数理解析研究所講究録
960巻 1996年 66-70

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、

「$x \neq 0$ 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

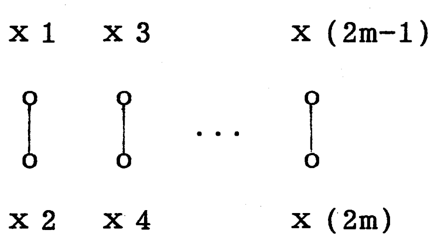
$$n = 2m$$

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 ｏ か ● 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。

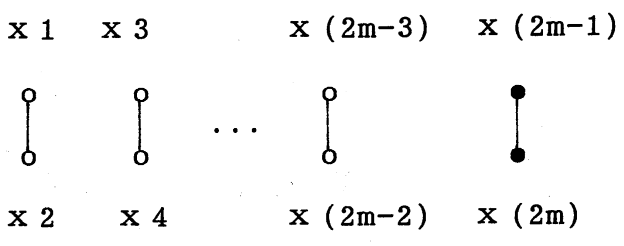
次にVの基底$X = \{x_1, x_2, \ldots, x_{(2m-1)}, x_{(2m)}\}$を上手に選べばそのグラフは次のいずれかになる。

(i)



(双曲型)

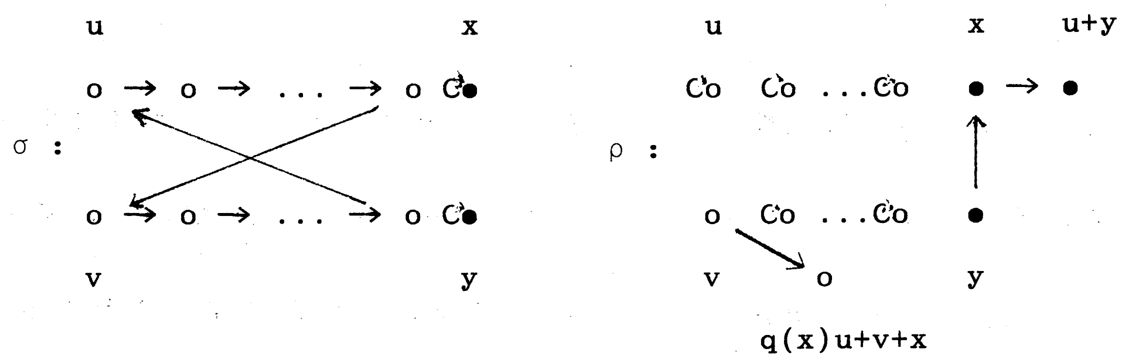
(ii)



(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 $u = x1$、$v = x2$、$x = x(2m-1)$、$y = x(2m)$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、

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

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

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

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

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.Ishibash, 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 $Sp_n(Z)$, J.Algebra 179(1996), 137-144.