NOTE RELATIVE AUX THÉORÈMES DES S-UNITÉS ET DES S-CLASSES

NOTE RELATIVE AUX THÉORÈMES DES S-UNITÉS ET DES S-CLASSES

par Jean-René JOLY

1. INTRODUCTION

Soit K un corps de nombres algébriques de degré n sur $\mathbf{Q}$, et désignons par A l'anneau des entiers de K, par U le groupe des unités de A et par r_1 (resp. $2r_2$) le nombre de plongements réels (resp. non réels) de K dans $\mathbf{C}$; on a $n = r_1 + 2r_2$, et $a = r_1 + r_2$ est égal au nombre de places archimédiennes de K. Si alors $|.|_1, |.|_2, \ldots, |.|_a$ sont les valeurs absolues normalisées correspondant à ces places, le classique *théorème des unités* de Dirichlet s'énonce:

(1) *Soit* $L : U \to \mathbf{R}^a$ *l'homomorphisme défini par*

$$x \mapsto (\log |x|_1, \log |x|_2, \ldots, \log |x|_a).$$

Le noyau de L *est le groupe* W *(fini, cyclique) des racines de l'unité appartenant à* K, *et l'image* $L(U)$ *est un réseau de rang* $r = a - 1$ *dans* $\mathbf{R}^a$. *Le groupe* U *est donc produit direct de* W *par un groupe abélien libre de rang* r.

Ce théorème se double du *théorème de la finitude du groupe des classes :*

(2) *L'ordre* h *du groupe des classes d'idéaux de* A *est fini.*

Ces deux théorèmes se démontrent facilement, on le sait, à l'aide du *théorème des corps convexes* de Minkowski: voir par exemple [3], chap. 12, ou [7], chap. 2, ou encore [10], chap. 4. Ils ont été généralisés par Hasse et Chevalley (voir [1]) de la façon suivante: soit S un ensemble fini de places de K contenant toutes les places archimédiennes, et soit D l'ensemble des places discrètes de K appartenant à S; si $s = \text{Card } S$ et si $d = \text{Card } D$, on a donc $s = a + d$. Notons $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_d$ les idéaux premiers de A correspondant aux places de D, $v_1, v_2, \ldots, v_d$ les valuations discrètes normalisées et $|.|_{a+1}, |.|_{a+2}, \ldots, |.|_s$ les valeurs absolues normalisées associées à ces places (voir [3], chap. 3), A_S l'anneau des S-entiers de K, c'est-à-dire l'anneau (de Dedekind) formé des $x \in K$ tels que $v(x) \geq 0$ pour toute

valuation discrète normalisée v autre que $v_1, v_2, ..., v_d$, et U_S le groupe des S-unités de K, c'est-à-dire le groupe des unités de A_S. Avec ces notations, Hasse et Chevalley ont donc démontré le *théorème des S-unités :*

(3) *Soit* $\Lambda : U_S \to \mathbf{R}^s$ *l'homomorphisme défini par*

$$x \mapsto (\log | x |_1, ..., \log | x |_a, \log | x |_{a+1}, ..., \log | x |_s).$$

Le noyau de Λ *est le groupe* W *des racines de l'unité appartenant à* K, *et l'image* $\Lambda(U_S)$ *est un réseau de rang* $s - 1 = r + d$ *dans* $\mathbf{R}^s$. *Le groupe* U_S *est donc produit direct de* W *par un groupe abélien libre de rang* $s - 1$.

Ce théorème se complète par le *théorème des S-classes :*

(4) *L'ordre* h_S *du groupe des classes d'idéaux de* A_S *est fini (en fait,* h_S *divise* h). *De plus, pour* S « *suffisamment grand* », h_S *est égal à* 1, *autrement dit,* A_S *est principal.*

Ces deux théorèmes (des S-unités et des S-classes) ont l'intérêt de permettre, grâce au lemme de Herbrand, une démonstration non analytique et relativement simple des deux inégalités fondamentales de la théorie du corps de classes (voir par exemple [4], chap. 5 et 6, ou [8], chap. VIII, §8-9). Les démonstrations de ces deux théorèmes qu'on trouve dans la littérature s'inspirent en général de l'article d'Artin-Whaples [2], et s'appuient sur des calculs de volumes et de densités: voir par exemple [5], [6]; dans cet ordre d'idées, la méthode la plus élégante consiste d'ailleurs à prouver tout d'abord la compacité du groupe J_K^1/K^* des classes d'idèles de volume 1, et à déduire de là les théorèmes (3) et (4): c'est la technique adoptée dans [8] et [9] (voir aussi [5], pp. 219-222).

Le but de la présente note est de donner des théorèmes (3) et (4) une démonstration directe à partir des classiques théorèmes (1) et (2) de Dirichlet; en plus de son caractère naturel, cette méthode a l'avantage de bien faire voir le mécanisme de la « dilatation » du groupe des S-unités et de la « contraction » du groupe des S-classes lorsqu'on « dilate » l'ensemble S. Le §2 est consacré à l'étude de l'anneau A_S. Les théorèmes (3) et (4) sont démontrés respectivement aux §3 et 4. Le §5 illustre par un exemple les démonstrations données aux §3 et 4.

2. Etude de l'anneau des S-entiers

Conservons les notations du §1. Puisque le groupe des classes de A est d'ordre fini (théorème (2)), il existe pour tout j tel que $1 \leq j \leq d$ un exposant $n_j \geq 1$ (l'ordre de la classe de $\mathfrak{p}_j$) tel que l'idéal $\mathfrak{p}_j^{n_j}$ soit principal, disons

$$\mathfrak{p}_j^{n_j} = x_j A \qquad (x_j \in A).$$

Il est clair que $v_j(x_j) = n_j$. En revanche, pour tout idéal premier $\mathfrak{q} \neq \mathfrak{p}_j$, on a $v_q(x_j) = 0$ (v_q désignant la valuation discrète normalisée associée à $\mathfrak{q}$: si $\mathfrak{q} = \mathfrak{p}_i$, $v_q = v_i$): dans le cas contraire, en effet, on aurait $x_j \in \mathfrak{q}$, donc $x_j A = \mathfrak{p}_j^{n_j} \subset \mathfrak{q}$, donc successivement $\mathfrak{p}_j \subset \mathfrak{q}$ et $\mathfrak{p}_j = \mathfrak{q}$ (contradiction!) puisque $\mathfrak{q}$ est premier et $\mathfrak{p}_j$ maximal.

Il résulte de là que les x_j sont des *S-unités*. Posons alors $t = x_1 x_2 \ldots x_d$ (c'est aussi une S-unité) et désignons par T la partie multiplicative $\{1, t, t^2, \ldots, t^m, \ldots\}$ de A.

Proposition 1.

(i) *Pour tout j tel que $1 \leq j \leq d$, on a $v_j(t) > 0$. Au contraire, pour tout idéal premier $\mathfrak{q} \notin D$ (on identifie pour simplifier les ensembles D et $\{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_d\}$), on a $v_q(t) = 0$.*

(ii) *L'anneau A_S des S-entiers de K est égal à l'anneau de fractions $T^{-1}A$.*

(iii) *A_S est un anneau de Dedekind.*

(iv) *L'application $\mathfrak{q} \mapsto \mathfrak{q}A_S$ établit une bijection de l'ensemble des idéaux premiers de A* n'appartenant pas à *D sur l'ensemble des idéaux premiers de A_S. Cette application « tue » les idéaux premiers appartenant à D: si $1 \leq j \leq d$, $\mathfrak{p}_j A_S = A_S$.*

(v) *L'application $\mathfrak{a} \mapsto \mathfrak{a}A_S$ est une surjection de l'ensemble des idéaux entiers de A sur l'ensemble des idéaux entiers de A_S. Pour que $\mathfrak{a}A_S = A_S$, il faut et il suffit que tous les facteurs premiers de $\mathfrak{a}$ appartiennent à D.*

Démonstration:

(i) résulte de la définition de t. (iii) et (iv) sont des conséquences immédiates de (ii) et des propriétés des anneaux de fractions (voir [10], chap. 5, prop. 1 et 3). Enfin (v) résulte immédiatement de (iii) et (iv).

Reste à prouver (ii). L'inclusion $T^{-1}A \subset A_S$ est évidente, puisqu'on a déjà remarqué que t est une S-unité, donc que les $1/t^m$ $(m \geq 0)$ sont des S-entiers. Inversement, soit $y \in A_S$, et considérons le produit yt^m $(m \geq 0)$. En tout $\mathfrak{q} \notin D$, on a, d'après (i),

$$v_q(yt^m) = v_q(y) \geq 0.$$

En $\mathfrak{p}_j \in D$, on a, toujours d'après (i),

$$v_j(yt^m) = v_j(y) + mv_j(t) \geq v_j(y) + m.$$

Choisissons pour m une valeur $\geq \sup_j |v_j(y)|$ et posons $x = yt^m$. Pour toute valuation discrète normalisée v de K, on a alors $v(x) \geq 0$: donc $x \in A$, $y = x/t^m \in T^{-1}A$, et finalement $A_S \subset T^{-1}A$, ce qui achève de démontrer (ii), et la proposition.

3. Démonstration du théorème (3)

Nous noterons $z_1, z_2, \ldots, z_s$ les coordonnées dans l'espace $\mathbf{R}^s = \mathbf{R}^a \times \mathbf{R}^d = \mathbf{R}^{r+1} \times \mathbf{R}^d$.

La démonstration se décomposera en quatre parties:

(a) *L'homomorphisme* Λ *a pour noyau* W.

En effet, si $x \in U_S$, l'égalité $\Lambda(x) = 0$ implique d'abord

$$|x|_{a+1} = \ldots = |x|_s = 1,$$

ce qui signifie que x est non seulement une S-unité, mais une unité de A; $\Lambda(x) = 0$ implique d'autre part $|x|_1 = \ldots = |x|_a = 1$, ce qui montre que cette unité x appartient au noyau de L, donc à W (théorème (1)); inversement, il est clair que $x \in W$ implique $\Lambda(x) = 0$. D'où (a).

(b) $\Lambda(U_S)$ *est un sous-groupe discret de* $\mathbf{R}^s$.

Les valeurs absolues $|.|_{a+1}, \ldots, |.|_s$ provenant de valuations discrètes, il est clair qu'on peut trouver dans $\mathbf{R}^d$ un voisinage V' de l'origine tel que la condition

$$(\log|x|_{a+1}, \ldots, \log|x|_s) \in V'$$

implique $|x|_{a+1} = \ldots = |x|_s = 1$, ce qui signifie (si $x \in U_S$) que x est en fait une unité de A. Soit alors V un voisinage *borné* de 0 dans $\mathbf{R}^a$: la double condition

$$x \in U_S \text{ et } \Lambda(x) \in V \times V'$$

peut s'écrire

$$x \in U \text{ et } L(x) \in V,$$

et d'après le théorème (1), ceci n'est possible que pour un nombre fini de x. D'où (b).

(c) $\Lambda(U_S)$ *est contenu dans l'hyperplan* $z_1 + z_2 + \ldots + z_s = 0$.

Supposons en effet $x \in U_S$ et décomposons l'idéal xA en facteurs premiers (dans A):

$$xA = \prod_{1 \leq j \leq d} \mathfrak{p}_j^{\nu_j(x)}.$$

Egalons les normes absolues des deux membres:

$$|Nx| = \prod_{1 \leq j \leq d} (N\mathfrak{p}_j)^{\nu_j(x)}.$$

Si $\sigma_1, \ldots, \sigma_n$ sont les plongements $K \to \mathbf{C}$ indexés de telle manière que $\sigma_1, \ldots, \sigma_{r_1}$ soient les plongements réels, et que, pour $1 \leq k \leq r_2$, σ_{r_1+k} et $\sigma_{r_1+r_2+k}$ soient complexes conjugués, la formule ci-dessus devient

$$\prod_{1 \leq i \leq r_1} |\sigma_i x| \cdot \prod_{r_1+1 \leq i \leq a} |\sigma_i x|^2 \cdot \prod_{1 \leq j \leq d} (N\mathfrak{p}_j)^{-\nu_j(x)} = 1,$$

soit, compte tenu de la définition des valeurs absolues normalisées:

$$\prod_{1 \leq i \leq s} |x|_i = 1.$$

(c) résulte de là, en prenant les logarithmes. Notons que nous venons en fait de redémontrer la formule du produit.

(d) $\Lambda(U_S)$ *contient un réseau de rang* $s - 1$.

C'est en principe la partie difficile: en réalité, tout le travail a été fait dans le théorème (1). Soit en effet $u_1, u_2, \ldots, u_r$ (rappel: $r = a-1 = r_1+r_2-1$) un système fondamental d'unités de K (nous utilisons le théorème (1)) et considérons le sous-groupe G de U_S engendré par $u_1, \ldots, u_r, x_1, \ldots, x_d$. $\Lambda(G)$ est un sous-groupe de $\Lambda(U_S)$ (donc un réseau de $\mathbf{R}^s$), et il est engendré par $\Lambda(u_1), \ldots, \Lambda(u_r), \Lambda(x_1), \ldots, \Lambda(x_d)$. La matrice de ces $r + d = s - 1$ vecteurs dans la base canonique de $\mathbf{R}^s = \mathbf{R}^a \times \mathbf{R}^d$ s'écrit

$$\begin{array}{l} \mathbf{R}^a \\ \\ \\ \\ \\ \mathbf{R}^d \end{array} \left\{ \begin{array}{c|c} M & X \\ \hline 0 & \begin{array}{l} \lambda_1 \\ \quad \lambda_2 \\ \qquad \ddots \\ \qquad\quad \ddots \\ \qquad\qquad \lambda_d \end{array} \end{array} \right.$$

M désignant la matrice de $L(u_1), \ldots, L(u_r)$ dans la base canonique de $\mathbf{R}^a$, et les λ_j désignant les quantités $\log |x_j|_j$. Par construction des x_j, on a $\lambda_1 \neq 0, \ldots \lambda_d \neq 0$; d'après le théorème (1), M est de rang $r = a - 1$: la matrice ci-dessus est donc de rang $r + d = s - 1$, et aussi le groupe $\Lambda(G)$, ce qui prouve (d).

(b), (c) et (d) montrent que $\Lambda(U_S)$ est un réseau de rang exactement $s - 1$, et le théorème (3) est démontré.

4. Démonstration du théorème 4

La partie (v) de la proposition 1 du §2 montre que l'application $\mathfrak{a} \mapsto \mathfrak{a}A_S$ définit un homomorphisme surjectif φ du groupe des idéaux de A sur le groupe des idéaux de A_S; comme φ transforme évidemment tout idéal principal en un idéal principal, φ donne lieu par passage au quotient à un homomorphisme surjectif du groupe des classes d'idéaux de A sur le groupe des classes d'idéaux de A_S; comme le premier groupe est fini, d'ordre h (théorème (2)), le second est lui aussi fini, d'ordre h_S diviseur de h, d'où la première assertion du théorème (4).

Le même raisonnement prouve d'ailleurs plus généralement que si $S \subset S'$, alors $h_{S'}$ divise h_S: pour achever de démontrer le théorème (4), il suffit donc de prouver ceci: *il existe un ensemble S tel que $h_S = 1$.*

Or, soient $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_h$ des idéaux entiers de A représentant les h classes d'idéaux de A, et soit $D = \{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_d\}$ l'ensemble des idéaux premiers de A qui divisent l'un au moins des $\mathfrak{a}_i$; enfin, soit S l'ensemble formé des places archimédiennes de K et des places discrètes appartenant à D; alors, $h_S = 1$: en effet, soit $\mathfrak{b}$ un idéal entier de A_S; il existe un idéal entier $\mathfrak{a}$ de A tel que $\mathfrak{b} = \mathfrak{a}A_S$ (prop. 1, (v)); d'autre part, il existe $y \in K^*$ et i tels que $\mathfrak{a} = y\mathfrak{a}_i$; enfin, $\mathfrak{a}_i$ se décompose en produit de facteurs premiers appartenant tous à D:

$$\mathfrak{a}_i = \mathfrak{p}_1^{m_1} \mathfrak{p}_2^{m_2} \ldots \mathfrak{p}_d^{m_d}.$$

D'où immédiatement (prop. 1, (iv))

$$\mathfrak{b} = yA_S;$$

$\mathfrak{b}$, idéal entier quelconque de A_S, est principal, et $h_S = 1$. Le théorème (4) est entièrement démontré.

Notons qu'il suffit, dans la démonstration ci-dessus, de prendre pour D une famille finie d'idéaux premiers dont les classes forment un système générateur du groupe des classes de A. Dans la pratique, il est facile de

déterminer explicitement une telle famille: on sait en effet (voir par exemple [10], p. 70) que toute classe d'idéaux de A contient un idéal entier $\mathfrak{a}$ tel que

$$N\mathfrak{a} \leqq M_K = \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n} \sqrt{|\Delta|},$$

Δ désignant le discriminant de K. On voit donc qu'on peut prendre pour D l'ensemble des idéaux premiers $\mathfrak{p}$ de A tels que $N\mathfrak{p} \leq M_K$. Bien entendu, l'ensemble D ainsi construit est en général « beaucoup trop grand »: mais il est clair que la détermination d'un D « minimal » équivaut pratiquement à la détermination de la structure du groupe des classes de A, ce qui est une autre affaire.

5. Un exemple explicite

Montrons pour terminer, sur un exemple numérique simple, que les méthodes précédentes mènent à des résultats tout à fait explicites. Nous considérons le corps quadratique imaginaire $K = \mathbf{Q}(\sqrt{-23})$, pour lequel $n = 2$, $r_1 = 0$, $r_2 = 1$, $a = 1$, $r = 0$, $W = \{1, -1\}$. Posons:

$$\alpha = \frac{-1+\sqrt{-23}}{2};$$

le polynôme minimal de α sur $\mathbf{Q}$ est $X^2 + X + 6$, et on a $A = \mathbf{Z}[\alpha]$, Δ (le discriminant) $= -23$. De là

$$\left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n} \sqrt{|\Delta|} = \frac{2\sqrt{23}}{\pi} \leq 4,$$

et le groupe des classes de A est engendré par les classes des facteurs premiers de 2 et de 3 dans A. Mais (pour $p = 2,3$) on a

$$A/pA = \mathbf{Z}[\alpha] / p\mathbf{Z}[\alpha] \simeq \mathbf{Z}[X] / (p, X^2+X+6)$$

d'où, puisque $6 \equiv 0 \pmod{p}$,

$$A/pA \simeq \mathbf{Z}[X] / (p, X^2+X) \simeq \mathbf{F}_p[X] / (X(X+1))$$

et finalement $A/pA \simeq \mathbf{F}_p \times \mathbf{F}_p$. Ainsi, 2 et 3 sont décomposés dans A, et le calcul ci-dessus montre plus précisément qu'on peut écrire

$$(2) = \mathfrak{p}\bar{\mathfrak{p}}, \quad (3) = \mathfrak{q}\bar{\mathfrak{q}},$$

avec

$$\mathfrak{p} = (2, \alpha), \quad \bar{\mathfrak{p}} = (2, \alpha+1),$$

et

$$\mathfrak{q} = (3, \alpha), \quad \bar{\mathfrak{q}} = (3, \alpha+1).$$

On vérifie sans peine que $\mathfrak{pq} = (\alpha)$, $\mathfrak{p}\bar{\mathfrak{q}} = (\alpha+1)$ et $\mathfrak{p}^3 = (\alpha+2)$. En revanche, $\mathfrak{p}^2$ n'est pas principal: car $N\mathfrak{p}^2 = 4$, mais $\mathfrak{p}^2 \neq (2)$, alors que 2 et -2 sont les seuls entiers de K ayant pour norme 4.

Il résulte de tout ceci que $\bar{\mathfrak{p}} \sim \mathfrak{p}^{-1}$, $\bar{\mathfrak{q}} \sim \mathfrak{q}^{-1}$, $\mathfrak{q} \sim \bar{\mathfrak{q}}^{-1} \sim \mathfrak{p}$, $\mathfrak{p}^3 \sim (1)$, mais qu'*on n'a pas* $\mathfrak{p}^2 \sim (1)$ (*ni* a fortiori $\mathfrak{p} \sim (1)$): le groupe des classes de A est donc cyclique d'ordre 3, engendré par la classe de $\mathfrak{p} = (2, \alpha)$.

Soit maintenant $\mathfrak{p}_\infty$ l'unique place archimédienne de K et posons

$$D = \{\mathfrak{p}\}, \quad S = \{\mathfrak{p}_\infty, \mathfrak{p}\}.$$

Alors, avec les notations du §1, on a $d = 1$, $s = 2$, $\mathfrak{p}_1 = \mathfrak{p}$, $n_1 = 3$, $x_1 = t = \alpha + 2$. Et on peut affirmer:

L'anneau A_S est formé des éléments de K du type $(x+y\alpha) / (\alpha+2)^m$ ($m \geq 0$; $x, y \in \mathbf{Z}$); A_S est un anneau principal: $h_S = 1$; enfin, le groupe U_S est formé des éléments du type $\pm (\alpha+2)^m$ ($m \in \mathbf{Z}$) (le fait que $\alpha + 2$ soit une « unité fondamentale » pour A_S tient à ce que $N(\alpha+2) = 8$ et que ni 2 ni 4 ne sont normes de S-unités de K).

BIBLIOGRAPHIE

[1] CHEVALLEY, La théorie du corps de classes. *Ann. of Math.* (1940), 41, pp. 394-418.
[2] ARTIN-WHAPLES, Axiomatic characterization of fields by the product formula for valuations. *Bull. Am. Math. Soc.* (1945), 51, pp. 469-492.
[3] ARTIN, *Theory of algebraic numbers*. Göttingen (1959).
[4] ARTIN-TATE, *Class field theory*. Harvard (1960).
[5] WEISS, *Algebraic number theory*. McGraw-Hill (1963).
[6] LANG, *Algebraic numbers*. Addison-Wesley (1964).
[7] BOREVICH-SHAFAREVICH, *Number theory*. Academic Press (1966).
[8] CASSELS-FRÖHLICH, *Algebraic number theory*. Academic Press (1967).
[9] WEIL, *Basic number theory*. Springer (1967).
[10] SAMUEL, *Théorie algébrique des nombres*. Hermann (1967).

Faculté des Sciences de Grenoble
Institut de Mathématiques pures

(Reçu le 30 julliet 1990)