BULLETIN DE LA S. M. F.

SERGE LANG

Sur les séries *L* d'une variété algébrique

Bulletin de la S. M. F., tome 84 (1956), p. 385-407

<http://www.numdam.org/item?id=BSMF_1956__84__385_0>

© Bulletin de la S. M. F., 1956, tous droits réservés.

L'accès aux archives de la revue « Bulletin de la S. M. F. » (http://smf.emath.fr/Publications/Bulletin/Presentation.html) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Bull. Soc. Math. France,
84, 1956, p. 385 à 407.

SUR LES SÉRIES L D'UNE VARIÉTÉ ALGÉBRIQUE;

PAR SERGE LANG.

1. Introduction. — DIRICHLET a démontré l'existence d'une infinité de nombres premiers p dans toute progression arithmétique $p \equiv a \pmod{m}$, où a est premier à m.

Dans la théorie du corps de classes, on a une autre interprétation de ce théorème d'existence. Soient $\mathbf{Q}$ le corps des nombres rationnels et E le corps des racines m-ièmes de l'unité. Alors à chaque nombre premier p ne divisant pas m, correspond l'automorphisme du corps E qui envoie chaque racine m-ième de l'unité dans sa p-ième puissance. Cet automorphisme est noté $(p, E/\mathbf{Q})$, et le théorème de Dirichlet peut s'interpréter en disant qu'à chaque élément σ du groupe de Galois de $E/\mathbf{Q}$ il existe une infinité de p tels que $(p, E/\mathbf{Q}) = \sigma$. On peut préciser cet énoncé en attribuant une densité à ces nombres premiers.

Plus généralement on prend un corps de nombres K comme corps de base, et l'on sait classifier les extensions abéliennes au moyen de progressions arithmétiques généralisées. Dans le cas non ramifié on prend le groupe des classes d'idéaux ordinaires, c'est-à-dire les idéaux de K modulo les idéaux principaux. On sait qu'il existe une extension abélienne maximale non ramifiée, dont le groupe de Galois est isomorphe au groupe des classes d'idéaux, groupe qu'on peut noter C_K. Cet isomorphisme s'obtient au moyen de la loi de réciprocité d'Artin, comme suit : Soit $\mathfrak{O}$ l'anneau des entiers de E, et $\mathfrak{p}$ un idéal premier de K. Alors, $\mathfrak{p}$ étant non ramifié, on a $\mathfrak{p}\mathfrak{O} = \mathfrak{P}_1 \dots \mathfrak{P}_r$, où les $\mathfrak{P}_i$ sont maximaux dans $\mathfrak{O}$. On considère le sous-groupe D du groupe de Galois G de E/K composé des éléments σ de G laissant l'un des $\mathfrak{P}_i$ invariant. Du fait que G est abélien, c'est le même pour tous les $\mathfrak{P}_i$. Ce groupe D, nommé groupe de décomposition, est cyclique et possède un générateur canonique σ (l'automorphisme de Frobenius) caractérisé par la congruence

$$\sigma\alpha \equiv \alpha^{N\mathfrak{p}} \pmod{\mathfrak{P}_i} \quad \text{pour tout } \alpha \in \mathfrak{O}, \tag{1}$$

$N\mathfrak{p}$ étant le nombre d'éléments du corps des résidus $\mathfrak{o}/\mathfrak{p}$.

Ce générateur σ est noté $(\mathfrak{p}, E/K)$, car il ne dépend que de $\mathfrak{p}$, et pas du $\mathfrak{P}_i$

dont on s'est servi, du fait que G est abélien. La loi de réciprocité d'Artin dit alors que le symbole $(\mathfrak{p}, E/K)$ ne dépend que de la classe de $\mathfrak{p}$ dans C_K. Le théorème de la progression arithmétique peut s'exprimer en disant que pour chaque élément σ de G il existe une infinité d'idéaux premiers $\mathfrak{p}$ tels que $(\mathfrak{p}, E/K) = \sigma$. Comme ARTIN l'a remarqué, on peut donc interpréter une progression arithmétique ou bien comme une classe d'idéaux premiers modulo les idéaux principaux, ou bien comme classe d'idéaux premiers ayant le même automorphisme de Frobenius dans un groupe de Galois. Le cas ramifié se traite de façon analogue. Si $\mathfrak{m}$ est le diviseur de ramification, on prend le groupe des diviseurs premiers à $\mathfrak{m}$ modulo le sous-groupe des diviseurs principaux, provenant des éléments f de K tels que $f \equiv 1 \pmod{\mathfrak{m}}$, la congruence étant prise au sens valuatif. Dans le cas des racines de l'unité, cette congruence se réduit précisément à la congruence ordinaire, ce qui justifie la terminologie.

Dans le cas d'une extension galoisienne non abélienne E/K, on ne connaît pas d'analogue aux classes d'idéaux, mais on a toujours l'automorphisme de Frobenius, qui est alors une classe de conjugaison, qu'on notera aussi $(\mathfrak{p}, E/K)$, définie encore par la congruence (1). On peut encore énoncer un théorème d'existence d'idéaux premiers dans une progression arithmétique, à savoir qu'à chaque classe de conjugaison dans G, il existe une infinité d'idéaux premiers $\mathfrak{p}$, tels que $(\mathfrak{p}, E/K)$ soit une classe donnée. De plus, on peut attribuer à ces idéaux une densité, que l'on trouvera calculée chez ARTIN [1]. La démonstration se fait au moyen de séries L. Dans le cas le plus simple, celui des entiers $\bmod m$, on prend un caractère χ du groupe multiplicatif des entiers $\bmod m$, et premiers à m, et l'on définit la série L par son logarithme

$$\log L(s, \chi) = \sum \frac{\chi(p^\mu)}{\mu p^{\mu s}},$$

la somme étant prise pour tous les p premiers à m, et μ entier ≥ 1. Dans le cas d'une extension galoisienne quelconque, on prend un caractère de G. Si σ est n'importe quel élément de la classe de conjugaison $(\mathfrak{p}, E/K)$, $\mathfrak{p}$ étant non ramifié, on définit

$$\chi(\mathfrak{p}^\mu) = \chi(\sigma^\mu).$$

La série L devient alors

$$\log L(s, \chi, E/K) = \sum \frac{\chi(\mathfrak{p}^\mu)}{\mu (N\mathfrak{p})^s},$$

la somme étant prise pour tous les idéaux premiers non ramifiés, et μ entier ≥ 1. ARTIN a montré [2] comment on pouvait compléter cette définition pour inclure les idéaux premiers ramifiés, mais il est inutile d'entrer ici dans ces considérations.

Bien entendu, dans le cas abélien, on peut définir directement la fonction

$L(s, \chi, E/K)$ par un produit eulérien, ou une somme, de la façon suivante :

$$\prod \frac{1}{1-\frac{\chi(\mathfrak{p})}{(N\mathfrak{p})^s}} = \sum \frac{\chi(\mathfrak{a})}{(N\mathfrak{a})^s}.$$

Comme d'habitude, on note par $\mathfrak{a}$ un idéal, c'est-à-dire un élément du groupe abélien libre engendré par les $\mathfrak{p}$, et $\chi(\mathfrak{a})$ est défini à partir des $\mathfrak{p}$ par linéarité. La somme est prise pour les $\mathfrak{a}$ entiers.

Il est facile de voir que la densité des idéaux premiers dans les progressions arithmétiques dépend du comportement des séries L pour $Re(s) > 1/2$. Si l'on sait que pour $\chi \neq \chi_1$ (χ_1 désignant une fois pour toutes le caractère principal) $L(s, \chi)$ n'a pas de zéro ni de pôle pour $Re(s) > 1/2$ (conjecture d'Artin) et que $L(s, \chi_1)$ a un pôle simple en $s = 1$, et pas d'autres zéros ni pôles pour $Re(s) > 1/2$ (hypothèse de Riemann), alors on voit par un calcul analytique simple qu'on a la densité voulue d'idéaux premiers dans une progression arithmétique, avec un terme d'erreur aussi bon que possible. Dans le cas de la fonction ζ, par exemple, on pose $\Lambda(n) = 0$ si $n = 1$, $\log p$ si $n = p^\mu$ est une puissance de p, et 0 si n n'est pas une puissance d'un nombre premier p. On pose

$$\Psi(x) = \sum_{n \leq x} \Lambda(n)$$

et l'on trouve alors

$$\Psi(x) = x + O\left(x^{\frac{1}{2}+\varepsilon}\right).$$

D'autre part, on sait que toutes ces questions ont un analogue dans le cas d'un corps de fonctions d'une variable sur un corps fini à q éléments (Schmidt [12] à la suite des travaux d'Artin). On a aussi la notion d'idéaux premiers du corps, mais on jouit d'un avantage de plus : le nombre d'éléments $N\mathfrak{p}$ du corps des restes est une puissance q^d. L'entier d est appelé le degré de $\mathfrak{p}$ et noté $\deg(\mathfrak{p})$. De ce fait, on voit que les puissances $(N\mathfrak{p})^s$ peuvent s'exprimer comme puissances de q, et il est alors utile de changer de variable : on pose $t = q^{-s}$, et la série L devient une série de puissances

$$\log L(t, \chi, E/K) = \sum_{\mathfrak{p}^\mu} \frac{\chi(\mathfrak{p}^\mu)}{\mu} t^{\mu \deg(\mathfrak{p})}.$$

Si $\chi = \chi_1$, alors la série L est la fonction ζ attachée au corps.

On sait que Weil a introduit une fonction ζ pour les variétés algébriques de dimension quelconque [13]. Il était donc naturel de chercher à définir les séries L dans ce cas plus général. Les séries L d'Artin se généralisent dans tous les cas de la façon suivante. Soit K un corps de fonctions sur le corps de constantes k, autrement dit

$$K = k(x_1, \ldots, x_n) = k(x).$$

On peut considérer (x) comme point générique d'une variété V qui est appelée un modèle de K. Chaque point Q de V détermine un anneau local dans K, et deux points ont le même anneau local si et seulement s'ils sont conjugués sur k.

Nous suivrons la terminologie de CHEVALLEY, et nous appellerons tout anneau local $\mathfrak{o}$ obtenu de cette manière une *localité* de K. [Si $\mathfrak{p}$ est l'idéal maximal de $\mathfrak{o}$ nous dirons aussi quelquefois que la paire $(\mathfrak{o}, \mathfrak{p})$, ou $\mathfrak{p}$ lui-même, sont des localités]. Une localité sera dite simple si le point Q est simple. Le corps k étant parfait, on sait que ceci équivaut à la condition que $\mathfrak{o}$ soit régulier. Les localités simples sont alors en correspondance biunivoque avec les cycles premiers rationnels de V sur k. (Par « cycle » nous entendrons toujours cycle de dimension zéro.)

Pour définir les séries L en dimension > 1, il suffit de prendre la définition donnée dans le cas de dimension 1, de remplacer la notion d'idéal premier par la notion de localité, et de prendre la somme pour toutes les localités $\mathfrak{p}$ d'un modèle de K. On sait par les travaux de KRULL que les groupes de décomposition et d'inertie se généralisent, et l'on a donc l'automorphisme de Frobenius. On peut alors chercher à démontrer un théorème de densité. C'est ce qui sera fait ici.

On voit que l'on peut aussi définir les localités pour un corps de type fini en caractéristique zéro, et l'on aura aussi des séries L. Il est à peine besoin de dire que la découverte des lois de décomposition (lois de réciprocité) dans ce cas serait d'un intérêt considérable. Mais jusqu'ici, nous ne savons rien sur ces séries L, en dehors de résultats qui dépendent de façon immédiate de ceux qu'on connaît en réduisant modulo une localité $\mathfrak{p}_0$ du corps de nombres contenu dans le corps de type fini K. Par exemple, démontrons la surjectivité de l'application de réciprocité pour une extension abélienne E de K. Soit $\mathfrak{p}$ une localité simple de K, non ramifiée dans E, et $D_{\mathfrak{p}}$ le groupe de décomposition de $\mathfrak{p}$ dans le groupe de Galois G de E sur K. Soit G' le sous-groupe de G engendré par les $D_{\mathfrak{p}}$, et soit E' le sous-corps de E invariant par G'. Alors tous les $\mathfrak{p}$ de K se décomposent complètement dans E'. Si k est le corps de nombres algébriques contenu dans K, autrement dit la clôture algébrique de $\mathbf{Q}$ dans K, on déduit d'abord de la remarque précédente que E' ne peut contenir une extension algébrique propre de k, en employant un résultat connu de la théorie des nombres, à savoir qu'il existe une infinité de localités de k qui ne se décomposent pas complètement dans une telle extension. On est donc ramené à une extension dite géométrique, et donc au résultat analogue en caractéristique p, après avoir réduit l'extension E de K mod $\mathfrak{p}_0$ pour n'importe quelle localité $\mathfrak{p}_0$ de k en dehors d'un ensemble fini exceptionnel.

Dans la suite de ce travail, nous nous bornerons exclusivement au cas de caractéristique p.

Nos résultats seront purement birationnels, et nous montrerons que les

séries L (pour un caractère $\neq \chi_1$) n'ont pas de zéro ni de pôle dans le cercle $|t| < q^{-\left(r-\frac{1}{2}\right)}$. Nous avons donné autre part [5] la conjecture relative au comportement sur le cercle $|t| = q^{-\left(r-\frac{1}{2}\right)}$, qui est aussi birationnellement invariant. Quant au comportement pour les cercles suivants, si les deux variétés U et V sont sans singularités et complètes, alors on peut conjecturer que les séries L sont comme des fonctions ζ, sauf que les termes $(1-t)$ et $(1-q^r t)$ sont absents.

Ce cas est relativement rare, car ABHYANKAR a démontré qu'en général on ne peut pas résoudre simultanément les singularités des deux corps K et E par un modèle V de K et sa normalisation U dans E. Néanmoins on sait dans le cas topologique que les séries L satisfont au même formalisme que celui d'Artin quand on prend l'espace quotient d'une variété par un groupe fini d'homéomorphismes. Ceci indique que la présence de singularités doit être considérée comme normale, et que les progrès que l'on pourra faire dans cette direction dépendent de l'étude plus précise de l'effet que les singularités peuvent avoir sur la fonction ζ d'une variété. Contrairement à ce que prétend WEIL dans sa « Footnote... » [15], il semble au contraire parfaitement approprié, et même essentiel, de mieux connaître comment de telles fonctions ζ se comportent, même si elles n'ont pas d'équation fonctionnelle.

D'ailleurs, pour revenir au cas topologique, si l'on prend une variété (topologique) U et un groupe fini d'homéomorphismes G de V (avec des hypothèses convenables) les nombres de Betti de l'espace quotient $V = U/G$ vérifient la dualité de Poincaré. Cela conduit à penser que dans le cas arithmétique on n'aurait besoin que d'un modèle U non singulier par exemple. La variété V aurait des singularités; mais on pourrait espérer que sa fonction ζ aurait encore une équation fonctionnelle.

Enfin, on peut chercher dans le cas abélien à montrer l'identité des séries L définies par le groupe de Galois à la manière d'Artin, avec des séries L définies par un caractère du groupe des cycles de dimension zéro. C'est ce que nous pouvons faire dans un grand nombre de cas : on se donne une application rationnelle $\alpha : V \to A$ de V dans une variété de groupe commutatif qui induit un homomorphisme du groupe des cycles sur V, rationnels sur k, dans le groupe des points rationnels A_k de A. On peut alors dire que deux cycles $\mathfrak{a}$ et $\mathfrak{b}$ sont dans la même progression arithmétique s'ils ont la même image dans A_k. Dans le cas des extensions non ramifiées, on prend pour A la variété d'Albanese de V, et l'on peut ainsi construire une théorie analogue à celle du corps de classes de HILBERT [6].

Dans le dernier numéro de ce travail, nous indiquerons brièvement comment on peut généraliser une partie de cette théorie en prenant un groupe commutatif sujet à la seule condition que l'image réciproque de ses revêtements (par des isogénies) soit biunivoque.

On pourrait aussi chercher à étendre cette théorie au cas non abélien en

prenant un groupe algébrique quelconque, mais pour le moment on ne sait à peu près rien sur cette question.

Je ne voudrais pas terminer cette introduction sans exprimer ma reconnaissance à J.-P. SERRE, qui a bien voulu se charger de la corection des phautes d'orthografe.

2. Le théorème de densité. — Soit V une variété abstraite, normale, définie sur un corps fini k a q éléments. Soit K/k un corps de fonctions de V/k, et E/K une extension galoisienne de K, de degré n et de groupe G. Nous ne nous occuperons que du cas géométrique, et nous supposerons donc que k est le corps de constantes de E. Alors la normalisation U de V dans E est une variété abstraite, projective si V l'est, et l'on a une application rationnelle $f: U \to V$ partout définie sur U et telle que l'image inverse d'un point Q de V contienne au plus n points de U. Cela se voit facilement en considérant la décomposition de l'anneau local de Q dans E (*voir* KRULL [4]). On dira que $f: U \to V$ est un *revêtement de degré n*. Si Q est simple sur V et s'il y a exactement n points P_i sur U au-dessus de Q, alors tous les P_i sont simples aussi. C'est immédiat, à partir du fait que l'idéal maximal de Q se remonte à l'idéal maximal de chacun des P_i (NAGATA [9]). Pour la convenance du lecteur, nous allons reproduire ici un argument géométrique dû à MATSUSAKA. La question étant locale, nous pouvons nous borner aux variétés affines.

PROPOSITION 1. — *Soit $f: U \to V$ une application rationnelle de degré n, séparable, partout définie, et telle que l'image inverse de chaque point de V soit un ensemble fini de points de U. Soit Q un point simple de V, et supposons que $\Gamma_f \cap (U \times Q)$ contienne exactement n points distincts $(P_i \times Q)$. Alors chaque P_i est simple sur U.*

Démonstration. — Soient S^N et S^M les espaces affines ambiants des variétés U et V respectivement. Soit L une variété linéaire de S^M telle que $V.L$ soit défini, et contienne Q avec multiplicité 1. L'intersection $\Gamma_f.(S^N \times L)$ est alors définie, sur $S^N \times S^M$, et est égale à $\sum m_i(P_i \times Q) + X$, où X est un cycle positif sur $S^N \times S^M$, ne contenant aucun des $P_i \times Q$. En projetant sur S^M, et en appliquant le théorème de projection, on voit qu'on obtient $nQ + X'$, où X' ne contient pas Q et, de ceci, on conclut que $\sum m_i = n$. Mais l'hypothèse montre que chaque $m_i = 1$. Par le critère de multiplicité 1, on en déduit que chaque $P_i \times Q$ est simple sur le graphe Γ_f, et donc que P_i est simple sur U.

Soit $\mathfrak{p}$ un cycle premier rationnel de V/k, de degré d. Alors on peut écrire $\mathfrak{p} = \sum Q^{(q^i)}$. Les cycles premiers rationnels de V/k sont en correspon-

dance biunivoque avec les anneaux locaux réguliers de K déterminés par n'importe quel point Q de $\mathfrak{p}$. Nous avons convenu dans l'introduction de les appeler des localités simples. Une telle localité est non ramifiée (au sens de KRULL [4]) si et seulement s'il existe n points distincts P_i dans U au-dessus de Q.

Si x est un point générique de V/k, nous identifions souvent $k(x)$ et K. On peut alors écrire $E=k(y)$, y étant un point générique de U/k tel que $f(y)=x$. Si σ est un automorphisme de E/K, alors (y, y^σ) est un point générique d'une correspondance birationnelle T_σ de U, et le groupe de Galois de E/K peut être identifié avec ce groupe de correspondances birationnelles. Pour chaque T_σ on a $f\circ T_\sigma = T_\sigma$. Ceci exprime géométriquement le fait que chaque σ laisse K invariant.

On sait d'après les travaux de KRULL [4] que les groupes de décomposition et d'inertie d'une localité se définissent comme dans le cas des corps de nombres algébriques. Nous allons répéter ici ces définitions pour le cas géométrique et arithmétique qui nous occupe.

Soit $\mathfrak{p}$ un cycle premier rationnel de V sur k, de degré d. Soit Q un point de $\mathfrak{p}$ et P n'importe quel point dans $f^{-1}(Q)$. On suppose que Q (donc $\mathfrak{p}$) est non ramifié. Alors il existe une transformation T de G uniquement déterminée par la condition $T(P)=P^{(q^d)}$, à une conjugaison près. Si l'on choisit un autre point Q_1 dans $\mathfrak{p}$ et un point P_1 dans $f^{-1}(Q_1)$, on voit immédiatement que la transformation T_1 telle que $T_1(P_1)=P_1^{(q^d)}$ est conjuguée à T dans G. Donc la classe de conjugaison de T est bien déterminée à partir de $\mathfrak{p}$. On la notera $(\mathfrak{p}, U/V)$ [ou $(\mathfrak{p}, E/K)$ si nous considérons les automorphismes du corps E/K plutôt que les transformations birationnelles]. Si G est abélien, cette classe de conjugaison se réduit à un seul élément.

Comme nous l'avons déjà dit plus haut, si χ est un caractère de G, μ un entier positif et T un élément de $(\mathfrak{p}, U/V)$, nous poserons

$$\chi(\mathfrak{p}^\mu)=\chi(T^\mu).$$

Nous allons maintenant profiter de la situation géométrique avec laquelle nous travaillons pour transformer la série L définie à partir des localités en une série L définie à partir des points.

Soit Q un point de V rationnel sur le corps k_m, unique extension de k de degré m. Si Q est simple sur V et non ramifié, on notera par $C_Q^{(m)}$ la classe de conjugaison associée à Q dans G comme on l'a fait plus haut, mais en prenant maintenant k_m comme corps de constantes. Autrement dit, $C_Q^{(m)}$ est l'unique classe contenant un élément T de G tel que pour P dans $f^{-1}(Q)$ on ait $T(P)=P^{(q^m)}$. On choisira un représentant de cette classe qu'on notera $T_Q^{(m)}$. Si $\mathfrak{p}$ est un cycle premier rationnel de V/k, de degré d divisant m, on a évidemment

$$(\mathfrak{p}, U/V)^{m/\deg(\mathfrak{p})}=T_Q^{(m)}$$

pour n'importe quel Q dans $\mathfrak{p}$.

Comme dans le présent travail nous nous occupons des séries L seulement du point de vue birationnel, nous allons adopter les conventions suivantes, quand il s'agira de points singuliers ou ramifiés : Soit Z un diviseur sur V, rationnel sur k, et contenant tous les points singuliers de V et tous les points ramifiés. Le corps k étant parfait, on peut supposer que toutes les composantes de Z ont la multiplicité 1. Un point Q de V appartient à Z si et seulement si tous ses conjugués (sur k) appartiennent aussi à Z. Si tel est le cas, on prendra $T_Q^{(m)}$ égal à l'élément neutre de G, et l'on posera $\chi(Q)=1$.

Nous nous servirons aussi de la définition de la série L à partir de sa dérivée logarithmique au lieu de son logarithme. Dans un cas comme celui-ci, on conviendra toujours de normer la fonction en prescrivant qu'elle prenne la valeur 1 pour $t=0$. Nous pouvons alors écrire

$$\frac{d}{dt}\log L(t,\chi,E/K)=\sum_{m=1}^{\infty}\left(\sum_{\deg(\mathfrak{p})\mid m}\chi(\mathfrak{p}^{m/\deg(\mathfrak{p})})\deg(\mathfrak{p})\right)t^{m-1}.$$

Compte tenu de nos remarques précédentes, on voit que le coefficient de t^{m-1} dans cette somme est égal à

$$\sum_{Q\in V_m}\chi(T_Q^{(m)}),$$

la somme étant prise pour tous les points Q de V rationnels sur k_m (ce ensemble étant noté V_m).

Nous allons maintenant énoncer le théorème principal que nous avons en vue.

THÉORÈME 1. — *Soit $f: U^r\to V^r$ un revêtement galoisien de groupe G, défini sur un corps fini k à q éléments. Soit Z un diviseur sur V, rationnel sur k, contenant tous les points singuliers et les points ramifiés de V. Soit χ un caractère simple de G. Alors il existe un nombre A dépendant de f, U, V, Z (mais pas de q) tel que*

$$\left|\sum\chi(T_Q)\right| \leq A q^{\left(r-\frac{1}{2}\right)} \qquad si\quad \chi\neq\chi_1$$

et

$$\left|\sum\chi(T_Q)-q^r\right|\leq A q^{\left(r-\frac{1}{2}\right)} \qquad si\quad \chi=\chi_1.$$

Le cas où $\chi=\chi_1$ est celui de la fonction ζ, et a déjà été démontré dans [7] et [11].

Dans le théorème, on a pris $T_Q=T_Q^{(1)}$, et les sommes sont prises pour Q dans $V_1=V_k$, l'ensemble des points rationnels de V dans k. On a $\chi(T_Q)=\chi(Q)$, en considérant Q comme point rationnel.

Le théorème sera démontré dans les nos 3 et 4. Nous allons en tirer ici quelques corollaires.

Pour commencer, on peut appliquer l'argument formel d'ARTIN [1] pour en tirer la densité des localités dans une progression arithmétique. Soit C une classe de conjugaison de G, et T un élément de C. Pour $m \to \infty$, le théorème donne

$$\sum_{Q \in V_m} \chi(T_Q^{(m)}) = O\left(q^{m\left(r-\frac{1}{2}\right)}\right) \qquad \text{si} \quad \chi \neq \chi_1$$

et

$$\sum_{Q \in V_m} \chi(T_Q^{(m)}) = q^{rm} + O\left(q^{m\left(r-\frac{1}{2}\right)}\right) \qquad \text{si} \quad \chi = \chi_1.$$

On multiplie par $\chi(T^{-1})$ et l'on fait la somme. Si l'on note $N(C, m)$ le nombre de points Q rationnels sur k_m ayant leur $T_Q^{(m)}$ dans la classe C donnée, et h le nombre d'éléments de C, alors on trouve (en employant les relations d'orthogonalité)

$$\frac{h}{n} N(C, m) = q^{rm} + O\left(q^{m\left(r-\frac{1}{2}\right)}\right).$$

Cette formule donne la densité des points, et l'on retrouve trivialement celle des localités. En effet, si un point Q dans V_m est de degré $d < m$, donc $d \mid m$, on a $d \leqq m/2$. Une estimation grossière montre que la contribution de ces points à $N(C, m)$ peut être absorbée dans le terme d'erreur d'ordre $q^{m\left(r-\frac{1}{2}\right)}$. Si le point Q est de degré m exactement, alors il détermine une localité $\mathfrak{p}$, et il y a exactement m points dans $\mathfrak{p}$. Donc si l'on note par $N_0(C, m)$ le nombre de localités de degré m telles que $(\mathfrak{p}, U/V)$ soit égal à la classe C donnée, on trouve

$$\frac{h}{n} N_0(C, m) = \frac{1}{m} q^{rm} + O\left(q^{m\left(r-\frac{1}{2}\right)}\right).$$

En particulier, quand m tend vers l'infini, le nombre de localités de degré m dans une progression arithmétique donnée tend aussi vers l'infini. Notons également que le théorème est formulé pour une variété abstraite, et que le diviseur peut être pris arbitrairement. Donc on peut toujours trouver les localités en dehors d'un ensemble algébrique $F \subset V$, $F \neq V$. Si deux variétés sont en correspondance birationnelle sur k, la correspondance est biholomorphe en dehors d'un tel ensemble algébrique. On voit donc que le contenu de notre théorème est bien birationnel.

Remarquons enfin que pour $\chi \neq \chi_1$, la série qui définit la dérivée logarithmique converge dans le cercle $|t| < q^{-\left(r-\frac{1}{2}\right)}$ (conséquence immédiate de nos inégalités) et donc que $L(t, \chi, U/V)$ ne peut avoir de zéros ou de

pôles dans ce cercle. En prenant la représentation l-adique de G dans la variété d'Albanese on a fait ailleurs la conjecture relative au comportement sur le cercle $|t| = q^{-\left(r-\frac{1}{2}\right)}$. Au-delà de ce cercle, on ne sait quelles représentations il faut prendre.

La démonstration du théorème 1 se fera par réduction directe au cas des courbes, en prenant un système algébrique de revêtements, et en employant les résultats connus pour les courbes (démontrés par WEIL [14]).

Pour la convenance du lecteur nous allons rappeler ici ces résultats, et inclure quelques remarques sur l'uniformité qu'on obtient dans l'estimation de la somme $\sum \chi(T_Q)$.

Supposons d'abord que nous ayons un revêtement $f: W \to C$ où les deux courbes W et C sont non singulières, mais où il peut y avoir des ramifications. Alors la série L est un polynome $\prod (1 - \alpha_i t)$, où les α_i sont des nombres algébriques de valeur absolue $q^{\frac{1}{2}}$. Il est essentiel aussi de remarquer que le degré de ce polynome est donné par la formule

$$\frac{1}{[W:C]} \sum_{T \in G} \chi(T^{-1}) \operatorname{Tr}(T_*),$$

où $\operatorname{Tr}(T_*)$ est la trace de la représentation l-adique de T, dérivée de la jacobienne de W. On voit donc que le degré du polynome est borné, en fonction du genre de la courbe W. Soit d ce degré. Alors en prenant la dérivée logarithmique de $\prod (1 - \alpha_i t)$, on trouve

$$\sum \chi(T_Q) = -\sum_{i=1}^{d} \alpha_i.$$

Ceci montre que pour les courbes qui nous occupent, notre somme est bornée par $A q^{\frac{1}{2}}$, pour un nombre A ne dépendant que du degré du caractère χ, du genre de W, et du degré $[W:C]$.

Naturellement, la série L considérée ci-dessus par WEIL est la série L complète, où l'on a tenu compte des points de ramification. Dans notre définition, où nous avons convenu de poser $\chi(T_Q) = 1$ si Q est ramifié, on voit que notre somme diffère de celle obtenue pour une courbe non singulière par une constante dépendant du nombre de points ramifiés.

Dans notre réduction au cas des courbes, nous obtiendrons des courbes spécialisées d'une courbe générique, et le nombre de points de ramification, ou de points singuliers sur chaque courbe sera uniformément borné. C'est ce qui nous permettra de démontrer notre théorème.

Nous supposerons désormais que V et U sont des variétés projectives et normales, et dans le numéro suivant, nous allons rappeler quelques propriétés de la courbe générique. Ensuite nous spécialiserons dans les corps finis.

3. **La courbe générique.** — Nous employons principalement comme références le début des *Critères d'équivalence* de WEIL [16], et l'article de CHOW [3]. On sait que la courbe générique C_u s'obtient en coupant V par des hyperplans génériques sur k, $H_{u_1}, \ldots, H_{u_{r-1}}$, où les u_i sont des points génériques indépendants de l'espace projectif $\mathbf{P}'$ dual de l'espace $\mathbf{P}$ dans lequel V est plongée. Le produit de $\mathbf{P}'$ avec lui-même $(r-1)$ fois est une variété qui sera notée Γ, et dont le point générique est $u=(u_1, \ldots, u_{r-1})$, produit des u_i. La courbe C_u est définie sur $k(u)=k_u$, et tout point générique x^* de C_u sur k_u est un point générique de V sur k. On a

$$C_u = V.H_{u_1}\ldots H_{u_{r-1}} = V.L_u,$$

si L_u est la variété linéaire intersection des H_{u_i}. Nous allons faire une liste des propriétés de C_u qui nous serviront pour les calculs que nous avons en vue.

1° La courbe C_u est non singulière, et tout point de C_u est simple sur V

Regardons maintenant l'image inverse de C_u par f. Je dis que c'est une courbe W_u et que f induit une application rationnelle $f_u: W_u \to C_u$ de façon naturelle, et de même degré que f. Il suffit de démontrer ceci pour l'intersection de V avec un hyperplan générique H_u, et c'est alors un résultat à peu près équivalent au théorème de Bertini (*voir*, par exemple, ZARISKI [18] et MATSUSAKA [8]). Plus précisément, rappelons le lemme suivant :

LEMME. — *Soit $k(x)$ une extension régulière d'un corps infini k de caractéristique $p>0$, et y, z deux éléments de $k(x)$ indépendants sur k et tels que z ne soit pas une puissance p-ième dans $k(x)$. Alors pour tous les éléments c de k sauf un nombre fini, $k(x)$ est une extension régulière de $k(y+cz)$.*

Si (x) est un point générique de V/k, indépendant de u, et (y) est un point générique de U/k tel que $f(y)=(x)$, alors on construit $V.H_u$ de la façon suivante. Supposons que (x) soit un point affine, $(x)=(x_1, \ldots, x_N)$. Si $u_{11}, \ldots, u_{1N}$ sont indépendants de (x) sur k, on pose

$$u_{1,N+1} = u_{11}x_1 + \ldots + u_{1N}x_N.$$

Alors la variété $V.H_u$ est le lieu du point générique (x) sur $k(u_{11}, \ldots, u_{1N+1})$. Étant donné que $k(y)$ est séparable sur $k(x)$, on voit par le lemme que l'extension $k_u(y)$ sur $k(u)$ est régulière [bien que le corps k soit fini, $k(u_{11})$ est infini, par exemple]. On peut monter ainsi jusqu'à la courbe C_u,

et l'on voit que W est le lieu de (y) sur $k(u)$. L'application rationnelle f_u est définie par $f_u(y) = (x)$. En résumé, on a :

2° L'image inverse $f^{-1}(C_u)$ est une courbe W_u, simple sur U. On a un diagramme commutatif

$$\begin{array}{ccc} W_u & \xrightarrow{i} & U \\ {\scriptstyle f_u}\downarrow & & \downarrow{\scriptstyle f} \\ C_u & \xrightarrow[i]{} & V \end{array}$$

où i est l'inclusion, et $f_u : W_u \to C_u$ est un revêtement galoisien de même degré que f (1).

(A vrai dire, nous nous sommes borné dans nos définitions d'un revêtement à des variétés normales. Dans le cas présent, W_u peut ne pas être normale. Pour être strict, il faudrait donc dire que f_u est une application rationnelle, partout définie, et telle que l'image inverse d'un point de C_u ne contienne qu'un nombre fini de points. Nous ferons un abus de langage, et dirons toujours que f_u est un revêtement.)

Le groupe de transformations birationnelles de U sur V peut être identifié à celui de W_u sur C_u, les conjugués de (y) sur $k_u(x)$ étant précisément les mêmes que sur $k(x)$. On peut aussi mettre cette condition sous forme de diagramme commutatif, à savoir

$$\begin{array}{ccc} W_u & \xrightarrow{i} & U \\ {\scriptstyle T_u}\downarrow & & \downarrow{\scriptstyle T} \\ W_u & \xrightarrow[i]{} & U \end{array}$$

Autrement dit, on a :

3° Chaque T de G induit une transformation birationnelle T_u de W_u, telle que $f_u T_u = T_u$, et l'application $T \to T_u$ est un isomorphisme de G sur le groupe de W_u sur C_u.

La courbe W_u peut avoir des singularités. Mais le nombre de ces singularités est borné. En fait, on peut donner une borne supérieure à ces singularités.

---

(1) On peut retrouver un critère d'équivalence classique par la méthode des revêtements, en procédant comme suit : soit X un diviseur sur V, rationnel sur le corps k (supposé algébriquement clos); supposons que l'ordre de la classe d'équivalence linéaire de X soit égal à m premier à la caractéristique, et soit φ une fonction telle que $(\varphi) = mX$. Alors, on voit que l'extension $K(\varphi^{1/m})/K$ conserve son degré par restriction à la courbe générique C_u; comme $X.C_u$ est le diviseur de la fonction induite par φ sur C_u, l'ordre de la classe de $X.C_u$ sur C_u est exactement m.

4° L'intersection $Z.C_u$ est définie, et est un cycle de dimension o sur C_u et sur V. (C'est l'intersection de Z avec L_u.) Si Q est un point de C_u qui n'est pas dans $Z.C_u$, alors il existe exactement n points distincts de W_u au-dessus de Q, qui sont tous simples sur U et sur W_u.

Notre dernière assertion découle de la proposition 1, n° 2.

Les seules singularités de W_u se trouvent par conséquent au-dessus des points de $Z.C_u$. Soit d leur nombre. Il y a au plus nd points singuliers sur W_u.

Nous observons maintenant que les propriétés formulées ci-dessus restent valables pour presque toutes les spécialisations de u dans la clôture algébrique de k. Il existe un sous-ensemble k-fermé F de Γ, $F \neq \Gamma$, tel que pour une spécialisation a de u avec $a \notin F$, et a rationnel sur $\bar{k}$, les propriétés restent valables si u est remplacé par a. Par exemple, L_u se spécialise en L_a, $C_u = V.L_u$ se spécialise en $C_a = V.L_a$, et $C_u.Z$ se spécialise en un cycle de même degré $C_a.Z$. L'image inverse $f^{-1}(C_a)$ est une courbe W_a, et f induit une application rationnelle séparable $f_a : W_a \to C_a$, partout définie, de même degré que f. Chaque T de G étant partout défini sur U, induit une transformation birationnelle de W_a/C_a. Si Q est un point de C_a non contenu dans $C_a.Z$, alors les n points de U au-dessus de Q sont dans W_a. Si T et T' sont deux éléments de G, et si l'on a $T_a = T'_a$, alors pour n'importe lequel des P tels que $f(P) = Q$, on a :

$$T(P) = T_a(P) = T'_a(P) = T'(P), \qquad \text{donc} \quad T = T'.$$

Le groupe de Galois de U/V peut donc être identifié avec celui de W_a/C_a.

4. **Démonstration du théorème 1.** — Par $\mathfrak{x}_{n+1}$ nous désignerons le nombre des points de l'espace projectif $\mathbf{P}$ qui sont rationnels sur k. On a

$$\mathfrak{x}_{n+1} = \frac{q^{n+1} - 1}{q - 1}.$$

Si Γ est comme précédemment la variété produit de $r - 1$ espaces projectifs $\mathbf{P}'$ (dual de $\mathbf{P}$) alors le nombre de points rationnels de Γ dans k est évidemment égal à $(\mathfrak{x}_{n+1})^{r-1}$.

Le nombre d'hyperplans dans $\mathbf{P}'$ rationnels sur k passant par un point rationnel Q donné est égal à $\mathfrak{x}_n$. Chaque point a de Γ détermine une variété linéaire, notée L_a, et le nombre des points rationnels sur k tels que L_a passe par le point donné Q est donc égal à $(\mathfrak{x}_n)^{r-1}$. (La variété linéaire L_a peut dégénérer, c'est-à-dire avoir une dimension plus grande que celle de L_u, mais ceci ne pourra se passer que sur le sous-ensemble algébrique propre de Γ.)

On a

$$\frac{\mathfrak{x}_{n+1}}{\mathfrak{x}_n} = q + \frac{1}{\mathfrak{x}_n}, \tag{1}$$

$$q^{n-1} \leq \mathfrak{x}_n. \tag{2}$$

Par conséquent,

$$\left|\left(\frac{\chi_{n+1}}{\chi_n}\right)^{r-1} - q^{r-1}\right| \leq A_1 q^{r-2}, \tag{3}$$

$$q^{(n-1)(r-1)} \leq \chi_n^{r-1}, \tag{4}$$

A_1 étant une constante dépendant seulement de n et de r.

Soit, comme ci-dessus, Z un diviseur sur V, rationnel sur k, contenant tous les points ramifiés et tous les points singuliers, et ayant toutes ses composantes avec multiplicité 1. Soit F le sous-ensemble k-fermé de Γ défini au numéro précédent. On notera comme d'habitude par V_k (ou V_1) les points de V rationnels sur k. Si χ est un caractère de G, la relation suivante est alors évidente [nous écrivons $\chi(Q)$ au lieu de $\chi(T_Q)$]

$$\sum_{Q \in V_k} \chi(Q) = \frac{1}{\chi_n^{r-1}} \sum_{a \in \Gamma_k} \sum_{Q \in V \cap L_a} \chi(Q).$$

Si X est un ensemble algébrique k-fermé, nous noterons $N(X)$ le nombre de points rationnels de X dans k. Il existe une constante A_2 telle que

$$N(F) \leq A_2 q^{n(r-1)-1} \leq A_2 \chi_n^{r-1} q^{r-2}.$$

On trouve ceci en notant que la dimension de Γ est $n(r-1)$, $\dim F < \dim \Gamma$, et en appliquant les résultats de [7] et l'inégalité (4).

On peut séparer la somme $\sum \chi(Q)$ selon que le point a est bon ou mauvais, c'est-à-dire selon qu'il est dans F ou non. Si $a \notin F$, alors $V \cap L_a = V.L_a$ est une courbe définie sur k, et l'on récrit la somme comme suit :

$$\frac{1}{\chi_n^{r-1}} \sum_{a \notin F} \sum_{Q \in V.L_a} \chi(Q) + \frac{1}{\chi_n^{r-1}} \sum_{a \in F} \sum_{Q \in V \cap L_a} \chi(Q).$$

Considérons d'abord le cas où $\chi = \chi_1$ est le caractère principal. Les deux sommes deviennent

$$\frac{1}{\chi_n^{r-1}} \sum_{a \notin F} N(V.L_a) + \frac{1}{\chi_n^{r-1}} \sum_{a \in F} N(V \cap L_a).$$

On va voir que la méthode que nous sommes en train d'employer pour compter les points de V donne le même résultat que celle de [7]. Considérons la première somme. D'après la théorie des courbes, on a

$$|N(V.L_a) - q| \leq A_3 q^{\frac{1}{2}}. \tag{5}$$

Compte tenu de l'inégalité pour $N(F)$ obtenue plus haut, et de l'inégalité (3), on trouve

$$\left|\frac{1}{\chi_n^{r-1}} \sum_{a \notin F} N(V.L_a) - q^r\right| \leq A_4 q^{\left(r-\frac{1}{2}\right)}.$$

Compte tenu du résultat connu concernant le nombre de points [7], ceci montre que la somme prise pour les bons points a donne déjà le nombre de points $N(V)$, à un terme d'ordre $q^{r-\frac{1}{2}}$ près. Donc la somme prise sur les mauvais points satisfait à une inégalité du type

$$\left| \frac{1}{\chi_n^{r-1}} \sum_{a \in F} N(V \cap L_a) \right| \leq A_5 q^{r-\frac{1}{2}}.$$

On a donc montré que si l'on compte par induction avec une famille d'hyperplans (comme dans [7]) ou si l'on compte comme ici par une famille de courbes, on trouve le même résultat.

Nous revenons maintenant à un caractère simple arbitraire χ. Alors $\chi(Q)$ a une valeur absolue uniformément bornée. Donc la seconde somme, prise pour les mauvais points, satisfait à la même estimation que celle que nous venons de trouver pour le caractère principal, c'est-à-dire est d'un ordre de grandeur $q^{r-\frac{1}{2}}$. Tout ce qui reste à démontrer est que la première satisfait à cette estimation quand $\chi \neq \chi_1$.

Pour $a \notin F$, si Q n'est pas dans $C_a.Z$, alors Q n'est pas ramifié dans W_a : les n points distincts de U au-dessus de Q sont précisément les n points distincts de W_a au-dessus de Q. D'après la proposition 1, ils sont donc simples sur W_a. Soit W_a' la courbe non singulière birationnellement équivalente à W_a sur k. Le nombre de points où la transformation entre W_a et W_a' n'est pas biholomorphe ne peut dépasser

$$[U : V] \deg(C_a.Z) = [W_a : C_a] \deg(C_a.Z),$$

autrement dit il est uniformément borné.

D'autre part, le genre de C_a est égal au genre de C_u pour $a \notin F$ (*cf.* [10]) et le nombre de points ramifiés de C_a dans W_a' n'excède pas $\deg(C_a.Z)$. Quant à la courbe W_a', son genre est aussi borné par celui de W_u. En effet, si l'on prend une extension inséparable de $k(u)$, on a une transformation birationnelle entre W_u et une courbe W_u' non singulière. [J'ignore si la $k(u)$-normalisation de W_u est déjà non singulière.] Comme nous spécialisons dans un corps fini (qui est parfait), la spécialisation de W_u' [défini sur une extension purement inséparable de $k(u)$] sera néanmoins définie sur $k(a)$. Le genre de W_a' est donc uniformément borné.

Les groupes de Galois de W_a'/C_a et de W_a/C_a peuvent alors être identifiés, en tant que groupes de transformations sur les points de W_a' et W_a respectivement, en dehors des points où la transformation birationnelle n'est pas biholomorphe.

De plus, si Q est un point de $C_a = V.L_a$ qui n'est pas dans $C_a.Z$, les n points P_i au-dessus de Q dans V coïncident avec les n points au-dessus de Q dans W_a. Si la transformation T de G induit T_a sur W_a, alors la

commutativité montre que $(Q, W_a/C_a) = (Q, U/V)_a$. De ces remarques, il résulte l'inégalité

$$\left| \sum_{Q \in C_a} \chi(Q) \right| \leq A_6 q^{\frac{1}{2}}$$

le nombre A_6 ne dépendant que des genres de W_a (plutôt W'_a), de C_a, et du nombre de points de ramification, tous bornés.

Mais le nombre de termes dans la somme prise pour les points $a \notin F$ est égal à $N(\Gamma) - N(F)$.

De plus, on a l'inégalité

$$\left| \frac{N(\Gamma) - N(F)}{\chi_n^{r-1}} \right| \leq A_7 q^{r-1}$$

qu'on déduit de (3) et de celle de $N(F)$ obtenue plus haut. En la combinant avec celle que nous venons de trouver pour les courbes, on trouve le théorème qu'il s'agissait de démontrer.

5. **L'image réciproque d'un revêtement.** — Soit V une variété abstraite, définie sur un corps k qu'on peut supposer parfait pour commencer. Soit $\alpha : V \to A$ une application rationnelle de V dans une variété de groupe commutatif A, α et A étant également définis sur k. (On pourrait s'occuper du cas plus général où A est une variété arbitraire, ou un groupe non commutatif, mais les applications que nous ferons porteront uniquement sur le cas d'un groupe commutatif. Nous nous plaçons donc immédiatement dans ce cas pour alléger l'exposition.) Nous supposerons de plus que V est sans singularités, et que α est défini en tout point de V. (Il ne s'agit pas de résoudre les singularités ; on enlève tout simplement les points singuliers, et les points où α n'est pas défini. Il reste toujours une variété abstraite.)

Soit $\lambda : B \to A$ une isogénie séparable, c'est-à-dire un homomorphisme séparable avec noyau fini. On suppose λ et B définis sur k. Si le noyau de λ est contenu dans les points rationnels B_k, on dira que k est *complet pour* λ. Nous supposerons ici qne c'est bien le cas.

Le revêtement $\lambda : B \to A$ est non ramifié, ce qui veut dire qu'il existe exactement n points distincts de B dans l'image réciproque d'un point de A. Nous allons maintenant voir comment on peut construire l'image réciproque de B/A, pour obtenir un revêtement U de V.

Soit (y) un point générique de B/k et $(x) = \lambda(y)$. L'extension $k(y)$ sur $k(x)$ est abélienne, et son groupe de Galois $\mathfrak{g}$ est le groupe des translations sur B par un sous-groupe de B_k. Chaque automorphisme peut se représenter par une translation

$$y \to y + b_i, \qquad (b_i \in \mathfrak{g}).$$

Soit v un point générique de V/k, et posons $K = k(v)$. Soit $\xi = \alpha(v)$.

Alors $x \to \xi$ est une spécialisation. Soit η n'importe quelle spécialisation de y sur $x \to \xi$. Le corps $k(\eta)$ ne dépend pas de la spécialisation η, car n'importe quelle autre est de type $\eta + b_i$, et l'on a

$$k(\eta) = k(\eta + b_i).$$

De plus, $k(\eta)$ contient $k(\xi)$. Le cycle $\sum(\eta + b_i)$ est l'unique spécialisation du cycle $\sum(y + b_i)$ sur $x \to \xi$.

Il se peut que k ne soit pas le corps des constantes de $k(\eta)$, ou que k ne soit pas le corps des constantes du corps composé $k(\nu, \eta)$. Nous supposerons qu'il l'est c'est-à-dire que k est algébriquement clos dans $k(\nu, \eta)$. On peut alors définir la normalisation U de V dans $E = k(\nu, \eta)$. Ce sera une variété normale, définie sur k (supposé parfait). On obtient ainsi un revêtement $f : U \to V$ qui sera dit *dérivé* du revêtement $\lambda : B \to A$, ou *image réciproque* de $\lambda : B \to A$.

On peut écrire $k(\nu, \eta) = k(u)$ où u est un point générique de U/k, et $f(u) = \nu$. On a une application rationnelle $\beta : U \to B$ définie par $\beta(u) = \eta$.

Si

$$[U : V] = [B : A],$$

autrement dit si $[k(u) : k(\nu)] = [k(y) : k(x)]$, on dira que l'image réciproque est *non dégénérée*. Si k est algébriquement clos et si l'image réciproque de tout revêtement de type $\lambda : B \to A$ donnée par une isogénie séparable λ est non dégénérée, on dira que V et A sont *bien adaptés par* α, ou simplement bien adaptés.

Considérons de plus près le cas non dégénéré.

La variété U peut encore se décrire d'une autre façon. Soit U_1 la variété dont le point générique sur k est (ν, η). Elle est birationnellement équivalente à U, et nous verrons dans un instant qu'en fait elle lui est biholomorphe.

Si Q est un point de V, alors la spécialisation $\nu \to Q$ détermine une spécialisation $\xi \to \xi'$, car nous avons supposé α partout défini. Si $\lambda^{-1}(\xi') = \sum \eta_i'$, où les η_i' sont les n points distincts au-dessus de ξ', alors la spécialisation $(\nu, \xi) \to (Q, \xi')$ se prolonge de manière unique en $\sum(\eta_i) \to \sum(\eta_i')$. On voit donc qu'au-dessus de chaque point Q de V il y a exactement n points de U_1. D'après la proposition 1, ils sont simples sur U_1 (car nous avons supposé V non singulière). De ceci on déduit immédiatement que U et U_1 sont biholomorphes, donc que U est non singulière. Ces remarques peuvent être résumées dans la proposition suivante :

PROPOSITION 2. — *Soit V une variété algébrique abstraite, non singulière.*

Soient $\alpha : V \to A$ une application rationnelle, partout définie, et $\lambda : B \to A$ une isogénie séparable. Supposons l'image réciproque $f : U \to V$ non dégénérée. Alors tous les points de V sont non ramifiés dans U, qui est non singulière.

Si l'image réciproque est dégénérée, on voit facilement qu'on peut la réduire au cas non dégénéré en passant à une extension du corps de constantes, et en prenant l'image réciproque d'un revêtement C intermédiaire à B/A. On voit aussi que nous n'avons pas employé l'hypothèse que A et B sont des groupes. Mais ici, nous nous intéressons particulièrement au cas où le corps de base k est fini, avec q éléments. Comme on sait, on peut alors définir un revêtement $\rho : A \to A$ par la formule

$$\rho(y) = y^{(q)} - y,$$

qui sera appelé le *q-revêtement de A*. On a alors les exemples suivants :

A est le groupe multiplicatif G_m. Les images réciproques par applications dans G_m donnent les extensions kummériennes cycliques de K.

A est un groupe de Witt W_μ [17]. On obtient alors les extensions cycliques de degré p^μ.

(On peut prendre aussi des produits de G_m et des produits de W_μ pour donner les extensions abéliennes).

A est la variété d'Albanese. On obtient alors le corps de classe de HILBERT [6].

On remarquera que toute isogénie séparable $\lambda : B \to A$ définie sur la clôture algébrique $\bar{k}$ d'un corps fini k peut toujours s'obtenir comme revêtement intermédiaire d'un q-revêtement. En effet, on prend un corps de définition fini k, complet pour λ. Alors la commutativité de λ et ρ montre que λ est intermédiaire. Cette construction arithmétique remplace avantageusement la division des périodes dans le cas d'une variété abélienne. Elle ne peut se faire naturellement que sur la clôture algébrique d'un corps fini, mais dans ce cas elle donne bien une idée générale de la structure de la tour d'isogénies séparables au-dessus de A.

Considérons de nouveau le cas d'une image réciproque non dégénérée d'un revêtement $\lambda : B \to A$. Le revêtement U/V est alors abélien, et le groupe d'automorphismes de $k(u)$ sur $k(v)$ (ou de transformations birationnelles de U sur V) s'identifie avec celui de $k(y)$ sur $k(x)$ (ou de B/A). En effet, le groupe de translations b_i s'interprète comme groupe de translations de $k(\eta)$ sur $k(\xi)$, chaque translation τ appliquant η sur $\eta + b_i$. De plus une transformation T dans le groupe G de U/V est déterminée de façon unique par la relation

$$\beta T = \tau\beta.$$

Si T et τ se correspondent de cette façon, nous noterons cette relation par $T \leftrightarrow \tau$.

On a alors une loi de réciprocité (loi de décomposition) pour les cycles premiers rationnels de V dans U, relative à (α, A). Si $\mathfrak{a}$ est un cycle sur A, $\pi(\mathfrak{a})$ désignera la somme des points de $\mathfrak{a}$. Si $\mathfrak{a}$ est rationnel sur k, alors $\pi(\mathfrak{a})$ est un point rationnel de A dans k. Pour un cycle $\mathfrak{a}$ de V, nous écrirons $\pi(\mathfrak{a})$ au lieu de $\pi(\alpha(\mathfrak{a}))$, pour simplifier. L'opération π dépend de α bien entendu, et devrait être notée π_α, mais comme il s'agira toujours de la même application α, nous écrirons tout simplement π.

Si $\mathfrak{p}$ est un cycle premier rationnel de V, et $\pi(\mathfrak{p}) = a$, on voit trivialement que

$$(\mathfrak{p}, U/V) \leftrightarrow (a, B/A).$$

En particulier, si $\pi(\mathfrak{a}) = 0$, alors $(\mathfrak{a}, U/V)$ est l'identité.

On peut alors interpréter l'existence de localités dans une progression arithmétique de la façon suivante :

THÉORÈME 2. — *On suppose V^r abstraite, non singulière, définie sur le corps fini k. Soit $\alpha : V \to A$ une application rationnelle, partout définie, et supposons que l'image réciproque par α du q-revêtement $\rho(y) = y^{(q)} - y$ de A soit non dégénérée. Soit a un point rationnel dans A_k, et soit $N_0(a, \mu)$ le nombre des cycles premiers rationnels de V/k tels que $\deg(\mathfrak{p}) = \mu$ et que $\pi(\mathfrak{p}) = a$. Désignons par h le nombre de points de A_k. Alors*

$$N_0(a, \mu) = \frac{1}{h\mu} q^{\mu r} + O\left(q^{\mu\left(r-\frac{1}{2}\right)}\right)$$

pour $\mu \to \infty$.

Le théorème est une traduction du résultat du paragraphe 2, compte tenu de l'identification entre le groupe de Galois et le groupe des points rationnels A_k.

En particulier, nous retrouverons ici les propositions qui servent dans la théorie du corps de classes et démontrées en Appendice dans [6], car on sait que l'image réciproque d'une isogénie séparable de la variété d'Albanese est non dégénérée. De plus, nous les retrouvons généralisées à des groupes commutatifs non complets, pourvu seulement que l'image réciproque soit non dégénérée. Ceci sera essentiel pour l'élaboration de la théorie du corps de classes des extensions ramifiées. Dans ce qui suit, nous allons montrer comment la partie arithmétique de [6] se généralise.

La partie algébrique, qui a pour but de montrer quels revêtements de V on obtient par image réciproque d'une isogénie reste à faire. Pour les revêtement non ramifiés, on sait qu'on les obtient tous par la variété d'Albanese, sauf ceux dus à la torsion, ou à certaines p-extensions.

6. Théorie du corps de classes. — Soit V une variété abstraite, et $\alpha : V \to A$ une application rationnelle de V dans une variété de groupe commutatif. On

suppose tout ceci défini sur le corps fini k. De plus, on supposera V sans singularités, et α défini en tout point de V. (Il suffira d'enlever les points offensants).

On peut alors définir les classes de cycles relatives à (α, A) de la façon suivante. Soit $Z(V, k)$ le groupe des cycles de V rationnels sur k. Soit $Z_0(V, k)$ le sous-groupe des cycles de degré o. Alors l'application π induit un homomorphisme de $Z(V, k)$ dans A_k, et de $Z_0(V, k)$ dans A_k. Le noyau de π dans $Z_0(V, k)$ sera noté $Z_\alpha(V, k)$. On l'appellera le *noyau de* (α, A). Le Le groupe facteur Z/Z_α sera appelé le groupe des *classes de cycles* $C_K(V)$; on pourrait démontrer que c'est un invariant birationnel, ne dépendant que de K et de α. Nous ne le démontrerons que dans le cas où l'image réciproque du q-revêtement de A est non dégénérée. C'est alors une conséquence immédiate de l'identification de A_k avec le groupe de Galois de U/V, au moyen de l'application de réciprocité. En effet, si l'on considère la décomposition d'une localité de V dans le corps E/K, E étant le corps de fonctions de U, on sait qu'il existe toujours un cycle $\mathfrak{a}$ de degré 1, rationnel sur k, tel que $(\mathfrak{a}, U/V) = 1$. L'application de réciprocité étant surjective, on voit immédiatement que si V_1 est un autre modèle de K/k, on peut prendre un cycle $\mathfrak{a}_1$ sur V_1 de degré 1 tel que $(\mathfrak{a}_1, U_1/V_1) = 1$. L'application des classes de cycles qui envoie $\mathfrak{a}$ sur $\mathfrak{a}_1$ est un isomorphisme.

Dans tout ce qui suit, on supposera que V et A sont bien adaptés par α. Alors π applique $Z_0(V, k)$ sur A_k. Soit E une extension finie arbitraire de K. On dira que E est de *type* (α, A) si la normalisation U de V dans le corps $E\bar{k}$ (définie sur $\bar{k}$) s'obtient comme image réciproque d'une isogénie séparable $\lambda : B \to A$, λ et B étant définis également sur $\bar{k}$. L'extension E/K peut ne pas être galoisienne, mais sur $\bar{k}$, elle devient abélienne, bien entendu.

Supposons que E soit galoisienne. Si E est de type (α, A), alors on sait par la proposition 2 que tous les points de V sont non ramifiés dans U, qui est non singulière. Soit k' le corps des constantes de E. Alors U est définie sur k'. On a des applications rationnelles

$$U \xrightarrow{f} V \xrightarrow{\alpha} A,$$

f étant défini sur k', et α sur k. On voit que αf est partout défini. U étant non singulière, on peut alors définir les classes de cycles $Z(U, k')$ comme ci-dessus, et l'on a un homomorphisme

$$S_K^E : C_E(U) \to C_K(V)$$

des classes de cycles de E dans celles de K, au moyen de la trace.

Toutes les notions employées pour énoncer la théorie du corps de classes sont maintenant définies, et les énoncés de [6] (dans le § 5 et le théorème 5 du § 9) ont un sens, si l'on remplace partout l'expression « de type Albanese » par « de type (α, A) ». Sauf pour le théorème de limitation

qui demande quelques remarques, les démonstrations données dans [6] s'appliquent sans changement. Il est donc inutile de les reproduire ici. (*Voir*, § 6 à 10 de [6]).

Remarquons seulement qu'en ce qui concerne la surjectivité de l'application de réciprocité, on peut la démontrer très simplement et directement dans une extension galoisienne E/K pouvant même admettre une extension du corps des constantes (et pas seulement géométrique comme nous l'avons fait plus haut). En effet, supposons E/K abélien pour simplifier. A chaque $\mathfrak{p}$ de V on associe le groupe de décomposition $D_{\mathfrak{p}}$ et l'on prend le corps K' fixe pour le sous-groupe engendré par les $D_{\mathfrak{p}}$. Il s'agit de montrer que $K'=K$. Tout $\mathfrak{p}$ se décompose complètement dans K' (on suppose naturellement $\mathfrak{p}$ non ramifié). S'il y avait une extension du corps de constantes dans K', on voit tout de suite que ce serait impossible. Nous sommes alors ramenés au cas géométrique, que nous connaissons.

Quant au théorème de limitation, supposons que F/K soit une extension galoisienne arbitraire. On rétrécit alors V en enlevant un sous-ensemble k-fermé X tel que tout point de $V-X$ soit non ramifié dans F. On peut de nouveau définir les classes de cycles. Elles ne changent pas pour $V-X$, et l'on en obtient pour F. De plus on a le lemme habituel :

LEMME. — *Soit F une extension galoisienne de K, et E une extension abélienne. Soit V un modèle abstrait de K, non singulier, et tel que toute localité soit non ramifiée dans EF. Soit $\mathfrak{q}$ une localité de F dans la normalisation de V dans F. Alors la restriction de $(\mathfrak{q}, EF/F)$ à E est égale à $(S_K^F(\mathfrak{q}), E/K)$.*

D'après le théorème d'existence, on prend pour E le corps de classes de type (α, A) appartenant au groupe de trace $S_K^F C_F$. Alors pour tout $\mathfrak{q}$ dans F, on doit avoir $(\mathfrak{q}, EF/F)=1$. Ceci est impossible, car on sait qu'il y a une infinité de localités de F qui ne se décomposent pas complètement dans E si $E \neq F$.

La seule différence entre la démonstration donnée ici et celle de [6] est que nous sommes forcés de définir les classes de cycles à partir de α, tandis que si l'on travaille avec la variété d'Albanese, on peut définir les classes de cycles à chaque étage indépendamment. Pour les définir dans le cas présent, il faut de plus passer par un rétrécissement, qui se trouve en fin de compte être sans importance.

Enfin, pour terminer, montrons comment on peut développer la théorie du corps de classes pour une courbe C dans le cas ramifié. Supposons pour commencer que C soit définie sur un corps k arbitraire. Grâce à un théorème de Rosenlicht (encore inédit) on sait que ses jacobiennes généralisées (que nous appellerons aussi jacobiennes de Rosenlicht) satisfont à la propriété d'application universelle pour les applications de C dans les variétés de groupe commutatif. On peut d'ailleurs se restreindre aux jacobiennes provenant d'un

anneau semi-local du type $k + \mathfrak{c}$ ou $\mathfrak{c}$ est un diviseur positif sur la courbe. Vu la remarque faite au paragraphe 5, que tous les revêtements abéliens d'une variété proviennent d'images réciproques d'isogénies de groupes algébriques commutatifs (sur le domaine universel, bien entendu) on peut conclure du théorème de Rosenlicht qu'ils proviennent tous d'images réciproques d'isogénies de jacobiennes généralisées du type ci-dessus. Comme Serre l'a remarqué, il s'ensuit immédiatement que l'application canonique $\alpha : C \to J$ de la courbe dans une jacobienne de Rosenlicht satisfait à la condition que nous avons énoncée plus haut, à savoir que l'image réciproque d'une isogénie de J conserve son degré, c'est-à-dire que C et (α, J) sont bien adaptées. Nous voyons donc que, pour les courbes, on obtient la classification géométrique qui nous fait défaut pour les variétés de dimension supérieure.

D'autre part, supposons C définie sur le corps fini k, et le diviseur $\mathfrak{c}$ rationnel sur k. D'après les résultats de Weil sur les groupes de transformations et les espaces homogènes, on sait qu'il existe une application canonique de C dans un espace principal homogène H de J, tous ces objets étant définis sur k. Comme k est fini, l'espace H possède un point rationnel [*cf.* S. LANG, *Algebraic groups over finite fields* (*Amer. J. Math.*, July 1956, th. 2)], et l'on peut donc trouver une application canonique de C dans J définie sur k. La courbe et sa jacobienne étant bien adaptées, nons obtenons donc la théorie du corps de classes comme nous l'avons indiqué au début de ce numéro.

De plus, on peut retrouver la théorie exprimée en langage d'idèles (et donc la théorie cohomologique avec le cocycle fondamental) par un raisonnement facile, comme le fit Chevalley lorsqu'il introduisit les idèles pour la première fois. On voit alors que si $\mathfrak{c}$ est le conducteur au sens classique d'une extension abélienne géométrique du corps de fonctions de la courbe C, cette extension est une image réciproque d'une isogénie de la jacobienne définie par l'anneau $k + \mathfrak{c}$.

BIBLIOGRAPHIE.

[1] E. ARTIN, *Ueber eine neue art von L-Reihen* (*Abh. math. Sem. Hamburg Univ.*, Bd. 2, 1924).

[2] E. ARTIN, *Zur theorie der L-Reihen mit allgemeinen gruppencharakteren* (*Abh. math. Sem. Hamburg Univ.*, Bd. 8, 1930).

[3] W. L. CHOW, *Abstract theory of the Picard and Albanese varieties* (à paraître dans les *Annals of Mathematics*).

[4] W. KRULL, *Galoische theorie der ganz abgeschlossene Stellenringe* (*Sitzungsberichte der phys.-med. Soz. zu Erlangen*, Bd. 67-68, 1935-1936).

[5] S. LANG, *L-series of a covering* (à paraître aux *Proceedings of the National Academy*, U. S. A., 1956).

[6] S. LANG, *Unramified class field theory* (à paraître dans les *Annals of Mathematics*, 1956).

[7] S. LANG et A. WEIL, *Number of points of varieties in finite fields* (*Amer. J. Math.*, vol. 72, No 4, octobre 1954, p. 818-827).

[8] T. MATSUSAKA, *The theorem of Bertini on linear systems in modular fields* (*Mem. College of Science, Univ. of Kyoto*, Series A, Math., vol. 26, No 1, juillet 1950).

[9] M. NAGATA, *On the theory of Henselian Rings* (*Nagoya math. J.* vol. 5, 1953, p. 45-57, et vol. 7, 1954, p. 1-19).

[10] Y. NAKAI, *On the genus of algebraic curves* (*Mem. College of Science, Univ. of Kyoto*, Series A, Math., No 2, 1952).

[11] L. B. NISNEVIC, *Ueber die Anzahl der Punkte einer algebraische Mannigfaltigkeit in einem endlichen Primkörper* (en russe *Doklady Akad. Nauk* U. S. S. R., 1954).

[12] F. K. SCHMIDT, *Die theorie der Klassenkörper...* (*Sitzungsberichten der phys. med. Soz. zu Erlangen*, Bd. 62, 1930, p. 267-284).

[13] A. WEIL, *Number of solutions of equations in finite fields* (*Bull. Amer. Math. Soc.*, vol. 55, No 5, 1949, p. 497-508).

[14] A. WEIL, *Sur les courbes algébriques et les variétés qui s'en déduisent* (Paris, Hermann, 1948).

[15] A. WEIL, *Footnote to a recent paper* (*Amer. J. Math.*, vol. 76, No 2, 1954).

[16] A. WEIL, *Critères d'équivalence* (*Math. Annalen*, Bd. 128, 1954).

[17] E. WITT, *Zyklische Körper und algebren der characteristik p vom Grad p^n* (*J. reine angew. Math.*, Bd. 176, 1936).

[18] O. ZARISKI, *Pencils on an algebraic variety and a new proof of a theorem of Bertini* (*Trans. Amer. math. Soc.*, 1941).

(Manuscrit reçu en avril 1956.)