2
Preliminares

2.1
Ação de Grupos

Uma **ação (à esquerda)** de um grupo $(G, \cdot)$ sobre um conjunto não-vazio X é uma aplicação

$$\begin{array}{rccc} \circ: & G \times X & \longrightarrow & X \\ & (g, x) & \longmapsto & g \circ x \end{array}$$

que satisfaz:

1. $e \circ x = x, \forall x \in X$.
2. $(g \cdot h) \circ x = g \circ (h \circ x), \forall g, h \in G, \forall x \in X$.

Neste caso, dizemos que G age sobre X.

De maneira análoga, definimos uma **ação (à direita)** de um grupo $(G, \cdot)$ sobre um conjunto não-vazio X como sendo a aplicação

$$\begin{array}{rccc} \circ: & X \times G & \longrightarrow & X \\ & (x, g) & \longmapsto & x \circ g \end{array}$$

que satisfaz:

1. $x \circ e = x, \forall x \in X$.
2. $x \circ (g \cdot h) = (x \circ g) \circ h, \forall g, h \in G, \forall x \in X$.

Em particular, se G é um grupo de permutações do conjunto $\Omega = \{1, 2, ..., n\}$, então a aplicação

$$\begin{array}{rccc} \circ: & G \times \Omega & \longrightarrow & \Omega \\ & (\sigma, j) & \longmapsto & \sigma \circ j \quad = \sigma(j) \end{array}$$

é uma ação de G sobre Ω.

Sejam X um conjunto não-vazio e G um grupo que age sobre X. A **órbita** $G(x)$ de um elemento x em X é definida por

$$G(x) = \{g \circ x \mid g \in G\}.$$

O **comprimento** $|G(x)|$ da órbita de x é a cardinalidade de $G(x)$. O conjunto das órbitas em X sobre a ação de G particionam X. A relação de equivalência associada é definida por: $x \sim y$, se e somente se, existe $g \in G$ tal que $g \circ x = y$.

Todo grupo G age sobre si mesmo por conjugação. Definindo $g \circ x = g^{-1}xg$, as órbitas são as classes de conjugação $[x] = \{g^{-1}xg \mid g \in G\}$.

Fixado x em X, o **estabilizador** de x é o subgrupo H_x de G consistindo de todos os elementos de G que aplicam x nele mesmo. Isto é,

$$H_x = \{g \in G \mid g \circ x = x\}.$$

Então podemos reinterpretar o Teorema de Lagrange como o Teorema órbita-estabilizador, que diz que o número de imagens de x sobre G é igual a $\frac{|G|}{|H_x|}$, isto é

$$[G : H_x] = \frac{|G|}{|H_x|} = |G(x)|.$$

Dado um conjunto finito Ω, denote por S_Ω o grupo de todas as permutações de Ω. Dizemos que um grupo G age **fielmente** sobre Ω se, e somente se, existe um homomorfismo injetor $\varphi : G \to S_\Omega$. Intuitivamente, isso significa que diferentes elementos de G induzem diferentes permutações.

2.2 Transitividade

Seja G um grupo de permutações agindo em um conjunto Ω com n elementos. Se para quaisquer dois pontos distintos x e y de Ω existe um elemento π de G que aplica x em y dizemos que G **é transitivo em** Ω. Em outras palavras, isso significa que para quaisquer x e y em Ω existe $\pi \in G$ tal que $x^\pi = y$. Mais geralmente, dizemos que G é k**-transitivo**, $k \leq n$, se para quaisquer dois conjuntos de pontos $x_1, ..., x_k$ e $y_1, ..., y_k$ com a propriedade que todos os x_i e todos os y_i são distintos $(1 \leq i \leq k)$ existe um elemento $\pi \in G$ que aplica x_i em y_i, para todo i. Em particular, 1-transitivo é o mesmo que transitivo.

O grupo S_n das permutações de n elementos é k-transitivo para todo $k \leq n$, e o grupo A_n das permutações pares de n elementos é k-transitivo para todo $k \leq n - 2$.

Observação 2.2.1. A notação de composição de duas permutações $\pi\rho$ não segue o padrão usual de composições de funções. Mais precisamente, $\pi\rho$

significa que aplicamos π e em seguida ρ. A fim de evitar essa confusão, escreveremos a^π ao invés de $\pi(a)$ e $a^{\pi\rho} = \pi(\rho(a))$ e as permutações são lidas da esquerda para a direita.

2.3 Primitividade

Seja H um grupo que age sobre um conjunto finito Ω_H. Uma **partição** de Ω_H é uma família de subconjuntos não-vazios de Ω_H cuja união é Ω_H. Chamamos os elementos da partição de blocos. Dizemos que uma partição é **preservada** por H quando para quaisquer a e b pertencentes ao mesmo bloco da partição de Ω_H, e para qualquer π de H, tem-se que os pontos a^π e b^π ainda estão no mesmo bloco.

Um **sistema bloco** para H é uma partição de Ω_H preservada por H. Há 2 sistemas blocos sempre preservados por qualquer grupo: um é a partição cujo único bloco é Ω_H, e o outro é a partição cujos blocos consistem de um único ponto de Ω_H. Esses são os sistemas blocos triviais. Um sistema bloco não trivial é dito um **sistema de imprimitividade**. Para $n \geq 3$, o grupo que admite sistema de imprimitividade é chamado **imprimitivo**, e um grupo não trivial que não é imprimitivo é dito **primitivo**. Dizemos que H **age primitivamente** em Ω_H quando o único sistema bloco que ele admite é o trivial. Observe que

$$\text{se } H \text{ é primitivo então } H \text{ é transitivo.} \tag{2.3.1}$$

De fato, se H não é transitivo então as órbitas de H formam um sistema de imprimitividade, logo H é imprimitivo. Mas a recíproca em geral não é verdadeira. Por exemplo, o subgrupo H de S_4, $|H| = 4$, gerado por $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ e $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ é transitivo e admite três sistemas de imprimitividade. A saber, $\{\{1,2\},\{3,4\}\}; \{\{1,3\},\{2,4\}\}; \{\{1,4\},\{2,3\}\}$. É claro que em um sistema bloco para um grupo transitivo imprimitivo todos os blocos tem que ter o mesmo tamanho. Porém, para grupos 2-transitivos a recíproca de (2.3.1) é válida, isto é,

todo grupo 2-transitivo é primitivo.

Provemos este fato pela contra-positiva. Seja H um grupo imprimitivo. Como Ω_H tem pelo menos três elementos a, b e c, e admite sistema de imprimitividade então temos pelo menos 2 blocos. Digamos que a e b estão em um bloco e c está em um outro bloco. Portanto não pode existir elemento em H que leve (a, b) em (a, c). Logo H não é 2-transitivo.

Proposição 2.3.1. *Suponha que o grupo G age transitivamente em Ω_G e seja H o subgrupo de G estabilizador de algum $a \in \Omega_G$. Então G age primitivamente em Ω_G se e somente se H é subgrupo maximal de G.*

Demonstração. Veja (9). □

Lema 2.3.2. ***(Lema de Iwasawa)*** *Se G é um grupo finito perfeito, agindo fielmente e primitivamente em um conjunto Ω_H, tal que um estabilizador pontual H tem um subgrupo normal abeliano A cujos conjugados geram G, então G é simples.*

Demonstração. Suponha K um subgrupo normal de G, $1 \lneq K \lhd G$, cujos elementos não fixam todos os elementos de Ω_H. Vamos provar que $K = G$. Podemos supor H o estabilizador pontual de $x \in \Omega_H$, com $K \lneq H$. Pela proposição 2.3.1 segue que H é um subgrupo maximal de G. como $K \lhd G$ temos $HK = \{hk, h \in H, k \in K\} = KH$. De fato, pois para qualquer $h \in H$ e $k \in K$ tem-se $hk = hkh^{-1}h = \tilde{k}h$, para algum $\tilde{k} \in K$. Donde, $H \lneq HK < G$ e como H é maximal segue que $HK = G$. Por hipótese, H tem um subgrupo normal abeliano A cujos conjugados geram G logo $AK < G$. Daí, e como todo elemento g de G pode ser escrito como $g = hk$ para algum $h \in H$ e $k \in K$ temos que

$$gag^{-1} = k^{-1}\underbrace{h^{-1}ah}_{\in A}k \underset{\substack{\uparrow \\ \exists \tilde{a} \in A}}{=} k^{-1}\tilde{a}k = \tilde{a}\underbrace{\tilde{a}^{-1}k^{-1}\tilde{a}}_{\in K}k \in AK$$

Logo $G = AK$. Portanto $G/K = AK/K \cong A/K \cap A$ e $A/K \cap A$ é abeliano (pois A é abeliano). Donde temos G/K abeliano. Como, por hipótese, G é perfeito segue $K = G$. Logo G é simples. □

2.4 Grupo perfeito

Seja G um grupo. Um elemento da forma $xyx^{-1}y^{-1}$, para $x, y \in G$ gerado, chama-se um **comutador**. O subgrupo de G gerado pelo conjunto dos comutadores é dito o **subgrupo comutador ou (subgrupo derivado)** de G e denota-se por $[G, G]$ ou G'.

Por exemplo, quando G é um grupo abeliano, o subgrupo comutador de G é o trivial, pois $xyx^{-1}y^{-1} = e$ para todo $x, y \in G$.

O subgrupo comutador $[G, G]$ de G é um subgrupo normal de G e $G/[G, G]$ é abeliano. Mais ainda, o subgrupo comutador é o menor subgrupo de G tal que o quociente é abeliano. Em outras palavras, G/N é abeliano se, e somente se, N contém o subgrupo comutador.

Dizemos que G é **perfeito** quando $G = [G, G]$ ou, equivalentemente, quando não existe subgrupo normal não trivial H de G tal que G/H seja abeliano. Por exemplo, todo grupo simples não abeliano é perfeito.

2.5 Produtos diretos e semi-diretos

Sejam G e H dois grupos. O **produto direto** de G e H é:

$$G \times H = \{(g, h) | g \in G, h \in H\}, \text{ onde}$$

o elemento neutro do grupo é $1_{G\times H} = (1_G, 1_H)$ e as operações do grupo são:

$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$$
$$(g, h)^{-1} = (g^{-1}, h^{-1}).$$

A fim de definirmos o produto semi-direto de G e H, $G : H$, suponha que podemos definir o homomorfismo ϕ abaixo que descreve a ação de G em H.

$$\begin{array}{rccccccc} \phi: & H & \longrightarrow & Aut(G) & & & & \\ & h & \longmapsto & \phi_h: & G & \longrightarrow & G \\ & & & & g & \longmapsto & \phi_h(g) \end{array}$$

O **produto semi-direto** de G e H é:

$$G : H = \{(g, h) \mid g \in G,\ h \in H\}, \text{ onde}$$

elemento neutro do grupo é $1_{G:H} = (1_G, 1_H)$ e as operações do grupo são:

$$(g_1, h_1)(g_2, h_2) = (g_1 \phi_{h_1}^{-1}(g_2), h_1 h_2)$$
$$(g, h)^{-1} = (\phi_h(g^{-1}), h^{-1}).$$

Seja L um grupo com subgrupos L_0 e L_1, tais que $L_0 \cap L_1 = \{e\}$. Considere o conjunto L_2

$$L_2 = L_0 L_1 = \{l_0 l_1 |\ l_0 \in L_0, l_1 \in L_1\}.$$

Em geral, L_2 não é subgrupo de L. Por exemplo, tomando $L = S_3, L_0 = \{e, (12)\}$ e $L_1 = \{e, (23)\}$. Mas temos duas situações em que isso ocorre. Quando L_0 e L_1 são subgrupos normais de L_2 temos que $L_2 = L_0 \times L_1$. Quando apenas L_0 é subgrupo normal de L_2 temos o produto semi-direto $L_2 = L_0 : L_1$.

O produto semi-direto é uma ferramenta muito importante na construção de grupos através dos grupos de automorfismos.

2.6 Grupo Linear Geral

Seja V um espaço vetorial de dimensão n sobre $\mathbb{F}_q$. O **grupo linear geral** $GL(V)$ é o grupo de todos os automorfismos de V. Sem perda de generalidade, nós podemos tomar V como o espaço vetorial $\mathbb{F}_q^n$ e identificar $GL(V)$ com o grupo $GL_n(q)$ de matrizes n x n invertíveis sobre $\mathbb{F}_q$.

Desde que $det(A.B) = det(A).det(B)$ temos que a aplicação determinante é um homomorfismo entre os grupos multiplicativos $GL_n(q)$ e $\mathbb{F}_q^*$. O núcleo desta aplicação é chamado de grupo linear especial e consiste de todas as matrizes $n \times n$ sobre $\mathbb{F}_q$ de determinante 1, denotamos este grupo por $SL_n(q)$. $SL_n(q)$ é subgrupo normal de $GL_n(q)$.

O centro Z desses grupos consiste de todas as matrizes λI_n, para algum $\lambda \in \mathbb{F}_q^*$, onde I_n é a matriz identidade $n \times n$. Assim, temos Z um subgrupo normal de $GL_n(q)$ e $SL_n(q)$ cuja ordem é $q-1$. O grupo linear projetivo $PGL_n(q)$ e o grupo linear projetivo especial $PSL_n(q)$ são os grupos quocientes de $GL_n(q)$ e $SL_n(q)$ pelos seus centros. $PSL_n(q)$, muitas vezes abreviado a $L_n(q)$, é grupo simples sempre que $n \geq 2$ exceto quando $n = 2$ e $q = 2$ ou $q = 3$. Para esses casos pequenos temos $PSL_2(2) \cong S_3$ e $PSL_2(3) \cong A_4$.

2.6.1 Ordem dos Grupos Lineares

Podemos calcular a ordem de $GL_n(q)$ através da contagem das colunas possíveis para uma matriz nesse grupo. A primeira coluna pode ser qualquer vetor exceto o vetor nulo, a segunda coluna pode ser qualquer vetor exceto um múltiplo do primeiro (pois do contrário o determinante seria zero) e, analogamente, a k-ésima coluna pode ser qualquer vetor que não seja combinação linear das $(k-1)$-ésimas colunas anteriores. Assim, temos $(q^n - q^{k-1})$ possibilidades para a k-ésima coluna da matriz, e então a ordem de $GL_n(q)$ é

$$|GL_n(q)| = (q^n - 1)(q^n - q)(q^n - q^2)...(q^n - q^{n-1}).$$

A ordem de $SL_n(q)$ e $PGL_n(q)$ são iguais e dadas por $\frac{|GL_n(q)|}{|Z|}$. De fato, $|SL_n(q)| = \frac{|GL_n(q)|}{|F_q^*|} = \frac{|GL_n(q)|}{q-1}$ e $|PGL_n(q)| = \frac{|GL_n(q)|}{|Z|} = \frac{|GL_n(q)|}{q-1}$.

Para calcularmos a ordem de $PSL_n(q)$ precisamos determinar o número de matrizes kI_n com determinante 1. Como $det(kI_n) = k^n$ precisamos solucionar a equação $x^n = 1$ em $\mathbb{F}_q$. Donde temos k o máximo divisor comum entre n e $q-1$ e a ordem de $PSL_n(q)$ é

$$|PSL_n(q)| = \frac{1}{mdc(n, q-1)}(q^n - 1)(q^n - q)(q^n - q^2)...(q^n - q^{n-1}).$$

2.6.2
$PSL_2(q)$ e a linha projetiva

A linha projetiva $PL(q)$ consiste dos $q+1$ valores de $\mathbb{F}_q \cup \{\infty\}$. Usaremos os seguintes nomes para os subconjuntos de $PL(q)$:

$$\Omega = PL(q), \quad \Omega' = \mathbb{F}_q = \Omega \backslash \{\infty\}, \quad Q = \{x^2 : x \in \mathbb{F}_q\},$$

$$N = \Omega \backslash Q, \quad Q' = Q \backslash \{0\}, \quad N' = N \backslash \{\infty\}.$$

Como existe isomorfismo entre $PSL_2(q)$ e o grupo das transformações de Möbius, segue que $PSL_2(q)$ torna-se o grupo das transformações $z \mapsto \frac{az+b}{cz+d}$, com $ad-bc \in Q$, agindo na linha projetiva $PL(q)$. O grupo $PSL_2(q)$ é gerado por três operações:

$$\alpha : x \longrightarrow x+1, \quad \beta : x \longrightarrow kx, \quad \gamma : x \longrightarrow -x^{-1}, \text{ onde}$$

$k \in Q'$. O conjunto de geradores e relações para o grupo $PSL_2(q)$ varia ligeiramente de acordo com a estrutura de q, quando q é côngruo a 3 módulo 4 temos:

$$PSL_2(q) = \langle \alpha, \beta, \gamma : \alpha^q = \beta^{\frac{1}{2}(q-1)} = \gamma^2 = \alpha^\beta \cdot \alpha^{-k} = (\beta\gamma)^2 = (\alpha\gamma)^3 = 1 \rangle,$$

onde α^β denota $\beta^{-1}\alpha\beta$.

2.7
Transformações lineares e semi-lineares

2.7.1
Transformações lineares

Sejam V e W dois espaços vetoriais sobre um corpo F. Uma aplicação $A : V \longrightarrow W$, que associa a cada $v \in V$ um vetor $A(v) \in W$, é dita uma **transformação linear** quando para quaisquer dois vetores x e y em V e $\alpha \in F$ temos que:

$$\begin{aligned} A(x+y) &= A(x) + A(y) \\ A(\alpha x) &= \alpha A(x) \end{aligned}$$

2.7.2
Transformações lineares monomiais

Considere F um corpo e a base padrão de F^n, ou seja, o conjunto $e_1 := (1, 0, ..., 0)$, ..., $e_n := (0, 0, ..., 1)$. Uma **transformação linear monomial** é uma aplicação F-linear $F^n \longrightarrow F^n$ tal que $e_i \longmapsto c_i e_{\pi(i)}$, para todo i, onde $c_i \in F^*$ e π é alguma permutação.

Seja M matriz com entradas em um corpo F. Se toda linha e toda coluna tem exatamente um elemento não nulo de F, então M é chamada uma **matriz monomial**. Em outras palavras, uma matriz monomial é uma matriz de permutação onde a entrada não nula é qualquer elemento não nulo do corpo F.

2.7.3
Tansformações semi-lineares

Sejam K e L corpos tais que $K \subseteq L$ é uma extensão de grau 2. Considere $\varphi : L \longrightarrow L$ o único automorfismo da extensão $K \subseteq L$ (φ fixa cada elemento de K). Seja $\alpha \in L \backslash K$; assim $L = K[\alpha]$.

Exemplo 1. $K = \mathbb{R},\ L = \mathbb{C},\ \varphi(z) = \overline{z},\ \alpha = i.$

Exemplo 2. $K = \mathbb{Z}/(2),\ L = \mathbb{F}_4,\ \varphi(z) = z^2,\ \alpha = w.$

Exemplo 3. $K = \mathbb{Q},\ L = \mathbb{Q}[\sqrt{2}],\ \varphi(a + b\sqrt{2}) = a - b\sqrt{2},\ \alpha = \sqrt{2}.$

Seja V um $L-$espaço vetorial de dimensão n. Consequentemente V é um $K-$espaço vetorial de dimensão $2n$. Seja $v_1, ..., v_n$ uma $L-$base de V. Então $v_1, \alpha v_1 ..., v_n, \alpha v_n$ é uma $K-$ base de V.

Exemplo 4. Considere o espaço vetorial $\mathbb{C}^2$ com base complexa $\{e_1, e_2\}$. Assim, temos $\{e_1, ie_1, e_2, ie_2\}$ base real para $\mathbb{C}^2$. A transformação $T : \mathbb{C}^2 \longrightarrow \mathbb{C}^2$ é descrita por uma matriz complexa 2×2

$$\begin{pmatrix} a_{11} + i\ b_{11} & a_{12} + i\ b_{12} \\ a_{21} + i\ b_{21} & a_{22} + i\ b_{22} \end{pmatrix}.$$

Assim, a matriz da transformação $\mathbb{R}-$linear $T : V \longrightarrow V$ é dada pela matriz real 4×4

$$\begin{pmatrix} a_{11} & -b_{11} & a_{12} & -b_{12} \\ b_{11} & a_{11} & b_{12} & a_{12} \\ a_{21} & -b_{21} & a_{22} & -b_{22} \\ b_{21} & a_{21} & b_{22} & a_{22} \end{pmatrix}.$$

Considere $GL(V, L)$ o grupo de todos os automorfismos T de V tais que T é $L-$linear inversível. Isso significa que, $GL(V, L) = \{T : V \longrightarrow V, \text{onde } T \text{ é } L - \text{linear inversível}\}$ de modo que para cada $T \in GL(V, L)$ e para quaisquer $v, v_1, v_2 \in V, z \in L$ valem as seguintes relações:

$$T(v_1 + v_2) = T(v_1) + T(v_2)$$
$$T(zv) = z\ T(v).$$

Da mesma forma, considere $GL(V, K) = \{T : V \longrightarrow V, \text{onde } T \text{ é } K - \text{linear inversível}\}$

Diremos que a transformação $T : V \longrightarrow V$ é $(K \subseteq L)-$**anti-linear** se para quaisquer $v_1, v_2 \in V$ e $z \in L$ tem -se

$$\begin{aligned} T(v_1 + v_2) &= T(v_1) + T(v_2) \\ T(zv) &= \varphi(z)T(v). \end{aligned}$$

Por simplicidade, diremos que a transformação é $(L)-$anti-linear ao invés de $(K \subseteq L)-$anti-linear.

Observação 2.7.1. Sejam T_1, T_2 e T_3 automorfismos de V tais que T_1 seja $L-$linear, T_2 e T_3 sejam $L-$anti-lineares então temos $T_1 \circ T_2$, $T_2 \circ T_1$ automorfismos de V $L-$anti-lineares e $T_2 \circ T_3$, $T_3 \circ T_2$ automorfismos de V $L-$lineares. De fato, $(T_1 \circ T_2)(zv) = T_1(T_2(zv)) = T_1(\overline{z}\ T_2(v)) = \overline{z}\ T_1(T_2(v))$, e $(T_2 \circ T_3)(zv) = T_2(T_3(zv)) = T_2(\overline{z}\ T_3(v)) = z\ (T_2 \circ T_3)(v)$ e analogamente para $T_2 \circ T_1$ e $T_3 \circ T_2$.

Dizemos que uma transformação $T : V \longrightarrow V$ é $L-$**semi-linear** se T é $L-$linear ou $L-$anti-linear.

Observação 2.7.2. Chamando de H o grupo dos automorfismos T de V tal que T é $L-$semi-linear temos que $GL(V, L) < H < GL(V, K)$, com índice de $GL(V, L)$ em H igual a 2. Logo,

$$GL(V, L) \lhd H < GL(V, K).$$

Vejamos alguns exemplos:

Exemplo 5. Considere o espaço vetorial $V = \mathbb{C}^2$. Sendo $\{(1, 0), (0, 1)\}$ uma $\mathbb{C}-$base para V, temos $\{(1, 0), i(1, 0), (0, 1), i(0, 1)\}$ uma $\mathbb{R}-$base de V.

Seja $T : V \longrightarrow V$ uma transformação $\mathbb{R}-$linear dada pela matriz $A \in \mathbb{R}^{4\times4}$ abaixo

$$A = \begin{pmatrix} c_{11} & c_{12} & c_{13} & c_{14} \\ c_{21} & c_{22} & c_{23} & c_{24} \\ c_{31} & c_{32} & c_{33} & c_{34} \\ c_{41} & c_{42} & c_{43} & c_{44} \end{pmatrix}.$$

Por definição, temos que T é $\mathbb{C}-$linear quando $T(iv) = i\ T(v)$ e T é $\mathbb{C}-$anti-linear sempre que $T(iv) = -i\ T(v)$, para todo $v \in \mathbb{C}$. Portanto, considere J a matriz abaixo que representa multiplicar por i os vetores de V:

$$J = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Assim, segue que T é $\mathbb{C}-$linear se e só se $AJ = JA$ e T é $\mathbb{C}-$anti-linear se e só se $AJ = -JA$. Fazendo as contas vem que a transformação T é $\mathbb{C}-$linear quando a matriz que a representa é da forma

$$A = \begin{pmatrix} a_{11} & b_{11} & a_{12} & b_{12} \\ b_{11} & -a_{11} & b_{12} & -a_{12} \\ a_{21} & b_{21} & a_{22} & b_{22} \\ b_{21} & -a_{21} & b_{22} & -a_{22} \end{pmatrix},$$

e $\mathbb{C}-$anti-linear quando for uma matriz do tipo

$$A = \begin{pmatrix} a_{11} & b_{11} & a_{12} & b_{12} \\ b_{11} & -a_{11} & b_{12} & -a_{12} \\ a_{21} & b_{21} & a_{22} & b_{22} \\ b_{21} & -a_{21} & b_{22} & -a_{22} \end{pmatrix}.$$

Exemplo 6. Considere o espaço vetorial $V = \mathbb{F}_4^2$. Temos $\{(1,0),(0,1)\}$ uma $\mathbb{F}_4-$base para V e $\{(1,0), w(1,0), (0,1), w(0,1)\}$ uma $\mathbb{R}-$base de V.

Considere uma transformação $T : V \longrightarrow V$, $\mathbb{F}_2-$linear dada pela matriz $A \in \mathbb{F}_2^{4\times 4}$ a seguir

$$A = \begin{pmatrix} c_{11} & c_{12} & c_{13} & c_{14} \\ c_{21} & c_{22} & c_{23} & c_{24} \\ c_{31} & c_{32} & c_{33} & c_{34} \\ c_{41} & c_{42} & c_{43} & c_{44} \end{pmatrix}.$$

Temos que T é $\mathbb{F}_4-$linear quando $T(wv) = w\ T(v)$ e T é $\mathbb{C}-$anti-linear sempre que $T(wv) = \overline{w}\ T(v)$, para todo $v \in \mathbb{C}$. Portanto, considere W a matriz abaixo que representa multiplicar por w os vetores de V:

$$W = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Consequentemente, T é $\mathbb{F}_4-$linear se e só se $AW = WA$ e T é $\mathbb{F}_4-$anti-linear se e só se $AW = W^2A$. Donde vem que a transformação T é $\mathbb{F}_4-$linear quando a matriz que a representa é da forma

$$A = \begin{pmatrix} a_{11} & b_{11} & a_{12} & b_{12} \\ b_{11} & a_{11}+b_{11} & b_{12} & a_{12}+b_{12} \\ a_{21} & b_{21} & a_{22} & b_{22} \\ b_{21} & a_{21}+b_{21} & b_{22} & a_{22}+b_{22} \end{pmatrix},$$

e $\mathbb{F}_4-$anti-linear quando for uma matriz do tipo

$$A = \begin{pmatrix} a_{11} & a_{11}+b_{11} & a_{12} & a_{12}+b_{12} \\ b_{11} & a_{11} & b_{12} & a_{12} \\ a_{21} & a_{21}+b_{21} & a_{22} & a_{22}+b_{22} \\ b_{21} & a_{21} & b_{22} & a_{22} \end{pmatrix}.$$

2.8 Formas bilineares

Sejam E e F espaços vetoriais sobre um corpo K. Uma **forma bilinear** é uma aplicação $B : E \times F \longrightarrow K$ satisfazendo:

1. $B(u+u', v) = B(u, v) + B(u', v)$
2. $B(u, v+v') = B(u, v) + B(u, v')$
3. $B(\lambda u, v) = B(u, \lambda v) = \lambda B(u, v)$,

para quaisquer $u, u' \in E$, $v, v' \in F$ e $\lambda \in \mathbb{R}$. Uma forma bilinear **simétrica** é tal que $B(u, v) = B(v, u)$, para todo $u \in E$ e $v \in F$.

Considere a forma bilinear simétrica

$$\begin{array}{rcl} B : K^n \times K^n & \longrightarrow & K \\ (u, v) & \longmapsto & \langle u, v \rangle. \end{array}$$

Dizemos que B é **não degenerada** se para todo $v \in K^n$, $v \neq 0$, existe $w \in K^n$ tal que $B(v, w) \neq 0$.

Um subespaço vetorial m-dimensional V de K^n é dito **totalmente singular** se e só se $B(v, w) = 0$ para quaisquer $v, w \in V$.

Chama-se o **dual** de K^n, denotado por $(K^n)^*$, o espaço vetorial dos funcionais K-lineares $w : K^n \longrightarrow K$. Note que $V^\perp = \{w : K^n \longrightarrow K; w|_V = 0\} \subseteq (K^n)^*,\ dimV^\perp = n - m$. De fato, seja $\{v_1, ..., v_m, v_{m+1}, ..., v_n\}$ uma base de k^n, onde $\{v_1, ..., v_m\}$ é uma base de V. Uma base de $V^\perp$ é dada $\{v_{m+1}, ..., v_n\}$, onde

$$w_i(v_j) = \begin{cases} 1 & se \quad i = j \\ 0 & se \quad i \neq j. \end{cases}$$

Observe que $B : K^n \times K^n \longrightarrow K$ define uma transformação linear

$$\begin{array}{rccccc} \tilde{B}: & K^n & \longrightarrow & (K^n)^* & & \\ & v & \longmapsto & K^n & \longrightarrow & K \\ & & & w & \longmapsto & B(v,w). \end{array}$$

Considere $\tilde{B}(V) = \{B(v, \cdot) : K^n \longrightarrow K\}$, segue que $dim\tilde{B}(V) = m$.

Proposição 2.8.1. *Se $V \subseteq K^n$ é totalmente singular então $dimV \leq n/2$.*

Demonstração. Seja $m = dimV = dim\tilde{B}(V)$. Como $V \subseteq K^n$ é totalmente singular temos que $\tilde{B}(V) \subseteq V^\perp$. Logo, $m = \tilde{B}(V) \leq dim(V^\perp) = n - m$ e portanto $m \leq n/2$. □

2.9 Códigos

Sejam $\mathbb{F}_q$ um corpo, onde q é primo ou alguma potência de primo, e $n \geq 0$, um inteiro. Um **código** $\mathcal{C}$ é um subconjunto de $\mathbb{F}_q^n$. Um código linear é um subespaço vetorial de $\mathbb{F}_q^n$ de dimensão d. O inteiro n é dito o **comprimento** do código. Usaremos, a palavra código para nos referimos a códigos lineares.

O **peso**, ou **peso de Hamming**, de um vetor $v \in \mathbb{F}_q^n$ é o seu número de coordenadas não nulas, e denotamos por $wt(v)$. A distância entre dois vetores x e y é $wt(x - y)$, isto é, o número de coordenadas onde eles diferem.

$$d_H(x, y) = wt(x - y) = |\{i \mid x_i \neq y_i\}|$$

O **peso mínimo** w de um código é

$$w = min\{d_H(x, y);\ x, y \in \mathcal{C}, x \neq y\}$$

Dizemos que um código $\mathcal{C}$ é $[n, d, w]$-código se este tem comprimento n, dimensão d e peso mínimo w. Os inteiros n, d, w são ditos os parâmetros do código. Usaremos os termos binário para códigos definidos sobre $\mathbb{F}_2 = \{0, 1\}$ e ternário sobre $\mathbb{F}_3 = \{0, 1, 2\}$.

Muitas vezes, chamaremos os vetores de um código $\mathcal{C}$ de palavras ou **codewords**. Um código de comprimento n, contendo M codewords e com

peso mínimo w é dito um (n, M, w) código. Fixado $c \in \mathcal{C}$ denotaremos por $A_i(c)$ o número de codewords com distância de Hamming a c igual a i. Os números $\{A_i(c)\}$ são chamados a **distribuição de peso** de $\mathcal{C}$ com respeito a c. Claramente $A_0(c) = 1$, $A_i(c) \geq 0$ e $\sum_i A_i(c) = M$. Para códigos lineares, $A_i(c)$ independente de c e portanto denotaremos $A_i(c)$ simplesmente por A_i.

O **peso enumerador (de Hamming)** de um código $\mathcal{C}$ é

$$W_{\mathcal{C}}(x, y) \;=\; \sum_{u \in \mathcal{C}} x^{n-wt(u)}\; y^{wt(u)} \;=\; \sum_{i=0}^{n} A_i\; x^{n-i}\; y^i;$$

que é um polinômio homogêneo com grau igual ao comprimento do código.

O peso enumerador de Hamming classifica codewords de acordo com o número de coordenadas não nulas. Informações mais detalhadas são fornecidas pelo **peso enumerador completo** (complete weight enumerator - c.w.e.), que nos diz exatamente a composição dos codewords de $\mathcal{C}$. Por exemplo, o peso enumerador completo de um código ternário é

$$\text{c.w.e.}_{\mathcal{C}}(x, y, z) \;=\; \sum_{u \in \mathcal{C}} x^{n_0(u)}\; y^{n_1(u)}\; z^{n_{-1}(u)},$$

onde $n_i(u)$ é o número de vezes que $i \in \mathbb{F}_3$ ocorre em u.

Agora daremos alguns exemplos de códigos que usaremos no decorrer desse trabalho, aqui faremos apenas uma apresentação breve. Mais adiante, estudaremos estes códigos com um pouco mais de detalhes.

O **Tetracode** $\mathcal{C}_4$ é um código ternário de parâmetros $[4, 2, 3]$, gerado pelos vetores

$$(1, 1, 1, 0) \qquad \text{e} \qquad (0, 1, -1, 1),$$

com peso enumerador

$$f_4 = x^4 + 8xy^3$$

e peso enumerador completo,

$$x\{x^3 + (y + z)^3\}.$$

O **Hexacode** H_6 é um $[6, 3, 4]$-código sobre $\mathbb{F}_4$, gerado pelos vetores

$$(0, 0, 1, 1, 1, 1), \qquad (0, 1, 0, 1, w, \overline{w}) \qquad \text{e} \qquad (1, 0, 0, 1, \overline{w}, w),$$

e tem o seguinte peso enumerador de Hamming:

$$f_6 = x^6 + 45x^2y^4 + 18y^6.$$

Como usual, consideramos $\mathbb{F}_4 = \{0, 1, w, \overline{w}\}$, com as seguintes relações:

$$w^3 = 1,\ 1 + w = \overline{w},\ 1 + \overline{w} = w,\ w + \overline{w} = w\overline{w} = 1,\ w^2 = \overline{w},\ \overline{w}^2 = w.$$

O **Código binário de Golay**, $\mathcal{C}_{24}$ é um código com parâmetros $[24, 12, 8]$ gerado pelos vetores

(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1),
(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1),
(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1),
(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1),
(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1),
(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1),
(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1),
(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1),
(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1),
(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1),
(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1),
(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0).

O código $\mathcal{C}_{24}$ tem a seguinte distribuição de peso

$$0^1\ 8^{759}\ 12^{2576}\ 16^{759}\ 24^1,$$

ou equivalentemente, tem peso enumerador

$$x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24}.$$

Muitas vezes chamaremos esse código simplesmente de **Código de Golay**.

Removendo uma coordenada fixa de todos os 2^{12} codewords do Código de Golay, obtemos o **Código binário de Golay (não estendido)**, $\mathcal{C}_{23}$, que é um código com parâmetros $[23, 12, 7]$ e tem a seguinte distribuição de peso

$$0^1\ 7^{253}\ 8^{506}\ 11^{1288}\ 12^{1288}\ 15^{506}\ 16^{253}\ 23^1.$$

O **Código ternário de Golay** $\mathcal{C}_{12}$ é um código com parâmetros [12,6,6] gerado por

(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1),
(0, 1, 0, 0, 0, 0, -1, 0, 1, -1, -1, 1),
(0, 0, 1, 0, 0, 0, -1, 1, 0, 1, -1, -1),
(0, 0, 0, 1, 0, 0, -1, -1, 1, 0, 1, -1),
(0, 0, 0, 0, 1, 0, -1, -1, -1, 1, 0, 1),
(0, 0, 0, 0, 0, 1, -1, 1, -1, -1, 1, 0).

O código $\mathcal{C}_{12}$ tem peso enumerador

$$x^{12} + 264x^6y^6 + 440x^3y^9 + 24y^{12}$$

e peso enumerador completo,

$$f_{12} = x^{12} + y^{12} + z^{12} + 22(x^6y^6 + y^6z^6 + z^6x^6) + 220(x^6y^3z^3 + x^3y^6z^3 + x^3y^3z^6).$$

Como antes, removendo uma coordenada fixa de todos os 3^6 vetores de $\mathcal{C}_{12}$, obtemos o **Código ternário de Golay (não estendido)** $\mathcal{C}_{11}$, que é um código com parâmetros $[11, 6, 5]$.

2.10 Sistema de Steiner

Considere $\Omega = \{1, 2, ..., c\}$. A família de subconjuntos de Ω é denotada por $P\Omega$. Defina a soma $A + B$ de dois subconjuntos A e B de Ω como sendo a **diferença simétrica** (ou **soma Booleana**) $A + B := (A \setminus B) \cup (B \setminus A)$. Cada subconjunto A de Ω pode ser representado por um **vetor característico** $(v_1, v_2, ..., v_c)$, onde $v_i = 1$ se $i \in A$ e $v_i = 0$ se $i \notin A$. Assim temos $P\Omega$ um espaço vetorial sobre $\mathbb{F}_2$.

Um **sistema de Steiner**, $S(a, b, c)$, é uma família de subconjuntos de um conjunto Ω que satisfaz as seguintes propriedades:

1. Ω tem c elementos chamados pontos;
2. se $B \in S(a, b, c)$ então B é um b-conjunto, isto é, B tem b elementos;
3. para qualquer conjunto A de $P\Omega$ com a elementos existe um único $B \in S(a, b, c)$ tal que $A \subseteq B$.

Chamaremos de **blocos** os elementos B de $S(a, b, c)$. Cada bloco $B \subseteq \Omega$ pode ser representado por um vetor característico de peso b. Assim os blocos de um sistema de Steiner $S(a, b, c)$ geram um código binário de comprimento c.

Por exemplo, o sistema de Steiner $S(2, 3, 7)$ é uma família de subconjuntos de 7 pontos tal que cada bloco contém 3 pontos e quaisquer 2 pontos determinam um único bloco. O sistema de Steiner $S(2, 3, 7)$ é único a menos de isomorfismo e o seu grupo de automorfismos é $PSL_2(7)$ de ordem 168.

Um sistema de Steiner não precisa ter grupo de automorfismos não trivial. De fato, é raro que isso aconteça. Por exemplo, existem 11084874829 sistemas de Steiner $S(2, 3, 19)$ não isomorfos e apenas 172248 deles tem grupo de simetria não trivial (ver (2).)

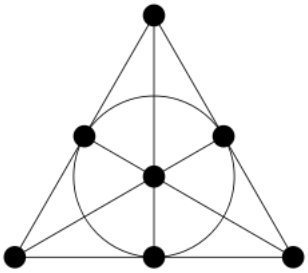

Figura 2.1: O sistema de Steiner $S(2, 3, 7)$.