J. Math. Kyoto Univ. (JMKYAZ)
13-1 (1973) 139-142

# A remark on Gaussian sums and algebraic groups

By

Takashi Ono

(Communicatel by Professor Nagata, July 25, 1972)

**1.** Let $f(X)$ be a non-constant polynomial in $\boldsymbol{Z}[X]$, $X=(X_1, \cdots, X_n)$. Denote by $f_p(X)$ the polynomial in $\boldsymbol{Z}_p[X]$ obtained from $f(X)$ by reducing the coefficients modulo $p$, where $\boldsymbol{Z}_p$ means the residue field. Let $\chi_p$ be a non-trivial character of the additive group of the field $\boldsymbol{Z}_p$, e.g. $\chi_p(a)=\exp(2\pi i p^{-1}a)$. We shall put

$$(1.1) \qquad G_p(\xi)=p^{-n}\sum_{x\in \boldsymbol{Z}_p^n}\chi_p(f_p(x)\xi), \quad \xi\in\boldsymbol{Z}_p,$$

and call this the Gaussian sum with respect to $f(X)$ at $p$. Clearly we have $|G_p(\xi)|\leqq 1$ and $G_p(0)=1$. It is Gauss's classical formula that

$$(1.2) \qquad |G_p(\xi)|=p^{-1/2} \text{ when } n=1,\ f(X)=X^2,\ p\neq 2 \text{ and } \xi\neq 0.$$

It is our purpose to generalize (1.2) to the case where $f(X)$ appears as a semi-invariant of an arbitrary connected algebraic group defined over $\boldsymbol{Q}$ having a non-trivial character defined over $\boldsymbol{Q}$.

**2.** For $\xi\in\boldsymbol{Z}_p$, denote by $N_p(\xi)$ the number of $x\in\boldsymbol{Z}_p^n$ such that $f_p(x)=\xi$. It is easy to verify the relation

$$(2.1) \qquad G_p(\xi)=p^{-1}\sum_{\eta\in\boldsymbol{Z}_p}p^{1-n}N_p(\eta)\chi_p(\xi\eta)$$

and the inversion

$$(2.2) \qquad p^{1-n}N_p(\eta)=\sum_{\xi\in\boldsymbol{Z}_p}G_p(\xi)\bar{\chi}_p(\xi\eta).$$

It follows from either (2.1) or (2.2) the following Parseval's relation:

(2.3) $$\sum_{\xi\in Z_p}|G_p(\xi)|^2=p^{-1}\sum_{\xi\in Z_p}(p^{1-n}N_p(\xi))^2.$$

By induction on $n$, one can prove easily that there is a positive constant $c_1$ depending only on $f(X)$ and not on $p$ such that

(2.4) $$N_p(\xi)\leqq c_1p^{n-1} \text{ for all } p \text{ and } \xi\in Z_p.$$

Substituting (2.4) in (2.3), we get

(2.5) $$\sum_{\xi\in Z_p^\times}|G_p(\xi)|^2\leqq c_2 \text{ for all } p,$$

where $Z_p^\times=Z_p-\{0\}$.

**3.** From now on, we shall consider a triple $(G, \omega, f)$ consisting of a connected algebraic group $G$ defined over $Q$, a non-trivial character $\omega$ of $G$ defined over $Q$ and a non-constant polynomial $f$ in $Z[X]$ such that

(3.1) $$f(tx)=\omega(t)f(x),\ x\in\Omega^n,\ t\in G,$$

where $\Omega$ means a universal domain containing $Q$.

We denote by $G_p$ the algebraic group defined over $Z_p$ obtained from $G$ by the reduction modulo $p$. For almost all $p$, $G_p$ remains connected, the reduced map $\omega_p$ remains to be a non-trivial character of $G_p$ defined over $Z_p$ and we have, for almost all $p$,

(3.2) $$f_p(tx)=\omega_p(t)f_p(x),\ x\in\Omega_p^n,\ t\in G_p,$$

where $\Omega_p$ means the universal domain over $Z_p$ obtained from $\Omega$. Denote by $G_{p,Z_p}$ the finite subgroup of $G_p$ consisting of points rational over $Z_p$. Using (3.2), we see that

(3.3) $$N_p(\omega_p(t)\xi)=N_p(\xi),\ \xi\in Z_p,\ t\in G_{p,Z_p}.$$

From (2.1), (3.3), we get

(3.4) $$G_p(\omega_p(t)\xi)=G_p(\xi)\ \ \xi\in Z_p,\ t\in G_{p,Z_p}.$$

Let

(3.5) $$Z_p=K_0+K_1+\cdots+K_{r_p},\ K_0=\{0\},$$

be the decomposition of $Z_p$ into the orbits under the action of the group $G_{p,Z_p}$. Denote by $\omega_{p,Z_p}$ the homomorphism $G_{p,Z_p}\rightarrow Z_p^\times$. Since $Z_p$ is a field, the cardinality of $K_i$ for $1\leqq i\leqq r_p$ is independent of $i$ and is equal to $[\mathrm{Im}(\omega_{p,Z_p})]$, here and from now on $[S]$ means the cardinality of a finite set $S$. Therefore we have the relation

(3.6) $$p-1=r_p[\mathrm{Im}(\omega_{p,Z_p})],$$

which implies also that

(3.7) $$r_p=[\mathrm{Cok}\,\omega_{p,Z_p}].$$

From (2.5), (3.4), (3.5), (3.6), we get

(3.8) $$r_p^{-1}(p-1)\sum_{i=1}^{r_p}|G_p(\xi_i)|^2\leqq c_2,\ \xi_i\in K_i.$$

In particular, in view of (3.7), we have, for almost all $p$,

(3.9) $$|G_p(\xi)|^2\leqq c_3 p^{-1}\ [\mathrm{Cok}\,\omega_{p,Z_p}],\ \xi\neq 0.$$

We now claim that

(3.10) $$[\mathrm{Cok}\,\omega_{p,Z_p}]\leqq c_4.$$

To prove (3.10), we first recall the Levi-Chevalley decomposition of $G$ over $\boldsymbol{Q}$: $G=UTS$, where $U$ is the unipotent radical of $G$, $R=UT$ is the radical of $G$, $A=TS$ is reductive, $T$ is a torus defined over $\boldsymbol{Q}$ which is the identity component of the center of $A$, $S$ is a semi-simple group which is the derived group of $A$. Since $U$, $S$ have no non-trivial characters, the non-triviality of $\omega$ implies that $\omega$ induces on $T$ a non-trivial character $\omega_T$. Now, let $T=T_0T_1$ be the decomposition where $T_0$ is the maximal $\boldsymbol{Q}$-trivial torus and $T_1$ is the torus having no non-trivial characters defined over $\boldsymbol{Q}$. Then, clearly, $\omega_T$ induces on $T_0$ a non-trivial character $\omega_{T_0}$. Finally, $T_0$ must contain a one dimensional $\boldsymbol{Q}$-trivial torus $T_2=G_m$ on which $\omega_{T_0}$ induces a non-trivial character $\omega_{T_2}$: $T_2=G_m\to G_m$. Hence $\omega_{T_2}(t)=t^e$ for some $e\geqq 1$. Now, for almost all $p$, $\omega_p:G_p\to G_{m,p}$ induces on $T_{2,p}=G_{m,p}$ the character $t\to t^e$ as above. Since $G\supset T_2$, $[\mathrm{Cok}\,\omega_{p,Z_p}]$ is a divisor of $[\mathrm{Cok}(\omega_{T_2})_{p,Z_p}]=(e,p-1)\leqq e$. Therefore the proof of (3.10) is complete.

Substituting (3.10) in (3.9) we obtain the following

**Theorem.** *Let $(G,\omega,f)$ be a triple of connected algebraic group $G$ defined over $\boldsymbol{Q}$, a non-trivial character $\omega$ of $G$ defined over $\boldsymbol{Q}$*

*and a non-constant polynomial* $f \in \mathbf{Z}[X]$ *satisfying* (3.1). *Then, we have* $|G_p(\xi)| \leqq cp^{-1/2}$ *for all* $p$ *and* $\xi \in \mathbf{Z}_p^\times$, *where* $c$ *is a positive constant depending only on the triple and not on* $p$.

THE JOHNS HOPKINS UNIVERSITY