Orthogonal groups $\mathcal{O}(n)$ over $GF(2)$ as automorphisms

Young-Jo Kwak

April, 2013

Orthogonal groups

Let (V, Q) be a quadratic vector space over $\mathbb{K}$.

Orthogonal groups

Let (V,Q) be a quadratic vector space over $\mathbb{K}$.
$\mathcal{O}(V,Q) := \left\{\gamma \in GL(V) : Q(\gamma x) = Q(x)\ \forall x \in V\right\}$ where
$$Q(x) = S(x,x) = {}^{t}xSx = \sum s_{ij}x_ix_j = \sum s_{ii}x_i^2 + 2\sum_{i<j} s_{ij}x_ix_j.$$

Orthogonal groups

Let (V, Q) be a quadratic vector space over $\mathbb{K}$.
$\mathcal{O}(V, Q) := \left\{\gamma \in GL(V) : Q(\gamma x) = Q(x)\ \forall x \in V\right\}$ where

$$Q(x) = S(x, x) = {}^t xSx = \sum s_{ij}x_ix_j = \sum s_{ii}x_i^2 + 2\sum_{i<j} s_{ij}x_ix_j.$$

$\mathcal{O}(\mathbb{K}^n, S) = \left\{M \in GL(n, \mathbb{K}) :\ {}^t MSM = S\right\}$ where

$$2S(x, y) = Q(x + y) - Q(x) - Q(y).$$

Orthogonal groups

Let (V,Q) be a quadratic vector space over $\mathbb{K}$.
$\mathcal{O}(V,Q) := \left\{\gamma \in GL(V) : Q(\gamma x) = Q(x)\ \forall x \in V\right\}$ where

$$Q(x) = S(x,x) = {}^t xSx = \sum s_{ij}x_ix_j = \sum s_{ii}x_i^2 + 2\sum_{i<j} s_{ij}x_ix_j.$$

$\mathcal{O}(\mathbb{K}^n, S) = \left\{M \in GL(n,\mathbb{K}) :\ {}^tMSM = S\right\}$ where

$$2S(x,y) = Q(x+y) - Q(x) - Q(y).$$

Due to $2=0$ in $\mathrm{char}\mathbb{K}=2$, re-define S as: $S(x,y) = Q(x+y) - Q(x) - Q(y)$.

Orthogonal groups

Let (V, Q) be a quadratic vector space over $\mathbb{K}$.
$\mathcal{O}(V, Q) := \left\{\gamma \in GL(V) : Q(\gamma x) = Q(x)\ \forall x \in V\right\}$ where

$$Q(x) = S(x, x) = {}^t x S x = \sum s_{ij} x_i x_j = \sum s_{ii} x_i^2 + 2 \sum_{i<j} s_{ij} x_i x_j.$$

$\mathcal{O}(\mathbb{K}^n, S) = \left\{M \in GL(n, \mathbb{K}) : {}^t M S M = S\right\}$ where

$$2S(x, y) = Q(x + y) - Q(x) - Q(y).$$

Due to $2 = 0$ in $\mathrm{char}\mathbb{K} = 2$, re-define S as: $S(x, y) = Q(x + y) - Q(x) - Q(y)$.
Q is diagonal and S is alternating.

Orthogonal groups

Let (V, Q) be a quadratic vector space over $\mathbb{K}$.
$\mathcal{O}(V, Q) := \left\{\gamma \in GL(V) : Q(\gamma x) = Q(x)\ \forall x \in V\right\}$ where

$$Q(x) = S(x, x) = {}^t x S x = \sum s_{ij} x_i x_j = \sum s_{ii} x_i^2 + 2 \sum_{i<j} s_{ij} x_i x_j.$$

$\mathcal{O}(\mathbb{K}^n, S) = \left\{M \in GL(n, \mathbb{K}) :\ {}^t MSM = S\right\}$ where

$$2S(x, y) = Q(x + y) - Q(x) - Q(y).$$

Due to $2 = 0$ in $\mathrm{char}\mathbb{K} = 2$, re-define S as: $S(x, y) = Q(x + y) - Q(x) - Q(y)$.
Q is diagonal and S is alternating.
Thus, orthogonal group $\mathcal{O}(V, Q)$ is the automorphisms preserving (V, Q).

Orthogonal groups

Let (V, Q) be a quadratic vector space over $\mathbb{K}$.
$\mathcal{O}(V, Q) := \left\{\gamma \in GL(V) : Q(\gamma x) = Q(x)\ \forall x \in V\right\}$ where

$$Q(x) = S(x, x) = {}^t xSx = \sum s_{ij}x_ix_j = \sum s_{ii}x_i^2 + 2\sum_{i<j} s_{ij}x_ix_j.$$

$\mathcal{O}(\mathbb{K}^n, S) = \left\{M \in GL(n, \mathbb{K}) :\ {}^tMSM = S\right\}$ where

$$2S(x, y) = Q(x + y) - Q(x) - Q(y).$$

Due to $2 = 0$ in $\mathrm{char}\mathbb{K} = 2$, re-define S as: $S(x, y) = Q(x + y) - Q(x) - Q(y)$.
Q is diagonal and S is alternating.
Thus, orthogonal group $\mathcal{O}(V, Q)$ is the automorphisms preserving (V, Q).

$\mathcal{O}(n) := \mathcal{O}(\mathbb{K}^n, I)$.

Orthogonal groups

Let (V, Q) be a quadratic vector space over $\mathbb{K}$.
$\mathcal{O}(V, Q) := \{\gamma \in GL(V) : Q(\gamma x) = Q(x)\ \forall x \in V\}$ where

$$Q(x) = S(x,x) = {}^t xSx = \sum s_{ij}x_ix_j = \sum s_{ii}x_i^2 + 2\sum_{i<j} s_{ij}x_ix_j.$$

$\mathcal{O}(\mathbb{K}^n, S) = \{M \in GL(n, \mathbb{K}) : {}^tMSM = S\}$ where

$$2S(x,y) = Q(x+y) - Q(x) - Q(y).$$

Due to $2 = 0$ in char$\mathbb{K} = 2$, re-define S as: $S(x,y) = Q(x+y) - Q(x) - Q(y)$.
Q is diagonal and S is alternating.
Thus, orthogonal group $\mathcal{O}(V, Q)$ is the automorphisms preserving (V, Q).

$\mathcal{O}(n) := \mathcal{O}(\mathbb{K}^n, I)$.
$\mathcal{O}(n) = \mathrm{Aut}\big(\mathfrak{o}(n)\big)$ over $\mathbb{C}$, $\mathbb{R}$.

Orthogonal groups

Let (V, Q) be a quadratic vector space over $\mathbb{K}$.
$\mathcal{O}(V, Q) := \left\{\gamma \in GL(V) : Q(\gamma x) = Q(x)\ \forall x \in V\right\}$ where

$$Q(x) = S(x, x) = {}^t xSx = \sum s_{ij} x_i x_j = \sum s_{ii} x_i^2 + 2 \sum_{i<j} s_{ij} x_i x_j.$$

$\mathcal{O}(\mathbb{K}^n, S) = \left\{M \in GL(n, \mathbb{K}) :\ {}^t MSM = S\right\}$ where

$$2S(x, y) = Q(x + y) - Q(x) - Q(y).$$

Due to $2 = 0$ in $\mathrm{char}\mathbb{K} = 2$, re-define S as: $S(x, y) = Q(x + y) - Q(x) - Q(y)$.
Q is diagonal and S is alternating.
Thus, orthogonal group $\mathcal{O}(V, Q)$ is the automorphisms preserving (V, Q).

$\mathcal{O}(n) := \mathcal{O}(\mathbb{K}^n, I)$.
$\mathcal{O}(n) = \mathrm{Aut}\big(\mathfrak{o}(n)\big)$ over $\mathbb{C}$, $\mathbb{R}$.
How about another field?

Orthogonal groups

Let (V, Q) be a quadratic vector space over $\mathbb{K}$.
$\mathcal{O}(V, Q) := \{\gamma \in GL(V) : Q(\gamma x) = Q(x)\ \forall x \in V\}$ where

$$Q(x) = S(x, x) = {}^t x S x = \sum s_{ij} x_i x_j = \sum s_{ii} x_i^2 + 2 \sum_{i<j} s_{ij} x_i x_j.$$

$\mathcal{O}(\mathbb{K}^n, S) = \{M \in GL(n, \mathbb{K}) : {}^t M S M = S\}$ where

$$2S(x, y) = Q(x+y) - Q(x) - Q(y).$$

Due to $2 = 0$ in $\mathrm{char}\mathbb{K} = 2$, re-define S as: $S(x, y) = Q(x+y) - Q(x) - Q(y)$.
Q is diagonal and S is alternating.
Thus, orthogonal group $\mathcal{O}(V, Q)$ is the automorphisms preserving (V, Q).

$\mathcal{O}(n) := \mathcal{O}(\mathbb{K}^n, I)$.
$\mathcal{O}(n) = \mathrm{Aut}\big(\mathfrak{o}(n)\big)$ over $\mathbb{C}$, $\mathbb{R}$.
How about another field?
The answer is Yes if it is over $GF(2)$.

Orthogonal groups

Let (V, Q) be a quadratic vector space over $\mathbb{K}$.
$\mathcal{O}(V,Q) := \left\{\gamma \in GL(V) : Q(\gamma x) = Q(x)\ \forall x \in V\right\}$ where

$$Q(x) = S(x,x) = {}^t x S x = \sum s_{ij} x_i x_j = \sum s_{ii} x_i^2 + 2 \sum_{i<j} s_{ij} x_i x_j.$$

$\mathcal{O}(\mathbb{K}^n, S) = \left\{M \in GL(n,\mathbb{K}) :\ {}^t MSM = S\right\}$ where

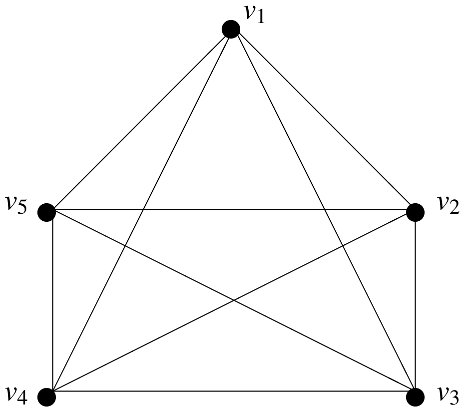
$$2S(x,y) = Q(x+y) - Q(x) - Q(y).$$

Due to $2 = 0$ in $\mathrm{char}\mathbb{K} = 2$, re-define S as: $S(x,y) = Q(x+y) - Q(x) - Q(y)$.
Q is diagonal and S is alternating.
Thus, orthogonal group $\mathcal{O}(V,Q)$ is the automorphisms preserving (V,Q).

$\mathcal{O}(n) := \mathcal{O}(\mathbb{K}^n, I)$.
$\mathcal{O}(n) = \mathrm{Aut}\big(\mathfrak{o}(n)\big)$ over $\mathbb{C}$, $\mathbb{R}$.
How about another field?
The answer is Yes if it is over $GF(2)$.
This is a verification of Steinberg 1961 that $\mathrm{Aut}\big(\mathfrak{o}(n)\big)$ over a square free field is simple, with non-simple exception $n = 5$.

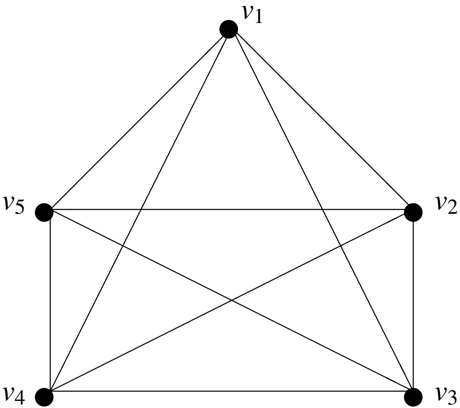
Combinatorial Basis $\mathfrak{C}$

Example: $n = 5$



Combinatorial Basis $\mathfrak{C}$

Example: $n = 5$



$$\mathfrak{C} = \left\{ v_1, \ldots, v_5,\ e_1, \ldots, e_{10},\ t_1, \ldots, t_{10},\ r_1, \ldots, r_5 \right\}$$

Combinatorial algebras $\mathfrak{C}(n)$

Df. Combinatorial basis $\mathfrak{C}$ over a fixed commutative ring K

$$\mathfrak{C} = \bigcup_{-1 \leq i \leq n-3} \mathfrak{C}_{[i]} \text{ where } \mathfrak{C}_{[-1]} = \{v_1, \ldots, v_n\} \text{ and for } 0 \leq i \leq n\text{-}3$$

$$\mathfrak{C}_{[i]} = \left\{X_1, \ldots, X_{\binom{n}{i+2}} : \text{each } X_j \text{ is an } (i+2) \text{ choice of dots in } \mathfrak{C}_{[-1]}\right\}$$

Combinatorial algebras $\mathfrak{C}(n)$

Df. Combinatorial basis $\mathfrak{C}$ over a fixed commutative ring K

$$\mathfrak{C} = \bigcup_{-1 \leq i \leq n-3} \mathfrak{C}_{[i]} \text{ where } \mathfrak{C}_{[-1]} = \{v_1, \ldots, v_n\} \text{ and for } 0 \leq i \leq n\text{-}3$$
$$\mathfrak{C}_{[i]} = \left\{X_1, \ldots, X_{\binom{n}{i+2}} : \text{each } X_j \text{ is an } (i+2) \text{ choice of dots in } \mathfrak{C}_{[-1]}\right\}$$

Let $X = \{v_{x(1)}, \ldots, v_{x(s)}\}, Y = \{v_{y(1)}, \ldots, v_{y(t)}\} \in \mathfrak{C}$. Then $X \cdot Y$ is:

$$X \cdot Y := \begin{cases} X \cup Y \setminus X \cap Y & \text{if } X \cap Y = \{\cdot\} \text{ for some dot } v_{x(i)} = v_{y(j)} \\ 0 & \text{otherwise} \end{cases}$$

Combinatorial algebras $\mathfrak{C}(n)$

Df. Combinatorial basis $\mathfrak{C}$ over a fixed commutative ring K

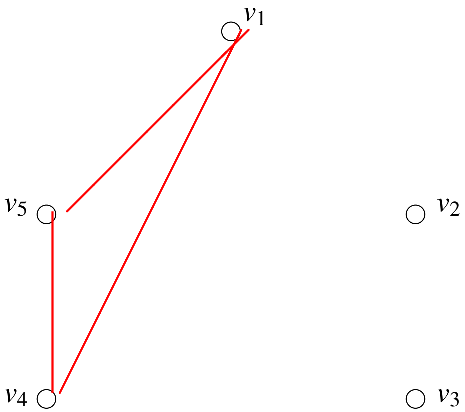
$$\mathfrak{C} = \bigcup_{-1 \le i \le n-3} \mathfrak{C}_{[i]} \text{ where } \mathfrak{C}_{[-1]} = \{v_1, \ldots, v_n\} \text{ and for } 0 \le i \le n\text{-}3$$
$$\mathfrak{C}_{[i]} = \left\{X_1, \ldots, X_{\binom{n}{i+2}} : \text{each } X_j \text{ is an } (i+2) \text{ choice of dots in } \mathfrak{C}_{[-1]}\right\}$$

Let $X = \{v_{x(1)}, \ldots, v_{x(s)}\}, Y = \{v_{y(1)}, \ldots, v_{y(t)}\} \in \mathfrak{C}$. Then $X \cdot Y$ is:

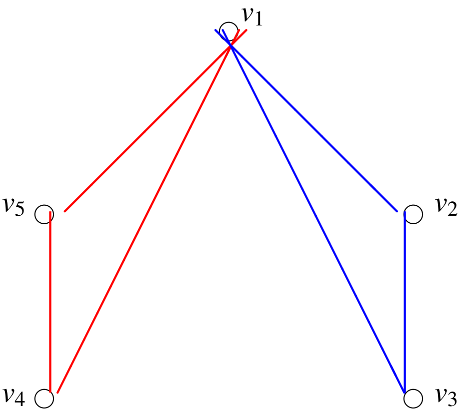
$$X \cdot Y := \begin{cases} X \cup Y \setminus X \cap Y & \text{if } X \cap Y = \{\cdot\} \text{ for some dot } v_{x(i)} = v_{y(j)} \\ 0 & \text{otherwise} \end{cases}$$

$\mathfrak{C}(n) = \bigoplus_{-1 \le i \le n-3} L_i$ is a non-associative commutative K-algebra where each L_i is a grading subspace spanned by $\mathfrak{C}_{[i]}$. If K is a field of char$K$ = 2, $\mathfrak{C}(n) = G(n) \bigotimes_{\mathbb{F}_2} K$ where $G(n)$ are simple Lie algebras over $GF(2)$ introduced by Kaplansky in 1982. We assume $K = GF(2)$ so that $\mathfrak{C}(n) = G(n)$.

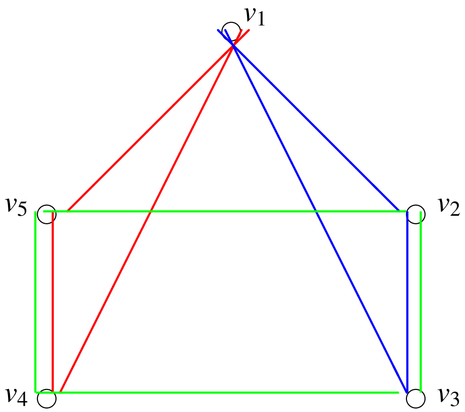
Multiplication in $\mathfrak{C}(5)$ - Case 1



Multiplication in $\mathfrak{C}(5)$ - Case 1

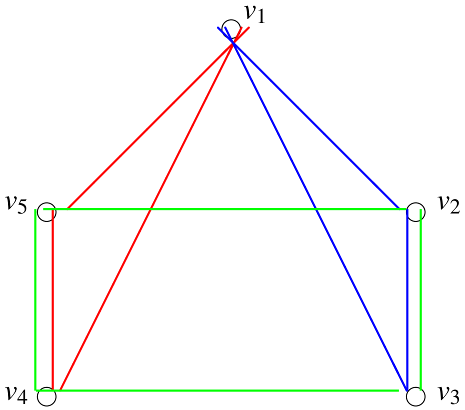


Multiplication in $\mathfrak{C}(5)$ - Case 1



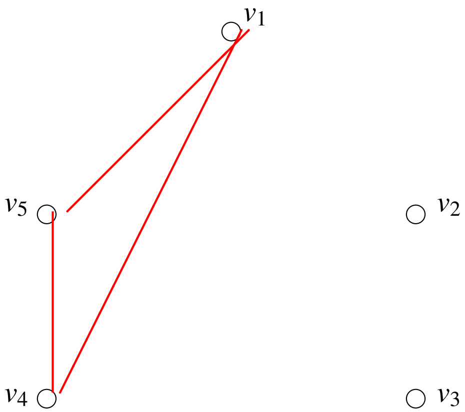
$X \cdot Y = Z$

Multiplication in $\mathfrak{C}(5)$ - Case 1

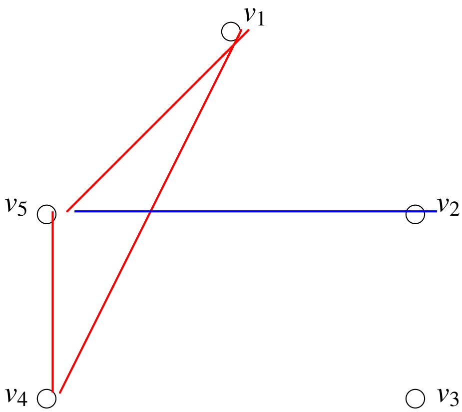


$$X \cdot Y = Z \qquad \text{but} \qquad Z \cdot Y = 0$$

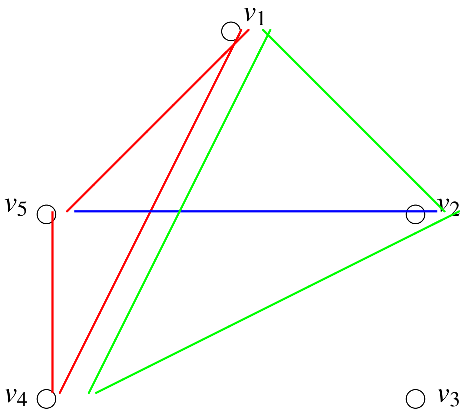
Multiplication in $\mathfrak{C}(5)$ - Case 2



Multiplication in $\mathfrak{C}(5)$ - Case 2

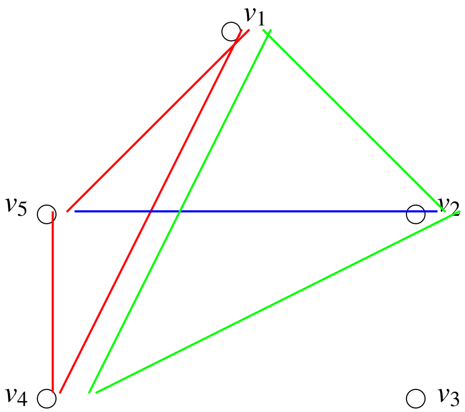


Multiplication in $\mathfrak{C}(5)$ - Case 2



$\color{red}{X} \cdot \color{blue}{Y} = \color{green}{Z}$

Multiplication in $\mathfrak{C}(5)$ - Case 2



$\color{red}{X} \cdot \color{blue}{Y} = \color{green}{Z}$ and $\color{green}{Z} \cdot \color{blue}{Y} = (\color{red}{X} \cdot \color{blue}{Y}) \cdot \color{blue}{Y} = \color{red}{X}$

Block multiplication in $\mathfrak{C}(10)$

	L_{-1}	L_0	L_1	L_2	L_3	L_4	L_5	L_6	L_7
L_{-1}	0	L_{-1}	L_0	L_1	L_2	L_3	L_4	L_5	L_6
L_0	L_{-1}	L_0	L_1	L_2	L_3	L_4	L_5	L_6	L_7
L_1	L_0	L_1	L_2	L_3	L_4	L_5	L_6	L_7	0
L_2	L_1	L_2	L_3	L_4	L_5	L_6	L_7	0	0
L_3	L_2	L_3	L_4	L_5	L_6	L_7	0	0	0
L_4	L_3	L_4	L_5	L_6	L_7	0	0	0	0
L_5	L_4	L_5	L_6	L_7	0	0	0	0	0
L_6	L_5	L_6	L_7	0	0	0	0	0	0
L_7	L_6	L_7	0	0	0	0	0	0	0

where $L_i \cdot L_j = L_{i+j}$ if -1 $\leq$ i+j $\leq$ n-3 and = 0 otherwise.

Block multiplication in $\mathfrak{C}(10)$

	L_{-1}	L_0	L_1	L_2	L_3	L_4	L_5	L_6	L_7
L_{-1}	0	L_{-1}	L_0	L_1	L_2	L_3	L_4	L_5	L_6
L_0	L_{-1}	L_0	L_1	L_2	L_3	L_4	L_5	L_6	L_7
L_1	L_0	L_1	L_2	L_3	L_4	L_5	L_6	L_7	0
L_2	L_1	L_2	L_3	L_4	L_5	L_6	L_7	0	0
L_3	L_2	L_3	L_4	L_5	L_6	L_7	0	0	0
L_4	L_3	L_4	L_5	L_6	L_7	0	0	0	0
L_5	L_4	L_5	L_6	L_7	0	0	0	0	0
L_6	L_5	L_6	L_7	0	0	0	0	0	0
L_7	L_6	L_7	0	0	0	0	0	0	0

where $L_i \cdot L_j = L_{i+j}$ if -1 $\leq$ i+j $\leq$ n-3 and = 0 otherwise.

$L_0 = \mathfrak{o}(n)$ is a simple subalgebra.

Example in $\mathcal{O}(5) = \mathrm{Aut}(L_0)$

Let $\alpha \in \mathcal{O}(5)$ with respect to $\mathfrak{C}_{[-1]} = \begin{pmatrix} v_1 & v_2 & v_3 & v_4 & v_5 \end{pmatrix}$

$$= \begin{pmatrix} \alpha(v_1) & \alpha(v_2) & \alpha(v_3) & \alpha(v_4) & \alpha(v_5) \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

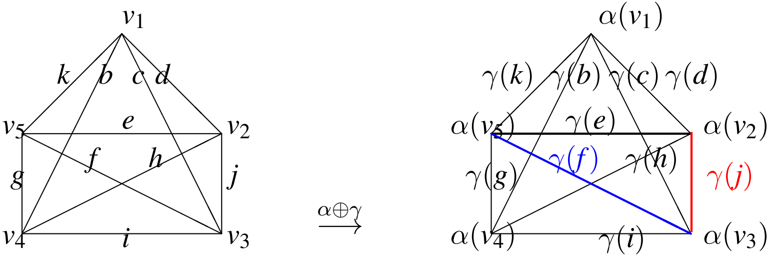
Example in $\mathcal{O}(5) = \mathrm{Aut}(L_0)$

Let $\alpha \in \mathcal{O}(5)$ with respect to $\mathfrak{C}_{[-1]} = \begin{pmatrix} v_1 & v_2 & v_3 & v_4 & v_5 \end{pmatrix}$

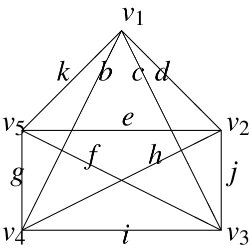
$$= \begin{pmatrix} \alpha(v_1) & \alpha(v_2) & \alpha(v_3) & \alpha(v_4) & \alpha(v_5) \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Then $\alpha \iff \alpha \oplus \gamma \in \mathrm{Aut}\big(K(5)\big)$ split automorphism
where $K(5) = L_{-1} \oplus L_0$
and $\gamma \in \mathrm{Aut}(L_0)$ with $\gamma(B) = {}^t\alpha B \alpha$ for all $B \in \mathfrak{o}(5)$.

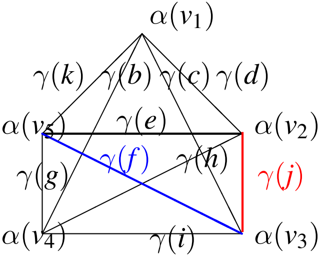
Example in $\mathcal{O}(5) = \mathrm{Aut}(L_0)$



Example in $\mathcal{O}(5) = \mathrm{Aut}(L_0)$



$\xrightarrow{\alpha\oplus\gamma}$



$$\gamma(e) = e + f + g + h + j$$

$$\gamma(j) = e + f + g + h + i$$

$$\gamma(f) = e + g + h + i + j$$

Make orientation

We have $\left[\gamma(j),\ \gamma(f)\right] = \gamma(e) = E_p + E_p^{\perp}$ where $E_p = \left[J_p, F_p^{\perp}\right] + \left[J_p^{\perp}, F_p\right]$.

Make orientation

We have $\left[\gamma(j),\ \gamma(f)\right] = \gamma(e) = E_p + E_p^{\perp}$ where $E_p = \left[J_p, F_p^{\perp}\right] + \left[J_p^{\perp}, F_p\right]$.

Let $p = v_2$. Then $E_p = j + h + e$.

Make orientation

We have $\left[\gamma(j),\ \gamma(f)\right] = \gamma(e) = E_p + E_p^\perp$ where $E_p = \left[J_p, F_p^\perp\right] + \left[J_p^\perp, F_p\right]$.

Let $p = v_2$. Then $E_p = j + h + e$.

Make orientation for $j = \{v_2, v_3\}$.

Make orientation

We have $\left[\gamma(j),\ \gamma(f)\right] = \gamma(e) = E_p + E_p^{\perp}$ where $E_p = \left[J_p, F_p^{\perp}\right] + \left[J_p^{\perp}, F_p\right]$.

Let $p = v_2$. Then $E_p = j + h + e$.

Make orientation for $j = \{v_2, v_3\}$.

$j = [f, e] + [h, i] + [i, h]$ in $\gamma(e) = \left[\gamma(j),\ \gamma(f)\right]$
where $[f, e] = [\{v_3, v_5\}, \{v_5, v_2\}]$ is in $[J_p^{\perp}, F_p]$
$[h, i] = [\{v_2, v_4\}, \{v_4, v_3\}]$ is in $[J_p, F_p^{\perp}]$
$[i, h] = [\{v_3, v_4\}, \{v_4, v_2\}]$ is in $[J_p^{\perp}, F_p]$.

Make orientation

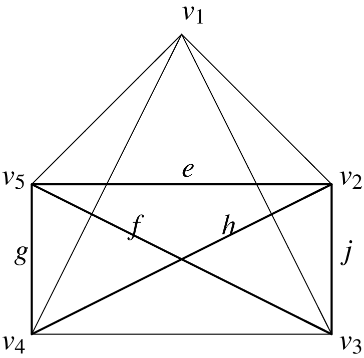
We have $\left[\gamma(j),\ \gamma(f)\right] = \gamma(e) = E_p + E_p^{\perp}$ where $E_p = \left[J_p, F_p^{\perp}\right] + \left[J_p^{\perp}, F_p\right]$.

Let $p = v_2$. Then $E_p = j + h + e$.

Make orientation for $j = \{v_2, v_3\}$.

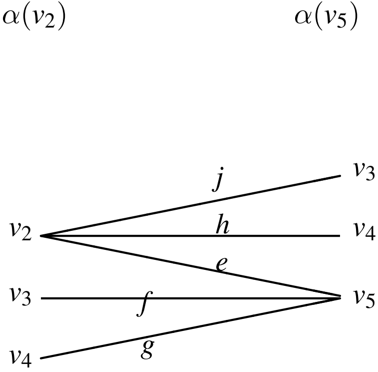
$j = [f, e] + [h, i] + [i, h]$ in $\gamma(e) = \left[\gamma(j),\ \gamma(f)\right]$
where $[f, e] = [\{v_3, v_5\}, \{v_5, v_2\}]$ is in $[J_p^{\perp}, F_p]$
$[h, i] = [\{v_2, v_4\}, \{v_4, v_3\}]$ is in $[J_p, F_p^{\perp}]$
$[i, h] = [\{v_3, v_4\}, \{v_4, v_2\}]$ is in $[J_p^{\perp}, F_p]$.

Hence $j = [h, i] = [\{v_2, v_4\}, \{v_4, v_3\}]$ is in $[J_p, F_p^{\perp}]$.
$j = \{v_2, v_3\}$ is oriented v_2 in $\gamma(j)$-side, that is $\alpha(v_2)$-side.



$\gamma(e)$ with respect to $\mathfrak{C}_{[0]}$

$\Longrightarrow$



Oriented form of $\gamma(e)$

Futher problems of $\mathcal{O}(n)$ as automorphisms.

1. Extending $GF(2)$ to characteristic 2 in general.

   Suppose $ax = [by, cz]$.

   $a = bc$, $b = ca$ and $c = ab$ iff $a = b = c = 1 \in \mathbb{F}_2(\theta)$.

   The triangle multiplication property no longer works in characteristic 2.

Futher problems of $\mathcal{O}(n)$ as automorphisms.

1. Extending $GF(2)$ to characteristic 2 in general.

   Suppose $ax = [by, cz]$.

   $a = bc$, $b = ca$ and $c = ab$ iff $a = b = c = 1 \in \mathbb{F}_2(\theta)$.

   The triangle multiplication property no longer works in characteristic 2.

2. Inverse Galois Problem: $\mathcal{O}(n) = \mathrm{Gal}\big(\mathbb{Q}(\ldots\ldots)/\mathbb{Q}(\ldots)\big)$.

   Our approach is from: $\mathcal{O}(n) = \mathrm{Aut}(L_0)$.