CORPS LOCAUX, NOTES DU COURS DE M2

par

Pierre Colmez

Table des matières

1. Corps locaux

1.1. Définition et exemples

Un *corps local* est un corps complet pour une valuation discrète. En particulier, si K est un corps local, et v est la valuation sur K, alors il existe $a > 0$ unique tel que $v(K^*) = a\mathbf{Z}$. Une *uniformisante* de K est alors n'importe quel élément π de K vérifiant $v(\pi) = a$.

Lemme 1.1. — *L'idéal maximal $\mathfrak{m}_K$ de l'anneau des entiers $\mathscr{O}_K$ de K est principal et un élément de K en est un générateur si et seulement si c'est une uniformisante.*

Démonstration. — Évident.

Exemple 1.2. — (i) $\mathbf{Q}_p$ muni de la valuation v_p est un corps local dont p est une uniformisante.

(ii) Si K est un corps, alors $K((T))$ muni de la valuation v_T est un corps local dont T est une uniformisante.

(iii) Le corps $\mathbf{Q}_p\{\{T\}\}$ des séries de Laurent $\sum_{n\in\mathbf{Z}} a_n T^n$, où $(a_n)_{n\in\mathbf{Z}}$ est une suite bornée d'éléments de $\mathbf{Q}_p$ tendant vers 0 quand n tend vers $-\infty$, devient un corps local si on le munit de la valuation v_p définie par $v_p(\sum_{n\in\mathbf{Z}} a_n T^n) = \inf_{n\in\mathbf{Z}} v_p(a_n)$. Son corps résiduel est $\mathbf{F}_p((T))$ qui n'est pas parfait (mais est un corps local) ; le corps $\mathbf{Q}_p\{\{T\}\}$ est un exemple de corps local de dimension 2.

Le théorème suivant, dont la démonstration utilise le lemme de Zorn, montre que l'exemple (ii) est typique.

Théorème 1.3. — *Si K est un corps local, et si k_K a même caractéristique que K, alors il existe un système de représentants de k_K dans $\mathscr{O}_K$ qui est un corps isomorphe à k_K, et le choix d'une uniformisante π de K induit un isomorphisme $K \cong k_K((T))$ envoyant π sur T.*

Définition 1.4. — Si A est un anneau et I est un idéal de A, on dit que A est *séparé et complet pour la topologie I-adique* si l'application naturelle de A dans $\varprojlim(A/I^nA)$ est un isomorphisme. La topologie I-adique sur A est alors celle qui fait de l'isomorphisme précédent un isomorphisme d'anneaux topologiques, $\varprojlim(A/I^nA)$ étant muni de la topologie produit, chacun des A/I^nA étant muni de la topologie discrète.

Lemme 1.5. — (i) *Si K est un corps complet pour une valuation v, et si $\pi \in K$ vérifie $v(\pi) > 0$, alors $\mathscr{O}_K$ est séparé et complet pour la topologie π-adique.*

(ii) *Si A est un anneau, si $\pi \in A$, si S est un et S est un système de représentants de $A/\pi A$ dans A, et si A est séparé et complet pour la topologie π-adique, alors tout élément de A peut s'écrire de manière unique sous la forme $\sum_{n=0}^{+\infty} s_n\pi^n$ avec $s_n \in S$.*

Démonstration. — (i) On note $\iota : \mathscr{O}_K \to \varprojlim(\mathscr{O}_K/\pi^n\mathscr{O}_K)$ l'application qui, à $x \in \mathscr{O}_K$, associe la suite des images de x modulo π^n. On a alors

• $\iota(x) = 0 \Leftrightarrow v(x) \geqslant nv(\pi)$ quel que soit $n \in \mathbf{N} \Leftrightarrow v(x) = +\infty \Leftrightarrow x = 0$, ce qui montre que ι est injective.

• Si $(x_n)_{n\in\mathbf{N}} \in \varprojlim(\mathscr{O}_K/\pi^n\mathscr{O}_K)$ et si $\hat{x}_n \in \mathscr{O}_K$ est un relèvement quelconque de x_n, alors $v(\hat{x}_{n+k} - \hat{x}_n) \geqslant nv(\pi)$ quels que soient $n, k \in \mathbf{N}$. Ceci montre que la suite $\hat{x}_n$ est de Cauchy, et sa limite x vérifie $v(x - \hat{x}_n) \geqslant nv(\pi)$ quel que soit $n \in \mathbf{N}$. On en déduit que $\iota(x) = (x_n)_{n\in\mathbf{N}}$, ce qui prouve la surjectivité de ι.

• « $v(x-y) \geqslant nv(\pi)$ » $\Leftrightarrow$ « $x = y$ dans $\mathscr{O}_K/\pi^k\mathscr{O}_K$, quel que soit $i \leqslant n$ », ce qui montre que la topologie induite par v sur $\mathscr{O}_K$ correspond à la topologie produit sur $\varprojlim(\mathscr{O}_K/\pi^n\mathscr{O}_K)$, chaque $\mathscr{O}_K/\pi^n\mathscr{O}_K$ étant muni de la topologie discrète.

(ii) Soit $s : A \to S$ l'application qui à x associe l'unique élément $s(x)$ de S vérifiant $x - s(x) \in \pi A$. Si $x \in A$, on définit par récurrence une suite $(x_n)_{n\in\mathbf{N}}$ d'éléments de A en posant $x_0 = x$ et, si $n \geqslant 1$, $x_n = \frac{1}{\pi}(x_{n-1} - s(x_{n-1}))$. On a alors $x = \sum_{i=0}^{n} s(x_i)\pi^i + \pi^{n+1}x_{n+1}$ quel que soit $n \in \mathbf{N}$, et donc $x = \sum_{n=0}^{+\infty} s(x_n)\pi^n$ ce qui prouve l'existence d'une écriture sous la forme mentionnée plus haut. D'autre part, si $\sum_{n=0}^{+\infty} s_n\pi^n = \sum_{n=0}^{+\infty} s'_n\pi^n$, alors réduisant modulo π, on obtient $s_0 = s'_0$

et une récurrence immédiate nous montre que $s_n = s'_n$ quel que soit $n \in \mathbf{N}$ d'où l'unicité de l'écriture.

Corollaire 1.6. — *Si K est un corps local, si S est un système de représentants de k_K dans $\mathscr{O}_K$, si π est une uniformisante de K, alors tout élément de $\mathscr{O}_K$ peut s'écrire de manière unique sous la forme $\sum_{n=0}^{+\infty} s_n \pi^n$ avec $s_n \in S$.*

Exemple 1.7. — Si $K = \mathbf{Q}_p$, on a $\mathscr{O}_K = \mathbf{Z}_p$ et $k_K = \mathbf{F}_p$, on peut prendre p comme uniformisante et $\{0, 1, \ldots, p-1\}$ ou $\{[x],\ x \in \mathbf{F}_p\}$ comme système de représentants de $\mathbf{F}_p$ dans $\mathbf{Z}_p$.

1.2. Généralités sur les p-anneaux

Définition 1.8. — Un anneau R de caractéristique p est *parfait* si l'élévation à la puissance p est un isomorphisme. (Si R est un corps on retombe sur la définition usuelle.) Si R est un anneau parfait de caractéristique p, *un idéal $\mathfrak{n}$ de R est parfait* s'il est stable par extraction de racines p-ième, ce qui équivaut à ce que $R/\mathfrak{n}$ soit parfait.

Définition 1.9. — Soient A un anneau et R un anneau de caractéristique p. On dit que A est *un p-anneau d'anneau résiduel R* s'il existe $\pi \in A$ tel que A soit séparé et complet pour la topologie π-adique et $R = A/\pi A$. Comme R est de caractéristique p, on a en particulier $p \in \pi A$. Un p-anneau est dit *strict* si $\pi = p$ et p n'est pas nilpotent dans A, et *parfait* s'il est strict et R est parfait.

Exemple 1.10. — (i) $\mathbf{Z}_p$ est un p-anneau parfait, car $\mathbf{F}_p$ est un corps parfait.

(ii) Si J est un ensemble quelconque, soit $W_J = \mathbf{Z}_p[X_j^{p^{-\infty}},\ j \in J] = \cup_{m \in \mathbf{N}} \mathbf{Z}_p[X_j^{p^{-m}},\ j \in J]$. On note $\widehat{W}_J$ le séparé complété de W_J pour la topologie p-adique (i.e $\widehat{W}_J = \varprojlim W_J/p^n W_J$), ce qui fait de $\widehat{W}_J$ un p-anneau strict d'anneau résiduel $\overline{W}_J = \mathbf{F}_p[X_j^{p^{-\infty}},\ j \in J]$ qui est parfait (on s'est clairement débrouillé pour).

Remarque 1.11. — Soit R un anneau parfait de caractéristique p. Le morphisme naturel de $\overline{W}_R$ dans R qui à $X_x \in \overline{W}_R$ associe x est surjectif, ce qui permet de voir tout anneau parfait comme un quotient d'un anneau du type $\overline{W}_J$ par un idéal parfait. Ceci permet de ramener beaucoup de questions concernant les anneaux parfaits de caractéristique p au cas des anneaux du type $\overline{W}_J$.

Proposition 1.12. — *Si A est un p-anneau d'anneau résiduel R et si $x \in A$, les deux conditions suivantes sont équivalentes :*

(i) x est inversible dans A ;

(ii) l'image $\overline{x}$ de x modulo π est inversible dans R.

Démonstration. — Si y est un inverse de x dans A, alors $\overline{y}$ est un inverse de $\overline{x}$ dans R. Réciproquement, si $\overline{y}$ est un inverse de $\overline{x}$ dans R, et si y est n'importe quel relèvement de $\overline{y}$ dans A, alors $z = 1 - xy \in \pi A$ et x admet comme inverse $y(\sum_{n=0}^{+\infty} z^n)$.

Corollaire 1.13. — *Si A est un p-anneau strict dont l'anneau résiduel est un corps, alors $B = A[\frac{1}{p}]$ est un corps.*

Démonstration. — Si $x \in B - \{0\}$, il existe un unique entier $n \in \mathbf{Z}$ tel que $p^n x \in A - pA$ et la proposition précédente montre que $p^n x$ est inversible dans A, ce qui permet de conclure.

1.3. Représentants de Teichmüller. — Si A est un anneau, on note $\mathbb{R}(A)$ l'ensemble des suites $x = (x^{(n)})_{n\in\mathbf{N}}$ d'éléments de A telles que l'on ait $(x^{(n+1)})^p = x^{(n)}$ quel que soit $n \in \mathbf{N}$. Dans tout ce qui suit, A est un p-anneau.

Lemme 1.14. — *Si x, y sont deux éléments de A vérifiant $x - y \in \pi A$, alors $x^{p^n} - y^{p^n} \in \pi^{n+1}A$ quel que soit $n \in \mathbf{N}$.*

Démonstration. — La formule du binôme montre que si $a \in A$ et $u \in \pi^n A$, alors $(a+u)^p - a^p \in \pi^{n+1}A$; on en déduit par récurrence sur n, le fait que si $a \in A$ et $u \in \pi A$, alors $(a+u)^{p^n} - a^{p^n} \in \pi^{n+1}A$, ce qui, appliqué à $a = x$ et $u = y - x$, permet de conclure.

Corollaire 1.15. — *Si $x = (x^{(n)})_{n\in\mathbf{N}} \in \mathbb{R}(R)$ et $\tilde{x}^{(n)}$ est un relèvement de $x^{(n)}$, alors la suite de terme général $(\tilde{x}^{(n+m)})^{p^m}$ converge dans A vers une limite $\psi_A^{(n)}(x)$ qui ne dépend que de x et $\psi_A(x) = (\psi_A^{(n)}(x))_{n\in\mathbf{N}} \in \mathbb{R}(A)$. De plus, on a $\psi_A(xy) = \psi_A(x)\psi_A(y)$.*

Démonstration. — Par construction, $(\tilde{x}^{(n+m+1)})^p - \tilde{x}^{(n+m)} \in \pi A$, et donc $(\tilde{x}^{(n+m+1)})^{p^{m+1}} - (\tilde{x}^{(n+m)})^{p^m} \in \pi^{m+1}A$, ce qui montre que la suite de terme général $(\tilde{x}^{(n+m)})^{p^m}$ converge dans A. Le fait que la limite ne dépende pas du choix des $\tilde{x}^{(n)}$ suit du fait que si on a deux choix, on en fabrique un troisième en panachant et que les trois limites sont égales. On démontre que $(\psi_A^{(n+1)}(x))^p = \psi_A^{(n)}(x)$ par passage à la limite, ce qui prouve que $\psi_A(x) = (\psi_A^{(n)}(x))_{n\in\mathbf{N}} \in \mathbb{R}(A)$. Finalement, la multiplicativité de ψ_A suit de ce que l'on peut prendre $\tilde{x}^{(n)}\tilde{y}^{(n)}$ comme relèvement de $(xy)^{(n)}$ dans A.

Remarque 1.16. — Si R est parfait, l'application qui à $x = (x^{(n)})_{n\in\mathbf{N}}$ associe $x^{(0)}$ est une bijection de $\mathbb{R}(R)$ sur R et l'application qui à $x \in R$ associe $[x] = \psi_A^{(0)}(x)$, (où x est considéré comme un élément de $\mathbb{R}(R)$) est multiplicative (i.e. $[xy] = [x][y]$ si $x, y \in R$) et l'image de $[x]$ dans $R = A/\pi A$ est x.

Définition 1.17. — L'élément $[x]$ de A est *le représentant de Teichmüller* de x dans A.

Exercice 1. — (i) Montrer que, si A est de caractéristique p, alors $[x+y] = [x] + [y]$ quels que soient $x, y \in R$.

(ii) Montrer que, si F est un corps local de caractéristique p, et si k_F est parfait, alors $F \cong k_F((T))$.

1.4. L'anneau des vecteurs de Witt d'un anneau parfait de caractéristique p. — On a vu que l'on pouvait écrire tout élément de $\mathbf{Z}_p$ de manière unique sous la forme $\sum_{i=0}^{+\infty} p^i\omega_i$, où les ω_i sont des représentants de Teichmüller d'éléments de $\mathbf{F}_p$ (i.e. des racines de l'équation $X^p - X = 0$). On peut se demander s'il est possible de décrire les lois d'addition et multiplication en utilisant cette écriture. C'est le cas et cela va nous mener à introduire les vecteurs de Witt.

Théorème 1.18. — *Si R est un anneau parfait de caractéristique p, il existe un p-anneau strict $W(R)$* (anneau des vecteurs de Witt à coefficients dans R)*, unique à isomorphisme unique près, dont l'anneau résiduel est R.*

De plus, $W(R)$ vérifie la propriété universelle suivante. Si A est un p-anneau d'anneau résiduel R', si $\overline{\theta} : R \to R'$ un morphisme d'anneaux, et si $\tilde{\theta} : R \to A$ est une application multiplicative relevant $\overline{\theta}$, il existe un unique morphisme d'anneau $\theta : W(R) \to A$ tel que si $x \in R$, alors $\theta([x]) = \tilde{\theta}(x)$.

Proposition 1.19. — *Si A est un p-anneau parfait d'anneau résiduel R, alors tout élément de A s'écrit de manière unique sous la forme $\sum_{i=0}^{+\infty} p^i[x_i]$, où les x_i sont des éléments de R.*

Démonstration. — C'est vrai pour tout système de représentants de R dans A (lemme 1.2).

Lemme 1.20. — *Soit J un ensemble d'indices. Si A est un p-anneau d'anneau résiduel R, si $\overline{\theta} : \overline{W}_J \to R$ un morphisme d'anneaux, et si $\tilde{\theta} : \overline{W}_J \to A$ est une application multiplicative relevant $\overline{\theta}$, il existe un unique morphisme d'anneau $\theta : \widehat{W}_J \to A$ tel que si $x \in \overline{W}_J$, alors $\theta([x]) = \tilde{\theta}(x)$.*

Démonstration. — L'unicité est claire : on doit avoir $\theta(\sum_{i=0}^{+\infty} p^i[x_i]) = \sum_{i=0}^{+\infty} p^i\tilde{\theta}(x_i)$. Montrons l'existence. Soit $f : W_J \to A$ le morphisme d'anneaux défini par $f(X_j^{p^{-m}}) = \tilde{\theta}(X_j^{p^{-m}})$ si $j \in J$ et $m \in \mathbf{N}$. On prolonge f par continuité en un morphisme $\hat{f} : \widehat{W}_J \to A$ et pour conclure, il suffit de prouver que si $x \in \overline{W}_J$, alors $\hat{f}([x]) = \tilde{\theta}(x)$. Le morphisme $\overline{f} : \overline{W}_J \to R$ induit par $\hat{f}$ coïncide par construction avec $\overline{\theta}$ sur $X_j^{p^{-m}}$ si $j \in J$ et $m \in \mathbf{N}$ et comme ces éléments engendrent $\overline{W}_J$, on en déduit l'égalité de $\overline{f}$ et $\overline{\theta}$. Ceci implique en particulier que si $x \in \overline{W}_J$ et $n \in \mathbf{N}$, alors $\hat{f}([x^{p^{-n}}]) - \tilde{\theta}(x^{p^{-n}}) \in \pi A$ et donc, d'après le lemme 1.14, que $\hat{f}([x]) - \tilde{\theta}(x) \in \pi^{n+1}A$ quel que soit $n \in \mathbf{N}$, et permet de conclure.

Soit $\mathbf{N} \amalg \mathbf{N}$ la réunion disjointe de deux copies de $\mathbf{N}$. Pour alléger un peu les notations, notons X_i et Y_i au lieu de $X_{1,i}$ et $X_{2,i}$ les variables de $W_{\mathbf{N}\amalg\mathbf{N}}$ Un élément $P(X,Y)$ de $\overline{W}_{\mathbf{N}\amalg\mathbf{N}}$ peut s'écrire de manière unique sous la forme

$$P(X,Y) = \sum_{\mathbf{r},\mathbf{s}} a_{\mathbf{r},\mathbf{s}} \Big(\prod_{i=0}^{+\infty} X_i^{r_i}\Big)\Big(\prod_{j=0}^{+\infty} Y_j^{s_j}\Big),$$

la somme portant sur les couples $(\mathbf{r},\mathbf{s})$ de familles d'éléments de $\mathbf{Z}[\frac{1}{p}]$ n'ayant qu'un nombre fini de termes non nuls et les $a_{\mathbf{r},\mathbf{s}}$ étant des éléments de $\mathbf{F}_p$ presque tous nuls.

Soient $(S_i(X,Y))_{i\in\mathbf{N}}$ et $(P_i(X,Y))_{i\in\mathbf{N}}$ les suites d'éléments de $\overline{W}_{\mathbf{N}\amalg\mathbf{N}}$ définie par

$$\sum_{i=0}^{+\infty} p^i[X_i] + \sum_{i=0}^{+\infty} p^i[Y_i] = \sum_{i=0}^{+\infty} p^i[S_i(X,Y)] \quad \text{et} \quad \Big(\sum_{i=0}^{+\infty} p^i[X_i]\Big)\Big(\sum_{i=0}^{+\infty} p^i[Y_i]\Big) = \sum_{i=0}^{+\infty} p^i[P_i(X,Y)].$$

Les polynômes S_i et P_i sont des polynômes universels permettant de décrire les lois d'addition et multiplication dans un p-anneau parfait si on écrit les éléments sous la forme $\sum_{i=0}^{+\infty} p^i[x_i]$, où les x_i sont des éléments de l'anneau résiduel. De manière précise, on a la proposition suivante.

Proposition 1.21. — *Si A est un p-anneau parfait d'anneau résiduel R, et si $x = (x_i)_{i\in\mathbf{N}}$ est une suite d'éléments de R, on note $\Sigma(x)$ l'élément $\sum_{i=0}^{+\infty} p^i[x_i]$ de A.*

Si $x = (x_i)_{i\in\mathbf{N}}$ et $y = (y_i)_{i\in\mathbf{N}}$ sont deux suites d'éléments de R, alors

$$\Sigma(x) + \Sigma(y) = \sum_{i=1}^{+\infty} p^i[S_i(x,y)] \quad \text{et} \quad \Sigma(x)\Sigma(y) = \sum_{i=1}^{+\infty} p^i[P_i(x,y)].$$

Démonstration. — Soit $\overline{\theta} : \overline{W}_{\mathbf{N}\amalg\mathbf{N}} \to R$ le morphisme défini par $\overline{\theta}(X_i) = x_i$ et $\overline{\theta}(Y_i) = y_i$ si $i \in \mathbf{N}$. Soit $\tilde{\theta} : \overline{W}_{\mathbf{N}\amalg\mathbf{N}} \to A$ l'application multiplicative définie par $\tilde{\theta}(x) = [\overline{\theta}(x)]$. D'après le lemme 1.20, il existe une unique morphisme $\theta : \widehat{W}_J \to A$ tel que l'on ait $\theta([z]) = [\overline{\theta}(z)]$ quel que soit $z \in \overline{W}_{\mathbf{N}\amalg\mathbf{N}}$. Soient alors $X = (X_i)_i$ et $Y = (Y_i)_{i\in I}$ les deux suites naturelles d'éléments de $W_{\mathbf{N}\amalg\mathbf{N}}$. On a par construction $\Sigma(x) = \theta(\Sigma(X))$ et $\Sigma(y) = \theta(\Sigma(Y))$, ce qui nous donne les formules

$$\begin{aligned}\Sigma(x) + \Sigma(y) =& \theta(\Sigma(X)) + \theta(\Sigma(Y)) = \theta(\Sigma(X) + \Sigma(Y)) \\ =& \theta(\sum_{i=0}^{+\infty} p^i[S_i(X,Y)]) = \sum_{i=0}^{+\infty} p^i[\overline{\theta}(S_i(X,Y))] = \sum_{i=0}^{+\infty} p^i[S_i(x,y)],\end{aligned}$$

ce qui donne le résultat pour la somme ; le produit se traitant exactement de la même manière, cela permet de conclure.

Remarque 1.22. — (i) La proposition 1.19 décrit un anneau parfait d'anneau résiduel R de manière ensembliste, en fonction de R, et la prop. 1.21 montre qu'il existe au plus une structure de p-anneau strict sur cet ensemble, qui fasse de R l'anneau résiduel. On en déduit l'unicité de $W(R)$.

(ii) Du fait de la distributivité de la multiplication par rapport à l'addition et de la continuité de l'addition, pour être capable de multiplier, additionner ou soustraire deux éléments de la forme $\Sigma(x)$ et $\Sigma(y)$, il suffit d'avoir une formule pour $[X] - [Y]$.

(iii) Comme $\Sigma(0) = 0$, on a $\Sigma(x) + \Sigma(y) = 0$, si $x = 0$ et $y = 0$; cela implique que les S_i, $i \in \mathbf{N}$, n'ont pas de terme constant. De même, $\Sigma(x)\Sigma(y) = 0$ si $x = 0$ ou $y = 0$, cela implique que les P_i n'ont pas de termes de degré 0 en les X_j ou en les Y_j.

Exercice 2. — Montrer que, si $i \in \mathbf{N}$, alors S_i (resp. P_i) est un polynôme homogène de degré 1 (resp. de degré 2) en $X_0, \dots, X_i, Y_0, \dots, Y_i$.

Lemme 1.23. — *Soit A un p-anneau strict d'anneau résiduel R parfait et $\mathfrak{n}$ un idéal parfait de R distinct de R, l'ensemble $W(\mathfrak{n}) = \{\sum_{i=0}^{+\infty} p^i[x_i] \mid x_i \in \mathfrak{n}$ quel que soit $i \in \mathbf{N}\}$ est un idéal fermé de A et $A/W(\mathfrak{n})$ est un p-anneau parfait d'anneau résiduel $R/\mathfrak{n}$.*

Démonstration. — On déduit de la prop 1.21 que $W(\mathfrak{n})$ est un sous-groupe additif de A, et qu'il est stable par multiplication par un élément de A car $v_X(P_i) = v_Y(P_i) > 0$ (rem. 1.22). Par ailleurs, $W(\mathfrak{n})$ est fermé par construction, et l'anneau résiduel de $A/W(\mathfrak{n})$ est $A/W(\mathfrak{n}) + pA = R/\mathfrak{n}$, ce qui termine la démonstration.

Revenons à la démonstration du théorème 1.18. L'unicité a déjà été démontrée au (i) de la rem. 1.22. Si R est parfait de caractéristique p, on peut l'écrire (de manière non unique) comme un quotient d'un $\overline{W}_J$ par un idéal parfait $\mathfrak{n}$. Le lemme précédent montre que $W(R) = \widehat{W}_J/W(\mathfrak{n})$ est un p-anneau parfait d'anneau résiduel R.

Il reste à prouver que $W(R)$ satisfait la propriété universelle demandée, mais cela se déduit du lemme 1.20 en composant tout avec la projection de $\overline{W}_J$ sur R et en remarquant que le morphisme de $\widehat{W}_J$ dans A que l'on obtient se factorise à travers $W(R)$.

Exemple 1.24. — (i) $W(\mathbf{F}_p) = \mathbf{Z}_p$.

(ii) Plus généralement, si K est un corps local de caractéristique 0 dont le corps résiduel k_K est parfait de caractéristique p, et dont p est une uniformisante, alors $K \cong W(k_K)[\frac{1}{p}]$.

Démonstration. — l'anneau des entiers de K est un p-anneau parfait d'anneau résiduel k_K, donc isomorphe à $W(k_K)$.

Exercice 3. — On définit par récurrence sur n, une suite $(U_n)_{u\in\mathbf{N}}$ d'éléments de $\mathbf{Z}[\frac{1}{p}][X,Y]$, en posant

$$U_n(X,Y) = \frac{1}{p^n}\Big(X^{p^n} + Y^{p^n} - \Big(\sum_{i=0}^{n-1} p^i U_i(X,Y)^{p^{n-i}}\Big)\Big).$$

(i) Calculer U_0 et U_1 et vérifier que $U_0, U_1 \in \mathbf{Z}[X,Y]$.

(ii) On se place dans l'anneau $S_{X,Y} = \mathbf{Z}[\widehat{X^{p^{-\infty}}, Y^{p^{-\infty}}}]$ et on écrit $X+Y$ sous la forme

$$X + Y = \sum_{i=0}^{+\infty} p^i [V_i(X,Y)], \quad \text{avec } V_i \in \mathbf{F}_p[X^{p^{-\infty}}, Y^{p^{-\infty}}].$$

(a) Montrer que $X^{p^n} + Y^{p^n} = \sum_{i=0}^{+\infty} p^i [V_i(X,Y)^{p^n}]$.

(b) On suppose que, quel que soit $i \leqslant n-1$, $U_i \in \mathbf{Z}[X,Y]$ et que l'image $\overline{U}_i$ de U_i dans $\mathbf{F}_p[X,Y]$ vérifie $\overline{U}_i = V_i^{p^i}$. Montrer que

$$\sum_{i=0}^{n-1} p^i U_i(X,Y)^{p^{n-i}} \equiv \sum_{i=0}^{n-1} p^i [V_i(X,Y)^{p^n}] \mod p^{n+1}.$$

En déduire que $U_n \in \mathbf{Z}[X,Y]$ et que $\overline{U}_n = V_n^{p^n}$.

(iii) Montrer que V_n est un polynôme en $X^{p^{-n}}$ et $Y^{p^{-n}}$, puis que S_n et P_n, donnant l'addition et la multiplication des vecteurs de Witt, sont des polynômes en les $X_j^{p^{j-n}}, Y_j^{p^{j-n}}$, avec $j \leqslant n$.

Proposition 1.25. — *Si R et R' sont deux anneaux parfaits de caractéristique p, l'application naturelle de* $\mathrm{Hom}(W(R), W(R'))$ *dans* $\mathrm{Hom}(R, R')$ *est une bijection.*

En particulier, le morphisme de Frobenius $x \to x^p$ sur R se relève en un automorphisme φ (de Frobenius) de $W(R)$.

Démonstration. — Si $\overline{\theta}$ est un morphisme de R dans R', on pose $\tilde{\theta}(x) = [\overline{\theta}(x)]$ et $\tilde{\theta}$ est une application multiplicative de R dans $W(R')$ relevant $\overline{\theta}$; on en déduit, utilisant la seconde partie du théorème, la surjectivité de l'application naturelle de $\mathrm{Hom}(W(R), W(R'))$ dans $\mathrm{Hom}(R, R')$.

Si θ est un morphisme de $W(R)$ dans $W(R')$, on a $\theta([x]) = \lim_{n\to+\infty} = \theta([x^{p^{-n}}])^{p^n} = [\overline{\theta}(x)]$ d'après le corollaire 1.15 (et la remarque 1.16), puisque $\theta([x^{p^{-n}}])$ est un relèvement dans $W(R')$ de $\overline{\theta}(x^{p^{-n}}) = (\overline{\theta}(x))^{p^{-n}}$, et l'injectivité suit de ce que $W(R)$ étant un p-anneau strict, la connaissance de $\theta([x])$ pour tout $x \in R$ est équivalente à la connaissance de θ d'après la proposition 1.19.

Exercice 4. — Soit k un corps algébriquement clos de caractéristique p.

(i) Montrer que $\varphi - 1 : W(k) \to W(k)$ est surjectif. Quel est son noyau ?

(ii) Montrer que, si $u \in W(k)^*$, alors il existe $x \in W(k)^*$ tel que $\frac{\varphi(x)}{x} = u$.

2. Extensions de corps locaux

Dans tout ce § (sauf mention explicite du contraire), F est un corps complet pour une valuation discrète, et le corps résiduel k_F est de caractéristique p.

2.1. Ramification et inertie. — Si F est un corps complet pour une valuation discrète et K est une extension finie de F , le corps résiduel k_K est une extension finie de k_F de degré $f = f(K/F)$ appelé indice d'inertie de l'extension K/F.

D'autre part, on a $v(K^*) \subset \frac{1}{[K:F]}v(F^*)$ et $v(F^*)$ est donc d'indice fini $e = e(K/F)$ dans $v(K^*)$. Cet indice est appelé indice de ramification de l'extension K/F.

Lemme 2.1. — *Soient $e = e(K/F)$ et $f = f(K/F)$. Soient $u_1, \dots, u_f$ des éléments de $\mathscr{O}_K$ dont les réductions modulo $\mathfrak{m}_K$ forment une base de k_K sur k_F et π_K une uniformisante de $\mathscr{O}_K$. Alors, les $\pi_K^j u_i$ pour $0 \leqslant j \leqslant e-1$ et $1 \leqslant i \leqslant f$ forment une base de $\mathscr{O}_K$ sur $\mathscr{O}_F$.*

Démonstration. — Soit S_F un système de représentants de k_F dans $\mathscr{O}_F$ et soit $S_K = S_F u_1 + \cdots + S_F u_f$, ce qui fait de S_K un système de représentants de k_K dans $\mathscr{O}_K$. Soit π_F une uniformisante de F. Comme $\mathscr{O}_K/\pi_F\mathscr{O}_K = \mathscr{O}_K/\pi_K^e\mathscr{O}_K$, on déduit du corollaire 1.6, le fait que $S_K + \pi_K S_K + \cdots + \pi_K^{e-1} S_K$ est un système de représentants de $\mathscr{O}_K/\pi_F\mathscr{O}_K$ et donc que tout élément de $\mathscr{O}_K$ peut s'écrire de manière unique sous la forme

$$\sum_{n=0}^{+\infty} \pi_F^n \Big(\sum_{j=0}^{e-1} \pi_K^j \Big(\sum_{i=1}^{f} s_{i,j,n} u_i \Big) \Big) = \sum_{j=0}^{e-1} \sum_{i=1}^{f} \pi_K^j u_i \Big(\sum_{n=0}^{+\infty} \pi_F^n s_{i,j,n} \Big)$$

avec $s_{i,j,n} \in S_F$, ce qui implique, utilisant le fait que tout élément de $\mathscr{O}_F$ peut s'écrire de manière unique sous la forme $\sum_{n=0}^{+\infty} \pi_F^n s_n$ avec $s_n \in S_F$, que tout élément de $\mathscr{O}_K$ peut s'écrire de manière unique sous la forme $\sum_{j=0}^{e-1} \sum_{i=1}^{f} \pi_K^j u_i y_{i,j}$ avec $y_{i,j} \in \mathscr{O}_F$. Ceci permet de conclure.

Corollaire 2.2. — $e(K/F)f(K/F) = [K : F]$.

Démonstration. — Une base de $\mathscr{O}_K$ sur $\mathscr{O}_F$ est aussi une base de K sur F.

Définition 2.3. — L'extension K/F est *non ramifiée* si $e(K/F) = 1$, et si k_K/k_F est séparable. Elle est *totalement ramifiée* si $e(K/F) = [K : F]$. Elle est *modérément ramifiée* si $e(K/F)$ est premier à la caractéristique du corps résiduel et si k_K/k_F est séparable, et *sauvagement ramifiée* dans le cas contraire.

Lemme 2.4. — *Si L/K et K/F sont deux extensions finies, alors $e(L/F) = e(L/K)e(K/F)$ et $f(L/F) = f(L/K)f(K/F)$*

Démonstration. — exercice.

Exercice 5. — (i) Montrer que si K et L sont deux extensions non ramifiées de F, alors $K \cdot L$ est une extension non ramifiée de F.

(ii) Construire un exemple où K et L sont deux extensions totalement ramifiées de F, et $K \cdot L$ n'est pas une extension totalement ramifiée de F.

2.2. Extensions totalement ramifiées

Si K est un corps local, un *polynôme d'Eisenstein* de degré d est un polynôme unitaire $P(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in K[X]$ tel que a_0 soit une uniformisante de K, et $a_1, \ldots, a_{d-1} \in \mathfrak{m}_K$. Comme on l'a déjà remarqué, la théorie des polygones de Newton permet de montrer qu'un tel polynôme est irréductible.

Lemme 2.5. — *Soit K un corps complet pour une valuation discrète et P un polynôme d'Eisenstein de degré d. Soit $L = K[X]/P$ et x l'image de X dans L. Alors*

(i) *Si $v(K^*) = u\mathbf{Z}$ avec $u > 0$, alors $v(x) = \frac{u}{d}$ et L/K est totalement ramifiée.*
(ii) *x est une uniformisante de L.*
(iii) *si $y = \sum_{i=0}^{d-1} a_i x^i$, alors $v(y) = \inf_i v(a_i) + i\frac{u}{d}$.*
(iv) *$1, x, \ldots, x^{d-1}$ forment une base de $\mathscr{O}_L$ (resp. L) sur $\mathscr{O}_K$ (resp. K).*

Démonstration. — Le (i) est une conséquence de la formule $v(x) = \frac{1}{[K:F]} v(\mathrm{N}_{K/F}(x))$ et du fait que P est d'Eisenstein. Le (ii) en est un corrolaire immédiat. Le (iii) est une conséquence du fait que tous les termes de la somme ont une valuation différente. Le (iv) est une conséquence immédiate du (iii).

Proposition 2.6. — *Si K/F est totalement ramifiée et si π_K est une uniformisante de K, alors π_K engendre $\mathscr{O}_K$ en tant que $\mathscr{O}_F$-algèbre et le polynôme minimal de π_K sur F est un polynôme d'Eisenstein.*

Réciproquement, si $P \in F[X]$ est un polynôme d'Eisenstein, si $K = F[X]/P$, et si x est l'image de X dans K, alors K est une extension totalement ramifiée de F et x en est une uniformisante.

Démonstration. — Le fait que π_K engendre $\mathscr{O}_K$ est une conséquence du lemme 2.1 appliquée à $f = 1$ et $u_1 = 1$. Si $[K : F] = d$, le polynôme minimal P de π_K est donc irréductible de degré d ; son polygone de Newton n'a donc qu'un pente. Par ailleurs, si $P = X^d + a_{d-1}X^{d-1} + \cdots + a_0$, on a $a_0 = \pm \mathrm{N}_{K/F}(\pi_K)$ et donc $v(a_0) = dv(\pi_K)$, ce qui implique que a_0 est une uniformisante de F. De plus, le fait que le polygone de Newton de P n'a qu'une pente se traduit par $v(a_i) \geqslant (d-i)v(\pi_K) > 0$, et donc $a_i \in \mathfrak{m}_K$ si $1 \leqslant i \leqslant d$. En conclusion P est d'Eisenstein. La réciproque est une conséquence du lemme 2.5.

2.3. Monogénéité de l'anneau des entiers

Remarque 2.7. — On vient de démontrer que si K est une extension finie de F totalement ramifiée, alors $\mathscr{O}_K$ est monogène sur $\mathscr{O}_F$ (i.e. il existe $x \in \mathscr{O}_K$ tel que l'on ait $\mathscr{O}_K = \mathscr{O}_F[x]$). Il s'agit là d'un cas particulier de la très utile proposition suivante.

Proposition 2.8. — *Si K est une extension finie de F, et si k_K/k_F est séparable, alors $\mathscr{O}_K$ est une extension monogène de $\mathscr{O}_F$.*

Démonstration. — Soient π_F et π_K des uniformisantes de F et K respectivement. Soit $y \in \mathscr{O}_K$ dont la réduction $\overline{y}$ modulo π_K est un élément primitif de k_K sur k_F (l'existence d'un tel élément est assurée par l'hypothèse k_K/k_F séparable). Soit $P \in \mathscr{O}_F[X]$ unitaire dont la réduction $\overline{P}$ modulo π_F est le polynôme minimal de $\overline{y}$ sur k_F. On a donc $P(y) \equiv 0$ mod. π_K et $P'(y) \not\equiv 0$ mod π_K car $\overline{y}$ est racine simple de $\overline{P}$. On en déduit le fait que $a \mapsto P(y+a\pi_K) = P(y)+a\pi_K P'(y)$ mod π_K^2 n'est pas identiquement nul sur $\mathscr{O}_K$, et donc qu'il existe $x = y + a\pi_K$ tel que $P(x)$ soit

une uniformisante de K. On peut alors utiliser le lemme 2.1 pour démontrer que les $x^i P(x)^j$ pour $0 \leqslant x \leqslant f-1$ et $0 \leqslant j \leqslant e-1$ forment une base de $\mathscr{O}_K$ sur $\mathscr{O}_F$, et donc que x engendre $\mathscr{O}_K$ comme $\mathscr{O}_F$-algèbre.

2.4. Extensions non ramifiées et dévissage des extensions finies

Théorème 2.9. — (i) *Si k est une extension finie séparable de k_F, il existe une unique extension non ramifiée $F(k)$ de F dont le corps résiduel est k.*

(ii) *Si L est une extension finie de F et si k_L/k_F est séparable, alors $F(k_L) \subset L$, l'extension $L/F(k_L)$ est totalement ramifiée, et $F(k_L)$ est l'unique extension non ramifiée de F ayant ces deux propriétés.*

Démonstration. — Soit $\overline{\alpha}$ un élément primitif de k/k_F, et soient $\overline{P} \in k_F[X]$ son polynôme minimal, et $P \in \mathscr{O}_F[X]$ unitaire dont la réduction est $\overline{P}$. D'après le lemme de Hensel, si L est une extension finie de F dont le corps résiduel contient k, alors L contient un unique racine α de P dont l'image dans k_L est $\overline{\alpha}$. On a alors $[F(\alpha) : F] \leqslant \deg P = [k : k_F]$. Comme d'autre part, le corps résiduel de $F(\alpha)$ contient $\overline{\alpha}$ par construction, on a $f(F(\alpha)/F) \geqslant [k : k_F]$; on en déduit l'égalité $[F(\alpha) : F] = [k : k_F] = f(F(\overline{\alpha})/F)$, ce qui implique que $F(\alpha)/F$ est non ramifiée. Maintenant, si L est une extension finie de F de corps résiduel k, on a $F(\alpha) \subset L$, d'après la discussion précédente, et $F(\alpha)$ ayant même corps résiduel que L, l'extension $L/F(\alpha)$ est totalement ramifiée ; en particulier, si L/F est non ramifiée, alors $L = F(\alpha)$. Ceci permet de conclure, avec $F(k) = F(\alpha)$.

Remarque 2.10. — Soit $\overline{F}$ une clôture algébrique de F. Comme la composée de deux extensions non ramifiée est non ramifiée, *l'extension maximale non ramifiée* F^{nr} de F, réunion de toutes les extensions non ramifiées de F, est un sous-corps de $\overline{F}$.

Exemple 2.11. — Le polynôme $X^q - X$ n'a que des racines simples dans $\overline{\mathbf{F}}_p$, et ses racines sont exactement les éléments de $\mathbf{F}_q$. On en déduit le fait que $\mathbf{Q}_p(\mathbf{F}_q)$ est le corps engendré par les racines du polynôme $X^q - 1$, c'est-à-dire par les racines $(q-1)$-ièmes de l'unité. L'extension maximale non ramifiée $\mathbf{Q}_p^{\mathrm{nr}}$ de $\mathbf{Q}_p$ est donc le sous-corps de $\overline{\mathbf{Q}}_p$ engendré par les racines de l'unité d'ordre premier à p.

Exercice 6. — Si $P \in \mathscr{O}_F[X]$ est unitaire et n'a que des racines simples dans $\overline{k}_F$, alors l'extension K de F engendrée par les racines de P est non ramifiée.

Exercice 7. — Montrer que, si K est de caractéristique 0, si k_F est parfait de caractéristique p, et si L est une extension finie de F, alors L contient l'anneau des vecteurs de Witt à coefficients dans k_L, et que $F(k_L)$ est le composé de F et $W(k_L)[\frac{1}{p}]$.

Exercice 8. — (i) Montrer que $\mathbf{Q}_p^{\mathrm{nr}} = \cup_{n \in \mathbf{N}} W(\mathbf{F}_{p^n})[\frac{1}{p}]$.

(ii) Montrer que $\mathbf{Q}_p^{\mathrm{nr}}$ n'est pas fermé dans $\mathbf{C}_p$, et que son adhérence est $W(\overline{\mathbf{F}}_p)[\frac{1}{p}]$.

Exercice 9. — Soit F un corps local de corps résiduel k_F de caractéristique p. Soit $\varphi : F \to F$ un morphisme continu, et soit K une extension finie non ramifiée, de degré n, de F.

(i) Montrer que $\varphi(\mathscr{O}_F) \subset \mathscr{O}_F$ et $\varphi(\mathfrak{m}_F) \subset \mathfrak{m}_F$. On note $\overline{\varphi} : k_F \to k_F$ le morphisme induit.

(ii) On suppose que $\overline{\varphi}(x) = x^p$, si $x \in k_F$. Soit $x \in \mathscr{O}_K$ dont le polynôme minimal $P = X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in \mathscr{O}_F[X]$ sur F a une réduction $\overline{P} \in k_F[X]$ qui est séparable. Montrer

qu'il existe $y \in \mathscr{O}_K$ unique dont la réduction modulo $\mathfrak{m}_K$ est $\overline{x}^p$ et qui est racine du polynôme P^φ défini par $P^\varphi(X) = X^d + \varphi(a_{d-1})X^{d-1} + \cdots + \varphi(a_0)$.

(iii) Montrer que φ s'étend de manière unique en un morphisme continu de K dans K tel que le morphisme induit sur k_K soit $x \mapsto x^p$.

(iv) Plus généralement, montrer que si $\overline{\varphi}$ s'étend en un morphisme de k_K dans k_K, alors φ s'étend de manière unique en un morphisme continu de K dans K tel que le morphisme induit sur k_K soit $\overline{\varphi}$.

2.5. Extensions modérément ramifiées

Proposition 2.12. — *Soit L/F une extension totalement ramifiée de degré $n = n_0 p^k$ avec $(n_0, p) = 1$. Alors L contient une unique extension K de F vérifiant $[K : F] = n_0$. De plus, il existe une uniformisante π_K de K telle que $\pi_K^{n_0} \in F$.*

Démonstration. — Soit π_L une uniformisante de L. On sait que π_L est racine d'un polynôme d'Eisenstein, et il existe donc π_F uniformisante de F, et $a_1, \ldots, a_{n-1} \in \mathscr{O}_F$ tels que l'on ait $\pi_L^n = u\pi_F$ avec $u = (1 + a_1\pi_L + \cdots + a_{n-1}\pi_L^{n-1}) \in \mathscr{O}_L^*$ vérifiant $v(u-1) > 0$. Comme $(n_0, p) = 1$, le lemme de Hensel permet de montrer que l'équation $v^{n_0} = u$ a une unique solution dans $1 + \mathfrak{m}_L$. On a alors $(v^{-1}\pi_L^{p^k})^{n_0} = \pi_F$, ce qui implique que L contient l'extension K définie par le polynôme d'Eisenstein $P(X) = X^{n_0} - \pi_F$ qui est totalement ramifiée de degré n_0 sur F.

Supposons maintenant que L contienne deux extensions K_1 et K_2 de F de degré n_0. Si on applique ce qui précède à ces deux extensions, on voit que si $i \in \{1, 2\}$, il existe une uniformisante π_i de K_i telle que $\pi_i^{n_0} \in F$. Mais alors $v(\pi_i) = \frac{1}{n_0}$, ce qui implique que $x = \frac{\pi_1}{\pi_2}$ est un élément de $\mathscr{O}_L^*$ dont la puissance n_0-ième appartient à F. Comme les corps résiduels de L et F sont les mêmes (puisque L/F est totalement ramifiée), on peut trouver $u \in \mathscr{O}_F$ tel que $v(xu^{-1} - 1) > 0$. Mais alors xu^{-1} est l'unique racine n_0-ième de $x^{n_0}u^{-n_0} \in 1 + \mathfrak{m}_F$ vérifiant $v(xu^{-1} - 1) > 0$, et $xu^{-1} \in 1 + \mathfrak{m}_F$ d'après le lemme de Hensel. On a donc $x \in F$, ce qui prouve que $K_1 = K_2$.

2.6. Extensions galoisiennes

Si L est une extension galoisienne finie de F et $\sigma \in \mathrm{Gal}(L/F)$, on a $v(\sigma(x)) = v(x)$ quel que soit $x \in L$. On en déduit le fait que $\sigma(\mathscr{O}_L) = \mathscr{O}_L$ et $\sigma(\mathfrak{m}_L) = \mathfrak{m}_L$ et donc que σ passe au quotient. On a donc une application naturelle de $\mathrm{Gal}(L/K)$ dans $\mathrm{Aut}_{k_F}(k_L)$ qui est de manière évidente un morphisme de groupes.

Définition 2.13. — On appelle *sous-groupe d'inertie* de $\mathrm{Gal}(L/F)$ le noyau $I_{L/F}$ de l'application naturelle de $\mathrm{Gal}(L/F)$ sur $\mathrm{Aut}_{k_F}(k_L)$. C'est un sous-groupe distingué de $\mathrm{Gal}(L/F)$.

Proposition 2.14. — *Soit L une extension finie de F telle que k_L/k_F soit séparable.*

(i) *Si L/F est galoisienne, alors k_L est une extension galoisienne de k_F.*

(ii) *Si L/K est non ramifiée, et si k_L/k_F est galoisienne, alors L/F est aussi galoisienne, et on a $\mathrm{Gal}(F(k)/F) \cong \mathrm{Gal}(k/k_F)$.*

(iii) *Si L/F est galoisienne, alors l'application naturelle $\mathrm{Gal}(L/F) \to \mathrm{Gal}(k_L/k_F)$ est surjective, et le corps fixé par le sous-groupe d'inertie $I_{L/F}$ est $F(k_L)$.*

Démonstration. — Si L/F est galoisienne et $\overline{\alpha} \in k_L$ est un élément primitif de k_L/k_k, soit $\overline{P} \in k_F[X]$ son polynôme minimal, $P \in \mathscr{O}_F[X]$ unitaire dont la réduction est $\overline{P}$ et $\alpha \in \mathscr{O}_{\overline{F}}$ se réduisant sur $\overline{\alpha}$. D'après la démonstration du th. 2.9, on a $\alpha \in F(k_L) \subset L$ et, comme L est

galoisienne, le polynôme P se décompose sur L sous la forme $P(X) = (X - \alpha_1)\dots(X - \alpha_f)$. D'autre part, P étant unitaire à coefficients entiers, ses racines sont des entiers et les réductions $\overline{\alpha}_i$ sont les racines de $\overline{P}$ qui se décompose sur k_L ce qui montre que k_L/k_F est normale donc galoisienne.

Réciproquement, si on suppose L/F non ramifiée et k_L/k_F galoisienne, alors $\overline{P}$ se décompose sur k_L sous la forme $\overline{P}(X) = (X - \overline{\alpha}_1)\dots(X - \overline{\alpha}_f)$ et P a une racine unique $\alpha_i \in F(k_L) = L$ se réduisant sur $\overline{\alpha}_i$. On en déduit le fait que P est scindé sur L et, comme $L = F(\alpha) = F(\alpha_1, \dots, \alpha_f)$, que L est une extension galoisienne de F. De plus, $\mathrm{Gal}(L/F)$ et $\mathrm{Gal}(k_L/k_F)$ sont en bijection naturelle avec les conjugués de $\overline{\alpha}$ et l'application naturelle de $\mathrm{Gal}(L/F)$ dans $\mathrm{Gal}(k_L/k_F)$ est une bijection.

Finalement, si L est une extension galoisienne de F, comme $\mathrm{Gal}(F(k_L)/F) \cong \mathrm{Gal}(k_L/k_F)$ est le quotient de $\mathrm{Gal}(L/F)$ par $I_{L/F}$, on a $\mathrm{Gal}(L/F(k_L)) = I_{L/F}$ et $F(k_L) = L^{I_{L/F}}$.

Proposition 2.15. — *Si L/F est une extension galoisienne telle que k_L/k_F est séparable, et si $I_{L/F}$ est le sous-groupe d'inertie de* $\mathrm{Gal}(L/F)$*, alors $I_{L/F}$ a un unique p-sous-groupe de Sylow $I^+_{L/F}$ qui est distingué dans $I_{L/F}$ et* $\mathrm{Gal}(L/F)$.

Démonstration. — Soit $K = L^{I_{L/F}}$. D'après la proposition 2.14, K est l'extension maximale non ramifiée de F contenue dans L et L/K est galoisienne totalement ramifiée de groupe de Galois $I_{L/F}$. Les p-sous-groupes de Sylow de $I_{L/F}$ correspondent donc, via la correspondance de Galois, aux extensions de K, contenues dans L et de degré premier à p, et comme il n'y a qu'une seule extension ayant ces propriétés d'après la prop. 2.12, le groupe $I_{L/F}$ n'a qu'un seul sous-groupe de Sylow que l'on notera $I^+_{L/F}$. Maintenant, si $g \in \mathrm{Gal}(L/F)$, alors $gI^+_{L/F}g^{-1}$ est un p-groupe contenu dans $I_{L/F}$ puisque $I_{L/F}$ est distingué dans $\mathrm{Gal}(L/F)$. Il est donc inclus dans $I^+_{L/F}$ puisque $I^+_{L/F}$ est l'unique p-Sylow de $I_{L/F}$. Ceci permet de conclure.

Définition 2.16. — Le p-Sylow $I^+_{L/F}$ de $I_{L/F}$ est *le sous-groupe d'inertie sauvage.*

2.7. Structure des extensions finies

Si on regroupe ce qui précède (propositions 2.12, 2.14 et 2.15 et théorème 2.9), on obtient le théorème suivant décrivant la structure des extensions finies d'un corps complet pour une valuation discrète.

Théorème 2.17. — *Si L est une extension finie de F telle que k_L/k_F soit séparable, alors L contient deux sous-extensions $L_0 \subset L_1$ de F qui sont uniquement déterminées par les propriétés suivantes.*

(i) *L_0/F est non ramifiée,*

(ii) *L_1/L_0 est totalement et modérément ramifiée,*

(iii) *L/L_1 est totalement ramifiée de degré une puissance de p.*

De plus, $L_0 = F(k_L)$, et il existe une uniformisante π de L_1 telle que $\pi^{[L_1:L_0]} \in L_0$. Finalement, si L/F est galoisienne, alors $L_0 = L^{I_{L/F}}$ et $L_1 = L^{I^+_{L/F}}$.

3. Théorie de la ramification supérieure

3.1. Groupes de ramification (en numérotation inférieure)

À partir de maintenant, F est un corps local de caractéristique 0 dont le corps résiduel k_F est parfait de caractéristique p. En particulier, toutes les extensions de k_F (et de F) sont séparables, et donc toutes les extensions finies de F peuvent se dévisser comme au théorème 2.17. De plus, si L est une telle extension, alors $\mathscr{O}_L$ est monogène sur $\mathscr{O}_F$ (proposition 2.8).

Si L est une extension finie de F, on note v_L la valuation de L normalisée par $v_L(L^*) = \mathbf{Z}$. On a donc $v_L(x) = e(L/F)v_F(x)$, si $x \in F$.

Lemme 3.1. — *Soit L une extension galoisienne finie de F de groupe de Galois G, et soit x un générateur de $\mathscr{O}_L$ en tant que $\mathscr{O}_F$-algèbre. Alors si $s \in G$, $v_L(s(x) - x) = \inf_{a \in \mathscr{O}_L} v_L(s(a) - a)$.*

Démonstration. — Si $a \in \mathscr{O}_L$, il existe $P \in \mathscr{O}_K[X]$ tel que l'on ait $a = P(x)$ et $s(a) - a = P(s(x)) - P(x)$ est divisible par $s(x) - x$, ce qui montre que $v_L(s(a) - a) \geqslant v_L(s(x) - x)$, ce qui permet de conclure.

Définition 3.2. — Si $s \in G$, on pose $i_L(s) = v_L(s(x) - x)$, ce qui ne dépend pas du choix de x d'après ce qui précède.

Exercice 10. — Montrer que si $i_L(s) > 0$, alors s fixe $K = L^{I_{L/F}}$ et $i_L(s) = v_L(s(\pi_L) - \pi_L)$ quelle que soit l'uniformisante π_L de L.

Lemme 3.3. — *Si s et t sont deux éléments de G, alors*
(i) $i_L(sts^{-1}) = i_L(t)$.
(ii) $i_L(st) \geqslant \inf(i_L(s), i_L(t))$ *avec égalité si* $i_L(s) \neq i_L(t)$.

Démonstration. — $i_L(sts^{-1}) = v_L(sts^{-1}(x) - x) = v_L(s(t(s^{-1}(x)) - s^{-1}(x))) = v_L(s^{-1}(x)) - s^{-1}(x)) = i_L(t)$ puisque $s^{-1}(x)$ est un générateur de $s^{-1}(\mathscr{O}_L) = \mathscr{O}_L$.
(ii) $i_L(st) = v_L(st(x) - x) = v_L(s(t(x) - x) + s(x) - x) \geqslant \inf(v_L(t(x) - x), v_L(s(x) - x))$ avec égalité si $v_L(t(x) - x) \neq v_L(s(x) - x)$.

Si $u \in [-1, +\infty[$, on pose $G_u = \{s \in G \mid i_L(s) \geqslant u + 1\}$

Proposition 3.4. — (i) *Si $u \in [-1, +\infty[$, G_u est un sous-groupe distingué de G.*
(ii) $G_{-1} = G$.
(iii) *Si $u \in]-1, 0]$, G_u est le sous-groupe d'inertie $I_{L/F}$ de G.*
(iv) *Si $u \in]0, 1]$, G_u le sous-groupe d'inertie sauvage $I^+_{L/F}$ de G.*
(v) $G_u = \{1\}$ *si u est assez grand.*

Démonstration. — Le (i) est une conséquence immédiate du lemme précédent, et le (ii) et le (v) sont des évidences.

(iii) Comme v_L ne prend que des valeurs entières, $G_u = G_0$ si $u \in]-1, 0]$. Par définition, le sous-groupe d'inertie est l'ensemble des $s \in G$ tels que l'on ait $v_L(s(a) - a) > 0$ quel que soit $a \in \mathscr{O}_L$. Mais $v_L(y) > 0$ est équivalent à $v_L(y) \geqslant 1$, ce qui montre que le sous-groupe d'inertie n'est autre que G_0.

(iv) On a de même $G_u = G_1$ si $u \in]0, 1]$. Soit π_L une uniformisante de L. Par définition, $s \in G_1$ si et seulement si $s \in G_0$ et s agit trivialement sur $\pi_L\mathscr{O}_L/\pi_L^2\mathscr{O}_L$. Soit $\eta : G_0 \to k_L^*$ défini par

$\eta(s) = \frac{s(\pi_L)}{\pi_L} \bmod \pi_L$. Comme $s(u) \equiv u \bmod \pi_L$, si $s \in G_0$ et $u \in \mathscr{O}_L^*$, on voit que η ne dépend pas du choix de π_L. De plus, on a $\eta(st) = s\big(\frac{t(\pi_L)}{\pi_L}\big)\frac{s(\pi_L)}{\pi_L} = \eta(s)\eta(t)$ puisque s agit trivialement sur k_L^*. Ceci fait de η un caractère de G_0 dont le noyau est G_1. En particulier, G_0/G_1 s'identifie à un sous-groupe (fini) du groupe des racines de l'unité de k_L^*. Cela implique que G_0/G_1 est cyclique, et comme k_L est de caractéristique p, cela implique que G_0/G_1 est d'ordre premier à p, et donc que G_1 contient le p-Sylow $I_{L/F}^+$ de G_0.

Soit $p^r e$ le cardinal de G_0, avec $(p, e) = 1$. Soient $K_0 = L^{I_{L/F}}$ et $K = L^{I_{L/F}^+}$, ce qui fait de K une extension totalement et modérément ramifiée de K_0. D'après le théorème de structure des extensions modérément ramifiées, il existe π_K uniformisante de K telle que π_K^e soit une uniformisante de K_0 ; en particulier $\frac{s(\pi_K)}{\pi_K}$ est une racine de l'unité d'ordre e, si $s \in G_0$. Par ailleurs, il existe $u \in \mathscr{O}_L^*$ tel que $\pi_K = u\pi_L^{p^r}$. On a donc $\frac{s(\pi_K)}{\pi_K} \equiv \big(\frac{s(\pi_L)}{\pi_L}\big)^{p^r} \bmod \pi_L$. Comme $\frac{s(\pi_K)}{\pi_K}$ est une racine de l'unité d'ordre premier à p, on en déduit les équivalences

$$s \in I_{L/F}^+ \Leftrightarrow \frac{s(\pi_K)}{\pi_K} = 1 \Leftrightarrow \big(\frac{s(\pi_L)}{\pi_L}\big)^{p^r} = 1 \Leftrightarrow \frac{s(\pi_L)}{\pi_L} = 1 \Leftrightarrow \eta(s) = 1 \Leftrightarrow s \in G_1,$$

ce qui termine la démonstration de la proposition.

Définition 3.5. — Les sous-groupes G_u pour $u \in [-1, +\infty[$ s'appellent les *sous-groupes de ramification* de G. Ils forment une filtration décroissante de G par des sous-groupes distingués.

Remarque 3.6. — Si K est un sous-corps de L contenant F et x est un générateur de $\mathscr{O}_L$ sur $\mathscr{O}_F$, alors c'est a fortiori un générateur de $\mathscr{O}_L$ sur $\mathscr{O}_K$. On en déduit le fait que si H est le sous-groupe de G fixant K et $u \in [-1, +\infty[$, alors $H_u = H \cap G_u$.

3.2. Numérotation supérieure des groupes de ramification. — La remarque précédente montre que la numérotation inférieure est bien adaptée pour l'inclusion (i.e. si l'on change le corps F). On peut se demander ce qui se passe par passage au quotient (i.e. si on remplace L par un sous-corps K galoisien sur F). Nous verrons que si H est un sous-groupe distingué de G, les sous-groupes de ramifications de G/H sont les images de ceux de G, mais avec une numérotation différente (théorème 3.10).

Proposition 3.7. — *Soit H un sous-groupe distingué de G, et soit K le sous-corps de L fixe par H. Alors, si $\sigma \in G/H$, on a $i_K(\sigma) = \frac{1}{e(L/K)} \sum_{s \to \sigma} i_L(s)$.*

Démonstration. — Si $\sigma = 1$ les deux membres valent $+\infty$. Supposons donc $\sigma \neq 1$. Soit x (resp. y) un générateur de $\mathscr{O}_L$ (resp. $\mathscr{O}_K$) comme $\mathscr{O}_F$-algèbre. Il s'agit de montrer que les deux éléments $a = y - \sigma(y)$ et $b = \prod_{s \to \sigma}(x - s(x))$ ont la même valuation, ou encore qu'ils définissent le même idéal de $\mathscr{O}_L$.

Soit P le polynôme minimal de x sur $\mathscr{O}_K$. On a $P(X) = \prod_{h \in H}(X - h(x))$. Si s_0 est un élément de G ayant pour image σ dans G/H, les autres sont de la forme $s_0 h$, où h décrit H. Le polynôme $P - s(P)$ a tous ses coefficients divisibles par $y - s_0(y) = a$; on en déduit le fait, en l'évaluant en x, que a divise b (on a $P(x) = 0$ et $s_0(P)(x) = b$).

Réciproquement, soit $Q \in \mathscr{O}_F[X]$ tel que l'on ait $y = Q(x)$. Le polynôme $Q(X) - \sigma(y)$ s'annule pour $X = s_0 h(x)$ si $h \in H$ car $Q(s_0 h(x)) = s_0 h(Q(x))) = s_0 h(y) = \sigma(y)$; il est donc divisible

dans $K[X]$ et dans $\mathcal{O}_K[X]$ (lemme de Gauss) par le polynôme $\prod_{h\in H}(X - s_0h(x))$. Évaluer le résultat en $X = x$ montre que b divise a.

Soit $\varphi_{L/F}$ la fonction de $[-1, +\infty[$ dans lui-même, définie par $\varphi_{L/F}(u) = \int_0^u \frac{dt}{[G_0:G_t]}$, avec la convention $[G_0 : G_t] = [G_t : G_0]^{-1}$ si $t < 0$. Cette fonction interviendra dans la renumérotation des groupes de ramification à laquelle il a été fait allusion plus haut.

Lemme 3.8. — $\varphi_{L/F}(u) + 1 = \frac{1}{e(L/F)} \sum_{s\in G} \inf(i_L(s), u + 1)$.

Démonstration. — Remarquons que les deux membres sont des fonctions continues de u affines par morceaux et coïncidant pour $u = 0$ puisque $i_L(s) \geqslant 1$ si et seulement si s est dans le sous-groupe d'inertie de G. Si u n'est pas un entier, la dérivée du membre de droite en u est égale au nombre d'éléments de G vérifiant $i_L(g) \geqslant u + 1$ divisé par $e(L/F)$, c'est-à-dire au nombre d'éléments de G_u divisé par le cardinal de G_0, autrement dit à $\frac{1}{[G_0:G_u]}$, ce qui est aussi la dérivée de $\varphi_{L/F}(u)$ en u. Ceci permet de conclure.

Corollaire 3.9. — *Si H est un sous-groupe de G, et si $K = L^H$, alors* $\varphi_{L/K}(u) + 1 = \frac{1}{e(L/K)} \sum_{s\in H} \inf(i_L(s), u + 1)$.

Démonstration. — Il suffit d'appliquer le lemme précédent à l'extension galoisienne L/K.

Théorème 3.10. — (Herbrand)
(i) $G_uH/H = (G/H)_v$ *avec* $v = \varphi_{L/K}(u)$.
(ii) $\varphi_{L/F} = \varphi_{K/F} \circ \varphi_{L/K}$.

Démonstration. — $\sigma \in G_uH/H$ si et seulement si il existe $s \in G_uH$ tel que $i_L(s) \geqslant u + 1$. Soit $j(\sigma) = \sup_{s\to\sigma} i_L(s)$ et soit s_0 réalisant le maximum.

D'après la proposition 3.7, on a $i_K(\sigma) = \frac{1}{e(L/K)} \sum_{h\in H} i_L(s_0h)$. D'autre part, par définition de $j(\sigma)$, on a $i_L(s_0h) \leqslant j(\sigma) = i_L(s_0)$ et, d'après le lemme 3.3, on a $i_L(s_0h) \geqslant \inf(i_L(s_0), i_L(h))$, avec égalité si $i_L(s_0) \neq i_L(h)$. On en déduit la formule $i_L(s_0h) = \inf(i_L(h), j(\sigma))$ quel que soit $h \in H$. On peut donc utiliser le corollaire 3.9 et on obtient $i_K(\sigma) = \varphi_{L/K}(j(\sigma) - 1) + 1$. On en tire les équivalences

$$\begin{aligned}\sigma \in G_uH/H \Leftrightarrow j(\sigma) - 1 \geqslant u &\Leftrightarrow \varphi_{L/K}(j(\sigma) - 1) \geqslant \varphi_{L/K}(u) \quad (\varphi_{L/K} \text{ croissante})\\ &\Leftrightarrow i_K(\sigma) - 1 \geqslant \varphi_{L/K}(u) \quad \text{d'après ce qui précède}\\ &\Leftrightarrow \sigma \in (G/H)_{\varphi_{L/K}(u)}.\end{aligned}$$

Ceci termine la démonstration du i). Pour démontrer le ii) remarquons que les fonctions $\varphi_{L/F}$ et $\varphi_{K/F} \circ \varphi_{L/K}$ sont continues, affines par morceaux et coïncident en $u = 0$. D'autre part, si u n'est pas un entier, la dérivée de $\varphi_{K/F} \circ \varphi_{L/K}$ en u est égale à $\varphi'_{K/F}(v)\varphi'_{L/K}(u)$, avec $v = \varphi_{K/F}(u)$ c'est à dire à

$$\frac{|(G/H)_v|}{e(K/F)} \frac{|H_u|}{e(L/K)} = \frac{|G_uH/H|}{e(K/F)} \frac{|H_u|}{e(L/K)} = \frac{|G_u|}{e(L/F)}$$

ce qui n'est autre que la dérivée de $\varphi_{L/F}$ en u. (La formule $|G_uH/H||H_u| = |G_u|$ vient de ce que $H_u = G_u \cap H$ et que l'on a la suite exacte $1 \to H_u \to G_u \to G_uH/H \to 1$.)

Définition 3.11. — Soit $\psi_{L/F}$ la fonction de $[-1,+\infty[$ dans $[-1,+\infty[$ réciproque de $\varphi_{L/F}$. On définit la numérotation supérieure des groupes de ramification en posant $G^v = G_{\psi_{L/F}(v)}$, ou, ce qui revient au même, $G_u = G^{\varphi_{L/F}(u)}$.

Proposition 3.12. — (i) $G^{-1} = G_{-1} = G$

(ii) *Si* $u \in]-1,0]$, $G^u = G_u$ *est le sous-groupe d'inertie de* G.

(iii) *Si* $u > 0$, *alors* G^u *est inclus dans le sous-groupe d'inertie sauvage de* G *et ce dernier est la réunion des* G^u *pour* $u > 0$.

Démonstration. — C'est une traduction de la proposition 3.4.

Exercice 11. — Montrer que $\psi_{L/F}(v) = \int_0^v [G^0 : G^t]dt$.

Proposition 3.13. — (i) $\psi_{L/F} = \psi_{L/K} \circ \psi_{K/F}$.

(ii) $(G/H)^v = G^v H/H$.

Démonstration. — Le (i) est une conséquence immédiate du (ii) du théorème d'Herbrand et du fait que $\psi_{L/F}$ est l'inverse de $\varphi_{L/F}$.

D'autre part, si $K = L^H$, on a par définition $(G/H)^v = (G/H)_x$, avec $x = \psi_{K/F}(v)$. Grâce au (i) du théorème d'Herbrand, $(G/H)_x = G_w H/H$, avec $w = \psi_{L/K}(x) = \psi_{L/F}(v)$, et donc $G_w = G^v$, ce qui permet de conclure.

Remarque 3.14. — Le (ii) de la proposition précédente montre que la numérotation supérieure passe au quotient.

3.3. La différente

Si K est un corps local, et si π_K est une uniformisante de K, un *idéal fractionnaire* $\mathfrak{a}$ de K est de la forme $\pi_K^n \mathscr{O}_K$, où $n \in \mathbf{Z}$ est uniquement déterminé par $\mathfrak{a}$. On pose $v_K(\mathfrak{a}) = n$, si $\mathfrak{a} = \pi_K^n \mathscr{O}_K$. Si $v_K(\mathfrak{a}) = n$, l'idéal $\mathfrak{a}^{-1}$ inverse de $\mathfrak{a}$ vérifie $v_K(\mathfrak{a}^{-1}) = -n$

Si L est une extension finie de F, et si $\mathfrak{a}$ est un idéal fractionnaire de L, soit $\mathfrak{a}^\vee$ le dual de $\mathfrak{a}$ pour la forme bilinéaire $(x,y) \mapsto \mathrm{Tr}_{L/F}(xy)$. Autrement dit $\mathfrak{a}^\vee = \{y \in L \mid \mathrm{Tr}_{L/F}(xy) \in \mathscr{O}_F,\ \forall x \in \mathfrak{a}\}$.

Lemme 3.15. — (i) $\mathfrak{a}^\vee$ *est un idéal fractionnaire de* L.

(ii) *La différente* $\mathfrak{d}_{L/F}$ *de l'extension* L/F, *inverse de* $\mathscr{O}_L^\vee$ *est un idéal de* $\mathscr{O}_K$.

(iii) $\mathfrak{a}^\vee = \mathfrak{a}^{-1}\mathfrak{d}_{L/F}^{-1}$.

(iv) *Si* $\mathfrak{a}$ *(resp.* $\mathfrak{b}$*) est un idéal fractionnaire de* L *(resp* F*), alors* $\mathrm{Tr}_{L/F}(\mathfrak{a}) \subset \mathfrak{b}$ *si et seulement si* $\mathfrak{a} \subset \mathfrak{b}\mathfrak{d}_{L/F}^{-1}$.

(v) *Si* $\mathfrak{a}$ *est un idéal fractionnaire de* L, *alors* $v_F(\mathrm{Tr}_{L/F}(\mathfrak{a})) = [\frac{v_L(\mathfrak{a}\mathfrak{d}_{L/F})}{e(L/F)}]$.

Démonstration. — Le (i) est évident. Le (ii) suit de ce que $\mathscr{O}_L^\vee$ contient $\mathscr{O}_L$ et donc que son inverse est contenu dans $\mathscr{O}_L$. Le (iii) suit du fait que $\mathfrak{a}\mathfrak{a}^{-1} = \mathscr{O}_L$ et le (iv) est immédiat. Finalement, compte-tenu du (iv), on a

$$\mathrm{Tr}_{L/F}(\mathfrak{a}) \subset \pi_F^b \mathscr{O}_F \Leftrightarrow \mathfrak{a} \subset \pi_F^b \mathfrak{d}_{L/F}^{-1} \Leftrightarrow e(L/F)b \leqslant v_L(\mathfrak{a}\mathfrak{d}_{L/F}) \Leftrightarrow b \leqslant [\frac{v_L(\mathfrak{a}\mathfrak{d}_{L/F})}{e(L/F)}],$$

la dernière équivalence venant de ce que $b \in \mathbf{Z}$.

Proposition 3.16. — *Si $e_1,\dots,e_d$ est une base de $\mathscr{O}_L$ sur $\mathscr{O}_F$, et si $e_1^*,\dots,e_d^*$ est la base de L sur F, duale de $e_1,\dots,e_d$ pour la forme bilinéaire $(x,y)\mapsto \mathrm{Tr}_{L/F}(xy)$, alors les coordonnées $x_1,\dots,x_d$ de $x\in L$ dans la base $e_1^*,\dots,e_d^*$, vérifient l'encadrement*

$$\inf_{1\leqslant i\leqslant d} v_L(x_i)\geqslant v_L(x)\geqslant \inf_{1\leqslant i\leqslant d} v_L(x_i)-v_L(\mathfrak{d}_{L/F}).$$

Démonstration. — Par définition de la différente, $e_1^*,\dots,e_d^*$ est une base de $\mathfrak{d}_{L/F}^{-1}$ sur $\mathscr{O}_F$; on en déduit la seconde inégalité. La première vient de ce que l'on a $x=\sum_{i=1}^d \mathrm{Tr}_{L/F}(e_ix)e_i^*$, et donc que $x_i=\mathrm{Tr}_{L/F}(e_ix)$, et $e_i\in\mathscr{O}_F$.

Proposition 3.17. — (Transitivité de la différente) *Si K (resp. L) est une extension finie de F (resp. K), alors $\mathfrak{d}_{L/F}=\mathfrak{d}_{L/K}\mathfrak{d}_{K/F}$.*

Démonstration. — Une utilisation répétée du (iv) du lemme 3.15 nous fournit les équivalence suivantes $x\in\mathfrak{d}_{L/F}^{-1}\Leftrightarrow \mathrm{Tr}_{L/F}(x\mathscr{O}_L)=\mathrm{Tr}_{K/F}(\mathrm{Tr}_{L/K}(x\mathscr{O}_L))\subset\mathscr{O}_F\Leftrightarrow\mathrm{Tr}_{L/K}(x\mathscr{O}_L))\subset\mathfrak{d}_{K/F}^{-1}$ $\Leftrightarrow x\mathscr{O}_L\subset\mathfrak{d}_{L/K}^{-1}\mathfrak{d}_{K/F}^{-1}$. On en déduit le résultat.

Proposition 3.18. — *Soit x un générateur de $\mathscr{O}_L$ comme $\mathscr{O}_F$-algèbre et soit $P\in F[X]$ le polynôme minimal de x sur F. Alors*

(i) $P\in\mathscr{O}_F[X]$

(ii) $\mathfrak{d}_{L/F}$ *est l'idéal de $\mathscr{O}_L$ engendré par $P'(x)$; autremant dit, $v_L(\mathfrak{d}_{L/F})=v_L(P'(x))$.*

Démonstration. — Posons $P(X)=X^n+a_{n-1}X^{n-1}+\cdots+a_0$. On a $v(a_0)=v(\mathrm{N}_{L/F}(x))=nv(x)\geqslant 0$, et comme P est irréductible, la théorie des polygônes de Newton montre que $v(a_i)\geqslant 0$ si $1\leqslant i\leqslant n-1$, ce qui prouve le (i)

(ii) Soient $x_1,\dots,x_n$ les racines de P dans $\overline{F}$. La décomposition en éléments simples de $\frac{1}{P(X)}$ dans $\overline{F}(X)$ est

$$\frac{1}{P(X)}=\sum_{i=1}^n\frac{1}{P'(x_i)(X-x_i)}$$

comme on le constate en multipliant les deux membres par $X-x_i$ et en évaluant le résultat en $X=x_i$. Développant les deux membres en séries entières de $\frac{1}{X}$, on obtient

$$\frac{1}{X^n}\Big(\frac{1}{1+\frac{a_{n-1}}{X}+\cdots+\frac{a_0}{X^n}}\Big)=\sum_{k=1}^{+\infty}\frac{1}{X^k}\sum_{i=1}^n\frac{x_i^{k-1}}{P'(x_i)}=\sum_{k=1}^{+\infty}\frac{1}{X^k}\mathrm{Tr}_{L/F}\Big(\frac{x^{k-1}}{P'(x)}\Big),$$

ce qui permet d'obtenir les formules

$$\mathrm{Tr}_{L/F}\Big(\frac{x^k}{P'(x)}\Big)=0,\ \text{si } k\leqslant n-2\quad\text{et}\quad\mathrm{Tr}_{L/F}\Big(\frac{x^{n-1}}{P'(x)}\Big)=1.$$

Utilisant le fait que les a_j sont des éléments de $\mathscr{O}_F$, et développant brutalement le terme de gauche de l'identité ci-dessus, on obtient $\mathrm{Tr}_{L/F}\big(\frac{x^k}{P'(x)}\big)\in\mathscr{O}_F$ quel que soit $k\in\mathbf{N}$. On en déduit l'inclusion $P'(x)^{-1}\mathscr{O}_L\subset\mathfrak{d}_{L/F}^{-1}$.

Réciproquement, les $\frac{x^i}{P'(x)}$ pour $0 \leqslant i \leqslant n-1$ forment une base de L sur F et si $y = \sum_{i=0}^{n-1} b_i \frac{x^i}{P'(x)} \in \mathfrak{d}_{L/F}^{-1}$, où les b_i sont des éléments de F, alors

$$\mathrm{Tr}_{L/F}(x^j y) = b_{n-j-1} + \sum_{k=1}^{j} b_{n-k} \mathrm{Tr}_{L/K}\Big(\frac{x^{n-k+j}}{P'(x)}\Big) \in \mathscr{O}_F,$$

ce qui permet de démontrer que $b_{n-j} \in \mathscr{O}_F$ par récurrence sur j, et donc que $\mathfrak{d}_{L/F}^{-1} \subset P'(x)^{-1}\mathscr{O}_L$, ce qui termine la démonstration.

Corollaire 3.19. — *Si L/F est une extension galoisienne, alors*

$$v_L(\mathfrak{d}_{L/F}) = \sum_{s \in G-\{1\}} i_L(s) = \int_{-1}^{+\infty} (|G_t| - 1)dt.$$

Démonstration. — D'après ce qui précède, si x est un générateur de $\mathscr{O}_L$ comme $\mathscr{O}_F$-algèbre, alors $v_L(\mathfrak{d}_{L/F}) = v_L(P'(x)) = v_L(\prod_{s\neq 1}(x - s(x))) = \sum_{s\neq 1} i_L(s)$, ce qui démontre la première des deux égalités. Pour démontrer la seconde, on peut faire une intégration par partie. La fonction $t \mapsto |G_t| - 1$ est constante, égale à $|G_{i+1}| - 1$, sur tout intervalle de la forme $]i, i+1]$; sa dérivée est donc $\sum_{i=-1}^{+\infty}(|G_{i+1}| - |G_i|)\delta_i$, où δ_i est la masse de Dirac en i. On obtient donc

$$\int_{-1}^{+\infty} (|G_t| - 1)dt = -\int_{-1}^{+\infty} (t+1) \sum_{i=-1}^{+\infty} (|G_{i+1}| - |G_i|)\delta_i = \sum_{i=-1}^{+\infty} (|G_{i+1}| - |G_i|)(i+1),$$

et le résultat suit de ce que l'on a $i_L(s) = i + 1$ si $s \in G_i - G_{i+1}$.

Exercice 12. — Soit $K = L^{G_0}$ l'extension maximale non ramifiée de F contenue dans L, soit π_L une uniformisante de L, soit $Q \in K[X]$ le polynôme minimal de π_L sur K, et soit $P(X) = X^{-1}Q(X+\pi_L) \in L[X]$. Montrer que l'on a $\mathrm{Newt}_P(x) + \varphi_{L/F}(x) = v_F(\mathfrak{d}_{L/F})$ si $x \in [0, [L:K]-1]$ (où l'on a utilisé la valuation $v_F = \frac{1}{e(L/F)} v_L$ pour normaliser le polygone de Newton de P).

Lemme 3.20. — *Soient $L \subset M$ deux extensions galoisiennes de F et $w \in [-1, +\infty[$, alors $M^{\mathrm{Gal}(M/F)^w} \cap L = L^{\mathrm{Gal}(L/F)^w}$.*

Démonstration. — Soient $G = \mathrm{Gal}(M/F)$ et $H = \mathrm{Gal}(M/L)$. Alors $M^{G^w} \cap L$ est le sous-corps de L fixé par $G^w H$ et donc aussi le sous-corps de L fixé par $G^w H/H$, et comme on a $G^w H/H = (G/H)^w$ d'après la proposition 3.13, cela permet de conclure.

Corollaire 3.21. — *Si K est une extension finie de F (pas nécessairement galoisienne) et $w \in [-1, +\infty[$, le corps $L^{\mathrm{Gal}(L/F)^w} \cap K$ ne dépend pas de l'extension galoisienne L de F contenant K. Il sera noté $K^{[w]}$.*

Proposition 3.22. — $v_F(\mathfrak{d}_{K/F}) = \int_{-1}^{+\infty} \Big(1 - \frac{1}{[K:K^{[w]}]}\Big) dw$.

Démonstration. — Soit L une extension finie de K galoisienne sur F. On note $G = \mathrm{Gal}(L/F)$ et H le sous-groupe de G fixant K. D'après la formule de transitivité pour les différentes et le corollaire précédent, on a

$$v_F(\mathfrak{d}_{K/F}) = v_F(\mathfrak{d}_{L/F}) - v_F(\mathfrak{d}_{L/K}) = \frac{1}{e(L/F)} \int_{-1}^{+\infty} (|G_t| - |H_t|)dt.$$

Effectuons alors le changement de variable $t = \psi_{L/F}(w)$. On a $G_t = G^w$, $H_t = G_t \cap H = G^w \cap H$ et $\psi'_{L/F}(w) = \frac{e(L/F)}{|G^w|}$, ce qui nous donne la formule $v_F(\mathfrak{d}_{K/F}) = \int_{-1}^{+\infty}\Big(1 - \frac{|G^w \cap H|}{|G^w|}\Big)$

Pour conclure, remarquons que $K^{[w]}$ est le sous-corps de L fixé par $G^w H$ (qui est un groupe de cardinal $\frac{|G^w||H|}{|G^w \cap H|}$ car G^w est distingué dans G) et donc $[K : K^{[w]}] = \frac{|G^w||H|}{|G^w \cap H|}\frac{1}{|H|} = \frac{|G^w|}{|G^w \cap H|}$.

Corollaire 3.23. — *L'extension K/F est non ramifiée si et seulement si $\mathfrak{d}_{K/F} = \mathscr{O}_K$.*

Démonstration. — D'après la formule ci-dessus, $v_F(\mathfrak{d}_{K/F}) = 0$ si et seulement si $K = K^{[w]}$ quel que soit $w > -1$. Comme $w \to K^{[w]}$ est croissante, on voit que $v_F(\mathfrak{d}_{K/F}) = 0$ si et seulement si $K = K^{[0]}$. On conclut en remarquant que $K^{[0]}$ est l'extension maximale non ramifiée de F contenue dans K puisque, si L est une extension galoisienne finie de F contenant K, le groupe $\mathrm{Gal}(L/F)^0$ est le sous-groupe d'inertie de $\mathrm{Gal}(L/F)$.

Exercice 13. — Soit $a \in \mathbf{Z}_p$, tel que a ne soit pas une puissance p-ième dans $\mathbf{Q}_p$.

(i) Montrer que $L = \mathbf{Q}_p(\boldsymbol{\mu}_p, a^{1/p})$ est une extension galoisienne de $\mathbf{Q}_p$, et déterminer son groupe de Galois.

(ii) Déterminer, selon les valeurs de a, les sous-groupes de ramification, le conducteur et la différente de L sur $\mathbf{Q}_p$.

3.4. Conducteur d'une extension

D'après la proposition 3.13, la numérotation supérieure des groupes de ramification passe au quotient. On peut donc l'étendre à une extension galoisienne infinie en définissant $\mathrm{Gal}(L/F)^v$ comme le sous-groupe des éléments de $\mathrm{Gal}(L/F)$ dont l'image dans $\mathrm{Gal}(K/F)$ est dans $\mathrm{Gal}(K/F)^v$, quelle que soit la sous-extension galoisienne finie K de L.

On peut en particulier prendre pour L une clôture algébrique $\overline{F}$ de F, et définir les sous-groupes G_F^w de G_F. En particulier, $\mathrm{G}_F^{-1} = \mathrm{G}_F$; le sous-groupe d'inertie I_F de G_F est égal G_F^w pour tout $w \in]-1, 0]$ et le sous-groupe d'inertie sauvage de G_F est la réunion des G_F^w, avec $w > 0$.

Si $w \geqslant 0$, on note $\overline{F}^{(w)}$ l'intersection des $\overline{F}^{\mathrm{G}_F^t}$, pour $t > w-1$. Si $L \subset \overline{F}$ est une extension de F, et si $w \geqslant 0$, on note $L^{(w)}$ le sous-corps $L \cap \overline{F}^{(w)}$ de L, et on définit le *conducteur* $c(L/F) \in [0, +\infty]$ de L comme la borne inférieure de l'ensemble des w tels que $L^{(w)} = L$. Si L est une extension finie de F, et si $w - 1$ n'est pas *un saut de la filtration* (i.e. si $L^{[w-1-\varepsilon]} = L^{[w-1+\varepsilon]}$ quel que soit $\varepsilon > 0$), le corps $L^{(w)}$ coïncide avec le corps $L^{[w-1]}$ défini au cor. 3.21.

Remarque 3.24. — D'après la prop. 3.22, le conducteur est relié à la valuation de la différente par la formule

$$v_F(\mathfrak{d}_{L/F}) = \int_{-1}^{+\infty}\Big(1 - \frac{1}{[L : L^{[w]}]}\Big)dw = \int_0^{c(L/F)}\Big(1 - \frac{1}{[L : L^{(w)}]}\Big)dw.$$

On en déduit l'encadrement

$$\frac{1}{2}c(L/F) \leqslant v_F(\mathfrak{d}_{L/F}) \leqslant c(L/F).$$

Lemme 3.25. — (i) *$c(L/F) = 0$ si et seulement si L est une extension non ramifiée de F ;*

(ii) *$c(L/F) = 1$ si et seulement si L est une extension modérément ramifiée de F ;*

(iii) *$c(L_1L_2/F) = \sup(c(L_1/F), c(L_2/F))$, si L_1 et L_2 sont deux extensions de F.*

Démonstration. — Les deux premiers points sont de simples traductions de la prop. 3.12, et l'inégalité $c(L_1L_2/F) \geqslant \sup(c(L_1/F), c(L_2/F))$ est immédiate sur la définition du conducteur. Réciproquement, si $w = \sup(c(L_1/F), c(L_2/F))$, on a $L_1 \subset \overline{F}^{(w)}$ et $L_2 \subset \overline{F}^{(w)}$, et donc $L_1L_2 \subset \overline{F}^{(w)}$ et $c(L_1L_2/F) \leqslant w$. Ceci permet de conclure.

Remarque 3.26. — On peut retraduire le (i) du lemme précédent en disant que $\overline{F}^{(w)}$ est l'extension maximale non-ramifiée F^{nr} de F si $w < 1$, et le (ii) en disant que $\overline{F}^{(1)}$ est l'extension maximale modérément ramifiée F^{mod} de F.

La démonstration du résultat suivant nous entrainerait un peu loin, mais nous en verrons un cas particulier plus loin.

Théorème 3.27. — (Hasse-Arf) *Si L/F est une extension abélienne, $c(L/F)$ est un entier.*

Remarque 3.28. — Jannsen et Wingberg ont donné en 1982 une description du groupe G_F dans le cas d'une extension finie F de $\mathbf{Q}_p$, $p \geqslant 3$. Le groupe G_F est topologiquement engendré par $[F : \mathbf{Q}_p] + 3$ éléments, et il y a deux relations dont une un peu désagréable à écrire... Le résultat est que ce groupe de dépend que de $[F : \mathbf{Q}_p]$, de $|k_F|$ et du nombre de racines de l'unité d'ordre une puissance de p dans F^{mod}. En particulier, connaître G_F en tant que groupe abstrait ne permet absolument pas de retrouver F. Par contraste, Mochizuki a montré en 1996, que G_F muni de sa filtration par les G_F^w permettait de retrouver F, ce qui montre que la filtration par les sous-groupes d'inertie est un invariant très fin.

L'exercice ci-dessous montre comment on peut retrouver k_F en ne connaissant que G_F^w pour $w \leqslant 0$ et $\cup_{w>0}\mathrm{G}_F^w$. La démonstration complète du théorème de Mochizuki utilise des techniques nettement plus sophistiquées de « théorie de Hodge p-adique » dont le chapitre suivant donnera un avant-goût.

Exercice 14. — Soit F une extension finie de $\mathbf{Q}_p$ de corps résiduel $\mathbf{F}_q$, et soit π une uniformisante de F. Les corps F^{nr} et F^{mod} sont des extensions galoisiennes de F. On note $G = \mathrm{Gal}(F^{\mathrm{mod}}/F)$, $H = \mathrm{Gal}(F^{\mathrm{mod}}/F^{\mathrm{nr}})$ et $\Gamma = \mathrm{Gal}(F^{\mathrm{nr}}/F)$. Le sous-groupe H de G est donc distingué et on a $\Gamma = G/H$.

(i) Montrer que le groupe $\mathrm{Gal}(\mathbf{F}_{q^n}/\mathbf{F}_q)$ est isomorphe à $\mathbf{Z}/n\mathbf{Z}$, avec $x \mapsto \sigma(x) = x^q$ comme générateur. En déduire que $\mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q)$ est isomorphe à $\widehat{\mathbf{Z}} = \prod_{\ell \text{ premier}} \mathbf{Z}_\ell$, et est topologiquement engendré par σ.

(ii) Montrer que Γ est isomorphe à $\widehat{\mathbf{Z}}$ et est topologiquement engendré par σ, où $\sigma(\zeta) = \zeta^q$ si ζ est une racine de l'unité d'ordre premier à p.

(iii) Montrer que F^{mod} est la réunion des $F^{\mathrm{nr}}(\pi^{1/n})$, pour n premier à p.

(iv) Montrer que $\tau \mapsto \frac{\tau(\pi^{1/n})}{\pi^{1/n}}$ est un isomorphisme de $\mathrm{Gal}(F^{\mathrm{nr}}(\pi^{1/n})/F^{\mathrm{nr}})$ sur $\boldsymbol{\mu}_n$, groupe des racines n-ièmes de l'unité dans F^{nr}. En déduire que H est abélien, isomorphe à $\prod_{\ell \neq p} \mathbf{Z}_\ell$.

(v) On choisit un relèvement $\tilde{\sigma}$ de σ dans G Montrer que l'on a $\tilde{\sigma}\tau\tilde{\sigma}^{-1} = \tau^q$, si $\tau \in H$.

(vi) Montrer que, si g est n'importe quel élément de G dont l'image dans Γ en est un générateur topologique, alors l'image de H par $\tau \mapsto g\tau g^{-1}\tau^{-1}$ est d'indice $q-1$ dans H.

(vii) On suppose maintenant que l'on sait juste que F est un corps local de caractéristique 0 de corps résiduel k_F fini, mais que l'on connait G_F comme groupe topologique abstrait muni de sa filtration par les G_F^w. Donner une recette permettant de retrouver k_F.

Pierre Colmez