D.E.A. de Mathématiques Pures
Epreuve du Module Théories galoisiennes par M. Matignon

Vendredi 21 mai 1999, 8h-12h, Salle 385

les documents sont autorisés.

Exercice 1. k désigne un corps algébriquement clos de caractéristique $p > 0$. Soit C une courbe projective lisse et irréductible sur k et $k(C)$ son corps de fonctions. On rappelle qu'il existe $f \in k(C) - k$ telle que l'extension $k(C)/k(f)$ soit séparable.

1. Montrer que le morphisme $f : C \to \mathbb{P}^1_k$ est ramifié en au plus un nombre fini de fibres.

2. On considère le morphisme $t : \mathbb{P}^1_k \to \mathbb{P}^1_k$ défini par $t(z) = z + z^{-p}$ où z est un paramètre de $\mathbb{P}^1_k$. Montrer que le morphisme t est non ramifié en dehors de la fibre $t = \infty$ et que dans la fibre $t^{-1}(\infty)$ il y a deux points de multiplicité respective p et 1.

3. En déduire qu'il existe un morphisme $C \to \mathbb{P}^1_k$ qui est étale en dehors de l'infini; ainsi toute courbe C/k est revêtement étale de la droite affine.

4. Que pouvez vous dire de la courbe C si ce morphisme est seulement modérément ramifié?

Exercice 2. Soit k une clôture algébrique de $\mathbb{F}_p$ et C/k une courbe algébrique projective lisse connexe. On suppose que le genre de C/k est $g > 1$. Soit σ un k-automorphisme de C/k ; on veut montrer qu'il existe $m > 0$ tel que $\sigma^m = \mathrm{Id}$.

1. Montrer qu'il existe un système d'équations homogènes à coefficients dans une extension finie $\mathbb{F}_q$ de $\mathbb{F}_p$ convenable

$$(*) \qquad 1 \leq i \leq t,\ F_i(X_0, ..., X_n) = 0$$

tel que C soit isomorphe à l'ensemble des solutions $V(C)$ du système dans $\mathbb{P}^n_k(k)$. On note $C_{\mathbb{F}_q}$ la courbe définie sur $\mathbb{F}_q$ par le système $(*)$. Montrer que pour un choix convenable de q l'automorphisme σ est un $\mathbb{F}_q$ automorphisme de $C_{\mathbb{F}_q}$ (remarquer que $C = C_{\mathbb{F}_q} \times_{\mathbb{F}_q} k$).

2. Un point $p := [x_0, ..., x_n] \in V(C) \subset \mathbb{P}^n_k(k)$ est dit rationnel sur F_{q^d} si les coordonnées sont dans F_{q^d}. On note $C(F_{q^d})$ l'ensemble des points rationnels sur F_{q^d}.

a) Montrer que le cardinal de $C(F_{q^d})$ est fini et que σ agit par permutation sur $C(F_{q^d})$.

b) Montrer qu'il existe d tel que le cardinal de $C(F_{q^d})$ soit $> 2g + 2$.

c) Conclure.

Exercice 3. En cours nous avons énoncé le théorème suivant:

Théorème. (Harbater) Soit C une courbe algébrique affine lisse et irréductible sur k . Soit $\overline{C}$, la complétion de C et g son genre. On note $P_1, ..., P_s$ les points de $\overline{C} - C$ et t_i un paramètre uniformisant en P_i . On a une suite exacte de groupes

$$0 \to \mathrm{H}^1(\overline{C}_{et}, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\alpha} \mathrm{H}^1(C_{et}, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\beta} \bigoplus_i \mathrm{H}^1(G_{k((t_i))}, \mathbb{Z}/p\mathbb{Z}) \to 0$$

(k est un corps algébriquement clos de caractéristique $p > 0$).

Nous en avons donné une preuve seulement dans le cas du genre 0 . Nous nous proposons de le montrer dans le cas général. Seule la surjectivité du dernier homomorphisme est à démontrer.

On note $k(C)$ le corps de fonctions de C/k , D le diviseur $P_1 + P_2 + ... + P_s$ et $L(nD)$ le k sous-espace vectoriel de $k(C)$ des fonctions f telle que $(f) + nD \geq 0$.

On note $Pol_{\,i}$ le k espace vectoriel $\dfrac{1}{t_i}k[\dfrac{1}{t_i}]$; il est gradué par la valuation v_i en P_i . Soit $V = \bigoplus_{1\leq i\leq s} Pol_{\,i}$; et V_n le sous-espace vectoriel des $(f_1, ..., f_s) \in V$ telles que $\forall i,\ v_i(f_i) + n \geq 0$.

Soit A l'algèbre des fonctions régulières sur C .

1. Construire une application k -linéaire $\Phi : A \to V$ qui à f associe ses partie polaires.

2. Déterminer le noyau de Φ

3. On note E le k -espace vectoriel quotient $\dfrac{V}{\Phi(A)}$; montrer que $\Phi(L(nD)) \subset V_n$ et que l'inclusion $V_n \subset V$ induit une injection $\iota : E_n := \dfrac{V_n}{\Phi(L(nD))} \to E$. En déduire que E est un k -espace vectoriel de dimension finie.

4. On note $F : k(C) \to k(C)$ l'application Frobenius $x \to x^p$; c'est une application p -linéaire.

i) Montrer que F induit une application p -linéaire de E dans E que l'on note encore F

ii) Soit $f \in E$ avec $\mathrm{F}(f) = f$ et $\alpha \in k$. En remarquant que $\alpha = \beta^p - \beta$ pour un $\beta \in k$ montrer qu'il existe $g \in E$ avec $\alpha f = \mathrm{F}(g) - g$.

iii) Soit $f \in E$ avec $\mathrm{F}^d(f) = 0$ pour un $d \in \mathbb{N}$; montrer qu'il existe $g \in E$ avec $f = \mathrm{F}(g) - g$.

iv) Soit $\wp$ l'application $\mathbb{F}_p$ -linéaire $\mathrm{F} - \mathrm{Id}$; montrer que $\wp(E) = E$. Conclure.

Exercice 4. On désigne par R un anneau de valuation discrte complet d'inégale caractéristique 2. Soit π une uniformisante de R , $k = R/(\pi)$ et v la valuation normalisée par $v(2) = 1$. On notera K le corps des fractions de R et K^{alg} une clôture algébrique de K munie de l'unique valuation prolongeant v .

I. On considère la série formelle:

$$f(Z) := -Z(1 + Z^3)^{-\frac{1}{3}} = -Z(1 - \frac{1}{3}Z^3 + ...) \in K[[Z]]$$

1) Montrer que $f(Z) \in R[[Z]]$ (on pourra montrer par récurrence sur n que le coefficient de Z^n est dans R).

2) Montrer qu'il existe un R -automorphisme σ d'ordre 2 de $R[[Z]]$ tel que $\sigma(Z) = f(Z)$

3) On note encore σ l'automorphisme du R -schéma $\mathrm{Spec}R[[Z]]$. Montrer que σ a exactement 4 points fixes de la forme $(Z - Z_i), 1 \leq i \leq 4$ où $Z_i \in K^{alg}$ et $v(Z_i) > 0$. Montrer que $v(Z_i - Z_j) = 1/3$ pour $i \neq j$ i.e. les 4 points sont équidistants.

4) Montrer que $R[[Z]]^\sigma = R[[T]]$ où $T := Z\sigma(Z)$. Montrer que les points $T(Z_i),\ 1 \leq i \leq 4$ sont équidistants.

II. Soit $\alpha \in R$ et $\mathcal{C}$ le R -schéma :

$$\mathcal{C} := \mathrm{Proj}\frac{R[X,Y,Z]}{(Y^2Z + \alpha XYZ + YZ^2 - X^3)}$$

1. Montrer que $\mathcal{C}$ est lisse sur R

2. Montrer que la courbe générique $E := \mathcal{C} \times_R K$ est une courbe elliptique d'équation affine $(2y + 1 + \alpha x)^2 = 4x^3 + (1 + \alpha x)^2$ où $x = X/Z,\ y = Y/Z$. On note τ l'involution elliptique; déterminer les coordonnées des 4 points fixes.

3. a) Montrer que τ se prolonge en un R -automorphisme de $\mathcal{C}$ que l'on note encore τ .

b) Soit $\tau(Y) := -\alpha X - Y - Z$, $U_1 := D^+{}_{(Z)}$ et $U_2 := D^+{}_{(Y\tau(Y))}$; montrer que $\mathcal{C} = U_1 \cup U_2$ et que les ouverts U_1 et U_2 sont stables par τ . On note A_i l'algèbre des fonctions régulières sur U_i . Les morphismes finis $\mathrm{Spec}U_i \to \mathrm{Spec}U_i/ < \tau > := \mathrm{Spec}A_i^{<\tau>}$ se recollent; on obtient ainsi le quotient $\mathcal{C}/ < \tau >$.

c) Montrer que l'injection $R[X,Z] \to \dfrac{R[X,Y,Z]}{(Y^2Z + \alpha XYZ + YZ^2 - X^3)}$ induit un morphisme $p : \mathcal{C} - V(X,Z) \to \mathbb{P}^1_R - \mathrm{Proj}R[X,Z] - V(Z)$ qui coincide avec $\mathrm{Spec}U_1 \to \mathrm{Spec}U_1/ < \tau >$. On admet que ce morphisme se prolonge en $p : \mathcal{C} \to \mathbb{P}^1_R$; ainsi p coincide avec le morphisme quotient $\mathcal{C} \to \mathcal{C}/ < \tau >$.

4. Montrer que le point $\infty := [X = 0, Y = 1, Z = 0]$ de la fibre spéciale $\mathcal{C}_s$ est l'unique point fixe de τ dans $\mathcal{C}_s$ et que son image est le point $[X = 1, Z = 0]$ de $(\mathrm{Proj}R[X,Z])_s$.

5. Soit $A := \hat{\mathcal{O}}_{\mathcal{C},\infty}$ l'anneau local complété de $\mathcal{C}$ au point ∞ . Montrer que $A \simeq R[[Z]]$ (on ne demande pas de trouver Z) et que τ induit un R -automorphisme d'ordre 2 de A .

6. Montrer que $A^{<\tau>} \simeq R[[\dfrac{Z}{X}]]$ où $T := \dfrac{Z}{X}$ est la coordonnée de l'ouvert affine $D^+{}_{(X)} \subset \mathrm{Proj}R[X,Z]$.

7. Montrer que l'image par p des points fixes de τ satisfont l'équation $4T + (T^2 + \alpha T)^2 = 0$; montrer que ces points sont équidistants si et seulement si $v(\alpha) \geq 2/3$ (on examinera le polygône de Newton du polynôme $4T + (T^2 + \alpha T)^2$). En déduire que si $v(\alpha) < 2/3$ l'automorphisme τ n'est pas conjugué dans $\mathrm{Aut}_R R[[Z]]$ à l'automorphisme σ construit en I.

UNE PROMENADE EN THEORIE DE GALOIS
CHAPITRE I
Theorie de Galois des corps

Dans ce chapitre K designe un corps de caractéristique $p \geq 0$ et K^a une cloture algebrique de K. Nous nous proposons d'etudier plus particulierement les extensions abeliennes (finies ou infinies) de K. Nous allons d'abord regarder la theorie de Galois infinie; chemin faisant nous verrons apparaitre des groupes profinis et nous evoquerons leur cohomologie. La theorie des extensions p-cycliques dite theorie de Kummer (en caracteristique premiere a p) ou d'Artin Schreier (en caracteristique $p > 0$) nous amenera a etudier les schemas en groupes et les isogenies. Nous introduirons les schemas en anneaux de Witt, nous presentons l'application a la classification des corps locaux a corps residuel parfait et la theorie d'Artin-Schreier-Witt des extensions p^n-cycliques. Enfin la theorie des p-extensions est bien connue en caracteristique $p > 0$; elle est due pour l'essentiel a E. Witt, nous montrerons que le groupe de Galois de la p-extension maximale en caracteristique $p > 0$ a un groupe de Galois qui est pro p-groupe libre (eventuellement trivial).

A. Theorie de Galois infinie

Definition. Soit N une extension algebrique de (pas necessairement de degre fini) du corps K, on dit qu'elle est *galoisienne* sur K si

a) elle est algebrique et separable sur K i.e. tout element de N est racine simple d'un polynome a coefficients dans K

b) elle est normale sur K; i.e. tout polynome irreductible a coefficients dans K ayant une racine dans N se decompose en produit de polynomes de degre 1

Proposition. Un corps N est Galoisien sur K ssi c'est une reunion d'extensions Galoisiennes finies de K.

Preuve: evident

Definition. Si N est une extension galoisienne de K, alors *le groupe de Galois* $\mathrm{Gal}(N/K)$ est le groupe des automorphismes de N fixant les elements de K

Topologie du groupe de Galois

Soit N/K une extension galoisienne et $\Gamma := \mathrm{Gal}(N/K)$. On munit N de la topologie discrete, l'ensemble N^N de la topologie produit des topologies discretes des facteurs ("topologie de la convergence simple dans N ") et le groupe Γ de la topologie induite par celle de N^N .

Soit Λ l'ensemble des sous-extensions de N de degre fini sur K . Pour $\sigma \in \Gamma$ et $E \in \Lambda$, notons $U_E(\sigma)$ l'ensemble des $\tau \in \Gamma$ qui ont meme restriction que σ a E . Si $E = K(x_1, x_2, ..., x_n)$, l'ensemble $U_E(\sigma)$ se compose des elements $\tau \in \Gamma$ tels que $\tau(x_i) = \sigma(x_i),\ 1 \leq i \leq n$. Il en resulte que la famille $(U_E(\sigma))_{E\in\Lambda}$ est une base du filtre des voisinages de $\sigma \in \Gamma$.

Lorsque N est de degre fini sur K , on a $N \in \Lambda$ et $U_N(\sigma) = \{\sigma\}$, donc la topologie de Γ est discrete; d'ailleurs le groupe Γ est fini dans ce cas.

Il suit de cette description que l'homomorphisme de restriction
$\mathrm{Gal}(N/K) \to \mathrm{Gal}(L/K)$ est continu pour toute sous-extension $L \subset N$ galoisienne sur K .

Soit A , une partie de Γ . Dire que A est ouverte signifie que, pour tout $\sigma \in A$ il existe $E \in \Lambda$ tel que $U_E(\sigma) \subset A$. L'adherence $\overline{A}$ de A se compose des $\sigma \in \Gamma$ tels que tout $E \in \Lambda$, il existe $\tau \in A$ ayant meme restriction a E que σ ; le corps des invariants de $\overline{A}$ est celui de A .

Soit ϵ l'element neutre de Γ et Λ' l'ensemble des sous-extensions de N qui sont galoisiennes de degre fini sur K . Puisque toute extension finie est dominee par une extension galoisienne finie de K , il suit que l'ensemble Λ' est cofinal dans Γ . De plus pour $E \in \Lambda'$, l'ensemble $U_E(\epsilon)$ est le noyau de l'homomorphisme de restriction de Γ dans $\mathrm{Gal}(E/K)$; comme le groupe $\mathrm{Gal}(E/K)$ est fini, il en resulte que $U_E(\epsilon)$ est un sous-groupe ouvert et ferme, distingue et d'indice fini dans Γ .

On a $U_E(\sigma) = \sigma U_E(\epsilon) = U_E(\epsilon)\sigma$ pour tout $\sigma \in \Gamma$ et $E \in \Lambda'$. Comme $U_E(\epsilon)$ est un sous-groupe distingue de Γ pour tout $E \in \Lambda'$ et que la famille $(U_E(\epsilon))_{E\in\Lambda'}$ est une base de voisinages de ϵ , la topologie de Γ est compatible avec la structure de groupe, autrement dit l'application $(\sigma, \tau) \to \sigma\tau^{-1}$ de $\Gamma \times \Gamma$ dans Γ est continue.

Proposition. Soit N une extension galoisienne de K . Le groupe de Galois $\Gamma = \mathrm{Gal}(N/K)$ est compact et totalement discontinu.

Preuve: Tout element σ de Γ a une base de voisinages ouverts et fermes $U_E(\sigma)$, donc Γ est totalement discontinu. On a $\{\sigma\} = \cap_{E\in\Lambda} U_E(\sigma)$, donc Γ est separe. Pour tout $x \in N$ l'orbite sous Γ de x est finie; ainsi Γ s'injecte dans un compact de N^N ; il reste a montrer que Γ est ferme dans N^N . Si $u \in N^N$ est adherent a Γ , pour tout couple (x, y) de points de N il existe $\sigma \in \Gamma$ avec $u(x) = \sigma(x)$, $u(y) = \sigma(y)$, $u(x+y) = \sigma(x+y)$, $u(xy) = \sigma(xy)$; ainsi $u(x+y) = u(x) + u(y)$ et $u(xy) = u(x)u(y)$. Par le meme raisonnement on a $u(x) = x$ pour tout $x \in K$; donc u est un K -homomorphisme de N dans N et puisque N/K est algebrique $u \in \Gamma$.

Le systeme $E \in \Lambda'$ muni de la relation d'inclusion et des applications de restriction forment un systeme projectif $\varprojlim\ \mathrm{Gal}(E/K)$; soit λ_E l'homomorphisme de restriction de Γ dans $\mathrm{Gal}(E/K)$, il est continu et la famille $(\lambda_E), E \in \Lambda'$ definit un homomorphisme continu $\lambda : \Gamma \to \varprojlim\ \mathrm{Gal}(E/K)$.

Proposition. L'homomorphisme $\lambda : \Gamma \to \varprojlim \operatorname{Gal}(E/K)$ est un isomorphisme de groupes topologiques.

Preuve: Puisque Γ est compact, que λ est continu et que le groupe $\varprojlim \operatorname{Gal}(E/K)$ est separe il suffit de prouver que λ est bijectif. Soit $u = (u_{|E})_{E\in\Lambda'}$ un element de $\varprojlim \operatorname{Gal}(E/K)$; $u_{|E}$ est un K-automorphisme de E et pour $E' \subset E$, $u_{|E'}$ est la restriction de $u_{|E}$ a E' . Puisque $N = \cup_{E\in\Lambda'} E$ il existe un unique $\sigma \in \Gamma$ qui coincide avec $u_{|E}$ sur E ; alors σ est l'unique element de Γ tel que $\lambda(\sigma) = u$. ///

Ainsi γ est limite projective de groupe finis; un tel groupe est appele groupe topologique profini.

Theoreme. Soit N une extension Galoisienne de K de groupe de Galois Γ . Il y a une correspondance bijective entre les sous-corps de N contenant K et les sous-groupes fermes de Γ . Plus precisement:

a) Pour un sous corps E de N contenant K , $H := \operatorname{Gal}(N/E)$ est un sous groupe ferme de Γ et $E = N^H$

b) Si H est un sous-groupe de Γ , alors $\operatorname{Gal}(N/N^H)$ est la fermeture de H dans Γ

de plus, les sous-groupes fermes distingues de Γ correspondent aux extensions Galoisiennes de K , et les sous-groupes ouverts correspondent aux extensions finies.

Preuve: exercice

Exemples.

a) On munit $\mathbb{Z}$ de la topologie pour laquelle les sous-groupes d'indice finis forment un systeme fondamental de voisinages; soit $\hat{\mathbb{Z}}$ la completion de $\mathbb{Z}$. Pour ℓ premier on note $\mathbb{Z}_\ell = \varprojlim \mathbb{Z}/\ell^n\mathbb{Z}$. Alors $\hat{\mathbb{Z}} = \prod_{\ell \text{ } premier} \mathbb{Z}_\ell$; et $\hat{\mathbb{Z}}/m\hat{\mathbb{Z}} = \mathbb{Z}/m\mathbb{Z}$ pour tout m . Soit $\mathbb{F}^a$ une cloture algebrique de $\mathbb{F}_q$; il y a un isomorphisme canonique

$$\hat{\mathbb{Z}} \to \operatorname{Gal}(\mathbb{F}^a/\mathbb{F}_q)$$

qui envoie $1 \in \hat{\mathbb{Z}}$ dans l'automorphisme $\sigma : x \to x^q$. L'extension de $\mathbb{F}_q$ de degre m correspond au sous-groupe $m\hat{\mathbb{Z}}$ de $\hat{\mathbb{Z}}$. Pour $\alpha \in \hat{\mathbb{Z}}$, on definit σ^α ; c'est l'element de $\operatorname{Gal}(\mathbb{F}^a/\mathbb{F}_q)$ tel que pour tout m , $\sigma^\alpha|\mathbb{F}_{q^m} = \sigma^a$ ou $a \in \mathbb{Z}$ est proche de α . L'isomorphisme ci-dessus envoie α sur σ^α .

b) Soit p un nombre premier et $\Omega_p := \cup_r \mathbb{Q}[\zeta_{p^r}]$, ou ζ_{p^r} est une racine primitive p^r -ieme de l'unite. Pour $u \in \mathbb{Z}_p^\times$, ecrivons $u = a_0 + a_1 p + ...$ avec $0 \le a_i < p-1$. On definit

$$\zeta_{p^r}^u = \zeta_{p^r}^{a_0 + a_1 p + \ldots + a_s p^s} \text{pour tout } s > r.$$

Ceci definit une action de $\mathbb{Z}_p^\times$ sur Ω_p et en fait un isomorphisme de groupes topologiques

$$\mathbb{Z}_p^\times \to \operatorname{Gal}(\Omega_p/\mathbb{Q})$$

Soit $\Omega := \cup_m \mathbb{Q}[\zeta_m]$, ou ζ_m est une racine primitive m -ieme de l'unite; alors $\Omega = \Omega_2.\Omega_3.\Omega_5...$ le compositum des extensions Ω_p dans $\mathbb{Q}^a$ et $\Omega_p \cap \Omega_{p'} = \mathbb{Q}$ si $p \ne p'$. Ainsi il y a un isomorphisme

$$\hat{\mathbb{Z}}^\times \to \operatorname{Gal}(\Omega/\mathbb{Q}) = \prod_p \operatorname{Gal}(\Omega_p/\mathbb{Q})$$

Il peut etre ainsi decrit: si ζ est une racine n -ieme de l'unite et si $u \in \hat{\mathbb{Z}}^{\times}$ alors

$$\zeta^u = \zeta^m,\ \forall m \in \mathbb{Z},\ m \equiv u \bmod n$$

Le lemme de Hensel montre facilement que $\mathbb{Z}_p$ contient les racines $p-1$ iemes de l'unite; soit $\Delta_p \subset \mathbb{Z}_p$ le sous groupe des racines $p-1$ -iemes de l'unite si $p > 2$ et $\{1, -1\}$ si $p = 2$. Les elements de $1 + p\mathbb{Z}_p$ sont clairement inversibles ainsi l'application $a \in (\mathbb{Z}_p, +) \to \exp pa \in (1 + p\mathbb{Z}_p, \times)$ est un isomorphisme de groupes. Considerant la projection $\mathbb{Z}_p \to \mathbb{Z}/p\mathbb{Z}$, il suit que tout element de $\mathbb{Z}_p^{\times}$ s'ecrit sous la forme que $u(1 + pa)$ avec $u \in \Delta_p$ et $a \in \mathbb{Z}_p$. Ainsi

$$\hat{\mathbb{Z}}^{\times} \simeq \Delta_p \times C_p$$

avec $C_p \simeq \mathbb{Z}_p$. Le theoreme de Kronecker-Weber dit que $\Omega = \mathbb{Q}^{ab}$, l'extension abelienne maximale de $\mathbb{Q}$.

Probleme Galois inverse

Le probleme Galois Inverse sur $\mathbb{Q}$ est de montrer que tout groupe fini est groupe de Galois sur $\mathbb{Q}$ i.e. tout groupe fini est un quotient de $\mathrm{Gal}(\mathbb{Q}^a/\mathbb{Q})$.

En particulier si G est un groupe fini abelien cela revient a dire que G est quotient de $\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$. Il est clair que la partie cyclique de $\mathrm{Gal}(\Omega/\mathbb{Q})$ ne peut fournir une reponse positive.

Soit donc $\Omega_p' = \Omega_p^{C_p} = \mathbb{Q}[\zeta_p]$ et $\mathrm{Gal}\mathbb{Q}[\zeta_p]/\mathbb{Q} \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ (si $p > 2$). Soit ℓ un nombre premier et m un entier. Le theoreme de Dirichlet sur les nombres premiers en progression arithmetique montre qu'il y a une infinite de nombres premiers $p \equiv 1 \bmod \ell^m$; ainsi pour tout r on peut exhiber une surjection de $\mathrm{Gal}(\Omega/\mathbb{Q})$ sur $(\mathbb{Z}/\ell^m\mathbb{Z})^r$; et donc tout groupe fini abelien est quotient de $\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$.

L'etude de $\mathrm{Gal}(\mathbb{Q}^a/\mathbb{Q})$ est la centre d'interet de plusieurs ecoles depuis une quinzaine d'annee; une conjecture est apparue apres les travaux de Grothendieck des annees 80 (jeu de Lego-Teichmuller) puis ceux de Drinfeld et de l'ecole japonaise d'Ihara.

Exercice. Montrer que $\mathrm{Gal}(\mathbb{Q}^a/\mathbb{Q})$ n'est pas engendre (topologiquement) par un nombre fini d'elements.

Remarque. En general, il peut exister des sous-groupes d'indice fini dans $\mathrm{Gal}(N/K)$ qui ne sont pas ouverts, (cf p. 12)

B) Cohomologie des groupes (cf Serre: Corps locaux p. 117 et Milne: Class field theory pp 41-76)

Soit G un groupe et A un groupe abélien noté additivement; on suppose que G opere sur A via un homomorphisme $G \to \mathrm{Aut}(A)$; on dit que A est un G -module. On definit $H^r(G, A)$ pour $r \in \mathbb{N}$; on a $H^0(G, A) = A^G$.

le groupe $H^1(G, A)$

Un 1 -cocycle de G dans A est une application $f : G \to A$ verifiant l'identite:

$$gf(g') - f(gg') + f(g) = 0$$

pour tout $g, g' \in G$. On peut additionner les 1 -cocycles composantes à composantes; les 1 -cocycles forment un groupe note $Z^1(G, A)$. On appelle 1 -cobord de G dans A une application $f : G \to A$ telle qu'il existe $a \in A$ tel que $f(g) = g.a - a$ pour tout $g \in G$. Il est clair qu'un 1 -cobord est un 1 -cocycle et que les 1 -cobords forment un groupe note $B^1(G, A)$. Le groupe quotient

$$Z^1(G, A)/B^1(G, A)$$

est appelle le premier groupe de cohomologie et se note $H^1(G, A)$.

Le groupe $H^2(G, A)$

Un 2-cocycle est une application f de $G \times G$ dans A verifiant l'identite:

$$g.f(g', g'') - f(gg', g'') + f(g, g'g'') - f(g, g') = 0.$$

On dit que c'est un syteme de facteurs. De telles fonctions se rencontrent dans la classification des extensions de G par A : soit E un groupe contenant A comme groupe invariant, le quotient etant G i.e. on a une suite exacte de groupes $0 \to A \to E \to G \to 0$; le groupe G opere par automorphisme interieurs sur A (soit $g \in G$ et $\tilde{g} \in E$ un representant; si $a \in A \subset E$ alors $\tilde{g}a\tilde{g}^{-1}$ est independant du representant $\tilde{g}$ de g). Soit $s : G \to E$ une section; si $g, g' \in G$, $s(g).s(g')$ et $s(gg')$ sont dans la meme classe modulo A et il existe un element $f(g, g')$ de A tel que l'on ait:

$$s(g).s(g') = f(g, g')s(gg')$$

Il est clair que la connaissance de f permet d'ecrire la loi de composition de E ; en exprimant l'associativite de cette loi on trouve que f est un systeme de facteurs. Changer s modifie f par un cobord (i.e. une application f de $G \times G$ dans A telle qu'il existe $h : G \to A$ avec $f(g, g') = gh(g') - h(gg') + h(g)$) et l'on peut construire une extension correspondant a un systeme de facteurs donne. Il suit que $H^2(G, A)$ est l'ensemble des classes d'extensions de G par A (les operations de G sur A etant fixees).

Exercice. Montrer que l'extension $\mathbb{Z}/p^{n+1}\mathbb{Z}$ de $G = \mathbb{Z}/p^n\mathbb{Z}$ par $A = \mathbb{Z}/p\mathbb{Z}$ est donnee par le cocycle $f : \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ defini par:

$$f(\bar{i}, \bar{j}) = \frac{1}{p^n}(\underline{i} + \underline{j} - \underline{(i + j)})$$

ou $\underline{i}$ est le representant dans $[0, p^n - 1]$ de la classe $\bar{i} \in \mathbb{Z}/p^n\mathbb{Z}$

Proposition. Soit G un groupe fini et $0 \to A \to B \to C \to 0$ une suite exacte de G -modules. Pour $q \geq 0$ il existe un homomorphismes de groupes (de decalage)

$$\delta : \mathrm{H}^q(G, C) \to \mathrm{H}^{q+1}(G, A)$$

et une suite exacte de cohomologie:

$$...\mathrm{H}^q(G, B) \to \mathrm{H}^q(G, C) \xrightarrow{\delta} \mathrm{H}^{q+1}(G, A) \to \mathrm{H}^{q+1}(G, A) \to ...$$

De plus les δ dependent “fonctoriellement” de la suite exacte donnee.

Preuve: Voir Serre, Cohomologie des groupes profinis, p.13 Corps locaux Chapitre VII

Cohomologie Galoisienne: extensions cycliques

On suppose que G est cyclique engendre par γ ; soit $\mathrm{Tr}_G : A \to A$ l'homomorphisme tel que $\mathrm{Tr}_G(a) = \sum_{\sigma \in G} \sigma(a)$ (en notation multiplicative Tr_G se note N_G). Soit $(1-\gamma)A$ les elements de A de la forme $a - \gamma a,\ a \in A$; alors $(1-\gamma)A \subset \ker Tr_G$. Il est facile de decrire les 1 -cocycles; soit $\{\alpha_{\sigma^i}\}, 0 \leq i \leq n-1$ un 1 -cocycle; alors $\alpha_{\sigma^0} = 0$ et si $\alpha_\sigma = a$ alors pour $1 \leq i \leq n-1$ on a $\alpha_{\sigma^i} = a + \sigma(a) + ... + \sigma^{i-1}(a)$ et puisque $\sigma^n = \sigma^0$ il suit que $a \in \ker Tr_G$; ainsi l'application qui au cocycle associe sa composante α_σ definit un homomorphisme surjectif $Z^1(G,A) \to \ker Tr_G$ qui induit un isomorphisme

$$\mathrm{H}^1(G,A) \to \ker Tr_G/(1-\gamma)A$$

le sous groupe $(1-\gamma)A$ est l'image de $B^1(G,A)$, d'ou le resultat.

Theoreme (Hilbert 90). Soit L/K une extension Galoisienne finie de groupe de Galois G . Pour l'operation de G sur L^* on a $H^1(G,L^*) = 1$ et pour l'operation sur le groupe additif de L on a $H^1(G,L) = 0$.

Preuve: Soit $\{\alpha_\sigma\}_{\sigma \in G}$ un 1 -cocycle de G dans L^* . On a

$$\alpha_\sigma \alpha_\tau^\sigma = \alpha_{\sigma\tau}$$

Par l'indépendance lineaire des caracteres (voir lemme ci-apres), il existe $\theta \in L$ tel que l'element

$$a = \sum_{\tau \in G} \alpha_\tau \tau(\theta) \neq 0$$

Alors

$$\sigma a = \sum_{\tau \in G} \alpha_\tau^\sigma \sigma\tau(\theta) = \alpha_\sigma^{-1} a$$

Ainsi $\alpha_\sigma = \sigma(a^{-1})/a^{-1}$.

Pour la partie additive du theoreme on considere un element θ de trace non nulle. Si $\{\alpha_\sigma\}_{\sigma \in G}$ est un 1 -cocycle de G dans le groupe additif L alors

$$a := \frac{1}{\mathrm{Tr}(\theta)} \sum_{\tau \in G} \alpha_\tau \tau(\theta)$$

satisfait l'equation $\alpha_\sigma = a - \sigma a$

Lemme (Artin) Soit G un monoide et L un corps. Soient $\chi_1, ..., \chi_n$ des caracteres distincts de G dans K (i.e. χ_i est un homomorphisme de G dans le groupe multiplicatif de L), alors ils sont lineairement independants sur L .

Cohomologie galoisienne: extensions galoisiennes infinies

Soit L/K une extension Galoisienne (non necessairement finie). Son groupe de Galois Γ est un groupe topologique compact, totalement discontinu, limite projective des groupes de Galois $\mathrm{Gal}(E/K)$ ou E parcourt l'ensemble des sous-extensions galoisiennes finies de K .

Soit A , un Γ -module; on dit que c'est un Γ -module topologique si pour tout $a \in A$, l'ensemble des $s \in \Gamma$ tels que $s(a) = a$ est un sous-groupe ouvert de Γ . Il revient au meme de dire que

$$A = \cup A^H$$

lorsque H parcourt les sous-groupe invariants ouverts de G . C'est le cas pour $A = L$ ou L^* (plus generalement c'est le cas lorsque A est le groupe des points rationnels sur L d'un schema en groupes de type fini sur K).

Si A est un Γ -module topologique, on definit $\mathrm{H}^q(\Gamma, A)$ par la formule

$$\mathrm{H}^q(\Gamma, A) = \varinjlim \mathrm{H}^q(\Gamma/H, A^H)$$

pour H parcourant l'ensemble des sous-groupes distingues ouverts de Γ (la limite inductive est prise relativement aux groupes d'inflation). Ces groupes de cohomologie jouissent de proprietes analogues a celles des groupes de cohomologie usuels et peuvent etre definis par des cochaines continues a valeur dans A . Nous y reviendrons au paragraphe D).

C) Extensions abeliennes

Soit K un corps de caractéristique $p \geq 0$; on se propose d'etudier les extensions aéliennes de K .

Theorie de Kummer

On fixe K^a une cloture algebrique de K . On note n un entier > 0 et on suppose que le groupe $\mu_n(K)$ des racines n -ieme de l'unite dans K est de cardinal n (i.e $(n,p) = 1$ et $\mu_n(K)$ est cyclique d'ordre n).

On dit que l'extension L/K est abelienne d'exposant divisant n si elle est abelienne et si son groupe de Galois $G = \mathrm{Gal}(L/K)$ est annule par n .

Soit A une partie de K^* ; on note $K(A^{1/n})$ la sous-extension de K^a engendree par les $\theta \in K^a$ tels que $\theta^n \in A$.

Lemme 1. $K(A^{1/n})$ est une extension abelienne de K d'exposant divisant n .

Preuve: Puisque les polynomes $X^n - a,\ a \in A$ sont separables sur K , $L = K(A^{1/n})$ est une extension separable et donc Galoisienne de K . Soit $\sigma \in \mathrm{Gal}(L/K)$ et soit $\theta \in K^a$ tel que $\theta^n \in A$. On a $\sigma(\theta)^n = \theta^n$; il existe donc $\zeta \in \mu_n(K)$ tel que $\sigma(\theta) = \zeta\theta$; cela implique que $\sigma^n(\theta) = \zeta^n\theta = \theta$, d'ou $\sigma^n = 1$. Si σ' est un autre element de $\mathrm{Gal}(L/K)$, il existe $\zeta' \in \mu_n(K)$ tel que $\sigma'(\theta) = \zeta'\theta$, d'ou $\sigma'\sigma(\theta) = \zeta\zeta'\theta = \sigma\sigma'(\theta)$ et donc $\sigma'\sigma = \sigma\sigma'$.

Lemme 2. Soit L une extension galoisienne de K . Il existe une unique application $(\sigma, a) \to < \sigma, a >$ de $\mathrm{Gal}(L/K) \times (L^n \cap K^*)/K^{*n})$ dans $\mu_n(K)$ telle pour tout $\sigma \in \mathrm{Gal}(L/K)$ et tout $\theta \in L^*$ avec $\theta^n \in K$, on ait,

$$< \sigma, \overline{\theta}^n >= \sigma(\theta)/\theta$$

ou $\overline{\theta}^n$ designe la classe de $\theta^n \bmod K^{*n}$. Cette application est bimultiplicative.

Preuve: Il suffit de remarquer que $\sigma(\theta)/\theta$ ne depend que de la classe de $\theta^n \bmod K^{*n}$.

Pour toute extension galoisienne L/K , notons

$$k_L : (L^n \cap K^*)/K^{*n} \to Hom\,(\mathrm{Gal}(L/K), \mu_n(K)),$$

$$k'_L : \mathrm{Gal}(L/K) \to Hom\,((L^n \cap K^*)/K^{*n}, \mu_n(K)),$$

les homomorphismes deduits de l'application bimultiplicative precedente.

Proposition. Pour toute extension galoisienne de degre fini L/K , l'homomorphisme k_L est bijectif.

Preuve: Soit $\theta \in L^*$ tel que $\theta^n \in K$ et que la classe de θ^n modulo K^{*n} appartienne au noyau de k_L . Pour tout $\sigma \in \mathrm{Gal}(L/K)$, on a $\sigma(\theta) = \theta$; donc $\theta \in K^*$ et $\theta^n \in K^{*n}$. Ce qui montre l'injectivite de k_L .

Soit $f : \mathrm{Gal}(L/K) \to \mu_n(K)$ un homomorphisme; pour tout $\sigma,\ \tau \in \mathrm{Gal}(L/K)$ on a

$$f(\sigma\tau) = f(\sigma)f(\tau) = f(\sigma).\sigma f(\tau), \quad f(\sigma)^n = 1$$

D'apres Hilbert 90, il existe $\theta \in L^*$ tel que $f(\sigma) = \sigma(\theta)/\theta$ pour tout $\sigma \in Gal(L/K)$; comme $f(\sigma)^n = 1$, on a $\sigma(\theta^n) = \theta^n$ pour tout $\sigma \in Gal(L/K)$, donc $\theta^n \in K^*$; si a est la classe de θ^n modulo K^{*n} on a par definition $f(\sigma) =< \sigma, a >$ pour tout $\sigma \in Gal(L/K)$, donc $f = k_L(a)$.

Corollaire. Si L/K est une extension galoisienne, l'homomorphisme k_L est injectif et son image est le groupe $Hom_c(\mathrm{Gal}(L/K), \mu_n(K))$ des homomorphismes continus du groupe topologique $\mathrm{Gal}(L/K)$ dans le
groupe discret $\mu_n(K)$

preuve: un homomorphisme de $\mathrm{Gal}(L/K)$ dans $\mu_n(K)$ est continu ssi il se factorise par un des quotients $\mathrm{Gal}(L_i/K)$ de $\mathrm{Gal}(L/K)$.

Theoreme. a) L'application $A \to K(A^{1/n})$ est une bijection croissante de l'ensemble des sous-groupes de K^* contenant K^{*n} sur l'ensemble des sous-extensions abeliennes d'exposant divisant n de K^a . L'application reciproque est $L \to L^n \cap K^*$.

b) Pour tout sous-groupe A de K^* avec $A \supset K^{*n}$, l'homomorphisme

$$k' : \mathrm{Gal}(K(A^{1/n}/K) \to Hom\,(A/K^{*n}, \mu_n(K))$$

est bijectif. Lorsque ce dernier groupe est muni de la topologie de la convergence simple, c'est un homeomorphisme.

c) Soit A un sous-groupe de K^* contenant K^{*n} . Pour chaque $a \in A/K^{*n}$ soit θ_a un element de K^a tel que θ_a^n soit un representant de a dans A . Alors les $\theta_a,\ a \in A/K^{*n}$ forment une base du K -espace vectoriel $K(A^{1/n})$. En particulier

$$[K(A^{1/n}) : K] = (A : K^{*n})$$

preuve: exercice

Exemples

1) Il existe une plus grande extension abelienne d'exposant divisant n de K contenue dans K^a ; elle s'obtient en adjoignant a K les racines n -iemes de tous ses elements; son groupe de Galois s'identifie a
$Hom\,(K^*/K^{*n}, \mu_n(K))$, donc aussi a $Hom\,(K^*, \mu_n(K))$

2) Prenons $K = \mathbb{Q}$ et $n = 2$. Alors $\mathbb{Q}^*/\mathbb{Q}^{*2}$ est un $\mathbb{F}_2$ -espace vectoriel admettant pour base $\{-1\}$ union l'ensemble des nombres premiers. La plus grande extension abelienne d'exposant 2 de $\mathbb{Q}$ contenue dans $\mathbb{C}$ est donc le sous-corps $\mathbb{Q}(i, \sqrt{2}, \sqrt{3}, \sqrt{5}, ...)$ de $\mathbb{C}$. Son groupe de Galois G est isomorphe au groupe produit $(\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$; le sous-groupe $\bigoplus \mathbb{Z}/2\mathbb{Z}$ est dense dans $(\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ et le quotient $(\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}/\bigoplus \mathbb{Z}/2\mathbb{Z}$ est $\mathbb{F}_2$ -espace vectoriel qui admet des sous-espaces de codimension finie et donc le groupe de Galois G admet des sous groupes d'indice fini qui ne sont pas ouverts.

Interpretation cohomologique, l'isogenie de Kummer

Soit n un entier premier a la caracteristique de K , on suppose que K contient les racines n -iemes de l'unite. Soit K^s une cloture separable de K et G_K le groupe de Galois de K^s/K , on a la suite exacte de G_K -modules:

$$1 \to \mu_n(K) \to K^{s*} \xrightarrow{u} K^{s*} \to 1$$

avec $u(x) = x^n$, puisque $\mathrm{H}^1(G_K, K^{s*}) = 0$ la suite exacte de cohomologie donne un isomorphisme
$K^*/K^{*n} \to \mathrm{H}^1(G_K, \mu_n(K)) = Hom\,(G_K, \mu_n(K))$. Cet isomorphisme fait correspondre a un element $a \in K^*$ l'homomorphisme $\varphi_a : G \to \mu_n(K)$ defini de la maniere suivante: on resout l'equation $x^n = a$ et l'on pose $s(x) = \varphi_a(s).x$ avec $\varphi_a(s) \in \mu_n(K)$

Theorie d'Artin-Schreier

Les preuves sont omises; c'est une traduction additive de la theorie de Kummer (ceci laisse presager une theorie qui unifie les deux theories!)

Dans ce paragraphe on note p un nombre premier et on suppose que K est un corps de caracteristique p . On note K^s une cloture algebrique separable de K et F l'endomorphisme de Frobenius du groupe additif de K^s defini par $\mathrm{F}(x) = x^p$; enfin on note $\wp$ l'endomorphisme $\mathrm{F} - \mathrm{Id}$. On a

$$\wp(x) = x^p - x$$

Le noyau de $\wp$ est le corps premier $\mathbb{F}_p$ de K . Pour toute partie A de K on note $K(\wp^{-1}(A))$ la sous-extension de K^s engendree par les $x \in K^s$ tels que $\wp(x) \in A$.

Lemme. $K(\wp^{-1}(A))$ est une extension abelienne de K d'exposant divisant p .

preuve: Les polynomes $X^p - X - a, a \in A$ sont separables sur K ainsi $L := K(\wp^{-1}(A))/K$ est galoisienne. Soit $\sigma \in \mathrm{Gal}(L/K)$ et soit $x \in \wp^{-1}(A)$; on a $\wp(\sigma(x)) = \wp(x)$; donc $\sigma(x) - x \in \mathbb{F}_p$; i.e. $\sigma(x) = x + i, i \in \mathbb{F}_p$. Cela implique que $\sigma^p = 1$; de meme si $\sigma' \in \mathrm{Gal}(L/K)$ alors $\sigma(x) = x + j, j \in \mathbb{F}_p$ et donc $\sigma\sigma' = \sigma'\sigma$

Lemme. Soit L une extension galoisienne de K . Il existe une unique application $(\sigma, a) \to [\sigma, a >$ de $\mathrm{Gal}(L/K) \times ((\wp(L) \cap K)/\wp(K))$ dans $\mathbb{F}_p$ telle que, pour tout

$\sigma \in \mathrm{Gal}(L/K)$ et tout $x \in L$ tel que $\wp(x) \in K$, on ait notant $\overline{\wp(x)}$ la classe de $\wp(x) \bmod \wp(K)$

$$[\sigma, x >= \sigma(x) - x$$

Cette application est $\mathbb{Z}$ -bilineaire i.e. $[\sigma\tau, a >= [\sigma, a > +[\tau, a >$ et $[\sigma, a+b >= [\sigma, a > +[\sigma, b >$

Pour toute extension galoisienne L de K, notons

$$a_L : (\wp(L) \cap K)/\wp(K)/\wp(K) \to Hom\,(\mathrm{Gal}(L/K), \mathbb{F}_p)$$

$$a'_L : \mathrm{Gal}(L/K) \to Hom\,((\wp(L) \cap K)/\wp(K), \mathbb{F}_p)$$

les homomorphismes deduits de l'application $\mathbb{Z}$ -bilineaire precedente.

Proposition. Pour toute extension galoisienne de degre fini L de K, l'homomorphisme a_L est bijectif.

preuve: consequence tu theoreme de Hilbert 90 (forme additive)

Corollaire. Si L/K est une extension galoisienne, l'homomorphisme a_L est injectif et son image est le groupe $Hom_c(\mathrm{Gal}(L/K), \mathbb{F}_p)$ des homomorphismes continus du groupe topologique $\mathrm{Gal}(L/K)$ dans le groupe discret $\mathbb{F}_p$)

Theoreme. a) L'application $A \to K(\wp^{-1}(A))$ est une bijection croissante de l'ensemble des sous-groupes de K contenant $\wp(K)$ sur l'ensemble des sous-extensions abeliennes d'exposant divisant p de K^s. L'application reciproque est $L \to \wp(L) \cap K$.

b) Pour tout sous-groupe A de K contenant $\wp(K)$ l'homomorphisme

$$a' : \mathrm{Gal}(K(\wp^{-1}(A))/K) \to Hom\,(A/\wp(K), \mathbb{F}_p)$$

est bijectif. Lorsque ce dernier groupe est muni de la topologie de la convergence simple, c'est un homeomorphisme.

c) Soit A un sous-groupe de K contenant $\wp(K)$ et soit B une base du $\mathbb{F}_p$ -espace vectoriel $A/\wp(K)$. Pour chaque $a \in B$ soit x_a un element de K^s tel que $\wp(x_a)$ soit un representant de a dans A. Alors les monomes $x^\alpha = \prod_{a \in B} x_a^{\alpha(a)}$ avec $\alpha = (\alpha(a))$ dans $\mathbb{N}^{(B)}$ tel que
$0 \leq \alpha(a) < p$ pour tout $a \in B$ forment une base du K -espace vectoriel $K(\wp^{-1}(A))$. En particulier

$$[K(\wp^{-1}(A)) : K] = (A : \wp(K))$$

Extensions p^2 -cycliques

D'apres Artin et Schreier ([Ar-Sc], Über eine Kennzeichnung der reell abgeschlossen Körper, Abh. Math, Sem. Hamburg 5 (1927)). Ils remarquent que si $x^p - x = a$ définit une extension cyclique de K alors il est possible de la plonger dans une extension cyclique de degré p^2. Précisément ils cherchent $P(X) \in K[X]$ de degre $< p$ tel que l'equation $y^p - y = P(x)$ definisse une extension p^2 -cyclique de K ; soit σ un generateur du groupe de Galois. Alors $\sigma(y) = ky + \Psi(x)$ ou $k \in \mathbb{F}_p$ et $\Psi(X) \in K[X]$ de degre $< p$

(dans une extension cyclique $K(x)/K$ de degre p si x est generateur d'Artin-Schreier, les autres generateurs sont de la forme $ax+b$ avec $a \in \mathbb{F}_p$ et $b \in K$) . En iterant cette formule on a $\sigma^p(y) = k^p y + k^{p-1}\Psi(X) + k^{p-2}\Psi(X+1) + ... + \Psi(X+p-1)$, ce qui vu que $\sigma^p(y) - y \in \mathbb{F}_p - 0$ (remarquer que $\sigma^p(P(x)) = P(x)$) montre les identites, $k^p = 1$ donc $k = 1$ et $\sum\limits_{0 \le i \le p-1} \Psi(x+i) = h \in \mathbb{F}_p - 0$. Puisque le terme constant dans $\sum\limits_{0 \le i \le p-1} (X+i)^k$ est nul pour $0 \le k \le p-2$ et vaut -1 pour $k = p-1$ il suit que $-h$ est le coefficient de $\Psi(X)$ de degre $p-1$; on peut donc supposer que $\sigma y = y + x^{p-1} + \Psi(x)$, $\Psi(X) \in K[X]$ de degre $< p-1$ et $\sigma^p y = y - 1$. Il est facile maintenant de resoudre l'equation fonctionnelle $f(X+1) - f(X) = \Psi(X)$ avec $f(X) \in K[X]$ de degre $< p$; ainsi quitte a changer y en $y + f(x)$ on peut supposer que $\sigma y = y + x^{p-1}$ et donc $P(X+1) - P(X) = (X+a)^{p-1} - X^{p-1}$.

Réciproquement $x^p - x = a$ et $y^p - y = P(x)$ avec $(*)\ P(X+1) - P(X) = (X+a)^{p-1} - X^{p-1}$ définissent bien une extension cyclique de degre p^2 puisque l'on peut prolonger l'automorphisme $x \to x+1$ de $K(x)$ par $y \to y + x^{p-1}$.

Remarque. Pour resoudre l'equation (*); on remarque que les polynomes binomiaux $\binom{n}{X} := \dfrac{X(X-1)...(X-n+1)}{n!}$, $0 \le n \le p-1$ forment une base sur K de l'espace vectoriel des polynomes dans $K[X]$ de degre $\le p-1$; d'autre part ils satisfont l'identite binomiale $\Delta\binom{n+1}{X} = \binom{n}{X}$ pour $n \le p-2$ ou Δ est l'operateur $\Delta(P) := P(X+1) - P(X)$. Ainsi on si $f(X) = \sum\limits_{0 \le n \le p-2} a_n \binom{n}{X}$ les solutions de l'equation $P(X) \in K[X],\ \Delta(P) = f(X)$ sont donnees par: $\sum\limits_{1 \le n \le p-1} a_n \binom{n}{X} + \ker\Delta$. Il est facile d'exhiber des polynomes non nuls dans $\ker\Delta$; par exemple $P(X^p - X)) \in \ker\Delta$ pour $P \in K[X]$ (il me semble que c'est en fait une descrition de $\ker\Delta$).

Extensions p^n -cycliques

Plus généralement E. Witt s'interesse aux extensions Galoisiennes de groupe un p-groupe ([W 1] Witt Konstrktion von galoisshen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f Crelle 174 (1936)). Nous reviendrons sur ce cadre general dans le paragraphe suivant. Il examine en particulier le cas cyclique de degre p^f generalisant ainsi [Ar-Sc]. Supposons construit L/K une extension cyclique de degre $p^{f-1}, f > 1$; soit s un générateur du groupe de Galois et $\mathrm{Tr}_{L/K}$ l'application trace. Soit $\chi \in \mathbb{F}_p$ non nul.

Analyse. Soit $M := L(\theta)$ une extension cyclique de degre p^f de K . Soit S un K -automorphisme de M qui prolonge s , alors $g := S^{p^{f-1}}$ engendre le groupe de Galois de M/L . On peut supposer que θ satisfait une equation $(F - Id)(\theta) = \gamma \in L$ et que $(g-1)\theta = \chi$. On a $(g-1)(S-1)\theta = (S-1)(g-1)\theta = (S-1)\chi = 0$, ainsi $(S-1)\theta = \delta \in L$. Alors $(s-1)\gamma = (s-1)(F-Id)(\theta) = (F-Id)(s-1)(\theta) = (F-Id)\delta$ et $\mathrm{Tr}_{L/K}\delta = \dfrac{S^{p^{f-1}} - 1}{S-1}(S-1)\theta = (g-1)\theta = \chi$.

Construction. Puisque la forme $Tr_{L/K}$ est non dégénérée il existe δ avec $Tr_{L/K}(\delta) = \chi$; alors $Tr_{L/K}(F - Id)(\delta) = 0$ et via le théorème 90 de Hilbert dans sa forme additive il existe $\gamma \in L$ avec $(s-1)\gamma = (F - Id)(\delta)$. Remarquons que si l'on change δ en $\delta + (s-1)\alpha$ avec $\alpha \in L$ alors on change γ en $\gamma + (F - Id)(\alpha)$. Ainsi verifier que l'equation $(F - Id)(\beta) = \gamma$ n'a pas de solution dans L revient a voir que $\gamma = 0$ est impossible. Si $\gamma = 0$; on a $(F - Id)(\delta) = 0$ et donc $\chi = 0$. Soit donc θ une racine de $(F - Id)(x) = \gamma$; alors $M := L(\theta)$ est de degre p^f sur K . Puisque $\theta + \delta$ satisfait l'équation $(F - Id)(x) = s\gamma$ il suit que s se prolonge en S par $S\theta = \theta + \delta$.

Interpretation cohomologique, l'isogenie d'Artin Schreier

C'est la suite exacte de G_K modules

$$0 \to \mathbb{Z}/p\mathbb{Z} \to K^s \xrightarrow{\wp} K^s \to 0.$$

En ecrivant la suite exacte de cohomologie, et en tenant compte de ce que

$$H^1(G_K, K^s) = 0$$

on obtient

$$K \xrightarrow{\wp} K \to \mathrm{H}^1(G_K, \mathbb{Z}/p\mathbb{Z}) \to 0$$

En d'autres termes, le groupe $Hom\,(G_K, \mathbb{Z}/p\mathbb{Z})$ des homomorphismes continus de G_K dans $\mathbb{Z}/p\mathbb{Z}$ est isomorphe a $K/\wp(K)$; l'isomorphisme en question fait correspondre a $a \in K$; l'homomorphisme $\varphi_a : G_K \to \mathbb{Z}/p\mathbb{Z}$ defini de la maniere suivante: on resout l'equation $x^p - x = a$ et l'on pose $s(x) = x + \varphi_a(s)$.

D. Sur la p -extension maximale d'un corps de caracteristique $p > 0$

Pro- p -groupes

Definition. Un groupe profini est un groupe topologique qui est limite projective de groupes finis (munis chacun de la topologie discrete). Un tel groupe est compact et totalement discontinu. Reciproquement, si G est compact totalement discontinu, G possede une base de voisinages de l'element neutre formee de sous-groupe ouverts distingues U , et G s'identifie a $\varprojlim G/U$; ce qui montre que G est profini.

Soit p un nombre premier. Un groupe profini H est appele pro- p -groupe si c'est une limite projective de p -groupes.

Soit I un ensemble et soit $L(I)$ le groupe discret libre engendre par des elements x_i indexes par I . Soit X la famille des sous-groupes distingues M de $L(I)$ tels que:

a) $L(I)/M$ est un p groupe fini,

b) M contient presque tous les x_i (i.e. sauf un nombre fini)

Posons $F(I) = \varprojlim L(I)/M$. Le groupe $F(I)$ est un pro- p -groupe que l'on appelle le pro- p -groupe libre engendre par les x_i L'adjectif libre est justifie par la proposition suivante:

Proposition. Si G est un pro- p -groupe, les morphismes de $F(I)$ dans G correspondent bijectivement aux familles $(g_i)_{i \in I}$ d'elements de G qui tendent vers zero suivant le filtre des complementaires des parties finies.

p -extension maximale d'un corps

Dans [W 1], E. Witt montre le théorème:

Théorème. Soit K un corps de caractéristique $p > 0$, F l'automorphisme de Frobenius; N la dimension éventuellement infini du $\mathbb{F}_p$ espace vectoriel $K/(F-Id)(K)$. Soit G un p -groupe de cardinal p^f , $n(G)$ le nombre minimal de générateurs. Une condition nécessaire et suffisante pour qu'il existe L/K une extension galoisienne de groupe de Galois G est que $n(G) \leq N$. Dans le cas où N est fini le nombre de telles extensions est $p^{N(f-n)}(p^N-1)(p^N-p)...(p^N-p^{n-1})/|Aut(G)|$.

Sa preuve utilise les homomorphismes croises; la cohomologie des groupes profinis permet de prouver ce resultat elegamment.

Lemme. Pour toute extension galoisienne K/k de groupe de Galois G on a $\mathrm{H}^q(G,K) = 0$, pour $q \geq 1$.

Preuve: En vertue de ce que nous avons dit concernant la cohomologie galoisienne des extensions infinies; il suffit de montrer le lemme dans le cas des extensions finies. Le theoreme de la base normale montre qu'il existe $x \in K$ tel que $K = k[G].x = \mathbb{Z}[G]M$ ou M est le groupe abelien kx (ainsi K est un G -module induit) et la cohomologie d'un tel module est triviale (cf. Milne, Class field Theory p. 45, "Shapiro's lemma", Serre, Cohomologie des groupes profinis, p. 11).

La suite exacte de cohomologie d'Artin-Schreier donne une suite exacte

$$\mathrm{H}^1(G_K, K^s) \to \mathrm{H}^2(G_K, \mathbb{Z}/p\mathbb{Z}) \to \mathrm{H}^2(G_K, K^s)$$

ainsi le lemme precedent montre que $\mathrm{H}^2(G_K, \mathbb{Z}/p\mathbb{Z}) = 0$. Soit N un sous-groupe ferme de G_K ; c'est le groupe de Galois de l'extension K^s/K^{sN} ; **on peut lui appliquer le resultat precedent** ainsi
$\mathrm{H}^2(N, \mathbb{Z}/p\mathbb{Z}) = 0$. Soit $G_{K(p)}$, le groupe de Galois de la p -extension maximale de K dans K^s et $N := \ker(G_K \to G_{K(p)})$ est un groupe ferme. Puisque N n'a pas de quotient qui soit un p -groupe il resulte que $\mathrm{H}^1(N, \mathbb{Z}/p\mathbb{Z}) = 0$. Il suit **de la suite spectrale** (cf. Serre, Cohomologie des groupes profinis, p.13) **que l'on a une suite exacte**

$$0 \to \mathrm{H}^1(G_{K(p)}, \mathbb{Z}/p\mathbb{Z}) \to \mathrm{H}^1(G_K, \mathbb{Z}/p\mathbb{Z}) \to \mathrm{H}^1(N, \mathbb{Z}/p\mathbb{Z}) \to$$

$$\to \mathrm{H}^2(G_{K(p)}, \mathbb{Z}/p\mathbb{Z}) \to \mathrm{H}^2(G_K, \mathbb{Z}/p\mathbb{Z})$$

Ainsi $\mathrm{H}^2(G_{K(p)}, \mathbb{Z}/p\mathbb{Z}) = 0$.

Suivant Serre, Cohomologie des groupes profinis, corollaire 2 p.128, cette propriete caracterise les pro- p -groupes libres. Ainsi:

Theoreme. Le groupe $G_{K(p)}$ est un pro- p -groupe libre de rang $\dim_{\mathbb{F}_p} \mathrm{H}^1(G_{K(p)}, \mathbb{Z}/p\mathbb{Z}) \simeq K/\wp(K)$

E. Groupes algebriques, Vecteurs de Witt

Nous avons vu que les suites exactes de Kummer et d'Artin -Schreier permettent de parametrer les extensions cycliques d'ordre quelconque en caracteristique 0 et seulement d'ordre p en caracteristique $p > 0$, ce sont des exemples de ce que l'on appelle "Extensions Galoisiennes generiques". On cherche un candidat pour les $\mathbb{Z}/p^n\mathbb{Z}$ -extensions en caracteristique $p > 0$. C'est E. Witt ([W 3]) qui découvre un procede qui généralise l'approche d'Artin-Schreier.

Groupes algebriques

Soit K un corps et K^a une cloture algebrique. Les varietes sont des schemas integres de type finis sur K ; une variete est definie sur K si elle admet localement pour la topologie de Zariski un systeme d'equations donnees par des polynomes a coefficients dans K .

Definition. Un groupe algebrique defini sur K est une variete algebrique G sur K et deux morphismes de K -varietes:

$$m:\ G \times G \to G \quad et \quad i : G \to G$$

satisfaisant les axiomes de groupes suivant:

1. Il y a un point $O \in G(K)$ tel que $m(P,O) = m(O,P) = P$ pour tout $P \in G$; on note $e : K \to G$ le morphisme definissant O .

2. $m(P, i(P)) = m(i(P), P) = O$ pour tout $P \in G$

3. $m(P, m(Q,R)) = m(m(P,Q), R)$ pour tout $P,Q,R \in G$

On dit que G est un groupe algebrique commutatif si de plus il satisfait:

4. $m(P,Q) = m(Q,P)$ pour tout $P,Q \in G$

Exemples.

1. Le groupe additif G_a et le groupe multiplicatif G_m sont les groupes alegbriques commutatifs

$$\mathbb{G}_a \simeq \mathbb{A}^1 \quad et \quad \mathbb{G}_m \simeq \{x \in \mathbb{A}^1 :\ x \neq 0\}$$

Les lois de groupe sont definies par les formules:

$$\mathbb{G}_a \times \mathbb{G}_a \to \mathbb{G}_a \quad (x,y) \to x + y$$

$$\mathbb{G}_m \times \mathbb{G}_m \to \mathbb{G}_m \quad (x,y) \to xy$$

2. Soit n un entier premier a la caractereristique de K ; on note μ_n le sous-groupe de $\mathbb{G}_m$ des racines n -iemes de l'unite. On a $\mu_n = \mathrm{Spec}K[T]/(T^m - 1)$; dans le cas ou $p = n$, on obtient une K -algebre non reduite! d'ou la necessite que nous rencontrerons dans le chapitre suivant d'introduire des schemas en groupes non reduits.

3. Le groupe lineaire est defini par

$$\mathrm{Gl}_n := \left\{ M = \begin{pmatrix} x_{11} & \dots & x_{1n} \\ \vdots & & \vdots \\ x_{n1} & \dots & x_{nn} \end{pmatrix} \in \mathbb{A}^{n^2} : \quad \det(M) \neq 0 \right\}$$

c'est un groupe algebrique dont la loi de groupe est donne par le produit matriciel. Remarquez que l'inverse $i(M) = M^{-1}$ est un morphisme sur Gl_n puisque la fonction $1/\det M$ est une fonction reguliere sur Gl_n .

4. Une courbe elliptique E/K est un groupe algebrique commutatif defini sur K ; contrairement aux exemples precedent il n'est pas affine, il est complet.

Algebres de Hopf.

Soit G un groupe algebrique affine defini sur K et $A := \mathcal{O}_G(G)$ (on note souvent $K[G]$ la K -algebre A ; ce qui prete malheureusement a confusion); les axiomes de groupes s'expriment par la commutativite des diagrammes suivants:

$$\begin{tikzcd}
A \otimes A \otimes A & A \otimes A \arrow[l, "m^* \otimes id"'] \\
A \otimes A \arrow[u, "id \otimes m^*"] & A \arrow[l, "m^*"'] \arrow[u, "m^*"']
\end{tikzcd}$$

$$\begin{tikzcd}
A & A \otimes A \arrow[l, "e^* \otimes id"'] \\
A \otimes A \arrow[u, "id \otimes e^*"] & A \arrow[l, "i^*"'] \arrow[u, "m^*"'] \arrow[ul, "id"']
\end{tikzcd}
\qquad
\begin{tikzcd}
A \otimes A \arrow[d, "m"'] & A \otimes A \arrow[l, "i^* \otimes id"'] \\
A & A \arrow[l, "e^*"'] \arrow[u, "m^*"'] \arrow[d, "m^*"] \\
A \otimes A \arrow[u, "m"] & A \arrow[l, "id \otimes i^*"']
\end{tikzcd}$$

La donnee (A, e, m, i) assujettie aux 3 diagrammes precedents est appelee une K - algebre de Hopf associative.

Exemples.

1. Le groupe additif $\mathbb{G}_a$. Dans ce cas $A = K[T]$, $e(T) = 0$, $m(T) = T \otimes 1 + 1 \otimes T$, $i(T) = -T$.

2. Le groupe lineaire Gl_n . L'anneau affine $A = K[T_{i,j}, 1/\det(T_{i,j})]$ ou $1 \leq i, j \leq n$, $e(T_{i,j}) = \delta_{i,j}$, $m(T_{i,j}) = \sum\limits_h T_{i,h} \otimes T_{h,j}$ et $i(T_{i,j}) = (-1)^{i+j} \dfrac{\det(T_{r,s})_{r \neq j, s \neq i}}{\det(T_{i,j})}$

3. Le groupe multiplicatif $\mathbb{G}_m$. On a donc $A = K[T, 1/T]$, $e(T) = 1$, $m(T) = T \otimes T$, $i(T) = T^{-1}$.

Categories, Foncteurs. cf. Douady, Algebre et theorie galoisiennes

Soit K un anneau et M_K la categorie des K -algebres commutatives.

Un K -foncteur est un foncteur covariant de M_K dans la categorie des ensembles E (i.e. une application $F : M_K \to E$ et pour tout couple $A, B \in M_K$ une application

$$F_{A,B} : Hom_{M_K}(A, B) \to Hom_E(F(A), F(B))$$

ces donnees etant assujeties a des compatibilites: $F_{A,A}(\mathrm{Id}_A) = \mathrm{Id}_{F(A)}$ et $F_{A,C}(g \circ f) = F_{B,C}(g) \circ F_{A,B}(f)$)

Exemple. La droite affine $\mathbb{A}^1_K$ est definie par $\mathbb{A}^1_K(R) = R$ pour tout $R \in M_K$.

Proposition. Soit F un foncteur de M_K dans la categorie des ensembles E . Si les elements dans $F(R)$ correspondent aux solutions dans R d'une famille d'equations, alors il existe une K -algebre A et une correspondance naturelle entre $F(R)$ et $Hom_K(A,R)$ (la reciproque marche).

Un tel foncteur F est dit representable et A represente F .

On peut donc definir un schema en groupe affine sur K comme un foncteur representable des K -algebres dans les groupes; si K est un corps on a parle de groupe algebrique affine.

Lemme. (Yoneda). Soient E et F deux foncteurs (a valeur dans les ensembles) representes par des K -algebres A et B . Les applications naturelles $E \to F$ correspondent aux homomorphismes de K -algebres $B \to A$.

On suppose desormais que K est un corps. Si C est une K -algebre de Hopf on note

$$G(C) := Hom_K(A,C)$$

cet ensemble est muni d'une loi de groupe comme il suit: Si $x,y \in G(C)$, le produit dans $G(C)$ de x et y est donne par le compose

$$A \xrightarrow{m^*} A \otimes A \xrightarrow{x \otimes y} C \otimes C \xrightarrow{mult} C,$$

ou $mult(a \otimes b) = ab$. Si $C \to C'$ est un homomorphisme de K -algebres alors $G(C) \to G(C')$ est un homomorphisme de groupes. Plus generalement pour tout groupe algebrique (non necessairement affine) son foncteur point: $C \to G(C)$ est un foncteur en groupes. Ainsi:

Proposition. Soit G un groupe algebrique defini sur K ; alors l'ensemble $G(K)$ des points rationnels est un sous-groupe de G

Homomorphismes, Sous-groupes

Definition. Un homomorphisme de groupes algebriques $\Phi: G \to H$ est un morphisme de varietes qui est aussi un homomorphisme de groupes i.e. $\Phi(O_G) = O_H$ et

$$\Phi(m_G(P,Q)) = m_H(\Phi(P), \Phi(Q))$$

pour tout $P, Q \in G$

Exemples.

1. Le determinant definit un homomorphisme de groupes algebriques

$$\det : \mathrm{Gl}_n \to \mathbb{G}_m$$

2. La multiplication par n sur une courbe elliptique

$$[n] : E \to E$$

est un morphisme de groupes algebriques; plus generalement une isogenie $E_1 \to E_2$ de courbes elliptiques est un morphisme de groupes algebriques.

Soit G un groupe algebrique sur K , un sous groupe H de G est une sous-variete de G qui est stable pour e, m, i .

La composante connexe de O dans G est un sous-groupe algebrique; on le note G^0, c' est un sous-groupe normal d'indice fini

Un sous-groupe normal N est un sous groupe stable par conjugaison i.e. $N = gNg^{-1}$ pour tout $g \in G$.

Un groupe algebrique est lisse puisque les translations $g \to gg'$ forme un groupe transitif d'automorphismes et que G possede au moins un point lisse. En particulier dans le cas des groupes algebriques les notions de connexite et d'irreductibilite coincident.

Soit $f : G \to G'$ un morphisme de groupes algebriques sur K, alors $\ker f$ est un sous groupe ferme normal, on peut montrer que $\mathrm{Im} f(G)$ est un sous-groupe ferme et $\dim G = \dim \ker f + \dim \mathrm{Im} f(G)$.

Definition. Un groupe algebrique lineaire est un sous-groupe d'un Gl_n qui est un sous-ensemble ferme de Gl_n

Exercice. Montrer que G_a est un groupe lineaire

On montre le

Theoreme. Un groupe algebrique affine connexe est un groupe lineaire

Groupes finis constants et algebre de groupes

Ici K est un corps algebriquement clos.

Soit G, un groupe fini et K^G la K-algebre des applications de G dans K, elle admet la presentation $\bigoplus_{g\in G} Ke_g$ avec les relations $e_g^2 = e_g$ et $e_g e_{g'} = 0$ pour $g \neq g'$ et enfin $\sum\limits_{g\in G} e_g = 1$ (comme application $e_g(g') = \delta_{g,g'}$).

On definit une structure d'algebre de Hopf:

la comultiplication $m^*(e_g) = \sum\limits_{g_1 g_2 = g} e_{g_1} \otimes e_{g_2}$; c'est l'application de K^G dans $K^{G\times G} \simeq K^G \otimes K^G$ induite par la multiplication dans G,

$i(e_g) = e_{g^{-1}}$ et

$e(e_g) = 1$ si g est l'element neutre de G et 0 autrement.

Le groupe algebrique ainsi defini s'appelle le groupe algebrique constant G ; on le note encore G.

On note $K[G]$ l'algebre du groupe G ; c'est le K-espace vectoriel sur les elements de G muni de la multiplication induite par celle de G ;

i) $\sum x_g.g = \sum y_g.g$ ssi $x_g = y_g$ pour tout $g \in G$

ii) $\sum x_g.g + \sum y_g.g = \sum (x_g + y_g).g$

iii) $(\sum x_g.g)(\sum y_h.h) = \sum z_t.t$ ou $t = \sum\limits_{gh=t} x_g y_h$

iv) $x(\sum x_g.g) = \sum (x x_g).g$

Dans cette algebre $1 := 1_K.1_G$, et $z := \sum x_g.g$ est inversible pour la multiplication si l'endomorphisme induit par la multiplication a gauche par z est inversible i.e. si le determinant $\det(x_{gh^{-1}})_{g,h}$ est non nul; il revient au meme de dire que $\det(x_{gh})_{g,h}$ est non nul.

Maintenant on considere l'anneau $K[T_g; g \in G]$ ou les T_g sont des indeterminees i.e. l'anneau de l'espace affine de dimension $n := |G|$; on le munit d'une structure "d'anneau algebrique" par

1. une co-addition: $a^*(T_g) = T_g \otimes 1 + 1 \otimes T_g$ qui induit $\mathbb{G}_a^n$ i.e. l'addition de $K[G]$

2. une co-multiplication: $m^*(T_g) = \sum_{g_1 g_2 = g} T_{g_1} \otimes T_{g_2}$ qui induit la multiplication de $K[G]$ (en effet si l'on considere les 2 points $(x_g), (y_h)$ de l'espace affine $\mathbb{A}_K^n$, ils correspondent a l'homomorphisme $K[T_g] \otimes K[T_h] \to K$ qui specialise T_g en x_g et T_h en x_h ; ce qui induit un homomorphisme $K[T_t] \to K[T_g] \otimes K[T_h] \to K$ dont le noyau correspond au point $(z_t = \sum_{gh=t} x_g y_h)$.

On definit ainsi un groupe algebrique muni d'une addition et d'une multiplication qui “represente” l'algebre de groupe $K[G]$; on le note $A(G)$.

Soit $\det(T_{gh}) \in K[T_g]$, le determinant de la matrice $(T_{gh})_{g,h \in G}$ et $U(G)$ l'ouvert principal $D_{(\det(T_{gh})}$ de $A(G)$; sur $U(G)$ on peut definir un inverse par $i(T_g) = \dfrac{1}{\det(T_{gh^{-1}})} \sum_{g \in G} m_{ge} T_g$ ou m_{gh} est le mineur a la position g, h de la matrice $(T_{gh^{-1}})$ et l'element neutre donne par $e(T_g) = T_g$; $U(G)$ est un groupe algebrique irreductible qui “represente” les unites de l'algebre de groupe $K[G]$.

L'injection canonique $G \to U(G)$ est representee par l'homomorphisme $K[T_g, g \in G, 1/\det(T_{gh})] \to K^G$ defini par $T_g \to e_g$ (il faut montrer que l'element $\det(e_{gh})$ est inversible dans K^G ; pour cela on peut utiliser la formule du determinant: $\det(e_{gh}) = \sum_\sigma \epsilon(\sigma) e_{g_1 g_{\sigma(1)}} e_{g_2 g_{\sigma(2)}} \ldots e_{g_n g_{\sigma(n)}}$ ou l'on a indicie les elements de G de 1 a n ; puisque les e_i sont des idempotents orthogonaux il suit que seuls subsistent les termes qui correspondent aux permutations σ telles que $g_1 g_{\sigma(1)} = g_2 g_{\sigma(2)} = \ldots = g_n g_{\sigma(n)}$ i.e. $g_{\sigma(i)} = g_i^{-1} g_1 g_{\sigma(1)}$. Fixons $g_\sigma(1) = h$, cela determine alors une seule permutation $\tilde{h}$ qui satisfait les relations precedentes et donc $\det(e_{gh}) = \sum_{h \in G} \epsilon(\tilde{h}) e_{g_1 h}$ qui est bien un inversible puisque son carre fait 1 . L'injection $G \to U(G)$ est par construction un morphisme de groupes algebriques et la multiplication a gauche par $g \in G$ sur $A(G)$ ou $U(G)$ est representee par l'automorphisme g^* de $K[T_g]$ ou $K[T_g, 1/\det(T_{gh})]$; $T_h \to T_{g^{-1}h}$ (on a bien ainsi $m((\delta_{g,h}), (x_h)) = (z_t)$ ou $z_t = \sum_{h,\ gh=t} \delta_{g,h} x_h = x_{g^{-1}t}$). On note $U(G)/G$ la variete affine quotient.

Par exemple si $G = \{1\}$ alors $U(G) = \mathbb{G}_m$.

Si l'on ne suppose plus K algebriquement clos; la construction precedente sur K^a est clairement definie sur K . On a alors:

Proposition. Soit G un groupe fini et L/K une extension galoisienne de groupe de Galois G ; il existe un carre cartesien:

$$\begin{array}{ccc} \mathrm{Spec} L & \to & U(G) \\ \downarrow & & \downarrow \\ \mathrm{Spec} K & \to & U(G)/G \end{array}$$

Preuve: Par le theoreme de la base normale il existe $x \in L$ tel que les $g(x),\ g \in G$ forment une base de L/K . On definit un homomorphisme de K -algebres $\gamma : K[G]_{(\det(T_{gh}))} \to L$ par $\gamma(T_g) = g(x)$. Alors γ est G -equivariant d'ou le carre cartesien.

Isogenies

Definition. Une isogenie est un homomorphisme de groupes algebriques sur K qui est surjectif et a noyau fini.

Dans le cas ou G est un groupe abelien on a donc une isogenie universelle

$$1 \to G \to U(G) \to U(G)/G \to 1$$

i) G est cyclique d'ordre n premier a $p := \mathrm{car} K$

L'algebre de groupe $K[G]$ est isomorphe a $K[T]/(T^n - 1)$; si K contient une racine primitive n -ieme, soit ζ , on peut decomposer $T^n - 1$ en produit de facteurs lineaires et apres changement de coordonnees affines la multiplication se diagonalise; ainsi $U(G)$ est isomorphe a $\mathbb{G}_m^n$.

On peut voir cela au niveau des algebres de Hopf; d'abord on calcule: $\det(T_{i+j}) = \prod_{0 \le i \le n-1} (\sum_{0 \le j \le n-1} \zeta^{ij} T_j)$ ou ζ est une racine primitive n -ieme de l'unite et $m^*(\sum_{0 \le i \le n-1} \zeta^{ij} T_j) = (\sum_{0 \le i \le n-1} \zeta^{ij} T_j) \otimes (\sum_{0 \le i \le n-1} \zeta^{ij} T_j)$. Si l'on pose $V_i := \sum_{0 \le i \le n-1} \zeta^{ij} T_j$; on a donc $m^*(V_i) = V_i \otimes V_i$ et
$K[T_i, 1/\det(T_{i+j})] = K[V_i, 1/\prod V_i]$ puisque $T_i := n \sum_{0 \le i \le n-1} \zeta^{ij} V_j$ et que $(n, p) = 1$ ///

Si on pose $g = 1 \in G = \mathbb{Z}/n\mathbb{Z}$; on a $g^* V_i = \zeta^i V_i$; ainsi la projection $pr : U(G) \to \mathbb{G}_m := \mathrm{Spec} K[T, 1/T]$ donnee par $T \to V_1$ est G -equivariante et si l'on designe par θ l'isogenie $\mathbb{G}_m \to \mathbb{G}_m$ definie par $\theta(z) = z^n$, on a un diagramme commutatif:

$$\begin{array}{ccc} U(G) & \xrightarrow{pr} & \mathbb{G}_m \\ \downarrow & & \downarrow \theta \\ U(G)/G & \to & \mathbb{G}_m \end{array}$$

qui montre que l'isogenie $U(G) \to U(G)/G$ est image reciproque de θ ; on retrouve ainsi la theorie de Kummer.

ii) G est cyclique d'ordre p^n ou $p := \mathrm{car} K$

On a encore $K[G] = K[T]/(T^{p^n} - 1)$; changeant T en $1 - T$, on voit que $K[G]$ est isomorphe a l'algebre $K[T]/(T^{p^n})$ des series formelles tronquees a l'ordre p^n . Si $n = 1$ nous allons montrer dans le paragraphe qui suit que $U(G) \simeq \mathbb{G}_m \times (\mathbb{G}_a)^{p-1}$; ainsi comme dans le cas Kummerien une projection sur l'un des facteurs G_a redonne l'isogenie d' Artin-Schreier. Si n est quelconque nous serons amenes a introduire les vecteurs de Witt et nous eluciderons alors la structure de $U(G)$ en terme des groupes de vecteurs Witt tronques.

Structure du groupe algebrique $U/U^{(n)}$

Soit U le groupe multiplicatif des series formelles $f(t) \in K[[t]]$ verifiant $v(f) = 0$ et soit $U^{(n)}$ le sous-groupe de U forme de celles qui verifient $v(1 - f) \ge n$; un element $f \in U^{(n)}$ se met donc sous la forme:

$$f = 1 + a_n t^n + ...$$

Les polynomes

$$f = a_0 + a_1 t + ... + a_{n-1} t^{n-1},\ a_0 \neq 0$$

forment un systeme de representants de $U/U^{(n)}$; ainsi on peut considerer $U/U^{(n)}$ comme un sous-ensemble ouvert de $\mathbb{A}_K^n$ et le munir de la loi de groupe correspondante.

Lemme. La structure algebrique precedente est compatible avec la structure de groupe de $U/U^{(n)}$. De plus elle est independante du choix de l'uniformisante t .

Preuve: Si $f = a_0 + a_1 t + ... + a_{n-1}t^{n-1}$ et $g = b_0 + b_1 t + ... + b_{n-1}t^{n-1}$ sont deux elements de $U/U^{(n)}$, leur produit h a pour representant $c_0 + c_1 t + ... + c_{n-1}t^{n-1}$, avec

$$c_i = \sum_{r+s=i} a_r b_s$$

La loi de composition est donc donnee par des formules polynomiales, ce qui montre qu'elle est partout reguliere. On verifie de meme la regularite de l'inverse et la regularite de l'operation definie par le changement de variable

$$t' = \alpha_1 t + ..., \quad \alpha_1 \neq 0$$

Soit $V_{(n)}$ le groupe $U^{[1)}/U^{(n)}$ sous-groupe de $U/U^{(n)}$ forme des representants $f = 1 + a_1 t + ... + a_{n-1}t^{n-1}$, alors

Lemme. Le groupe $U/U^{(n)}$ est isomorphe au produit de $\mathbb{G}_m$ par le groupe $V_{(n)}$

Preuve. En effet toute fonction f s'ecrit d'une facon et d'une seule comme produit d'une constante $a_0 \neq 0$ par une fonction $g \in V_{(n)}$ et cette decomposition est compatible avec la structure algebrique de $U/U^{(n)}$.

Le groupe $V_{(n)}$ est une variete biregulierement isomorphe a $\mathbb{A}_K^{n-1}$; plus precisement:

Lemme. Pour tout entier $i, 1 \leq i \leq n-1$ soit g_i une serie formelle d'ordre i (i.e. $v(g_i) = i$). Alors tout element de $V_{(n)}$ s'ecrit d'une seule maniere sous la forme d'un produit:

$$g = (1 + a_1 g_1)...(1 + a_{n-1}g_{n-1})$$

ou les a_i sont des constantes. L'application qui a g fait correspondre $(a_1, ...a_{n-1})$ est une application bireguliere de $V_{(n)}$ sur $\mathbb{A}_K^{n-1}$

Preuve en exercice.

Lemme. Le groupe algebrique $V_{(n)}$ est un groupe unipotent isomorphe au groupe des matrices de la forme

$$\begin{pmatrix} 1 & a_1 & a_2 & a_3 & ... & a_{n-1} \\ 0 & 1 & a_1 & a_2 & ... & a_{n-2} \\ 0 & 0 & 1 & a_1 & ... & a_{n-3} \\ \vdots & \vdots & \vdots & \vdots & ... & \vdots \\ 0 & 0 & 0 & 0 & ... & 1 \end{pmatrix}$$

l'isomorphisme s'obtient en faisant correspondre a t la matrice nilpotente de Jordan d'ordre n .

Structure du groupe $V_{(n)}$ en caracteristique zero.

On peut definir l'exponentielle $\exp(g) = 1 + g + ... + \dfrac{g^n}{n!} + ...$ pour toute serie formelle g dont l'ordre est > 0

Proposition. Pour tout entier $i, 1 \leq i \leq n-1$, soit g_i une serie formelle d'ordre i . Tout element $g \in V_{(n)}$ peut alors se mettre de maniere unique sous la forme de produit

$$g = \exp(a_1 g_1) ... \exp(a_{n-1}g_{n-1})$$

ou les a_i sont des constantes. L'application qui a g fait correspondre $(a_1, ..., a_{n-1})$ est un isomorphisme biregulier du groupe algebrique $V_{(n)}$ sur le groupe $(\mathbb{G}_a)^{n-1}$

Preuve: L'existence et l'unicite est elementaire et le resultat vient de la relation $\exp(g_1 + g_2) = \exp(g_1)\exp(g_2)$.

Corollaire. En caracteristique zero, le groupe $U/U^{(n)}$ est isomorphe a $\mathbb{G}_m \times (\mathbb{G}_a)^{n-1}$

Structure du groupe $V_{(n)}$ en caracteristique $p > 0$ et $n < p$.

La preuve precedente marche mutatis mutandis en considerant au lieu de l'exponentielle, l'exponentielle tronquee $\exp_n X = 1 + X + ... + \frac{X^n}{n!}$. Ainsi $V_{(n)}$ est encore isomorphe au groupe $(\mathbb{G}_a)^{n-1}$

Vecteurs de Witt.

Nous présentons les vecteurs de Witt en suivant la présentation moderne qu'ont donné Witt ([W2]) et d'autres cf. [De-Ga], [De], dans les années 60.

On fixe un nombre premier p ; nous devinons la necessite d'introduire un nouveau type d'exponentielle liee au nombre premier p

1. Les exponentielles de Artin-Hasse

Soit K un anneau; on note M_K la catégory des K -anneaux (i.e. les K -algèbres associatives unitaires avec un élément unité). On note Λ_K le K -groupe affine qui a $R \in M_K$ associe le groupe multiplicatif $\Lambda_K(R) := 1 + tR[[t]]$ des séries formelles en R de terme constant 1 . On a une filtration naturelle par les sous-groupes $\Lambda_K^{(n)}(R) = 1 + t^n R[[t]]$.

Soit $F := 1 - t + ...$ un élément fixé de $\Lambda_K(K)$; considèrons

$$\varphi : \ {\mathbb{A}_K^1}^{\mathbb{N}^+} \to \Lambda_K$$

définie par: $\varphi((a_n)) = \prod F(a_n t^n)$.

Si $K = \mathbb{Q}$, $F := \exp(-t)$; alors $F(at)F(bt) = F((a+b)t)$ ainsi φ est un isomorphisme. Si K est un corps de caractéristique $p > 0$ on ne peut pas trouver un tel F (traiter le cas $p = 2$). Par contre il est aisé de montrer par induction que pour tout F on a une formule:

$$(*) \quad F(at)F(bt) = \prod_{i>0} F(\lambda_i(a,b)t^i)$$

où $\lambda_i(X,Y) \in K[X,Y]$. On va chercher F tel que les λ_i soient nuls si i n'est pas une puissance de p puisque les problemes sont dans les exposants multiples de p . Le problème est donc de casser l'exponentielle en " p -composantes".

Considérons la fonction de Moebius μ définie par: $\mu(n) = 0$, si n est divisible par le carré d'un nombre premier et $\mu(p_1 ... p_k) = (-1)^k$, si $p_1, ..., p_k$ sont des nombres premiers distincts; enfin $\mu(1) = 1$; pour $n > 1$ on a

$$\sum_{d|n} \mu(d) = 0$$

Il suit que

$$-t = \sum_{n \geq 1} -\frac{1}{n} t^n \left(\sum_{d|n} \mu(d)\right) = \sum_{d \geq 1} \frac{\mu(d)}{d} \sum_m \left(-\frac{1}{m} t^{dm}\right) = \sum_{d \geq 1} \frac{\mu(d)}{d} \log(1 - t^d)$$

et donc

$$\exp(-t) = \prod_n (1 - t^n)^{\mu(n)/n}$$

Considérons $F(t) := \prod_{(n,p)=1} (1 - t^n)^{\mu(n)/n} = 1 - t + ... \in \Lambda(\mathbb{Z}_{(p)})$

où $\mathbb{Z}_{(p)} = S^{-1}\mathbb{Z}$ avec $S = \mathbb{Z} - p\mathbb{Z}$ **i.e. on peut prendre $k = \mathbb{Z}_{(p)}$ dans la formule (*).**

Puisque $\mu(n) \neq 0$ implique que p^2 ne divise pas n ; il suit que: $\exp(-t) = F(t)/F(t^p)^{1/p}$ ainsi $F(t) = \exp L(t)$ avec

$$L(t) = -(t + \frac{t^p}{p} + \frac{t^{p^2}}{p^2} + ... + \frac{t^{p^i}}{p^i} + ...)$$

Alors $\lambda_i \in \mathbb{Z}_{(p)}[X, Y]$. En regardant cette formule pour $R = \mathbb{Q}$, il suit que $\lambda_i = 0$ pour $i \notin p^{\mathbb{N}}$; ainsi

$$(1) \quad F(at)F(bt) = \prod_{i \geq 0} F(\Psi(a, b)t^{p^i})$$

L'exponentielle d'Artin-Hasse est le morphisme

$$E : {\mathbb{A}^1_{\mathbb{Z}_{(p)}}}^{\mathbb{N}} \to \Lambda_{\mathbb{Z}_{(p)}}$$

défini par

$$(2) \quad E((a_0, ...,), t) = \prod_{n \geq 0} F(a_n t^{p^n}).$$

De (1) il suit facilement qu'il existe $S_i \in \mathbb{Z}_{(p)}[X_0, ...X_i, Y_0, ..., Y_i]$ tels que

$$E((a_i), t)E((b_i), t) = E((S_i(a_0, ..., a_i, b_0, ..., b_i)), t)$$

Il suit de (2) que pour R une $\mathbb{Z}_{(p)}$ -algebre tout $P \in \Lambda(R)$ s'ecrit de maniere unique sous la forme

$$P(t) = \prod_{(n,p)=1} E(\vec{a}_n, t^n)$$

avec $\vec{a}_n \in R^{\mathbb{N}}$.

Anneaux de Witt sur $\mathbb{Z}$

On a

$$(3) \quad E((a_0, ...,), t) = \exp(-\sum_{n \geq 0} t^{p^n} \Phi_n / p^n)$$

avec $\Phi_n(a_0, ...) = a_0^{p^n} + p a_1^{p^{n-1}} + ...p^n a_n$ et

$$(4) \quad \Phi_n(a_0, ..., a_n) + \Phi_n(b_0, ..., b_n) = \Phi_n(S_0, ..., S_n)$$

Lemme. $S_n \in \mathbb{Z}[X_0, ..., X_n, Y_0, ..., Y_n]$

Nous avons vu que les coefficients sont dans $\mathbb{Z}_{(p)}$; mais il suit facilement de (4) que les coefficients sont dans $\mathbb{Z}[p^{-1}]$. Le lemme suit alors de $\mathbb{Z}_{(p)} \cap \mathbb{Z}[p^{-1}] = \mathbb{Z}$.

Exercice: $S_0(X_0, Y_0) = X_0 + Y_0$, $S_1(X_0, X_1, Y_0, Y_1) = X_1 + Y_1 + \frac{X_0^p + Y_0^p - (X_0 + Y_0)^p}{p}$ ∎

Theoreme. Il y a une unique loi de groupe commutatif sur ${\mathbb{A}^1_{\mathbb{Z}}}^{\mathbb{N}}$ satisfaisant les deux proprietes equivalentes suivantes:

i) $E : {\mathbb{A}^1_{\mathbb{Z}}}^{\mathbb{N}} \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)} \to \Lambda_{\mathbb{Z}_{(p)}}$ est un homomorphisme

ii) Chaque $\phi_n : {\mathbb{A}^1_{\mathbb{Z}}}^{\mathbb{N}} \to \mathbb{G}_{a,\mathbb{Z}}$ est un homomorphisme

Preuve. Cela revient à voir que l'on définit une loi de groupe commutatif via les formules

$$(a_0, a_1, ..., a_n, ...) \oplus (b_0, b_1, ..., b_n, ...) =$$

$$(S_0(a_0, b_0), S_1(a_0, a_1, b_0, b_1), ..., S_n(a_0, ..., a_n, b_0, ..., b_n), ...)$$

d'élément unité $(0, 0, ...)$. L'associativité, la commutativité et la propriété qui définit l'élément neutre s'expriment par des identités polynomiales à coefficients dans $\mathbb{Z}$ et les coefficients des S_i. Ces identités sont satisfaite après changement de base à $\mathbb{Z}[p^{-1}]$ à cause de (4) et puisque $\Phi_n : {\mathbb{A}^1_{\mathbb{Z}[p^{-1}]}}^{\mathbb{N}} \to {\mathbb{A}^1_{\mathbb{Z}[p^{-1}]}}^{\mathbb{N}}$ est un isomorphisme cela suffit puisque $\mathbb{Z} \subset \mathbb{Z}[p^{-1}]$. Si $p \neq 2$ on a $\Phi_n(-X_0, -X_1, ...) = -\Phi_n(X_0, X_1, ...)$; il suit que l'opposé de (a_n) est $(-a_n)$. Pour $p = 2$; l'opposé est défini par des polynômes à coefficents dans $\mathbb{Z}_{(p)} \cap \mathbb{Z}[p^{-1}] = \mathbb{Z}$. Le $\mathbb{Z}$-schéma ${\mathbb{A}^1_{\mathbb{Z}}}^{\mathbb{N}}$ muni de la loi de groupe construite au-dessus s'appelle le $\mathbb{Z}$-groupe de Witt de longueur infinie relatif à p ; on le note W.

Remarque: La preuve du théorème montre que si l'on inverse p, la loi de groupe se linéarise après changement de coordonnées.

Exercice. Si $p = 2$, montrer que $\ominus(X_0, X_1, ...) = (-X_0, -X_1 - X_0^2, -X_2 - X_0^4 - X_0^2 X_1 - X_1^2, ...)$

Si $w = (a_n) \in W(R) = R^{\mathbb{N}}$, a_n est la n-ieme composante de w et $\Phi_n(w)$ la n-ieme composante fantôme de w.

Soit $T : W \to W$, le monomorphisme défini par

$$T(a_0, a_1, ...) = (0, a_0, a_1, ...)$$

alors $\Phi_0(Tw) = 0, \Phi_n(Tw) = p\Phi_{n-1}(w), \quad n \geq 1$; il suit que T est un homomorphisme de groupe appelé décalage (Vershiebung en allemand).

On définit le groupe W_n des vecteurs de Witt de longueur n par la suite exacte de foncteurs de groupes

$$0 \to W \xrightarrow{T^n} W \xrightarrow{R_n} W_n \to 0$$

i.e. $W_n(R) = \mathrm{Coker} T^n(R)$ pour tout R. On a

$$(a_0, a_1, ...) = (a_0, ..., a_{n-1}, 0, ...) \oplus T^n(a_n, a_{n+1}, ...)$$

ce qui signifie qu'en tant que schéma W_n est ${\mathbb{A}^1_K}^n$, le morphisme de projection $W \to W_n$ étant $(a_0, ...) = (a_0, ..., a_{n-1})$. La loi de groupe sur W_n est

$$(a_0, ..., a_{n-1}) \oplus (b_0, ..., b_{n-1}) =$$

$$(S(a_0, b_0), ..., S_{n-1}(a_0, ..., a_{n-1}, b_0, ..., b_{n-1}))$$

. En particulier $W_1 = \mathbb{G}_a$. On note $R : W_{n+1} \to W_n$ la projection telle que $R(a_0, ..., a_n) = (a_0, ..., a_{n-1})$; on a alors une suite exacte

$$0 \to W_m \xrightarrow{T^n} W_{n+m} \xrightarrow{R^m} W_m \to 0$$

De plus les projections $W \to W_n$ induisent un isomorphisme $W = \varprojlim W_n$. Soit $\tau : \mathbb{A}^1_{\mathbb{Z}} \to W$ le morphisme défini par $a \to (a, 0, 0, ...)$; on a $\Phi_n \tau(a) = a^{p^n}$ et $E(\tau(a), t) = F(at)$

Théoreme. Il y a une unique structure d'anneau sur le $\mathbb{Z}$ -groupe W telle que l'une des deux propriétés suivantes soient satisfaites:

i) Chaque $\Phi_n : W \to \mathbb{G}_{a,\mathbb{Z}}$ est un homomorphisme d'anneaux

ii) $\tau(ab) = \tau(a)\tau(b)$ pour tout $a, b \in R$ une $\mathbb{Z}$ -algèbre.

Preuve: Si l'on inverse p ; $(\Phi_n) : W \otimes_{\mathbb{Z}} \mathbb{Z}[p^{-1}] \to {\mathbb{G}_{a,\mathbb{Z}[p^{-1}]}}^{\mathbb{N}}$ est un isomorphisme, d'ou l'existence et l'unicité de la structure d'anneau sur $W \otimes_{\mathbb{Z}} \mathbb{Z}[p^{-1}]$ satisfaisant i) et puisque $\Phi_n(\tau(a) = a^{p^n}$ la relation ii) est satisfaite.

Inversement considérons une structure d'anneau sur ${\mathbb{A}^1_{\mathbb{Z}[p^{-1}]}}^{\mathbb{N}}$ telle que $(a^{p^n}).(b^{p^n}) = ((ab)^{p^n})$; la multiplication est donnée par des polynômes $(x_n).(y_n) = (\sum a^{(n)}_{i,j} x_i y_j)$ avec $\sum a^{(n)}_{i,j} a^{p^i} b^{p^j} = (ab)^{p^n}$; il suit que $(x_n).(y_n) = (x_n y_n)$.

La multiplication dans $W \otimes_{\mathbb{Z}} \mathbb{Z}[p^{-1}]$ est donnée par des polynômes $M_n(X_0, ...X_n, Y_0, ..., Y_n) \in \mathbb{Z}[p^{-1}][X_0, ...X_n, Y_0, ..., Y_n]$ tels que

$$(a_0, ..., a_n) \odot (b_0, ..., b_n) = (M_n(a_0, ...a_n, b_0, ..., b_n))$$

Par définition $\Phi_i((M_n)) = \Phi_i((X_n)).\Phi_i((Y_n))$; le lemme suivant montre que $M_n \in \mathbb{Z}[X_0, ...X_n, Y_0, ..., Y_n]$.

Lemme. Comme les relations algébriques qui traduisent la structure d'anneau sont à coefficients dans $\mathbb{Z}$ et satisfaites lorsque l'on rend p inversible; elles sont satifaite.

Le $\mathbb{Z}$ -anneau W est appelé l'anneau des vecteurs de Witt. Les morphismes de projection $R_n : W \to W_n$ et $R : W_{n+1} \to W_n$ sont des homomorphismes d'anneaux.

L'anneau de Witt sur le corps k

Dans ce paragraphe k désigne un corps de caractéristique p . On désigne par $W_k, W_{n,k}$ les k -anneaux $W \otimes_{\mathbb{Z}} k$ resp. $W_n \otimes_{\mathbb{Z}} k$; remarquez que la composante fantôme devient $(a_n) \to a_0^{p^n}$. On définit le morphisme de Frobenius $F : W_k \to W_k$ par $F(a_0, ..., a_n, ...) = (a_0^p, ..., a_n^p, ...)$; c'est un homomorphisme d'anneaux.

Proposition. Soit R une k -algèbre si $x = (a_0, ..., a_n, ...) \in W_k(R)$ alors $px = x \oplus x \oplus .... \oplus x = (0, a_0^p, ..., a_n^p, ...)$

Preuve: Dans l'anneau W on a,

$$px = x \oplus x \oplus .... \oplus x = (P_0(a_0), P_1(a_0, a_1), ..., P_n(a_0, a_1, ..., a_n), ...)$$

où $P_n(X_0, X_1, ..., X_n) \in \mathbb{Z}[X_0, ..., X_n]$ et

$$p\Phi_n(a_0, ..., a_n) = \Phi_n(P_0(a_0), P_1(a_0, a_1), ..., P_n(a_0, a_1, ..., a_n))$$

La proposition revient à montrer les congruences $P_0(X_0) \equiv 0 \bmod p$ et pour $n > 0$ $P_n(X_0, X_1, ..., X_n) \equiv X_{n-1}^p \bmod p$.

Montrons cela par récurrence sur n . On a $P_0(X_0) = pX_0$ et supposons pour $1 < i < n$ que $P_i = X_{i-1}^p + pR_i$ avec $R_i \in \mathbb{Z}[X_0, ..., X_i]$ alors

$$(*) \quad p(X_0^{p^n} + pX_1^{p^{n-1}} + ... + p^n X_n) = P_0^{p^n} + pP_1^{p^{n-1}} + ... + p^n P_n$$

On remarque que $(X+pY)^{p^i} = X^{p^i} \mathrm{mod} p^{i+1}$, ainsi

$$P_{n-i}^{p^i} = (X_{n-i-1}^p + pR_{n-i})^{p^i} \equiv X_{n-i-1}^{p^{i+1}} \mathrm{mod} p^{i+1}$$

et donc $p^{n-i}P_{n-i}^{p^i} \equiv p^{n-i}X_{n-i-1}^{p^{i+1}} \mathrm{mod} p^{n+1}$ et donc (*) vue modulo p^{n+1} donne la congruence $P_n(X_0, X_1, ..., X_n) \equiv X_{n-1}^p \mathrm{mod} p$.

Remarque. On a donc la relation dans W_k ; $FV = VF = p\mathrm{Id}$ (V est le décalage ou Verschiebung)

Corollaire. Supposons k parfait, alors $W(k)$ est un anneau de valuation discrète complet et $W(k)/pW(k) = k$.

Preuve: On a $FW(k) = W(k)$ puisque k est parfait ainsi; $p^nW(k) = V^nF^nW(k) = V^nW(k)$ et $W(k) = \varprojlim W(k)/p^nW(k)$ de plus
$W(k)/pW(k) = W_1(k) = \mathbb{G}_a(k) = k.$

Proposition. Supposons k parfait, soit A un anneau noethérien local complet à corps résiduel k . Soit $\pi : A \to k$ la projection canonique; alors il existe un unique homomorphisme d'anneaux $u : W(k) \to A$ compatible avec les projections $W(k) \to k$ et π .

Si de plus A est un anneau de valuation discrète complet avec $p.1_A \neq 0$, alors A est un $W(k)$ -module libre de rang $[A/pA : k]$; en particulier si pA est l'idéal maximal de A , alors u est un isomorphisme.

Preuve. Notons m_A l'ideal maximal de A Supposons avoir construit $u : W(k) \to A$ un homomorphisme qui satisfait la proposition; alors $\tau' := u\tau : k \to A$ est compatible avec la multiplication et $\pi\tau' = \mathrm{Id}$ un tel τ' est unique puisque $\tau'(\alpha) \in \cap(\pi^{-1}(\alpha^{p^{-n}}))^{p^n}$ qui n'a qu'un element (en effet si $a = x^{p^n}$ et $b = y^{p^n}$ on montre en utilisant la formule du binome et par recurrence sur n que $a \equiv b \ \mathrm{mod} m_A^{n+1}$). D'autre part, tout $x \in W(k)$ peut s'ecrire:

$$x = (\alpha_0, \alpha_1, ...) = (\alpha_0, 0, 0, ...) \oplus (0, \alpha_1, 0, ...) \oplus (0, 0, \alpha_2, 0, ...) \oplus ... =$$

$$\tau(\alpha_0) \oplus p\tau(\alpha_1^{1/p}) \oplus p^2\tau(\alpha_2^{1/p^2}) \oplus ....$$

et $u(x)$ doit etre

$$\tau'(\alpha_0) \oplus p\tau'(\alpha_1^{1/p}) \oplus p^2\tau'(\alpha_2^{1/p^2}) \oplus ....$$

, d'ou l'unicite de u .

On peut maintenant construire u en s'inspirant de la formule precedente. Pour cela considerons l'homomorphisme d'anneaux donne par les composantes fantomes $\Phi_n : W_{n+1} \to A$. Si $x_i \in m_A$ alors $\Phi_n((x_n)) \in m_A^{n+1}$ ce qui induit un diagramme commutatif

$$\begin{array}{ccc} W_{n+1}(A) & \xrightarrow{\Phi_n} & A \\ W_{n+1}(\pi) \downarrow & & \downarrow can. \\ W_{n+1}(k) & \xrightarrow{\tilde{\Phi}_n} & A/m_A^{n+1} \end{array}$$

Soit $\sigma : k \to k$ l'automorphisme donne par $\sigma(x) = x^{1/p}$ et soit
$u_n := \tilde{\Phi}_n \circ W_{n+1}(\sigma^n)$; alors si $a_0, ..., a_n \in A$

$$u_n(\pi(a_0^{p^n}), ..., \pi(a_n^{p^n})) = a_0^{p^n} + pa_1^{p^{n-1}} + ... + p^n a_n \ \mathrm{mod} m_A^{n+1}$$

ceci montre que

$$u := \varprojlim u_n \quad W(k) \to A$$

est un homomorphisme d'anneaux.

Pour le reste de la proposition considerons $a_1, ..., a_e$ une base de A modulo pA ; elle engendre le $W(k)$ -module A . Ainsi A est un $W(k)$ module de type fini sans torsion puisque $p^n.1_A \neq 0$ et donc libre de rang $[A/pA : k]$.

Exemple. Si $k = \mathbb{F}_p$ la proposition precedente montre que $W(\mathbb{F}_p) = \mathbb{Z}_p$ et si $k = \mathbb{F}_p^a$ alors $W(\mathbb{F}_p^a) = \mathbb{Z}_p^{nr}$

L'isogenie d'Artin-Schreier-Witt

Ici le corps de base est le corps fini $\mathbb{F}_p$ et on note W_n le schema de Witt tronque sur $\mathbb{F}_p$.

Comme dans le cas de $\mathbb{G}_a$ on note $\wp = \mathrm{F} - \mathrm{Id}$ le morphisme de groupes algebriques

$$W_n \xrightarrow{\wp} W_n$$

defini par

$$\wp(x_0, x_1, ..., x_{n-1}) =$$

$$(x_0^p, x_1^p, ..., x_{n-1}^p) \ominus (x_0, x_1, ..., x_{n-1}) = (x_0^p - x_0, x_1^p - x_1 + c(x_0^p, -x_0), ...)$$

ou $c(x, y) = \dfrac{x_0^p + y_0^p - (x_0 + y_0)^p}{p}$ le noyau est donc l'ensemble des points $(x_0, x_1, ..., x_{n-1})$ fixes par le Frobenius i.e. $W_n(\mathbb{F}_p) = \mathbb{Z}/p^n\mathbb{Z}$, d'ou la suite exacte pour tout corps K de caracteristique $p > 0$.

$$(*) \quad 0 \to \mathbb{Z}/p^n\mathbb{Z} \to W_n(K^s) \xrightarrow{\wp} W_n(K^s) \to 0$$

Theoreme.(Hilbert 90) Soit $G_K := \mathrm{Gal}(K^s/K)$ alors

$$\mathrm{H}^1(G_K, W_n(K^s)) = 0$$

Cela se montre par recurrence sur n ; en effet on a une suite exacte

$$0 \to W_n \to W_{n+1} \to W_1 \to 0$$

ainsi $\mathrm{H}^1(G, W_n(K^s)) \to \mathrm{H}^1(G, W_{n+1}(K^s))\mathrm{H}^1(G, W_1(K^s))$ ///

En ecrivant la suite exacte de cohomologie correspondant a $(*)$, et en tenant compte de ce que

$$H^1(G_K, W_n(K^s)) = 0$$

on obtient

$$W_n(K) \xrightarrow{\wp} W_n(K) \to \mathrm{H}^1(G_K, \mathbb{Z}/p^n\mathbb{Z}) \to 0$$

En d'autres termes, le groupe $Hom\,(G_K, \mathbb{Z}/p\mathbb{Z})$ des homomorphismes continus de G_K dans $\mathbb{Z}/p^n\mathbb{Z}$ est isomorphe a $W_n(K)/\wp(W_n(K))$ et l'iso-morphisme en question fait correspondre a

$$\vec{a} := (a_0, a_1, ..., a_{n-1}) \in W_n(K)$$

l'homomorphisme

$$\varphi_{\vec{a}} : G_K \to \mathbb{Z}/p^n\mathbb{Z}$$

defini de la maniere suivante: on resout le systeme d'equations

$$\wp(\vec{x}) = \vec{a}$$

ou $\vec{x} := (x_0, x_1, ..., x_{n-1})$ ainsi

$$(x_0^p, x_1^p, ..., x_{n-1}^p) \ominus (x_0, x_1, ..., x_{n-1}) = (a_0, a_1, ..., a_{n-1})$$

et l'on pose $s(\vec{x}) = \vec{x} \oplus \varphi_{\vec{a}}(s)$. Notez que $\varphi_{\vec{a}}$ est surjective ssi l'équation $x_0^p - x_0 = a_0$ est irréductible sur K ; de plus les problemes de plongements dans une extension p^n -cycliques sont resolubles.

Structure du groupe $U/U^{(n)}$ en caracteristique $p > 0$

Nous allons comme promis devicer la structure de $V_{(n)}$; on note $E(\vec{a}_n, t)$ l'exponentielle de Hasse. Vues les proprietes de l'exponantielle E , il suffit de traduire la preuve (p.24) vue en caracteristique 0 .

On a donc la

Proposition. Pour tout i premier a p et $\geq n-1$, soit r_i le plus petit entier r tel que $p^r \geq n/i$; et soit g_i une serie formelle d'ordre i . Alors tout element $g \in V_{(n)}$ peut se mettre de maniere unique sous forme de produit

$$g = \prod_{(i,p)=1,\ 1 \leq i \leq n-1} E(\vec{a}_i, g_i)$$

ou les $\vec{a}_i$ sont des vecteurs de Witt de longueur r_i . L'application qui a g , fait correspondre les $\vec{a}_i$ est un isomorphisme birregulier du groupe $V_{(n)}$ sur le produit des groupes de Witt W_{r_i}

Corollaire. En caractreristique $p > 0$, le groupe local $U/U^{(n)}$ est isomorphe au produit de $\mathbb{G}_m$ par des groupes de Witt.

En particulier reprenant les notations du debut de E); dans le cas de $G = \mathbb{Z}/p^n\mathbb{Z}$ et en caracteristique $p > 0$ nous voyons que le groupe algebrique $U(G)$ est isomorphe a $\mathbb{G}_m \times V_{(p^n)}$ et $V_{(p^n)}$ est isomorphe a un produit de groupes W_{r_i} ou tous les r_i sont $< n$ sauf un qui vaut n . La projection sur ce dernier facteur induit alors un diagramme commutatif

$$\begin{array}{ccc} U(\mathbb{Z}/p^n\mathbb{Z}) & \to & W_n \\ \downarrow & & \wp\downarrow \\ U(\mathbb{Z}/p^n\mathbb{Z})/\mathbb{Z}/p^n\mathbb{Z} & \to & W_n \end{array}$$

On retrouve ainsi l'universalite de la suite d'Artin-Schreier-Witt.

F) Extensions generiques et probleme de Noether.

CHAPITRE II
Theorie de Galois des courbes algebriques

Dans ce chapitre k designe un corps de caractéristique $p \geq 0$ et k^a une cloture algebrique de k . Soit C/k une courbe algebrique lisse et connexe et $\overline{C}$ sa compactification; on note $S := \overline{C} - C$ et $K := k(C)$ le corps de fonctions de la courbe C/k . Nous nous proposons d'etudier plus particulierement les extensions abeliennes (finies ou infinies) de K non ramifiees en dehors de S (S est eventuellement vide . C'est volontairement que nous nous placons dans le cadre "restrictifs" des corps de fonctions; cela va nous permettre d'utiliser les resultats vus au chapitre I et nous eviter d'introduire de nouvelles theories cohomologiques.

A. Theorie de Kummer

Soit $p \geq 0$ la carcteristique de k et n un entier premier a p .

L'isogenie de Kummer

$$1 \to \mu_n \to \mathbb{G}_m \to \mathbb{G}_m \to 1$$

est universelle pour les extensions Galoisiennes de groupe $\mathbb{Z}/n\mathbb{Z}$ ($1 \in \mathbb{Z}/n\mathbb{Z}$ est identifie a une racine primitive n -ieme de l'unite). Soit $U \subset C$ un ouvert affine de la courbe algebrique C et $A := \mathcal{O}_C(U)$ la k -algebre des fonctions regulieres sur U . On note $H(U)$ le sous-ensemble de $\mathrm{H}^1(G_K, \mu_n(K)) = Hom\,(G_K, \mu_n(K))$ qui induit des extensions de K non ramifiees au-dessus de U ; puisque le compositum de deux extensions non ramifiees au-dessus de U est encore non ramifiee au-dessus de U , il suit que $H(U)$ herite d'une stucture de groupe; on le note $\mathrm{H}^1(U_{et}, \mu_n)$. Plus generalement cette definition "faisceautique" permet de definir $\mathrm{H}^1(C_{et}, \mu_n)$ meme dans le cas ou C est complete; les elements de $\mathrm{H}^1(C_{et}, \mu_n)$ s'appellent des μ_n torseurs sur C parcequ'il s'agit des revetements galoisiens de C de groupe $\mathbb{Z}/n\mathbb{Z}$ munis d'une action de Galois pointee. On peut donner une interpretation de $\mathrm{H}^1(C_{et}, \mu_n)$ en termes de faisceaux inversibles.

Proposition. Le groupe $\mathrm{H}^1(C_{et}, \mu_n)$ s'identifie a l'ensemble (modulo isomorphisme) des paires (L, Φ) ou L est un faisceau inversible sur C et $\Phi : \mathcal{O}_C \to L^{\otimes n}$ est un isomorphisme.

Preuve: Fixons $\theta \in k$, une racine primitive n -ieme de l'unite. Par definition un μ_n -torseur sur C est donne sur un recouvrement affine U_i de C par des algebres $B_i \simeq \mathcal{O}_C(U_i)[T_i]/(T_i^n - a_i)$ munies d'une action de Galois qui fixe l'action sur l'indeterminee T_i via l'homomorphisme $\chi : G_K \to \mathbb{Z}/n\mathbb{Z}$; precisement l'action de $1 \in \mathbb{Z}/1\mathbb{Z}$ est $T_i \to \theta T_i$; de plus B_i est etale sur $\mathcal{O}_C(U_i)$ i.e. $a_i \in \mathcal{O}_C(U_i)^*$ et la condition de recollement est donnee pour $i \neq j$ par $\dfrac{a_i}{a_j} \in \mathcal{O}_C(U_i \cap U_j)^{*n}$. Le faisceau L est le faisceau inversible defini par $L(U_i) := \mathcal{O}_C(U_i)T_i \in K^s$ et l'isomorphisme $\Phi : \mathcal{O}_C \to L^{\otimes n}$ est donne localement $\Phi(U_i)(1) = T_i^n = a_i \in \mathcal{O}_C(U_i)^*$.

Reciproquement a la donnee de (L, Φ) ou L est un faisceau inversible sur C et $\Phi : \mathcal{O}_C \to L^{\otimes n}$ un isomorphisme, on associe le μ_n -torseur sur C , $Y := \mathrm{Spec} B$ ou B est la $\mathcal{O}_C$ -algebre coherente $\oplus_{0 \leq i \leq n-1} L^{\otimes i}$ ou la multiplication est donnee par:

$$L^{\otimes i} \otimes L^{\otimes j} \xrightarrow{can} L^{\otimes (i+j)}, \quad i + j \leq n - 1,$$

$$L^{\otimes i} \otimes L^{\otimes j} \xrightarrow{can} L^{\otimes (i+j)} = L^{\otimes (n-(n-i-j))} \xrightarrow{\Phi^{-1} \otimes 1} L^{\otimes (i+j-n)}, \quad i + j \geq n.$$

Ainsi

Proposition. L'isogenie de Kummer donne naissance a une suite exacte de groupes:

$$1 \to \mu_n(\Gamma(C, \mathcal{O}_C)) \to \Gamma(C, \mathcal{O}_C)^* \xrightarrow{n} \Gamma(C, \mathcal{O}_C)^* \to \mathrm{H}^1(C_{et}, \mu_n) \to Pic(C) \xrightarrow{n} Pic(C)$$

ou n designe le morphisme induit par $x \to x^n$

On remarquera que $Pic(C) \simeq H^1(C_{Zar}, \mathcal{O}_C^*)$ et $\mathbb{G}_m(\mathcal{O}_C) = \mathcal{O}_C^*$; ce qui suggere que pour une theorie cohomologique adequate cette suite est la longue suite exacte deduite de l'isogenie de Kummer.

Nous allons examiner les consequences dans les cas ou C est affine ou bien complete.

Proposition. Soit C/k une courbe algebrique lisse connexe et $\overline{C}$ sa compactification; on note g le genre de $\overline{C}$ et s le cardinal de $S := \overline{C} - C$. Alors si

$$s = 0, \quad \mathrm{H}^1(C_{et}, \mu_n) \simeq (\mathbb{Z}/n\mathbb{Z})^{2g}$$

et si

$$s \geq 1, \quad \mathrm{H}^1(C_{et}, \mu_n) \simeq (\mathbb{Z}/n\mathbb{Z})^{2g+s-1}.$$

Preuve: Considerons d'abord le cas ou $s = 0$ et $g > 0$. Alors $\Gamma(C, \mathcal{O}_C) = k$ et donc $\mathrm{H}^1(C_{et}, \mu_n)$ s'identifie avec le groupe des points de n torsion $Pic(C)_n$ de $Pic(C)$ qui est aussi le groupe des points de n torsion de $Pic^0(C)$. Puisque $Pic^0(C) \simeq Jac(C)$ le resultat vient alors de la structure du groupe des points de n torsion d'une une variete abelienne sur k pour $(n, p) = 1$ (cf. Mumford, Abelian varieties).

Dans le cas ou $s > 0$; les choses sont moins evidentes puisque les termes de la suite exacte:

$$1 \to \Gamma(C, \mathcal{O}_C)^*/\Gamma(C, \mathcal{O}_C)^{*n} \to \mathrm{H}^1(C_{et}, \mu_n) \to Pic(C)_n \to 1$$

ne sont en general pas aises a calculer. Par exemple pour calculer $Pic(C)_n$ on a une suite exacte

$$\mathbb{Z}^s \xrightarrow{\alpha} Pic(\overline{C}) \xrightarrow{res} Pic(C)$$

induite par la restriction des faisceaux de $\overline{C}$ a C ; l'application α est ainsi definie: soit $\overline{C} - C := \{x_i,\ 1 \leq i \leq s\}$ alors $\alpha((n_i)_{n_i \in \mathbb{Z}})$ est la classe du diviseur $\sum\limits_{1 \leq i \leq s} n_i x_i$. Le noyau de α correspond aux diviseurs a support dans les s points de $\overline{C} - C := \{x_i,\ 1 \leq i \leq s\}$ lineairement equivalent a 0 , ce qui s'ecrit $\sum\limits_{1 \leq i \leq s} n_i = 0$ et $\sum\limits_{1 \leq i \leq s} n_i \Phi(x_i) = 0$ dans $Jac(X)$. Ainsi $\ker \alpha = 0$ pour $n = 1$ et pour $n > 1$ en general les points $\Phi(x_i) \in Jac(X)$ ne sont pas $\mathbb{Z}$ independants (regarder le cas des tores complexes).

Il faut donc un argument fort pour conclure. Dans le cas $s = 0$, la proposition exprime le fait que le revetement etales abelien maximal d'exposant n est image reciproque de l'isogenie

$$Pic(C)^0 \xrightarrow{n} Pic(C)^0$$

Dans le cas ou $k = \mathbb{C}$, cela montre que les revetements topologiques de C de groupe $\mathbb{Z}/n\mathbb{Z}$ sont en bijection avec les revetements etales de C ; c'est un cas particulier des theoremes GaGa (cf. Serre Topics in Galois theory).

Dans le cas $s > 0$, Rosenlicht a introduit les jacobiennes generalisees; elles remplissent le meme role que remplissent les jacobiennes dans le cas complet (cf. Serre Groupes algebriques et corps de classes). On peut prouver ainsi la proposition. Une autre voie plus riche est de construire une theorie du groupe fondamental algebrique sur les vecteur de Witt (c'est un pont entre les caracteristiques p et 0); on arrive en caracteristique 0 les theoremes GaGa de Serre permettent alors d'utiliser les resultats transcendants connus dans le cadre des surfaces de Riemann non compactes.

B. Theorie d'Artin-Schreier-Witt

Soit $p > 0$ la carcteristique de k .

L'isogenie d'Artin-Schreier

$$0 \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{G}_a \xrightarrow{\wp} \mathbb{G}_a \to 0$$

induit pour tout ouvert affine U de C une suite exacte

$$0 \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{G}_a(\mathcal{O}_C(U)) \xrightarrow{\wp} \mathbb{G}_a(\mathcal{O}_C(U))$$

qui est le debut d'une longue suite exacte; plus precisement:

Proposition. L'isogenie d'Artin-Schreier donne naissance a une suite exacte de groupes:

$$0 \to \Gamma(C, \mathcal{O}_C)/\wp(\Gamma(C, \mathcal{O}_C)) \to \mathrm{H}^1(C_{et}, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\delta} \mathrm{H}^1(C_{Zar}, \mathcal{O}_C)^F \to 0$$

ou rappelons le F designe le morphisme de Frobenius et $\wp = F - I$ et

$$\mathrm{H}^1(C_{Zar}, \mathcal{O}_C)^F := \{c \in \mathrm{H}^1(C_{Zar}, \mathcal{O}_C) | \mathbb{F}(c) = c\}$$

Preuve: un element de $\mathrm{H}^1(C_{et}, \mathbb{Z}/p\mathbb{Z})$ est un revetement Galoisien etale de C avec action de Galois on dit que c'est un torseur sous $\mathbb{Z}/p\mathbb{Z}$; il est donne sur un recouvrement affine convenable $\mathcal{U} := (U_i)_i$ par des algebres: $B_i \simeq \mathcal{O}_C(U_i)[T_i]/(T_i^p - T_i - a_i)$ et l'action de $1 \in \mathbb{Z}/p\mathbb{Z}$ est donnee par $\sigma(T_i) = T_i + 1$. Sur $U_i \cap U_j$ on a donc $T_j - T_i = f_{i,j} \in \mathcal{O}_C(U_i \cap U_j)$ (invariance par σ) et donc $f_{j,k} - f_{i,k} + f_{i,j} = 0$ i.e. $(f_{i,j}) \in Z^1(\mathcal{U}, \mathcal{O}_C)$ est un 1 -cocycle; de plus $(*)$ $a_j - a_i = f_{i,j}^p - f_{i,j} \in \mathcal{O}_C(U_i \cap U_j)$; l'homomorphisme δ est alors donne sur ce torseur par l'image de $(f_{i,j})$ dans $\mathrm{H}^1(C_{Zar}, \mathcal{O}_C)$ qui tombe bien grace a la relation (*) dans $\mathrm{H}^1(C_{Zar}, \mathcal{O}_C)^F$. Monotrons que le noyau de δ est $\Gamma(C, \mathcal{O}_C)/\wp(\Gamma(C, \mathcal{O}_C))$. En effet si il existe $b_i \in \mathcal{O}_C(U_i)$ tel que $(f_{i,j} = b_j - b_i)$; alors $a_i - b_i^p + b_i \in \mathcal{O}_C(U_i)$ definit une section dans $\Gamma(C, \mathcal{O}_C)$ modulo $\wp(\Gamma(C, \mathcal{O}_C))$.

Corollaire. Si C est affine la suite

$$0 \to \Gamma(C, \mathcal{O}_C)/\wp(\Gamma(C, \mathcal{O}_C)) \to \mathrm{H}^1(C_{et}, \mathbb{Z}/p\mathbb{Z}) \to 0$$

est exacte.

B . 1) La courbe C est complete.

Dans ce paragraphe C , designe une courbe complete sur k non singuliere de genre g . Alors

Theoreme (Hasse-Witt). Soit C une courbe lisse connexe complete sur un corps algebriquement clos k ; on note g le genre de C/k alors il existe un entier $h,\ 0 \leq h \leq g$ tel que $\mathrm{H}^1(C_{et}, \mathbb{Z}/p\mathbb{Z}) \simeq (\mathbb{Z}/p\mathbb{Z})^h$

Preuve: puisque k est algebriquement clos seul $\mathrm{H}^1(C_{Zar}, \mathcal{O}_C)^F$ presente une difficulte; notons V le k espace vectoriel $\mathrm{H}^1(C_{Zar}, \mathcal{O}_C)$ c'est un k -espace vectoriel de dimension g muni de l'action p -lineaire du Frobenius i.e. $F(\lambda v) = \lambda^p v$. Soient $e_1, e_2, ..., e_r$ des elements de V^F que l'on suppose lineairement independants sur $\mathbb{F}_p$; alors si $\sum_{i \in I} \lambda_i e_i = 0$ est une liaison a coefficients dans k de longueur minimale avec $\lambda_{i_0} = 1$; alors $\sum_{i \in I} f(\lambda_i e_i) = \sum_{i \in I} \lambda_i^p e_i = 0$ est une autre liaison de meme longueur ainsi la difference $\sum_{i \in I} (\lambda_i^p) e_i = 0$ est une relation triviale et donc les $\lambda_i = 0$ pour $i \in I$; ce qui montre qu'il n'y a pas de liaison dans k . Ainsi V^F est un $\mathbb{F}_p$ -espace vectoriel de dimension $\leq g$.

Remarque. La methode precedente s'etend pour determiner le groupe $\mathrm{H}^1(C_{et}, \mathbb{Z}/p^n\mathbb{Z})$ en utilisant l'isogenie d'Artin-Schreier-Witt; le faisceau cette fois-ci est $W_n(\mathcal{O}_C)$ et $\mathrm{H}^1(C_{et}, \mathbb{Z}/p^n\mathbb{Z}) \simeq \mathrm{H}^1(C_{Zar}, W_n(\mathcal{O}_C))^F \simeq W_n(\mathbb{Z}/p\mathbb{Z})^h = (\mathbb{Z}/p^n\mathbb{Z})^h$; plus generalement on montre le theoreme:

Theoreme (Safarevic). Soit C une courbe lisse connexe complete sur un corps algebriquement clos k et $\pi_1^{(p)}$ le groupe de Galois de la p -extension maximale non ramifiee de $k(C)/k$; c'est un pro- p -groupe libre a h generateurs.

Notons seulement que le theoreme decoule de la nullite du groupe $H^2(\pi_1^{(p)}, \mathbb{Z}/p\mathbb{Z})$ qui elle meme provient de son identification avec le groupe de cohomologie etale $\mathrm{H}^2(C_{et}, \mathbb{Z}/p\mathbb{Z})$ qui lui est nul parce que la dimension de C est 1.

La preuve qu'en a donne Safarevic utilise une autre voie; il montre une formule qui compare les invariants de Hasse-Witt d'une courbe et d'un revetement etale galoisien de groupe un p -groupe. Plus generalement on montre la formule de Deuring-Safarevic

Theoreme. Soit $\pi : X \rightarrow C$ un revetement de courbes lisses completes galoisien de groupe de Galois G un p -groupe et Br le lieu de branchement si $P \in Br$ on note e_P l'indice de ramification (c'est une puissance de p); alors si h_X resp. h_C designent les invariants de Hasse-Witt de X, C on a la relation:

$$h_X - 1 = |G|(h_C - 1) + \sum_{P \in Br} |G|(1 - e_P^{-1})$$

Pour une preuve voir S. Nakajima (Math Zeitschrift 1985)

Definition On dit qu'une courbe lisse complete C/k de genre g est ordinaire (resp. supersinguliere) si $h = g$ (resp. h=0).

Corollaire Soit $\pi : X \rightarrow C$ un revetement etales de courbes completes lisses et galoisien de groupe de Galois G un p -groupe. Alors C est une courbe ordinaire ssi X est ordinaire.

Preuve: La formule d'Hurwitz permet de comparer les genres g_X, g_C de X et C . On a $2(g_X - 1) = 2|G|(g_C - 1)$.

La formule de Deuring-Safarevic permet aussi de construire des courbes supersinguliere en effet on a le

Corollaire Soit $\pi : X \to \mathbb{P}^1$ un revetement Galoisien etale de la droite affine de groupe un p-groupe alors $h_X = 0$ ssi la ramification est totale au-dessus de l'infini; de plus le genre de X est arbitrairement grand.

Preuve: On peut appliquer le theoreme precedent a $C = \mathbb{P}^1$ et $Br := \infty$ alors si X est un revetement etale de la droite affine de groupe un p-groupe on a $h_X - 1 = |G|(0-1) + |G|(1 - e_\infty^{-1})$. La formule d'Hurwitz montre que le genre de X est alors $2(g_X - 1) = 2|G|(0-1) + d_\infty$; par exemple si $|G| = p$ on montrera que $d_\infty = (m+1)(p-1)$ ou m est un entier > 0 et premier a p ; alors $g_X = (p-1)(m+1)/2$. C'est le cas pour X defini par l'equation $x^p - x = t^m$.

On ne connait pas de formule donnant la variation de l'invariant de Hasse-Witt dans les revetements galoisien de groupe un groupe cyclique d'ordre ℓ si $(\ell, 1) = 1$.

En general on peut se poser la question de calculer l'invariant de Hasse-Witt pour une courbe complete C/k donnee. Nous allons d'abord faire quelques rappels:

Interpretation classique des groupes de cohomologie $\mathrm{H}^1(C, \mathcal{O}_C)$ et $\mathrm{H}^1(C, \Omega^1)$ et Rappels sur les differentielles.

Soit $K := k(C)$ le corps des fonctions rationnelles sur C ; nous considerons K comme faisceau constant sur C contenant $\mathcal{O}$ comme sous-faisceau. On a donc la suite exacte:

$$(1) \quad 0 \to \mathcal{O}_C \to K \to K/\mathcal{O}_C \to 0.$$

Puisque K est le faisceau constant et que X est irreductible, on a
$\mathrm{H}^1(X, K) = 0$;alors la suite exacte de cohomologie associee a (1) donne:

$$(2) \quad K \to \mathrm{H}^0(C, K/\mathcal{O}_C) \to \mathrm{H}^1(C, \mathcal{O}_C) \to 0.$$

Cette derniere suite est facile a interpreter. Soit R l'algebre des repartitions sur C ; un element $r \in R$ est une famille $\{r_x\}_{x \in C}$ ou les r_x sont des elements de K appartenant a $\mathcal{O}_C$ pour tout $x \in C$ sauf au plus un nombre fini. Les repartitions pour lesquelles $r_x \in \mathcal{O}_C$ pour tout x forment un sous-anneau de $R(0)$ de R. Le corps K se plonge dans R par l'application diagonale. Le faisceau $\mathcal{F} := K/\mathcal{O}_C$ est un faisceau “gratte ciel”: si s est une section au-dessus d'un voisinage U d'un point P, il existe $U' \subset U$ du point P tel que $s = 0$ sur $U' - P$. Il s'ensuit que $\mathrm{H}^0(C, K/\mathcal{O}_C)$ s'identifie a la somme directe des fibres $\mathcal{F}_P$ pour P parcourant C et donc isomorphe a $R/R(0)$; ainsi (2) donne un isomorphisme:

$$(3) \quad R/(R(0) + K) \simeq \mathrm{H}^1(C, \mathcal{O}_C)$$

Remarque. Une formule analogue a (3) vaut pour $\mathrm{H}^1(C, W_n(\mathcal{O}_C)$

Differentielles, cf Hartshorne p.172

Soit A un anneau, B une A-algebre et M un B-module. On rappelle qu'une A-derivation de B dans M est une application $d : B \to M$ telle que (1) d est additive et (2) $d(b_1 b_2) = b_1 d(b_2) + b_2 d(b_1)$, enfin (3) $d(a) = 0$. On définit le module des formes differentielles relatives de B sur A comme etant le B-module $\Omega_{B/A}$ qui satisfait la propriete universelle suivante: pour tout B-module M et pour toute A-derivation $d' : B \to M$ il existe un unique homomorphisme de B-module $f : \Omega_{B/A} \to M$ tel que $d' = f \circ d$.

Si X est une variete algebrique sur k, en se ramenant au cas affine on definit un faisceau algebrique coherent Ω sur X par ses fibres $\Omega_x := \Omega_{\mathcal{O}_{X,x}/k}$; on a

$$\Omega_{k(X)/k} = \Omega_x \otimes_{\mathcal{O}_{X,x}} k(X)$$

Si X est reguliere en x et si $t_1, ..., t_r$ est un systeme regulier de parametres en x, les dt_i forment une base de Ω_x ainsi le faisceau Ω est localement libre au-dessus de l'ouvert des points reguliers de X.

Dans le cas ou $X = C$, Ω est un sous faisceau du faisceau constant $\Omega_{k(X)/k}$ et si t est une uniformisante en $x \in C$ pour $\omega \in \Omega_{k(X)/k}$ on peut ecrire $\omega = f dt$ avec $f \in K$. On pose alors en supposant $\omega \neq 0$;

$$v_x(\omega) = v_x(f).$$

Cette definition est independante du choix de la fonction t. Soit $k((t))$, le complete de $\mathcal{O}_{X,x}$ en x, alors $f = \sum_{n \geq n_0} a_n t^n \in k((t))$ et on verifie que le coefficient a_{-1} ne depend pas du parametre t. On definit le residu de ω en x par la formule:

$$Res_x(\omega) = a_{-1}$$

On montre que l'on a une dualite entre $R/(R(0) + K)$ et $\mathrm{H}^0(C, \Omega_C)$ via la forme bilineaire

$$< r, \omega >:= \sum_{x \in C} Res_x(r_x \omega)$$

Matrice de Hasse-Witt

Choisissons une base $\{\omega_1, ..., \omega_g\}$ de $\mathrm{H}^0(C, \Omega_C)$, il lui correspond une base duale de $R/(R(0) + K)$ i.e. il existe g points $x_1, ..., x_g$ de C tels que si t_i est parametre uniformisant en x_i les repartitions: $r_i = \{r_{i,x}\}$ ou $r_{i,x} = 0$ si $x \neq x_i$ et $r_{i,x_i} = 1/t_i$ forment une base du k-espace vectoriel $R/(R(0) + K)$.

Soit $A = (a_{i,j})$ la matrice de F par rapport a la base des r_i. Par definition on a

$$r_i^p \equiv \sum_{1 \geq j \geq g} a_{i,j} r_j \mod (R(0) + K) \quad 1 \geq i \geq g$$

Ces congruences signifient qu'il existe des fonctions $g_i \in K$ telles que:

$$g_i \equiv r_i^p - \sum_{1 \geq j \geq g} a_{i,j} r_j \mod R(0)$$

en d'autres termes chaque g_i est reguliere en dehors des points $x_i, 1 \leq i \leq g$ et admet $\delta_{i,j}/t_j^p - a_{i,j}/t_j$ pour partie polaire en x_i. La matrice A s'appelle la matrice de Hasse-Witt de C. Le lien avec l'invariant de Hasse-Witt est donne par le:

Theoreme. (Hasse-Witt) L'invariant de Hasse-Witt de la courbe complete C est egal au rang de la matrice

$$AF(A)F^2(A)...F^{g-1}(A)$$

ou A est une matrice de Hasse-Witt et si $A=(a_{i,j})$ alors $F(A)=(a_{i,j}{}^p)$. En particulier la courbe C est ordinaire si et seulement si $\det A \neq 0$ et C est supersinguliere si et seulement si $AF(A)F^2(A)...F^{g-1}(A)=0.$

Preuve: c'est une consequence du lemme

Lemme (Hasse-Witt). Soit k un corps algebriquement clos de caracteristique $p>0$ et V un k -espace vectoriel de dimension d sur k . Soit $f: V \to V$ une application p -lineaire alors $V^f := \{v \in V \mid f(v)=v\}$ est un $\mathbb{F}_p$ espace vectoriel. Soit V_s le k -sous-espace vectoriel de V engendre par V^f et $V_n := \{v \in V \mid f^n(v)=0\}$; c'est un k -sous-espace vectoriel de V et

(i) $\dim_k V_s = \dim_{\mathbb{F}_p} V^f \geq n$.

(ii) $V=V_s \oplus V_n$ (somme directe de k espaces vectoriels)

(iii) Soient $B:=\{e_1,...,e_n\}$ et $B':=\{e'_1,...,e'_n\}$ deux bases de V/k et soient $A=(a_{i,j}$ resp: $A'=(a'_{i,j}$ la matrice des coordonnees de $f(e_j)$, $1 \leq j \leq n$ dans la base B (resp: de $f(e'_j)$, $1 \leq j \leq n$ dans la base B'). Soit P la matrice de l'identite de la base B' dans la base B (matrice de passage de B a B') alors $A'=P^{-1}AF(P)$.

(iv) $\dim_k V_s$ est egal au rang de la matrice $AF(A)F^2(A)...F^{n-1}(A)$

Preuve du lemme. On a deja vu que V^f est un $\mathbb{F}_p$ -espace vectoriel de dimension $\leq d$; c'est (i). Il est d'autre part immediat que $V \supset V_s \oplus V_n$.

Pour la suite de la demonstration il est commode suivant Hasse-Witt d'introduire la k -algebre des polynomes de Ore; c'est $k[\Theta]$ ou Θ satisfait la regle de commutation $\alpha \in k$, $\Theta\alpha = \alpha^p\Theta$. Soit $S=\sum_{0\leq i\leq s} \alpha_i\Theta^i \in k[\Theta]$, un polynome de degre s dont le terme non nul de plus bas degre est $\alpha_r \neq 0$. Nous allons resoudre l'equation

$$(*) \quad Q \in k[\Theta], \quad \lambda \in k, \quad (1-\Theta)Q=\lambda S$$

On ecrit $Q=q_0+q_1\Theta+...+q_t\Theta^t$ ou $q_i \in k$ a determiner; on obtient le systeme d'equations

$q_0=\lambda\alpha_0$

$1 \leq i \leq s, \quad q_i = q_{i-1}^p + \lambda\alpha_i$

$q_s=q_{s+1}=....=q_t=0$

Ce systeme a pour solutions

$q_0=q_1=...=q_{r-1}=0$ et pour

$r \leq i \leq n$, $q_i=\alpha_i\lambda+\alpha_{i-1}\lambda^p+...+\alpha_r\lambda^{p^{i-r}}$ et enfin

$q_t=q_{t-1}^p=...=q_s^{p^{s-t}}=0$.

Puisque q_s est un polynome en λ de degre p^{s-r} et puisque $q'_s(\lambda)=\alpha_s \neq 0$ $q_s(\lambda)$ a p^{s-r} racines distinctes; le systeme a donc p^{s-r} solutions correspondant aux racines dans k de $q_s(\lambda)=\alpha_s\lambda+\alpha_{s-1}\lambda^p+...+\alpha_r\lambda^{p^{s-r}}$.

Revenons a la demonstration du lemme et plus precisement a l'inclusion $V \subset V_s \oplus V_n$.

On munit V d'une structure de $k[\Theta]$ -module a gauche par la formule

$$\sum_i \alpha_i\Theta^i.v := \sum_i \alpha_i f^i(v)$$

il est bien clair V_s et V_n sont des sous- $k[\Theta]$ -modules de V .

Soit v un vecteur non nul de V et $M := k[\Theta].v$ et M_s, M_n les sous- $k[\Theta]$ modules correspondant, il suffit donc de montrer l'inclusion $M \subset M_s \oplus M_n$.

Soit $S \in k[\Theta]$ le polynome non nul et de plus bas degre tel que $S.v = 0$ (il existe bien via des arguments de dimension). On va appliquer la formule (*) a S ; soient λ_i, $1 \leq i \leq p^{s-r}$ les racines (distinctes) de q_s et $Q(\lambda_i) := q_0(\lambda_i) + q_1(\lambda_i)\Theta + ... + q_{s-1}(\lambda_i)\Theta^{s-1}$ les p^{s-r} solutions de (*). Alors les vecteurs $v_i := Q(\lambda_i).v$ sont 2 a 2 distincts par la minimalite de S et ils satisfont l'equation $(\Theta - 1).v_i = \lambda_i S.v = 0$ i.e. $v_i \in V^f$. Ainsi $\dim_k M_s \geq s - r$.

D'autre part, on peut ecrire $S = \Theta^r T$ ou T est un polynome dont le terme constant est non nul et de degre $s - r$,alors les r vecteurs

$$T.v, \Theta T.v, ..., \Theta^{r-1}T.v$$

sont dans M_n puisque $r \leq s$ et ils sont k -independants par la minimalite de S . Ainsi $\dim_k M_n \geq r$ et donc $\dim_k M_s \oplus M_n \geq s = \dim_k M$ .///

Nous montrons l'egalite $\dim_k V_s = \mathrm{rg} AF(A)F^2(A)...F^{n-1}(A)$ Designons par $[v]$ le vecteur colonne des coordonnees de v dans la base B , on a $[\Theta.v] = A[v]^p$ ou $[v]^p$ est le vecteur colonne dont les coordonnees sont celles de v elevees a la puissance p . Ainsi $[\Theta^n.v] = AA^p...A^{p^{n-1}}[v]^{p^n}$, et puisque k est parfait il suit que $\dim_k V_n = n - \mathrm{rg} AA^p...A^{p^{n-1}}$ ///

Calcul de l'invariant de Hasse-Witt: l'operation de Cartier-Tate

Soit K/k un corps de fonctions d'une variable sur un corps parfait k de caracteristique $p > 0$ et $x \in K - K^p$; alors $K = K^p(x)$ et si $d: K \to \Omega_{K/k}$ est la derivation canonique de K , alors $dx \neq 0$. Tout element $f \in K$ peut s'ecrire $f = f_0^p + f_1^p x + ... + f_{p-1}^p x^{p-1}$ avec $f_i \in K$ et puisque l'on peut integrer x^i pour $0 \leq i \leq p-2$, $\omega := f dx \in \Omega_{K/k}$ peut s'ecrire sous la forme $(*)\ \omega = d\Phi + \Psi^p dx/x$ avec $\Phi = f_0^p x + f_1^p x^2/2 + ... + f_{p-2}^p x^{p-2}/(p-2)$ et $\Psi = f_{p-1}x$. Puisque $df = (f_1^p x + ... + f_{p-1}^p x^{p-1})dx$ il suit que l'equation $dx/x = df$ n'a pas de solution dans K et donc l'ecriture sous la forme (*) est unique. On definit l'operateur de Cartier $\mathcal{C} : \Omega_{K/k} \to \Omega_{K/k}$ par la formule

$$\mathcal{C}(\omega) = f_{p-1}dx$$

Proposition. La matrice de l'homomorphisme p^{-1} -lineaire $\mathcal{C} : \mathrm{H}^0(C, \Omega) \to \mathrm{H}^0(C, \Omega)$ dans la base (ω_j) est egale a la matrice $(A^t)^{1/p}$ Frobenius inverse de la transposee de la matrice de l'application p -lineaire Frobenius exprimee dans la base duale (r_j) .

Preuve: On verifie que $Res_P(f dx) = (Res_P \mathcal{C}(f dx))^p$. En effet on peut supposer que x est parametre uniformisant en P , alors

$$Res_P f dx = Res_P f_{p-1}^p x^p dx/x, \quad Res_P \mathcal{C}(f dx) = Res_P f_{p-1} dx$$

d'ou le resultat. D'autrepart on verifie facilement que $\mathcal{C}(f^p\omega) = f\mathcal{C}(\omega)$ et donc pour r une repatition on a $Res_P(r_P \mathcal{C}\omega) = Res_P \mathcal{C}(r_p^p \omega)$, ainsi $< r^p, \omega >= (< r, \mathcal{C}\omega >)^p$ et donc si (ω_j) est une base de $\mathrm{H}^0(C, \Omega)$ et r_j la base duale on a par definition de F , $r_j^p = \sum_i a_{i,j} r_i$

et $< r_j^p, \omega_i >= a_{i,j} =< r_j, \mathcal{C}\omega_i >)^p$; ainsi si $\mathcal{C}\omega_j = \sum_i \alpha_{i,j}\omega_i$ alors $a_{i,j} = \alpha_{j,i}^p$; i.e. la matrice de $\mathcal{C}$ dans la base ω_i est $(A^t)^{1/p}$. ///

Application: calcul de l'invariant de Hasse-Witt dans le cas d'une courbe hyperelliptique.

On suppose que la caracteristique de k est $p > 2$. Soit C la courbe hyperelliptique d'equation $y^2 = f(x)$ ou $f(x) \in k[x]$ est un polynome de degre $2g+1$ et sans racines multiples. Une base de $\mathrm{H}^0(C,\Omega)$ est donnee par les g differentielles $\omega_i = \dfrac{x^{i-1}dx}{y}$, $1 \leq i \leq g$. Suivant Manin on ecrit $\omega_i = x^{i-1}y^{-p}y^{p-1}dx = y^{-p}x^{i-1}f(x)^{p-1/2}dx$. On ecrit $f(x)^{p-1/2} = \sum_{0\leq j\leq N} c_j x^j$ ou $N = (2g+1)(p-1)/2$. Alors

$$\omega_i = y^{-p}(\sum_{j,i+j\not\equiv 0 \mathrm{mod} p} c_j x^{j+i-1}dx) + \sum_\ell c_{(\ell+1)p-i}\frac{x^{\ell p}}{y^p}x^{p-1}dx.$$

Dans la derniere somme on a $0 \leq \ell \leq \dfrac{N+i}{p} - 1 < g - \dfrac{1}{2}$. Puisque $\mathcal{C}(df) = 0$; il suit que $\mathcal{C}(\omega_i) = \sum_{0\leq \ell\leq g-1} c_{(\ell+1)p-i}^{1/p}\dfrac{x^i}{y}dx = \sum_{1\leq\ell\leq g} c_{(\ell)p-i}^{1/p}\omega_\ell$, ainsi la matrice

$$A = \begin{pmatrix} c_{p-1} & c_{p-2} & \cdots & c_{p-g} \\ c_{2p-1} & c_{2p-2} & \cdots & c_{2p-g} \\ \vdots & \vdots & \cdots & \vdots \\ c_{gp-1} & c_{gp-2} & \cdots & c_{gp-g} \end{pmatrix}$$

est la transposee de la matrice de Hasse-Witt dans la base duale des ω_i .

Dans le cas ou $g = 1$ et $f(x) = x(x-1)(x-\lambda)$ l'invariant de Hasse-Witt est O ou 1 suivant que c_{p-1} est nul ou pas. On peut calculer $f(x)^{p-1/2} = (\lambda x)^{p-1/2}(1-x)^{p-1/2}(1-x/\lambda)^{p-1/2}$ alors

$$c_{p-1} = \sum_{0\leq i\leq p-1/2} \binom{k}{i}^2 \lambda^i$$

Puisque les classes d'isomorphismes des courbes elliptiques sur k sont donnees par le $j = 2^8\dfrac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$ invariant en particulier il suit que pour p donne il n'y a qu'un nombre fini de classes d'isomorphisme de courbes elliptiques supersingulieres. En fait Igusa a remarque que le polynome $c_{p-1}(\lambda)$ satisfait l'equation differentielle en λ :

$$\lambda(\lambda-1)f'' + (1-2\lambda)f' - 1/4f = 0$$

(c'est l'equatin des periodes de la courbe elliptique complexe $E(\mathbb{C}) : y^2 = x(x-1)(x-\lambda)$) il suit de la que les racines de $c_{p-1}(\lambda)$ sont simples. Puisque le morphisme $j(\lambda) : \mathbb{P}^1 \to \mathbb{P}^1$ est de degre 6 et ramifie uniquement en $0, 1728, \infty$ un calcul elementaire montre que le nombre de classes d'isomorphismes de courbes elliptiques supersingulieres sur k et de j invariant $\neq 0, 1728$ vaut $[p/12]$ et donc en general ce nombre vaut $[p/12]$, $[p/12]+1$ ou $[p/12]+2$. En particulier le lieu ordinaire est Zariski dense dans le moduli des courbes elliptiques sur k et la courbe elliptique "generique" $E/k(\lambda) : y^2 = x(x-1)(x-\lambda)$ est ordinaire. Ces resultats se generalisent dans le cas $g > 1$.

Invariant de Hasse-Witt et points de p-torsion de la Jacobienne.

La correspondance est plus subtile que dans le cas Kummerien et elle a ete pour la premiere fois percue par Witt et H. Schmidt (Crelle, Nr 176, 1936).

Une idee naive est de considerer une equation du corps de fonctions defini par un revetement non ramifie p-cyclique de la courbe C. Par exemple supposons que $X^p - X = f$ avec $f \in K$ definisse un tel revetement; on voit bien que le diviseur des poles $(f)_\infty$ de f vaut pD mais il ne s'agit la que d'une condition necessaire!!!

Proposition. Le groupe Pic_p^0 est canoniquement isomorphe au groupe additif des differentielles $\omega \in \mathrm{H}^0(C,\Omega)$ qui verifient $\mathcal{C}\omega = \omega$. En particulier c'est un groupe fini isomorphe a $(\mathbb{Z}/p\mathbb{Z})^h$.

Preuve: on definit l'application $\vartheta : Pic_p^0 \to \mathrm{H}^0(C,\Omega)$.

Soit $d \in Pic_p^0$ et soit D un diviseur dans la classe de d ; puisque $pd = O$ il existe une fonction $f \neq 0$ telle que $pD = (f)$; posons $\omega = df/f$. Si l'on change D en un diviseur equivalent $D+(g)$ ceci a pour effet de multiplier f par g^p et ne change donc pas df/f ; il reste a voir que $\omega = \in \mathrm{H}^0(C,\Omega)$; soit $P \in C$ et t un parametre uniformisant en P alors $f = t^{np}u$ ou u est une unite en P ; puisque $df/f = du/u$ il suit que $v_P(\omega) \geq 0$ /// On note $df/f = \vartheta(f)$. L'application ϑ est clairement un homomorphisme injectif de groupes et $\mathcal{C}(df/f) = \mathcal{C}(f^{p-1}df/f^p) = \mathcal{C}(f^{p-1}df)/f = df/f$.

Pour conclure on utilise le theoreme suivant du a Jacobson et generalise par Cartier dans le cadre de la geometrie algebrique.

Theoreme (Jacobson-Cartier). Soit $\omega \in K$, une CNS pour qu'il existe $f \in K$ telle que $\omega = df/f$ est que $\mathcal{C}\omega = \omega$.

Admettons pour l'instant ce theoreme pour voir que ϑ est surjective; soit $\omega \in \mathrm{H}^0(C,\Omega)$ avec $\mathcal{C}\omega = \omega$; par le theoreme precedent $\omega = df/f$ et puisque la differentielle ω est reguliere il suit que $v_P(f) \in p\mathbb{Z}$ pour tout point $P \in C$; ainsi $(f) = pD$ .///

Preuve du theoreme de Jacobson (d'apres Jacobson). Le cadre naturel est celui des D-modules. Soit D une k-derivation de K/k ; si $a \in K$ on note encore a l'endomorphisme de K de multiplication par a. On a une regle de commutation

$$(1) \quad a' := aD - Da = [a, D]$$

C'est la definition de a' ; i.e. $[a, D]$ est une derivation qui evaluee en $f \in K$ donne $(-D(a))f$; l'endomorphisme de multiplication par $-D(a)$.

Notez que D est identiquement nulle sur K^p ; ainsi peut-on remplacer les constantes k par K^p. Puisque $[K : K^p] = p$ on est ramene a etudier l'algebre $\mathcal{L}$ des K^p endomorphismes engendree par D et les K^p-endomorphismes de multiplication par les elements de K. Si l'on fixe une base e_i de K/K^p l'application qui a $\Delta \in \mathcal{L}$ associe la matrice des coordonnees de $\Delta(e_i)$ dans la base $(e_i$ definit un isomorphisme de K^p-algebres entre $\mathcal{L}$ et l'algebre des matrices $M_p(K^p)$ des matrices a p lignes et p colones et a coefficients dans K^p. Notons que D^p est une derivation; ainsi on a la relation

$$(2) \quad D^p = \alpha D$$

pour α convenable dans K .

Le theoreme de Jacobson donne une CNS pour que $c \in K$ soit de la forme b'/b .

Considerons pour cela la derivation $D_1 := D + c$; on montre par recurrence la formule suivante:

$$D_1^n = \sum_{0 \leq i \leq n} \binom{n}{i} D^{n-i} V_i(c)$$

ou

$$V_1(c) = c, \quad V_j(c) = V_{j-1}(c)' + V_{j-1}(c)c$$

qui pour $n = p$ donne

$$D_1^p = D^p + V_p(c).$$

Il est clair que D_1 satisfait la condition (1) ; ainsi la correspondance $D \to D + c$, $a \to a$ definit un K^p -automorphisme de $\mathcal{L}$ si et seulement si $D_1^p = \alpha D_1$; i.e.

$$(3) \quad V_p(c) = \alpha c.$$

D'autre part puisque les K^p -automorphismes de $M_p(K^p)$ sont interieurs; il existe $B \in \mathcal{L}$ tel que

$$(4) \quad B^{-1} a B = a, \quad B^{-1} D_1 B = D$$

pour tout $a \in K$. Puisque la K^p algebre engendree par $a \in K, B$ est un sous corps commutatif de $\mathcal{L}$ il suit que $B = b \in K$. La relation (4) est equivalente a $c = b'/b$. Il reste donc a exprimer $V_p(c)$;

Lemme (Jacobson). $V_p(c) = c^p + c^{(p-1)}$.

Preuve: On verifie par recurrence les formules:

$$V_j(c) = \sum_{1 \leq i \leq j} P_{ij}, \quad P_{ij} = \sum \frac{j!}{\alpha! \beta! ...} (\frac{c}{1!})^{\alpha} (\frac{c'}{2!})^{\beta} ...,$$

ou la derniere sommation est etendue aux entiers naturels tels que

$$\alpha + \beta + \gamma + ... = i, \quad \alpha + 2\beta + 3\gamma + ... = j.$$

Deduisons le theoreme de Jacobson-Cartier. On a $K = \bigoplus_{0 \leq i \leq p-1} K^p t^i$, pour D on prend ∂_t ; ainsi $\alpha = 0$ et la condition $\omega := f dt = dg/g = \partial_t(g)/g dt$ se traduit par $f = \partial_t(g)/g$. Nous pouvons appliquer ce qui precede: une cns est que $0 = V_p(f) = f^p + f^{(p-1)} = f^p + (p-1)! f_{p-1}^p$ ou $f = f_0^p + f_1^p t + ... + f_{p-1}^p t^{p-1}$; ce qui n'est autre que la condition $\mathcal{C}\omega = \omega$ ./ / /

QUESTION: On aimerait associer a $d \in Pic_p^0$ une equation d'un $\mathbb{Z}/p\mathbb{Z}$ -torseur sur C .

B.2) La courbe C est supposee affine.

On note $\overline{C}$, la completion de C et g son genre. On note $P_1, ..., P_s$ les points de $\overline{C} - C$ et t_i un parametre uniformisant en P_i .

Considerons un $\mathbb{Z}/p\mathbb{Z}$ -torseur sur C ; il est donne par une equation

$$X^p - X = f \in \mathcal{O}(C)$$

ainsi il induit un $\mathbb{Z}/p\mathbb{Z}$ -torseur sur le corps de fraction $k((t_i))$ du complete de l'anneau local en P_i ; ces derniers sont donnes par la theorie d'Artin-Schreier que nous allons pour un instant presenter.

Extension p^n -cycliques d'un corps de series formelles

On considere donc un corps de series formelles $k((t))$ sur un corps algebriquement clos k de caracteristique $p > 0$; on a la suite d'Artin-Schreier:

$$0 \to k((t)) \xrightarrow{\wp} k((t)) \to \mathrm{H}^1(G_{k((t))}, \mathbb{Z}/p\mathbb{Z}) \to 0$$

Puisque $\wp(k[[t]]) = k[[t]]$ on peut donner prendre des representants du groupe $k((t))/\wp k((t))$ dans les parties polaires $\sum_{1 \leq j \leq m} \dfrac{a_j}{t^j}$; mieux quitte a ajouter une fonction de la forme $\wp(f)$ on peut supposer que $(m,p) = 1$ et que les a_j sont nuls pour $p|j$. L'entier $m+1$ est uniquement determine par le torseur, on l'appelle le conducteur de Hasse. Pour voir cela on remarque la partie polaire s'ecrit $t^{-m}(a_m + a_{m-1}t + ...)$ avec $a_m \neq 0$; puisque $(m,p) = 1$ c'est une puissance m -ieme; ainsi quitte a faire un changement de parametre, l'equation s'ecrit $X^p - X = t^{-m}$. On verifie facilement que $z := X^{-1/m} \in k((t))[X]$ et que c'est une uniformisante de l'extension $k((t))[X] = k((z))$. Soit σ l'automorphisme de $k((t))[X]$ tel que $\sigma(X) = X + 1$ (quitte a multiplier X par un entier on peut toujours supposer cela); alors $\sigma(z)/z = (1 + z^m)^{-1/m}$ et $m = v_z(\sigma(z)/z - 1)$ est le premier saut de ramification.

On vient de montrer la

Proposition. Les classes de conjugaisons des k -automorphismes d'ordre p du groupe $Aut_k k((z))$ est en bijection l'ensemble $\mathbb{N} - p\mathbb{N}$. La bijection en question associe a $m \in \mathbb{N} - p\mathbb{N}$ l'automorphisme $\sigma(z) = z(1 + z^m)^{-1/m}$.

Corollaire. Le degre de l'ideal differente dans l'extension $k((t))[X]/k((t))$ est $(m+1)(p-1)$.

Preuve: puisque l'extension est monogene la differente est engendree par $f'(z)$ ou $f(Z)$ est le polnome minimal de z sur $k((t))$. Et $v_z(f'(z)) = \sum_{1 \leq i \leq p-1} v_z(z - \sigma^i(z)) = (p-1)v_z(z - \sigma(z))$ //

Il est beaucoup plus difficile de decrire les classes de conjugaisons des k -automorphismes d'ordre p^2 . On montre le

Lemma. Soient $a_j \in k$ and $p_{j,p-i} \in k[x], \quad 0 \leq j < m_1, \quad 0 < i < p,$ des polynomes de degres respectifs $d_{j,p-i}$ et supposons que $(m_1, p) = 1$. Les equations

$$x_1^p - x_1 = t^{-m_1}$$

et

$$x_2^p - x_2 =$$
$$c(x_1^p, -x_1) + \sum_{0 \leq s < m_1(p-1)} a_s t^{-s} + \sum_{0 \leq j < m_1} t^{-jp} \sum_{0 < i < p} (x_1^p - x_1)^i p_{j,p-i}(x_1^p - x_1)^p$$

definissent une extension p^2 -cyclique de $k((t))$ et le degre de la differente est

$$(m_1+1)(p-1)p+(m_2+1)(p-1),$$

ou

$$m_2 := \max_{\substack{0\leq j<m_1 \\ 0<i<p}} \left(p^2 m_1, p(jp+(i+pd_{j,p-i})m_1)\right) - (p-1)m_1$$

et $c(x,y)=((x+y)^p-x^p+(-y)^p)/p$. De plus puisque le semi-groupe $p\mathbb{N}+m_1\mathbb{N}$ contient les entiers $>(m_1-1)(p-1)$, il suit que toute extension p^2-cyclique de $k((t))$ admet une telle representation.

Preuve. Puisque $(m_1,p)=1$ il suit que $z:=x_1^{-1/m_1}$ est un parametre uniformisant de $k((t))[x_1]$. On doit calculer le conducteur de l'extension $k((t))[x_1,x_2]/k((t))[x_1]$. On peut facilement exprimer
$1/t=z^{-p}(1-z^{m_1(p-1)})^{-1/m_1}$ (a une constante multiplicative pres), alors

$$c(x_1^p,-x_1)=-z^{-p^2m_1+(p-1)m_1}+\cdots$$

donne une contribution en terme de z-valuation plus grande que tout t^{-j}, $0<j<m_1(p-1)$. Les autres termes peuvent etre arranges sous forme de polynomes en t^{-1} et regardant les termes d'exposant premier a p, on voit que le terme de plus haut degre en z^{-1} vient seulement du polynome

$$t^{-jp}(x_1^p-x_1)^i(p_{j,p-i}(x_1^p-x_1))^p.$$

Apres des transformations standards pour eliminer les puissances p-iemes, les puissances premieres a p d'ordre maximal en z^{-1} donnent le conducteur indique.

Il faut maintenant justifier que les expressions dans le second membre de la seconde equation donnent des representantsd'Artin-Schreier-Witt pour toutes les extensions p^2-cycliques. Cela vient du developpement en t^{-1}, chaque monome t^{-l}, avec $l\geq m_1(p-1)$ et premier a p, apparait effectivement dans les expressions du type decrit. Les monomes apparaissant comme puissances p-iemes peuvent s'eliminer en faisant une transformation a la variable x_2 de l'extension. ///

Remarque. Notez que $x_2-\sum_{0\leq j<m_1} t^{-j}\sum_{0<i<p}(x_1)^i p_{j,p-i}(x_1^p-x_1)$ est un representant d'Artin-Schreier de l'extension p-cyclique $k((t))[x_1,x_2]/k((t))[x_1]$.

Revetements p-cyclique etales d'une courbe affine: un principe local-global.

Theoreme. (Harbater) Soit C une courbe algebrique affine lisse et irreductible sur k . Soit $\overline{C}$, la completion de C et g son genre. On note $P_1,\ldots,P_s$ les points de $\overline{C}-C$ et t_i un parametre uniformisant en P_i . On a une suite exacte de groupes

$$0\to \mathrm{H}^1(\overline{C}_{et},\mathbb{Z}/p\mathbb{Z})\xrightarrow{\alpha}\mathrm{H}^1(C_{et},\mathbb{Z}/p\mathbb{Z})\xrightarrow{\beta}\bigoplus_i \mathrm{H}^1(G_{k((t_i))},\mathbb{Z}/p\mathbb{Z})\to 0$$

Preuve: Soit $X\to\overline{C}$ un $\mathbb{Z}/p\mathbb{Z}$ -torseur sur $\overline{C}$; par changement de base $C\to\overline{C}$, il induit un $\mathbb{Z}/p\mathbb{Z}$ -torseur sur C ; d'ou l'homomorphisme injectif α . Maintenant si $Y\to$

C un $\mathbb{Z}/p\mathbb{Z}$-torseur sur C, il induit par changement de base au complete $k((t_i))$ en P_i du corps de fonctions $k(C)$ un $\mathbb{Z}/p\mathbb{Z}$-torseur sur $k((t_i))$ d'ou un homomorphisme $\mathrm{H}^1(C_{et}, \mathbb{Z}/p\mathbb{Z}) \to \mathrm{H}^1(G_{k((t_i))}, \mathbb{Z}/p\mathbb{Z})$ qui induit β en prenant l'homomorphisme diagonal. Il est clair que le noyau de β correspond aux $\mathbb{Z}/p\mathbb{Z}$-torseur sur C etales au dessus des P_i ; donc a $\mathrm{H}^1(\overline{C}_{et}, \mathbb{Z}/p\mathbb{Z})$. Le seul point delicat est "le principe local-global"; i.e. les conditions locales dans $\bigoplus_i \mathrm{H}^1(G_{k((t_i))}, \mathbb{Z}/p\mathbb{Z})$ determinent un $\mathbb{Z}/p\mathbb{Z}$-torseur sur C.

Nous examinerons ici seulement le cas facile ou $\overline{C} = \mathbb{P}^1$. Soit x un parametre de $\mathbb{P}^1$ et supposons que $t_i := x - x_i$ est parametre uniformisant en P_i. Puisque $\mathrm{H}^1(G_{k((t_i))}, \mathbb{Z}/p\mathbb{Z}) \simeq k[1/t_i]/\wp(k[1/t_i])$ soit donc $Q_i(x) \in k[1/x - x_i]$ une partie polaire en x_i pour $1 \leq i \leq s$. Considerons le torseur $Z^p - Z = \sum_{1 \leq i \leq s} Q_i(x)$. Pour $i \neq j$ on a $1/x - x_i \in k[[x - x_j]]$ et donc par le lemme de Hensel $\sum_{1 \leq i \leq s,\ i \neq j} Q_i(x) \in k[[x - x_j]] = \wp(k[[x - x_j]])$; ainsi le torseur au-dessus de C induit les torseurs locaux en x_i donnes par les partie polaires $Q_i(x)$.

Remarque. Notez bien la difference avec le cas $(n,p) = 1$; dans ce dernier cas il n'y a pas de principe local-global.

Réf'erences.

D. Harbater, Moduli of p-covers of curves. Communications in Algebra 8 (12) (1980), 1095-1122.

N. Katz, Local-to-global extensions of representations of fundamental groups, Ann. Inst. Fourier, 36, 4 (1986), 69-106.

Revetements galoisiens etales d'une courbe affine: conjectures d'Abhyankar

Toujours k est un corps algebriquement clos de caracteristique $p > 0$ et $S \neq \emptyset$ de cardinal s i.e. C est affine.

Soit G un groupe fini. Soit $p(G)$ le sous-groupe engendré par les sous-groupes de Sylow. Le groupe $G/p(G)$ est le plus grand quotient de G d'ordre premier à p. Si G est groupe de Galois d'un revetement etale connexe fini de C alors $G/p(G)$ est d'ordre premier a p et c'est aussi un groupe de Galois d'un revetement etale connexe fini de C ; Grothendieck a montre (SGA 1) (c'etait une conjecture de Weil) que ce cas se releve en caracteristique zero et donc $G/p(G)$ est engendré par $2g + s - 1$ éléments. En 1957, Abhyankar a fait la conjecture que cette condition est suffisante:

Conjecture (AC). Un groupe fini G est groupe de Galois d'un revetement etale connexe fini de C ssi $p(G)$ peut-être engendré par $2g + s - 1$ éléments.

La conjecture d'Abhyankar pour la droite affine

On a donc $C = \mathbb{A}^1 = \mathrm{Spec} k[X]$, le corps k étant algébriquement clos de caractéristique $p > 0$. Puisque $2g + s - 1 = 0$, la conjecture (AC) prend alors la forme suivante:

Conjecture (AC- $\mathbb{A}^1$) *Un groupe G est groupe de Galois d'un revetement etale connexe fini de $\mathbb{A}^1$ si et seulement si G est engendré par ses p-groupes de Sylow.*

Un groupe tel que $G = p(G)$ est appelé quasi- p-groupe.

Divers groupes ont été réalisés "explicitement".

Soit q , une puissance de p , et soit Σ un groupe algébrique semi-simple simplement connexe sur $\mathbb{F}_q$. Soit $G = \Sigma(\mathbb{F}_q)$, le groupe des $\mathbb{F}_q$ -points de Σ ; Nori a montre que G est groupe de Galois d'un revetement etale connexe fini de $\mathbb{A}^1$.

Abhyankar a donne des realisations explicites du groupe alterné A_n si $p \neq 2$ et $n \geq p$; du groupe symétrique S_n si $p = 2$. Il les réalise comme clôture galoisienne des revêtements associés à l'équation pour diverses valeurs de p et t : $Y^n - XY^t + 1 = 0$

L'interet dans la conjecture d'Abhyankar a ete relance par Serre en 90 (Note aux CRAS).
Soit $1 \to N \to \tilde{G} \to G \to 1$, une suite exacte de groupes finis. Supposons que $\tilde{G}$ soit un quasi- p -groupe, et que N soit résoluble. Alors Serre montre que si G vérifie (AC- $\mathbb{A}^1$), il en est de même pour $\tilde{G}$; en particulier les groupes résolubles satisfont (AC- $\mathbb{A}^1$).

Finalement Raynaud a donne une preuve en 90 de la conjecture AC- $\mathbb{A}^1$ et Harbater et Pop en ont deduit la conjecture generale.

Réf'erences. Voir l'expose de Serre au seminaire Bourbaki (1990)

Raynaud, M. Revetements de la droite affine en caracteristique $p > 0$ et conjecture d'Abhyankar. Invent. Math. 116 (1994), no. 1-3, 425–462.

Harbater, D. Abhyankar's conjecture on Galois groups over curves. Invent. Math. 117 (1994), no. 1, 1–25.

Pop, F. Etale Galois covers of affine smooth curves. The geometric case of a conjecture of Shafarevich. On Abhyankar's conjecture. Invent. Math. 120 (1995), no. 3, 555–578.

C. Le Groupe des k -automorphismes d'une courbe C/k .

Dans ce paragraphe k designe un corps algebriquement clos de caracteristique $p \geq 0$ et C est une courbe complete lisse connexe de genre g .

Le genre 0

On a vu que $C \simeq \mathbb{P}^1$; ainsi $k(C) = k(t)$. Un k -automorphisme de $k(C)$ est donne par l'image f de t ; puisque le degre de l'extension $k(t)/k(f)$ est donne par le degre de $(f)_\infty$ il suit que f a exactement un pole et un zero i.e. $f = \dfrac{at+b}{bt+d}$ avec $a, b, c, d \in k$ et $ad - bc \neq 0$; c'est une homographie. Reciproquement une homographie est un k -automorphisme de $\mathbb{P}^1$.

Le genre 1

Soit O un point de C , le couple (C, O) est une courbe elliptique i.e. un groupe algebrique complet de dimension 1 sur le corps k ; le point O est l'element neutre du groupe. En considerant les sections des faisceaux $\mathcal{O}(-nO)$ on montre que (C, O) se plonge dans $\mathbb{P}^2_k$ comme une cubique

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

le point O etant le point a l'infini $[0, 1, 0]$. Puisqu'un automorphisme de la courbe elliptique preserve les k -espaces vectoriels $L(nO)$ il suit facilement qu'ils proviennent d'automorphismes de $\mathbb{P}^2$ preservant le point O .

Si l'on note T l'ensemble des translations de $\tau_P \in T$ definie par $\tau(Q) = Q \oplus P$; c'est un groupe d'automorphismes de C isomorphe a $C(k)$ et $\mathrm{Aut}C$ est produit semi-direct de T et de $\mathrm{Aut}(C, O)$

Theoreme. Soit (C,O) une courbe elliptique sur un corps k algebriquement clos, alors $\mathrm{Aut}(C, O)$ est un groupe fini d'ordre divisant 24 et $\mathrm{Aut}C$ est produit semidirect du groupe $\mathrm{Aut}(C, O)$ et du groupe $(C(k), \oplus)$. Plus precsement si l'on note $j(C)$ le j invariant on a:

1. $|\mathrm{Aut}(C, O)| = 2$ si $j(C) \neq 0, 1728$
2. $|\mathrm{Aut}(C, O)| = 4$ si $j(C) = 1728$ et $\mathrm{car}k \neq 2, 3$
3. $|\mathrm{Aut}(C, O)| = 6$ si $j(C) = 0$ et $\mathrm{car}k \neq 2, 3$
4. $|\mathrm{Aut}(C, O)| = 12$ si $j(C) = 1728 = 0$ si $\mathrm{car}k = 3$
5. $|\mathrm{Aut}(C, O)| = 24$ si $j(C) = 728 = 0$ si $\mathrm{car}k = 2$

Le genre ≥ 2

Le resultat important dans ce cas est le

Theoreme. Soit C une courbe complete lisse sur un corps algebriquement clos k . Si le genre de C est ≥ 2 alors le groupe $\mathrm{Aut}_k C$ des k -automorphismes de C est fini.

Preuve: Dans Hartshorne on trouve une preuve dans le cas ou la caracteristique du corps k est nulle. La meme methode marche en caracteristique $p > 0$ mais les preuves sont techniquement bien plus compliquees. La methode consiste a exhiber une famille finie de cardinal $> 2(g + 1)$ de points speciaux sur la courbe (des points de Weierstrass); qui sont stables par les k -automorphismes. Le lemme suivant montre alors que $\mathrm{Aut}_k C$ opere fidelement sur la famille.

Lemme. Soit C une courbe de genre $g \geq 2$ sur un corps algebriquement clos k et $\sigma \neq \mathrm{Id}$ un k -automorphisme de C alors σ a au plus $2g + 2$ points fixes.

Preuve: Soit $P \in X$ avec $\sigma(P) \neq P$; on a $l((g+1)P) = l(K-(g+1)P)+g+1+1-g \geq 2$. Puisque $l(O) = 1$, il existe $1 \leq r \leq g+1$ et $f \in L(rP)-L((r-1)P)$ i.e. $(f)_\infty = rP$. Posons $h = f - f \circ \sigma$; on a $(h)_\infty = rP + r\sigma^{-1}(P)$; il suit que h a au plus $2r$ zeros et donc que σ a au plus $2r \leq 2g + 2$ points fixes.

Remarque. Pour une autre preuve valant en toute caracteristique mais utilisant la theorie de l'intersection sur les surfaces voir:

Samuel, P. Lectures on old and new results on algebraic curves. Notes by S. Anantharaman. Tata Institute of Fundamental Research Lectures on Mathematics, No. 36 Tata Institute of Fundamental Research, Bombay 1966 ii+127+iii pp.

Kani, Ernst Bounds on the number of nonrational subfields of a function field. Invent. Math. 85 (1986), no. 1, 185–198.

C'est un autre probleme que d'exhiber une borne ne dependant que du genre. Nous allons voir une representation naturelle du groupe des automorphismes et qui est tres importante dans les problemes de modules. La reference est:

A. Grothendieck, Techniques de construction en geometrie analytique, Seminaire H. Cartan, 1960-61, 17. (avec un appendice de Serre)

Lemme. (Serre) Soit A une variete abelienne sur k , et $n \geq 3$ un entier premier a $\mathrm{car}k := p$. Soit σ un automorphisme de A d'ordre fini; on suppose que σ opere trivialement sur les points de n torsion de A alors $\sigma = \mathrm{Id}$.

Theoreme. Soit C une courbe de genre $g \geq 2$ sur un corps algebriquement clos k et $Jac(C)$ la jacobienne de C . Soit σ un automorphisme de C induisant l'identite sur $Jac(C)$, alors σ est l'identite.

Idee de la preuve: Il suffit de montrer que σ a alors un point fixe O ; alors $\sigma(P-0) = P-O$ et donc le diviseur $\sigma(P)-P$ est lneairement equivalent a 0 ce qui impose $\sigma(P) = P$ puisque $g(C) > 0$. Pour voir que σ a un point fixe on utilise un theoreme du point fixe de Lefschetz (cf. Harsthorne p. 453).

Ainsi $\mathrm{Aut}_k C$ se plonge dans $GL_{2g}(\mathbb{Z}/n\mathbb{Z})$ pour $n = 3$ ou 5 . En fait on peut donner des bornes polynomiales en g.

Theoreme. (Hurwitz) Soit C une courbe de genre $g \geq 2$ sur un corps algebriquement clos k de aracteristique 0 , alors $|\mathrm{Aut}_k(C)| \leq 84(g-1)$.

La preuve (laissee en exercice) consiste a considerer le revetement galoisien de groupe $G \simeq \mathrm{Aut}_k(C)$; $C \to C/G$ et analyser la formule d'Hurwitz; il est essentiel ici que la ramification soit moderee; en particulier la meme borne marche pour un groupe G d'ordre premier a p . Cette borne est atteinte pour une infinite de valeurs de g . Precisement on montre que la courbe de Klein

$$x^3y + y^3z + z^3x = 0$$

qui est de genre 3 a 168 automorphismes, cf. Reyssat, E Quelques aspects des surfaces de Riemann. Progress in Mathematics, 77. Birkhauser Boston, Inc., Boston, MA,1989. viii+166 pp.

En fait comme le remarque Reyssat si C est une courbe com)plete qui atteint la borne d'Hurwitz, si n est un entier nous avons vu que $\mathrm{H}^1(C_{et}, \mu_n) \simeq Pic(C)_n \simeq (\mathbb{Z}/n\mathbb{Z})^{2g}$; considerons $k(C')/k(C)$ l'extension abelienne maximale dans $k(C)^s$ de $k(C)$ qui est non ramifiee et d'exposant divisant n . Si G est son groupe de Galois on a donc $Hom\,(G, \mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^{2g}$; il suit que $G \simeq (\mathbb{Z}/n\mathbb{Z})^{2g}$; montrons que C' atteint alors la borne d'Hurwitz. En effet $g(C')-1 = n^{2g}(g(C)-1)$ et si $\sigma \in \mathrm{Aut}_k C$, il se prolonge en un k -automorphisme $\tilde{\sigma}$ de $k(C)^s$ (considerer le corps fixe de σ) et $\tilde{\sigma}(k(C'))$ definit un revetement etale de $k(C)$ de groupe $(\mathbb{Z}/n\mathbb{Z})^{2g}$, c'est donc $\tilde{\sigma}(k(C'))$. Ainsi σ se prolonge en un k -automorphisme de $k(C')$. Ainsi $|\mathrm{Aut}_k C'| \geq n^{2g}|\mathrm{Aut}_k C|$; d'ou le resultat annonce.

Si la caracteristique de k est $p > 0$ la borne d'Hurwitz est facilement mise en defaut.

Proposition. Soit k un corps algebriquement clos de caracteristique $p > 3$; et C la courbe non singuliere de modele plan $y^2 = x^p - x$; then $\mathrm{Aut}_k(C) \simeq PGL_2(\mathbb{F}_p) \ltimes \mathbb{Z}/2\mathbb{Z}$. En particulier $|\mathrm{Aut}_k(C)| > 84(g-1)$.

Preuve: Plus generalement soit C/k la courbe projective lisse dont un modele plan est donne par l'equation hyperelliptique $y^2 = f(x)$; on peut supposer que $f(x) \in k[x]$ a toutes ses racines simples et que $\deg f = 2g+1$ (i.e. le lieu de branchement contient ∞).

Soit i l'automorphisme de C/k defini par $i(y)=-y,\ i(x)=x$, nous allons montrer que cet automorphisme est uniquement defini, on l'appelle l'involution hyperelliptique.

Considerons la forme differentielle $\omega=\frac{dx}{y}=2\frac{ydy}{f'(x)}$, on verifie facilement que $v_p(\omega)=0$ pour point $p\in C$ avec $x(p)\neq\infty$; ainsi le diviseur canonique K est lineairement equivalent a $(2g-2)\infty$ et plus generalement a $(2g-2)p_i$ (notez que $(x-x(p_i))\sim 2(\infty-p_i)$). Nous allons determiner l'espace lineaire $L((2g-2)\infty)$. Puisque $(x)_\infty=2\infty$ il suit que $\cup_{n\in\mathbb{N}}L(n\infty)=k[x]$, la cloture integrale de $k[x]$ dans $k(C)$. Un exercice montre que $k[x]\ =k[x]\oplus k[x]$. Soit $g=a(x)+yb(x)\in k[x]$, alors $v_\infty(a(x)+yb(x))=\inf(2\deg_x a,2g+1+2\deg_x b$ ainsi $L((2g-2)\infty)=\sum_{0\leq i\leq g-1}kx^i$ et donc si $p\in C$ est tel que $x(p)\neq x(p_i)$ alors $L(K-2p)=(x-x(p))^2k[x]\cap\sum_{0\leq i\leq g-1}kx^i$, ainsi $l(K-2p)=g-2$ et avec Riemann-Roch $l(2P)=l(K-2p)+2+1-g=1$; i.e. $L(2P)=k$. Ainsi les points tels que $l(2P)=2$ (i.e. les points de Weierstrass) sont les points de ramification; d'ou l'unicite de l'involution hyperelliptique.

Il suit que les k -automorphismes de C induisent un automorphisme de $k(x)$ qui permute les points de branchement; ainsi $\mathrm{Aut}C=G\ \ltimes\mathbb{Z}/2\mathbb{Z}$ ou $G\subset PGL_2(k)$ est le sous-groupe des homographies de la droite projective sur k qui permutent les points de branchement.

Dans l'exemple considere les points de branchements sont exactement les points rationnels sur $\mathbb{F}_p$; et puisqu'une homographie est donnee par l'image de $O,1,\infty$ il suit facilement que $G=PGL_2(\mathbb{F}_p)$; ainsi on a $|\mathrm{Aut}_k(C)|=2\frac{(p^2-1)(p^2-p)}{p-1}=2p(p^2-1)>84(g-1)$.

Theoreme. (Stichtenoth) Soit C une courbe de genre $g\geq 2$ sur un corps algebriquement clos k de aracteristique $p>0$, alors $|\mathrm{Aut}_k(C)|\leq 16g^4$ excepte dans le cas des courbes $y^q+y=x^{q+1}$ ou q parcourt les puissance de p ; auquel cas $g(C)=q(q-1)/2$ et $|\mathrm{Aut}_k(C)|=q^3(q^3+1)(q^2-1)$.

La taille du groupe des automorphismes en caracteristique p est conditionne par la complexite du groupe (par exemple etre abelien) et l'invariant de Hasse-Witt; on constate sur des exemples que lorsque le groupe est gros souvent $h=0$. Ainsi

Theoreme. (Nakajima) Soit C une courbe de genre $g\geq 2$ sur un corps algebriquement clos k de caracteristique $p>0$. Soit $G\subset\mathrm{Aut}_k(C)$ un sous-groupe abelien. Alors,

i) Si $p\neq 2$, alors $|G|\leq 4g+4$;

ii) Si $p=2$, alors $|G|\leq 4g+2$;

iii) Les estimations ci-dessus sont les meilleurs possible i.e. pour une infinite d'entiers $g\geq 2$, il existe C et G qui satisfont $g(C)=g$ et $|G|\leq 4g+4$ si $p\neq 2$, resp. $|G|\leq 4g+2$ si $p=2$.

Theoreme. (Nakajima) Soit C une courbe de genre $g\geq 2$ sur un corps algebriquement clos k de caracteristique $p>0$. On suppose que la courbe C est ordinaire alors $|\mathrm{Aut}_k(C)|\leq 84(g-1)g$

Réf'erences.

Automorphismes

Garcia, On higher order Weirstrass points and the finiteness of the automorphism group, Manuscripta Math 78, 413-416.

Nakajima, Equivariant form of the Deuring-Safarevic formula for Hasse-Witt invariants, Math. Z. 190 (1985), 559-566.

Nakajima, On abelian automorphism groups of algebraic curves, J. London Math. Soc. (2), 36, (1987), 23-32.

Nakajima, p-ranks and automorphism groups of algebraic curves, Transactions of AMS, 303, (1987), 595-607.

Stichtenoth, Uber die Automorphismengruppe eines algebraichen Funktionenkorpers von Primzahlcharakteristik, I,II, Arch. Math. 24 (1973), 527-544, 615-631.

Invariants de Hasse-Witt

Hasse H., Witt E. Zyklische unverzweigte Erweiterungskorper vom Primzahlgrade p uber einem algebraischen Functionenkorper der Charakteristik p, Monastsh. Math. Phys. 43 (1936), 477-492.

Serre, Cohomologie des varietes en caracteristique $p > 0$, 1960, Oeuvres completes,

Jacobson, Abstract derivation and Lie algebra, Trans. Math. Soc. 42 (1937), 206-224

Manin, Y. The Hasse-Witt-matrix of an algebraic curve. Transl. AMS, vol. 45, 245 (1965)

Cartier, P. Questions de rationnalite des diviseurs en geometrie algebrique, Bull. Soc. math. France, 86, 1958, 177-251

Samuel, P. Lectures on unique factorization domains. Notes by M. Pavman Murthy. Tata Institute of Fundamental Research Lectures on Mathematics, No. 30 Tata Institute of Fundamental Research, Bombay 1964 ii+84+iii pp.

Mathieu, Seminaire Bourbaki, Mars 99

CHAPITRE III

Deformation des revetements galoisiens de courbes algebriques

0. Rappels

Morphismes lisses

Definition. Soit A un anneau local noetherien d'ideal maximal $\mathcal{M}$, alors $\dim A \leq \dim_{A/\mathcal{M}} \frac{\mathcal{M}}{\mathcal{M}^2}$. On dit que A est regulier si l'inegalite precedente est une egalite.

Definition. Soit X un schema de type fini sur un corps k et k^{alg} une cloture algebrique de k . On dit que X est lisse en un point ferme $x \in X$ si les points de $X_{k^{alg}}$ dont l'image dans X est x , sont des points reguliers de $X_{k^{alg}}$. On dit que X est lisse sur k s'il est lisse en tous ses points fermes.

Definition. Soit $f : X \to Y$ un morphisme de type fini. On dit que f est lisse s'il est plat et si pour tout $y \in Y$ la fibre $X_y \to k(y)$ est lisse.

Anneau locaux henseliens

Lemme de Hensel. Soit R un anneau de valuation discrete complet. Soit f un polynome unitaire a coefficients dans R et tel que $\overline{f} = g_0 h_0$ ou g_0, h_0 sont unitaires et copremiers, alors f se factorise en $f = gh$ avec g et h unitaires et $\overline{g} = g_0$, $\overline{h} = h_0$.

Definition. Soit A un anneau local qui satisfait la conclusion du lemme de Hensel; on dit que A est henselien.

Theoreme. Soit A un anneau local; les proprietes suivantes sont equivalentes:

i) A est henselien

ii) Soient $f_1, ..., f_n \in A[T_1, ..., T_n]$, si il existe $a = (a_1, ..., a_n) \in k^n$, avec $\overline{f}_i(a) = 0,\ 1 \leq i \leq n$ et $\det((\partial \overline{f}_i / \partial \overline{T}_j)(a)) \neq 0$, alors il existe $a, b \in A^n$ tels que $\overline{b} = a$ et $f_i(b) = 0,\ 1 \leq i \leq n$

Voir Milne, Etale cohomology (l'implication i) donne ii) n'est pas facile!)

Dimension des courbes planes passant par m points donnes

Definition. Soit C/k une courbe algebrique reduite sur un corps k algebriquement clos. Un point $p \in C$ est dit point double ordinaire si $\mathcal{O}_{C,p}$ est reduit et si l'une des proprietes equivalentes suivantes est satisfaite:

i) $\mathcal{O}_{C,p} = \{f \in \mathcal{O}'_{C,p} \mid f(p_1) = f(p_2)\}$ ou $\mathcal{O}'_{C,p}$ est la cloture integrale de $\mathcal{O}'_{C,p}$ dans son anneau total des fractions et p_1, p_2 sont les ideaux maximaux de $\mathcal{O}'_{C,p}$ au-dessus de p .

ii) $\dim_k \mathcal{O}'_{C,p} / \mathcal{O}_{C,p} = 1$ et $\mathcal{O}'_{C,p}$ a deux ideaux maximaux

iii) $\hat{\mathcal{O}_{C,p}} \simeq \frac{k[[z_1, z_2]]}{z_1 z_2}$

Lemme. Soit k un corps algebriquement clos. Soit $G(X, Y, T) = 0$, une courbe plane irreductible de degre d dont les points singuliers sont des points doubles ordinaires $P_1, P_2, ..., P_m$. Soit

$$V(d, P_1, ..., P_m) := \{F \in k[X, Y, T],\ homogenes, d = \deg_{tot} F, F(P_i) = 0$$

alors $V \cup \{0\}$ est sous- k -espace vectoriel de $k^{\frac{d(d+3)}{2}+1}$ de dimension $\frac{d(d+3)}{2}+1-m$.

Preuve: a) Quitte a faire un changement lineaire homogene des variables, on se ramene a $G = G_0(X,T) + G_1(X,T)Y + ... + Y^d$ et $P_i = [x_i, y_i, 1]$ et $x_i \neq 0$. Soient $C = \mathrm{Proj}\frac{k[X,Y,T]}{G}$, $\Psi : Z \to C$, la normalisation de C .

b) $[x,y,t] \to [x,t]$ definit un morphisme fini de degre d , $\varphi : C \to \mathbb{P}^1$. On a $(x/t) = D' - D$ ou $\deg D = d$ (ona $D = \varphi^*(\infty)$). De plus soient $Q_i, Q'_i \in Z$ tels que $P_i = \Psi(Q_i) = \Psi(Q'_i)$.

c) Soit $E = -(Q_1+Q'_1+...+Q_n+Q'_n)+dD$. Soit $F \in V$, alors $F(x/t, y/t, 1) \in k(C)$ et $F(x/t, y/t, 1) \in L(E)$.

d) Soit $f \in L(E)$, alors on doit montrer qu'il existe $F(X,Y,T)$, homogene avec $f = F(x/t, y/t, 1)$ et $\deg_{tot} F \leq d$, $\deg_Y F < d$. Il suit que $F(P_i) = 0$ et que $F + G \in V$. Si donc $f_1, ..., f_s$ est une base de $L(E)$, il suit de d) et c) que $G, G+F_1, G+F_2, ..., G+F_s$ est une base de $V \cup \{0\}$. Donc $\dim V = l(E) + 1$.

On a $g(Z) = \frac{(d-1)(d-2)}{2} - m$ et $\deg E = d^2 - 2m$, $\deg K = 2g(Z) - 2 = (d-1)(d-2) - 2m$; ainsi $\deg(K - E) < 0$ et donc Riemann-Roch donne $l(E) = l(E) - l(K - E) = \deg E + 1 - g(Z) = \frac{d(d+3)}{2} + 1 - m$.

1. Deformation des courbes lisses

Dans ce paragraphe; k designe un corps algebriquement clos de caracteristique $p > 0$ et C une courbe algebrique projective lisse connexe sur k .

La premiere question naturelle qui se pose pour passer a la caracteristique 0 est trouver un relevement en caracteristique 0 ; precisement:

Definition. Soit R un anneau de valuation discrete fini sur l'anneau des vecteurs de Witt $W(k)$ et $K := \mathrm{Fr}R$. On appelle relevement sur R de C/k un schema $\mathcal{C}$ propre et lisse sur R dont la fibre speciale $\mathcal{C}_s := \mathcal{C} \times_R k$ est isomorphe sur k a C .

Remarque 1. Le schema $\mathcal{C}/R$ est une surface reguliere: si $x \in C$ est un point ferme l'anneau $\mathcal{O}_{\mathcal{C},x}$ est un anneau local et $\mathcal{O}_{\mathcal{C},x}/(\pi)$ est l'anneau local de la fibre speciale qui est lisse par hypothese. Soit donc t_x un parametre uniformisant et $T \in \mathcal{O}_{\mathcal{C},x}$, un relevement, alors (π, T) est l'ideal maximal $\mathcal{M}$ de $\mathcal{O}_{\mathcal{C},x}$; ainsi $\dim \mathcal{O}_{\mathcal{C},x} = 2$ et donc $\dim_k \mathcal{M}/M^2 \geq 2$. Puisque $\mathcal{M}$ est engendre par deux elements on a egalite.///

Attention! la R -algebre $R[X,Y]/(XY - \pi)$ definit une surface reguliere bien qu'elle ne soit pas lisse.

Remarque 2. On peut caracteriser l'anneau local d'une surface lisse par son complete. Le complete $\mathcal{M}$ -adique de l'anneau local $\mathcal{O}_{\mathcal{C},x}$ est isomorphe a $R[[T]]$. Montrons cela: l'homomorphisme de R algebres $f : R[T] \to A := \mathcal{O}_{\mathcal{C},x}$ defini par $f(T) = T$ est continu et induit un homomorphisme surjectif au niveau des completes $f : R[[T]] \to \hat{A}$. Voyons qu'il est injectif; en effet sinon l'anneau $\hat{A}$ serait de dimension < 2 ; ce qui contredit l'egalite $\dim A = \dim \hat{A}$ (cf. Matsumura, p.175).

Proposition. Soit $g := g(C)$, le genre de la courbe C/k . Soit $\mathcal{C}$ un relevement sur R de C . Alors la fibre generique $\mathcal{C}_\eta = \mathcal{C} \times_R K$ est une courbe propre lisse connexe sur K de genre arithmetique $\dim_K \mathrm{H}^1(\mathcal{C}_\eta, \mathcal{O}_{\mathcal{C}_\eta})$ est egal a g .

Preuve. C'est une propriete generale des morphismes propres et plat. Disons ici que l'on peut montrer que $\mathcal{C}$ est un R -schema projectif de dimension relative 1; en particulier $\mathcal{C} = \mathrm{Proj} S$ pour S une R -algebre plate homogene engendree par ses elements de degre 1. Le polynome de Hilbert de S est un polynome $P_{\mathcal{C}}(t) = at + b$ tel que pour tout $n \geq 0$, $P_{\mathcal{C}}(n) = \chi(\mathcal{O}_{\mathcal{C}}(n))$ et pour $n >> 0$, $P_{\mathcal{C}}(n) = \dim_R S_n$. Ainsi la platitude de S donne l'egalite des caracteristique d'Euler des faisceaux structuraux aux fibres generiques et speciales. Puisque ces fibres sont lisses, on conclut a l'egalite des genres.

Theoreme. On consider C comme au-dessus, alors il existe un relevement $\mathcal{C}$ sur $W(k)$ de C/k ; en particulier $\mathcal{C}_{W(k)} \times R$ est un relevement de C sur R .

Preuve: Il faut bien se rendre compte qu'il y a une vrai difficulte. Par exemple la courbe C/k est en general donnee par une famille de polynomes homogenes; si on releve stupidement ces polynomes; l'ideal engendre sur R peut donner des relations nouvelles modulo π (la condition de platitude empeche ce phenomene!). Mumford et Serre ont donne des exemples de varietes lisses sur k de dimension > 1 qui ne se relevent pas en caracteristique 0 . Par contre un cas simple dans lequel des relations n'apparaissent pas est celui des hypersurfaces (l'ideal est alors principal!). La preuve que nous presentons dans le cas des courbes est due a H. Popp (Zur Reduktionstheorie algebraischer Funktionenkorper vom Transzendenzgrad. I. Existenz einer regularen Reduktion zu vorgegebenem Funktionenkorper als Restklassenkorper. Arch. Math. (Basel) 17 1966 510–522).

I. Il existe C_{sing}/k une courbe projective integre dans $\mathbb{P}^2_k$ definie par le polynome homogene $f(X,Y,T)$ birationnelle a C/k et dont les points singuliers $(p_i = [x_i, y_i, t_i])_{1 \leq i \leq m}$ soient des points doubles ordinaires.

Pour une preuve voir Hartshorne pp. 309-311. On peut cependant faire quelques commentaires sur la demonstration. On sait que C est projective, i.e. C est un ferme de dimension 1 d'un $\mathbb{P}^n_k$. On s'interesse au plus petit tel entier n . L'idee est de faire des projections issues d'un point O sur des hyperplans ne contenant pas O . Une telle projection pr induit une immersion fermee de C ssi O n'appartient pas a une droite passant par deux points (confondus ou pas) de la courbe C (notez qu'alors pr induit un isomorphisme des espaces tangents; ainsi si x est regulier il en est de meme de $pr(x)$. Il reste a savoir quand il est possible de trouver $O \in \mathbb{P}^n_k$ convenable. Ceci se fait par un argument de comptage de dimensions. On note $\mathrm{Sec}(C)$ la reunion des secantes a C , alors $\mathrm{Sec}(C)$ est localement ferme dans $\mathbb{P}^n$; c'est l'image de $(C \times C - \Delta) \times \mathbb{P}^1$ dans $\mathbb{P}^n$ (ou δ designe la diagonale de $C \times C$); c'est donc de dimension ≤ 3 . De meme la reunion des tangentes est l'image de $C \times \mathbb{P}^1$ et donc de dimension ≤ 2 . Ainsi des projections successives donnent un plongement de C dans $\mathbb{P}^3_k$. En general il n'est pas possible de trouver un plongement dans $\mathbb{P}^2_k$ puisque les courbes planes non singulieres ont un genre de la forme $\dfrac{(d-1)(d-2)}{2}$ (par exemple une courbe de genre 2 n'est pas plane!). Cependant on peut aller a $\mathbb{P}^2$ si l'on accepte des points doubles ordinaires comme singularites; puisqu'on peut enlever les secantes tangentes.

II. Il existe $F(X,Y,T) \in R[X,Y,T]$ homogene, $\deg_{tot} F = \deg_{tot} f = d$, $\overline{F} = f$ et tel que la courbe $Y \subset \mathbb{P}^2_k$ definie par le polynome $F(X,Y,T)$ admet m points singuliers

$(P_i = [X_i, Y_i, T_i])_{1 \le i \le m}$ qui sont des points doubles ordinaires; de plus si on normalise les coordonnees de P_i par $0 = \inf(v(X_i), v(Y_i), v(T_i))$ alors $\overline{P}_i := [\overline{X}_i, \overline{Y}_i, \overline{T}_i] = p_i$ pour $1 \le i \le m$.

Preuve: Quitte a faire un changement lineaire des variables, on se ramene au cas ou les points singuliers $p_i = [x_i, y_i, t_i]$ satisfont $t_i = 1$; ce qui ramene la recherche de F a un probleme affine.

Considerons les polynomes $F_t := \sum_{i+j \le d} Z_{i,j} X_t^i Y_t^j \in R[X_t, Y_t, Z_{i,j}]$, $1 \le t \le m$ et $G_t := \dfrac{\partial F_t}{\partial X_t}$, $H_t := \dfrac{\partial F_t}{\partial Y_t}$. Par hypothese il existe $\underline{a} := [x_t, y_t, z_{i,j}]$ a coordonnees dans k tel que le systeme pour $1 \le t \le m$

$$(*) \begin{array}{r} F_t(X_t, Y_t, Z_{i,j}) = 0 \\ G_t(X_t, Y_t, Z_{i,j}) = 0 \\ H_t(X_t, Y_t, Z_{i,j}) = 0 \end{array}$$

On peut facilement calculer la matrice jacobienne modulo π en $\underline{a}$. C'est la matrice $3m \times (\dfrac{(d+1)(d+2)}{2} + 2m)$

$$J(\underline{a}) = \begin{pmatrix} ...x_t^i y_t^j.... & ...0... & ...0... \\ \vdots & \vdots & \vdots \\ ...i x_t^{i-1} y_t^j.... & ...0\dfrac{\partial^2 F_t}{\partial X_t^2}(p_t)0... & ...0\dfrac{\partial^2 F_t}{\partial Y_t \partial X_t}(p_t)0... \\ ...j x_t^i y_t^{j-1}.... & ...0\dfrac{\partial^2 F_t}{\partial X_t \partial Y_t}(p_t)0... & ...0\dfrac{\partial^2 F_t}{\partial Y_t^2}(p_t)0... \\ \vdots & \vdots & \vdots \end{pmatrix}$$

Puisque les determinants 2×2 , $\det \begin{vmatrix} \dfrac{\partial^2 F_t}{\partial X_t^2}(p_t) & \dfrac{\partial^2 F_t}{\partial Y_t \partial X_t}(p_t) \\ \dfrac{\partial^2 F_t}{\partial X_t \partial Y_t}(p_t) & \dfrac{\partial^2 F_t}{\partial Y_t^2}(p_t) \end{vmatrix}$ ne sont pas nuls, le lemme du paragraphe 0 qui donne la dimension des courbes planes passant par m points donnes montre que le rang de $J(\underline{a})$ est $3m$ (notez que l'on a bien $\dfrac{(d+1)(d+2)}{2} + 2m \ge 3m$, puisque le genre de C_{sing} est $\dfrac{(d-1)(d-2)}{2} - m \ge 0$). D'autre part la propriete de relevement sur un anneau henselien des solutions d'un systeme d'equations algebriques rappelle au paragraphe 0; montre qu'il existe $\underline{b} = (X_t, Y_t, Z_{i,j})$ dans $R^{\frac{(d+1)(d+2)}{2}+2m}$ qui satisfait $(*)$ et tel que $\overline{b} = a$. Le polynome $F(X, Y, T) = \sum_{i+j \le d} Z_{i,j} X^i Y^j T^{d-i-j}$ est solution de II.

III. Soit $\mathcal{C}_{sing} := \mathrm{Proj} \dfrac{R[X, Y, T]}{(F)}$, c'est un R -schema projectif plat sur R de dimension relative 1. La fibre generique est une courbe plane de genre geometrique $\dfrac{(d-1)(d-2)}{2} - m$, et la fibre speciale est C_{sing} . Soit $\mathcal{C} \to \mathcal{C}_{sing}$ la normalisation; alors $\mathcal{C}$ satisfait le theoreme. L'idee pour prouver cela est la suivante: l'anneau local $\mathcal{C}_{sing}$ au point generic de la fibre speciale est reduit de dimension 1et son ideal maximal est engendre par π ; ainsi c'est un anneau de valuation discrete de corps de fraction $k(\mathcal{C}_{sing})$, il est donc integralement clos; ainsi la fibre speciale de la R -courbe est integre et birationnelle a C_{sing} . Puisque la fibre generique est lisse un calcul de la caracteristique d'Euler-Poincare permet de conclure.

2. Deformation des courbes avec un groupe automorphismes

i) Relevement global

On reprend les notations du paragraphe precedent. On notera (C,G) le couple forme d'une courbe C propre lisse sur k et G un sous-groupe fini de $\mathrm{Aut}_k(C)$. On se propose d'etudier la deformation en carateristique 0 d'une courbe munie d'un groupe fini d'automorphismes, le cas precedement traite correspondant a une courbe munie du groupe trivial. Comme on le verra il est trop restrictif de se limiter a la recherche d'un relevement sur $W(k)$; il faut considerer eventuellement R, un anneau de valuation discrete fini au-dessus de $W(k)$.

Definition. On appelle relevement sur R de $(C, G \subset \mathrm{Aut}_k C)$, la donnee d'un couple $(\mathcal{C}, i : G \to \mathrm{Aut}_R \mathcal{C})$ ou $\mathcal{C}$ est un relevement sur R de C tel que $i : G \to \mathrm{Aut}_R \mathcal{C}$ induise modulo π l'inclusion $G \subset \mathrm{Aut}_k C)$ (apres identification de C et $\mathcal{C}_s$).

Il suit du chapitre precedent que si (C,G) ne satisfait pas la borne d'Hurwitz $|G| \leq 84(g-1)$, il n'y a pas de relevement sur tout R. Il s'agit d'une obstruction globale au relevement.

ii) Relevement local

Nous nous proposons d'etudier les obstructions locale au relevement. Precisement supposons donne $(\mathcal{C}, G)$ un relevement sur R de (C,G) et soit $x \in \mathcal{C}$ un point ferme; alors l'anneau local $\mathcal{O}_{\mathcal{C},x}$ est lisse sur R il est equivalent de dire que son complete $\mathcal{M}$-adique est isomorphe a $R[[Z]]$ et modulo π il donne $k[[z]]$, le complete de l'anneau $\mathcal{O}_{C,x}$ (z est parametre uniformisant en x). Soit $I_x := \{\sigma \in G \in \mathrm{Aut}_C \mid \sigma(x) = x\}$, c'est le groupe d'inertie de G en $x \in C$ (c'est aussi le groupe de decomposition puisque k est algebriquement clos) et c'est un groupe de k-automorphismes de $k[[z]]$. L'existence du relevement $(\mathcal{C}, G)$ sur R permet de considerer aussi x comme point de $\mathcal{C}$ ainsi $I_x = \{\sigma \in G \in \mathrm{Aut}_{\mathcal{C}} \mid \sigma(x) = x\}$ est un groupe de R-automorphismes de $R[[z]]$ qui induit modulo π, $I_x \subset \mathrm{Aut}_k k[[z]]$. On est ainsi amene a considerer la condition de relevement local:

Definition. Soit G un groupe fini et $f : G \to \mathrm{Aut}_k k[[z]]$ un homomorphisme injectif. Nous dirons que f a la propriete de relevement si on a un diagramme commutatif d'homomorphismes de groupes:

$$\begin{array}{ccc} \mathrm{Aut}_k k[\![z]\!] & \longleftarrow & \mathrm{Aut}_R R[\![Z]\!] \\ f\uparrow & \nearrow & \\ G & & \end{array}$$

Utilisant la geometrie rigide ou formelle on montre le theoreme suivant:

Theoreme du Principe local-global. Soit C une courbe propre et lisse sur k et $f : G \to \mathrm{Aut}_k C)$ une realisation du groupe fini G comme groupe d'automorphismes de C/k. Soit $x \in C$ et $I_x \subset G$ le groupe d'inertie de G en x; il opere via f comme groupe d'automorphismes du complete $k[[z]]$ de l'anneau local de C en x. Alors $(C, f : G \to \mathrm{Aut}_k C)$ a la propriete de relevement sur R si et seulement si pour tout $x \in C$, $f_{|I_x \subset G} : I_x \to \mathrm{Aut}_k k[[z]]$ a la propriete de relevement.

Ce theoreme montre que les obstructions sont de nature locales; il devient alors interessant de comprendre du point de vue local pourquoi (C, G) avec C donne par l'equation $y^2 = x^p - x$ pour $p > 3$ et $G = \mathrm{Aut}_k C$ n'a pas la propriete de relevement. Nous allons d'abord examiner plus en detail la geometrie du R -schema $\mathrm{Spec} R[[Z]]$.

3. Geometrie du disque ouvert p -adique

Dans ce paragraphe R designe un anneau de valuation discrete fini sur l'anneau des vecteurs de Witt sur k et π est un parametre uniformisant. On note $K := \mathrm{Fr} R$ et $\tilde{K}$ une cloture algebrique de K equippee de l'unique valeur absolue prolongeant celle de K .

Lemme de Division. Soient $f, g \in R[[Z]]$ et supposons que $f = a_0 + a_1 Z + ...$, avec $a_i \in \pi R$ pour $0 \leq i \leq n-1$ et $a_n \in R^{\times}$. Alors il existe un unique couple (q, r) avec $q \in R[[Z]]$ et $r \in R[Z]$, $\mathrm{deg} r \leq n-1$ et

$$g = qf + r$$

.

Preuve: On montre l'unicite qui se ramene a considerer l'equation $qf + r = 0$ avec les conditions du dessus. Si q, r ne sont pas nuls, on peut supposer que π ne divise pas r ou q . En reduisant modulo π on voit que $\pi | r$ et donc que $\pi | qf$ et puisque π ne divise pas f alors $\pi | q$; ce qui donne une contradiction. Ainsi $q = r = 0$.

L'existence est un petit peu plus difficile. On definit un operateur de decalage $\tau = \tau_n$: $R[[Z]] \to R[[Z]]$ par la formule:

$$\tau(\sum_{i \geq 0} b_i Z^i) = \sum_{i \geq n} b_i Z^{i-n}$$

Clairement τ est R -lineaire et satisfait:

i) $\tau(Z^n h(Z)) = h(Z)$ pour tout $h(Z) \in R[[Z]]$;

ii) $\tau(h(Z)) = 0$ ssi $h(Z) \in R[Z]$ et $\mathrm{deg} h(Z) \leq n-1$

On peut ecrire

$$f(Z) = \pi P(Z) + Z^n U(Z),$$

ou $P(Z) \in R[Z]$ et $\mathrm{deg} P(Z) < n$ et $U(Z) = a_n + a_{n+1} Z + ... = \tau(f(Z))$. Puisque $a_n \in R^{\times}$, $U(Z)$ est une unite de $R[[Z]]$. Soit

$$q(Z) = \frac{1}{U(Z)} \sum_{j \geq 0} (-1)^j \pi^j (\tau \circ \frac{P}{U})^j \circ \tau(g)$$

ou par exemple

$$(\tau \circ \frac{P}{U})^2 \circ \tau(g) = \tau(\frac{P}{U} \tau(\frac{P}{U} \tau(g)))$$

Remarquez que chaque terme de la somme peut contribuer dans le terme constant mais le facteur π^j rend la somme convergente. Ainsi $q(Z) \in R[[Z]]$. Puisque

$$qf = \pi q P + Z^n q U,$$

on a

$$\tau(qf) = \pi\tau(qP) + \tau(Z^n qU) = \pi\tau(qP) + qU.$$

Mais

$$\pi\tau(qP) = \pi(\tau \circ \frac{P}{U}) \circ (\sum_{j\geq 0} (-1)^j \pi^j (\tau \circ \frac{P}{U})^j \circ \tau(g)) = \tau(g) - qU.$$

Ainsi

$$\tau(qf) = \tau(g).$$

Par ii) il suit que $g = qf + r$ et $\deg r \leq n-1$ ./ / /

Definition. $P(Z) \in R[Z]$ est dit distingue si

$$P(Z) = Z^n + a_{n-1}Z^{n-1} + ... + a_0$$

avec $a_i \in \pi R$ pour $0 \leq i \leq n-1$.

Theoreme de Preparation de Weierstrass. Soit

$$f(Z) = \sum_{i\geq 0} a_i Z^i \in R[[Z]],$$

avec $a_i \in \pi R$ pour $0 \leq i \leq n-1$ et $a_n \in R^\times$. Alors f s'ecrit de maniere unique sous la forme $f(Z) = P(Z)U(Z)$, ou $U(Z) \in R[[Z]]$ est une unite et $P(Z)$ est un polynome distingue de degre n .

Plus generalement, si $f(Z) \in R[[Z]]$ est non nul, il y a une unique ecriture:

$$f(Z) = \pi^d P(Z)U(Z)$$

ou P, U sont comme precedement et $d \in \mathbb{N}$

Preuve: La seconde partie suit clairement de la premiere. Prouvons la premiere partie: soit $g(Z) = Z^n$ comme dans le lemme de division ci-dessus. Alors

$$Z^n = q(Z)f(Z) + r(Z)$$

avec $\deg r \leq n-1$.

Puisque

$$q(Z)f(Z) \equiv q(Z)Z^n(a_n + ...) \mathrm{mod} \pi,$$

on doit avoir $r(Z) \equiv 0 (\mathrm{mod} \pi)$. Ainsi $P(Z) = Z^n - r(Z)$ est un polynome distingue de degre n . Soit q_0 le terme constant de $q(Z)$. Comparant les coefficients de Z^n , on a $1 \equiv q_0 a_n \mathrm{mod} \pi$. Ainsi $q_0 \in R^\times$ et donc $q(Z)$ est une unite. Soit $U(Z) := 1/q(Z)$. Alors $f(Z) = P(Z)U(Z)$ comme desire. Puisque tout polynome distingue de degre n peut s'ecrire $P(Z) = Z^n - r(Z)$, on peut transformer l'equation $f(Z) = P(Z)U(Z)$ en

$$Z^n = U(Z)^{-1} f(Z) + r(Z)$$

L'unicite dans le lemme de division montre l'unicite de P et U . / / /

Geometrie du disque ouvert sur R

Soit $\mathcal{P}$, un ideal premier non nul de $R[[Z]]$.

- **Les points de la fibre speciale** $X_{(k)} := X \times_R k$ **.**

Si $\pi \in \mathcal{P}$, alors $\pi = \mathcal{P}$ ou bien il existe $f \in \mathcal{P} - (\pi)$ alors le theoreme de preparation de Weierstrass montre que l'on peut supposer que $f = P$ est un polynome distingue et puisque $\pi \in \mathcal{P}$, on peut supposer que $P = Z^n$ ainsi $\mathcal{P} = (\pi, Z)$.

- **Les points de la fibre generique** $X_{(K)} := X \times_R K$ **.**

Supposons donc que $\pi \notin \mathcal{P}$. Soit $f \in \mathcal{P}$ non nul alors le theoreme de preparation de Weierstrass montre que l'on peut supposer que $f = P$ est un polynome distingue irreductible sur K . Si $g \in \mathcal{P}$; le lemme de division montre que $g = qf + r$ avec $\deg r < \deg f$; ainsi $r \in \mathcal{P}$; de l'irreductibilite de f il suit que $r = 0$ et donc $\mathcal{P} = (f)$. Notez que les racines d'un polynome distingue sont dans $\tilde{R} := \{z \in \tilde{K} \mid |z| < 1\}$; c'est ce fait qui nous amene par abus de langage a appeler X le disque ouvert sur R (il y a abus car la bonne terminologie est modele minimal du disque ouvert sur R). En particulier les points rationnels sur R sont les ideaux de la forme $Z - z$ avec $z \in \pi R$ et s'identifie avec l'ideal maximal πR . Plus generalement $X_{(K)}$ s'identifie avec $\tilde{R}$ modulo l'action du groupe de Galois $\mathrm{Gal}(K^{alg}/K)$.

Automorphismes du disque ouvert ayant au moins un point fixe

Soit σ un R -automorphisme of $R[[Z]]$. Il est uniquement determine par l'image de Z

$$\sigma(Z) = a_0 + a_1 Z + ... + a_i Z^i + ...,$$

et puisque l'anneau $R[[Z]]$ est local un tel homomorphisme est continu et donc $a_0 \in \pi R$ et puisque c'est un automorphisme $a_1 \in R^{\times}$.

σ induit un automorphisme du R -schema X , que l'on note $\tilde{\sigma}$ dont l'action sur les points rationnels est donnee par

$$\tilde{\sigma}((Z - z)) = ((Z - \sum_{i \geq 0} a_i z^i))$$

Un tel point rationnel est un point fixe si et seulement $z \in \pi R$ et $z = \sum_{i \geq 0} a_i z^i$. Plus generalement, $P \in X$ est un point fixe ssi $P = (\pi)$ ou (0) ou $P \supset (\sigma(Z) - Z)$. Dans ce qui suit nous referrons a ce dernier ensemble quand nous parlons de points fixes et nous parlerons de points fixes geometrique pour designer les points qu'ils definissent dans la fibre generique geometrique.

- **Existence de points fixes**

Soit σ un R -automorphisme de $R[[Z]]$ qui n'induit pas l'identite modulo π , alors σ a au moins un point fixe.

Proof. Using the writing above, suppose first that $a_1 \equiv 1 \mod \pi R$. Then since σ doesn't induce the identity residually, one knows that there is an a_i $(i > 1)$ which is a unit. Let m be the first $i > 1$ such that a_i is a unit. Then by the Weierstrass Preparation Theorem the series

$$\sigma(Z) - Z = f_m(Z) u(Z)$$

where $f_m(Z)$ is a distinguished polynomial of degree m and the series $u(Z)$ is a unit in $R[\![Z]\!]$. It follows that the points of X which contain $f_m(Z)$ are the fixed points for σ. Finally if $a_1 \not\equiv 1 \bmod \pi R$, we repeat the above argument with $m = 1$. (Note that in this case σ has only one fixed point which is rational.)

- **Automorphismes d'ordre fini**

We shall need the following lemmas:

Lemma 1. ([C] Lemma 14 p. 245) Let $e \in \mathbb{N}^\times$ and $f(Z) \in R[\![Z]\!]$, such that $f(Z) \equiv Z \bmod (Z^2)$ and defines an R-automorphism of $R[\![Z]\!]$ of order e. Then $e = 1$.

We shall also use a weak form of Lemma 15 from [C].

Lemma 2. Consider the series $f(Z) = a_0 + a_1 Z + \cdots + a_n Z^n + \cdots \in R[\![Z]\!]$, $a_0 \in \pi R$, and for $e \in \mathbb{N}^\times$ let $f^e(Z) = b_0 + b_1 Z + \cdots$. Then one has $b_0 \equiv a_0(1 + a_1 + \cdots + a_1^{(e-1)}) \bmod a_0^2 R$ and $b_1 \equiv a_1^e \bmod a_0 R$.

Proof. By induction on e: Check that

$$\begin{aligned} f^{(e+1)}(Z) &= a_0 + a_1 f(Z) + \cdots \\ &= a_0 + a_1(b_0 + b_1 Z + \cdots) + a_2(b_0 + b_1 Z + \cdots)^2 + \cdots \\ &= a_0 + a_1 b_0 + a_2 b_0^2 + \cdots + Z(a_1 b_1 + 2a_2 b_0 b_1 + \cdots) + \cdots \end{aligned}$$

From this one deduces that $a_0 + a_1 b_0 + a_2 b_0^2 + \cdots \equiv a_0 + a_1 b_0 \bmod a_0^2 R$, and $a_1 b_1 + 2a_2 b_0 b_1 + \cdots \equiv a_1 b_1 \bmod a_0 R$.

Corollary 3. If σ is an automorphism of $R[\![Z]\!]$ of order e, with $(e,p) = 1$, then σ has a rational fixed point.

Proof. Suppose $a_0 \neq 0$, $\sigma(Z) = a_0 + a_1 Z + \cdots$ and that $\sigma^e(Z) = b_0 + b_1 Z + \cdots = Z$. Then by the Lemma above $1 + a_1 + \cdots + a_1^{(e-1)} \equiv 0 \bmod a_0 R$. Hence as $e \not\equiv 0 \bmod p$, it follows that $a_1 \not\equiv 1 \bmod \pi R$. Therefore the automorphism σ doesn't induce the identity residually, and hence by the above paragraph on Existence of sixed points, it must have a rational fixed point.

Remark. The analysis in Coleman [C], section 5, is more precise: namely he proves that there are no automorphism of order p over $R = W(k)$, for $p > 3$.

- **Linearization.** *Let e be an integer prime to p and $f(Z) \in R[\![Z]\!]$ a power series with $f(Z) \equiv sZ \bmod (Z^2)$, which defines an R-automorphism of $R[\![Z]\!]$ of order e. Then there exists $Z' \in ZR[\![Z]\!]$ such that $f(Z') = sZ'$.*

Proof. Observe that as that the order of f is e then s is an e-th root of unity. Consider the Lagrange-Hilbert resolvant:

$$Z' = Z + s^{-1} f(Z) + s^{-2} f^2(Z) + \ldots + s^{-(e-1)} f^{e-1}(Z).$$

Then $f(Z') = sZ'$, and moreover $Z' \equiv eZ \bmod (Z^2)$, with e a unit in R as $(e,p) = 1$.

The following example shows that not every automorphism of finite order is linearizable.

Example. Let ζ be a primitive p-th root of unity and $\sigma(Z) = \zeta Z(1+Z)^{-1}$, then $\sigma^p(Z) = Z$ and 0, $\zeta - 1$ are the fixed points.

- **Comparison of the different.**

Let σ be an automorphism of $R[\![Z]\!]$ of finite order n. We denote the inertia group at π in $\langle\sigma\rangle$ by I_π and assume that it is the identity group so that σ has at least one fixed point. Enlarging R we can assume that 0 is such a fixed point and that $\sigma(Z) = \zeta Z(1 + a_1 Z + \cdots)$, where ζ is a primitive n-th root of unity (see Lemma 1 above).

Claim 1. *Let* $T = Z\sigma(Z)\cdots\sigma^{n-1}(Z) = \epsilon Z^n(1+\cdots)$ *where* $\epsilon = (-1)^{(n-1)}$. *Then* $R[\![Z]\!]^{\langle\sigma\rangle} = R[\![T]\!]$.

Proof. From [Bourbaki, Alg Com], chap. 7, corollary, p. 40, one knows that $R[\![Z]\!]$ is a finite free $R[\![T]\!]$-module of rank n, generated by $1, Z, Z^2, \ldots, Z^{n-1}$. On the other hand by a dimension consideration it follows that $\mathrm{Fr}(R[\![Z]\!]^{\langle\sigma\rangle}) = \mathrm{Fr}(R[\![T]\!])$. As $R[\![Z]\!]^{\langle\sigma\rangle}$ is integral over $R[\![T]\!]$ which is integrally closed, the claim follows.

Claim 2. *Let* d_η, *resp.* d_s, *be the degrees of the generic, resp. special differents for the extension* $R[\![Z]\!]/R[\![T]\!]$. *Then* $d_\eta = d_s$.

Proof. Let $f(X) = \prod_{0\le i<n} (X - \sigma^i(Z))$ be the irreducible polynomial of Z over $R[\![T]\!]$. Then $f'(Z) = p(Z)u(Z)$ where $p(Z)$ is a distinguished polynomial and $d_\eta = \deg_Z p(Z)$. For the special different we have

$$d_s = v_z\big(\prod_i (z - \overline{\sigma}^i(z))\big)$$

and so the result follows by the Weierstrass Preparation Theorem. We remark that the same equality for the different holds for towers of such cyclic extensions, see also 3.4.

Claim 3. *Let* F *be the set of geometric fixed points of* σ *and suppose* m *is the first integer such that the coefficient* a_m *in* $\sigma(Z) - Z = (\zeta - 1)Z + \cdots + \zeta a_i Z^{i+1} + \cdots$ *is a unit. Then* $|F| = m + 1$.

Proof. First note that by assumption $I_\pi = \mathrm{Id}$, the identity group, so the integer m exists. If $\zeta \not\equiv 1 \bmod \pi$, then σ has a unique fixed point. Suppose $\zeta \equiv 1 \bmod \pi$ (i.e. n is a p-power). Then $m > 0$, and the geometric fixed points are given by the zeros of the distinguished polynomial $f_m(Z)$ of $\sigma(Z) - Z$. Let Z_0 be such a zero, then the derivative at Z_0

$$\sigma'(Z_0) = 1 + f'_m(Z_0)u(Z_0)$$

is a primitive n-th root of unity ($\mathrm{o}(\sigma) = n$) and so $f'_m(Z_0) \neq 0$. Hence the roots are distinct, thus giving $m+1$ geometric fixed points. Observe that if $n = p$ this corroborates the previous fact $d_\eta = d_s$.

Remark. One checks that the integer m appearing in 3.3 is the conductor of the residual extension $k[\![z]\!]/k[\![z]\!]^{\langle\sigma\rangle} = k[\![t]\!]$.

It is known that claim 2 has a converse in the germ of curves context which follows from a formula given by Kato [K], section 5. Namely, given a finite morphism of strict henselizations of local rings of R-curves at closed points one can express the difference between the degrees of the generic and special differents in terms of Milnor numbers at the closed point. As our context is that of completions of local rings, for the convenience of the reader we give an adapted proof in the special case we use.

• **Local criterion for good reduction.** *Let* $A = R[\![T]\!]$ *and* B *be a finite* A*-module which is a normal integral local ring, and set* $A_K = A \otimes_R K$, *resp.* $B_K = B \otimes_R K$. *We assume that* $B/\pi B = B_0$ *is reduced and setting* $A_0 := A/\pi A$, *that the extension* B_0/A_0 *is generically étale. Let* $\tilde{B}_0$ *be the integral closure of* B_0 *and define* $\delta_k(B) = \dim_k \tilde{B}_0/B_0$. *Let* d_η *resp.* d_s *be the degrees of the generic resp. special differents, i.e. the degrees of the differents for the extensions* B_K/A_K *resp.* B_0/A_0. *Then* $d_\eta = d_s + 2\delta_k(B)$ *and moreover if* $d_\eta = d_s$ *it follows that* $\delta_k(B) = 0$ *and* $B = R[\![Z]\!]$.

Proof. It follows from EGA IV, chapter 0, corollary to Proposition 17.3.4, that B is a free A-module say of rank r. Following [Serre , Corps locaux], chapter III we consider $\det_A(B) := \bigwedge_A^r B$ and define

$$\mathrm{T}_{B/A} : \det_A(B) \otimes_A \det_A(B) \longrightarrow A \qquad (*)$$

to be the homomorphism induced by the symmetric bilinear form:

$$B \times B \longrightarrow A; \quad (x, y) \mapsto \mathrm{Tr}_{B/A}(xy),$$

where $\mathrm{Tr}_{B/A} : B \longrightarrow A$ is the trace map. Then $\mathrm{Im}\,\mathrm{T}_{B/A} = cA$ for some $c = \pi^n P(T)$ in A with $n \geq 0$ and $P(T)$ a distinguished polynomial. Tensoring $(*)$ by K we obtain

$$\mathrm{T}_{B_K/A_K} : \det_{A_K}(B_K) \otimes_{A_K} \det_{A_K}(B_K) \longrightarrow A_K.$$

It follows $d_\eta = \mathrm{Coker}\,\mathrm{T}_{B_K/A_K} = \deg P$. On the other hand setting $\mathrm{T}' = \pi^{-n}\mathrm{T}_{B/A}$, $\mod \pi$ this induces a homomorphism

$$\mathrm{T}'_0 : \det_{A_0}(B_0) \otimes_{A_0} \det_{A_0}(B_0) \longrightarrow A_0.$$

Moreover $\mathrm{Im}\,\mathrm{T}'_0 = (c/\pi^n)A_0 = t^{\deg P} A_0$ so $\dim_k \mathrm{Coker}\,\mathrm{T}'_0 = \deg P$.

Now consider $\tilde{\mathrm{T}}'_0$ to be the homomorphism defined as in $(*)$ from the extension $A_0 \subset \tilde{B}_0$:

$$\tilde{\mathrm{T}}'_0 : \det_{A_0}(\tilde{B}_0) \otimes_{A_0} \det_{A_0}(\tilde{B}_0) \longrightarrow A_0.$$

Then $\dim_k \mathrm{Coker}\,\tilde{\mathrm{T}}'_0 = d_s$ and it follows from [Serre, Corps locaux], Chap. III, Proposition 5, that $\dim_k \mathrm{Coker}\, T'_0 = d_s + 2\delta_k(B)$. Collecting the previous equalities we obtain the desired equality.

If $d_\eta = d_s$, then $B_0 = \tilde{B}_0 = k[\![z]\!]$ and it follows from [Bourbaki, Alg com], chapter 9, §2, No. 5, that $B = R[\![Z]\!]$.

• **Obstructions to liftings of automorphisms.**

Soit G un groupe fini d'automorphisme ayant la propriete de relevement. On suppose que G est abelien alors G est cyclique ou G est un p-groupe. La raison immediate est que sinon G contient un sous groupe de la forme $(Z/pZ)^2 \times Z/lZ$ avec p ne divise pas l . Or $Z/lZ =< \sigma >$ est d'ordre premier à p ; ainsi σ admet 1 seul point fixe z . Si $\tau \in G$ est d'ordre p puisque σ et τ commutent il suit que z est aussi point fixe de τ . Ainsi si $(Z/pZ)^2 =< \tau_1, \tau_2 >$ on a une contradiction par le lemme de Coleman.

• **Example 1.** Suppose $char(k) = 2$ and set $G = \left(\mathbb{Z}/2\mathbb{Z}\right)^2$. Let $u \in k$ with $u^2 \neq u$ and consider the covers of $k(\!(t)\!)$ defined by

$$x_1^2 - x_1 = \frac{1}{t} \quad \text{and} \quad x_2^2 - x_2 = \frac{u^2}{t}.$$

These covers are lifted to covers over $R = W(k)$ by the equations:

$$\frac{(-2X_1+1)^2-1}{4} = \frac{1}{T} \quad \text{and} \quad \frac{(-2X_2+1)^2-1}{4} = \frac{U^2}{T}$$

where $U \in R$ lifts u. The equation for the compositum of these two covers is $X_2^2 - X_2 = U^2(X_1^2 - X_1)$ and setting $Z := X_2 - UX_1$, this becomes

$$Z^2 + (2UX_1 - 1)Z = (U - U^2)X_1. \tag{$*$}$$

Remark that $\mathrm{Fr}(R[T, X_1, Z]) = \mathrm{Fr}(R[Z]) = K(Z)$, i.e., the projective line $\mathbb{P}^1_K$.

From the equation $X_1^2 - X_1 = \dfrac{1}{T}$ we see that

$$|T| < 1 \iff |X_1| > 1$$

and from $(*)$ that

$$|X_1| \le 1 \ \Rightarrow \ |Z| \le 1$$

Now assume $|X_1| > 1$ and $|Z| \le 1$, then $|X_1| = |Z^2 - Z + 2UX_1Z|$ and so $|X_1| = |2UX_1Z|$, i.e. $|Z| = \dfrac{1}{|2U|}$ which is a contradiction. Hence

$$|T| < 1 \iff |Z| > 1.$$

The group G is realized as the group of automorphisms of the disc $|Z| > 1$, i.e., of $R[\![Z^{-1}]\!]$, by

$$\sigma_1(Z) = (4-U)\frac{Z+U}{2Z-1+U}$$
$$\sigma_2(Z) = (1-U)\frac{Z-1}{2Z-1+U}.$$

One checks that each of these automorphisms has order 2. Notice that this cover gives rise to a global G-lifting over $\mathbb{P}^1_R$.

- **Example 2.** Consider the covers of $k(\!(t)\!)$ defined by the equations

$$x_1^p - x_1 = \frac{1}{t^{m_1}}, \quad \text{with } m_1 \not\equiv 0, -1 \bmod p$$

and

$$x_2^p - x_2 = \frac{c_{m_2}}{t^{m_2}} + \cdots + \frac{c_1}{t}, \quad \text{with } (m_2, p) = 1,$$

$c_{m_2} \ne 0$ and $c_{m_2} \notin \mathbb{F}_p$ if $m_1 = m_2$. Then if $m_2 \ge m_1$ the compositum of these covers cannot be lifted over any R dominating $W(k)$. Note, we need the condition $c_{m_2} \notin \mathbb{F}_p$ if $m_1 = m_2$ to ensure that no other subextension of $k(\!(t)\!)$ in the compositum has smaller conductor than m_1. We know that $x_1 + wx_2$, $w \in \mathbb{F}_p$, are Artin-Schreier generators for these extensions and now the above condition guarantees there is no cancellation which would give smaller conductor.

- **Ramification in p^n-cyclic covers of the disc – the Hasse-Arf Theorem.**

Let $k[\![z]\!]/k[\![t]\!]$ be a G-galois extension with $G = \langle\sigma\rangle$ cyclic of order p^n. Assume that G can be lifted as a G galois cover of the disc $X \longrightarrow X/G$. Let F_l be the geometric fixed points of σ^{p^l} and $N_l := |F_l|$, $0 \leq l < n$. The p-cyclic cover $X/\langle\sigma^{p^{l+1}}\rangle \longrightarrow X/\langle\sigma^{p^l}\rangle$ is unramified over the image of $F_{l+1} - F_l$; this means that σ^{p^l} defines a partition of $F_{l+1} - F_l$ in orbits of length p, hence $p|(N_{l+1} - N_l)$. Note that the conductor for this p-cyclic extension is $N_l - 1$, so $N_l > 0$.

This congruence above is the classical Hasse-Arf congruences for p^n-cyclic covers (see [S], p. 84) and following Serre's notation one has $N_0 = 1+i_0, \ldots, N_l = 1+i_0+pi_1+\cdots+p^l i_l$. The fact that at each stage $N_{l+1}-N_l \neq 0$ (which gives the full Hasse-Arf Theorem) follows from the non-triviality of the conductors.

We remark that the method of thickening $\operatorname{Spec} k[\![z]\!]$ in $\operatorname{Spec} R[\![Z]\!]$ was recently successfully exploited by Lubin, [L], in order to give a new proof of Sen's Theorem on formal power series (this is an extension of Hasse-Arf congruences). In fact he only needs to lift the series $\overline{\sigma}(z) \in k[\![z]\!]$ in $\sigma(Z)$ such that $\sigma(Z) - Z$ has only simple zeros (but may have infinite order). For automorphism $\overline{\sigma}$ of finite order this is clearly a less stringent condition than what we intend to do, i.e., to lift in an automorphism σ of finite order.

Local lifting in the $p^a e$-cyclic case with $a \leq 2$

In this section we begin by recalling certain results from Oort-Sekiguchi-Suwa, [O-S-S] and Sekiguchi-Suwa, [S-S 1]. In [O-S-S] the pe-cyclic case, $(e,p) = 1$, is studied and in [S-S 1] the generic p^n-cyclic case. Our aim here is to treat the local lifting of G galois $p^a e$-cyclic covers with $a \leq 2$. Here we follow the Sekiguchi-Suwa exposition from [S-S 1].

1. Kummer theory.

Let ℓ be an integer with $\ell \geq 2$ and K be a field containing μ_ℓ, the group of ℓ-th roots of unity ($char(K) \not| \ell$). Let X a K-scheme, then one has the following exact sequence of sheaves of groups on the étale site on X (Kummer exact sequence):

$$1 \to \boldsymbol{\mu}_{\ell,K} \to \mathbb{G}_{m,K} \xrightarrow{\theta_\ell} \mathbb{G}_{m,K} \to 1 \qquad \theta_\ell : t \mapsto t^\ell \tag{1}$$

and a long exact cohomology sequence

$$\mathbb{G}_{m,K}(X) \to H^1(X_{et}, \boldsymbol{\mu}_{\ell,K}) \to H^1(X_{et}, \mathbb{G}_{m,K}) \to H^1(X_{et}, \mathbb{G}_{m,K}).$$

Here $H^1(X_{et}, \boldsymbol{\mu}_{\ell,K})$ is identified with the set the set of isomorphy classes of $\mathbb{Z}/\ell\mathbb{Z}$-torsors over X. Now let X be the spectrum of a local K-algebra B, then as $H^1(\operatorname{Spec} B, \mathbb{G}_{m,K}) = 0$ (Hilbert theorem 90) it follows that the map

$$\mathbb{G}_m(\operatorname{Spec} B) \to H^1(\operatorname{Spec} B, \boldsymbol{\mu}_\ell)$$

is surjective. This means that for any ℓ-cyclic étale extension C of B, there exists a morphism $f : \operatorname{Spec} B \to \mathbb{G}_{m,K}$ and $\operatorname{Spec} C$ is given by the fibre product:

$$\begin{array}{ccc} \operatorname{Spec} C & \longrightarrow & \mathbb{G}_{m,K} \\ \big\downarrow & & \big\downarrow \theta_\ell \\ \operatorname{Spec} B & \longrightarrow & \mathbb{G}_{m,K} \end{array} \tag{2}$$

2. Artin-Schreier-Witt theory.

Let k be a field of characteristic $p > 0$ and $W_{n,k}$ be the Witt-group scheme of dimension n (the truncated Witt-vectors). Let X be a k-scheme. This time one has the following exact sequence (for the étale site):

$$W_{n,k}(X) \to H^1(X_{et}, \mathbb{Z}/p^n\mathbb{Z}) \to H^1(X_{et}, W_{n,k}) \to H^1(X_{et}, W_{n,k}) \tag{3}$$

In particular, if X is affine, then $H^1(X, W_{n,k}) = 0$. Therefore, we get the surjectivity of the map

$$W_{n,k}(X) \to H^1(X_{et}, \mathbb{Z}/p^n\mathbb{Z}).$$

We shall use the following facts: $W_{n,k}$ is the extension of $\mathbb{G}_{a,k}$ by $W_{n-1,k}$ and one has the commutative diagram:

$$\begin{array}{ccccccccc} 0 & \to & \mathbb{Z}/p\mathbb{Z} & \to & \mathbb{Z}/p^n\mathbb{Z} & \to & \mathbb{Z}/p^{n-1}\mathbb{Z} & \to & 0 \\ & & \cap & & \cap & & \cap & & \\ 0 & \to & \mathbb{G}_{a,k} & \to & W_{n,k} & \to & W_{n-1,k} & \to & 0 \end{array} \tag{4}$$

3. Sekiguchi-Suwa theory.

Assertion 1. ([S-S 1] Theorem 7.1.) There exists a smooth group scheme $\mathcal{W}_n$ over the discrete valuation ring $R := \mathbb{Z}_{(p)}[\mu_{p^n}]$, containing the constant group scheme $(\mathbb{Z}/p^n\mathbb{Z})_R$, such that the exact sequence

$$0 \to (\mathbb{Z}/p^n\mathbb{Z})_R \to \mathcal{W}_n \xrightarrow{\psi_n} \mathcal{W}_n/(\mathbb{Z}/p^n\mathbb{Z})_R \to 0 \tag{5}$$

has the Artin-Schreier-Witt exact sequence as special fibre and an exact sequence of Kummer type

$$1 \to \boldsymbol{\mu}_{p^n} \to \mathbb{G}_m^n \to \mathbb{G}_m^n \to 1$$

as the generic fibre. Moreover, for each n with $n \geq 2$, there exists a commutative diagram consisting of horizontal exact sequences

$$\begin{array}{ccccccccc} 0 & \to & (\mathbb{Z}/p\mathbb{Z})_R & \to & (\mathbb{Z}/p^n\mathbb{Z})_R & \to & (\mathbb{Z}/p^{n-1}\mathbb{Z})_R & \to & 0 \\ & & \cap & & \cap & & \cap & & \\ 0 & \to & \mathcal{W}_{1,R} & \to & \mathcal{W}_{n,R} & \to & \mathcal{W}_{n-1,R} & \to & 0 \end{array} \tag{6}$$

which gives a deformation of (4) to a commutative diagram consisting of exact sequences of multiplicative groups

$$\begin{array}{ccccccccc} 1 & \to & \boldsymbol{\mu}_p & \to & \boldsymbol{\mu}_{p^n} & \to & \boldsymbol{\mu}_{p^{n-1}} & \to & 1 \\ & & \cap & & \cap & & \cap & & \\ 1 & \to & \mathbb{G}_m & \to & (\mathbb{G}_m)^n & \to & (\mathbb{G}_m)^{n-1} & \to & 1 \end{array} \tag{7}$$

Now this exact sequence is universal for étale p^n-cyclic coverings of local rings dominating R. Namely one has the following:

Assertion 2. ([S-S 1], Theorem 3.8.) Let B be a local R-algebra which is flat over R. Then

$$H^1(\operatorname{Spec} B, \mathcal{W}_n) = 0$$

i.e. the canonical map

$$(\mathcal{W}_n/(\mathbb{Z}/p^n\mathbb{Z})_R)(B) \to H^1(\mathrm{Spec} B, (\boldsymbol{\mu}_{p^n})_R)$$

is surjective.

Moreover, if C is a flat local R-algebra which is an unramified p^n-cyclic covering of B then there exists an R-morphism

$$f : \mathrm{Spec}\, B \longrightarrow \mathcal{W}_n/(\mathbb{Z}/p^n\mathbb{Z})_R,$$

and the covering

$$\mathrm{Spec}\, C \longrightarrow \mathrm{Spec}\, B$$

is given by the fibre product:

$$\begin{array}{ccc} \mathrm{Spec}\, C & \longrightarrow & \mathcal{W}_n \\ \big\downarrow & & \big\downarrow \psi_n \\ \mathrm{Spec}\, B & \xrightarrow{f} & \mathcal{W}_n/(\mathbb{Z}/p^n\mathbb{Z})_R \end{array}$$

We shall apply this last theorem to the case where $B = R[[T]]_{(\pi)}$ (here π is the uniformizing parameter of R); this solves the local lifting for p^n-cyclic groups generically. This lifting is therefore of the same nature as Garuti's, but in [G] the method is valid for general groups, (see the introduction).

In order to smoothen the singularities of [G], we need to give the map ψ_n below explicitly:

$$\psi_n : \mathcal{W}_n \longrightarrow \mathcal{W}_n/(\mathbb{Z}/p^n\mathbb{Z})_R.$$

We shall do this in the p^2-cyclic case, i.e. $n = 2$. Following [S-S 1], Theorem 7.1, one can take:

$$\mathcal{W}_2 = \mathrm{Spec}\, R[X_1, X_2, (\lambda X_1 + 1)^{-1}, (\lambda X_2 + F_1(X_1))^{-1}]$$

where

$$F_1(X_1) = 1 + \mu X_1 + \frac{1}{2!}\mu^2 X_1^2 + \cdots + \frac{1}{(p-1)!}\mu^{p-1} X_1^{p-1} =: \mathrm{E}xp_p(\mu X_1)$$

is the Artin-Hasse exponential truncated at degree p,

$$\mu = \pi - \pi^2/2 + \cdots + (-1)^p \pi^{p-1}/(p-1)$$

and $\pi = \zeta_{(2)} - 1$. Here $\zeta_{(2)}$ is a primitive p^2-th root of unity.

As explained in [S-S 1], proof of Theorem 8.4, the group scheme $\mathcal{V}_2 := \mathcal{W}_2/(\mathbb{Z}/p^2\mathbb{Z})_R$ is given by a polynomial $G_1(X_1)$ such that:

$$\mathcal{V}_2 = \mathrm{Spec}\, R[X_1, X_2, (\lambda^p X_1 + 1)^{-1}, (\lambda^p X_2 + G_1(X_1))^{-1}]$$

and G_1 satisfies the congruence equation:

$$G_1(\psi_1(X_1)) \equiv F_1(X_1)^p (\lambda X_1 + 1)^{-1} \bmod \lambda^p.$$

Here $\psi_1(X_1)=((\lambda X_1+1)^p-1)/\lambda^p$ and the isogeny ψ_2 is then
$\psi_2(X_1,X_2)=(\psi_1(X_1),X_2')$ with

$$X_2'=(1/\lambda^p)[(\lambda X_2+F_1(X_1))^p-(\lambda X_1+1)G_1(\psi_1(X_1))](\lambda X_1+1)^{-1}.$$

In Lemma 5.2 we shall prove that for F_1 as above, the polynomial $G_1(Z)=\mathrm{E}xp_p(\mu^pZ)$ works and then

$$X_2'=(1/\lambda^p)[(\lambda X_2+F_1(X_1))^p-(\lambda X_1+1)\mathrm{E}xp_p(\mu^p(\psi_1(X_1))](\lambda X_1+1)^{-1}.$$

Theorem. We keep the notations from the previous lemma and let $A_s\in R$, $0<s<m_1(p-1):=r$ be given. Then the equations

$$((\lambda X_1+1)^p-1)/\lambda^p=T^{-m_1}$$

and

$$\begin{aligned}&\big[\lambda X_2+\mathrm{E}xp_p(\mu X_1)\big(1+\sum_{\substack{0\le j<m_1\\0<i<p}}T^{-j}\mu^i(p-i)!P_{j,i}(T^{-m_1})\big)\big]^p\\&=\big(G(T^{-1})+p\mu^p\sum_{0<s<r}A_sT^{-s}\big)(\lambda X_1+1)\end{aligned}$$

define a p^2-cyclic cover, $\mathcal{C}$, of $\mathbb{P}^1_R$ which after normalisation is étale outside the disc $|T|<1$. The special fiber is smooth and induces the extension of $k[\![t]\!]$ defined by the equations

$$\begin{aligned}x_1^p-x_1&=t^{-m_1}\\x_2^p-x_2&=c(x_1^p,-x_1)+\sum_{0<s<r}a_st^{-s}\\&\quad-\sum_{\substack{0\le j<m_1\\0<i<p}}t^{-jp}(x_1^p-x_1)^ip_{j,p-i}(x_1^p-x_1)^p\end{aligned}$$

where the polynomials $p_{j,p-i}$ and coefficients a_s are the residues of $P_{j,p-i}$ and A_s, respectively. In this way we cover all p^2-cyclic extensions of $k[\![t]\!]$.

- **Automorphisms of order p^ℓ and Lubin-Tate formal groups.**

We would like to thank the referee for pointing out the following method of producing order p^ℓ automorphisms of p-adic open discs without inertia at π, for $\ell\ge1$. Although these automorphisms have quite special numerical data, for $\ell\ge3$ this is the only way we know of producing such automorphisms. Although we will concentrate on the case $\ell=1$ below, the reader may easily adapt the reasoning to the general case. Our reference to formal groups is [H].

Let K be a finite totally ramified degree n extension of $\mathbb{Q}_p[\zeta]$, where ζ is a primitive p-th root of unity. Let R be the ring of integers in K and π be a uniformizing parameter. We consider the series

$$f(Z):=Z+\frac{Z^p}{\pi}+...+\frac{Z^{p^k}}{\pi^k}+...\in K[\![Z]\!],$$

observing the important fact that $f(Z)$ converges on the open disc $\{z\in K\mid v(z)>0\}$.

Then (see [H, Hazewinkel] p. 46)

$$F(Z_1, Z_2) := f^{-1}(f(Z_1) + f(Z_2)) \in R[\![Z_1, Z_2]\!]$$

and

$$[\pi]_F(Z) := f^{-1}(\pi f(Z)) \in R[\![Z]\!],$$

and so defines a Lubin-Tate formal group, i.e., $[\pi]_F(Z) \equiv \pi Z \bmod Z^2$ and $f(Z) \equiv Z^p \bmod \pi$. It is easily seen that for any $a \in R$ there is a unique series $[a]_F(Z) \in R[\![Z]\!]$ such that $[a]_F(F(Z_1, Z_2)) = F([a](Z_1), [a](Z_2))$ and $[a]_F(Z) \equiv aZ \bmod Z^2$. Moreover, the map $a \to [a]_F(Z)$ defines an injective homomorphism from R to the endomorphism ring of the formal group law $F(Z_1, Z_2)$. Hence, in particular, $\sigma(Z) := [\zeta](Z) = f^{-1}(\zeta f(Z))$ is an order p -automorphism of $R[\![Z]\!]$.

We now describe the fixed points of $\sigma(Z)$ and the corresponding Hurwitz data. Using the equality $\zeta - 1 = u\pi^n$ for some unit $u \in R$, it follows that $[\zeta - 1](X) \equiv (\zeta - 1)Z \bmod Z^2$ and that $[\zeta - 1](Z) \equiv Z^{p^n} \bmod \pi$. One deduces that $\sigma(Z) - Z$ has Weierstrass degree p^n (see II.1) and so σ has p^n fixed points. If we let z be such a fixed point, then the relation $f(\sigma(Z)) = \zeta f(Z)$ shows that z is a root of $f(Z)$ in the open disc (although the converse is false). Moreover, differentiating and evaluating at z one obtains $f'(z)\sigma(Z)'_{Z=z} = \zeta f'(z)$, and as $f'(z) \equiv 1 \bmod \pi$, it follows that $\sigma(Z)'_{Z=z} = \zeta$, i.e. $H_\sigma = (1, 1, ..., 1)$.

Now we describe the geometry of F_σ : First we remark that it is easy to describe the zeroes of $f(Z)$ inside the open disc. Indeed, examining the Newton polygon of the Laurent series $f(Z)$ we see that the non-trivial zeroes lie on circles centered at 0 and having radii $v(z) = 1/(n(p-1)^2 p^{m-1})$, for any $1 \leq m$. On each such circle there are $p^m - p^{m-1}$ zeroes and an exercise shows that these points are in p distinct classes counting the zero class. Moreover, the geometry in each class mimics that in the zero class. In fact the congruence $[\zeta - 1](Z) \equiv Z^{p^n} \bmod \pi$ shows that the zeroes z of $f(Z)$, which are also fixed points of σ, have radius $v(z) > 1/(n(p-1)^2 p^n)$. As $p^n = 1 + (p-1) + (p^2 - p) + \cdots + (p^n - p^{n-1})$ it follows that the fixed points of σ are exactly 0 and the zeroes of f on the circles of radius $v(z) = 1/(n(p-1)^2 p^{m-1})$ about 0, for $1 \leq m \leq n$. It follows that the oriented tree $\mathcal{D}_s^o$ is characterized by the property that on each internal component there are p new branching components and that there are p fixed points on each terminal component. (One could equally well say that the dual graph is a tree having valency p at each vertex). Note that each oriented path of maximal length has n edges, which is the same as asserting that the graphs $d(\sigma, Z_i)$ have n breaks. Moreover, these graphs all coincide and this gives us a way of producing trees of arbitrary length. **Réf'erences.**

N. Bourbaki, *Algèbre Commutative*, Hermann, Paris 1961.

J. Bertin, *Obstructions locales au relèvement de revêtements galoisiens de courbes lisses*, C.R. Acad. Sci. Paris, 326, Série I, (1998), 55–58.

J. Bertin, A. Mézard, *Déformations formelles des revêtements sauvagement ramifiés de courbes algébriques*, Prépublication $n^0 439$ de l'Institut Fourier, (1998).

B. Green, M. Matignon, *Liftings of Galois Covers of Smooth Curves*, Compositio Math., **113** (1998), 239–274.

B. Green, M. Matignon, *Order p automorphisms of the open disc of a p-adic field*, J. Amer. Math. Soc. 12 (1999), pp. 269-303.

M. Hazewinkel, *Formal Groups and Applications*, Pure and Applied Mathematics **78**, Academic Press, 1978.

M. Matignon, *p-groupes abéliens de type $(p, ..., p)$ et disques ouverts p-adiques*, Manuscripta Math, à Paraitre.

J. S. Milne, *Étale Cohomology*, Princeton Mathematical Series, **33**, (1980).

F. Oort, *Lifting Algebraic Curves, Abelian Varieties, and Their Endomorphisms to Characteristic Zero*, Proceedings of Symposia in Pure Mathematics, Vol 46 (1987).

F. Oort, T. Sekiguchi, N. Suwa, *On the deformation of Artin-Schreier to Kummer*, Ann. scient. Éc. Norm. Sup., 4^{eme} série, t. **22** (1989), 345–375.

Réf'erences.

Chapitre I.

Bourbaki, Algebre chapitre V

Milne, Etale cohomology (http://www.math.lsa.umich.edu/ $\sim$ jmilne.)

Milne, Class field theory (http://www.math.lsa.umich.edu/ $\sim$ jmilne.)

Serre, Groupes algebriques, corps de classes

Serre, Corps locaux

Serre, Cohomologie galoisienne

Serre, Topics in Galois theory

Borel, Linear algebraic groups

Demazure, Lecture on p-divisible groups

Waterhouse, Introduction to affine group schemes

Silverman, Advance topics on elliptic curves

Mumford, Abelian varieties [Ar] Kennzeichnung des Körpers der reellen algebraischen Zahlen, Abh. Math. Sem. Hamburg 8 (1924)

[Ar-Sc], Über eine Kennzeichnung der reell abgeschlossen Körper, Abh. Math, Sem. Hamburg 5 (1927)

[W 1] Witt Konstrktion von galoisshen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f Crelle 174 (1936)

[W 2] Witt Zyklische Körper und Algebren der Charakteristik p vom Grad p^n (1937)

[W 3] Witt Vektorkalkül und Endomorphismen der Einspotenzreihengruppe (Oeuvre completes de E. Witt)

[H] Harder, An Essay on Witt Vectors (Oeuvre completes de E. Witt)

[Sa] Saltman, Generic Galois Extensions and Problems in Field Theory, Advances in Math 43,250-283 (1982)

References: Invariants de Hasse-Witt

Hasse H., Witt E. Zyklische unverzweigte Erweiterungskorper vom Primzahlgrade p uber einem algebraischen Functionenkorper der Charakteristik p, Monastsh. Math. Phys. 43 (1936), 477-492.

Serre, Cohomologie des varietes en caracteristique $p > 0$, 1960, Oeuvres completes,

Jacobson, Abstract derivation and Lie algebra, Trans. Math. Soc. 42 (1937), 206-224

Manin, Y. The Hasse-Witt-matrix of an algebraic curve. Transl. AMS, vol. 45, 245 (1965)

Cartier, P. Questions de rationnalite des diviseurs en geometrie algebrique, Bull. Soc. math. France, 86, 1958, 177-251

Samuel, P. Lectures on unique factorization domains. Notes by M. Pavman Murthy. Tata Institute of Fundamental Research Lectures on Mathematics, No. 30 Tata Institute of Fundamental Research, Bombay 1964 ii+84+iii pp.

Mathieu, Seminaire Bourbaki, Mars 99