Gelfand pairs obtained from the finite upper half planes over $\mathbb{Z}/2^n\mathbb{Z}$

Makoto Tagami

Abstract

The general linear group G over $\mathbf{Z}/2^n\mathbf{Z}$ acts transitively on the finite upper half plane over $\mathbf{Z}/2^n\mathbf{Z}$ where $\mathbf{Z}$ denotes the ring of rational integers. In this paper, it is showed that the pair of G and the stabilizer of a point on the plane is a Gelfand pair.

1 Introduction

The finite upper half planes over finite fields and rings were introduced as finite analogues of the Poincaré upper half plane. The general linear groups act transitively on the planes by the fractional linear transformation. In general, a finite group G and the subgroup H is called a Gelfand pair if the permutaion character of the action of G on the right cosets G/H by the multiplication from the left side is multiplicity-free. It has already been well-known that in the case of finite fields for all primes and finite rings for odd primes the general linear group and the stabilizer of a point on the plane is a Gelfand pair (see [1] and [5]). In this paper, we shall generalize the finite upper half planes over finite rings for odd primes to that over all primes and then show that the general linear group and the stabilizer of a point on the plane is a Gelfand pair.

2 The definition of finite upper half planes

First we review the definition of the finite upper half planes over $\mathbb{Z}/p^n\mathbb{Z}$ for an odd prime p in order to define the planes over $\mathbb{Z}/2^n\mathbb{Z}$. We denote the group of units of a ring R by $U(R)$.

Let p be an odd prime and $R_n[T]$ the polynomial ring over $R_n := \mathbb{Z}/p^n\mathbb{Z}$ with an indetermine T. Fix a generator δ of $U(R_n)$ and define $Q(T) := T^2 - \delta$. Then, we consider the quatient ring $M_n := R_n[T]/(Q(T))$ where $(Q(T))$ denotes the ideal of $R_n[T]$ generated by $Q(T)$. M_n becomes an extension ring of R_n. Under these notations, we define the finite upper half plane H_n for an odd prime as follows:

$$H_n := \{x + yT \in M_n \mid x \in R_n,\ y \in U(R_n)\}.$$

Then, H_n is a subset of $U(M_n)$ (see [5]). Even if we take any other monic polynomial of degree 2 which is not presented as a mulitiplication of two monic polynomials of degree 1 and then make the extension ring with the polynomial instead of the above $Q(T)$, this ring is isomorphic to the above M_n as R_n-algebras.

Next we shall consider the finite upper half planes over $\mathbb{Z}/2^n\mathbb{Z}$ in the similar way to the case of odd primes.

Let $R_n := \mathbb{Z}/2^n\mathbb{Z}$. For convenience, we put $R_0 = 0$. Let $Q(T)$ be a monic polynomial of degree 2 which is not presented as a mulitiplication of two monic polynomials of degree 1 and define $M_n := R_n[T]/(Q(T))$. Then, we shall define the finite upper half planes as follows.

Definition 2.1. The finite upper half plane over $\mathbb{Z}/2^n\mathbb{Z}$ is defined by

$$H_n := \{x + yT \in M_n \mid x \in R_n,\ y \in U(R_n)\}.$$

Let G be the general linear group over R_n, that is to say,

$$G = G_n := \mathrm{GL}(2, R_n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \ a, b, c, d \in R_n,\ ad - bc \in U(R_n) \right\}.$$

In the same way to the case of odd primes, G acts transitively on H_n as follows: $g \cdot z := \frac{az+b}{cz+d}$ for $z \in H_n$ and $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$.

By the following lemma, we see that M_n does not depend on how to take a monic polynomial $Q(T)$ of degree 2 which is not presented as a mulitiplication of two monic polynomials of degree 1 similar to the case of odd primes. Therefore the finite upper half plane is unique up to isomorphism of G-spaces.

Lemma 2.1. *Let $Q(T)$ be any monic irreducible polynomial of degree 2 which is not presented as a mulitiplication of two monic polynomials of degree 1. Then, as R_n-algebras*

$$R_n[T]/(Q(T)) \simeq R_n[T]/(T^2 - T + 1).$$

Proof. We denote the polynomial obtained by taking mod 2 for $Q(T)$'s coefficients by $\overline{Q(T)}$. Put $Q(T) = T^2 - AT + B$. By Hensel's lemma ([4], Theorem 8.3), $Q(T)$ is not presented as a mulitiplication of two monic polynomials of degree 1 if and only if $\overline{Q(T)}$ is irreducible over R_1. So we see that both A and B are odd.

In order to prove this lemma, it is sufficient to verify the existence of C and D such that $(CT + D)^2 - (CT + D) + 1 = 0$ in $R_n[T]/(Q(T))$. Because then, the mapping $CT + D \mapsto T$ gives an isomorphism from $R_n[T]/(Q(T))$ to $R_n[T]/(T^2 - T + 1)$.

Substitute $T^2 = AT - B$ into $(CT + D)^2 - (CT + D) + 1 = 0$. Then, we get $(C^2A + 2CD - C)T + (-C^2B + D^2 - D + 1) = 0$. So we only have to look for solutions C and D of the following simultaneously equations:

$$C(CA + 2D - 1) = 0, \tag{1}$$

$$-C^2B + D^2 - D + 1 = 0. \tag{2}$$

From (2), C is odd. So from (1), $CA+2D-1 = 0$. Substitute $C = -A^{-1}(2D-1)$ into (2). Finally we obtain

$$D^2 + D = (B - A^2)/(4B - A^2).$$

But it is easy to see that any even number in R_n can be written by the form $D^2 + D$. This comletes the proof of the lemma. □

From now on, we shall consider only $Q(T) = T^2 - T + 1$.

3 Gelfand pairs obtained from finite upper half planes

We denote the stabilizer of T by K. Clearly,

$$K := \{g \in G \mid g \cdot T = T\} = \left\{ \begin{pmatrix} c+d & -c \\ c & d \end{pmatrix} \Big| \, c, d \in R_n, \ (c,d) \not\equiv 0 \pmod 2 \right\}.$$

We define the affine group A as follows:

$$A = A_n := \left\{ \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} \Big| \, x \in R_n, \ y \in U(R_n) \right\}.$$

The affine group A forms a complete set of representatives of the right cosets of G by K, that is to say, G is decomposed into the right cosets by K as follows:

$$G = \sum_{g \in A} gK.$$

In general, for a group G and subgroup H, if $HgH = zHg^{-1}H$ holds for any g in G, (G,H) is a Gelfand pair (see Theorem 1 in [6] p.308). Therefore, it is sufficient to show $KgK = Kg^{-1}K$ for any g in A.

We obtain the following condition by an elementary calculation. For $g_i = \begin{pmatrix} y_i & x_i \\ 0 & 1 \end{pmatrix} \in A \ (i = 1, 2)$,

$$Kg_1K = Kg_2K \Longleftrightarrow \exists k = \begin{pmatrix} c+d & -c \\ c & d \end{pmatrix} \in K \text{ s.t } kg_1K = g_2K \Longleftrightarrow$$

there exists $(c,d) \not\equiv 0 \pmod 2$ such that

$$\begin{pmatrix} x_1 - x_2 & x_1 - 1 - x_1x_2 + y_1y_2 \\ y_1 - y_2 & y_1 - y_1y_2 - x_2y_1 - y_2x_1 \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \pmod{2^n} \qquad (3)$$

In particular, put $g_2 = {g_1}^{-1}$ and $x_1 = 2^l u$, $y_1 = v$ where $0 \leq l \leq n$, and $u, \ v \in U(R_n)$. Then since $\begin{pmatrix} y_1 & x_1 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} {y_1}^{-1} & -x_1{y_1}^{-1} \\ 0 & 1 \end{pmatrix}$, the existence of solutions $(c,d) \not\equiv 0 \pmod 2$ of the equation obtained from (3) shows $Kg_1K = Kg_1{}^{-1}K$:

$$\begin{pmatrix} 2^l uv^{-1}(v+1) & 2^l u(1+2^l uv^{-1}) \\ v^{-1}(v+1)(v-1) & (v-1)(1+2^l uv^{-1}) \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \pmod{2^n} \qquad (4)$$

In order to verify the existence of solutions, we define 2-adic valuation.

Definition 3.1 (2-adic valuation). Let a be a nonzero elememt in R_n. If $2^l \parallel a$ (i.e. $2^l \mid a$ and $2^{l+1} \nmid a$), we define $h(a) := l$. When $a = 0$, define $h(a) := n$. We call h the 2-adic valuation of R_n.

The following lemma follows [5].

Lemma 3.1. *Let* $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ *for* $a_{ij} \in R_n$ *and* h *the 2-adic valuation of* R_n. *Assume that* A *is a nonzero matrix. We put* $h := \min_{1 \le i,j \le 2} h(a_{ij})$, $a_{ij} = 2^h a'_{ij}$ *and* $A' := \begin{pmatrix} a'_{11} & a'_{12} \\ a'_{21} & a'_{22} \end{pmatrix}$ *where* $a'_{ij} \in R_{n-h}$. *Then, there exits a vector* $(x, y) \not\equiv (0,0) \pmod 2$ *such that* $A \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \pmod{2^n}$ *if and only if* $\det A' \equiv 0 \pmod{2^{n-h}}$.

By Lemma 3.1, the existence of solutions of (4) is verified by caluculating the values of 2-adic valuation of the entries of the coefficient matrix.

When $l = 0$, since $h(v^{-1}(v+1)(v-1)) \le h(uv^{-1}(v+1))$ and $h((v-1)(1+uv^{-1})) \le h(u(1+uv^{-1}))$, the condition of Lemma 3.1 holds. When $l \ge 1$,

$$\begin{aligned} h((1,1)\text{entry}) &= l + h(1+v), \\ h((1,2)\text{entry}) &= l, \\ h((2,1)\text{entry}) &= h(v+1) + h(v-1), \\ h((2,2)\text{entry}) &= h(v-1). \end{aligned}$$

By the four equations above, we see $h((1,1)\text{entry}) < h((1,2)\text{entry})$, $h((2,1)\text{entry}) < h((2,2)\text{entry})$, and so the condition of Lemma 3.1 also holds. After all, we obtain the following by joining to the result of [5].

Theorem 3.1. *Let* p *be arbitrary prime,* G_n *the general linear group over* $\mathbb{Z}/p^n\mathbb{Z}$, *and* K_n *the stabilizer of a point on the finite upper half plane. Then,* (G_n, K_n) *is a Gelfand pair.*

Acknowledgement The author would like to thank Professor Keith Conrad for his significant advices to this paper.

References

[1] J. Angel, Finite upper half planes over finite fields, *Finite Fields Appl.*, 2(1996), 62-86.

[2] E. Bannai and T. Ito, *Algebraic Combinatorics I, Association Schemes*, Benjamin/Cummings, Menlo Park, CA, 1984.

[3] R. Evans, Spherical functions for finite upper half planes with characteristic 2, *Finite Fields Appl.*, 1 (1995), 376-394.

[4] H. Matsumura, Commutative algebra, Benjamin, 1970.

[5] M. Tagami, Symmetric association schemes attached to finite upper half planes over rings, to appear in *Linear Algebra and Its Applications.*

[6] A. Terras, *Fourier Analysis on Finite Groups and Applications*, London Math. Soc., 1999.