Sobre o teorema de Artin-Weil

Elza F. Gomide

Sobre o Teorema de Artin-Weil

O estudo das variedades sobre um corpo finito conduziu à seguinte conjetura (Artin-Weil):

"Seja V uma variedade sem pontos singulares, definida sobre um corpo finito k. Seja N_ν o número de pontos racionais em V sobre a extensão k_ν de grau ν de k. Então a série formal $\sum_{\nu=1}^{\infty} N_\nu Z^{\nu-1}$ é a expansão de uma função racional de Z."

Esta conjetura foi demonstrada para curvas e ainda outras variedades de tipo particular (A.Weil, Les Courbes Algébriques et les variétés qui s'en déduisent, e Nurbers of Solutions of Equations in Finite Fields). Este trabalho contem pesquisas sobre essa conjetura.

Bibliografia

1) A.Weil - Les Courbes Algébriques et les variétés qui s'en déduisent.

2) A.Weil - Numbers of Solutions of Equations in Finite Fields - Bull. Am. Math. Soc., vol.55, n.5 (May,1949), pp. 497 a 508.

1. INTRODUÇÃO

Caracteres de um grupo abeliano finito.

Seja G um grupo abeliano com n elementos e seja χ uma aplicação de G no corpo dos números complexos que satisfaça à condição de homomorfismo

(1) $$\chi(a\,b) = \chi(a)\chi(b)$$

e ainda à condição

(2) $$\chi(1) \neq 0.$$

Dizemos que χ é um caracter do grupo G.

De (1) e (2) segue imediatamente que $\chi(1) = 1$.

O grupo abeliano G de ordem n é um produto direto de grupos cíclicos $G_1, \ldots, G_r$, de ordens $n_1, \ldots, n_r$ com $n = n_1 \ldots n_r$. Todo elemento $a \in G$ pode ser representado, de uma única maneira, na forma

$$a = \omega_1^{\nu_1} \ldots \omega_r^{\nu_r},$$

onde os ω_i são fixos, $\omega_i \in G_i$, e $0 \leqslant \nu_i < n_i$ $(i = 1, \ldots, r)$.

De (1) vem

$$\chi(a) = \chi(\omega_1^{\nu_1} \ldots \omega_r^{\nu_r}) = \chi(\omega_1)^{\nu_1} \ldots \chi(\omega_r)^{\nu_r}.$$

Por outro lado

$$\chi(\omega_i)^{n_i} = \chi(\omega_i^{n_i}) = \chi(1) = 1 \qquad (i = 1, \ldots, r),$$

portanto $\chi(\omega_i)$ é uma raiz n_i-ésima ζ_i da unidade $(i = 1, \ldots, r)$ e temos

(3) $$\chi(a) = \chi(\omega_1^{\nu_1} \ldots \omega_r^{\nu_r}) = \zeta_1^{\nu_1} \ldots \zeta_r^{\nu_r}$$

o que mostra que o valor de $\chi(a)$ fica determinado para todo $a \in G$ uma vez dados os valores dos $\chi(\omega_i)$, raizes n_i-ésimas da unidade.

Reciprocamente, seja ζ_i uma raiz n_i-ésima arbitrária da unidade $(i = 1, \ldots, r)$. A aplicação χ de G no corpo dos números complexos definida pela equação (3) é um caracter de G. O número de caracteres distin-

tos de G é portanto $n_1 n_2 \ldots n_r$, que é o número de elementos de G.

De (3) segue, para todo $a \in G$

$$|\chi(a)| = 1$$

e de (2) e (3)

$$\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi}(a)$$

Chama-se caracter principal de G o caracter χ_0 tal que $\chi_0(a) = 1$ para todo $a \in G$.

Sejam χ_1 e χ_2 dois caracteres de G e consideremos a aplicação de G no corpo dos números complexos definida por

$$\chi(a) = \chi_1(a)\chi_2(a)^{-1}$$

χ é evidentemente um caracter de G. Concluimos pois que os caracteres de G formam um grupo multiplicativo, no qual χ_0, o caracter principal, é o elemento unidade. A este grupo chamamos grupo dual de G, e o representamos por $\tilde{G}$. É facil verificar que G é isomorfo a $\tilde{G}$.

Calculemos agora $\sum_{a \in G} \chi(a)$ para um caracter χ arbitrário. Por (3) esta soma pode ser posta na forma

$$(4) \qquad \sum_{a \in G} \chi(a) = \prod_{i=1}^{r} (1 + \zeta_i + \ldots + \zeta_i^{n_i - 1})$$

Mas ζ_i é uma raiz n_i-ésima da unidade, logo, ou $\zeta_i = 1$, ou $1 + \zeta_i + \ldots + \zeta_i^{n_i - 1} = 0$

Portanto o segundo membro de (4) é igual a 0, a menos que

$$\zeta_1 = \zeta_2 = \ldots = \zeta_r = 1$$

e neste caso χ é o caracter principal, para o qual a soma considerada é evidentemente igual a n. Temos pois

$$(5) \qquad \sum_{a \in G} \chi(a) = \begin{cases} n \text{ se } \chi = \chi_0 \\ 0 \text{ se } \chi \neq \chi_0 \end{cases}$$

Pondo $\chi = \chi_1 \chi_2^{-1}$ obtemos

(6) $$\frac{1}{n}\sum_{a\in G}\chi_1(a)\overline{\chi}_2(a) = \begin{cases} 1 \text{ se } \chi_1 = \chi_2 \\ 0 \text{ se } \chi_1 \neq \chi_2 \end{cases}$$

Sejam $\chi_1,\ldots,\chi_n$ os caracteres de G numa certa ordem, $a_1,\ldots,a_n$ os elementos de G. Consideremos a matriz $A = \|c_{ik}\|$ onde $c_{ik} = \chi_i(a_k)$, e seja A' a matriz transposta de A. Por (6) temos

$$A.\overline{A}' = n.I$$

onde I é a matriz unitária de ordem n, e portanto

$$\overline{A}'.A = nI \quad \longrightarrow \quad \overline{A}.A' = n.I \text{ ?}$$

o que dá

(7) $$\frac{1}{n}\sum_{\chi}\chi(a)\overline{\chi}(a') = \begin{cases} 1 \text{ se } a = a' \\ 0 \text{ se } a \neq a' \end{cases}$$

Somas de Gauss para um corpo finito.

Seja k um corpo com q elementos. Consideremos o grupo aditivo dos elementos de k, que é um grupo abeliano finito, e os caracteres deste grupo, isto é, as aplicações φ do grupo no corpo dos números complexos que satisfazem às condições

$$\varphi(a+b) = \varphi(a)\varphi(b) \; ; \; \varphi(0) \neq 0$$

Designaremos o grupo dos caracteres φ por $\tilde{k}$, e o caracter principal por φ_0.

Por outro lado, consideremos o grupo multiplicativo k^* dos elementos de k distintos de zero, e o grupo $\tilde{k}^*$ dos caracteres χ deste grupo. k^* é um grupo cíclico de q-1 elementos, portanto um caracter χ qualquer fica completamente determinado quando se dá o seu valor para um gerador ω de k^*. Como $\chi(\omega^{q-1}) = \chi(\omega)^{q-1} = 1$, temos $\chi(\omega) = \zeta$, onde ζ é uma raiz (q-1)-ésima da unidade: $\zeta = e^{2\pi i\alpha}$ onde α é um número racional tal que $(q-1)\alpha \equiv 0 \pmod 1$, e que podemos escolher satisfazendo

$0 \leqslant \alpha < 1$. Dado um α tal que $(q-1)\alpha \equiv 0 \pmod 1$, indicaremos por χ_α o caracter tal que $\chi_\alpha(\omega) = e^{2\pi i \alpha}$, ω sendo um gerador de k^* fixado. A α inteiro corresponde o caracter principal.

Definiremos χ_α para o elemento 0 pela convenção: $\chi_\alpha(0) = 0$ se $\alpha \not\equiv 0 \pmod 1$ e $\chi_\alpha(0) = 1$ se $\alpha \equiv 0 \pmod 1$.

Chamam-se somas de Gauss de k as somas

$$g(\chi) = \sum_x \chi(x)\,\varphi(x)$$

onde φ é um caracter aditivo fixado, e χ é um qualquer caracter multiplicativo, φ e χ não principais.

Verifica-se facilmente a seguinte propriedade das somas de Gauss:

(8) $$g(\chi)\,\overline{g}(\chi) = q$$

Deve-se a Davenport e Hasse (J. Reine Angew. Math. vol.172 (1935) pp. 151-182) a demonstração de uma importante relação entre as somas de Gauss num corpo finito e nas extensões deste corpo. Seja k_ν a extensão algébrica de grau ν de k. Seja ω um gerador fixo de k^*, e seja ω' um gerador de k_ν^* tal que a norma $N(\omega')$ de ω' sobre k seja ω. Designemos por χ' os caracteres de k_ν^*, e por χ os caracteres de k^*. Então se $(q-1)\alpha \equiv 0 \pmod 1$, χ'_α é um caracter de k_ν^* que satisfaz $\chi'_\alpha(x) = \chi_\alpha[N(x)]$ para todo $x \in k_\nu^*$. φ sendo um caracter aditivo fixo, não principal, de k, seja φ' a aplicação de k_ν no corpo dos números complexos definida por $\varphi'(x) = \varphi[T(x)]$ para todo $x \in k_\nu$, onde $T(x)$ indica o traço de x sobre k. φ' é um caracter aditivo, não principal, de k_ν. Seja

$$g'(\chi'_\alpha) = \sum_x \chi'_\alpha(x)\,\varphi'(x)$$

Então (teorema de Davenport e Hasse)

(9) $$-g'(\chi'_\alpha) = \left[-g(\chi_\alpha)\right]^\nu$$

Definiremos ainda as chamadas somas de Jacobi para o corpo k. Sejam $\alpha_1, \ldots, \alpha_r$ números racionais satisfazendo

$$(q-1)\,\alpha_i \equiv 0\ ,\quad \alpha_i \equiv 0 \pmod 1\ ,\quad (i=1,\dots,r)$$

e consideremos a soma

$$\sum_{\sum x_i = 0} \chi_{\alpha_1}(x_1)\dots\chi_{\alpha_r}(x_r)$$

É facil ver que se $\sum \alpha_i \equiv 0 \pmod 1$ esta soma é 0. Defato, nesta soma os termos em que um qualquer dos x_i é igual a 0 são nulos, pois os χ_{α_i} são caracteres não principais; podemos excluí-los, e fazer nos restantes a substituição $x_i = x_1 . u_i$ $(2 \leqslant i \leqslant r)$. A um sistema fixo de valores dos u_i, satisfazendo $1 + \sum_{i=2}^{r} u_i = 0$, correspondem na soma dada $q-1$ termos, obtidos dando a x_1 todos os valores distintos de 0, cuja soma é

$$\sum_{x_1 \neq 0} \chi_{\alpha_1}(x_1).\chi_{\alpha_2}(x_1 u_2)\dots\chi_{\alpha_r}(x_1 u_r) =$$

$$= \chi_{\alpha_2}(u_2)\dots\chi_{\alpha_r}(u_r) \sum_{x_1 \neq 0} \chi_{\alpha_1+\alpha_2+\dots+\alpha_r}(x_1)$$

e $-\sum_{x_1 \neq 0} \chi_{\alpha_1+\alpha_2+\dots+\alpha_r}(x_1) = 0$ se $\sum \alpha_i \not\equiv 0 \pmod 1$.

Suponhamos então agora $\alpha_1,\dots,\alpha_r$ satisfazendo $(q-1)\,\alpha_i \equiv 0$, $\alpha_i \not\equiv 0$, $\sum_{i=1}^{r} \alpha_i \equiv 0 \pmod 1$. Chamamos soma de Jacobi para o corpo k, relativa a $\alpha_1,\dots,\alpha_r$, a soma

$$(10) \qquad j(\alpha) = \frac{1}{q-1} \sum_{\sum x_i = 0} \chi_{\alpha_1}(x_1)\dots\chi_{\alpha_r}(x_r)$$

Estas somas estão ligadas às somas de Gauss pela relação

$$(11) \qquad j(\alpha) = \frac{1}{q}\, g(\chi_{\alpha_1})\dots g(\chi_{\alpha_r})$$

De (8) e (11) segue

$$(12) \qquad j(\alpha)\,\overline{j}(\alpha) = q^{r-2}$$

De (9) (teorema de Davenport e Hasse), estendendo os caracteres de k a k_ν, e indicando por $j'(\alpha)$ a soma de Jacobi para k_ν relativa aos α_j, deduz-se

$$(13) \qquad j'(\alpha) = (-1)^{r(\nu-1)} \cdot j(\alpha)^\nu$$

Estas são as propriedades dos caracteres de um grupo abeliano finito, e das somas de Gauss e Jacobi de um corpo finito, que serão utilizadas neste trabalho.

As demonstrações das propriedades das somas de Gauss e Jacobi aqui enunciadas, e do teorema de Davenport e Hasse, encontram-se em A. Weil, Numbers of Solutions of Equations in Finite Fields, Bull. Am. Math. Soc., vol.55, n.5 (May,1949), pp.500 e seguintes.

2. Sobre o número de pontos racionais de uma variedade em um corpo k finito e suas extensões.

I. Seja k um corpo com q elementos e E o espaço vetorial de s dimensões sobre k. Seja k^* o grupo multiplicativo de k e E^* o produto direto de k^* s vezes por si próprio, considerado como parte de E.

Seja A o sub-grupo multiplicativo de E^* definido pela equação

$$x_1^{a_1} \dots x_s^{a_s} = 1$$

onde os expoentes são inteiros e $a_1 + \dots + a_s = a \neq 0$ (o que significa que A não é um "cone"). Supomos ainda $a_i < q-1$.

Se M indicar o número de elementos de A, temos

$$M = \frac{1}{q-1} \sum_{\chi, x} \chi(x_1^{a_1} \dots x_s^{a_s})$$

onde χ percorre o dual $\hat{k}^*$ de k^*, e os x_i percorrem k^*.

Seja ω um gerador de k^*, que fixamos de uma vez por todas, e α um número satisfazendo $(q-1)\alpha \equiv 0 \pmod 1$; então conforme a convenção χ_α indica o caracter de k^* tal que $\chi_\alpha(\omega) = e^{2\pi i \alpha}$ e podemos escrever

$$M = \frac{1}{q-1} \sum_{\alpha, x} \chi_\alpha(x_1^{a_1} \dots x_s^{a_s})$$

$$(0 \leqslant \alpha < 1, (q-1)\alpha \equiv 0 \pmod 1, x_i \in k^*)$$

Consideremos agora o sub-grupo aditivo B de E definido por

$$x_1 = \xi_1 t \dots x_s = \xi_s t$$

$\xi_1, \dots, \xi_s$ fixos em k, não nulos, t percorrendo k (isto é, B é uma reta de E).

O número de pontos comuns a A e a B será dado por

$$N = \frac{1}{q-1} \sum_{\alpha, t} \chi_\alpha(\xi_1^{a_1} \dots \xi_s^{a_s}) \chi_\alpha(t^{a_1 + \dots + a_s})$$

$$(0 \leqslant \alpha < 1, (q-1)\alpha \equiv 0 \pmod 1, t \in k^*)$$

e, por (5), segue

$$(14) \qquad N = \sum_{\alpha} \chi_{\alpha}(\xi_1^{a_1} \ldots \xi_s^{a_s})$$

$$(0 \leqslant \alpha < 1, (q-1)\alpha \equiv a\alpha \equiv 0 \pmod 1)$$

Consideremos o problema análogo para as extensões de k : seja k_ν a extensão de grau ν de k , E_ν o espaço vetorial de s dimensões sobre k_r ; k_r^* seja o grupo multiplicativo de k_r , E_r^* o produto direto de k_r^* s vezes por si proprio, considerado como parte de E_ν . Em E_ν^* consideremos o sub-grupo multiplicativo A_ν definido por

$$x_1^{a_1} \ldots x_s^{a_s} = 1$$

Então, sendo M_ν o número de elementos de A_ν , temos

$$M = \frac{1}{q^\nu - 1} \sum_{\chi', x} \chi'(x_1^{a_1} \ldots x_s^{a_s})$$

χ' percorrendo $\widetilde{k}_\nu^*$ e $(x_1, \ldots, x_s)$ percorrendo E_ν^* .

Tomemos em k_ν^* , um gerador ω' tal que $N(\omega') = \omega$; indiquemos por $\chi_\alpha^{(\nu)}$ os caracteres de k_ν^* ; então se $(q-1)\alpha \equiv 0 \pmod 1$, $\chi_\alpha^{(\nu)}(x) = \chi_\alpha[N(x)]$ para todo $x \in k_\nu^*$.

Seja B_ν o sub-grupo aditivo de E_ν definido por

$$x_1 = \xi_1 t \ \ldots \ x_s = \xi_s t \qquad t \text{ percorrendo } k_\nu$$

O número de pontos comuns a A_ν e B_ν será dado por

$$N_\nu = \sum_{\alpha} \chi_\alpha^{(\nu)}(\xi_1^{a_1} \ldots \xi_s^{a_s}) \qquad (0 \leqslant \alpha < 1,\ a\alpha \equiv (q^\nu - 1)\alpha \equiv 0 \pmod 1)$$

que podemos escrever

$$(15) \qquad N_\nu = 1 + \sum_{\alpha} \chi_\alpha^{(\nu)}(\xi_1^{a_1} \ldots \xi_s^{a_s}) \qquad (0 < \alpha < 1, a\alpha \equiv (q^\nu - 1)\alpha \equiv 0 \pmod 1)$$

Formemos a série de potências geradora para N_ν , isto é, a série formal $\sum_\nu N_\nu Z^{\nu-1}$; vamos demonstrar que esta série é o desenvolvimento de uma função racional de Z.

Com efeito, seja α um número satisfazendo $0 < \alpha < 1$, $a\alpha \equiv 0 \pmod 1$;

designemos por $\mu(\alpha)$ o menor inteiro tal que $(q^{\mu}-1)\alpha \equiv 0 \pmod 1$. Então se $(q^{\nu}-1)\alpha \equiv 0 \pmod 1$, ν é um múltiplo de $\mu(\alpha)$, isto é, esse α só comparece em N_ν se $\nu = \lambda\mu(\alpha)$ com λ inteiro.

Por outro lado, $\xi_1^{a_1} \ldots \xi_s^{a_s} = \xi \in k$, logo a norma $N'(\xi)$ de ξ tomada em $k_{\lambda\mu}$ relativamente a k é igual a $N(\xi)^{\lambda}$, sendo $N(\xi)$ a norma de ξ tomada em k_μ relativamente a k, e portanto

$$\sum_{\lambda=1}^{\infty} \chi_\alpha^{(\lambda\mu(\alpha))}(\xi) Z^{\lambda\mu(\alpha)-1} = \frac{\chi_\alpha^{(\mu(\alpha))}(\xi) Z^{\mu(\alpha)-1}}{1 - \chi_\alpha^{(\mu(\alpha))}(\xi) Z^{\mu(\alpha)}}$$

e temos

$$\sum_{\nu=1}^{\infty} N_\nu Z^{\nu-1} = \frac{1}{1-Z} + \sum_{\alpha} \frac{\chi_\alpha^{(\mu(\alpha))}(\xi) Z^{\mu(\alpha)-1}}{1 - \chi_\alpha^{(\mu(\alpha))}(\xi) Z^{\mu(\alpha)}}$$

$$(0 < \alpha < 1, a\alpha \equiv 0 \pmod 1)$$

ou ainda

$$\sum_{\nu=1}^{\infty} N_\nu Z^{\nu-1} = -\frac{d}{dZ}\log(1-Z) - \sum_{\alpha} \frac{1}{\mu(\alpha)} \frac{d}{dZ} \log\left(1 - \chi_\alpha^{(\mu(\alpha))}(\xi) Z^{\mu(\alpha)}\right)$$

$$(0 < \alpha < 1, a\alpha \equiv 0 \pmod 1)$$

Consideremos novamente o mesmo sub-grupo multiplicativo A de E^* e seja agora B o sub-grupo aditivo de E definido por

$$b_1 x_1 + \ldots + b_s x_s = 0$$

isto é, um hiperplano de E . Suponhamos os b_i não todos nulos. Seja ainda N o número de pontos comuns a A e a B, temos

$$N = \frac{1}{q-1} \sum_{\alpha, x} \chi_\alpha(x_1^{a_1} \ldots x_s^{a_s})$$

sendo a soma estendida aos α que satisfazem $0 \leqslant \alpha < 1$, $(q-1)\alpha \equiv 0 \pmod 1$ e $(x_1, \ldots, x_s)$ percorrendo B^*, intersecção de B com E^*.

Seja m o número de elementos de B^*. Então

$$(16) \qquad N = \frac{m}{q-1} + \frac{1}{q-1} \sum_{\alpha, x} \chi_\alpha(x_1^{a_1} \dots x_s^{a_s})$$

$$(0 < \alpha < 1,\ (q-1)\alpha \equiv 0 \pmod 1) \quad (x_1, \dots, x_s) \in B^*$$

Suponhamos que um dos b_i, por exemplo b_1, seja nulo. Então podemos escrever

$$N = \frac{m}{q-1} + \frac{1}{q-1} \sum_{\lambda=2}^{s} \sum_{b_i x_i = 0} \chi_\alpha(x_2^{a_2} \dots x_s^{a_s}) \sum_{x_1 \neq 0} \chi_\alpha(x_1)^{a_1}$$

$$(0 < \alpha < 1,\ (q-1)\alpha \equiv 0 \pmod 1))$$

ou seja, por (5)

$$N = \frac{m}{q-1} + \sum_{\lambda=2}^{s} \sum_{b_i x_i = 0} \chi_\alpha(x_2^{a_2} \dots x_s^{a_s})$$

$$(0 < \alpha < 1,\ (q-1)\alpha \equiv a_1\alpha \equiv 0 \pmod 1))$$

e nesta soma a variavel correspondente ao coeficiente nulo não comparece.

Suponhamos pois todos os b_i não nulos; caso contrário, o problema se resolve analogamente, usando número menor de variáveis. Façamos em (16) a substituição de x_i por x_i/b_i. Resulta

$$(17) \qquad N = \frac{m}{q-1} + \frac{1}{q-1} \sum_{\alpha} \overline{\chi}_\alpha(b_1^{a_1} \dots b_s^{a_s}) \sum_{\sum x_i = 0} \chi_\alpha(x_1)^{a_1} \dots \chi_\alpha(x_s)^{a_s}$$

$$(0 < \alpha < 1,\ (q-1)\alpha \equiv 0 \pmod 1))$$

Ponhamos $\alpha_1 = a_1\alpha \dots \alpha_s = a_s\alpha$. Então, se $\sum \alpha_i = a\alpha \equiv 0 \pmod 1$, a última soma em (17) dá q-1 vezes a soma de Jacobi relativa a esses α_i, a qual designaremos ainda com $j(\alpha)$; caso contrário, esta soma é igual a 0. Portanto

$$(18) \qquad N = \frac{m}{q-1} + \sum_{\alpha} \overline{\chi}_\alpha(b_1^{a_1} \dots b_s^{a_s})\, j(\alpha)$$

$$(0 < \alpha < 1,\ a\alpha \equiv (q-1)\alpha \equiv 0 \pmod 1)$$

Passemos agora às extensões k_ν de k, como fizemos acima. Seja N_ν o número de pontos comuns a A_ν, sub-grupo multiplicativo de E_ν^* definido por

$$x_1^{a_1} \dots x_s^{a_s} = 1 \qquad (x_i \in k_\nu^*)$$

e B_ν o hiperplano de E_ν definido por

$$b_1 x_1 + \dots + b_s x_s = 0 \qquad (x_i \in k_\nu)$$

e seja m_ν o número de pontos de B_ν^*, intersecção de B_ν com E_ν^*. Temos

$$N_\nu = \frac{m}{q^\nu - 1} + \sum_\alpha \overline{\chi}_\alpha^{(\nu)}(b_1^{a_1} \dots b_s^{a_s})\, j^{(\nu)}(\alpha)$$

$$(0 < \alpha < 1,\ (q^\nu - 1)\alpha \equiv a\alpha \equiv 0 \pmod 1)$$

onde $\overline{\chi}_\alpha^{(\nu)}$ e $j^{(\nu)}(\alpha)$ indicam respectivamente os caracteres e as somas de Jacobi em k_ν.

É facil ver que $m_\nu = \frac{q^\nu - 1}{\tilde{q}^\nu}\left[(q^\nu - 1)^{s-1} + (-1)^s\right]$. Ponhamos para abreviar $b_1^{a_1} \dots b_s^{a_s} = b$. Temos então

$$N = q^{\nu(s-2)} - \binom{s-1}{1} q^{\nu(s-3)} + \dots + \binom{s-1}{s-2}(-1)^s + \sum_\alpha \overline{\chi}_\alpha^{(\nu)}(b)\, j^{(\nu)}(\alpha)$$

$$(0 < \alpha < 1,\ (q^\nu - 1)\alpha \equiv a\alpha \equiv 0 \pmod 1)$$

Formemos a série de potências $\sum N_\nu Z^{\nu-1}$ geradora, e vamos demonstrar que é o desenvolvimento de uma função racional de Z. Seja α um número satisfazendo $a\alpha \equiv 0 \pmod 1$, $0 < \alpha < 1$, e seja $\mu(\alpha)$ o menor inteiro tal que $(q^\mu - 1)\alpha \equiv 0 \pmod 1$. Então se $(q^\nu - 1)\alpha \equiv 0 \pmod 1$, ν é múltiplo de $\mu(\alpha)$, $\nu = \lambda\mu(\alpha)$, λ inteiro. Como vimos acima

$$\chi_\alpha^{(\lambda\mu)}(b) = \chi_\alpha^{(\mu)}(b)^\lambda$$

Por outro lado, por (13) temos

$$j^{(\lambda\mu)}(\alpha) = (-1)^{(\lambda-1)s}\, j^{(\mu)}(\alpha)^\lambda$$

e para esse α fixo obtemos

$$\sum_{\lambda=1}^{\infty} (-1)^{(\lambda-1)s} \chi_\alpha^{(\mu)}(b)^\lambda\, j^{(\mu)}(\alpha)^\lambda Z^{\mu\lambda - 1} =$$

$$= (-1)^{s-1} \frac{1}{\mu(\alpha)} \frac{d}{dZ} \log\left(1 - (-1)^s \chi^{(\mu(\alpha))}(b)\, j^{(\mu(\alpha))}(\alpha) Z^{\mu(\alpha)}\right)$$

e finalmente

$$\sum_{\nu} N_\nu Z^{\nu-1} = -\sum_{h=0}^{s-2} (-1)^h \binom{s-1}{h} \frac{d}{dZ}\log(1-q^{s-2-h}Z) +$$

$$+ (-1)^{s-1} \sum_{\alpha} \frac{1}{\mu(\alpha)} \frac{d}{dZ}\log(1-(-1)^s \chi_\alpha^{(\mu(\alpha))}(b)\, j^{(\mu(\alpha))}(\alpha) Z^{\mu(\alpha)})$$

$$(0 < \alpha < 1,\ a\alpha \equiv 0 \pmod 1)$$

II. Dada a equação de uma hipersuperfície do espaço de s dimensões sobre k, corpo com q elementos

$$(19) \qquad \sum_{i=1}^{r} a_i x_1^{m_{1i}} \dots x_s^{m_{si}} = 0 \qquad a_i \in k^* \quad (i = 1, \dots, r)$$

seja N_ν o número de soluções dessa equação, isto é, o número de pontos racionais na hipersuperfície sobre o corpo k_ν, extensão de grau ν de k. Propomo-nos estudar a série geradora $\sum_\nu N_\nu Z^{\nu-1}$.

Para isto, tomemos ν bastante grande para que $m_{ij} < q^\nu - 1$ $(i=1,\dots,r,$ $j=1,\dots,s)$ e consideremos a equação

$$(20) \qquad \sum_{i=1}^{r} a_i y_i = 0$$

que representa um hiperplano de espaço vetorial de r dimensões sobre k_ν.

Consideremos tambem o grupo multiplicativo B_ν definido pelas equações paramétricas

$$(21) \qquad y_i = x_1^{m_{1i}} \dots x_s^{m_{si}} \qquad (i = 1, \dots, r)$$

onde os x_j $(j = 1, \dots, s)$ descrevem independentemente k_ν^*. Então $y_i \in k_\nu^*$ e B_ν é sub-grupo de E_ν^*, produto direto de k_ν^* r vezes por si próprio.

Escrevamos as equações (3) sob a forma

$$(22) \qquad F_i \equiv y_i^{-1} x_1^{m_{1i}} \dots x_s^{m_{si}} = 1$$

Fixemos os y_i de modo a satisfazer (20). O número M_ν de soluções em x das equações (22) será

$$M_\nu = \frac{1}{(q^\nu - 1)^r} \sum_{\chi, x} \chi_1(F_1) \dots \chi_r(F_r)$$

onde os χ_i $(i = 1, \dots, r)$ percorrem independentemente $\tilde{k}_\nu^*$ e os x_j percorrem independentemente k_ν^* $(j = 1, \dots, s)$, ou seja

$$M_\nu = \frac{1}{(q^\nu-1)^r} \sum_{(\alpha_i),(x_j)} \chi_{\alpha_1}(F_1)\ldots\chi_{\alpha_r}(F_r)$$
$$(0\leq\alpha_i<1,\ (q^\nu-1)\alpha_i\equiv 0 \pmod 1)\ (i=1,\ldots,r)$$
$$x_j\in k_\nu^*\ (j=1,\ldots,s)$$

Fixando os α_i e decompondo a soma relativa aos x no produto de somas para cada x_j, vemos que o fator em x_j é

$$\sum_{x_j\in k_\nu^*} \chi_{\alpha_1}(x_j^{m_{j1}})\ldots\chi_{\alpha_r}(x_j^{m_{jr}}) \qquad (j=1,\ldots,s)$$

que dá $q^\nu-1$ se $\sum_{i=1}^r m_{ji}\alpha_i\equiv 0 \pmod 1$, e 0 caso contrário. Portanto

$$(23)\qquad M_\nu = \frac{1}{(q^\nu-1)^{r-s}} \sum_{\alpha} \overline{\chi}_{\alpha_1}(y_1)\ldots\overline{\chi}_{\alpha_r}(y_r)$$
$$(0\leq\alpha_i<1,\ (q^\nu-1)\alpha_i\equiv 0 \pmod 1)\ (i=1,\ldots,r)$$
$$\sum_i m_{ji}\alpha_i\equiv 0 \pmod 1\ (j=i,\ldots,s)$$

Seja $\overline{N}_\nu$ o número de pontos comuns ao hiperplano A_ν definido por (20) e a B_ν. Temos então

$$(24)\qquad \overline{N}_\nu = \frac{1}{(q^\nu-1)^{r-s}} \sum_{(\alpha_i)}\sum_{(y_i)} \overline{\chi}_{\alpha_1}(y_i)\ldots\overline{\chi}_{\alpha_r}(y_r)$$

somando para $y_i\in k_\nu^*$ satisfazendo (20) e para os α_i satisfazendo às mesmas condições que em (23).

Vamos agora considerar somas relativas a $\chi_{\alpha_1}(y)\ldots\chi_{\alpha_r}(y_r)$, sob diferentes condições que passamos a enunciar.

Condições γ
$$\begin{cases} 0\leq\alpha_i<1,\ y_i\in k_\nu\ (i=1,\ldots,r) \\ \sum_i a_i y_i = 0,\ \sum_\lambda m_{ji}\alpha_i\equiv 0 \pmod 1\ (j=1,\ldots,s) \\ (q^\nu-1)\alpha_i\equiv 0 \pmod 1\ (i=1,\ldots,r) \end{cases}$$

Condições γ_0 { condições γ , mais as condições $y_i=0$ e $\alpha_i\equiv 0 \pmod 1$

Condições γ_{ij} $(i \neq j)$ $\left\{\right.$condições γ , mais $y_i = y_j = 0$, $\alpha_i \equiv \alpha_j \equiv 0 \pmod 1$

condições γ_{ijk}, γ_{ijkl}, ..., com índices todos distintos correspondendo aos dos y que são nulos e dos α que são inteiros.

Em correspondência, temos as somas

$$A = \sum_{(y)(\alpha)} \overline{\chi}_{\alpha}(y_1) \ldots \overline{\chi}_{\alpha_n}(y_r) \text{ sob as condições } \gamma$$

$$A_i = \sum_{(y)(\alpha)} \chi_{\alpha_1}(y_1) \ldots \overline{\chi}_{\alpha_n}(y_r) \text{ sob as condições } \gamma_i$$

$$A_{ij} = \sum_{(y)(\alpha)} \chi_{\alpha_1}(y_1) \ldots \overline{\chi}_{\alpha_n}(y_r) \text{ sob as condições } \gamma_{ij}$$

e A_{ijk}, etc. definidos com as condições $\gamma_{ijk}, \ldots$

Consideremos outro grupo de condições

Condições γ' $\left\{\begin{array}{l} 0 \leqslant \alpha_i < 1, \; y_i \in k_\nu^* \\ \sum_i a_i y_i = 0 \;, \quad \sum_i m_{ji} \alpha_i \equiv 0 \pmod 1 \quad (j = 1, \ldots, s) \\ (q^\nu - 1)\alpha_i \equiv 0 \pmod 1 \end{array}\right.$

Condições γ'_i $\left\{\begin{array}{l} \text{para os } \alpha : \text{ as condições } \gamma \text{ e mais } \alpha_i \equiv 0 \pmod 1 \\ \text{para os } y : y_i = 0 \;, \; y_j \in k_\nu^* \;\; (j \neq i) \;, \; \sum_j a_j y_j = 0 \end{array}\right.$

Condições γ'_{ij} $(i \neq j)$ $\left\{\begin{array}{l} \text{para os } \alpha : \text{ as condições } \gamma \text{ e mais } \alpha_i \equiv \alpha_j \equiv 0 \pmod 1 \\ \text{para os } y : y_i = y_j = 0, \; y_k \in k_\nu^* \;\; (k \neq i, k \neq j) \\ \qquad\qquad \sum a_k y_k = 0 \end{array}\right.$

e assim condições γ'_{ijk}, etc. Ponhamos ainda

$$A' = \sum_{(y)(\alpha)} \chi_{\alpha_1}(y_1) \ldots \overline{\chi}_{\alpha_r}(y_r) \text{ sob as condições } \gamma'$$

$$A'_i = \sum_{(y),(\alpha)} \bar{\chi}_{\alpha_1}(y_1)\ldots\bar{\chi}_{\alpha_r}(y_r) \text{ sob as condições } \gamma'_i$$

$$A'_{ij} = \sum_{(y),(\alpha)} \bar{\chi}_{\alpha_1}(y_1)\ldots\bar{\chi}_{\alpha_r}(y_r) \text{ sob as condições } \gamma'_{ij}$$

etc..

Então temos

$$\bar{N}_\nu = \frac{1}{(q^\nu-1)^{r-s}} A' \tag{25}$$

$$A = A' + \sum_i A'_i + \sum_{(ij)} A'_{ij} + \sum_{(ijk)} A'_{ijk} + \ldots \tag{26}$$

$$A_1 = A'_1 + \sum_{\substack{i \\ i\neq 1}} A'_{1i} + \sum_{\substack{(ij) \\ i\neq 1 \\ j\neq 1}} A'_{1ij} + \ldots$$

onde nas somas tomamos os índices um a um, em seguida pares de índices distintos,etc.. As equações do sistema (26) contêm 2^r termos A', e existem 2^r equações deste tipo, em que os primeiros membros são os A. Resolvendo para A' obtem-se

$$A' = A - \sum_i A_i + \sum_{(ij)} A_{ij} - \sum_{(ijk)} A_{ijk} + \ldots$$

e portanto

$$\bar{N} = \frac{1}{(q^\nu-1)^{r-s}} \left[A - \sum_i A_i + \sum_{(ij)} A_{ij} - \ldots \right]$$

Observemos que $A_{12\ldots r} = 1$, pois se reduz a $\chi_o(0)\ldots\chi_o(0) = 1$.

Tambem $A'_{12\ldots r} = 1$. Por outro lado, os A com r-1 índices são ainda iguais a 1, pois se anulamos r-1 dos y, o restante tambem é nulo, devido à condição $\sum a_i y_i = 0$, e então na soma há um só termo não nulo, que é o que corresponde a todos os α nulos, $\chi_o(0)\ldots\chi_o(0) = 1$. Entretanto os A' com r-1 índices são nulos, pois não podemos ter

r-1 dos y nulos, o r-ésimo em k_y^*, e $\sum a_i y_i = 0$.

Consideremos a soma A

$$A = \sum_{(y),(\alpha)} \overline{\chi}_{\alpha_1}(y_1) \ldots \overline{\chi}_{\alpha_r}(y_r) \quad \text{sob as condições } \gamma$$

Se $\alpha_1 = \alpha_2 = \ldots = \alpha_r = 0$, somando em y_i obtemos o número de pontos do hiperplano $\sum_{i=1}^{r} a_i y_i = 0$, que é $q^{\nu(r-1)}$. Vamos demonstrar que os termos em que alguns dos α são nulos e os restantes diferentes de zero têm soma nula.(*)

Com efeito, consideremos os termos com $\alpha_1 = \ldots = \alpha_t = 0$ $(t < r)$ e $\alpha_{t+1}, \ldots, \alpha_r$ não nulos, fixados. Se dermos valores arbitrários a $y_{t+1}, \ldots, y_r$, e somarmos em relação a $y_1, \ldots, y_t$, como $\chi_{\alpha_i}(y_i) = 1$ $(i = 1, \ldots, t)$ qualquer que seja y_i, obtemos o número de pontos do hiperplano cujas coordenadas $y_{t+1}, \ldots, y_r$ têm os valores fixados. Este número é $q^{\nu(r-1)}$. Portanto a soma dos termos correspondentes a esses α dados é

$$q^{\nu(t-1)} \prod_{j=t+1}^{r} \sum_{y_j} \overline{\chi}_{\alpha_j}(y_j)$$

Em cada uma das somas $\sum_{y_j} \chi_{\alpha_j}(y_j)$ y_j percorre k_y, portanto, como χ_{α_j} não é principal $(j = t+1, \ldots, r)$, estas somas são todas nulas.

Restam pois apenas os termos em que $\alpha_1 \ldots \alpha_r \neq 0$, e mais o termo $q^{\nu(r-1)}$ que corresponde a $\alpha_1 = \ldots = \alpha_r = 0$.

Consideremos agora as seguintes condições

(*) Cf. A. Weil, Solutions of equations in finite fields, Bull. Am. Math. Soc., vol.55, n.5 (May,1949), p.499.

Condições γ''
$$\begin{cases} 0<\alpha_i<1\ ,\ y_i \in k_\nu \quad (i=1,\dots,r) \\ \sum_i a_i y_i = 0\ ,\quad \sum m_{ji}\alpha_i \equiv 0 \pmod 1 \quad (j=1,\dots,s) \\ (q^\nu-1)\alpha_i \equiv 0 \pmod 1 \quad (i=1,\dots,r) \end{cases}$$

Condições γ''_λ
$$\begin{cases} \alpha_i \equiv 0 \pmod 1\ ,\ 0<\alpha_j<1 \quad (j\neq i);\ y_i=0,\ y_j \in k_\nu^* \quad (j\neq i) \\ \sum_j a_j y_j = 0\ ,\quad \sum m_{kj}\alpha_j \equiv 0 \pmod 1 \quad (k=1,\dots,s) \\ (q^\nu-1)\alpha_j \equiv 0 \pmod 1 \end{cases}$$

condições γ''_{ij}, etc..

Definimos em seguida as somas

$$A'' = \sum_{(y)(\alpha)} \overline{\chi}_{\alpha_1}(y_1)\dots\overline{\chi}_{\alpha_n}(y_r) \quad \text{sob as condições } \gamma''$$

$$A''_i = \sum_{(y)(\alpha)} \overline{\chi}_{\alpha_1}(y_1)\dots\overline{\chi}_{\alpha_n}(y_r) \quad \text{sob as condições } \gamma''_\lambda$$

etc..

O raciocínio precedente mostra que

$$A = q^{\nu(r-1)} + A''$$

pois nas somas com $\alpha_1\dots\alpha_r \neq 0$ o resultado é o mesmo quer y_i percorra k_ν^*, quer percorra k_ν, visto que $\chi(0)=0$ para todo χ não principal

Repetindo o raciocínio para os A_i, etc. obtemos

$$A_i = q^{\nu(r-2)} + A''_i\ ;\quad A_{ij} = q^{\nu(r-3)} + A_{ij}\ ;\ \dots$$

e substituindo em $\overline{N}_\nu$, vem

$$\overline{N}_\nu = \frac{1}{(q^\nu-1)^{r-s}}\left[q^{\nu(r-1)} - rq^{\nu(r-2)} + \binom{r}{2} q^{\nu(r-3)} - \dots\right] +$$

$$+ \frac{1}{(q^\nu-1)^{r-s}}\left[A'' - \sum_i A''_i + \sum_{(ij)} A''_{ij} - \dots\right]$$

onde os termos em A'' com r e r-1 índices são tomados iguais a 0.

Vamos agora introduzir em A'' as somas de Gauss. Para isto, consideremos um caracter aditivo fixo ψ, não principal, de k_ν, e a soma

$$g(\chi) = \sum_x \chi(x)\psi(x)$$

Se χ não é principal, $\chi(0) = 0$ e podemos fazer x percorrer k_ν^*. Ponhamos tx em lugar de x, com t arbitrário, não nulo. Resulta

$$g(\chi) = \chi(t) \sum_x \chi(x)\psi(tx)$$

Permutando t e x

$$g(\chi) = \chi(x) \sum_t \chi(t)\psi(tx)$$

Lembrando que $g(\chi)\bar{g}(\chi) = q^\nu$, temos

$$g(\chi)\bar{\chi}(x) \sum_t \bar{\chi}(t)\bar{\psi}(tx) = q^\nu$$

donde

$$\chi(x) = \frac{g(\chi)}{q^\nu} \sum_t \bar{\chi}(t)\bar{\psi}(tx)$$

(para $x = 0$, $\chi(x) = 0$ e $\sum_t \bar{\chi}(t)\bar{\psi}(0) = \sum_t \bar{\chi}(t) = 0$ e portanto a igualdade ainda vale).

Como os caracteres que comparecem em A'' não são principais podemos fazer esta transformação e resulta

$$A'' = \frac{1}{q^{\nu r}} \sum \bar{g}(\chi_{\alpha_1}) \ldots \bar{g}(\chi_{\alpha_r}) \sum_{t_i} \chi_{\alpha_1}(t_1) \ldots \chi_{\alpha_r}(t_r) \cdot$$

$$\cdot \sum_{y_i} \psi(t_1 y_1 + \ldots + t_r y_r)$$

$(0 < \alpha_i < 1,\ (q^\nu - 1)\alpha_i \equiv 0 \pmod 1,\ y_i \in k_\nu,$
$t_i \in k_\nu^*\ (i = 1, \ldots, r),\ \sum a_i y_i = 0$
$\sum m_{ji}\alpha_i \equiv 0 \pmod 1\ (j = 1, \ldots, s)$

Consideremos a soma

$$\sum_{y_i} \psi(t_1 y_1 + \ldots + t_r y_r)$$

$\varphi(t_1y_1 + \ldots + t_ry_r)$ é um caracter do grupo aditivo A_ν definido no espaço vetorial de r dimensões pela equação $\sum a_iy_i = 0$. A soma dos valores deste caracter para todos os elementos do grupo é 0 se o caracter não for principal. Como φ não é caracter principal de k_ν, para que a soma não seja nula é necessário e suficiente que $\sum t_iy_i = 0$ para todo sistema (y_i) tal que $\sum a_iy_i = 0$, isto é, que $t_i = ta_i$, onde $t \in k_\nu^*$. Se isto se der, a soma $\sum_{y_i} \varphi(\sum_i t_iy_i)$ dá o número de pontos de A_ν, que é $q^{\nu(r-1)}$ (ver A.Weil, Solutions of equations in finite fields, p.501).

Portanto

$$A'' = \frac{1}{q^\nu} \sum_{\alpha_i} \bar{g}(\chi_{\alpha_1}) \ldots \bar{g}(\chi_{\alpha_r}) \cdot \cdot \sum_t \chi_{\alpha_1}(a_1) \ldots \chi_{\alpha_r}(a_r) \chi_{\alpha_1 + \ldots + \alpha_r}(t)$$

Por outro lado

$$\sum_t \chi_{\alpha_1 + \ldots + \alpha_r}(t) = \begin{cases} q^\nu - 1 \text{ se } \sum \alpha_i \equiv 0 \pmod 1 \\ 0 \text{ caso constrário} \end{cases}$$

e temos

$$A'' = \frac{q^\nu - 1}{q^\nu} \sum_{\alpha_i} \chi_{\alpha_1}(a_1) \ldots \chi_{\alpha_r}(a_r) \bar{g}(\chi_{\alpha_1}) \ldots \bar{g}(\chi_{\alpha_r})$$

$$(0 < \alpha_i < 1,\ (q^\nu - 1)\alpha_i \equiv 0 \pmod 1 \ (i = 1, \ldots, r)$$

$$\sum m_{ji}\alpha_i \equiv 0 \pmod 1 \ (j = 1, \ldots, s)$$

$$\sum \alpha_i \equiv 0 \pmod 1)$$

Temos fórmulas análogas para A_i'', etc., sempre com o fator $\frac{q^\nu - 1}{q^\nu}$; o mesmo raciocínio vale enquanto houver menos de r-1 índices.

Vamos definir $g(\chi)$ para o caracter principal. φ sendo um caracter aditivo não principal

$$g(\chi_0) = \sum_{x \in k^*} \psi(x) = -1$$

Seja então

$$B = \sum_{(\alpha_i)} \chi_{\alpha_1}(a_1) \ldots \chi_{\alpha_r}(a_r) \bar{g}(\chi_{\alpha_1}) \ldots \bar{g}(\chi_{\alpha_r})$$

sob as condições

$$0 \leqslant \alpha_i < 1, \quad (q^\nu - 1)\alpha_i \equiv \sum \alpha_i \equiv \sum_i m_{ji}\alpha_i \equiv 0 \pmod 1$$

Fazendo a soma para todos os sistemas (α_i) em que todos os α_i são diferentes de zero obtem-se $A'' \frac{q^\nu}{q^\nu - 1}$; a soma dos termos em que $\alpha_i = 0$ e $\alpha_j \neq 0$ $(j \neq i)$ dá $-A_i'' \frac{q^\nu}{q^\nu - 1}$, e assim por diante. Enfim, se r-2 dos α são nulos os outros dois tambem são. Temos

$$\bar{N}_\nu = q^{-\nu} \left[(q^\nu - 1)^s - (-1)^r (q^\nu - 1)^{s-r} \right] +$$

$$+ \frac{(q^\nu - 1)^{s-r+1}}{q^\nu} \sum_{(\alpha_i)} \chi_{\alpha_1}(a_1) \ldots \chi_{\alpha_r}(a_r) \bar{g}(\chi_{\alpha_1}) \ldots \bar{g}(\chi_{\alpha_r})$$

sendo a soma estendida aos sistemas (α_i) de r números racionais módulo 1, não todos nulos, satisfazendo $(q^\nu - 1)\alpha_i \equiv 0 \pmod 1$ e mais $\sum \alpha_i \equiv 0$, $\sum_i m_{ji}\alpha_i \equiv 0 \pmod 1$ $(j = 1, \ldots, s)$

Podemos ainda dar outra forma à expressão de $\bar{N}_\nu$. Se $\alpha_1, \ldots, \alpha_r$ são diferentes de zero, temos por (11)

$$\frac{1}{q^\nu} g(\chi_{\alpha_1}) \ldots g(\chi_{\alpha_r}) = j(\alpha_1, \ldots, \alpha_r)$$

Se um dos α , por exemplo, α_1, é nulo, temos

$$\frac{1}{q^\nu} g(\chi_{\alpha_1}) \ldots g(\chi_{\alpha_r}) = -\frac{1}{q^\nu} g(\chi_{\alpha_2}) \ldots g(\chi_{\alpha_r})$$

Vamos definir $j(\alpha)$ ainda para o caso em que um dos α é igual a zero. Seja por exemplo $\alpha_1 = 0$; então pomos

$$j(\alpha_1,\ldots,\alpha_r) = -\, j(\alpha_2,\ldots,\alpha_r)$$

Mais geralmente, se t dos α ($t<r$), por exemplo, $\alpha_1,\ldots,\alpha_t$ são nulos

$$j(\alpha_1,\ldots,\alpha_r) = (-1)^t j(\alpha_{t+1},\ldots,\alpha_r)$$

Então temos

$$(27)\qquad \overline{N}_\nu = q^{-\nu}\left[(q^\nu-1)^s - (-1)^r(q^\nu-1)^{s-r}\right] + (q^\nu-1)^{s-r+1}\sum_{(\alpha_i)}\chi_{\alpha_1}(a_1)\ldots\chi_{\alpha_r}(a_r)\,\overline{j}(\alpha)$$

sendo a somatória estendida aos sistemas (α_i) de números racionais módulo 1, não todos nulos, que satisfazem às condições

$$0\leq\alpha_i<1\ ,\ (q^\nu-1)\alpha_i \equiv \sum\alpha_i \equiv \sum_i m_{ji}\alpha_i \equiv 0 \pmod 1 \quad (j=1,\ldots,s)$$

Observemos que a convenção feita para $j(\alpha)$ quando alguns dos α (mas não todos) são nulos conserva a validade da fórmula (13), consequência do teorema de Davenport e Hasse.

Consideremos as condições $\sum\alpha_i \equiv \sum_i m_{ji}\alpha_i \equiv 0 \pmod 1$ $(j=1,\ldots,s)$. São s+1 condições, independentes de ν, para $\alpha_1,\ldots,\alpha_r$. Se $r\leq s+1$, sendo r a característica da matriz dos coeficientes dos primeiros membros das congruências, existe número <u>finito</u> de soluções. Para cada sistemas (α_i) que satisfaça a essas condições (os α_i não sendo todos nulos), consideremos o número $\mu(\alpha)$ definido com sendo o menor inteiro tal que $(q^\mu-1)\alpha_i \equiv 0 \pmod 1$ $(i=1,\ldots,r)$. Então se $(q^\nu-1)\alpha_i \equiv 0 \pmod 1$ $(i=1,\ldots,r)$, $\nu=\lambda\mu(\alpha)$ com λ inteiro. Consideremos então para esses α sòmente as extensões $k_{\lambda\mu(\alpha)}$ de k $(\lambda=1,2,\ldots)$.

Escolhendo o gerador $\omega^{(\nu)}$ de k_ν^* de modo que $N(\omega^{(\nu)})=\omega$ sendo $N(\omega^{(\nu)})$ tomada em k_ν relativamente a k, temos

$$\chi_{\alpha_i}^{(\lambda\mu)}(a_i) = \chi_{\alpha_i}^{(\mu)}(a_i)^\lambda \qquad \text{e} \qquad \overline{j}^{(\lambda\mu)}(\alpha) = (-1)^{r(\lambda-1)}\overline{j}^{(\mu)}(\alpha)^\lambda$$

associando aos caracteres e somas de Jacobi índices correspondentes ao grau do corpo em que são tomados sobre k.

Para esse sistema $\alpha_1, \ldots, \alpha_r$ fixado, vemos que a série $\sum_{\lambda=1}^{\infty} \chi_{\alpha_1}^{(\lambda\nu)}(a_1) \ldots \chi_{\alpha_r}^{(\lambda\nu)}(a_r)\, \overline{j}^{(\lambda\nu)}(\alpha)\, Z^{\lambda\nu-1}$ é uma série geométrica de razão $(-1)^r \chi_{\alpha_1}^{(\nu)}(a_1) \ldots \chi_{\alpha_r}^{(\nu)}(a_r)\, \overline{j}^{(\nu)}(\alpha)\, Z^{\nu}$.

Portanto se $r \leq s+1$, a série $\sum_{\nu} \overline{N}_\nu Z^{\nu-1}$ se decompõe na soma de um número finito de séries geométricas, donde se conclue que é o desenvolvimento de uma função racional de Z.

Voltemos ao problema inicial, que era estudar a série $\sum_{\nu} N_\nu Z^{\nu-1}$ em que N_ν é o número de pontos racionais da hipersuperfície de equação

$$\sum_{i=1}^{r} a_i x_1^{m_{1i}} \ldots x_s^{m_{si}} = 0$$

sobre k_ν. Vemos que $\overline{N}_\nu$ é o número dos pontos cujas coordenadas são todas diferentes de zero. Fazendo na equação dada $x_i = 0$ e aplicando o raciocínio precedente obtemos o número dos pontos em que $x_i = 0$ e $x_j \neq 0$ $(j \neq i)$, e assim por diante, anulando em seguida duas variáveis, depois três, etc.. Podemos pois escrever a série $\sum_{\nu} N_\nu Z^{\nu-1}$ como soma de séries do tipo estudado.

Se $s+1 < r$ existem infinitos sistemas de α_i possíveis, e o estudo da série torna-se muito complicado. Mas é interessante notar que nos dois casos extremos, $s = 1$ e $s = 2$, o resultado sobre a série $\sum_{\nu} N_\nu Z^{\nu-1}$ é conhecido por outros caminhos. Por exemplo seja $s = 1$, isto é, seja o caso de uma equação

$$P(x) = 0$$

em uma única variavel, com coeficientes em k. Decomponhamos $P(x)$ em fatores irredutíveis sobre k:

$$P(x) = \prod_{\rho=1}^{d} P_\rho(x)$$

e seja d_ρ o grau de $P_\rho(x)$; então

$$N_\nu = \sum_{\rho=1}^{d} N_\nu^{(\rho)}$$

onde $N_\nu^{(\rho)}$ é o número de soluções de $P_\nu(x) = 0$ sobre k_ν; tem-se

$$N_\nu^{(\rho)} = \begin{cases} d_\rho & \text{se } \nu \equiv 0 \pmod{d_\rho} \\ 0 & \text{se } \nu \not\equiv 0 \pmod{d_\rho} \end{cases}$$

e portanto

$$\sum_\nu N_\nu Z^\nu = \sum_{\rho=1}^{d} d_\rho \left(\sum_{\nu=1}^{\infty} Z^{d_\rho \nu} \right) = \sum_{\rho=1}^{d} \frac{d_\rho Z^{d_\rho}}{1 - Z^{d_\rho}}$$

O teorema é ainda verdadeiro para 2 variáveis (cf. A.Weil "Les Courbes Algébriques et les variétés qui s'en déduisent" - pp.72 e seguintes). Porem parece muito dificil demonstrar o teorema para $s = 1$ ou $s = 2$ usando a expressão obtida para $\overline{N}_\nu$.

Entretanto no caso $s+1 < r$ a expressão (27) permite dar uma limitação interessante para $\overline{N}_\nu$, para ν fixo.

Com efeito, pela fórmula (12) e pela convenção feita sobre $j(\alpha)$ no caso em que alguns dos α são nulos, temos

$$\left| j(\alpha) \right| \leq q^{\nu(r-2)/2}$$

Por outro lado, o número de sistemas (α_i) que satisfazem $\sum \alpha_i \equiv \sum_i m_{ji} \alpha_i \equiv 0$ $(j = 1, \ldots, s)$ e $(q^\nu - 1)\alpha_i \equiv 0 \pmod 1$ $(i = 1, \ldots, r)$ com $0 \leq \alpha_i < 1$ é da ordem de $(q^\nu - 1)^{(r-s-1)}$. Vemos pois que para ν bastante grande, o último termo da equação (27) é limitado superiormente em módulo por $q^{\nu r/2}$.