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 ?