

素体 $F = \{0, 1\}$ 上の直交群の 2 元生成

城西大学理学部 石橋宏行 (Hiroyuki Ishibashi)

$F = \{0, 1\}$ は標数 2 の素体、 V は F 上 n 次のベクトル空間で 2 次写像 $q : V \longrightarrow F$ を付与されているものとする。即ち q は F の元 a と V の元 x とに対し、

$$(1) \quad q(ax) = a^2 q(x)$$

を満たし、

$$(2) \quad B(x, y) = q(x + y) - q(x) - q(y)$$

と置けば B は対称双一次写像である。この様な V を F 上の 2 次空間と言う。

2 次空間 V 上の一般線型群 $GL(V)$ の部分群

$$O(V) = \{\sigma \in GL(V) \mid q(x) = q(\sigma x) \text{ for all } x \text{ in } V\}$$

を V 上の直交群と言う。

我々の目的は $O(V)$ の 2 元生成を示す事である。従って、 $G = O(V)$ と置き、 $G = \langle \sigma, \rho \rangle$ なる G の 2 元 σ, ρ の存在を示す。ただし、 V

は非退化、即ち、

$$「x \neq 0 \text{ ならば } B(x, V) \neq \{0\}」$$

と仮定する。又簡単のため、 $B(x, y)$ を xy で示す。

まず V が非退化なる仮定より

$$n = 2m$$

を得る。

証明の前に V の2次元空間としての構造をグラフを用いて表す事にする。

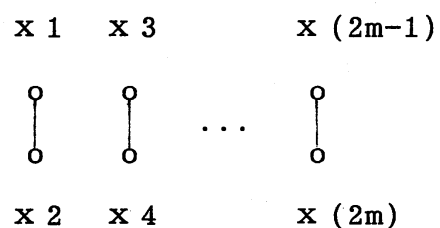
即ち V の元 x は $q(x) = 0$ か $\neq 0$ かにより $\circ$ か $\bullet$ かで示し、 V の

2元 x, y は $xy = 0$ か $\neq 0$ かにより—で結ばないか結ぶかで示す事

にする。 $F = \{0, 1\}$ であるから、この V のグラフは完全に q を表現する。

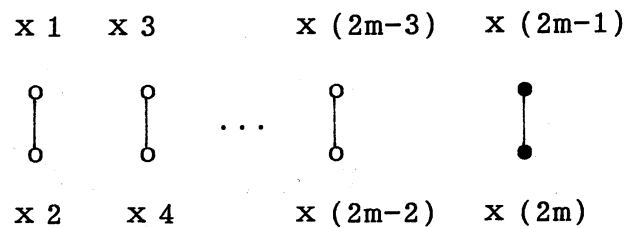
次に V の基底 $X = \{x_1, x_2, \dots, x_{(2m-1)}, x_{(2m)}\}$ を上手に選べばそのグラフは次のいずれかになる。

(i)



(双曲型)

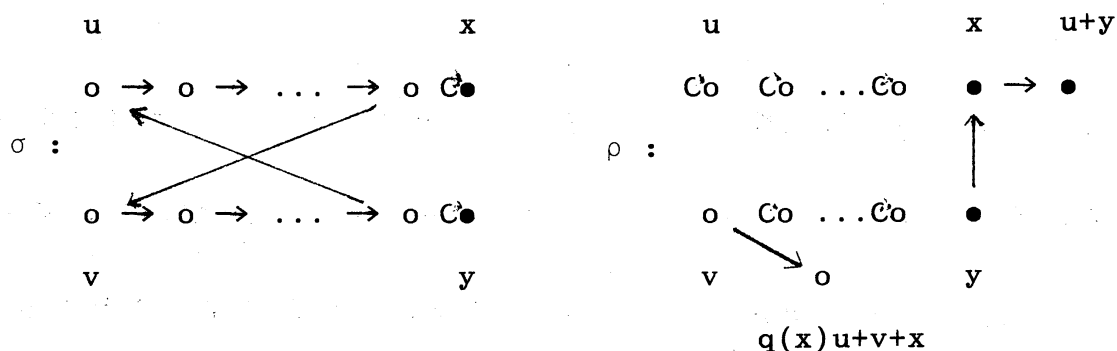
(ii)



(非双曲型)

V が (i) 双曲型の場合は既に証明されている(石橋[2])ので、 V が (ii) 非双曲型の場合に証明すればよい訳であるが、ここで行う証明法は (i)、(ii) いずれの場合にも適用出来るものである。

さて、証明であるが、 G の元は線型写像であるから、 G の生成元 σ, ρ は V の基底 X の上で定義すればよい。そこで $u = x_1$ 、 $v = x_2$ 、 $x = x_{(2m-1)}$ 、 $y = x_{(2m)}$ とおき



と定義すれば、明らかに σ, ρ は基底 X の上で q を保存する。従って、これらを V 上に線型に広げれば σ, ρ は G の元となる。ここで σ, ρ の X に関する行列表示をそれぞれ A, B と書く事にし、 $F(h, k)$ を

$$F(1, 2j-1) = (A^{B^{j-1}} A^{-1})^2$$

$$F(1, 2j) = (A^{B^{m-2+j}} A^{-1})^2$$

$$F(2, 2j-1) = (A^{B^{j-1}} A^{-B^m})^2$$

$$F(2, 2j) = (A^{B^{m-2+j}} A^{-B^m})^2$$

と定義すれば、 G の任意の元 π の行列表示 C に対し、 $F(h, k)C$ は C に

次の i) - iv) の右辺の操作を施す事と同じであるから、

$$(i) \quad F(2j-1)C = \left[\begin{array}{l} C \text{ の } 1 \text{ 行に } C \text{ の } 2j \text{ 行を加え、} \\ C \text{ の } (2j-1) \text{ 行に } C \text{ の } 2 \text{ 行を加える} \end{array} \right]$$

$$(ii) \quad F(2j-1)C = \left[\begin{array}{l} C \text{ の } 1 \text{ 行に } C \text{ の } (2j-1) \text{ 行を加え、} \\ C \text{ の } 2j \text{ 行に } C \text{ の } 2 \text{ 行を加える} \end{array} \right]$$

$$(iii) \quad F(2j-1)C = \left[\begin{array}{l} C \text{ の } 2 \text{ 行に } C \text{ の } 2j \text{ 行を加え、} \\ C \text{ の } (2j-1) \text{ 行に } C \text{ の } 1 \text{ 行を加える} \end{array} \right]$$

$$(iv) \quad F(2j-1)C = \left[\begin{array}{l} C \text{ の } 2 \text{ 行に } C \text{ の } (2j-1) \text{ 行を加え、} \\ C \text{ の } 2j \text{ 行に } C \text{ の } 1 \text{ 行を加える} \end{array} \right]$$

行列の基本変換と同様 $F(h, k)$ を C の左から繰り返し掛ける事により、 C

を単位行列に出来る。従って G は σ, ρ で生成される。

参考文献

- [1] H.Ishibashi and A.G.Earnest, Two-Element Generation of The Orthogonal Groups over Finite Fields, J.Algebra 165(1994), 164-171.
- [2] H.Ishibashi, Two-Element Generation of The Hyperbolic Orthogonal Groups over The Finite Fields F_2 , 数理解析研究所講究録 910, 半群.形式言語及び語の組み合わせ論シンポジウム (1995), 36-39.
- [3] H.Ishibashi, Two-Element Generation of The Integral Symplectic Group $Sp_n(\mathbb{Z})$, J.Algebra 179(1996), 137-144.