Trasformata di Fourier discreta

Sia $v(x)$ polinomio in $GF(q)$, $v(x)=v_0+v_1x+v_2x^2+...v_{N-1}x^{N-1}$.
La trasformata di Fourier di $v(x)$ è definita dal polinomio:

$$V(x)=V_0+V_1x+V_2x^2+...+V_{N-1}x^{N-1}$$

dove i coefficienti V_i sono calcolati come segue:

$$V_j=\sum_{i=0}^{N-1}\alpha^{ij}v_i \quad .$$

Si definisce antitrasformata di Fourier la trasformazione da $V(x)$ a $v(x)$, con i coefficienti v_i calcolati come segue:

$$v_i=\frac{1}{N}\sum_{j=0}^{N-1}\alpha^{-ij}V_i$$

Si osserva che la definizione non ha senso per tutti gli α e gli N , ci sono delle limitazioni. In particolare, perchè sia valida, deve valere transitivamente ossia:

$$v_i=\frac{1}{N}\sum_{j=0}^{N-1}\alpha^{-ij}\sum_{k=0}^{N-1}\alpha^{kj}v_k$$

(nota che l'indice è stato cambiato di nome per non cambiare il significato della scrittura).
La scrittura può essere modificata come:

$$v_i=\frac{1}{N}\sum_{k=0}^{N-1}v_k\sum_{j=0}^{N-1}\alpha^{-ij}\alpha^{kj} \quad \text{quindi}$$

$$v_i=\frac{1}{N}\sum_{k=0}^{N-1}v_k\sum_{j=0}^{N-1}\alpha^{j(k-i)}$$

Definendo $A(k)=\sum_{j=0}^{N-1}\alpha^{j(k-i)}$ posso scrivere:

$$v_i=\frac{1}{N}\sum_{k=0}^{N-1}v_kA(k)$$

Perchè l'uguaglianza sia vera $A(k)$ deve valere 1 se $k=i$, in modo che la somma di N termini v_i si semplifichi con la frazione fuori dal segno di somma, e 0 se $k\neq i$.
Nel primo caso, $k=i$,

$$A(k)=\sum_{j=0}^{N-1}\alpha^{j0}=N$$

è sempre verificata. Nel secondo caso, $k\neq i$, questo non si può dire sempre:

$$A(k)=\sum_{j=0}^{N-1}\alpha^{j(k-i)}=?$$

Si può dimostrare che $A(k)=0$ quando $k\neq i$ se e α è di ordine N . Infatti, si può verificare facilmente che questa equazione è sempre vera:

$$(x^N-1)=(x-1)(1+x+x^2+...+x^{N-1})$$

ossia:

$$(x^N-1)=(x-1)\sum_{j=0}^{N-1}x^j$$

Sostituendo ad x α^r , dove $r=k-i$, si trova:

$$(\alpha^{rN}-1)=(\alpha^r-1)\sum_{j=0}^{N-1}\alpha^{jr}$$

Si nota che dal momento che vale l'ipotesi $k\neq i$ allora $r\neq 0$ e quindi $\alpha^r\neq 1$, quindi il primo termine (α^r-1) è sempre diverso da zero. Ciò detto, scrivere:

$A(k)=\sum_{j=0}^{N-1}\alpha^{jr}=0$ equivale a scrivere:

$\alpha^{rN}-1=0$ ossia

$\alpha^{rN}=1$

ma questo è vero se α ha ordine N, per cui tutte le potenze multiple di N danno come risultato 1.

Concludendo la definizione di trasformata di Fourier ha senso solo per α ed N tali che α ha ordine N.