ENS de Lyon
Université Claude Bernard Lyon 1

Département de Mathématiques

Groupe de Witt des nombres rationnels

Élève
Martin BAGET

Enseignant
Grégory BERHUY

11 décembre 2024

Table des matières

1 Présentation d'un groupe de Witt **2**

2 Nombres p-adiques et morphismes ∂'_p **6**

3 Structure du groupe de Witt $W(\mathbb{Q})$ **8**

3.1 Le groupe de Witt $W(\mathbb{F}_2)$ 8

3.2 Le théorème de structure 8

3.3 Compléments de théorie des groupes 9

3.4 Preuve du théorème de structure 10

3.5 Principes de Hasse 12

On rappelle que l'on note $< a_1, ..., a_n >$ pour la forme quadratique $a_1X_1^2 + ... + a_nX_n^2$, et qu'en caractéristique différente de 2 toute forme quadratique peut être mise sous cette forme (réduction de Gauss). Le lecteur est supposé connaître les théorèmes de prolongement, de simplification et de décomposition de Witt, ainsi que le principe du gonflement hyperbolique. On rappelle aussi la relation suivante, fondamentale et utilisée à de multiples reprises :

Proposition 1 (Relation de Witt)**.** *Soit K un corps de caractéristique différente de 2, $a, b \in K^\times$ avec $a + b \neq 0$. On a*

$$< a, b > \simeq < a + b, ab(a + b) >$$

Démonstration. On pose $q =< a, b >$. Soit $D = \mathrm{Vect}(1, 1)$. D est régulier donc $D^\perp$ est un supplémentaire de D, et on peut prendre u un vecteur directeur de cette droite. Dans la base orthogonale $((1, 1), u)$, q s'écrit $< a+b, c >$ et en prenant le déterminant $ab = (a+b)c$ à un carré près. On peut donc en multipliant u par un scalaire avoir $c = ab(a + b)$. □

1 Présentation d'un groupe de Witt

On fixe un corps K de caractéristique différente de 2. Toutes les formes quadratiques considérées sont supposées régulières.

Définition 1 (Groupe de Witt)**.** *L'ensemble des classes d'équivalence de matrices symétriques inversibles à coefficients dans K pour la relation de congruence muni de l'addition orthogonale forme un monoïde. Lorsqu'on le quotiente par le sous-monoïde des formes hyperboliques, on obtient un groupe. C'est le groupe de Witt de K, noté W(K).*

Proposition 2. *On a les isomorphismes de groupes*

- $W(\mathbb{C}) \simeq \mathbb{Z}/2\mathbb{Z}$
- $W(\mathbb{R}) \simeq \mathbb{Z}$
- *Si p est un nombre premier congru à 1 modulo 4, alors* $W(\mathbb{F}_p) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
- *Si p est un nombre premier congru à 3 modulo 4, alors* $W(\mathbb{F}_p) \simeq \mathbb{Z}/4\mathbb{Z}$

Démonstration.

- Tout forme quadratique sur $\mathbb{C}$ de dimension au moins 2 est isotrope. Ainsi les seules formes anisotropes à équivalence près sont la forme nulle et <1>
- Si une forme quadratique prend des valeurs positives et négatives alors, par le théorème des valeurs intermédiaires, elle est isotrope. On en déduit que les formes quadratiques anisotropes sont celles définies positives ou définies négatives, c'est-à-dire à isomorphisme près celles de la forme <1, ..., 1> ou <-1, ..., -1>. Comme -<1> = <-1> dans le groupe de Witt, $n \mapsto n\times < 1 >$ est l'isomorphisme recherché.
- On rappelle que si K est un corps fini, et que si ϵ est un élément fixé qui n'est pas un carré, alors les seules formes anisotropes sont la forme nulle, <1>, $< \epsilon >$ et $< 1, -\epsilon >$. <1>+<1> et $< \epsilon > + < \epsilon >$ sont nuls dans le groupe de Witt si et seulement si leur déterminant vaut -1, c'est-à-dire si et seulement si -1 est un carré modulo p. Si p est congru à 1 modulo 4, c'est le cas, donc $W(\mathbb{F}_p)$ contient deux élément d'ordre 1 et est donc isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Sinon, <1> est d'ordre 4 donc $W(\mathbb{F}_p)$ est isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

□

La définition du groupe de Witt donne immédiatement la proposition suivante qui permet de construire des morphismes de groupe sur celui-ci.

Proposition 3 (Propriété universelle du groupe de Witt)**.** *Soit G un groupe abélien et f une fonction qui à une forme quadratique sur K associe un élément de G. On suppose que f s'annule sur les formes hyperboliques et que pour toutes formes quadratiques q_1, q_2, on a*

$$f(q_1 \perp q_2) = f(q_1) + f(q_2)$$

Alors f se factorise en un morphisme de groupe $W(K) \to G$.

La résultat final de cette partie sera de donner un second critère pour construire des morphismes sur un groupe de Witt, que l'on utilisera ensuite pour étudier le groupe de Witt des rationnels.

Définition 2 (Groupe abélien libre sur $K^\times$)**.** *L'ensemble $\mathbb{Z}^{K^\times}$ muni de l'addition composante par composante forme un groupe. Le sous-ensemble des éléments dont seulement un nombre fini de composantes sont non nulles en est un sous-groupe, on l'appelle groupe abélien libre sur $K^\times$ et on le note $\mathbb{Z}[K^\times]$. Pour $k \in K^\times$, on note $\overline{k}$ l'élément envoyant k sur 1, et tous les autres éléments sur 0.*

Le second critère va s'appuyer sur une présentation du groupe de Witt de K, c'est-à-dire une écriture de W(K) comme le quotient du groupe abélien sur $K^\times$ par un de ses sous-groupes. En fait, on a un morphisme $\alpha : \mathbb{Z}[K^\times] \to W(K)$ (bien) défini, pour $k_1, ..., k_r \in K^\times, n_1, ..., n_r \in \mathbb{Z}$ par

$$\alpha(n_1.\overline{k_1} + ... + n_r.\overline{k_r}) = n_1 \times < k_1 > + ... + n_r \times < k_r >$$

et donc le premier théorème d'isomorphisme donne

$$W(K) \simeq \mathbb{Z}[K^\times]/\mathrm{Ker}(\alpha)$$

La question est donc de trouver le noyau du morphisme α. On peut déjà noter que l'on a $\overline{\lambda} - \overline{\lambda\mu^2} \in Ker(\alpha)$ pour tous $\lambda, \mu \in K^\times$, puisque la forme quadratique $< \lambda, -\lambda\mu^2 >$ est hyperbolique. De même pour $\overline{1} + \overline{-1}$. On a également le résultat suivant, moins évident :

Proposition 4. *Pour tous $\lambda, \mu \in K^\times$, si $\lambda + \mu \neq 0$, alors*

$$\overline{\lambda} + \overline{\mu} - \overline{\lambda + \mu} - \overline{\lambda\mu(\lambda + \mu)} \in Ker(\alpha)$$

Démonstration. On a la relation de Witt $< \lambda, \mu > \simeq < \lambda + \mu, \lambda\mu(\lambda + \mu) >$, donc si $\phi =< \lambda, \mu >$, la forme quadratique $q =< \lambda, \mu, -(\lambda + \mu), -\lambda\mu(\lambda + \mu) >$ vérifie $q \simeq \phi \perp -\phi$ et est hyperbolique. Sa classe de Witt-équivalence est donc bien nulle. □

On en déduit que le sous-groupe de $\mathbb{Z}[K^\times]$ engendré par ces éléments, que l'on note H, appartient au noyau de α. La fin de cette partie va consister à prouver que l'on a en fait égalité. On commence par travailler sur les plans quadratiques, puis on généralise grâce au lemme-clé dit des bases orthogonales.

Proposition 5. *Soient $a, b, c, d \in K^\times$ tels que $< a, b > \simeq < c, d >$. Alors $\overline{a} + \overline{b} - \overline{c} - \overline{d} \in H$.*

Démonstration. $< a, b >$ représente c donc on peut trouver $x, y \in K$ tels que $c = ax^2 + by^2$. On distingue trois cas,

— Si y $= 0$, $x \neq 0$ et on a donc $< c, d > \simeq < a, b > \simeq < ax^2, b > = < c, b >$ puis par simplification $< d > \simeq < b >$ donc $d = bz^2$ pour un $z \in K^\times$. Ainsi $\overline{a} + \overline{b} - \overline{c} - \overline{d} = (\overline{a} - \overline{ax^2}) + (\overline{b} - \overline{bz^2}) \in H$.

— Si x $= 0$, on procède de même.

— Sinon, $< a, b > \simeq < ax^2, b > \simeq < ax^2, by^2 > \simeq < c, abcx^2y^2 >$ et le déterminant donne l'existence de $z \in K^\times$ tel que $d = abcx^2y^2z^2$. On traduit ces équivalences par $\overline{a} + \overline{b} - \overline{c} - \overline{d} = (\overline{a} - \overline{ax^2}) + (\overline{b} - \overline{by^2}) + (\overline{ax^2} + \overline{by^2} - \overline{c} - \overline{abcx^2y^2}) + (\overline{abcx^2y^2} - \overline{d}) \in H$.

□

Lemme 1 (des bases orthogonale)**.** *Soient $(x_1, ..., x_n)$ et $(y_1, ..., y_n)$ deux bases orthogonales d'un espace quadratique régulier non nul (E, q). Il existe alors une suite finie $(B_1, ..., B_l)$ de bases orthogonales de (E, q) avec $B_1 = (x_1, ..., x_n)$, $B_l = (y_1, ..., y_n)$ et, pour $1 \leqslant i < l$, B_i et B_{i+1} qui diffèrent d'au plus deux composantes.*

Démonstration. On procède par récurrence sur n. Pour $n \leqslant 2$, c'est trivial. Supposons donc $n \geqslant 3$. Notons H l'hyperplan $\mathrm{Vect}(y_1, ..., y_{n-1})$. On distingue trois cas :

— Si un seul des vecteurs $(x_1, ..., x_n)$ n'appartient pas à H, il est dans la droite $H^\perp$ donc colinéaire à y_n. On l'échange avec x_n en le multipliant par le coefficient adapté pour obtenir y_n. On est alors ramené à l'espace quadratique régulier (H, q_H) et on conclut grâce à l'hypothèse de récurrence.

— Si exactement deux vecteurs parmi $(x_1, ..., x_n)$ n'appartiennent pas à H, disons x_i et x_j, on considère la droite $D = H \cap \mathrm{Vect}(x_i, x_j)$. D est alors régulière donc anisotrope car c'est l'orthogonal de $\mathrm{Vect}(x_k)_{k \neq i,j}$ régulier dans (H, q_H) régulier. On peut remplacer x_i par un vecteur directeur de D, et x_j par un vecteur directeur de l'orthogonal de D dans $Vect(x_i, x_j)$ régulier. On est alors ramené au cas précédent.

— Si l'on a au moins trois vecteurs x_i, x_j, x_k en dehors de H, alors $D_1 = H \cap \mathrm{Vect}(x_i, x_j)$, $D_2 = H \cap \mathrm{Vect}(x_i, x_k)$ et $D_3 = H \cap \mathrm{Vect}(x_j, x_k)$ sont trois droites distinctes du plan $P = H \cap \mathrm{Vect}(x_i, x_j, x_k)$. Or $\mathrm{Vect}(x_i, x_j, x_k)$ étant régulier, ses lagrangiens sont de dimension au plus 1. En particulier q ne peut pas s'annuler sur P. Cela impose qu'elle ne s'annule pas simultanément sur D_1, D_2 et D_3. On peut donc comme précédemment remplacer un des vecteurs par un vecteur de H. Quitte à recommencer s'il y avait strictement plus de trois vecteurs en dehors de H, on se ramène aussi au cas précédent.

□

Théorème 1 (de la chaîne d'équivalence)**.** *Soient $(a_1, ..., a_n), (b_1, ..., b_n) \in (K^\times)^n$ tels que $< a_1, ..., a_n > \simeq < b_1, ..., b_n >$. Il existe alors un entier l et des éléments $a_{i,j}$ pour $1 \leqslant i \leqslant l$ et $1 \leqslant j \leqslant n$ tels que*

— *pour tout j, $a_{1,j} = a_j$ et $a_{l,j} = b_j$*

— *pour tout i, $< a_{i,1}, ..., a_{i,n} > \simeq < a_1, ..., a_n >$*

— *pour tout $i < l$, $(a_{i,1}, ..., a_{i_n})$ et $(a_{i+1,1}, ..., a_{i+1,n})$ diffèrent d'au plus deux composantes*

Démonstration. Si l'on considère $q = < a_1, ..., a_n >$ sur K^n dans la base canonique, l'hypothèse nous donne une base orthogonale dans laquelle q s'écrit $< b_1, ..., b_n >$. On considère alors les listes des valeurs de q sur les vecteurs des bases données par le lemme des bases orthogonales. □

Théorème 2 (de Witt).

$$Ker(\alpha) = H$$

Démonstration. On a vu $H \subseteq \mathrm{Ker}(\alpha)$. Réciproquement, soit $x \in \mathrm{Ker}(\alpha)$, on l'écrit

$$x = \overline{a_1} + ... + \overline{a_n} - \overline{b_1} - ... - \overline{b_m}$$

Quitte à considérer -x, on peut supposer $n \geqslant m$. On pose $\phi =< a_1, ..., a_n >$ et $\psi =< b_1, ..., b_n >$. Alors par hypothèse $\phi \perp -\psi$ est hyperbolique donc n+m est pair, n-m aussi et

$$\phi \perp -\psi \simeq \psi \perp -\psi \perp \frac{n-m}{2} \times < 1, -1 >$$

puis par simplification

$$\phi \simeq \psi \perp \frac{n-m}{2} \times < 1, -1 >$$

On peut compléter le m-uplet $(b_1, ..., b_m)$ en un n-uplet $(b_1, ..., b_n)$ en rajoutant des couples (1, -1), puis appliquer le théorème de la chaîne d'équivalence qui donne $(a_{i,j})$. Si

$$y = \sum_{j=1}^{n} \overline{a_j} - \overline{b_j}$$

on a donc

$$y = \sum_{i=1}^{l-1} \sum_{j=1}^{n} \overline{a_{i+1,j}} - \overline{a_{i,j}}$$

et pour i < l, $\sum_{j=1}^{n} \overline{a_{i+1,j}} - \overline{a_{i,j}} \in H$. En effet, cette somme se résume à une différence $\overline{a_{i+1,r}} + \overline{a_{i+1,s}} - \overline{a_{i,r}} - \overline{a_{i,s}}$ pour deux indices r, s distincts, avec par simplification $< a_{i+1,r}, a_{i+1,s} > \simeq < a_{i,r}, a_{i,s} >$, et donc la proposition 4 donne le résultat. Ainsi $y \in H$ puis

$$x = y + \frac{n-m}{2}(\overline{1} + \overline{-1}) \in H$$

□

Proposition 6 (Seconde propriété universelle du groupe de Witt). *Soit G un un groupe abélien et $f : K^\times \to G$. On suppose que*

- $f(\lambda\mu^2) = f(\lambda)$ *pour tous* $\lambda, \mu \in K^\times$
- $f(-1) = -f(1)$
- $f(\lambda) + f(\mu) = f(\lambda + \mu) + f(\lambda\mu(\lambda + \mu))$ *pour tous* $\lambda, \mu \in K^\times$ *avec* $\lambda + \mu \neq 0$

Alors il existe un unique morphisme de groupes $\overline{f} : W(K) \to G$ tel que $\overline{f}(< a >) = f(a)$ pour tout $a \in K^\times$.

2 Nombres p-adiques et morphismes ∂'_p

p est un nombre premier qui peut ici être égal à 2. On ne s'attarde pas ici sur la construction des nombres p-adiques. Il s'agit principalement ici de donner une vision pratique des nombres p-adiques pour énoncer quelques propriétés élémentaires et construire des morphismes entre groupes de Witt intéressants. On notera que le passage par les nombres p-adiques n'est pas essentiel pour le théorème de structure de $W(\mathbb{Q})$ (section 3.2). Cependant, la construction est plus naturelle dans ce cadre, et sera utile pour le principe de Hasse faible (section 3.5).

Définition 3. *Il existe un corps, noté $\mathbb{Q}_p$, et appelé corps des nombre p-adiques, tel que tout élément r est représenté de façon unique par une suite $(r_k)_{k\in\mathbb{Z}}$ d'entiers entre 0 et p-1, qui est nulle pour k suffisamment proche de $-\infty$. On note*

$$r = \sum a_k p^k$$

L'addition se fait terme à terme puis avec des retenues, la multiplication consiste en un produit de convolution lui aussi suivi de retenues. À tout nombre p-adique non nul r, on associe sa valuation p-adique, notée $v_p(r)$ qui est le plus petit entier k tel que $a_k \neq 0$, ainsi que son résidu p-adique, noté $res_p(r)$, qui est le a_k correspondant vu comme élément de $\mathbb{F}_p^\times$. On appelle entier p-adique un nombre p-adique de valuation p-adique positive. L'ensemble des entiers p-adiques forme un sous-anneau de $\mathbb{Q}_p$ noté $\mathbb{Z}_p$. On appelle unité p-adique un nombre p-adique de valuation p-adique nulle. Les unités p-adiques sont exactement les inversibles de $\mathbb{Z}_p$, et forment donc le sous-groupe multiplicatif $\mathbb{Z}_p^\times$.

Le corps $\mathbb{Q}_p$ peut aussi être construit comme le complété de $\mathbb{Q}$ pour la distance p-adique. En particulier, $\mathbb{Q}$ s'injecte naturellement dans $\mathbb{Q}_p$. À partir de notre définition, c'est clair que $\mathbb{Z}$ s'injecte naturellement dans Z_p, et donc $\mathbb{Q}$ aussi puisque $\mathbb{Q}_p$ contient les inverses. On peut même donner une formule à partir de l'égalité formelle

$$\frac{1}{1-X} = \sum_{i=0}^{+\infty} X^i$$

Pour un rationnel $r = \frac{a}{b}$ sous forme irréductible, on peut écrire $r = p^m \frac{a'}{b'}$ où a' et b' sont premiers avec p et m est la valuation p-adique de r au sens usuel. Le théorème de Bézout donne deux entier u, v tels que $b'u + pv = 1$. Alors

$$r = p^m \frac{a'}{b'} = p^m a' \frac{u}{1-pv} = p^m a' u \sum_{i=0}^{+\infty} (pv)^i = \sum_{k=m}^{+\infty} a' u v^{k-m} p^k$$

puis avec des retenues pour terminer. Cette formule nous donne en particulier que m est aussi la valuation p-adique au sens de la définition et que

$$\mathrm{res}_p(r) = a'.b'^{-1}$$

où a' et b' sont vus comme éléments de $\mathbb{F}_p^\times$.

Définition 4. *Le fait que $\mathbb{Q}$ est un sous-corps de $\mathbb{Q}_p$ permet de voir une forme quadratique rationnelle q également comme une forme quadratique sur $\mathbb{Q}_p$. On note q_p cette forme*

quadratique. On note aussi q_∞ la forme quadratique associée à une forme quadratique rationnelle lorsque vue comme forme quadratique réelle. Ces formes quadratiques sont appelées les localisées de la forme quadratique q. Cela donne naturellement des morphismes $W(\mathbb{Q}) \to W(\mathbb{Q}_p)$ et $W(\mathbb{Q}) \to W(\mathbb{R})$ appelés morphismes de localisation.

Lemme 2. *Les applications $v_p : \mathbb{Q}_p^\times \to \mathbb{Z}$ et $res_p : \mathbb{Q}_p^\times \to \mathbb{F}_p^\times$ sont des morphismes de groupes.*

Lemme 3. *Soient $a, b \in \mathbb{Q}_p^\times$.*

- *Si $v_p(a) > v_p(b)$, alors $v_p(a+b) = v_p(b)$ et $res_p(a+b) = res_p(b)$*
- *Si $v_p(a) \neq v_p(a+b)$ et $v_p(b) \neq v_p(a+b)$, alors $v_p(a) = v_p(b)$ et $res_p(b) = -res_p(a)$*

Proposition 7. *Il existe un unique morphisme de groupes $\partial'_p : W(\mathbb{Q}_p) \to W(\mathbb{F}_p)$ tel que*

$$\partial'_p(< r >) = \left| \begin{array}{ll} < res_p(r) > & \text{si } v_p(r) \text{ est impaire} \\ 0 & \text{sinon} \end{array} \right.$$

pour tout $r \in \mathbb{Q}_p^\times$.

Démonstration. On applique la seconde propriété universelle du groupe de Witt à $\delta'_p : \mathbb{Q}_p^\times \to W(\mathbb{Q}_p)$ qui à $r \in \mathbb{Q}_p^\times$ associe la classe d'équivalence de Witt souhaitée. Pour cela il faut vérifier que δ'_p vérifie les relations nécessaires : pour $\lambda, \mu \in \mathbb{Q}_p^\times$,

- $\delta'_p(\lambda\mu^2) = 0 = \delta'_p(\lambda)$ si $v_p(\lambda)$ est pair, et sinon
$$\delta'_p(\lambda\mu^2) =< \mathrm{res}_p(\lambda)\mathrm{res}_p(\mu)^2 >=< \mathrm{res}_p(\lambda) >= \delta'_p(\lambda)$$
- $\delta'_p(-1) = 0 = -\delta'_p(1)$.
- On veut finalement prouver que $\delta'_p(\lambda+\mu) + \delta'_p(\lambda\mu(\lambda+\mu)) = \delta'_p(\lambda) + \delta'_p(\mu)$. Il faut distinguer de nombreux cas. Par symétrie, il suffit de vérifier les suivants.

Cas	Terme de gauche	Terme de droite
$v_p(\lambda)$, $v_p(\mu)$ et $v_p(\lambda+\mu)$ pairs	0	0
$v_p(\lambda)$ et $v_p(\mu)$ pairs, $v_p(\lambda+\mu)$ impair	$< \mathrm{res}_p(\lambda+\mu), \mathrm{res}_p(\lambda\mu(\lambda+\mu)) >$	0
$v_p(\lambda)$ pair, $v_p(\mu)$ impair, $v_p(\lambda) < v_p(\mu)$	$< \mathrm{res}_p(\lambda\mu(\lambda+\mu)) >$	$< \mathrm{res}_p(\mu) >$
$v_p(\lambda)$ pair, $v_p(\mu)$ impair, $v_p(\lambda) > v_p(\mu)$	$< \mathrm{res}_p(\lambda+\mu) >$	$< \mathrm{res}_p(\mu) >$
$v_p(\lambda)$, $v_p(\mu)$ et $v_p(\lambda+\mu)$ impairs	$< \mathrm{res}_p(\lambda+\mu), \mathrm{res}_p(\lambda\mu(\lambda+\mu)) >$	$< \mathrm{res}_p(\lambda), \mathrm{res}_p(\mu) >$
$v_p(\lambda)$ et $v_p(\mu)$ impairs, $v_p(\lambda+\mu)$ pairs	0	$< \mathrm{res}_p(\lambda), -\mathrm{res}_p(\lambda) >$

Le premier et le dernier cas sont immédiats. Dans le troisième et le quatrième, il suffit d'exprimer le résidu de gauche. Dans le deuxième cas, puisque $\mathrm{res}_p(\mu) = -\mathrm{res}_p(\lambda)$, le déterminant vaut -1 donc la forme est bien hyperbolique. Enfin pour le cinquième cas, on distingue encore des sous-cas :

- si $v_p(\lambda) \neq v_p(\mu)$, on a simplement un facteur carré dans le terme de gauche.
- si $v_p(\lambda) = v_p(\mu) < v_p(\lambda+\mu)$, les deux formes sont de déterminant -1 donc hyperboliques.
- si $v_p(\lambda) = v_p(\mu) = v_p(\lambda+\mu)$, il s'agit de la relation de Witt.

□

3 Structure du groupe de Witt $W(\mathbb{Q})$

3.1 Le groupe de Witt $W(\mathbb{F}_2)$

Le groupe de Witt $W(\mathbb{F}_2)$ n'a pas été défini ni même étudié car le cas de la caractéristique 2 est particulier. En fait, la définition donnée ne fonctionne pas dans de cas ! La raison est que sur un corps fini de caractéristique 2, si q est une forme quadratique, $q \perp -q$ n'est pas hyperbolique à priori. On a en effet que $< 1, -1 >$ n'est pas hyperbolique puisque représentant 1 en deux valeurs, alors que $q(x, y) = xy$ ne représente 1 qu'en une seule valeur. En fait la forme hyperbolique n'est pas diagonalisable. La définition du groupe de Witt tombe donc à l'eau.

Nous n'allons pas nous intéresser à l'étude des formes quadratiques en caractéristique 2 ici. Pour résoudre ce problème - et faire fonctionner le théorème de structure de $W(\mathbb{Q})$ - on définit $W(\mathbb{F}_2)$ comme le groupe à deux éléments 0 et $< 1 >$, c'est-à-dire que l'on quotiente les classes de formes quadratiques admettant une base orthogonale par le sous-groupe engendré par $< 1, -1 >$.

3.2 Le théorème de structure

Proposition 8. *Pour tout p premier, il existe un unique morphisme de groupes ∂_p : $W(\mathbb{Q}) \to W(\mathbb{F}_p)$ tel que*

$$\partial_p(< a >) = \left| \begin{array}{ll} < \frac{a}{p} > & \textit{si } p \textit{ divise } a \\ 0 & \textit{sinon} \end{array} \right.$$

pour tout entier a sans facteur carré.

Démonstration. Il s'agit de voir que la composée du morphisme de localisation et de ∂'_p convient. □

Théorème 3. *L'application*

$$\Phi : \left\{ \begin{array}{rcl} W(\mathbb{Q}) & \to & W(\mathbb{R}) \oplus \bigoplus\limits_{p \text{ premier}} W(\mathbb{F}_p) \\ q & \mapsto & q_\infty + \sum\limits_{p \text{ premier}} \partial_p(q) \end{array} \right.$$

est un isomorphisme de groupes.

Avant d'attaquer la démonstration, voyons quelques cas particuliers et conséquences de ce théorème.

Exemple 1. *Comment trouver une forme quadratique rationnelle q telle que $q_{\mathbb{R}} =< 1, 1 >$, $\partial_2(q) =< 1 >$, $\partial_3(q) =< 2, 1 >$, $\partial_5(q) = 0$ et $\partial_7(q) =< 5 >$. On traite les conditions sur les nombres premiers par ordre décroissant puis la condition réelle. On commence par satisfaire la condition pour 7 en prenant $< 35 >$. Alors son image par ∂_5 est $< 2 >$, donc pour satisfaire également la condition sur 5 on considère $< 35, -10 >$. Puis $< 35, -10, 6, 3 >$ et enfin $< 35, -10, 6, 3, 2 >$ pour satisfaire toutes les conditions sur les nombres premiers. On adapte enfin la signature réduite : $< 35, -10, 6, 3, 2, -1 >$ est solution (mais pas forcément de dimension minimale !).*

Exemple 2. *La forme quadratique rationnelle* $q =< 57, -10, -2, 85, -3, 17 >$ *est-elle hyperbolique. Sa signature réduite est bien nulle donc* $q_{\mathbb{R}} = 0$ *(dans le groupe de Witt). On écrit les décompositions en nombres premiers :*

- *57 = 3.19*
- *19 = 2.5*
- *2 = 2*
- *85 = 5.17*
- *3 = 3*
- *17 = 17*

On peut tout de suite conclure que q n'est pas hyperbolique : en effet, un seul des coefficients est divisible par 19 donc $\partial_{19}(q)$ *est de dimension 1 donc non hyperbolique.*

Exemple 3. *On cherche maintenant à savoir si* $q =< 57, -10, -38, 85, -3, 17 >$ *est hyperbolique (on a juste multiplié -2 par 19 par rapport à la précédente). La signature réduite est toujours nulle et cette fois les images par les morphismes* ∂_p *sont tous de dimension paire. On a*

$$\partial_2(q) =< -5, -19 >=< 1, -1 >= 0$$

$$\partial_3(q) =< 19, -1 >=< 1, -1 >= 0$$

$$\partial_5(q) =< -2, 17 >=< -2, 2 >= 0$$

$$\partial_{17}(q) =< 5, 1 >$$

$$\partial_{19}(q) =< 3, -2 >$$

Il reste à savoir si les deux dernières formes sont hyperboliques. Comme elles sont de dimension 2, il suffit de savoir si leur déterminant est égal à -1 modulo un carré. Pour 17, comme $17 \equiv 1[4]$*, -1 est un carré modulo 17. La forme est donc hyperbolique si et seulement si 5 est un carré modulo 17. Or*

$$\left(\frac{5}{17}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{17-1}{2}}\left(\frac{17}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1$$

Ainsi il ne s'agit pas non plus d'une forme hyperbolique.

3.3 Compléments de théorie des groupes

Définition 5 (Filtration)**.** *On appelle filtration d'un groupe G une suite croissante de sous-groupes de G dont l'union est égale à G.*

Lemme 4 (des cinq)**.** *Soient G, G', H, H', K, K' des groupes, i, i',* π*,* π'*, f, g, h des morphismes vérifiant le diagramme commutatif suivant :*

$$\begin{tikzcd} H \arrow[r, hook, "i"] \arrow[d, "f"] & G \arrow[r, two heads, "\pi"] \arrow[d, "g"] & K \arrow[d, "h"] \\ H' \arrow[r, hook, "i'"] & G' \arrow[r, two heads, "\pi'"] & K' \end{tikzcd}$$

où l'on a deux suites exactes courtes $H \to G \to K$ *et* $H' \to G' \to K'$*.*
Si f et h sont des isomorphismes, alors g aussi.

Démonstration. — Surjectivité : Soit $y \in G'$. Puisque $h \circ \pi$ est surjective, on peut introduire $x \in G$ tel que $h \circ \pi(x) = \pi' \circ g(x) = \pi'(y)$. Alors $y - g(x) \in \mathrm{Ker}(\pi') = \mathrm{Im}(i')$ donc on peut écrire $y - g(x) = i'(y')$ pour un $y' \in H'$. f est surjective donc on a $x' \in H$ tel que $y' = f(x')$. Alors $y = g(x) + i' \circ f(x') = g(x) + g \circ i(x') = g(x + i(x'))$.

— Injectivité : Soit $x \in \mathrm{Ker}(g)$. Alors $x \in \mathrm{Ker}(\pi' \circ g) = \mathrm{Ker}(h \circ \pi)$. h est injective donc $x \in \mathrm{Ker}(\pi) = \mathrm{Im}(i)$. Écrivons $x = i(x')$ où $x' \in H$. Alors $x' \in \mathrm{Ker}(g \circ i) = \mathrm{Ker}(i' \circ f)$. Or $i' \circ f$ est injective d'où $x' = 0$ puis $x = 0$.

□

Lemme 5. *Soient G et H deux groupes abéliens, $(G_n)_{n \in \mathbb{N}^*}$ une filtration de G, $(H_n)_{n \in \mathbb{N}^*}$ une filtration de H, $\psi : G \to H$ un morphisme de groupes. On suppose que*

— *$\phi(G_n) \subseteq H_n$ pour tout n*

— *ϕ induit un isomorphisme entre G_0 et H_0*

— *ϕ induit un isomorphisme entre G_{n+1}/G_n et H_{n+1}/H_n pour tout n*

Alors ϕ est un isomorphisme.

Démonstration. On commence par prouver par récurrence que $\phi_n : G_n \to H_n$ est un isomorphisme. C'est vrai pour n = 0 par hypothèse. Si c'est vrai à un rang n, alors on a le diagramme commutatif

$$\begin{tikzcd}
G_n \arrow[r, hook, "i"] \arrow[d, "\phi_n"] & G_{n+1} \arrow[r, two heads, "\pi"] \arrow[d, "\phi_{n+1}"] & G_{n+1}/G_n \arrow[d, "\psi"] \\
H_n \arrow[r, hook, "i'"] & H_{n+1} \arrow[r, two heads, "\pi'"] & H_{n+1}/H_n
\end{tikzcd}$$

où ψ est l'isomorphisme induit par ϕ, i et i' sont les inclusions canoniques donc injectives, π et π' les projections canoniques donc surjectives, et où l'on a bien deux suites exactes. ϕ_n et ψ sont des isomorphismes donc par le lemme des cinq ϕ_{n+1} aussi.

On en déduit ensuite aisément que ϕ est un isomorphisme :

— surjectivité : pour $h \in H$, on a un entier n tel que $h \in H_n$. ϕ_n est surjectif donc h admet un antécédent dans $G_n \subseteq G$.

— injectivité : si $\phi(g) = \phi(g')$, alors on introduit un entier n tel que $g \in G_n$ et $g' \in G_n$, ce qui est possible puisque (G_n) est croissante. ϕ_n est injective ce qui impose $g = g'$.

□

3.4 Preuve du théorème de structure

On note (p_n) la suite des nombres premiers.

On va prouver le théorème de structure grâce aux notions de la section précédente. On pose $G = W(\mathbb{Q})$ et $H = W(\mathbb{R}) \oplus \bigoplus_{p \text{ premier}} W(\mathbb{F}_p)$ ainsi que les filtrations

— (G_n) de G où, pour $n \in \mathbb{N}^*$, G_n est le sous-groupe engendré par $< k >$ pour k entiers dont les diviseurs premiers sont parmi les $p_1, ..., p_n$.

— (H_n) de H où, pour $n \in \mathbb{N}^*$, $H_n = W(\mathbb{R}) \oplus W(\mathbb{F}_{p_1}) \oplus ... \oplus W(\mathbb{F}_{p_n}) \oplus \{0\} \oplus \{0\} \oplus ...$

L'hypothèse $\Phi(G_n) \subseteq H_n$ est bien vérifiée. Les lemmes suivants permettent alors de conclure :

Lemme 6. *Φ induit un isomorphisme entre G_1 et H_1.*

Démonstration. Considérons une classe de Witt-équivalence rationnelle de G_1. Si l'on écrit une matrice diagonale représentant la forme anisotrope associée avec des coefficients entiers sans facteurs carrés, celle-ci ne possède que des coefficients 1 ou 2. Par ailleurs par la relation de Witt $< 1,1 > \simeq < 2,2 >$, donc on peut en fait l'écrire avec zéro ou un seul 2. Réciproquement, cela forme bien des classes distinctes car les discriminants ne sont pas dans la même classe de carré (i.e. $\sqrt{2}$ est irrationnel). Φ associe à une telle matrice sa classe de Witt-équivalence réelle qui correspond à sa dimension et sa classe de Witt-équivalence sur $\mathbb{F}_2$ qui correspond à la parité du nombre de 2. C'est donc bien un isomorphisme. □

Lemme 7. *Soit $n > 0$, a un entier dont les diviseurs premiers sont parmi $p_1, ..., p_n$. Soit r le reste de a modulo p_{n+1}. Alors*

$$< p_{n+1}a, -p_{n+1}r > \in G_n$$

Démonstration. On note $p = p_{n+1}$. On prouve d'abord le résultat pour $a \geqslant 0$ par récurrence.

— Si $a < p$, $r = a$ donc $< pa, -pr >$ est hyperbolique et appartient bien à G_n.

— Si $a \geqslant p$, ou de façon équivalente $a > p$ puisque p ne divise pas a, l'hypothèse permet d'écrire $a = bc$ avec $p < b < p^2$ (il suffit de prendre pour b le plus petit diviseur de a qui est strictement plus grand que p ; il est alors nécessairement strictement plus petit que p^2, puisque si on le divise pas l'un de ses facteurs premiers, il devient plus petit que p, et ce facteur premier est également plus petit que p par hypothèse sur a). On pose alors la division euclidienne de b par p, $b = pe + f$. Alors $f < p$, et $e < p$ (puisque $b < p^2$) donc les diviseurs premiers de e et f sont parmi $p_1, ..., p_n$. On peut écrire par la relation de Witt

$$< pa, -pfc > \simeq < p(b-f)c, p(b-f)cafc > \simeq < ce, aef > \in G_n$$

Or $< pfc, -pr > \in G_n$ par hypothèse de récurrence, donc

$$< pa, -pr > = < pa, -pfc > + < pfc, -pr > \in G_n$$

Pour $a < 0$, on procède de même mais par récurrence descendante :

— si $-p < a < 0$, on utilise la relation de Witt

$$< pa, -pr > = < pa, -p(a+p) > \simeq < -p^2, -p^2.pa.(-p(a+p)) > = < -1, a(a+p) > \in G_n$$

— si $a < -p$, on pose comme au-dessus $a = bc$ avec $p < b < p^2$, $b = ep + f$ avec $|e|, |f| < p$. Il vient de la même manière $< pa, -pfc > \in G_n$ puis $< pa, -pr > \in G_n$.

□

Lemme 8. *Φ induit un isomorphisme entre G_{n+1}/G_n et H_{n+1}/H_n pour tout n.*

Démonstration. Fixons n et posons $p = p_{n+1}$. H_{n+1}/H_n s'identifie canoniquement à $W(\mathbb{F}_p)$. On va construire le morphisme réciproque à ∂_p grâce à la présentation du groupe de Witt $W(\mathbb{F}_p)$. L'idée de base est que pour tout élément $\overline{a} \in \mathbb{F}_p^\times$ et pour tout représentant $a \in \mathbb{Z}$, on voudrait envoyer $\overline{a}$ sur $< pa > \in G_{n+1}/G_n$. Cependant cela pose deux

problèmes : premièrement il n'est pas clair que cette définition est indépendante du représentant choisi, deuxièmement il n'est même pas clair que l'élément $< pa >$ que l'on obtient appartient à G_{n+1}, puisque a pourrait très bien avoir des facteurs premiers plus grands que $p_{n+1} = p$. Il se trouve que ces deux problèmes se résolvent simultanément si au lieu de considérer un représentant $a \in \mathbb{Z}$ quelconque, on se limite aux a dont les facteurs premiers sont parmi les p_1, ..., p_n : le deuxième problème est corrigé de façon immédiate, et le premier problème l'est aussi par le (technique) lemme précédent. On a donc une fonction $f : \mathbb{F}_p^\times \to G_{n+1}/G_n$ bien définie ; montrons qu'elle satisfait aux conditions permettant de la prolonger au groupe de Witt. La difficulté réside essentiellement dans le bon choix des représentants :

— $1, -1 \in \mathbb{F}_p^\times$ ont pour représentants $1, -1 \in \mathbb{Z}$ qui n'ont aucun facteurs premiers, donc
$$f(1) + f(-1) =< p, -p >\simeq< 1, -1 >= 0 \bmod G_n$$

— pour $\overline{a}, \overline{b} \in \mathbb{F}_p^\times$, $0 < a, b < p$ leurs représentants "canoniques", les facteurs premiers de ab^2 sont inclus dans ceux de a et b, donc parmi les p_1, ..., p_n, et on a donc
$$f(\overline{a}\overline{b}^2) =< pab^2 >\simeq< pa >= f(\overline{a})$$

— pour $\overline{a}, \overline{b} \in \mathbb{F}_p^\times$ avec $a + b \neq 0$, on choisit comme représentant $a \in \mathbb{Z}$ de $\overline{a}$ le représentant "canonique" : $0 < a < p$, mais pour $\overline{b}$ il est plus commode de choisir l'unique représentant $b \in \mathbb{Z}$ vérifiant $-p < b < 0$ (c'est-à-dire que l'on retire p au représentant "canonique"). L'avantage de ce choix est qu'on a $-p < a + b < p$ (et $a + b \neq 0$ par hypothèse), et ainsi $a + b$ et $ab(a + b)$ sont des représentants aux facteurs premiers convenables pour $\overline{a}\overline{b}$ et $\overline{a}\overline{b}(\overline{a} + \overline{b})$ respectivement, et on peut les utiliser pour écrire :
$$f(a + b) + f(ab(a + b)) =< p(a + b), pab(a + b) >$$
D'autre part on a la relation de Witt :
$$f(a) + f(b) =< pa, pb >\simeq< p(a + b), p^3ab(a + b) \simeq< p(a + b), pab(a + b) >$$
d'où l'égalité souhaitée.

Ainsi f induit bien une fonction sur le groupe de Witt : $W(\mathbb{F}_p) \to G_{n+1}/G_n$. Il est essentiellement immédiat que c'est la réciproque recherchée à la fonction ∂_p. □

3.5 Principes de Hasse

Théorème 4 (Principe de Hasse faible)**.** *Deux formes quadratiques rationnelles ϕ et ψ sont Witt-équivalentes si et seulement si c'est le cas de ϕ_p et ψ_p pour tout p premier ou infini.*

Démonstration. Il s'agit de prouver que le morphisme Ψ qui à une forme rationnelle associe ses localisées est injectif. Or si on le compose avec l'identité sur $W(\mathbb{R})$ et, pour p premier, le morphisme ∂'_p sur $W(\mathbb{Q}_p)$, on obtient l'isomorphisme Φ. L'injectivité de Φ impose celle de Ψ. □

Théorème 5 (Principe de Hasse fort ou théorème de Hasse-Minkowski)**.** *Une forme quadratique rationnelle ψ est isotrope si et seulement si c'est le cas de ψ_p pour tout p premier ou infini.*

La démonstration ce résultat est l'objet principal de la suite du groupe de travail.