ et $\wp$ premier dans $\mathcal{O}_K$. Si $2u \notin \wp$, montrer que $\wp$ n'est pas ramifié dans L. Si $2 \in \wp$, $u \notin \wp$ et $u = b^2 - 4c$ pour $b, c \in \mathcal{O}_K$, montrer que $\wp$ n'est pas ramifié dans L.
5. On admet que le groupe des classes d'idéaux de $K = \mathbb{Q}(\sqrt{-14})$ est $Cl(\mathcal{O}_K) \simeq \mathbb{Z}/4\mathbb{Z}$. Montrer que le corps de classes de Hilbert de K est $L = K(\alpha)$ avec $\alpha = \sqrt{2\sqrt{2} - 1}$.

Exercice 3 (Groupe des normes de $\mathbb{Q}_p[\zeta_{p^n}]$) Soient p un nombre premier, $n \geq 1$ un entier, K le corps des racines p^n-ièmes de l'unité sur $\mathbb{Q}$, K_p le corps des racines p^n-ièmes de l'unité sur $\mathbb{Q}_p$. On désire montrer que le groupe des normes de K_p à $\mathbb{Q}_p$, $N_{K_p/\mathbb{Q}_p}(K_p^*)$ est égal à $p^{\mathbb{Z}}(1 + p^n\mathbb{Z}_p)$.

1. Prouver d'abord cette égalité en utilisant la théorie globale du corps de classes pour l'extension $K/\mathbb{Q}$.

   Dans les question suivantes, on utilise une méthode purement locale pour prouver le même résultat.

2. Soit Φ_{p^n} le polynôme cyclotomique. Prouver que $\Phi_{p^n}(1 - X)$ est irréductible sur $\mathbb{Q}_p$. Quels sont les degrés d'inertie et de ramification de $K_p/\mathbb{Q}_p$? Calculer $N_{K_p/\mathbb{Q}_p}(1 - \xi)$ où ξ est une racine primitive p^n-ième de l'unité dans K_p.
3. Supposons p impair. Quelle est l'image de $1+p\mathbb{Z}_p$ par $x \mapsto x^{p-1}$? l'image de $1+p\mathbb{Z}_p$ par $x \mapsto x^{p^n-1}$? celle de $\mathbb{Z}_p^*$ par $x \mapsto x^{p^{n-1}(p-1)}$? En déduire le résultat voulu en utilisant la théorie locale du corps de classes pour $K_p/\mathbb{Q}_p$.
4. Supposons $p = 2$, $n \geq 2$ (le cas $n = 1$ est trivial pour $p = 2$). Quelle est l'image de $1 + 4\mathbb{Z}_2$ par $x \mapsto x^2$? par $x \mapsto x^{2^n-1}$? Quelle est l'image de $\mathbb{Z}_2^*$ par $x \mapsto x^{2^{n-1}}$? Montrer que $5^{2^{n-2}}$ est une norme de K_2 sur $\mathbb{Q}_2$ (on pourra commencer par $n = 2$). En déduire le résultat voulu.

Exercice 4 Soient K un corps local et L_1, L_2 deux extensions abéliennes finies de K, de groupes de normes associés $\mathcal{N}_{L_i} = N_{L_i/K}(L_i^*)$.

1. Montrer que $\mathcal{N}_{L_1L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$.
2. En déduire que $L_1 \subset L_2$ si et seulement si $\mathcal{N}_{L_2} \subset \mathcal{N}_{L_1}$.

Exercice 5 (Conducteur local) Soient L/K une extension abélienne de corps locaux et $n \geq 0$ le plus petit entier tel que $1 + \mathfrak{p}_K^n \subset \mathcal{N}_L$. On appelle *conducteur de L/K* l'idéal $\mathfrak{f} = \mathfrak{p}_K^n$.

1. Justifier l'existence de l'entier n définissant le conducteur.
2. Montrer que l'extension L/K est non ramifiée si et seulement si $\mathfrak{f} = 1$.

M2R Université de Paris-Sud
2006-2007 Séance 11 du 8 janvier 2007

Feuille 9 : Corps de classes

Exércice 1 (Compléments à l'exercice 2 de la feuille précédente) Soit $K = \mathbb{Q}(\sqrt{-5})$. On admet que le nombre de classes de K est 2.

1. Montrer que le corps de classes de Hilbert de K est $L = K(i)$.
2. En déduire que si p est un nombre premier, alors

$$\exists x, y \in \mathbb{Z} \text{ tels que } p = x^2 + 5y^2 \iff p = 1 \text{ ou } 9 \mod 20.$$

Exercice 2 (Compléments à l'exercice 4 de la feuille précédente)

1. Déduire de l'exercice 4 précédent que $\mathcal{N}_{L_1} \subset \mathcal{N}_{L_2} \iff L_2 \subset L_1$.
2. Montrer que $\mathcal{N}_{L_1 \cap L_2} = \mathcal{N}_{L_1} \cdot \mathcal{N}_{L_2}$.

Exercice 3 (Kronecker-Weber) Soit $n \in \mathbb{N}$. On pose

$$\mathcal{N}_n = \mathbb{Q}^* \cdot \left(\mathbb{R}_+^* \times \prod_{p \nmid n} \mathbb{Z}_p^\times \times \prod_{p \mid n} (1 + p^{v_p(n)} \mathbb{Z}_p) \right).$$

1. Montrer que si $\mathcal{N}$ est un sous-groupe ouvert de $\mathbb{I}_\mathbb{Q}$ contenant $\mathbb{Q}^*$ et d'indice fini, alors $\mathcal{N}$ contient un $\mathcal{N}_n$ pour un entier n convenable.
2. En déduire le *théorème de Kronecker-Weber* : toute extension abélienne finie de $\mathbb{Q}$ est contenue dans une extension cyclotomique $\mathbb{Q}[\zeta_n]$ où ζ_n est une racine de l'unité.

Exercice 4 (**Corps de classes de rayons** selon Neukirch *Alg. Nb. theory*) Soit K un corps de nombres. On note $\{\mathfrak{p} \nmid \infty\}$ l'ensemble des idéaux maximaux de l'anneau des entiers $\mathcal{O}_K$. À tout idéal entier de $\mathcal{O}_K$,

$$\mathfrak{m} = \prod_{\mathfrak{p} \nmid \infty} \mathfrak{p}^{n_\mathfrak{p}} \text{ avec } \quad n_\mathfrak{p} \geq 0 \quad \text{et } n_\mathfrak{p} = 0 \text{ pour tout } \mathfrak{p} \text{ sauf un nombre fini,}$$

on associe un sous groupe de $\mathbb{I}_K$:

$$\mathbb{I}_K^\mathfrak{m} = \prod_{\mathfrak{p} \nmid \infty} (1 + \mathfrak{p}^{n_\mathfrak{p}}) \times \prod_{v \mid \infty} U_v \quad \text{où } 1 + \mathfrak{p}^0 = \mathcal{O}_K^\times \quad \text{et où} \quad U_v = \begin{cases} \mathbb{R}_+^* \text{ si } v \text{ est réelle} \\ \mathbb{C}^* \text{ si } v \text{ est complexe} \end{cases}.$$

1. Montrer que les sous-groupes ouverts d'indice fini de $\mathbb{I}_K$ contenant K^* sont les sous-groupes contenant $K^* \cdot \mathbb{I}_K^\mathfrak{m}$. Les corps K_m associés aux idéaux $\mathfrak{m}$ par la théorie du corps de classes sont appelés les *corps de classes de rayons*[1], ou *ray class fields* modulo $\mathfrak{m}$.
2. Montrer que le corps de classes de rayons mod 1, noté $K^{(1)}$, est la plus grande extension abélienne de K non ramifiée en toutes les places finies de K.
3. Montrer que si $\mathfrak{m} \mid \mathfrak{m}'$ alors $K_m \subset K_{\mathfrak{m}'}$.
4. *(Kronecker-Weber généralisé)* Si L/K est une extension abélienne de corps de nombres, alors elle est contenue dans un corps de classes de rayons $K_\mathfrak{m}$ modulo $\mathfrak{m}$ pour un idéal entier $\mathfrak{m}$ convenable.

[1] cette définition est celle de Neukirch. Il en existe une autre, plus classique et un peu plus générale qui permet notamment de voir le corps de classes de Hilbert comme un corps de classes de rayons, ce qui n'est pas forcément le cas avec la définition adoptée ici.

M2R Université de Paris-Sud
2006-2007 Séance 12 du 15 janvier 2007

Feuille 10 : Corps de classes

Exercice : On considère le corps de nombres $F = \mathbb{Q}(i) = \mathbb{Q}(\zeta_4)$. On sait que $\mathcal{O}_F = \mathbb{Z}[i]$ est un anneau principal et que ses unités sont $1, -1, i, -i$. On pose $\pi = i - 1$. L'extension $F/\mathbb{Q}$ est non ramifiée hors de 2 et on a $2\mathcal{O}_F = (\pi)^2$. On note F_π le complété de F pour la valuation associée à l'idéal π.

3.1 On considère les extensions abéliennes finies de F (dans $\mathbb{C}$) dont le groupe de Galois est annulé par 2 et qui sont non ramifiées hors de $\pi\mathcal{O}_F$.
Prouver qu'il existe une telle extension E/F qui contient toutes les autres, qu'elle est de degré 4 sur F et galoisienne sur $\mathbb{Q}$.
Décrire $F^* N_{E/F}(\mathbb{A}_E^*)$ sous la forme $F^* \Pi_v H_v$ où H_v est un sous-groupe ouvert de F_v^*, avec $H_v = U_v$ pour presque tout v.
Exprimer également E sous la forme $F(\sqrt{a}, \sqrt{b})$ avec $a, b \in F^*$ bien choisis.

3.2 Montrer que E est le corps de décomposition sur $\mathbb{Q}$ du polynôme $X^8 + 4$. Décrire l'action sur E de la conjugaison complexe c.
Montrer que E est cyclique sur $K = \mathbb{Q}(\sqrt{-2})$.

On notera σ un générateur de $\mathrm{Gal}(E/K)$ et encore c l'image dans $\mathrm{Gal}(E/\mathbb{Q})$ de la conjugaison complexe. On a $c\sigma c^{-1} = \sigma^3 = \sigma^{-1}$.

3.3 Montrer que $L = KF$ est la sous-extension abelienne maximale de E sur $\mathbb{Q}$.
Décrire $\mathbb{Q}^* N_{E/\mathbb{Q}}(\mathbb{A}_E^*)$.

3.4 Selon la classe de p modulo 8, discuter la ramification (i.e le nombre d'idéaux de $\mathcal{O}_L$ au-dessus de p, avec le degré d'inertie correspondant) d'un nombre premier impair p, dans l'extension $L/\mathbb{Q}$.
Lorsque $p \not\equiv 1 \mod 8$, discuter la ramification de p premier impair dans l'extension $E/\mathbb{Q}$.

3.5 Montrer que $N_\pi = F_\pi^* \cap F^* N_{E/F}(\mathbb{A}_E^*)$ est engendré par F_π^{*2} et l'image dans F_π des éléments de F^* qui sont des unités hors de π.
Déterminer l'image dans F_π^*/N_π du groupe des unités de F_π.
En déduire que $E/\mathbb{Q}$ est totalement ramifiée en 2.
Notant v la place de L au-dessus de 2 et w la place de E au-dessus de v, prouver que $N_{E_w/\mathbb{Q}_2}(E_w^*)$ est égal à $N_{L_v/\mathbb{Q}_2}(L_v^*)$.
Montrer que $N_{L_v/\mathbb{Q}_2}(L_v^*)$ est engendré par 2 et $1 + 8\mathbb{Z}_2$.

3.6 On suppose maintenant que p est un nombre premier congru à 1 modulo 8, et on écrit $p = X^2 + Y^2$, avec X et Y entiers. Prouver qu'on peut prendre X congru à 1 modulo 4 et Y divisible par 4.
Montrer que p est totalement décomposé dans $E/\mathbb{Q}$ si et seulement si l'idéal maximal de $\mathbb{Z}(i)$ engendré par $a = X + iY$ est totalement décomposé dans E/F, ce qui équivaut encore au fait que a, vu comme uniformisante du complété F_a de F en cet idéal, est dans le groupe $F^* N_{E/F}(\mathbb{A}_E^*)$.
Prouver que cela arrive précisément quand il existe un élément y de F qui est une unité hors de π, tel que ay soit un carré dans F_π.
Prouver que enfin que cette dernière condition équivaut à $X + Y$ congru à 1 modulo 8. (Indication : remarquer que toute unité de F_π s'écrit sous la forme $i^r(1+2\pi\alpha)$, $r \in \mathbb{Z}, \alpha \in \mathcal{O}_{F_\pi}$).