A Mathematician’s Insight into the Saniga-Planat Theorem

Finite Projective Geometries in Quantum Theory (A Mini-Workshop)

Tatranská Lomnica, August 2nd, 2007

TU WIEN

TECHNISCHE UNIVERSITÄT WIEN

VIENNA UNIVERSITY OF TECHNOLOGY

DIFFERENTIALGEOMETRIE UND GEOMETRISCHE STRUKTUREN

HANS HAVLICEK

FORSCHUNGSGRUPPE DIFFERENTIALGEOMETRIE UND GEOMETRISCHE STRUKTUREN

INSTITUT FÜR DISKRETE MATHEMATIK UND GEOMETRIE

TECHNISCHE UNIVERSITÄT WIEN

havlicek@geometrie.tuwien.ac.at

Bridging the Gap

The Saniga-Planat Theorem links

- Kronecker products of Pauli matrices,
- symplectic polar spaces over $\mathrm{GF}(2)$,
- finite-dimensional vector spaces over $\mathrm{GF}(2)$ which are endowed with a non-degenerate alternating bilinear form.

Pauli Matrices

We consider the Pauli matrices

$$\sigma_1 := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ \sigma_2 := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \ \sigma_3 := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{1}$$

with entries in $\mathbb{C}$. Each σ_p is Hermitian, i. e. $\sigma_p = \sigma_p^{\mathrm{H}}$ (Hermitian transpose, conjugate transpose) and unitary, i. e. $\sigma_p^{-1} = \sigma_p^{\mathrm{H}}$. Hence $\sigma_p^{-1} = \sigma_p$.

Let $(G, \cdot)$ be the subgroup of the unitary group $(\mathrm{U}_2, \cdot)$ generated by $\sigma_1, \sigma_2, \sigma_3$. This group G consists of all finite products of Pauli matrices and their inverses.
(An empty product is, by definition, the identity matrix, which will be denoted by σ_0.)

Problem

Problem 1. Given the group $(G, \cdot)$ we aim at constructing “in a natural way”:

- The Galois field with two elements, i. e. $(\mathrm{GF}(2), +, \cdot)$,
- A two-dimensional vector space over the field $(\mathrm{GF}(2), +, \cdot)$.

Multiplication in G

Multiplication in G is governed by the following system of relations:

$$\begin{aligned}
&\sigma_p\sigma_p = \sigma_0 && \text{for all } p \in \{1,2,3\}, \\
&\sigma_p\sigma_q = i\sigma_r && \text{for all even permutations } \begin{pmatrix} 1 & 2 & 3 \\ p & q & r \end{pmatrix}, \\
&\sigma_p\sigma_q = -i\sigma_r && \text{for all odd permutations } \begin{pmatrix} 1 & 2 & 3 \\ p & q & r \end{pmatrix}.
\end{aligned} \tag{2}$$

G is finite

The group G has precisely $16 = 2^4$ elements:

$$G = \left\{ i^j \sigma_k \mid j, k \in \{0, 1, 2, 3\} \right\} \tag{3}$$

It is a non-commutative group, because

$$\sigma_p \sigma_q = -\sigma_q \sigma_p \text{ for all } p, q \in \{1, 2, 3\} \text{ with } p \neq q.$$

So G cannot be isomorphic to the additive group of any vector space.

The additive group of any vector space is commutative.

The Centre of G

The centre of G equals

$$Z(G) = \left\{ i^j \sigma_0 \mid j \in \{0, 1, 2, 3\} \right\}. \tag{4}$$

It is isomorphic to the cyclic group $(\mathbb{Z}_4, +)$, whence it cannot be isomorphic to the additive group of a vector space.

Any non-zero vector $\vec{v}$ of a vector space over a field $\mathbb{F}$ generates (with respect to addition) a cyclic group which is either isomorphic to $(\mathbb{Z}, +)$ or isomorphic to $(\mathbb{Z}_p, +)$, where $p = \operatorname{Char} \mathbb{F}$ is a prime number.

The Commutator Subgroup of G

The group theoretic commutator of $\alpha, \beta \in G$ is defined as

$$[\alpha, \beta] := \alpha\beta\alpha^{-1}\beta^{-1}.$$

It is not to be confused with their ring theoretic commutator $\alpha\beta - \beta\alpha$, which is usually also written as $[\alpha, \beta]$, but will not be used throughout this lecture!

Hence

$$[\alpha, \beta]\beta\alpha := \alpha\beta.$$

The commutator subgroup $[G, G]$ of G is the subgroup generated by all commutators $[\alpha, \beta]$, where α and β range in G. From (2), (3), and (4) one easily obtains

$$[G, G] = \{\sigma_0, -\sigma_0\} \cong \mathbb{Z}_2. \tag{5}$$

In fact, $([G, G], \cdot)$ is isomorphic to the additive group of $\mathrm{GF}(2)$ via $\sigma_0 \mapsto 0$, $-\sigma_0 \mapsto 1$.

Result

The commutator subgroup $([G, G], \cdot)$ can serve as a model of the additive group of the Galois field $\mathrm{GF}(2)$.

Note that multiplication in this field is trivial.

The Significance of $[G, G]$

Let Γ and Γ' be arbitrary groups and $f : \Gamma \to \Gamma'$ a homomorphism. The image $f(\Gamma)$ is a commutative subgroup of Γ' if, and only if,

$$[\Gamma, \Gamma] \subset \ker f.$$

Or, in other words: Given a normal subgroup Σ of Γ the factor group Γ/Σ is commutative if, and only if, $[\Gamma, \Gamma] \subset \Sigma$.

Returning to our settings we obtain

$$G/[G, G] \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Hence $G/[G, G]$ is isomorphic to the additive group of a three-dimensional vector space over $\mathrm{GF}(2)$.

What is the geometric meaning (if any) of the group $G/[G, G]$?

The Centre Revisited

Since $Z(G) = \{\sigma_0, -\sigma_0, i\sigma_0, -i\sigma_0\}$ contains $[G, G] = \{\sigma_0, -\sigma_0\}$, the factor group

$$G/Z(G) = \{Z(G)\sigma_0, Z(G)\sigma_1, Z(G)\sigma_2, Z(G)\sigma_3\} \tag{6}$$

is a commutative group of order $16 : 4 = 4$. Each of its elements coincides with its inverse, so we have

$$G/Z(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

For example, an isomorphism is given by

$$Z(G)\sigma_0 \mapsto (0,0),\ Z(G)\sigma_1 \mapsto (1,0),\ Z(G)\sigma_2 \mapsto (0,1),\ Z(G)\sigma_3 \mapsto (1,1).$$

Result

The factor group $(G/Z(G), \cdot)$ is isomorphic to the additive group of a two-dimensional vector space over $\mathrm{GF}(2)$.

Problem

Problem 2. Endow the vector space $G/Z(G)$ with a non-degenerate alternating bilinear form which reflects in some way if two elements of G commute or not.

The Commutator Subgroup Revisited

Let Γ be an arbitrary group. The following properties hold for all $\alpha, \alpha_1, \alpha_2, \beta \in \Gamma$:

$$
\begin{aligned}
[\alpha, \alpha] &= \iota \text{ (the identity in } \Gamma\text{).} \\
[\beta, \alpha] &= \beta\alpha\beta^{-1}\alpha^{-1} = (\alpha\beta\alpha^{-1}\beta^{-1})^{-1} = [\alpha, \beta]^{-1}. \\
[\alpha_1\alpha_2, \beta] &= (\alpha_1\alpha_2)\beta(\alpha_1\alpha_2)^{-1}\beta^{-1} \\
&= \alpha_1 \underbrace{\alpha_2\beta\alpha_2^{-1}\beta^{-1}} \alpha_1^{-1} \underbrace{\alpha_1\beta\alpha_1^{-1}\beta^{-1}} \\
&= \alpha_1[\alpha_2, \beta]\alpha_1^{-1} \cdot [\alpha_1, \beta].
\end{aligned}
$$

We have $[G, G] = \{\sigma_0, -\sigma_0\}$, whence for G these formulas turn into

$$
\begin{aligned}
[\alpha, \alpha] &= \sigma_0. \\
[\beta, \alpha] &= [\alpha, \beta]. \\
[\alpha_1\alpha_2, \beta] &= [\alpha_1, \beta] \cdot [\alpha_2, \beta].
\end{aligned}
\tag{7}
$$

The Commutator Mapping

Let $\alpha, \beta \in G$. Then

$$\begin{aligned} [Z(G)\alpha, Z(G)\beta] &= [Z(G), Z(G)] \cdot [Z(G), \beta] \cdot [\alpha, Z(G)] \cdot [\alpha, \beta] \\ &= [\alpha, \beta]. \end{aligned}$$

Thus, $[\alpha, \beta]$ remains unaltered if α and β are replaced with any other element of $Z(G)\alpha$ and $Z(G)\beta$, respectively.

Altogether we obtain a well defined mapping

$$G/Z(G) \times G/Z(G) \to [G, G] : \big(Z(G)\alpha, Z(G)\beta\big) \mapsto [\alpha, \beta]$$

which, by abuse of notation, will also be denoted by $[\cdot, \cdot]$. For all $\alpha, \beta \in G$ we have

$$\alpha\beta = \beta\alpha \quad \Leftrightarrow \quad [\alpha, \beta] = \sigma_0 \quad \Leftrightarrow \quad \big[Z(G)\alpha, Z(G)\beta\big] = \sigma_0.$$

An Alternating Bilinear Form

The ultimate step merely amounts to applying the isomorphisms from the above:

$$\begin{aligned} G/Z(G) \to \mathrm{GF}(2)^2 \quad &: \quad Z(G)\sigma_0 \mapsto (0,0),\ Z(G)\sigma_1 \mapsto (1,0), \\ &\quad\ \ Z(G)\sigma_2 \mapsto (0,1),\ Z(G)\sigma_3 \mapsto (1,1). \\ [G,G] \to \mathrm{GF}(2) \quad &: \quad \sigma_0 \mapsto 0,\ -\sigma_0 \mapsto 1. \end{aligned}$$

By virtue of these isomorphisms, we obtain a mapping

$$[\cdot,\cdot] : \mathrm{GF}(2)^2 \times \mathrm{GF}(2)^2 \to \mathrm{GF}(2).$$

Due to (7) and the trivial multiplication in $\mathrm{GF}(2)$, this is an alternating bilinear form.

Result

The mapping $[\cdot,\cdot] : \mathrm{GF}(2)^2 \times \mathrm{GF}(2)^2 \to \mathrm{GF}(2)$ is an alternating bilinear form. Its matrix with respect to the standard basis of $\mathrm{GF}(2)^2$ equals

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

i. e., we have a non-degenerate form.

Summary

We have an exact sequence of groups

$$
\begin{array}{ccccccccc}
\{1\} & \longrightarrow & Z(G) & \longrightarrow & G & \longrightarrow & \underbrace{G/Z(G)}_{\cong \mathrm{GF}(2)^2} & \longrightarrow & \{1\} \\
\hline
1 & \longmapsto & \sigma_0 & & & & & & \\
 & & \alpha & \longmapsto & \alpha & & & & \\
 & & & & \beta & \longmapsto & Z(G)\beta & & \\
 & & & & & & Z(G)\gamma & \longmapsto & 1
\end{array}
$$

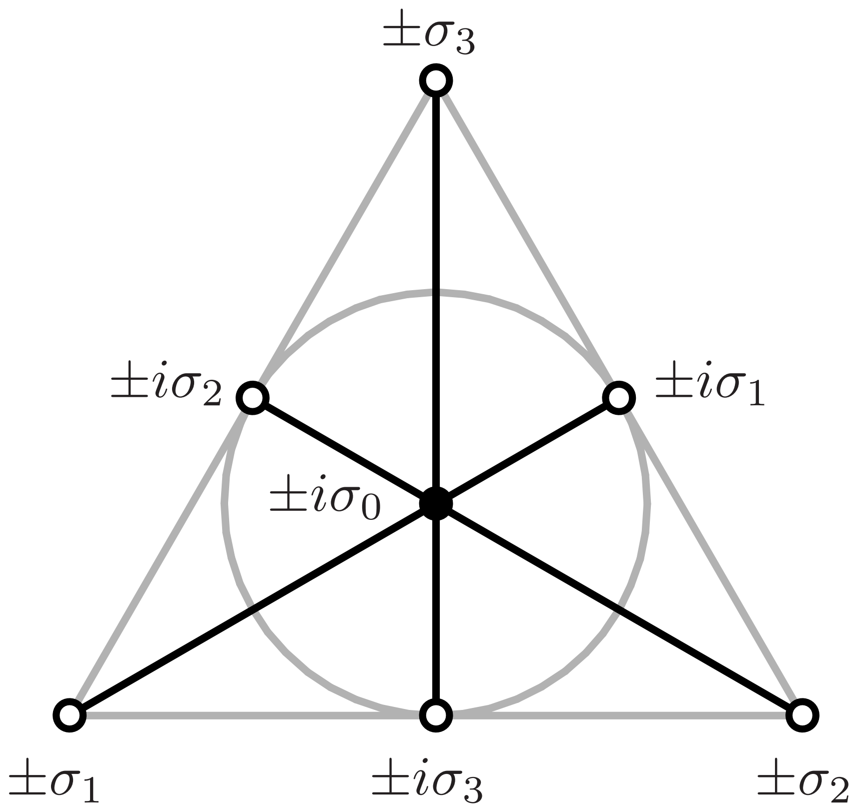
and the following commutative diagram:

$$
\begin{tikzcd}
G \times G \arrow[rr] \arrow[dr, "{[\cdot,\cdot]}"'] & & \underbrace{G/Z(G) \times G/Z(G)}_{\cong \mathrm{GF}(2)^2 \times \mathrm{GF}(2)^2} \arrow[dl, "{[\cdot,\cdot]}"] \\
 & \underbrace{[G,G]}_{\cong \mathrm{GF}(2)} &
\end{tikzcd}
$$

(Koen Thas, 2007.)

Remark

The group $G/[G,G]$ (without its identity element) may be illustrated as the smallest projective plane. It is endowed with a degenerate symplectic polarity which assigns to each point $p \neq \pm i\sigma_0$ the unique line through p and $\pm i\sigma_0$. The lines through $\pm i\sigma_0$ represent commuting elements of $G \setminus \{\pm\sigma_0\}$.



Part 2

Kronecker Products

We now extend our results from the first part of this lecture to Kronecker products of Pauli matrices.

This will be a straightforward task.

The Group G_N

Let $N \geq 1$ be a fixed integer. We consider N-fold Kronecker products of the identity matrix σ_0 and the Pauli matrices

$$\sigma_1 := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ \sigma_2 := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \ \sigma_3 := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

There are 4^N such products, all of them unitary, and they form a basis of the space of complex $2^N \times 2^N$ matrices.

Let $(G_N, \cdot)$ be the subgroup of the unitary group $(\mathrm{U}_{2^N}, \cdot)$ generated by all products

$$\sigma_{p_1} \otimes \sigma_{p_2} \otimes \cdots \otimes \sigma_{p_N} \ \text{ with } \ p_1, p_2, \ldots p_N \in \{0, 1, 2, 3\}.$$

Problem

Problem 3. Given the group $(G_N, \cdot)$ we aim at constructing "in a natural way":

- The Galois field with two elements, i. e. $(\mathrm{GF}(2), +, \cdot)$,
- A 2^N-dimensional vector space over the field $(\mathrm{GF}(2), +, \cdot)$.

G_N is finite

For all $p_1, p_2, \ldots p_N, q_1, q_2, \ldots, q_N \in \{0,1,2,3\}$ and all $z \in \mathbb{C}$ the following hold:

$$
\begin{aligned}
(\sigma_{p_1} \otimes \sigma_{p_2} \otimes \cdots \otimes \sigma_{p_N})(\sigma_{q_1} \otimes \sigma_{q_2} \otimes \cdots \otimes \sigma_{q_N}) &= (\sigma_{p_1}\sigma_{q_1}) \otimes (\sigma_{p_2}\sigma_{q_2}) \otimes \cdots \otimes (\sigma_{p_N}\sigma_{q_N}) \\
(\sigma_{p_1} \otimes \sigma_{p_2} \otimes \cdots \otimes \sigma_{p_N})^{-1} &= \sigma_{p_1}^{-1} \otimes \sigma_{p_2}^{-1} \otimes \cdots \otimes \sigma_{p_N}^{-1} \\
\sigma_{p_1} \otimes \cdots \otimes (z\sigma_{p_k}) \otimes \cdots \otimes \sigma_{p_N} &= z(\sigma_{p_1} \otimes \cdots \otimes \sigma_{p_k} \otimes \cdots \otimes \sigma_{p_N})
\end{aligned}
$$

The last equation will only be used for $z \in \{1, -1, i, -i\}$.

The group G_N has precisely 4^{N+1} elements,

$$G_N = \{i^j(\sigma_{p_1} \otimes \sigma_{p_2} \otimes \cdots \otimes \sigma_{p_N}) \mid j, p_1, p_2, \ldots p_N \in \{0,1,2,3\}\}, \tag{8}$$

and it is a non-commutative group, because $G \otimes \sigma_0 \otimes \cdots \otimes \sigma_0$ is a subgroup of G_N isomorphic to G. So G_N cannot be isomorphic to the additive group of any vector space.

The Centre of G_N

Fix an index $k \in \{1, 2, \dots, N\}$. An arbitrary element of G_N, say

$$i^j(\sigma_{p_1} \otimes \cdots \otimes \sigma_{p_k} \otimes \cdots \otimes \sigma_{p_N}),$$

is permutable with all elements of

$$\sigma_0 \otimes \cdots \sigma_0 \otimes \underbrace{G}_{k} \otimes \sigma_0 \otimes \cdots \otimes \sigma_0 \subset G_N$$

if, and only if, $\sigma_{p_k} = \sigma_0$. As k varies, we obtain:

The centre of G_N equals the cyclic group

$$Z(G_N) = \left\{ i^j(\sigma_0 \otimes \sigma_0 \otimes \cdots \otimes \sigma_0) \mid j \in \{0, 1, 2, 3\} \right\} \cong \mathbb{Z}_4, \tag{9}$$

whence it cannot be isomorphic to the additive group of a vector space.

The Commutator Subgroup of G_N

It is easy to calculate commutators in G_N, since we have

$$[i^j(\sigma_{p_1} \otimes \cdots \otimes \sigma_{p_N}), i^k(\sigma_{q_1} \otimes \cdots \otimes \sigma_{q_N})] = [\sigma_{p_1}, \sigma_{q_1}] \otimes \cdots \otimes [\sigma_{p_N}, \sigma_{q_N}]. \tag{10}$$

From (10) one immediately obtains

$$[G_N, G_N] = \{\sigma_0 \otimes \sigma_0 \otimes \cdots \otimes \sigma_0, -(\sigma_0 \otimes \sigma_0 \otimes \cdots \otimes \sigma_0)\} \cong \mathbb{Z}_2. \tag{11}$$

In fact, $([G_N, G_N], \cdot)$ is isomorphic to the additive group of $\mathrm{GF}(2)$ via

$$\sigma_0 \otimes \sigma_0 \otimes \cdots \otimes \sigma_0 \mapsto 0, \quad -(\sigma_0 \otimes \sigma_0 \otimes \cdots \otimes \sigma_0) \mapsto 1.$$

Result

The commutator subgroup $([G_N, G_N], \cdot)$ can serve as a model of the additive group of the Galois field $\mathrm{GF}(2)$.
Note that multiplication in this field is trivial.

Factoring through $[G_N, G_N]$

Now we exhibit the factor group $G_N/[G_N, G_N]$. From

$$i^j(\sigma_{p_1} \otimes \sigma_{p_2} \otimes \cdots \otimes \sigma_{p_N}) \cdot i^j(\sigma_{p_1} \otimes \sigma_{p_2} \otimes \cdots \otimes \sigma_{p_N}) = (-1)^j(\sigma_0 \otimes \sigma_0 \otimes \cdots \otimes \sigma_0)$$

each element of $G_N/[G_N, G_N]$ coincides with its inverse.

Since $4^{N+1} : 2 = 2^{2N+1}$, we obtain

$$G_N/[G_N, G_N] \cong \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2}_{2N+1}.$$

Hence $G_N/[G_N, G_N]$ is isomorphic to the additive group of a $2N + 1$-dimensional vector space over $\mathrm{GF}(2)$.

What is the geometric meaning (if any) of the group $G_N/[G_N, G_N]$?

The Centre Revisited

The factor group

$$G_N/Z(G_N) = \big\{Z(G_N)(\sigma_{p_1} \otimes \sigma_{p_2} \otimes \cdots \otimes \sigma_{p_N}) \mid p_1, p_2, \ldots p_N \in \{0,1,2,3\}\big\} \qquad (12)$$

is a commutative group of order $4^{N+1} : 4 = 4^N$, since the centre $Z(G_N)$ contains the commutator subgroup $[G_N, G_N]$. Each element of $G_N/Z(G_N)$ coincides with its inverse, so

$$G_N/Z(G_N) \cong \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2}_{2N}.$$

In order to describe an isomorphism explicitly, we use a function

$$\vartheta : \{0,1,2,3\} \to \mathbb{Z}_2^2 : 0 \mapsto (0,0),\ 1 \mapsto (1,0),\ 2 \mapsto (0,1),\ 3 \mapsto (1,1).$$

Then an isomorphism is given by

$$Z(G_N)(\sigma_{p_1} \otimes \sigma_{p_2} \otimes \cdots \otimes \sigma_{p_N}) \mapsto \big(\vartheta(p_1), \vartheta(p_2), \ldots, \vartheta(p_N)\big).$$

Result

The factor group $(G_N/Z(G_N), \cdot)$ is isomorphic to the additive group of a 2^N-dimensional vector space over $\mathrm{GF}(2)$.

Problem

Problem 4. Endow the vector space $G_N/Z(G_N)$ with a non-degenerate alternating bilinear form which reflects in some way if two elements of G_N commute or not.

The Commutator Subgroup Revisited

Recall that

$$[G_N, G_N] = \{\sigma_0 \otimes \sigma_0 \otimes \cdots \otimes \sigma_0, -\sigma_0 \otimes \sigma_0 \otimes \cdots \otimes \sigma_0\}$$

is isomorphic to $\mathbb{Z}_2$. Hence the following properties hold for all $\alpha, \alpha_1, \alpha_2, \beta \in G_N$:

$$\begin{aligned} [\alpha, \alpha] &= \sigma_0 \otimes \sigma_0 \otimes \cdots \otimes \sigma_0. \\ [\beta, \alpha] &= [\alpha, \beta]. \\ [\alpha_1 \alpha_2, \beta] &= [\alpha_1, \beta] \cdot [\alpha_2, \beta]. \end{aligned} \tag{13}$$

The Commutator Mapping

Let $\alpha, \beta \in G_N$. Then

$$\begin{aligned}[Z(G_N)\alpha, Z(G_N)\beta] &= [Z(G_N), Z(G_N)] \cdot [Z(G_N), \beta] \cdot [\alpha, Z(G_N)] \cdot [\alpha, \beta] \\ &= [\alpha, \beta].\end{aligned}$$

Thus, $[\alpha, \beta]$ remains unaltered if α and β are replaced with any other element of $Z(G_N)\alpha$ and $Z(G_N)\beta$, respectively.

Altogether we obtain a well defined mapping

$$G_N/Z(G_N) \times G_N/Z(G_N) \to [G_N, G_N] : \big(Z(G_N)\alpha, Z(G_N)\beta\big) \mapsto [\alpha, \beta]$$

which, by abuse of notation, will also be denoted by $[\cdot, \cdot]$. For all $\alpha, \beta \in G_N$ we have

$$\alpha\beta = \beta\alpha \;\Leftrightarrow\; [\alpha, \beta] = \sigma_0 \otimes \sigma_0 \otimes \cdots \otimes \sigma_0 \;\Leftrightarrow\; \big[Z(G_N)\alpha, Z(G_N)\beta\big] = \sigma_0 \otimes \sigma_0 \otimes \cdots \otimes \sigma_0.$$

An Alternating Bilinear Form

The ultimate step merely amounts to applying the isomorphisms from the above:

$$\begin{aligned} G_N/Z(G_N) \to \mathrm{GF}(2)^{2N} \quad &: \quad Z(G_N)(\sigma_{p_1} \otimes \sigma_{p_2} \otimes \cdots \otimes \sigma_{p_N}) \mapsto \big(\vartheta(p_1), \vartheta(p_2), \ldots, \vartheta(p_N)\big). \\ [G_N, G_N] \to \mathrm{GF}(2) \quad &: \quad \sigma_0 \otimes \sigma_0 \otimes \cdots \otimes \sigma_0 \mapsto 0, \quad -\sigma_0 \otimes \sigma_0 \otimes \cdots \otimes \sigma_0 \mapsto 1. \end{aligned}$$

By virtue of these isomorphisms, we obtain a mapping

$$[\cdot, \cdot] : \mathrm{GF}(2)^{2N} \times \mathrm{GF}(2)^{2N} \to \mathrm{GF}(2).$$

Due to (13) and the trivial multiplication in $\mathrm{GF}(2)$, this is an alternating bilinear form.

Result

The mapping $[\cdot,\cdot] : \mathrm{GF}(2)^{2N} \times \mathrm{GF}(2)^{2N} \to \mathrm{GF}(2)$ is an alternating bilinear form. Its matrix with respect to the standard basis of $\mathrm{GF}(2)^2$ equals

$$\mathrm{diag}\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right),$$

i. e., we have a non-degenerate form.

Summary

We have an exact sequence of groups

$$
\begin{array}{ccccccccc}
\{1\} & \rightarrow & Z(G_N) & \rightarrow & G_N & \rightarrow & \underbrace{G_N/Z(G_N)}_{\cong \mathrm{GF}(2)^{2N}} & \rightarrow & \{1\} \\
\hline
1 & \mapsto & \sigma_0 \otimes \cdots \otimes \sigma_0 & & & & & & \\
 & & \alpha & \mapsto & \alpha & & & & \\
 & & & & \beta & \mapsto & Z(G_N)\beta & & \\
 & & & & & & Z(G_N)\gamma & \mapsto & 1
\end{array}
$$

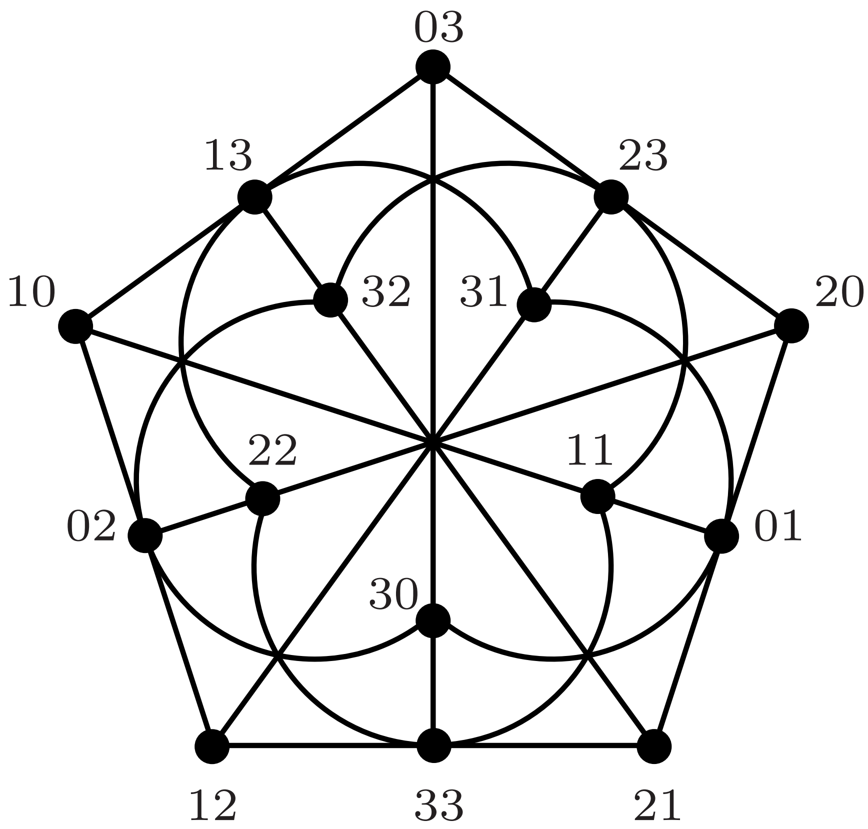
and the following commutative diagram:

$$
\begin{tikzcd}
G_N \times G_N \arrow[rr] \arrow[dr, "{[\cdot,\cdot]}"'] & & \underbrace{G_N/Z(G_N) \times G_N/Z(G_N)}_{\cong \mathrm{GF}(2)^{2N} \times \mathrm{GF}(2)^{2N}} \arrow[dl, "{[\cdot,\cdot]}"] \\
& \underbrace{[G_N, G_N]}_{\cong \mathrm{GF}(2)} &
\end{tikzcd}
$$

(Koen Thas, 2007.)

An Illustration

In our illustration of the case $N = 2$ the element $Z(G_2)\sigma_j \otimes \sigma_k$ is denoted by jk.



(Metod Saniga, 2007.)