On the structure of a Hecke ring of a Chevalley group over a finite field

By Nagayoshi IWAHORI

Dedicated to Professor Masao Sugawara

§ 0. Introduction.

We shall consider in this note the structure of the Hecke ring $\mathcal{H}(G, B)$ of a Chevalley group G over a finite field $\boldsymbol{F}_q$ with respect to a Borel subgroup B of G. The notion of a Hecke ring or the ring of double cosets given in G. Shimura [5] (L'algèbre des transformations) coincides in this case with the commutor algebra of $\rho(G)$ where ρ is the linear representation of G determined by the permutation representation of G on G/B (see § 1) since the group G is finite. Our main result is to provide a characterization of the ring $\mathcal{H}(G, B)$ in terms of its generators and defining relations (§ 4). It turns out that the generators and the defining relations of $\mathcal{H}(G, B)$ are closely related with those for the Weyl group W of G, or, with those for the group ring $\boldsymbol{Z}[W]$. More precisely, if $w_1, \cdots, w_l$ denote the reflections in W associated to simple roots $\alpha_1, \cdots, \alpha_l$, then it is well known (see [4, Expose 14], [8]. Also a proof is given in § 2.) that W is generated by $w_1, \cdots, w_l$ together with the defining relations

$$(1)\qquad \begin{cases} w_i^2=1\,, & (i=1,\cdots,l) \\ w_iw_j=w_jw_i\,, & \text{if}\quad \theta_{ij}=\pi/2\,, \\ w_iw_jw_i=w_jw_iw_j\,, & \text{if}\quad \theta_{ij}=2\pi/3\,, \\ (w_iw_j)^2=(w_jw_i)^2\,, & \text{if}\quad \theta_{ij}=3\pi/4\,, \\ (w_iw_j)^3=(w_jw_i)^3\,, & \text{if}\quad \theta_{ij}=5\pi/6\,. \end{cases}$$

where θ_{ij} means the angle between α_i and α_j. On the other hand, if we denote by $\omega_1, \cdots, \omega_l$ the elements in G which induce $w_1, \cdots, w_l$ respectively, then the double cosets $S_i=B\omega_iB$ $(i=1, \cdots, l)$ regarded as elements in $\mathcal{H}(G, B)$ generate the ring $\mathcal{H}(G, B)$ together with the defining relations

$$(2)\qquad \begin{cases} S_i^2=q\cdot 1+(q-1)S_i\,, & (i=1,\cdots,l)\,, \\ S_iS_j=S_jS_i\,, & \text{if}\quad \theta_{ij}=\pi/2\,, \\ S_iS_jS_i=S_jS_iS_j\,, & \text{if}\quad \theta_{ij}=2\pi/3\,, \\ (S_iS_j)^2=(S_jS_i)^2\,, & \text{if}\quad \theta_{ij}=3\pi/4\,, \\ (S_iS_j)^3=(S_jS_i)^3\,, & \text{if}\quad \theta_{ij}=5\pi/6\,. \end{cases}$$

Thus $\mathscr{H}(G, B)$ may be thought of as a 'deformation' of $\boldsymbol{Z}[G]$. In this respect a theorem of R. Steinberg [6] establishes the triviality of the deformation when G is of type A_l:

$$\mathscr{H}_{\boldsymbol{Q}}(G, B)=\mathscr{H}(G, B)\otimes_{\boldsymbol{Z}}\boldsymbol{Q}\cong\boldsymbol{Q}[W]\,. \tag{3}$$

Actually Steinberg's result is much stronger: for any parabolic subgroup H of G, $G\supset H\supset B$,

$$\mathscr{H}_{\boldsymbol{Q}}(G, H)\cong\mathscr{H}_{\boldsymbol{Q}}(W, W_H) \tag{4}$$

where W_H is the subgroup of W associated to H. So it seems natural to conjecture the validity of (3), (4) for every semi-simple algebraic group. We hope to treat this question some day in the future.

In §1, to make this note self-contained, we give the definition of the Hecke ring $\mathscr{H}(G, H)$ given in [5] associated to a group G and a subgroup H of G which is commensurable with any conjugate $x^{-1}Hx$. But we gave the definition of $\mathscr{H}(G,H)$ in a slightly different form using some measure on G and the convolution product w.r.t. this measure. Also several basic properties of $\mathscr{H}(G, H)$ are stated.

In §2, a theorem about the Weyl group is given. Firstly we define a notion of the *reduced expression* of an element w in W. The expression $w=w_{i_1}\cdots w_{i_r}$ is called reduced (with respect to the generators $w_1,\cdots, w_l$) if r is the least integer for w among these expressions. Now denote by $n(w)$ the number of positive roots which are sent into negative roots by w. Then it is shown that $w=w_{i_1}\cdots w_{i_r}$ is a reduced expression if and only if $n(w)=r$. (This result seems to be not new but we provide a proof for the sake of completeness.) Then our main result in §2 (Theorem 2.6) is the following: let Ω be any associative semi-group and $\Delta_1,\cdots,\Delta_l\in\Omega$. Suppose $\Delta_1,\cdots,\Delta_l$ satisfy the relations (1) except $\Delta_i^2=1$ $(i=1,\cdots,l)$. Then for any two reduced expressions

$$w=w_{i_1}\cdots w_{i_r}=w_{j_1}\cdots w_{j_r}$$

of w, we have $\Delta_{i_1}\cdots\Delta_{i_r}=\Delta_{j_1}\cdots\Delta_{j_r}$.

Thus we can separate off the relations $w_i^2=1$ in (1) from others. This provides a main tool for the characterization of $\mathscr{H}(G, B)$ in §4. Also using above theorem we give a proof of the characterization of the Weyl group W by (1).

In §3, for a Chevalley group G over a finite field $\boldsymbol{F}_q$, we consider the Hecke ring $\mathscr{H}(G, B)$ of G where B is a Borel subgroup of G. By Bruhat decomposition (see [2]), G is a disjoint union of B-double cosets $B\omega(w)B$, where $\omega(w)$ is an element in G inducing $w\in W$. Using the properties of this decomposition given in [2], we shall show that every double coset $B\omega(w)B$ is equal to $S_{i_1}\cdots S_{i_r}$ in the

ring $\mathcal{H}(G, B)$, where $w=w_{i_1}\cdots w_{i_r}$ is any reduced expression for w (Theorem 3.2). Thus $S_1, \cdots, S_l$ generate $\mathcal{H}(G, B)$. Then (2) is proved easily (Theorem 3.2).

In § 4, the main theorem is proved. The proof is a simple combination of theorems in § 2, § 3. In § 5, several applications of the main theorem are given.

Finally I should like to thank Professors O. Goldman and R. Steinberg for the suggesting and helpful conversations and criticisms while I was a member at the Institute for Advanced Study in 1960–62.

§ 1. Hecke rings.

Let G be a group and H a subgroup of G. If a subset A of G is H-left invariant, i.e. if $HA=A$, then A is decomposed into a disjoint union of H-cosets: $A=\bigcup_i Hx_i$. The set consisting of H-cosets Hx in A is denoted by $H\backslash A$. In the following the cardinality of a set S is denoted by $|S|$. Now for $x\in G$, let $K=H\cap x^{-1}Hx$. Then the map

$$\varphi: \quad K\backslash H \to H\backslash HxH$$

defined by $\varphi(Kh)=Hxh$ $(h\in H)$ is bijective. In fact, it is clearly surjective, and we have for $h, h'\in H$,

$$Kh=Kh' \Longleftrightarrow h'h^{-1}\in K \Longleftrightarrow h'h^{-1}\in x^{-1}Hx \Longleftrightarrow Hxh=Hxh'.$$

Thus we have $|K\backslash H|=[H:K]=|H\backslash HxH|$ $(x\in G)$. We shall denote this index $[H:H\cap x^{-1}Hx]$ by $\mathrm{ind}_H(x)$ or simply by $\mathrm{ind}(x)$. It is easy to see that

$$\mathrm{ind}(hxh')=\mathrm{ind}(x) \quad (\text{for any } x\in G,\ h\in H,\ h'\in H).$$

Now we assume that the following condition (A) is satisfied for the pair G, H:

(A) $$[H:H\cap x^{-1}Hx]<\infty \quad \text{for any } x\in G.$$

(in other words, H is commensurable with $x^{-1}Hx$ for any $x\in G$). Denote by $H\backslash G/H$ the set of all double cosets of G of type HxH, $x\in G$. Let $\mathcal{H}(G, H)$ be the free Z-module generated by the elements of $H\backslash G/H$. Then under the assumption (A), a multiplication is defined on $\mathcal{H}(G, H)$ which makes $\mathcal{H}(G, H)$ a ring over Z (see [5]). $\mathcal{H}(G, H)$ is called the *Hecke ring* of the pair G, H. We shall give here however another (but equivalent) definition of the ring $\mathcal{H}(G, H)$.

Let us denote by $\mathfrak{M}$ the set consisting of all H-left invariant subsets of G. A measure μ on $\mathfrak{M}$ is defined by $\mu(A)=|H\backslash A|$ for $A\in\mathfrak{M}$. Clearly μ is a completely additive measure on $\mathfrak{M}$. Moreover μ is right invariant, i.e. if $A\in G$, and $g\in G$, then $Ag\in\mathfrak{M}$ and $\mu(Ag)=\mu(A)$.

Now denote by $L(G, H)$ the space of all complex-valued, $\mathfrak{M}$-measurable, μ-

summable functions f defined on G such that

(1) $f(hgh')=f(g)$ for any $h\in H$, $h'\in H$, $g\in G$,

(2) $\mu(S(f))<\infty$ where $S(f)=\{x\in G;\ f(x)\neq 0\}$.

Then $L(G,H)$ is a vector space over the complex number field C and is closed with respect to the convolution product, i.e. if $f_1, f_2\in L(G,H)$ then the function f_1*f_2 defined by

$$(f_1*f_2)(x)=\int_G f_1(xy^{-1})f_2(y)\,d\mu(y) \qquad (x\in G)$$

is also in $L(G,H)$. In fact (1) is clear and (2) is checked as follows. We have $S(f_1*f_2)\subset S(f_1)S(f_2)$. Now $S(f_1)=\bigcup_{i=1}^{r} Hx_i$, $S(f_2)=\bigcup_{j=1}^{s} Hy_j$ imply $\mu(S(f_1)S(f_2))<\infty$ by the condition (A). Hence we get $\mu(S(f_1*f_2))<\infty$. Because of the right invariance of the measure μ, the convolution product is associative. Hence $L(G,H)$ is an associative algebra over C.

Now denote by χ_A the characteristic function of a subset A of G:

$$\chi_A(x)=\begin{cases} 1 & \text{for } x\in A \\ 0 & \text{for } x\notin A. \end{cases}$$

Then for any double coset $A=HaH$ $(a\in G)$, χ_A is in $L(G,H)$ by the condition (A). It is easy to see that $\{\chi_A;\ A\in H\backslash G/H\}$ is a base of the vector space $L(G,H)$. Thus we may identify the free Z-module $\mathcal{H}(G,H)$ generated by $A\in H\backslash G/H$ with the Z-submodule of $L(G,H)$ generated by the $\{\chi_A, A\in H\backslash G/H\}$. Therefore in the following we shall regard $\mathcal{H}(G,H)\subset L(G,H)$.

PROPOSITION 1.1. *The structure constants of the associative algebra $L(G,H)$ with respect to the base $\{\chi_A;\ A\in H\backslash G/H\}$ are non-negative integers.*

Hence $\mathcal{H}(G,H)$ is a subring of $L(G,H)$ and $L(G,H)\cong\mathcal{H}(G,H)\otimes_Z C$.

PROOF. Let $A, B\in H\backslash G/H$ and $\chi_A*\chi_B=\sum \mu_{A,B}^C\chi_C$ (finite sum) with $\mu_{A,B}^C\in C$. Let c be any element in C. Then

(3) $$\mu_{A,B}^C=(\chi_A*\chi_B)(c)=\int_G \chi_A(cx^{-1})\chi_B(x)\,d\mu(x)=\mu(A^{-1}c\cap B).$$

Hence $\mu_{A,B}^C$ is a non-negative integer, Q.E.D.

REMARK. $\mu_{A,B}^C$ is positive if and only if $c\in AB$ i.e. if and only if $C\subset AB$.

Clearly χ_H is the unit element of the ring $\mathcal{H}(G,H)$. Now let us prove the equivalence of the convolution product with the multiplication A, B of two double cosets A, B given in Shimura [5]. In fact, let

$$A=\cup Ha_i, \qquad B=\cup Hb_j$$

be disjoint unions, then $A^{-1}c=\cup a_i^{-1}Hc$ is also a disjoint union and

$$A^{-1}c\cap B=\bigcup_{i,j}(a_i^{-1}Hc\cap Hb_j)\,.$$

Now we have

$$\begin{aligned}Hb_j\subset A^{-1}c &\Longleftrightarrow b_j\in A^{-1}c \Longleftrightarrow b_j\in a_i^{-1}Hc \text{ for some } i\\ &\Longleftrightarrow Ha_ib_j=Hc \text{ for some } i\,.\end{aligned}$$

Thus we get

$$(4)\qquad \mu^C_{A,B}=\mu(A^{-1}c\cap B)=\sum_j\mu(A^{-1}c\cap Hb_j)=\sum_{i,j}\mu(Ha_ib_j\cap Hc)\,,$$

i.e. $\mu^C_{A,B}$ is equal to the number of (i,j) such that $Ha_ib_j=Hc$. Hence the equivalence was proved. Using (4), it is immediate that if N is a normal subgroup of G such that $G\supset H\supset N$, then we have

$$\mathscr{H}(G,H)\cong\mathscr{H}(G/N,H/N)\qquad \text{canonically.}$$

Now the map $L(G,H)\to C$ defined by $f\to\int_G f(x)d\mu(x)$ is clearly an algebra-homomorphism. The value of this integral for $f=\chi_{HaH}$ $(a\in G)$ is equal to $\mu(HaH)$ $=\mathrm{ind}(a)$. Thus we denote $\int_G f(x)d\mu(x)$ also by $\mathrm{ind}(f)$. We shall also denote by $\mathrm{ind}(A)$ instead of $\mathrm{ind}(\chi_A)$ for $A\in H\backslash G/H$.

LEMMA 1.2. *Let $a,b\in G$ and $A=HaH$, $B=HbH$, $C=HabH$. Then*

$$\chi_A*\chi_B=\chi_C\Longleftrightarrow \mathrm{ind}(ab)=\mathrm{ind}(a)\,\mathrm{ind}(b)\,.$$

PROOF. Put $\chi_A*\chi_B=\sum_D\mu^D_{A,B}\chi_D$. Clearly $\mu^C_{A,B}>0$. Now we have

$$\mathrm{ind}(A)\,\mathrm{ind}(B)=\sum_D\mu^D_{A,B}\,\mathrm{ind}(D)\,.$$

Hence $\mu^D_{A,B}>0$ implies that $\mathrm{ind}(A)\mathrm{ind}(B)\geqq\mathrm{ind}(D)$. Now $\chi_A*\chi_B=\chi_C$ implies that $\mathrm{ind}(ab)$ $=\mathrm{ind}(a)\,\mathrm{ind}(b)$ obviously. Conversely, if $\mathrm{ind}(ab)=\mathrm{ind}(a)\,\mathrm{ind}(b)$, then we get $\mathrm{ind}(A)$ $\times\mathrm{ind}(B)=\mathrm{ind}(C)$. Consequently $\mu^D_{A,B}=0$ for any $D\in H\backslash G/H$, $D\neq C$. Thus we have $\chi_A*\chi_B=\chi_C$, Q.E.D.

We shall use later the following formula for $\mu^C_{A,B}$.

LEMMA 1.3. *Let $A,B,C\in H\backslash G/H$ and $A=\bigcup_i Ha_i$ (disjoint union), $B=HbH$, $C=HcH$. Then*

$$(5)\qquad \mu^C_{A,B}=\mu(A^{-1}c\cap B)=\frac{\mathrm{ind}(b)}{\mathrm{ind}(c)}\,\sharp\{i;\ Ha_ibH=HcH\}\,.$$

PROOF. Let $K=H\cap b^{-1}Hb$ and $H=\bigcup_j Kh_j$ be a disjoint union. Then, as was noted above, $HbH=\bigcup_j Hbh_j$ is a disjoint union. Now we have $Ha_ibH=HcH$ if and only if $Ha_ibh_jH=HcH$. Hence

$$\sharp\{(i,j);\ Ha_ibh_jH=HcH\}=\mathrm{ind}(b)\,\sharp\{i;\ Ha_ibH=HcH\}\,.$$

On the other hand, if $C=\bigcup_k Hc_k$ is a disjoint union, then we have

$$Ha_ibh_jH=HcH \Longleftrightarrow a_ib\cdot h_j\in HcH \Longleftrightarrow a_ib\cdot h_j\in Hc_k \text{ for some } k$$
$$\Longleftrightarrow Ha_ibh_j=Hc_k \text{ for some } k.$$

Then we get

$$\sharp\{(i,j);\ Ha_ibh_jH=HcH\}=\sum_k \sharp\{(i,j);\ Ha_ibh_j=Hc_k\}$$
$$=\sum_k \mu_{A,B}^{Hc_kH} \quad \text{(by (4))}.$$

Since $Hc_1H=Hc_2H=\cdots=C$, this is equal to $\mathrm{ind}(c)\cdot\mu_{A,B}^{C}$, Q.E.D.

Let us observe that when G is a locally compact topological group and H is an open compact subgroup of G, then the condition (A) is satisfied and that with respect to the convolution product using the right invariant Haar measure dx on G normalized by $\int_H dx=1$, $L(G,H)$ is also an associative algebra, and actually this convolution product coincides with the convolution product defined above using the measure μ. Because we have $\mu(HaH)=\int_{HaH} dx$ for every $a\in G$.

In particular when H is finite, the discrete topology on G makes H open and compact. Hence, in the group algebra $\boldsymbol{C}[G]$, if we put $e=|H|^{-1}\sum_{h\in H} h$, then we have $e^2=e$ and $L(G,H)=e\cdot\boldsymbol{C}[G]\cdot e$. We have moreover $\chi_{HaH}=|H|^{-1}\sum_{x\in HaH} x$. ($e$ is the unit element of $\mathscr{H}(G,H)$). This shows that $L(G,H)$ is a semi-simple associative algebra over $\boldsymbol{C}$ when G is a finite group. We shall close this section by the following proposition which seems to be well-known.

PROPOSITION 1.4. *Let G be a finite group and H a subgroup of G. Let K be a field and ρ the representation of G over K induced by the trivial representation of H, i.e. ρ is the representation of G given by the $K[G]$-module $V=K[G]\underset{K[H]}{\otimes} K$. Suppose that the characteristic of K does not divide the order of H. Then $\mathscr{H}_K(G,H)=\mathscr{H}(G,H)\underset{Z}{\otimes}K$ is isomorphic to the commutor algebra A of $\rho(G)$ in* $\mathrm{End}(V)$.

N.B. $\quad A=\{\sigma\in\mathrm{End}(V);\ \sigma\cdot\rho(x)=\rho(x)\cdot\sigma \text{ for every } x\in G.\}$

PROOF. V can be identified in an obvious manner with the vector space over K spanned by the cosets $xH(x\in G)$ as its base. Or V can be identified with the subspace $K[G]\cdot e$ of $K[G]$ where $e=|H|^{-1}\sum_{h\in H} h$. Now the linear map $\varphi: S\to S(e)$ from A into V is injective. In fact, if $S(e)=0$, then for any $u\in V$ we have $S(u)=S(ue)=uS(e)=0$. Now since $e^2=e$ we have $S(e)=eS(e)\in eK[G]e=\mathscr{H}_K(G,H)$. Thus φ is a linear map from A into $\mathscr{H}_K(G,H)$. φ is surjective. In fact, let $a\in\mathscr{H}_K(G,H)$. Then we have $\varphi(S_a)=a$, where S_a is an element of A defined by $S_a(u)=ua(u\in V)$. Also we have $\varphi(S_1S_2)=\varphi(S_2)\varphi(S_1)$. Hence φ is an anti-isomorphism between two algebras A and $\mathscr{H}_K(G,H)$. On the other hand, it is easy

to see that the anti-involution $x \to x^{-1}$ of G induces an anti-involution of $\mathfrak{H}_K(G, H)$. Thus $A \cong \mathfrak{H}_K(G, H)$, Q.E.D.

COROLLARY 1.5. *We use the same notations as in Proposition 1.4.*

(i) *Let $K=\boldsymbol{C}$ and $\rho = m_1\rho_1 + \cdots + m_r\rho_r$ be a decomposition of the representation ρ into irreducible representations $\rho_1, \cdots, \rho_r$ with multiplicities $m_1, \cdots, m_r$ respectively. Then $\mathfrak{H}_{\boldsymbol{C}}(G, H)$ is isomorphic with the direct sum of total matric algebras of degree $m_1, \cdots, m_r$:*

$$\mathfrak{H}_{\boldsymbol{C}}(G, H) \cong M_{m_1}(\boldsymbol{C}) \oplus M_{m_2}(\boldsymbol{C}) \oplus \cdots \oplus M_{m_r}(\boldsymbol{C}) .$$

(ii) *If the characteristic of the field K does not divide the order of G, then $\mathfrak{H}_K(G, H)$ is a semi-simple algebra.*

REMARK. It is seen similarly that for subgroups H_1, H_2 of a finite group G, we have

$$|H_1 \backslash G / H_2| = \sum_i m_i n_i = \frac{|G|}{|H_1| \cdot |H_2|} \sum_{\mathfrak{K}} \frac{|\mathfrak{K} \cap H_1| \cdot |\mathfrak{K} \cap H_2|}{|\mathfrak{K}|} ,$$

where m_i and n_i are multiplicities of an irreducible representation ρ_i in the induced representations $\boldsymbol{C}[G] \underset{\boldsymbol{C}[H_1]}{\otimes} \boldsymbol{C}$ and $\boldsymbol{C}[G] \underset{\boldsymbol{C}[H_2]}{\otimes} \boldsymbol{C}$ respectively and $\mathfrak{K}$ ranges over the set of all conjugate classes of G.

§ 2. A property of the Weyl group of a complex semi-simple Lie algebra.

Let $\mathfrak{g}$ be a complex semi-simple Lie algebra and $\mathfrak{h}$ a Cartan sub-algebra of $\mathfrak{g}$. Let Δ be the root system of $\mathfrak{g}$ with respect to $\mathfrak{h}$ and Π a fundamental root system. Let W be the Weyl group of $\mathfrak{g}$ with respect to $\mathfrak{h}$. For each $\alpha \in \Delta$, we denote by w_α the reflection with respect to the hyperplane $\{H \in \mathfrak{h};\ \alpha(H)=0\}$. Let $\Pi = \{\alpha_1, \cdots, \alpha_l\}$, then $w_1, \cdots, w_l$ generate W, where $w_i = w_{\alpha_i}$ $(i=1, \cdots, l)$. (see [4]). Denote the subset $1, w_1, \cdots, w_l$ of W by $\mathfrak{S}$. Then we have

$$\{1\} = \mathfrak{S}^0 \subset \mathfrak{S}^1 \subset \mathfrak{S}^2 \subset \cdots \subset W, \quad \bigcup_{i=0}^{\infty} \mathfrak{S}^i = W ,$$

where $\mathfrak{S}^i = \mathfrak{S}^{i-1}\mathfrak{S}$ $(i=2, 3, \cdots)$, $\mathfrak{S}^1 = \mathfrak{S}$. Then for any element $w \in W$, there is one and only one integer i, $i \geqq 0$, such that $w \in \mathfrak{S}^i - \mathfrak{S}^{i-1}$. (We put $\mathfrak{S}^{-1} = \phi =$ the empty set.) Let us denote this number i by $l(w)$. Note that $l(w)=r$ means that w can be written as a product of r w_i's but can not be written as a product of fewer number of the w_i's.

Now denote by $\Delta^+(\Delta^-)$ the set of all positive (negative) roots in Δ (with respect to a linear ordering which makes every root in Π positive). Denote also for an element w of W by Δ_w^+ the subset $w^{-1}(\Delta^-) \cap \Delta^+$ of Δ^+. Denote by $n(w)$ the cardinality of the set Δ_w^+. The following lemma is well known (see [4]).

LEMMA 2.1. (i) $w_i(\Delta^+-\{\alpha_i\})=\Delta^+-\{\alpha_i\}$.

(ii) *If* $n(w)=0$, *then* $w=1$.

Now we shall show that $n(w)=l(w)$ for any $w\in W$.

LEMMA 2.2. (i) $w_i(\Delta_w^+-\{\alpha_i\})=\Delta_{ww_i}^+-\{\alpha_i\}$ *for any* $w\in W$ *and* $i=1,\cdots,l$.

(ii) *For any* $w\in W$ *and for any* i, $1\leqq i\leqq l$, α_i *is contained in* Δ_w^+ *or in* $\Delta_{ww_i}^+$. *Moreover,* α_i *is contained only in one of the* Δ_w^+, $\Delta_{ww_i}^+$. *We have also*

$$n(w)-1=n(ww_i), \quad \text{if } \alpha_i\in\Delta_w^+,$$
$$n(w)+1=n(ww_i), \quad \text{if } \alpha_i\notin\Delta_w^+,$$

(iii) $n(w)=l(w)$ *for any* $w\in W$.

PROOF. (i) If $\alpha\in\Delta_w^+-\{\alpha_i\}$, then by Lemma 2.1 we have $w_i(\alpha)\in\Delta^+$. Since $ww_iw_i(\alpha)=w(\alpha)\in\Delta^-$ we get $w_i(\alpha)\in\Delta_{ww_i}^+$. Moreover, $w_i(\alpha)\neq\alpha_i$ because of $\alpha\neq-\alpha_i=w_i(\alpha_i)$. Thus we obtained $w_i(\Delta_w^+-\{\alpha_i\})\subset\Delta_{ww_i}^+-\{\alpha_i\}$. Applying this inclusion relation for ww_i, we get $w_i(\Delta_{ww_i}^+-\{\alpha_i\})\subset\Delta_w^+-\{\alpha_i\}$, i.e. $\Delta_{ww_i}^+-\{\alpha_i\}\subset w_i(\Delta_w^+-\{\alpha_i\})$. Thus we proved that $w_i(\Delta_w^+-\{\alpha_i\})=\Delta_{ww_i}^+-\{\alpha_i\}$.

(ii) Assume $\alpha_i\in\Delta_w^+$ and $\alpha_i\in\Delta_{ww_i}^+$. Then $w(\alpha_i)\in\Delta^-$, $ww_i(\alpha_i)\in\Delta^-$. Thus $-w(\alpha_i)\in\Delta^-$, which is a contradiction. Similarly, if we assume $\alpha_i\notin\Delta_w^+$ and $\alpha_i\notin\Delta_{ww_i}^+$, then we have a contradiction. Thus α_i belongs to one and only one of the Δ_w^+, $\Delta_{ww_i}^+$. If $\alpha_i\in\Delta_w^+$, then $\alpha_i\notin\Delta_{ww_i}^+$, i.e. $\Delta_{ww_i}^+=\Delta_{ww_i}^+-\{\alpha_i\}$. Hence we get $n(w)-1=n(ww_i)$ by (i). Similarly if $\alpha_i\notin\Delta_w^+$, then $\alpha_i\in\Delta_{ww_i}^+$ and we get $n(w)+1=n(ww_i)$.

(iii) Let $k=n(w)$. If $k=0$, then $w=1$ by Lemma 2.1. Hence $l(w)=0=n(w)$. Now let us complete the proof by the induction on k. Assume $n(w)=l(w)$ is valid for $w\in W$ with $n(w)\leqq k-1$. Now let $w\in W$, $n(w)=k>0$. Then $w\neq1$. Therefore there exists a root $\alpha\in\Delta^+$ such that $w(\alpha)\in\Delta^-$ by Lemma 2.1, (ii). Now α is a linear combination of $\alpha_1,\cdots,\alpha_l$ with non-negative integral coefficients: $\alpha=m_1\alpha_1+\cdots+m_l\alpha_l$. Then some $w(\alpha_i)$ must be in Δ^-. Hence $\alpha_i\in\Delta_w^+$. Let $w'=ww_i$. Then $\alpha_i\in\Delta_w^+$ implies $n(w')=n(w)-1=k-1$ by (ii). Hence we have $n(w')=l(w')=k-1$ by our induction assumption. Then $w'\in\mathfrak{S}^{k-1}$ and we get $w=w'w_i\in\mathfrak{S}^k$. Thus we get $l(w)\leqq k=n(w)$. So we have only to show that $n(w)\leqq l(w)$. Put $l(w)=j$. Then w can be written as $w=w_{i_1}\cdots w_{i_j}$ for some $i_1,\cdots,i_j$ such that $1\leqq i_1,\cdots,i_j\leqq l$. Now for any $u\in W$ and for any i, $1\leqq i\leqq l$, we have $n(uw_i)\leqq n(u)+1$ by (ii). Hence we get $n(w)\leqq j=l(w)$, Q.E.D.

We shall call an expression $w=w_{i_1}w_{i_2}\cdots w_{i_k}$ $(1\leqq i_1,\cdots,i_k\leqq l)$ of $w\in W$ *reduced* if $k=n(w)=l(w)$.

LEMMA 2.3. *Let* $w\in W$. *Then there exists a reduced expression of* w, $w=w_{i_1}\cdots w_{i_k}$ *with* $i_k=i$, *if and only if* $\alpha_i\in\Delta_w^+\cap\Pi$.

PROOF. If $w=w_{i_1}\cdots w_{i_k}$ is a reduced expression with $i_k=i$, then $w'=w_{i_1}\cdots w_{i_{k-1}}$ is also a reduced expression for $w'=ww_i$. In fact, if $w'=w_{i_1}\cdots w_{i_{k-1}}$ is not reduced,

then $n(w')<k-1$ and we have $n(w)<k$ which is a contradiction. Hence we have $n(w')=n(w)-1$. Then by Lemma 2.2 (ii) we have $\alpha_i \in \Delta_w^+ \cap \Pi$.

Conversely, let $\alpha_i \in \Delta_w^+ \cap \Pi$. Put $w'=ww_i$. Then $n(w')=n(w)-1$ by Lemma 2.2, (ii). Let $w'=w_{i_1}\cdots w_{i_{k-1}}$ $(k=n(w))$ be any reduced expression for w'. Then $w=w_{i_1}\cdots w_{i_{k-1}}w_i$ is a reduced expression for w because of $n(w)=k$, Q.E.D.

Let us denote by θ_{ij} the angle between two vectors α_i, α_j. As is well known, [4], as for the values of θ_{ij}, only the following four cases are possible:

(i) $\theta_{ij}=\pi/2$. Then $w_iw_j=w_jw_i$.

(ii) $\theta_{ij}=2\pi/3$. Then $w_iw_jw_i=w_jw_iw_j$.

(iii) $\theta_{ij}=3\pi/4$. Then $(w_iw_j)^2=(w_jw_i)^2$.

(iv) $\theta_{ij}=5\pi/6$. Then $(w_iw_j)^3=(w_jw_i)^3$.

It is also known that these relations together with $w_i^2=1$ $(i=1,\cdots,l)$ form a system of defining relations for the Weyl group W with respect to the generators $w_1,\cdots,w_l$. (see [4], [8]). We shall give another proof of this fact at the end of § 2.

We shall use later the following

LEMMA 2.4. (i) *If* $\theta_{ij}=\pi/2$, *then* $n(w_iw_j)=n(w_jw_i)=2$ *and* $\Delta^+_{w_iw_j}=\{\alpha_i, \alpha_j\}$.

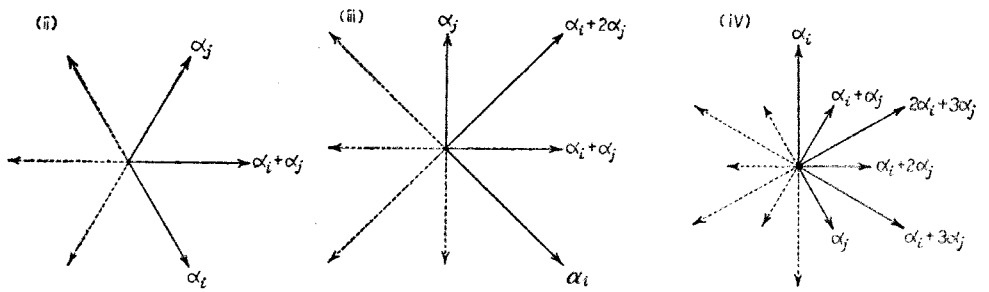
(ii) *If* $\theta_{ij}=2\pi/3$, *then* $n(w_iw_jw_i)=n(w_jw_iw_j)=3$ *and* $\Delta^+_{w_iw_jw_i}=\{\alpha_i, \alpha_j, \alpha_i+\alpha_j\}$.

(iii) *If* $\theta_{ij}=3\pi/4$ *and* $\|\alpha_i\|>\|\alpha_j\|$, *then* $n((w_iw_j)^2)=n((w_jw_i)^2)=4$ *and* $\Delta^+_{(w_iw_j)^2}=\{\alpha_i, \alpha_j, \alpha_i+\alpha_j, \alpha_i+2\alpha_j\}$.

(iv) *If* $\theta_{ij}=5\pi/6$ *and* $\|\alpha_i\|>\|\alpha_j\|$, *then* $n((w_iw_j)^3)=n((w_jw_i)^3)=6$ *and* $\Delta^+_{(w_iw_j)^3}=\alpha_i, \alpha_j, \alpha_i+\alpha_j, \alpha_i+2\alpha_j, \alpha_i+3\alpha_j, 2\alpha_i+3\alpha_j\}$.

PROOF. (i) Since $w_iw_j \in \mathfrak{S}^2$ we have $n(w_iw_j)=l(w_iw_j)\leqq 2$. On the other hand it is easy to check that $\alpha_i, \alpha_j \in \Delta^+_{w_iw_j}$. Hence $n(w_iw_j)\geqq 2$ and we get also $n(w_jw_i)=2$ and $\Delta^+_{w_iw_j}=\{\alpha_i, \alpha_j\}$. (ii), (iii), (iv) are also proved similarly.

REMARK. The cases (ii), (iii), (iv) are explained by the following root diagrams.



From these pictures and analogous considerations as in Lemma 2.4 it is easy to determine the set Δ_w^+ for any element w in the subgroup of W generated by two elements w_i and w_j (this subgroup is a dihedral group of order 4, 6, 8, 12

respectively according to cases (i), (ii), (iii), (iv).) In particular we have the

LEMMA 2.5. (i) *If* $\theta_{ij}=\pi/2$, *then* $w_i(\alpha_j)\in\Delta^+$.

(ii) *If* $\theta_{ij}=2\pi/3$, *then* $w_i(\alpha_j)\in\Delta^+$, $w_jw_i(\alpha_j)\in\Delta^+$.

(iii) *If* $\theta_{ij}=3\pi/4$, *then* $w_i(\alpha_j)\in\Delta^+$, $w_jw_i(\alpha_j)\in\Delta^+$, $w_iw_jw_i(\alpha_j)\in\Delta^+$.

(iv) *If* $\theta_{ij}=5\pi/6$, *then* $w_i(\alpha_j)\in\Delta^+$, $w_jw_i(\alpha_j)\in\Delta^+_w$, $w_iw_jw_i(\alpha_j)\in\Delta^+$, $(w_jw_i)^2(\alpha_j)\in\Delta^+$, $(w_iw_j)^2w_i(\alpha_j)\in\Delta^+$.

Now in order to state some universality property of W, we define several notations. Let us call a finite sequence $(i_1,\cdots,i_r)$ of integers *admissible* if $1\leqq i_1,\cdots,i_r\leqq l$ and $n(w_{i_1}\cdots w_{i_r})=r$. We denote by $\mathfrak{F}$ the set of all admissible sequences. Let us define a map $\lambda\to w(\lambda)$ from $\mathfrak{F}$ into W by $w(\lambda)=w_{i_1}\cdots w_{i_r}$ where $\lambda=(i_1,\cdots,i_r)$. This map is clearly surjective. We shall call two elements λ and μ in $\mathfrak{F}$ *equivalent* (in notation $\lambda\sim\mu$) if $w(\lambda)=w(\mu)$. Obviously $\sim$ is an equivalence relation in $\mathfrak{F}$. If $\lambda=(i_1,\cdots,i_r)$, $\mu=(j_1,\cdots,j_s)$ are equivalent admissible sequences, then we have $r=n(w_{i_1}w_{i_2}\cdots w_{i_r})=n(w_{j_1}w_{j_2}\cdots w_{j_s})=s$. We shall call r the *length* of $\lambda=(i_1,\cdots,i_r)$.

THEOREM 2.6. *Let* Ω *be an associative semi-group and* $\Delta_1,\cdots,\Delta_l$ *be elements in* Ω *such that for any distinct integers* i,j *between* 1 *and* l *the following relations are valid:*

(i) $\Delta_i\Delta_j=\Delta_j\Delta_i$, *if* $\theta_{ij}=\pi/2$,

(ii) $\Delta_i\Delta_j\Delta_i=\Delta_j\Delta_i\Delta_j$, *if* $\theta_{ij}=2\pi/3$,

(iii) $(\Delta_i\Delta_j)^2=(\Delta_j\Delta_i)^2$, *if* $\theta_{ij}=3\pi/4$,

(iv) $(\Delta_i\Delta_j)^3=(\Delta_j\Delta_i)^3$, *if* $\theta_{ij}=5\pi/6$,

where θ_{ij} *is the angle between the simple roots* α_i *and* α_j. *Let* $\lambda\to\Delta(\lambda)$ *be the map from* $\mathfrak{F}$ *into* Ω *defined by* $\Delta(\lambda)=\Delta_{i_1}\cdots\Delta_{i_r}$ *for* $\lambda=(i_1,\cdots,i_r)\in\mathfrak{F}$. *Then we have* $\Delta(\lambda)=\Delta(\mu)$ *if* $\lambda\sim\mu$.

PROOF. Let $\lambda=(p_1,\cdots,p_k)$ and $\mu=(q_1,\cdots,q_k)$ be in $\mathfrak{F}$ and $\lambda\sim\mu$. If $k=1$, we have clearly $\Delta(\lambda)=\Delta(\mu)$. We shall prove the theorem by the induction on the length k of λ. Suppose $k\geqq 2$ and the theorem is valid for all $\lambda,\mu\in\mathfrak{F}$ which are equivalent and of length$<k$. If $p_k=q_k$, then from $w_{p_1}\cdots w_{p_k}=w_{q_1}\cdots w_{q_k}$ we have $w_{p_1}\cdots w_{p_{k-1}}=w_{q_1}\cdots w_{q_{k-1}}$. Hence by the induction assumption we get $\Delta_{p_1}\cdots\Delta_{p_{k-1}}=\Delta_{q_1}\cdots\Delta_{q_{k-1}}$ and consequently $\Delta(\lambda)=\Delta(\mu)$. Thus we may assume that $p_k\neq q_k$. Denote by θ the angle between α_{p_k} and α_{q_k}. Then since $p_k\neq q_k$, θ is one of the following four values: $\pi/2$, $2\pi/3$, $3\pi/4$, $5\pi/6$.

Now since $w_{p_1}\cdots w_{p_k}=w_{q_1}\cdots w_{q_k}$ and these are reduced expressions, we have by Lemma 2.3,

$$w_{q_1}\cdots w_{q_k}(\alpha_{p_k})\in\Delta^-.$$

Hence there is an integer i with $2\leqq i\leqq k$ such that $w_{q_i}\cdots w_{q_k}(\alpha_{p_k})\in\Delta^+$ and $w_{q_{i-1}}w_{q_i}\cdots w_{q_k}(\alpha_{p_k})\in\Delta^-$. Then $w_{q_i}\cdots w_{q_k}(\alpha_{p_k})$ must coincide with $\alpha_{q_{i-1}}$ by Lemma

2.1, (i): $w_{q_i}\cdots w_{q_k}(\alpha_{p_k})=\alpha_{q_{i-1}}$. This implies that $(w_{q_i}\cdots w_{q_k})w_{p_k}(w_{q_i}\cdots w_{q_k})^{-1}=w_{q_{i-1}}$, i.e.

$$(1)\qquad w_{q_i}\cdots w_{q_k}w_{p_k}=w_{q_{i-1}}w_{q_i}\cdots w_{q_k}.$$

We distinguish two cases here according to $i>2$ or $i=2$. Suppose $i>2$. Then both side of (1) are of the same length$<k$ and the right hand side is clearly a reduced expression. Hence we see that $(q_i,\cdots,q_k,p_k)$ is also in $\mathfrak{N}$ and by our induction assumption we get

$$(2)\qquad \Delta_{q_i}\cdots\Delta_{q_k}\Delta_{p_k}=\Delta_{q_{i-1}}\Delta_{q_i}\cdots\Delta_{q_k}$$

Now (1) and $w_{p_1}\cdots w_{p_k}=w_{q_1}\cdots w_{q_k}$ imply that

$$w_{q_1}\cdots w_{q_{i-2}}w_{q_i}\cdots w_{q_k}w_{p_k}=w_{q_1}\cdots w_{q_k}=w_{p_1}\cdots w_{p_k}$$

i.e. $w_{q_1}\cdots w_{q_{i-2}}w_{q_i}\cdots w_{q_k}=w_{p_1}\cdots w_{p_{k-1}}$. Both side of the above equation are of the same length $k-1$ and reduced. Hence we get by our induction assumption that

$$(3)\qquad \Delta_{q_1}\cdots\Delta_{q_{i-2}}\Delta_{q_i}\cdots\Delta_{q_k}=\Delta_{p_1}\cdots\Delta_{p_{k-1}}.$$

From (2) and (3) we get

$$\begin{aligned}\Delta(\lambda)=\Delta_{p_1}\cdots\Delta_{p_k}&=\Delta_{q_1}\cdots\Delta_{q_{i-2}}\Delta_{q_i}\cdots\Delta_{q_k}\Delta_{p_k}\\&=\Delta_{q_1}\cdots\Delta_{q_{i-2}}\Delta_{q_{i-1}}\cdots\Delta_{q_k}=\Delta(\mu)\end{aligned}$$

as desired.

Thus we may assume in the following that $i=2$ in (1). We have then

$$(4)\qquad w_{p_1}\cdots w_{p_k}=w_{q_1}\cdots w_{q_k}=w_{q_2}\cdots w_{q_k}w_{p_k}.$$

Hence we have also $w_{p_1}\cdots w_{p_{k-1}}=w_{q_2}\cdots w_{q_k}$, which implies that

$$\Delta_{p_1}\cdots\Delta_{p_{k-1}}=\Delta_{q_2}\cdots\Delta_{q_k}$$

Thus to prove $\Delta(\lambda)=\Delta(\mu)$ it is sufficient to show

$$(*)\qquad \Delta_{q_2}\cdots\Delta_{q_k}\Delta_{p_k}=\Delta_{q_1}\cdots\Delta_{q_k}.$$

Now let us distinguish two cases here according to $\theta=\pi/2$ or $\theta>\pi/2$.

Suppose $\theta=\pi/2$. Then (4) and $w_{p_k}w_{q_k}=w_{q_k}w_{p_k}$ imply that

$$w_{q_2}\cdots w_{q_{k-1}}w_{p_k}=w_{q_1}\cdots w_{q_{k-1}}.$$

Hence by induction assumption we get

$$(5)\qquad \Delta_{q_2}\cdots\Delta_{q_{k-1}}\Delta_{p_k}=\Delta_{q_1}\cdots\Delta_{q_{k-1}}.$$

Then using $\Delta_{p_k}\Delta_{q_k}=\Delta_{q_k}\Delta_{p_k}$ (since $\theta=\pi/2$), (5) gives (*) immediately. Therefore in the following we may assume that $\theta>\pi/2$. Then θ is equal to $2\pi/3$ or $3\pi/4$ or

$5\pi/6$. Hence by Lemma 2.5 we have $w_{pk}(\alpha_{qk})\in\Delta^+$, $w_{qk}w_{pk}(\alpha_{qk})\in\Delta^+$. Moreover we get from (5) using Lemma 2.3,

$$w_{q_2}\cdots w_{qk}w_{pk}(\alpha_{qk})\in\Delta^- .$$

Then we see as before that there is an integer j with $2\leqq j\leqq k$ such that

(6) $$w_{qj}\cdots w_{qk}w_{pk}w_{qk}=w_{qj-1}w_{qj}\cdots w_{qk}w_{pk} .$$

We distinguish here again two cases according to $j>3$ or $j=3$. Suppose $j>3$. Then both sides of (6) are of length $k-j+3<k$ and are reduced. We have then by our induction assumption

(7) $$\Delta_{qj}\cdots\Delta_{qk}\Delta_{pk}\Delta_{qk}=\Delta_{qj-1}\Delta_{qj}\cdots\Delta_{qk}\Delta_{pk} .$$

Now (6) and (4) imply that

$$w_{q_1}\cdots w_{qk}=w_{q_2}\cdots w_{qj-2}w_{qj}\cdots w_{qk}w_{pk}w_{qk} ,$$

i.e. $$w_{q_1}\cdots w_{qk-1}=w_{q_2}\cdots w_{qj-2}w_{qj}\cdots w_{qk}w_{pk} .$$

Hence by the induction assumption we get

(8) $$\Delta_{q_1}\cdots\Delta_{qk-1}=\Delta_{q_2}\cdots\Delta_{qj-2}\Delta_{qj}\cdots\Delta_{qk}\Delta_{pk} .$$

From (7) and (8) we get (*) easily.

Thus in the following we may assume that $j=3$ in (6). We have then

(9) $$\begin{aligned} w_{p_1}\cdots w_{pk}&=w_{q_1}\cdots w_{qk}\\ &=w_{q_2}\cdots w_{qk}w_{pk}\\ &=w_{q_3}\cdots w_{qk}w_{pk}w_{qk} .\end{aligned}$$

Hence we have $w_{q_1}\cdots w_{qk-1}=w_{q_3}\cdots w_{qk}w_{pk}$, which gives in turn

(10) $$\Delta_{q_1}\cdots\Delta_{qk-1}=\Delta_{q_3}\cdots\Delta_{qk}\Delta_{pk} .$$

We distinguish here two cases according to $\theta=2\pi/3$ or $\theta>2\pi/3$.

Suppose $\theta=2\pi/3$. Then we have $w_{qk}w_{pk}w_{qk}=w_{pk}w_{qk}w_{pk}$, which combined with (9) gives

$$w_{q_3}\cdots w_{qk-1}w_{pk}=w_{q_2}\cdots w_{qk-1} .$$

Then we get by our induction assumption

(11) $$\Delta_{q_3}\cdots\Delta_{qk-1}\Delta_{pk}=\Delta_{q_2}\cdots\Delta_{qk-1} .$$

On the other hand we have $\Delta_{pk}\Delta_{qk}\Delta_{pk}=\Delta_{qk}\Delta_{pk}\Delta_{qk}$ since $\theta=2\pi/3$. Then we get easily from (11)

$$\Delta_{q_3}\cdots\Delta_{qk-1}\Delta_{qk}\Delta_{pk}\Delta_{qk}=\Delta_{q_2}\cdots\Delta_{qk-1}\Delta_{qk}\Delta_{pk} ,$$

which gives (*) when combined with (10).

Therefore we may assume in the following that $\theta>2\pi/3$. Then we have by Lemma 2.5

$$w_{qk}(\alpha_{pk})\in\Delta^+,\ w_{pk}w_{qk}(\alpha_{pk})\in\Delta^+,\ w_{qk}w_{pk}w_{qk}(\alpha_{pk})\in\Delta^+ .$$

Moreover we have by (9) $w_{q_3}\cdots w_{qk}w_{pk}w_{qk}(\alpha_{pk})\in\Delta^-$. Hence there exists as before an integer t with $4\leqq t\leqq k$ such that

$$w_{q_t}\cdots w_{qk}w_{pk}w_{qk}w_{pk}=w_{q_{t-1}}w_{q_t}\cdots w_{qk}w_{pk}w_{qk} . \tag{12}$$

We distinguish two cases here according to $t>4$ or $t=4$.

Suppose $t>4$. Then, using our induction assumption twice, (*) is proved in a similar way as before, taking (10) into account.

Thus in the following we may assume $t=4$ in (12). We have then

$$\begin{aligned} w_{p_1}\cdots w_{pk}&=w_{q_1}\cdots w_{qk}\\ &=w_{q_2}\cdots w_{qk}w_{pk}\\ &=w_{q_3}\cdots w_{qk}w_{pk}w_{qk}\\ &=w_{q_4}\cdots w_{qk}w_{pk}w_{qk}w_{pk} . \end{aligned} \tag{13}$$

Hence we have $w_{q_2}\cdots w_{qk-1}=w_{q_4}\cdots w_{qk}w_{pk}$, which gives in turn

$$\Delta_{q_2}\cdots\Delta_{qk-1}=\Delta_{q_4}\cdots\Delta_{qk}\Delta_{pk} . \tag{14}$$

We distinguish two cases here according to $\theta=3\pi/4$ or $\theta>3\pi/4$.

Suppose now $\theta=3\pi/4$. Then $(w_{qk}w_{pk})^2=(w_{pk}w_{qk})^2$ and (13) imply

$$w_{q_4}\cdots w_{qk-1}w_{pk}=w_{q_3}\cdots w_{qk-1} .$$

Hence we have $\Delta_{q_4}\cdots\Delta_{qk-1}\Delta_{pk}=\Delta_{q_3}\cdots\Delta_{qk-1}$. Now we have $(\Delta_{qk}\Delta_{pk})^2=(\Delta_{pk}\Delta_{qk})^2$ since $\theta=3\pi/4$. Thus we get

$$\Delta_{q_4}\cdots\Delta_{qk-1}(\Delta_{qk}\Delta_{pk})^2=\Delta_{q_3}\cdots\Delta_{qk}\Delta_{pk}\Delta_{qk} .$$

Then we get (*) using (14) and (10).

Therefore, in the following we may assume that $\theta>3\pi/4$. Then we have $\theta=5\pi/6$. Hence we have by Lemma 2.5

$$w_{pk}(\alpha_{qk})\in\Delta^+,\ w_{qk}w_{pk}(\alpha_{qk})\in\Delta^+,\ w_{pk}w_{qk}w_{pk}(\alpha_{qk})\in\Delta^+,\ (w_{qk}w_{pk})^2(\alpha_{qk})\in\Delta^+ .$$

Moreover we have $w_{q_4}\cdots w_{qk-1}(w_{qk}w_{pk})^2(\alpha_{qk})\in\Delta^-$ by (13). Hence there is an integer s with $5\leqslant s\leqslant k$ such that

$$w_{q_s}\cdots w_{qk}(w_{pk}w_{qk})^2=w_{q_{s-1}}\cdots w_{qk-1}(w_{qk}w_{pk})^2 . \tag{15}$$

Let us distinguish two cases here according to $s>5$ or $s=5$.

Suppose $s>5$. Then analogous computation as before yields (*). Therefore in the following we may assume $s=5$. We have then

(16)
$$\begin{aligned} w_{p_1}\cdots w_{p_k} &= w_{q_1}\cdots w_{q_k} \\ &= w_{q_2}\cdots w_{q_k}w_{p_k} \\ &= w_{q_3}\cdots w_{q_k}w_{p_k}w_{q_k} \\ &= w_{q_4}\cdots w_{q_{k-1}}(w_{q_k}w_{p_k})^2 \\ &= w_{q_5}\cdots w_{q_k}(w_{p_k}w_{q_k})^2 . \end{aligned}$$

Hence we have also $w_{q_3}\cdots w_{q_{k-1}}=w_{q_5}\cdots w_{q_k}w_{p_k}$. Thus we get

(17)
$$\Delta_{q_3}\cdots\Delta_{q_{k-1}}=\Delta_{q_5}\cdots\Delta_{q_k}\Delta_{p_k} .$$

Now since $\theta=5\pi/6$, we have by Lemma 2.5

$$w_{q_k}(\alpha_{p_k})\in\Delta^+,\ w_{p_k}w_{q_k}(\alpha_{p_k})\in\Delta^+,\ w_{q_k}w_{p_k}w_{q_k}(\alpha_{p_k})\in\Delta^+ ,$$
$$(w_{p_k}w_{q_k})^2(\alpha_{p_k})\in\Delta^+,\ w_{q_k}(w_{p_k}w_{q_k})^2(w_{p_k})\in\Delta^+ .$$

On the other hand we have by (16) $w_{q_5}\cdots w_{q_k}(w_{p_k}w_{q_k})^2(\alpha_{p_k})\in\Delta^-$. Then there is an integer h with $6\leqq h\leqq k$ such that

(18)
$$w_{q_h}\cdots w_{q_k}(w_{p_k}w_{q_k})^2w_{p_k}=w_{q_{h-1}}w_{q_h}\cdots w_{q_k}(w_{p_k}w_{q_k})^2 ,$$

i.e.

(19)
$$w_{q_h}\cdots w_{q_{k-1}}(w_{q_k}w_{p_k})^3=w_{q_{h-1}}\cdots w_{q_{k-1}}(w_{q_k}w_{p_k})^2w_{q_k} .$$

We distinguish two cases here according to $h>6$ or $h=6$.

Suppose $h>6$. Then we obtain (*) by using our induction assumption.

Therefore, finally we may assume $h=6$ in (19). We have then

(20)
$$\begin{aligned} w_{p_1}\cdots w_{p_k} &= w_{q_1}\cdots w_{q_k} \\ &= w_{q_2}\cdots w_{q_k}w_{p_k} \\ &= w_{q_3}\cdots w_{q_k}w_{p_k}w_{q_k} \\ &= w_{q_4}\cdots w_{q_{k-1}}(w_{q_k}w_{p_k})^2 \\ &= w_{q_5}\cdots w_{q_{k-1}}(w_{q_k}w_{p_k})^2w_{q_k} \\ &= w_{q_6}\cdots w_{q_{k-1}}(w_{q_k}w_{p_k})^3 . \end{aligned}$$

Hence we have $w_{q_6}\cdots w_{q_{k-1}}w_{q_k}w_{p_k}=w_{q_4}\cdots w_{q_{k-1}}$. Thus we get

(21)
$$\Delta_{q_6}\cdots\Delta_{q_k}\Delta_{p_k}=\Delta_{q_4}\cdots\Delta_{q_{k-1}} .$$

Now we have $(w_{q_k}w_{p_k})^3=(w_{p_k}w_{q_k})^3$ since $\theta=5\pi/6$, hence we get from (20) $w_{q_6}\cdots w_{q_{k-1}}(w_{p_k}w_{q_k})=w_{q_5}\cdots w_{q_k}$. Thus we get

(22)
$$\Delta_{q_6}\cdots\Delta_{q_{k-1}}\Delta_{p_k}\Delta_{q_k}=\Delta_{q_5}\cdots\Delta_{q_k} .$$

On the other hand we have $(\Delta_{p_k}\Delta_{q_k})^3=(\Delta_{q_k}\Delta_{p_k})^3$ since $\theta=5\pi/6$. Then we have easily from (22) $\Delta_{q_6}\cdots\Delta_{q_{k-1}}(\Delta_{q_k}\Delta_{p_k})^3=\Delta_{q_5}\cdots\Delta_{q_k}(\Delta_{p_k}\Delta_{q_k})^2$. Then we get (*) using the equations (21), (17), (14) and (11), Q.E.D.

COROLLARY 2.7. *Let Θ be the group generated by l symbols $\Delta_1, \cdots, \Delta_l$ together with the defining relations:*

(i) $\Delta_i^2=1$, $\quad i=1, \cdots, l$

(ii) $\Delta_i\Delta_j=\Delta_j\Delta_i$, $\quad$ *if* $\theta_{ij}=\pi/2$,

(iii) $\Delta_i\Delta_j\Delta_i=\Delta_j\Delta_i\Delta_j$, $\quad$ *if* $\theta_{ij}=2\pi/3$,

(iv) $(\Delta_i\Delta_j)^2=(\Delta_j\Delta_i)^2$, $\quad$ *if* $\theta_{ij}=3\pi/4$,

(v) $(\Delta_i\Delta_j)^3=(\Delta_j\Delta_i)^3$, $\quad$ *if* $\theta_{ij}=5\pi/6$,

where θ_{ij} is the angle between two simple roots α_i and α_j.

Let $\varphi : \Theta \to W$ be the homomorphism defined by $\varphi(\Delta_i)=w_i$ for $i=1, \cdots, l$. Then φ is bijective and we have $\Theta \cong W$.

PROOF. Let $\mathfrak{F}_0$ be a subset of $\mathfrak{F}$ such that the map $\lambda \to w(\lambda)$ from $\mathfrak{F}$ onto W is bijective on $\mathfrak{F}_0$. Denote by Θ_0 the subset of Θ consisting of 1 and the $\Delta(\lambda)$, $\lambda \in \mathfrak{F}_0$, where $\Delta(\lambda)$ means $\Delta_{i_1} \cdots \Delta_{i_r}$ if $\lambda=(i_1, \cdots, i_r)$. Since $\varphi(1)=1$, $\varphi(\Delta(\lambda))=w(\lambda)$, φ is bijective on Θ_0. Hence it is sufficient to show that $\Theta=\Theta_0$. Now since every Δ_i is contained in Θ_0, it is enough to show that Θ_0 is a subgroup of Θ.

Let $\lambda=(i_1, \cdots, i_r) \in \mathfrak{F}_0$. Then $w(\lambda)^{-1}=w(\mu)$ where $\mu=(i_r, \cdots, i_1)$. Since $n(w(\lambda)^{-1})=n(w(\lambda))=r$, μ is in $\mathfrak{F}$. Hence there exists an element ν in $\mathfrak{F}_0$ such that $\mu \sim \nu$. By Theorem 2.6, we have then $\Delta(\mu)=\Delta(\nu)$. Hence $\Delta(\lambda)^{-1} \in \Theta_0$.

Thus it is enough to show that $\Delta(\lambda)\cdot\Delta(\mu) \in \Theta_0$ for any two elements λ, μ in $\mathfrak{F}_0$. This will be the case if we show that $\Delta(\lambda)\cdot\Delta_i \in \Theta_0$ for any $\lambda \in \mathfrak{F}_0$ and for any i, $1 \leqq i \leqq l$. Let $\lambda=(i_1, \cdots, i_r)$ and suppose $\lambda'=(i_1, \cdots, i_r, i)$ is an admissible sequence. Then there exists an element $\mu \in \mathfrak{F}_0$ such that $\lambda' \sim \mu$. Hence we get $\Delta(\lambda)\Delta_i=\Delta(\lambda')=\Delta(\mu) \in \Theta_0$. Suppose $\lambda'=(i_1, \cdots, i_r, i)$ is not admissible. By Lemma 2.2 and Lemma 2.3 there exists an element μ in $\mathfrak{F}$ such that $\lambda \sim \mu$, $\mu=(j_1, \cdots, j_r)$, $j_r=i$. Hence we have

$$\Delta(\lambda)\Delta_i=\Delta_{j_1} \cdots \Delta_{j_{r-1}}\Delta_i\Delta_i=\Delta_{j_1} \cdots \Delta_{j_{r-1}}$$

Since $\mu'=(j_1, \cdots, j_{r-1})$ is clearly admissible, there is an element ν in $\mathfrak{F}_0$ such that $\mu' \sim \nu$. Then we have by Theorem 2.6 $\Delta_{j_1} \cdots \Delta_{j_{r-1}}=\Delta(\nu) \in \Theta_0$, Q.E.D.

§ 3. The Hecke ring of a Chevalley group over a finite field with respect to a Borel subgroup.

Let $\mathfrak{g}$ be a complex semi-simple Lie algebra. We use the same notations $\mathfrak{h}, \Delta, \Pi, W$ etc. as in § 2. Let K be a field. C. Chevalley constructed in [2] for the pair $\mathfrak{g}$, K a group G. In the following we use the notations in [2]. In particular, the subgroups $\mathfrak{U}, \mathfrak{H}$ and $\{x_\alpha(t);\ t \in K\}=\mathfrak{X}_\alpha$ (the one parameter subgroup associated to the root α) of G will play important roles. Also we fix a map $w \to \omega(w)$ from W into the subgroup $\mathfrak{W}$ of G which satisfies $\zeta(\omega(w))=w$ $(w \in W)$ where $\zeta : \mathfrak{W} \to W$

is the homomorphism defined in [2 p. 37]. Now we consider the case where K is a finite field F_q consiting of q elements.

Let us denote by B the subgroup $\mathfrak{U}\mathfrak{H}$ of G (the Borel subgroup) and consider the Hecke ring $\mathcal{H}(G, B)$.

LEMMA 3.1. *For any element x in G, there exists one and only one element w in W such that $BxB=B\omega(w)B$. Moreover we have*

$$\mathrm{ind}\,(x)=q^{n(w)}$$

where $n(w)=|\Delta_w^+|$.

PROOF. G can be expressed as a disjoint union:

$$G=\bigcup_{w\in W}\mathfrak{U}\mathfrak{H}\omega(w)\mathfrak{U}_w''$$

(the Bruhat decomposition. see [2, p. 42]). Since $\mathfrak{U}_w''\subset\mathfrak{U}\subset B$, we have $G=\bigcup_{w\in W}B\omega(w)B$. Now this is a disjoint union. In fact, if $B\omega(w)B=B\omega(w')B$, then $\omega(w')=b_1\omega(w)b_2$ for some b_1, b_2 in B. Put $b_2=hu$, $h\in\mathfrak{H}$, $u\in\mathfrak{U}$. Then since $\mathfrak{H}\omega(w)=\omega(w)\mathfrak{H}$ (cf. [2, p. 36]) we may write $\omega(w)h=h'\omega(w)$ for some $h'\in\mathfrak{H}$. Put $u=u'u''$, $u'\in\mathfrak{U}_w'$, $u''\in\mathfrak{U}_w''$. Then by $\omega(w)\mathfrak{U}_w'\omega(w)^{-1}\subset\mathfrak{U}$ (cf. [2, p. 42]), we have $\omega(w)u'=u_1\omega(w)$ for some $u_1\in\mathfrak{U}$. Hence

$$\omega(w')=b_1h'\omega(w)u'u''=b_1h'u_1\omega(w)u''.$$

Now clearly $b_1h'u_1$ is in $B=\mathfrak{U}\mathfrak{H}$. Hence by the uniqueness of the decomposition of an element in $\mathfrak{U}\mathfrak{H}\omega(w)\mathfrak{U}_w''$ as a product of elements in $\mathfrak{U}$, $\mathfrak{H}$, $\omega(w)\mathfrak{U}_w''$ (cf. [2, Th. 2]) we have

$$b_1h'u_1=1,\ \omega(w')=\omega(w),\ u''=1.$$

Since $\omega: W\to\mathfrak{W}$ satisfies $\zeta\circ\omega=id.$, we have $w'=w$.

To show that $\mathrm{ind}\,(x)=q^{n(w)}$ for $x\in B\omega(w)B$, it is enough to show that $\mathrm{ind}\,(\omega(w))=q^{n(w)}$ since $\mathrm{ind}\,(bxb')=\mathrm{ind}\,(x)$ for any $b, b'\in B$. (cf. § 1) Now we have

$$\begin{aligned}B\cap\omega(w)B\omega(w)^{-1}&=\mathfrak{H}\mathfrak{U}\cap\omega(w)(\mathfrak{H}\mathfrak{U}_w'\mathfrak{U}_w'')\omega(w)^{-1}\\&=\mathfrak{H}\mathfrak{U}\cap\mathfrak{H}\omega(w)\mathfrak{U}_w'\mathfrak{U}_w''\omega(w)^{-1}.\end{aligned}$$

Put $K'=\omega(w)\mathfrak{U}_w'\omega(w)^{-1}$, $K''=\omega(w)\mathfrak{U}_w''\omega(w)^{-1}$. Then we have

$$B\cap\omega(w)B\omega(w)^{-1}=\mathfrak{H}\mathfrak{U}\cap\mathfrak{H}K'K''.$$

By the formulas (cf. [2, p. 36, p. 35])

$$h(\chi)x_\alpha(t)h(\chi)^{-1}=x_\alpha(\chi(\alpha)t),\quad \omega(w)x_\alpha(t)\omega(w)^{-1}=x_{w(\alpha)}(\pm t),$$

$\mathfrak{H}K'$ is a subgroup of $\mathfrak{H}\mathfrak{U}$ and K' is a normal subgroup of $\mathfrak{H}K'$. Also K'' is a subgroup of $\mathfrak{U}$. Hence we have

$$B\cap\omega(w)B\omega(w)^{-1}=(\mathfrak{H}K')(\mathfrak{H}\mathfrak{U}\cap K'').$$

Now since $\mathfrak{H}\mathfrak{U}\cap\mathfrak{B}=1$ (cf. [2, p. 42]), we have

$$\mathrm{ind}\,(\omega(w)^{-1})=[B:\mathfrak{H}K']=[\mathfrak{U}:K']=[\mathfrak{U}:\mathfrak{U}'_w]=[\mathfrak{U}''_w:1]=q^{n(w)}.$$

On the other hand, $\omega(w)^{-1}\in\mathfrak{H}\omega(w^{-1})$. Thus we get $\mathrm{ind}\,(\omega(w^{-1}))=q^{n(w)}$ for any $w\in W$. Now $\Delta^+_{w^{-1}}=-w^{-1}\Delta^+_w$ implies that $n(w)=n(w^{-1})$ which completes the proof.

In the following, we shall denote the element $\chi_{B\omega(w)B}$ of $\mathscr{H}(G,B)$ (in the notation of § 1) by $S(w)$. Also we denote $S(w_i)$ by S_i. The unit element $S(1)$ of $\mathscr{H}(G,B)$ is denoted by 1. Also for the sake of simplicity, we omit the symbol $*$ in the convolution product when we consider the product in the ring $\mathscr{H}(G,B)$. We have then $\mathrm{ind}\,(S(w))=q^{n(w)}$ (for any $w\in W$).

THEOREM 3.2. (i) *The $S(w)$, $w\in W$, form a base of the free $\boldsymbol{Z}$-module $\mathscr{H}(G,B)$.*

(ii) *If $w=w_{i_1}\cdots w_{i_r}$ is a reduced expression for $w\in W$, then*

$$S(w)=S_{i_1}\cdots S_{i_r}.$$

Consequently $1,S_1,\cdots,S_l$ generate the ring $\mathscr{H}(G,B)$.

(iii) *The generators $1,S_1,\cdots,S_l$ satisfy the following relations.*

$$(\sharp)\qquad\begin{cases}1\cdot S_i=S_i\cdot 1=S_i, & (i=1,\cdots,l)\\ S_i^2=q\cdot 1+(q-1)\cdot S_i, & (i=1,\cdots,l)\\ S_iS_j=S_jS_i, & \text{if } \theta_{ij}=\pi/2,\\ S_iS_jS_i=S_jS_iS_j, & \text{if } \theta_{ij}=2\pi/3,\\ (S_iS_j)^2=(S_jS_i)^2, & \text{if } \theta_{ij}=3\pi/4,\\ (S_iS_j)^3=(S_jS_i)^3, & \text{if } \theta_{ij}=5\pi/6.\end{cases}$$

PROOF. (i) Obvious by Lemma 3.1.

(ii) Put $v_1=w_{i_1}$, $v_2=w_{i_1}w_{i_2},\cdots$, $v_r=w_{i_1}\cdots w_{i_r}=w$. Then these are reduced expressions for $v_1,v_2,\cdots,v_r$ respectively (Lemma 2.2 and Lemma 2.3.). Then we get $n(v_i)=i$ $(i=1,\cdots,r)$. Then we have by Lemma 3.1, $\mathrm{ind}\,(\omega(v_i))=q^i$ for $i=1,\cdots,r$. Now since $\omega(v_j)\equiv\omega(w_{i_1})\cdots\omega(w_{i_j})$ mod. $\mathfrak{H}$, we have

$$\mathrm{ind}\,(\omega(w_{i_1})\cdots\omega(w_{i_j}))=q^i=\mathrm{ind}\,(\omega(w_{i_1})\cdots\omega(w_{i_{j-1}}))\cdot\mathrm{ind}\,(\omega(w_{i_j})).$$

Then by Lemma 1.2, we get

$$S(v_{j-1})S(w_{ij})=S(v_j)\quad\text{for } j=2,\cdots,r.$$

Hence we have $S(w)=S_{i_1}S_{i_2}\cdots S_{i_r}$, Q.E.D.

(iii) By (ii) and Lemma 2.4, these relations are obvious except $S_i^2=q\cdot 1+(q-1)\cdot S_i$. Let $K=B\cap\omega(w_i)^{-1}B\omega(w_i)$. Then since $w_i^2=1$, we have $\omega(w_i)^{-1}\equiv\omega(w_i)$ mod. $\mathfrak{H}$ and $K=B\cap\omega(w_i)B\omega(w_i)^{-1}=\mathfrak{H}\omega(w_i)\mathfrak{U}'_{w_i}\omega(w_i)^{-1}$ (see the proof of Lemma 3.1.). Now $\mathfrak{U}'_{w_i}$ is generated by the $x_\alpha(t)$ $(\alpha\in\Delta^+-\{\alpha_i\},\ t\in\boldsymbol{F}_q)$. Then we have $\omega(w_i)\mathfrak{U}'_{w_i}\omega(w_i)^{-1}=\mathfrak{U}'_{w_i}$

since $w_i(\Delta^+-\{\alpha_i\})=\Delta^+-\{\alpha_i\}$. Thus we have $K=\mathfrak{H}\mathfrak{U}'_{w_i}$. Hence by $\mathfrak{U}=\mathfrak{U}'_{w_i}\mathfrak{U}''_{w_i}$ we obtain $B=K\mathfrak{U}''_{w_i}$. Clearly $\mathfrak{U}''_{w_i}=\mathfrak{X}_{\alpha_i}=\{x_{\alpha_i}(t)\,;\,t\in\boldsymbol{F}_q\}$. Then we get $K\cap\mathfrak{U}''_{w_i}=1$. In fact, if $hu'=u''$ for some $h\in\mathfrak{H}$, $u'\in\mathfrak{U}'_{w_i}$, $u''\in\mathfrak{U}''_{w_i}$, then $h=u''u'^{-1}$ and we get $h=u'=u''=1$ since $\mathfrak{H}\cap\mathfrak{U}=1$, $\mathfrak{U}'_{w_i}\cap\mathfrak{U}''_{w_i}=1$ (cf. [2, p. 41~42]). Thus we get the following disjoint unions:

$$B=\bigcup_t Kx_{\alpha_i}(t),\quad B\omega(w_i)B=\bigcup_t B\omega(w_i)x_{\alpha_i}(t)\quad(t\in\boldsymbol{F}_q).$$

Hence

$$\begin{aligned}B\omega(w_i)BB\omega(w_i)B&=B\omega(w_i)B\omega(w_i)B=\bigcup_t B\omega(w_i)x_{\alpha_i}(t)\omega(w_i)B\\&=\bigcup_t B\omega(w_i)x_{\alpha_i}(t)\omega(w_i)^{-1}B=\bigcup_t Bx_{-\alpha_i}(t)B.\end{aligned}$$

since $\omega(w_i)^{-1}\mathfrak{H}=\omega(w_i)\mathfrak{H}$ and $\omega(w_i)x_{\alpha_i}(t)\omega(w_i)^{-1}=x_{-\alpha_i}(\pm t)$. Now $x_{-\alpha_i}(t)\in B\omega(w_i)B$ if $t\neq0$. In fact, using the homomorphism

$$\phi_{\alpha_i}:SL(2,\boldsymbol{F}_q)\to G\quad\text{(see [2, p. 36])}$$

and

$$\begin{pmatrix}1&-t\\0&1\end{pmatrix}\begin{pmatrix}t&0\\0&t^{-1}\end{pmatrix}\begin{pmatrix}1&0\\t&1\end{pmatrix}\begin{pmatrix}1&-t^{-1}\\0&1\end{pmatrix}\begin{pmatrix}-1&0\\0&-1\end{pmatrix}=\begin{pmatrix}0&1\\-1&0\end{pmatrix},$$

we have $x_{-\alpha_i}(t)=\phi_{\alpha_i}\begin{pmatrix}1&0\\t&1\end{pmatrix}\in B\omega(w_i)B$ since $\phi_{\alpha_i}\begin{pmatrix}z&0\\0&z^{-1}\end{pmatrix}\in\mathfrak{H}$, $\phi_{\alpha_i}\begin{pmatrix}1&t\\0&1\end{pmatrix}=x_{\alpha_i}(t)$, $\phi_{\alpha_i}\begin{pmatrix}0&1\\-1&0\end{pmatrix}\equiv\omega(w_i)$ mod. $\mathfrak{H}$. Thus $B\omega(w_i)BB\omega(w_i)B=B\cup B\omega(w_i)B$. From this and $(B\omega(w_i)B)^{-1}=B\omega(w_i)^{-1}B=B\omega(w_i)B$ we see that $B\cup B\omega(w_i)B$ is a subgroup of G. Also by § 1, we see that

$$S_i^2=\lambda\cdot1+\mu\cdot S_i,$$

where λ,μ are positive integers. Let us determine λ and μ using Lemma 1.3. Firstly

$$\lambda=\frac{\operatorname{ind}(\omega(w_i))}{\operatorname{ind}(1)}\,\#\{t\in\boldsymbol{F}_q\,;\,B\omega(w_i)x_{\alpha_i}(t)\omega(w_i)B=B\}=q,$$

because we have $B\omega(w_i)x_{\alpha_i}(t)\omega(w_i)B=B\omega(w_i)x_{\alpha_i}(t)\omega(w_i)^{-1}B$ and this is equal to B if and only if $t=0$ (since $\omega(w_i)x_{\alpha_i}(t)\omega(w_i)^{-1}=x_{-\alpha_i}(\pm t)$). Secondly we have

$$\begin{aligned}\mu&=\frac{\operatorname{ind}(\omega(w_i))}{\operatorname{ind}(\omega(w_i))}\,\#\{t\in\boldsymbol{F}_q\,;\,B\omega(w_i)x_{\alpha_i}(t)\omega(w_i)B=B\omega(w_i)B\}\\&=\#\{t\in\boldsymbol{F}_q\,;\,\omega(w_i)x_{\alpha_i}(t)\omega(w_i)^{-1}\in B\omega(w_i)B\}.\end{aligned}$$

As we have seen above, $t\neq0$ implies that $\omega(w_i)x_{\alpha_i}(t)\omega(w_i)^{-1}=x_{-\alpha_i}(\pm t)\in B\omega(w_i)B$. Of course $t\neq0$ implies that $\omega(w_i)x_{\alpha_i}(t)\omega(w_i)^{-1}\in B$. Thus we get $\mu=q-1$, which completes the proof.

REMARK. (i) Theorem 3.2 is also valid for the pair G', B', where G' is the

group denoted also by G' in Chevalley [2, p. 47] and B' is the corresponding Borel subgroup, i.e. $B'=\mathfrak{H}'\mathfrak{U}$, where $\mathfrak{H}'$ is the subgroup of $\mathfrak{H}$ defined in [2, p. 47].
(ii) Theorem 3.2 is also valid for the pair Δ, B, where Δ is the group recently constructed by R. Steinberg [7]. Because all the tools needed to prove Theorem 3.2 exist also in this case.

§ 4. A characterization of the ring $\mathscr{H}(G, B)$ in terms of generators and defining relations.

In § 3 we have shown that $\mathscr{H}(G, B)$ is generated over $\boldsymbol{Z}$ by $1, S_1, \cdots, S_l$ and these generators satisfy (♯) of § 3. Of course by Theorem 3.2 (i) the rank of the free $\boldsymbol{Z}$-module $\mathscr{H}(G, B)$ is equal to the order of the Weyl group W.

In this section we shall prove that (♯) form the *defining relations* for the ring $\mathscr{H}(G, B)$. Namely, let $\mathfrak{R}$ be the ring over $\boldsymbol{Z}$ generated by $1, \Delta_1, \cdots, \Delta_l$ together with the defining relations (♯). (Of course each S_i should be replaced by Δ_i in (♯).) Then there is a homomorphism $\varphi : \mathfrak{R} \to \mathscr{H}(G, B)$ such that $\varphi(1)=1$, $\varphi(\Delta_i)=S_i$ $(i=1, \cdots, l)$. We shall show that φ is a bijective map.

Let $\mathfrak{F}_0$ be a subset of the set $\mathfrak{F}$ of all admissible sequences such that the map $\lambda \to w(\lambda)$ from $\mathfrak{F}$ onto W (defined in § 2) induces a bijection from $\mathfrak{F}_0$ onto W. Let $\mathfrak{R}_0$ be the $\boldsymbol{Z}$-submodule of $\mathfrak{R}$ spanned by $\{1\} \cup \{\Delta(\lambda)\,;\, \lambda \in \mathfrak{F}_0\}$, where the map $\lambda \to \Delta(\lambda)$ from $\mathfrak{F}$ into $\mathfrak{R}$ is defined by $\Delta(\lambda)=\Delta_{i_1} \cdots \Delta_{i_r}$ for $\lambda=(i_1, \cdots, i_r) \in \mathfrak{F}$. Then the restriction $\varphi|\mathfrak{R}_0$ of φ on $\mathfrak{R}_0$ is a bijective map from $\mathfrak{R}_0$ onto $\mathscr{H}(G, B)$. In fact, if we have

$$\nu \cdot 1 + \sum_{\lambda \in \mathfrak{F}_0} \nu_\lambda \cdot \Delta(\lambda) = 0\,, \quad (\nu, \nu_\lambda \in \boldsymbol{Z})$$

then taking φ-images, we have $\nu \cdot 1 + \sum_{\lambda \in \mathfrak{F}_0} \nu_\lambda \cdot S(\lambda) = 0$, where $S(\lambda)=S_{i_1} \cdots S_{i_r}$ for $\lambda=(i_1, \cdots, i_r)$. Now, since 1 and the $S(\lambda)$, $\lambda \in \mathfrak{F}_0$ form a basis of the free $\boldsymbol{Z}$-module $\mathscr{H}(G, B)$, we have $\nu=0$ and $\nu_\lambda=0$ for all $\lambda \in \mathfrak{F}_0$. Hence $\varphi|\mathfrak{R}_0$ is injective. By Theorem 3.2, $\varphi|\mathfrak{R}_0$ is also surjective. Thus $\varphi|\mathfrak{R}_0$ is bijective. So we have only to show that $\mathfrak{R}_0=\mathfrak{R}$.

Now since $1, \Delta_1, \cdots, \Delta_l$ are all contained in $\mathfrak{R}_0$, it is enough to show that $\mathfrak{R}_0$ is a subring of $\mathfrak{R}$. Let us show that $\Delta(\lambda) \cdot \Delta_i \in \mathfrak{R}_0$ for any $\lambda \in \mathfrak{F}_0$ and for any integer i between 1 and l. (Then we have clearly $\Delta(\lambda) \cdot \Delta(\mu) \in \mathfrak{R}_0$ for any λ, μ in $\mathfrak{F}_0$.) Let $\lambda=(i_1, \cdots, i_r) \in \mathfrak{F}_0$. If the sequence $\lambda'=(i_1, \cdots, i_r, i)$ is admissible, then there is an admissible sequence μ in $\mathfrak{F}_0$ such that $\lambda' \sim \mu$. Then by Theorem 2.6 we have $\Delta(\lambda')=\Delta(\mu)$. Hence we get $\Delta(\lambda) \cdot \Delta_i = \Delta(\lambda') \in \mathfrak{R}_0$. Now suppose that the sequence $\lambda'=(i_1, \cdots, i_r, i)$ is not admissible. Then by Lemmas 2.2, 2.3 the simple root α_i belongs to Δ_w^+ where $w=w_{i_1} \cdots w_{i_r}$. Hence there exists an element $\mu=(j_1, \cdots, j_r)$ in $\mathfrak{F}$ such that $\lambda \sim \mu$ and $j_r=i$. Then we get

$$\begin{aligned}\Delta(\lambda)\cdot\Delta_i=\Delta(\mu)\cdot\Delta_i&=\Delta_{j_1}\cdots\Delta_{j_{r-1}}\Delta_i^2\\&=\Delta_{j_1}\cdots\Delta_{j_{r-1}}(q\cdot 1+(q-1)\Delta_i)\\&=q\cdot\Delta_{j_1}\cdots\Delta_{j_{r-1}}+(q-1)\Delta(\mu)\,.\end{aligned}$$

Now since $\mu'=(j_1,\cdots,j_{r-1})$ is also admissible, there exists an admissible sequence ν in $\mathfrak{S}_0$ such that $\mu'\sim\nu$. Then we have

$$\Delta(\lambda)\cdot\Delta_i=q\cdot\Delta(\nu)+(q-1)\cdot\Delta(\lambda)\in\mathfrak{R}_0\,.$$

Thus we have proved the main theorem of this note:

THEOREM 4.1. *The Hecke ring $\mathscr{H}(G,B)$ is generated by $1,S_1,\cdots,S_l$ together with the defining relations (♯).*

COROLLARY 4.2. *The elements $S(w)$ of $\mathscr{H}(G,B)$ satisfy the following relations.*

$$\begin{aligned}&S(w)S_i=q\cdot S(ww_i)+(q-1)\cdot S(w)\,, && \text{if } \alpha_i\in\Delta_w^+\,,\\&S(w)S_i=S(ww_i)\,, && \text{if } \alpha_i\notin\Delta_w^+\,.\end{aligned}$$

PROOF. Obvious from the proof of Theorem 4.1.

§ 5. Applications.

THEOREM 5.1. *Let $Sp(n,\boldsymbol{F}_q)$ be the symplectic group of degree $2n$ over the finite field $\boldsymbol{F}_q$: $Sp(n,\boldsymbol{F}_q)=\{x\in GL(2n,\boldsymbol{F}_q)\,;\,{}^txJx=J\}$ where $J=(a_{ij})$ is a matrix of degree $2n$ given by*

$$a_{ij}=\begin{cases}1 & \text{if } i+j=2n+1,\ 1\leqq i\leqq n\\-1 & \text{if } i+j=2n+1,\ n+1\leqq i\leqq 2n\\0 & \text{otherwise}\,.\end{cases}$$

Let B be the subgroup of $Sp(n,\boldsymbol{F}_q)$ defined by $B=Sp(n,\boldsymbol{F}_q)\cap T(2n,\boldsymbol{F}_q)$, where $T(2n,\boldsymbol{F}_q)$ is the subgroup of $GL(2n,\boldsymbol{F}_q)$ consisting of all upper triangular matrices. Let $SO(2n+1,\boldsymbol{F}_q)$ be the special orthogonal group of degree $2n+1$ over $\boldsymbol{F}_q$ defined by $SO(2n+1,\boldsymbol{F}_q)=\{x\in SL(2n+1,\boldsymbol{F}_q)\,;\,{}^txJ'x=J'\}$ where $J'=(b_{ij})$ is a matrix of degree $2n+1$ defined by

$$b_{ij}=\begin{cases}1 & \text{if } i+j=2n+2\\0 & \text{otherwise}\,.\end{cases}$$

Let B' be the subgroup of $SO(2n+1,\boldsymbol{F}_q)$ defined by $B'=SO(2n+1,\boldsymbol{F}_q)\cap T(2n+1,\boldsymbol{F}_q)$.

Then $\mathscr{H}(Sp(n,\boldsymbol{F}_q),B)\cong\mathscr{H}(SO(2n+1,\boldsymbol{F}_q),B')$. if $2\nmid q$.

PROOF. As we have remarked in § 1, if N is a normal subgroup of G such that $G\supset H\supset N$, where H is a subgroup of G satisfying the condition (A), then we have $\mathscr{H}(G,H)\cong\mathscr{H}(G/N,H/N)$ canonically. Thus Theorem 4.1 is still valid for $\mathscr{H}(Sp(n,\boldsymbol{F}_q),B)$ and for $\mathscr{H}(SO(2n+1,\boldsymbol{F}_q),B')$ because the corresponding Chevalley groups are obtained from $Sp(n,\boldsymbol{F}_q)$, $SO(2n+1,\boldsymbol{F}_q)$ by taking the quotient groups

with respect to the center (see E. Abe [1], R. Ree [3]).

Now by the well known inversion relation between the root systems of B_n, C_n i.e. that of Dynkin diagrams gives the same relation for the generators $w_1, \cdots, w_n$ of their Weyl groups. Hence the corresponding generators of the Hecke ring satisfy the same relations. Thus we get the isomorphism of the Hecke rings, Q.E.D.

COROLLARY 5.2. *Let ρ be the complex linear representation of $Sp(n, \boldsymbol{F}_q)$ induced by the trivial representation of B and let $\rho = m_1\rho_1 + m_2\rho_2 + \cdots + m_r\rho_r$ be the decomposition of ρ into irreducible representations $\rho_1, \cdots, \rho_r$ with multiplicities $m_1, \cdots, m_r$. Also let σ be the complex linear representation of $SO(2n+1, \boldsymbol{F}_q)$ induced by the trivial representation of B' and let $\sigma = m'_1\sigma_1 + m'_2\sigma_2 + \cdots + m'_s\sigma_s$ be the decomposition of σ into irreducible representations $\sigma_1, \cdots, \sigma_s$ with multiplicities $m'_1, \cdots, m'_s$. Then $r=s$ and we have $m_1 = m'_1, \cdots, m_r = m'_r$ for a suitable ordering of indices.*

PROOF. Since $\mathcal{H}_C(Sp(n, \boldsymbol{F}_q), B) \cong \mathcal{H}_C(SO(2n+1, \boldsymbol{F}_q), B')$, this is a immediate consequence of Cor. 1.5.

As the second application of Theorem 4.1, we shall determine the set $\mathrm{Hom}(\mathcal{H}(G, B), \boldsymbol{C})$. (The homomorphism considered here should map the unit element of $\mathcal{H}(G, B)$ into the unit element of $\boldsymbol{C}$.) Let *sgn* be the map which sends S_i into -1 for all i. Then it is easy to verify that *sgn* preserves all the relations in (♯). Thus *sgn* is in the set $\mathrm{Hom}(\mathcal{H}(G, B), \boldsymbol{C})$.

If the complex semi-simple Lie algebra $\mathfrak{g}$ is decomposed into a direct sum of simple Lie algebras $\mathfrak{g}_1, \cdots, \mathfrak{g}_r$, then it is easy to see that the corresponding Chevalley group G is decomposed into the direct product of corresponding Chevalley groups $G_1, \cdots, G_r$ and the Borel subgroup B is also decomposed into direct product of corresponding Borel groups $B_1, \cdots, B_r$. Hence we get easily

$$\mathcal{H}(G, B) \cong \mathcal{H}(G_1, B_1) \underset{Z}{\otimes} \mathcal{H}(G_2, B_2) \underset{Z}{\otimes} \cdots \underset{Z}{\otimes} \mathcal{H}(G_r, B_r) .$$

Thus we may consider only the case where $\mathfrak{g}$ is simple. Then using Theorem 4.1, we get easily the

THEOREM 5.3. (i) *If $\mathfrak{g}$ is of type $A_l (l \geqq 1)$, $D_l (l \geqq 4)$, $E_l (l = 6, 7, 8)$, then* $\mathrm{Hom}(\mathcal{H}(G, B), \boldsymbol{C})$ *consists of two elements ind and sgn.*

(ii) *If $\mathfrak{g}$ is of type $B_l (l \geqq 2)$, $C_l (l \geqq 3)$, G_2, F_4, then* $\mathrm{Hom}(\mathcal{H}(G, B), \boldsymbol{C})$ *consists of four elements ind, sgn, φ and ψ. More precisely*

$$\begin{cases} \varphi(S_1) = \cdots = \varphi(S_{l-1})q\,, \quad \varphi(S_l) = -1 \\ \psi(S_1) = \cdots = \psi(S_{l-1}) = -1\,, \quad \psi(S_l) = q \end{cases} \qquad (\textit{if } \mathfrak{g} \textit{ is of type } B_l, C_l)$$

$$\begin{cases} \varphi(S_1) = q\,, \quad \varphi(S_2) = -1 \\ \psi(S_1) = -1\,, \quad \psi(S_2) = q \end{cases} \qquad (\textit{if } \mathfrak{g} \textit{ is of type } G_2)$$

$$\begin{cases} \varphi(S_1)=\varphi(S_2)=q\,, & \varphi(S_3)=\varphi(S_4)=-1 \\ \psi(S_1)=\psi(S_2)=-1\,, & \psi(S_3)=\psi(S_4)=q \end{cases} \qquad (\textit{if } \mathfrak{g} \textit{ is of type } F_4)$$

We shall give finally an involutive automorphism of the ring $\mathcal{H}(G, B)$ which interchanges ind and sgn, and also φ and ψ if they exist. This involution is due to O. Goldman.

Put $\widehat{S}_i=(q-1)\cdot 1-S_i$ $(i=1,\cdots,l)$. Then we have $\widehat{S}_i=-q\cdot S_i^{-1}$ in $\mathcal{H}_Q(G, B)$ and it is easy to verify that $\widehat{S}_1,\cdots\widehat{S}_l$ satisfy the relation (♯). Thus we get a homomorphism of the ring $\mathcal{H}(G, B)$ which maps S_i to $\widehat{S}_i$ for $i=1,\cdots,l$. We denote this homomorphism by $S\to\widehat{S}$ $(S\in\mathcal{H}(G, B))$.

THEOREM 5.4. (i) *$S\to\widehat{S}$ is an involutive automorphism of the ring $\mathcal{H}(G, B)$:* $\widehat{\widehat{S}}=S$

(ii) $\widehat{S(w)}=\mathrm{sgn}(S(w))\,\mathrm{ind}(S(w))\,S(w)^{-1}$ *for every* $w\in W$. *(in the ring $\mathcal{H}_Q(G, B)$.)*

(iii) $\mathrm{ind}(\widehat{S})=\mathrm{sgn}(S)$, $\mathrm{sgn}(\widehat{S})=\mathrm{ind}(S)$ *for every* $S\in\mathcal{H}(G, B)$.

(iv) *If G is of simple type and of type B_l, C_l, G_2, F_4, then*

$$\varphi(\widehat{S})=\psi(S),\ \psi(\widehat{S})=\varphi(S).$$

PROOF. (i) It is enough to show that $\widehat{\widehat{S}}_i=S_i$ for $i=1,\cdots,l$. But this is immediate from the definition of $\widehat{S}_i$.

(ii) Let $w=w_{i_1}\cdots w_{i_r}$ be any reduced expression of w. Then we have by Cor. 4.2, $S(w)=S_{i_1}\cdots S_{i_r}$. Then we get $\widehat{S(w)}=(-1)^r q^r S_{i_r}^{-1}\cdots S_{i_1}^{-1}=\mathrm{sgn}(S(w))\,\mathrm{ind}(S(w))\,S(w)^{-1}$.

(iii) It is sufficient to show these formulas for $S=S_i$ $(i=1,\cdots,l)$. But this is immediate from the definition of $\widehat{S}_i$.

(iv) is proved similarly as in (iii).

University of Tokyo

References

[1] E. Abe, On the groups of C. Chevalley, J. Math. Soc. Japan, **11** (1959), 15-41.

[2] C. Chevalley, Sur certains groupes simples, Tôhoku Math. J., **7** (1955), 14-66.

[3] R. Ree, On some simple groups defined by Chevalley, Trans. Amer. Math. Soc., **84** (1957), 392-400.

[4] Séminaire C. Chevalley, Classification des groupes de Lie algébriques, Paris, (1956-58). Exposé 14.

[5] G. Shimura, Sur les integrales attachées aux formes automorphes, J. Math. Soc. Japan, **11** (1959), 291-311.

[6] R. Steinberg, A geometric approach to the representations of the full linear group over a Galois field, Trans. Amer. Math. Soc., **71** (1951), 274-282.

[7] R. Steinberg, Générateurs, relations, et revêtements de groupes algébriques, Colloque sur la théorie des groupes algébrique, Bruxelles, 1962, 113-127.

[8] E. Witt, Spiegerungsgruppen und Aufzählung halbeinfacher Liescher Ringe, Abh. Math. Sem. Univ. Hamberg, **14** (1941), 289-322.

(Received November 6, 1963)

Added in Proof.

[9] J. Tits, Théorème de Bruhat et sous-groupes paraboliques, C. R. Acad. Sc. t. 254 (1962), 2910-2912.