UNIQUENESS OF THE ALGEBRA OF POLYNOMIAL FUNCTIONS ON A FINITE GROUP

Akira NISHIKAWA

§ 1. Introduction and notation

Let S be a set, F a field. Denote by $M_F(S)$ the F-algebra of all F-valued functions on S.

Let G be a group, x an element in G, and f in $M_F(G)$. We define $x \cdot f$ and $f \cdot x$ as the elements in $M_F(G)$ by

$$(x \cdot f)(y) = f(yx), \quad (f \cdot x)(y) = f(xy) \quad (y \in G).$$

Then, $M_F(G)$ is a two sided module on the group ring FG.

The group multiplication $G \times G \longrightarrow G$ induces an F-algebra-homomorphism

$$\sigma: M_F(G) \longrightarrow M_F(G \times G).$$

On the other hand, there is a canonical injection

$$\pi: M_F(G) \otimes_F M_F(G) \longrightarrow M_F(G \times G),$$

and we identify $M_F(G) \otimes_F M_F(G)$ with $\mathrm{Im}\pi$.

Now it is easily seen that for f in $M_F(G)$, $\sigma(f) \in \mathrm{Im}\pi$ if and only if $FG \cdot f$ is finite dimensional. A function with this property is called a representative function on G.

We denote by $R_F(G)$ the set of all representative functions on G. Then the following results are known:

(1) $R_F(G)$ is a F-subalgebra of $M_F(G)$.

(2) Denote by γ the restriction of σ on $R_F(G)$, then
$\mathrm{Im}\gamma \subset R_F(G) \otimes_F R_F(G)$.

(3) $R_F(G)$ is a Hopf algebra, where γ is the comultiplication, $c: R_F(G) \longrightarrow F$ such that $c(f) = f(1)$ is the counit, and $\delta: R_F(G) \longrightarrow R_F(G)$ such that $\delta(f)(x) = f(x^{-1})$ $(x \in G)$ is the antipode.

The structure of an affine algebraic group over the field F consists of a pair (G, A), where G is a group, and A is a sub Hopf algebra of $R_F(G)$ satisfying the following conditions:

(1) A is a finitely generated F-algebra.

(2) A separates the elements of G, *i.e.*, for x, y in G such that $x \neq y$, there

exists a in A such that $a(x) \neq a(y)$.

(3) Every F-algebra–morphism $A \longrightarrow F$ is the evaluation $a \mapsto x^\circ(a) = a(x)$ at an element x of G.

The second and the third conditions mean that the canonical map $x \mapsto x^\circ$ of G into $\mathrm{Alg}_F(A, F)$ is bijective, and we shall identify G with $\mathrm{Alg}_F(A, F)$.

When (G, A) is the structure of an affine algebraic group over F, A is called the algebra of polynomial functions on G.

Although all groups are not affine algebraic groups ([3]), any finite group is an affine algebraic group.

If G is a finite group, then the natural map

$$\pi : M_F(G) \otimes_F M_F(G) \longrightarrow M_F(G \times G)$$

is bijective, hence

$$M_F(G) = R_F(G).$$

In § 2, we shall give a proof that for a finite group G, $(G, M_F(G))$ is the structure of an affine algebraic group.

In § 3, we shall prove that for a finite group G, if (G, A) is the structure of an affine algebraic group, then A is identical with $M_F(G)$.

§ 2. A proof that finite groups are affine algebraic groups

If S is a non-empty set, then we have canonical identification

$$(FS)^* = M_F(S),$$

where $(FS)^*$ is the dual of FS, F-space with the basis S.

Especially if G is a finite group, then

$$(FG)^* = R_F(G).$$

Lemma 1. *If G is a finite group, then $(G, (FG)^*)$ is the structure of an affine algebraic group.*

Proof. Let G be a finite group. $(FG)^*$ is then finite dimensional, especially a finitely generated F-algebra.

As $(FG)^*$ is the set of all F-valued functions, it naturally separates the elements of G.

Hence,

$$G \subset \mathrm{Alg}_F((FG)^*, F).$$

On the other hand, for any Hopf algebra H,

$$\mathrm{Alg}_F(H, F) = \mathrm{G}(H^\circ),$$

where $\mathrm{G}(H^\circ)$ is the set of all grouplike elements of the dual Hopf algebra H° ([2]).
Hence here,

$$\mathrm{Alg}_F((FG)^*, F) = \mathrm{G}((FG)^{**}) = \mathrm{G}(FG) \supset G$$

By linear independence of grouplike elements, we have

$$|\mathrm{G}(FG)| \leqq \dim_F FG = |G|.$$

Therefore

$$\mathrm{Alg}_F((FG)^*, F) = G,$$

which completes the proof.

§ 3. Uniqueness of the algebra of polynomial functions

Theorem 2. *If G is a finite group, and (G, A) is the structure of an affine algebraic group, then A is equal to $(FG)^*$.*

Proof. Write n as the order of G, then

$$\dim_F (FG)^* = |G| = n.$$

By the definition of the affine algebraic group,

$$A \subset R_F(G) = (FG)^*,$$
$$G \cong \mathrm{Alg}_F(A, F).$$

Using the result of Lemma 1, we think the following composition of maps:

$$G = \mathrm{Alg}_F((FG)^*, F) \xrightarrow{res} \mathrm{Alg}_F(A, F) \cong G. \qquad (*)$$

Observing the process of construction, this composition is the identity map on G.
On the other hand,

$$\mathrm{Alg}_F(A, F) \subset \mathrm{Hom}_F(A, F) = A^*,$$

and all the elements of $\mathrm{Alg}_F(A, F)$ are linearly independent, since

$$\mathrm{Alg}_F(A, F) = \mathrm{G}(A^\circ) = \mathrm{G}(A^*).$$

So by the equality (*), $\mathrm{Alg}_F(A, F)$ consists of n elements.
Therefore

$$\dim_F A = \dim_F A^* = n = \dim_F (FG)^*,$$

and so

$$A = (FG)^*,$$

which completes the proof.

References

1. HOCHSCHILD, G. : Introduction to Affinne Algebraic Groups, (1971) Holden-Day, Inc.
2. SWEEDLER, M. E. : Hopf Algebras, (1969) Benjamin
3. TAFT, E. J. : Reflexivility of algebras and coalgebras, American Journal of Mathematics (1972) 1111–1130.