Resumo de Grupos e Representações

Aula 1 - Série de composição

Definição 1.1. Seja G um grupo. Considere a cadeia $G_0 = G > G_1 > G_2 > \cdots > G_k = 1$ de subgrupos de G. Dizemos que uma cadeia assim tem **comprimento k**. Se $G_i \lhd G$, $\forall\, i$, então a cadeia é dita **normal**. Se $G_i \lhd G_{i-1}$, $\forall\, i$, então a cadeia é dita **subnormal**.

Definição 1.2. Seja G um grupo. Dizemos que a cadeia $H_0 = G > H_1 > \cdots > H_m = 1$ é um **refinamento** da cadeia $G_0 = G > G_1 > \cdots > G_k$, se $\{G_0, \ldots, G_k\} \subseteq \{H_0, \ldots, H_m\}$. Se a inclusão for própria, então dizemos **refinamento próprio**.

Definição 1.3. Um grupo G é dito **simples**, se $G \neq 1$ e só possuir G e 1 como subgrupos normais.

Definição 1.4. Uma cadeia subnormal é dita **série de composição**, se não tem refinamento próprio.

Lema 1.1. Uma cadeia subnormal é série de composição se, e somente se, todos os quocientes são simples.

Definição 1.5. Seja G um grupo. Assuma $G_0 = G > G_1 > \cdots > G_k = 1$ e $H_0 = G > H_1 > \cdots > H_m = 1$ são séries subnormais. Dizemos que elas são **séries equivalentes**, se $k = m$ e se existe $\sigma \in S_k$ tal que $G_{i-1}/G_i \cong H_{\sigma(i)-1}/H_{\sigma(i)}$.

Aula 2 - Teorema de Jordan-Hölder

Lema 2.1. Sejam $A, B \lhd G$, com $A \neq B$ e $A, B \neq G$ tais que G/A e G/B são simples. Então $G/A \cong B/A \cap B$ e $G/B \cong A/A \cap B$.

Teorema 2.1 (Jordan-Hölder)**.** Se um grupo G possui duas séries de composição, então elas são equivalentes.

Teorema 2.2. Os grupos simples finitos são conhecidos.

Definição 2.1. Sejam G grupo e $x, y \in G$. Definimos **o comutador de x e y** por $[x, y] = x^{-1}y^{-1}xy$. Definimos também o **subgrupo comutador de G** como sendo $G' = \langle [x, y] \mid x, y \in G \rangle$.

Definição 2.2. Sejam G um grupos e $X \leq G$. Dizemos que X é **subgrupo característico**, se $\alpha(X) = \{\alpha(x) \mid x \in X\} = X$, $\forall\, \alpha \in \mathrm{Aut}(G)$ e denotamos por $X \lhd_{char} G$.

Lema 2.2. Seja G um grupo. Então G' é subgrupo característico.

Lema 2.3. Assuma que $X \leq Y \leq G$.

1. Se $X \lhd_{char} Y$ e $Y \lhd_{char} G$, então $X \lhd_{char} G$.
2. Se $X \lhd_{char} Y$ e $Y \lhd G$, então $X \lhd G$.

Lema 2.4.

a) $G' \lhd G$.

b) G/G' é abeliano.

c) $H \lhd G$ tal que G/H é abeliano, se, e somente se, $G' \subset H$.

Definição 2.3. Denote $G^{(0)} = G$, $G^{(1)} = G'$, $G^{(2)} = G''$ e assim por diante. Então a série $G_0 = G^{(0)} = G > G^{(1)} > G^{(2)} > \ldots$ é dita **série derivada de G**

Lema 2.5. Seja $G = G_0 > G_1 > \cdots > G_k > \ldots$ uma cadeia subnormal tal que G_i/G_{i+1} é abeliano, $\forall\, i \geq 0$. Então $G^{(i)} \leq G_i$, $\forall\, i \geq 1$.

Aula 3 - Grupos abelianos elementares e minimais normais

Lema 3.1. Seja G uma grupo. As seguintes afirmações são equivalentes.

1. Existe uma cadeia normal $G_0 = G > G_1 > \cdots > G_k = 1$.
2. Existe uma cadeia subnormal $G_0 = G > G_1 > \cdots > G_m = 1$, com G_i/G_{i+1} abeliano, para todo i.
3. Existe algum $r \geq 1$ tal que $G^{(r)} = 1$.

Definição 3.1. Um grupo G é dito **solúvel**, se existe $k \geq 0$ tal que $G^{(k)} = 1$.

Teorema 3.1. Se $|G| \leq 100$, então G é solúvel ou $G \cong A_5$.

Teorema 3.2 (Ore)**.** Se G é um grupo solúvel simples não abeliano, então $G' = G = \{[x, y] \mid x, y \in G\}$.

Exemplo 3.1. A série derivada de S_4 é

$$S_4 > A_4 > X > 1$$

onde $X = \langle (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) \rangle$.

Definição 3.2. Um grupo abeliano G é dito **abeliano elementar**, se existe um primo p tal que $x^p = 1$, $\forall\, x \in G$.

Proposição 3.1.

- Seja G um grupo finito. Então G é abeliano elementar se, e somente se, $G \cong C_p \times \cdots \times C_p$, para algum p primo.
- Se $G \cong C_p \times \cdots \times C_p$, então G é um espaço vetorial sobre $\mathbb{F}_p$.

Definição 3.3. Um subgrupo normal $1 \neq N \lhd G$ é **minimal normal**, se $\forall\, M \lhd G$ tal que $M \lneqq N$, então $M = 1$.

Lema 3.2. Sejam G e K grupos.

1. Se $\varphi : G \to K$ é homomorfismo, então $\varphi(G^{(i)}) = \varphi(G)^{(i)}$.
2. Se $N \lhd G$, então $\left(G/N\right)^{(i)} = G^{(i)}N/N$.
3. Se G é solúvel, $H \leq G$ e $N \lhd G$, então H é solúvel e G/N é solúvel.
4. Se $N \lhd G$ e G/N são solúveis, então G é solúvel.
5. Se $|G| = p^n$, com p primo, então G é solúvel.
6. Suponha que G possua série de composição. G é solúvel se, e somente se, os fatores de composição de G são cíclicos de ordem p.
7. Se G é solúvel finito e $N \lhd G$ é minimal normal de G, então N é abeliano elementar.

Aula 4 - Subgrupos de Hall

Definição 4.1. Sejam $\pi \subseteq \mathbb{P} = \{n \in \mathbb{N}_{>1} \mid n \text{ é primo}\}$ e $m \in \mathbb{N}$. Dizemos que m é um **π-número**, se π contém todos os primos que dividem m. Dizemos que m é um **π'-número**, se m for um $\mathbb{P} \setminus \pi$-número, isto é, se π não contém nenhum primo que divide m.

Exemplo 4.1. 60 é um $\{2,3,5,11\}$-número e é um $\{11,13,19\}'$-número.

Definição 4.2. Sejam $\pi \subseteq \mathbb{P} = \{n \in \mathbb{N}_{>1} \mid n \text{ é primo}\}$ e G um grupo finito. Dizemos que G é um **π-grupo**, se π contém todos os primos que dividem $|G|$. Dizemos que G é um **π'-grupo**, se G for um $\mathbb{P} \setminus \pi$-grupo, isto é, se π não contém nenhum primo que divide $|G|$.

Exemplo 4.2.

1. Se $\pi = \{p\}$, então G é π-grupo, se, e somente se, G é um p-grupo finito.
2. A_5 é um $\{2, 3, 5, 11\}$-grupo e é um $\{11, 13, 19\}'$-grupo.

Definição 4.3. Seja G um grupo finito e p um primo. Um subgrupo $P \leq G$ é um **p-subgrupo de Sylow**, se P é um π-grupo e $[G : P]$ é um π'-número, com $\pi = \{p\}$.

Teorema 4.1 (Teorema de Sylow)**.** Seja G um grupo finito.

1. Existe p-subgrupo de Sylow em G, para todo p.
2. Dois tais subgrupos são conjugados.
3. A quantidade desses subgrupos é congruente a 1 módulo p.

Definição 4.4. Sejam G um grupo finito e $\pi \subseteq \mathbb{P}$. Um subgrupo $H \leq G$ é dito **π-subgrupo de Hall**, se H é um π-grupo e $[G : P]$ é um π'-número.

Exemplo 4.3.

1. Seja $G = C_5 \times S_4$.
   (a) Seja $\pi = \{2, 3\}$. Então $S_4 \cong 1 \times S_4$ é um $\{2, 3\}$-subgrupo de Hall de G.
   (b) Seja $\pi = \{2, 5\}$. Se H é um $\{2, 5\}$-subgrupo de Hall de G, então $[G : H]$ é um π'-número, ou seja, $2, 5 \nmid [G : H]$. Como $[G : H] \mid |G| = 2^3 \cdot 3 \cdot 5$, então $[G : H] = 3$, consequentemente, $|H| = 40$.
   (c) Seja $\pi = \{3, 5\}$. Pelo mesmo motivo de antes, se H é um $\{3, 5\}$-subgrupo de Hall de G, então $[G : H] = 8$, logo $|H| = 15$.
2. Seja $G = A_5$. Então G não possui $\{3, 5\}$-subgrupo de Hall, pois se tivesse, sua ele seria um subgrupo cíclico de ordem 15, mas A_5 não possui permutação de ordem 15.

Lema 4.1 (Argumento de Frattini)**.** Sejam G um grupo finito e $N \lhd G$. Seja P um p-subgrupo de Sylow de N. Então $G = N_G(P)N$.

Definição 4.5. Seja G um grupo e $X \leq G$. Um subgrupo Y é dito **complemento de X em G**, se $G = XY$ e $X \cap Y = 1$.

Teorema 4.2 (Teorema de Schur-Zassenhaus (1934))**.** Seja G um grupo finito e seja $N \lhd G$ tal que $\text{mdc}(|G|, [G : N]) = 1$. Então N tem complemento em G. Além disso, se N ou G/N é solúvel, então dois tais complementos são conjugados.

Teorema 4.3 (Teorema de Feit-Thompson (1964))**.** Se G é um grupo de ordem ímpar, então G é solúvel.

Aula 5 - Teorema de Hall – parte 1

Lema 5.1. Seja G um grupo solúvel de ordem ap^n, onde p é primo e $p \nmid a$. Assuma que M é o único subgrupo minimal normal de G e $|M| = p^n$. Então G possui $\{p\}'$-subgrupo de Hall (ou, alternativamente, G possui um subgrupo de ordem a ou, ainda, M possui complemento em G e dois complementos são conjugados).

Teorema 5.1 (Teorema de Hall)**.** Seja G um grupo finito. Os seguintes são equivalentes:

- G é um grupo solúvel.
- Existe um π-subgrupo de Hall em G para todo $\pi \subseteq \mathbb{P}$.

Além disso, se G é solúvel, então os π-subgrupos de Hall são conjugados.

Aula 6 - Teorema de Hall – parte 2; cadeia central

Lema 6.1. Se G é grupo finito e G possui $\{p\}'$-subgrupo de Hall para todo primo p, então G é solúvel.

Teorema 6.1 (Burnside ($\sim$ 1910))**.** Se $|G| = p_1^{\alpha_1} p_2^{\alpha_2}$, com p_1, p_2 primos, então G é solúvel.

Observação 6.1. Existe classificação de grupos finitos simples (CGFS), contudo, esse teorema que foi enunciado por volta de 1980 é extremamente complicado. Pela complexidade de tal teorema, dividiu-se os teoremas acerca de grupos finitos simples naqueles cuja demonstração se usa o CGFS e aqueles que não. Por exemplo, o teorema de Burnside não usa CGFS. Os dois teoremas abaixo usam.

- (Conjectura de Schreier) Se G é finito simples, então $\mathrm{Out}(G) = {}^{\mathrm{Aut}(G)}\!/_{\mathrm{Inn}(G)}$ é solúvel.
- Um grupo finito simples possui um p-subgrupo de Sylow cíclico.

Definição 6.1. Seja G um grupo. Seja $G_1 > G_2 > \cdots > G_k$ uma cadeia normal. Dizemos que essa cadeia é **central**, se ${}^{G_i}\!/_{G_{i+1}} \leq \mathcal{Z}\left({}^{G}\!/_{G_{i+1}}\right)$.

Aula 7 - Cadeia central superior e inferior

Lema 7.1. Seja $K \leq H \leq G$, com $K \trianglelefteq G$. Então $[H, G] \leq K \Leftrightarrow {}^{H}\!/_{K} \leq \mathcal{Z}\left({}^{G}\!/_{K}\right)$.

Definição 7.1. Defina $\zeta_0(G) = 1$ e $\zeta_1(G) = \mathcal{Z}(G)$. Para $i \geq 2$, defina $\zeta_{i+1}(G)$ como sendo, pelo teorema da correspondência, o único subgrupo de $\zeta_i(G)$, tal que ${}^{\zeta_{i+1}(G)}\!/_{\zeta_i(G)} \leq \mathcal{Z}\left({}^{G}\!/_{\zeta_i(G)}\right)$. A cadeia $\zeta_0(G) \leq \zeta_1(G) \leq \cdots \leq \zeta_n(G)$, para algum n, é dita **cadeia central superior**. Dizemos também que $\zeta_i(G)$ é o **i-ésimo centro de G**. Definimos $\zeta(G) = \cup_{i=1}^{n} \zeta_i(G)$ e o denominamos **hipercentro de G**.

Observação 7.1. Temos que $\zeta_i(G), \zeta(G) \leq_{\text{char}} G$, logo $\zeta_i(G), \zeta(G) \trianglelefteq G$.

Definição 7.2. Defina $\gamma_1(G) = G$ e $\gamma_{i+1}(G) = [\gamma_i(G), G]$. A cadeia $\gamma_1(G) \geq \gamma_2(G) \geq \cdots \geq \gamma_n(G)$, para algum n, é dita **cadeia central inferior**.

Observação 7.2. Temos que $\gamma_i(G) \leq_{\text{char}} G$ e ${}^{\gamma_i(G)}\!/_{\gamma_{i+1}(G)} \leq \mathcal{Z}\left({}^{G}\!/_{\gamma_{i+1}(G)}\right)$, para todo $i \geq 1$.

Exemplo 7.1.

1. Seja $G = S_4$, então $\zeta_i(G) = 1$, $\forall\, i \geq 0$, ou seja, a cadeia central superior só possui um termo. A cadeia central inferior é $G \geq A_4$.
2. Seja $G = D_8 = \langle a, b \mid a^8 = b^2 = 1 \text{ e } ab = ba^{-1} \rangle$. Então a cadeia central superior é igual a cadeia central inferior: $1 \leq \langle a^4 \rangle \leq \langle a^2 \rangle \leq G$.

Exercício 7.1.

1. Se G é abeliano finito e p é primo, então $\{g \in G \mid |g| = p^i\}$ é o p-subgrupo de Sylow de G.
2. Se $X, Y \trianglelefteq G$, então $[X, Y] \trianglelefteq G$.
3. Se $X, Y \leq_{\text{char}} G$, então $[X, Y] \leq_{\text{char}} G$.
4. Se $X, Y \trianglelefteq G$, então $[X, Y] \leq X \cap Y$.

Aula 8 - Grupo Nilpotente

Lema 8.1. Seja G um grupo.

1. Seja $G_1 = G > G_2 > \cdots$ uma série central em G. Então $\gamma_i(G) \leq G_i$, para todo i.
2. Seja $1 = H_0 < H_1 < H_2 < \cdots$ uma série central em G. Então $H_i \leq \zeta_i(G)$, para todo i.

Teorema 8.1. Seja G um grupo. As seguintes afirmações são equivalentes.

1. Existe algum k tal que $\zeta_k(G) = G$.

2. Existe algum ℓ tal que $\gamma_\ell(G) = 1$.

3. Existe uma série central $G = G_1 > G_2 > \cdots > G_n = 1$.

Definição 8.1. Um grupo G é **nilpotente** se ele satisfaz uma das condições do teorema 8.1.

Lema 8.2. Sejam $G \neq 1$ um grupo, $H \leq G$ e $N \trianglelefteq G$. Então

1. Se G é nilpotente, então H e G/N são nilpotentes.

2. Se G é nilpotente, então $\mathcal{Z}(G) \neq 1$.

3. G é nilpotente se, e somente se, $G/\mathcal{Z}(G)$ é nilpotente.

4. Se G e H são nilpotentes, então $G \times H$ é nilpotente.

Corolário 8.1. Se G é p-grupo finito, então G é nilpotente.

Corolário 8.2. Se G_i é um p_i-grupo finito, com $i = 1, \ldots, k$, então $G_1 \times \cdots \times G_k$ é nilpotente.

Definição 8.2. Sejam G um grupo e $M \lneq G$. Dizemos que M é um **subgrupo maximal**, se para todo $X \leq G$ tal que $M \lneq X \leq G$, temos que $X = G$.

Exercício 8.1.

1. Assuma que $A, B \leq G$, $A = \langle X \rangle$ e $B = \langle Y \rangle$, onde $X, Y \subseteq G$. Então $[A, B] = \langle [x, y] \mid x \in X, y \in Y \rangle^{AB}$, ou seja, é o menor subgrupo normalizado por AB que contém $[x, y]$.

2. D_n é nilpotente $\Leftrightarrow$ $n = 2^k$, onde D_n é o grupo de simetrias de um n-ágono.

3. Nilpotente $\Rightarrow$ sóluvel.

Aula 9 - Subgrupo de Frattini

Lema 9.1. Seja G um grupo nilpotente.

1. Se $H \lneq G$, então $H \lneq N_G(H) = \{g \in G \mid H^g = H\}$.

2. Se $M \leq_{\max} G$, então $M \trianglelefteq G$ e $[G : M] = p$, onde p é primo.

3. Se $1 \neq N \trianglelefteq G$, então $N \cap \mathcal{Z}(G) \neq 1$.

Teorema 9.1. Um grupo finito é nilpotente se, e somente se, todos os seus subgrupos de Sylow são normais. Neste caso, G é produto direto de seus subgrupos de Sylow.

Observação 9.1. Sejam G um grupo e $H \leq G$.

1. Dizemos que H é **subgrupo não trivial** se $H \neq 1$. Neste caso, pode ser que $H = G$.

2. Dizemos que H é **subgrupo próprio** se $H \neq G$. Neste caso, pode ser que $H = 1$.

Definição 9.1. Seja G um grupo. Definimos o **subgrupo de Frattini** como sendo $\Phi(G) = \cap_{M \leq_{\max} G} M$.

Definição 9.2. Sejam G um grupo e $x \in G$. Se $\forall\, X \subseteq G \ \langle X, x\rangle = G$ implicar que $\langle X\rangle = G$, dizemos que x é **não gerador**.

Lema 9.2. Se G é finito, então $\Phi(G) = \{x \in G \mid x\text{é não gerador}\}$.

Corolário 9.1. Se G é finito, então $\Phi(G)$ é nilpotente.

Teorema 9.2. Se G é p-grupo finito, então $\Phi(G) = G'G^p$, onde $G^p = \{g^p \mid g \in G\}$.

Exercício 9.1.

1. Se G é um grupo finito e P é um subgrupo de Sylow de G, então $N_G(N_G(P)) = N_G(P)$.

2. Se G é um grupo e $N_1, \ldots, N_k$ são subgrupos normais de G tais que $[N_i, N_j] = 1$ e $G = N_1 \ldots N_k$, então $G \cong N_1 \times \cdots \times N_k$.

3. Se $N \trianglelefteq G$ tal que $N \leq \Phi(G)$, então $\Phi({}^{G}\!/_{N}) = {}^{\Phi(G)}\!/_{N}$

Aula 10 - Teorema da base de Burnside e grupo de Heisenberg

Observação 10.1. Seja G um grupo finito abeliano elementar. Então existe p primo tal que $g^p = 1, \forall\, g \in G$. Pelo teorema fundamental dos grupos abelianos, $G = C_p \times \cdots \times C_p$ (d vezes). Assim, G pode ser considerado um espaço vetorial sobre $\mathbb{F}_p$, onde se $\alpha \in \mathbb{F}_p = \{0, \ldots, p-1\}$, então $\alpha g = g + \cdots + g$ (α vezes). Neste caso, $\dim G = d$. Se $H \subseteq G$ e $\rho : G \to G$. Então

- H é subgrupo $\Leftrightarrow$ H é subespaço.

- ρ é automorfismo $\Leftrightarrow$ ρ é linear invertível.

Assim, $\mathrm{Aut}(G) = GL(d, \mathbb{F}_p) = GL(d, p)$. Além disso, o conjunto minimal de geradores é base e se $X \subseteq G$ é um sistema minimal de geradores, então $|X| = \dim G = d$. Note que se o grupo não for abeliano elementar, então o conjunto minimal de geradores pode ter tamanhos diferentes como é o caso de $C_2 \times C_3 = \langle a\rangle \times \langle b\rangle$, pois $\{a, b\}$ e $\{ab\}$ são conjuntos minimais de geradores.

Exemplo 10.1. $G = Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. Então $\Phi(G) = \langle -1 \rangle$ e ${}^{G}\!/_{\Phi(G)} = C_2 \times C_2$. Assim, $\dim {}^{G}\!/_{\Phi(G)} = 2$ e $G = \langle i, j \rangle$.

Teorema 10.1 (Teorema da Base de Burnside)**.** Seja G um p-grupo finito e seja $X \subseteq G$ um sistema minimal de geradores. Então $|X| = \dim {}^{G}\!/_{\Phi(G)} = \log_p \dfrac{|G|}{|\Phi(G)|}$.

Exemplo 10.2. O grupo $G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{F} \right\}$, onde $\mathbb{F}$ é um corpo, é dito **grupo de Heisenberg sobre** $\mathbb{F}$. Temos que $G' = \mathcal{Z}(G) = \left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; b \in \mathbb{F}. \right\}$ Assim, a cadeia central inferior é $G > G' > 1$, logo G é nilpotente. Se $\mathbb{F} = \mathbb{F}_p$ é corpo finito de característica p, ou seja, $q = p^d$, então $|G| = q^3 = p^{3d}$ é p-grupo e mais G é um p-subgrupo de Sylow de $GL(3, q)$. Além disso, $G^p \leq G'$, logo $\Phi(G) = G'$. Assim, $\dfrac{|G|}{|\Phi(G)|} = q^2 = p^{2d}$, logo $\dim_{\mathbb{F}_p} {}^{G}\!/_{\Phi(G)} = 2d$. Se $B = \{\alpha_1, \ldots, \alpha_d\}$ é uma base de $\mathbb{F}_q$ sobre $\mathbb{F}_p$, então $\left\{ \begin{pmatrix} 1 & \alpha_i & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & \alpha_j \\ 0 & 0 & 1 \end{pmatrix} \right\}$ é um conjunto minimal de geradores de G.

Se $Q \leq G(3, q)$ é um p-subgrupo, então, pelo teorema de Sylow, um conjugado $Q^X = X^{-1}QX$ está contido em G. Assim, existe uma base de $\mathbb{F}_q^3$ na qual Q tem forma triangular superior com 1 na diagonal.

Exercício 10.1.

1. Se $X = \{x_1, \ldots, x_d\}$ é um conjunto minimal de geradores de G, então temos que $\{x_1\Phi(G), \ldots, x_d\Phi(G)\}$ é conjunto gerador de ${}^{G}\!/_{\Phi(x)}$.

Aula 11 - Ação de um grupo

Definição 11.1. Seja Ω um conjunto. Definimos $\mathrm{Sym}(\Omega)$ como sendo o conjunto $\{\varphi : \Omega \to \Omega \mid \varphi \text{ é bijeção}\}$. Um subgrupo $G \leq \mathrm{Sym}(\Omega)$ é chamado **grupo de permutação**. Se $\Omega = \{1, \ldots, n\}$, então denotamos $\mathrm{Sym}(\Omega)$ por S_n.

Definição 11.2. Sejam Ω um conjunto e G um grupo. Dizemos que **G age em Ω**, $\Omega \curvearrowleft G$, se existe um função $\varphi : \Omega \times G \to \Omega$, $(\omega, g) \mapsto \omega g$ tal que

i) $\omega 1_G = \omega$, $\forall\, \omega \in \Omega$.

ii) $\omega(gh) = (\omega g)h$, $\forall\, \omega \in \Omega$, $\forall\, g, h \in G$.

Exemplo 11.1.

1. Se $G \leq \mathrm{Sym}(\Omega)$, então G age em Ω: se $\omega \in \Omega$ e $g \in G$, defina a ação como ωg. Note que $g : \Omega \to \Omega$.

2. Sejam V espaço vetorial sobre $\mathbb{F}^n$, com $\mathbb{F}$ corpo, e $G = GL(n, \mathbb{F}) = \{A \in \mathcal{M}_{n\times n}(\mathbb{F}) \mid \det A \neq 0\}$. Então G age em V: se $v \in V$ e $g \in G$ defina a ação como vg, isto é, multiplicação do vetor v com a matriz g.

3. Ainda considerando o exemplo acima, seja $\mathcal{P}(V) = \{\langle v\rangle \mid v \in V \setminus \{0\}\}$, onde $\langle v\rangle = \{\alpha v \mid \alpha \in \mathbb{F}\}$. Tal conjunto é dito **espaço projetivo de** V. Nesse caso $G = GL(n, \mathbb{F})$ age em $\mathcal{P}(V)$: se $\langle v\rangle \in \mathcal{P}(V)$ e $g \in G$, defina a ação como $\langle v\rangle g = \langle vg\rangle$.

4. Todo grupo age nele mesmo:

   (a) segundo a ação definida como sendo a própria operação do grupo.

   (b) segundo a conjugação, isto é, se $\omega, g \in G$, então a ação é $\omega^g = g^{-1}\omega g$.

5. Se G é grupo e $\Omega = \{H \mid H \leq G\}$, então G age em Ω: $(H, g) \mapsto H^g = g^{-1}Hg$.

6. Se G é grupo, $H \leq G$ e $\Omega = \{Hg \mid g \in G\}$, então G age em Ω: $(Hx, g) \mapsto Hxg$.

Observação 11.1. Dado uma ação de G em um conjunto Ω, ωg, podemos definir um homomorfismo $\varphi : G \to \mathrm{Sym}(\Omega)$, fazendo $g \mapsto \omega\varphi_g = \omega g$. Reciprocamente, dado um homomorfismo $\varphi : G \to \mathrm{Sym}(\Omega)$, $g \mapsto \omega\varphi_g$, podemos definir uma ação de G em Ω, fazendo $\omega g = \omega\varphi_g$.

Definição 11.3. Uma ação de G em Ω é **fiel** se o homomorfismo correspondente é injetivo.

Observação 11.2. Se a ação é fiel, G pode ser considerado um grupo de permutações.

Aula 12 - Órbita e estabilizador

Observação 12.1. Sejam G grupo e Ω um conjunto. Considere que G age sobre Ω. Então a relação $\sim$ em Ω, definida como

$$\alpha \sim \beta \Leftrightarrow \exists\, g \in G \;\; \alpha g = \beta$$

define uma relação de equivalência.

Definição 12.1. Seja $\omega \in \Omega$. Definimos a **órbita de ω**, ωG, como sendo a classe de equivalência de ω segundo a relação $\sim$, isto é, $\omega G = \{\omega g \in \Omega \mid \forall\, g \in G\}$. Dizemos que G é **transitivo** em Ω, se Ω é uma órbita. Caso contrário, G é dito **intransitivo**. Definimos o **estabilizador de** ω como sendo $G_\omega = \{g \in G \mid \omega g = \omega\}$.

Lema 12.1. Sejam $\Omega \curvearrowleft G$ e $\alpha, \beta \in \Omega$ tais que existe $g \in G$ tal que $\alpha g = \beta$. Então $G_\beta = (G_\alpha)^g = g^{-1} G_\alpha g$.

Exemplo 12.1. Considere $V = \mathbb{F}^n \curvearrowleft G = GL(n, \mathbb{F})$, pela multiplicação do vetor v com a matriz g, vg. Então V é intransitivo, pois as órbitas são $\{0\}$ e $V \setminus \{0\}$. Seja $v = (1, 0, \ldots, 0)$. Então $G_v = \left\{ \begin{pmatrix} 1 & 0 & \cdots & 0 \\ * & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ * & * & \cdots & * \end{pmatrix} \right\}$ Seja $u = (u_1, u_2, \ldots, u_n)$. Então. pelo lema 12.1 $G_u = g^{-1} G_v g$, com $g = \begin{pmatrix} u \\ * \end{pmatrix}$, uma vez que $vg = u$.

Observação 12.2. Sejam $\Omega \curvearrowleft G$ transitiva e $\alpha \in \Omega$. Então $\ker = \{g \in G \mid \omega g = \omega \ \forall\, \omega \in \Omega\} = \cap_{\omega \in \Omega} G_\omega = \cap_{g \in G} (G_\alpha)^g = \mathrm{Core}_G(G_\alpha)$ (maior subgrupo normal de G contido em G_α).

Definição 12.2. Dizemos que $\boldsymbol{\Omega \curvearrowleft G}$ **é equivalente a** $\boldsymbol{\Delta \curvearrowleft G}$, se existe uma bijeção $\varphi : \Omega \to \Delta$ tal que $(\omega g)\varphi = (\omega \varphi) g$, para todo $g \in G$ e para todo $\omega \in \Omega$.

Teorema 12.1 (Teorema de órbita e estabilizador)**.** Sejam $\Omega \curvearrowleft G$ transitiva e $\alpha \in \Omega$. Defina um mapa $\varphi : \Omega \to [G : G_\alpha]$, $\beta \to \{g \in G \mid \alpha g = \beta\}$. Então φ está bem definida e é uma equivalência entre as ações $\Omega \curvearrowleft G$ e $[G : G_\alpha] \curvearrowleft G$.

Corolário 12.1.

1. Toda ação transitiva de um grupo é equivalente à ação sobre um conjunto de classes laterais a direita.

2. $|\Omega| = |G : G_\alpha|$. Em particular, se G e Ω são finitos, então $|G| = |G_\alpha||\Omega|$. Portanto, $|\Omega| \mid |G|$.

Exemplo 12.2. Seja $G \curvearrowleft G$, segundo a conjugação, isto é, $(x, g) \mapsto g^{-1} x g = x^g$. A órbita de x é uma classe de conjugação x^G, o estabilizador de x é $G_x = C_G(x)$ e $|x^G| = |G : C_G(x)|$.

Aula 13 - Partição primitiva

Exemplo 13.1. Assuma $\Omega \curvearrowleft G$ transitiva. Seja $\alpha \in \Omega$ e $K \leq G$. Então K é transitivo (a ação é transitiva restrita a K) $\Leftrightarrow$ $G_\alpha K = G$.

Definição 13.1. Sejam $\Omega \curvearrowleft G$ transitiva e $\mathcal{P} = \{\Delta_1, \ldots, \Delta_m\}$ uma partição de Ω. Dizemos que $\mathcal{P}$ é **preservada por G**, se $\Delta_i g = \Delta_j$, para todo $g \in G$ e para todo $\Delta_i \in \mathcal{P}$. Neste caso, dizemos que a partição é **G-invariante**. Se as únicas partições G-invariantes são $\{\Omega\}$ e $\{\{\alpha\} \mid \alpha \in \Omega\}$, então dizemos que G é **primitivo**. Caso contrário, G é dito **imprimitivo**.

Exemplo 13.2.

- Sejam $G = D_4$ e $\Omega = \{1, 2, 3, 4\}$. Então D_4 é imprimitivo.
- Sejam $GL(n, \mathbb{F})$, $n \geq 2$ e $\mathbb{F} \neq \mathbb{F}_2$, e $\Omega = \mathbb{F}^n \backslash \{0\}$. Então $GL(n, \mathbb{F})$ é imprimitivos.
- Sejam S_n, A_n e $\Omega = \{1, \ldots, n\}$. Então S_n e A_n são primitivos.
- Sejam $SL(n, \mathbb{F})$, $GL(n, \mathbb{F})$ e $\Omega = \{\langle v \rangle \mid v \in \mathbb{F}^n \setminus \{0\}\}$. Então $SL(n, \mathbb{F})$ e $GL(n, \mathbb{F})$ são primitivos.

Definição 13.2. Seja $\Omega \curvearrowleft G$. Dizemos que G é **2-transitivo em Ω**, se para todo $\alpha, \beta, \gamma, \delta \in \Omega$ tal que $\alpha \neq \beta$ e $\gamma \neq \delta$, existe $g \in G$ tal que $\alpha g = \gamma$ e $\beta g = \delta$.

Exercício 13.1.

1. Seja G um grupo com $|G| \geq 2$. Mostre que G tem pelo menos 3 órbitas em G com ação de conjugação.
2. Sejam $\Omega \curvearrowleft G$ transitiva e $\mathcal{P} = \{\Delta_1, \ldots, \Delta_m\}$ G-invariante. Mostre que
   (a) $|\Delta_i| = |\Delta_j|$.
   (b) $\mathcal{P} \curvearrowleft G$ transitiva.
   (c) Considere G_{Δ_i} (estabilizador de Δ_i em $\mathcal{P}$). Então G_{Δ_i} é transitivo em Δ_i.
   (d) Se G é 2-transitivo em Ω, então G é primitivo em Ω.

Aula 14 - Classes de conjugação de S_n

Teorema 14.1. Sejam $\Omega \curvearrowleft G$ transitiva e $\alpha \in \Omega$. Então G é primitivo $\Leftrightarrow$ G_α é subgrupo maximal em G.

Exemplo 14.1.

- Seja $\Omega = \{1, 2, \ldots, n\} \curvearrowleft G = S_n$. Então $G_n = S_{n-1} \leq_{\max} S_n$.
- Seja $\Omega = \{1, 2, \ldots, n\} \curvearrowleft G = A_n$. Então $G_n = A_{n-1} \leq_{\max} A_n$.
- Sejam $\Omega = \{\langle v \rangle \mid v \in \mathbb{F}^n \setminus \{0\}\} \curvearrowleft G = GL(n, \mathbb{F})$ e $v = \langle (1, 0, \ldots, 0) \rangle$. Então $G_v = \left\{ A = \begin{pmatrix} \alpha & 0 & \cdots & 0 \\ & & * & \end{pmatrix} \;\middle|\; \alpha \in \mathbb{F}^* \text{ e } \det A \neq 0 \right\} \leq_{\max} GL(n, \mathbb{F})$.

Definição 14.1. Seja $\Omega = \{1, \ldots, n\}$, $n \geq 3$. Considere $G = S_n$ e $\Phi_n \in \mathbb{Q}[x_1, \ldots, x_n]$, definido como $\Phi_n = \prod_{i<j}(x_i - x_j)$. Se $g \in S_n$, defina $\Phi_n g = \prod_{i<j}(x_{ig} - x_{jg})$. Então $\Phi_n g = \pm \Phi_n$, logo G age em $\Delta = \{\Phi_n, -\Phi_n\}$. O estabilizador de Φ_n é o **grupo alternado**, A_n.

Exemplo 14.2.

1. Classes de conjugação de S_5.

Classe	1	$(1,2)$	$(1,2,3)$	$(1,2,3,4)$	$(1,2)(3,4)$	$(1,2,3)(4,5)$	$(1,2,3,4,5)$
Quantidade	1	10	20	30	15	20	24

2. Classes de conjugação de A_5.

Classe	1	$(1,2,3)$	$(1,2)(3,4)$	$(1,2,3,4,5)$	$(1,5,4,3,2)$
Quantidade	1	20	15	12	12

Observação 14.1. A_5 é simples.

Exercício 14.1.

1. Assuma que C é uma classe de conjugação de S_n contida em A_n. Então uma das seguintes afirmações é válida:

   - C é uma classe de A_n.
   - $C = C_1 \cup C_2$, onde C_1, C_2 são classes de A_n, com $|C_1| = |C_2|$ e $C_2 = \{g^{-1} \mid g \in C_1\}$

   A segunda condição acima ocorre se, e somente se, um representante de C é produto de ciclos disjuntos de comprimentos ímpares 2 a 2 distintos.

Aula 15 - Simplicidade de A_n e lema de Iwasawa

Teorema 15.1. Seja $n \geq 5$. Então A_n é simples.

Definição 15.1. Sejam $\mathbb{F}$ um corpo, $GL(n,\mathbb{F}) = \{A \in \mathrm{Mat}_{n\times n}(\mathbb{F}) \mid \det A \neq 0\}$, $SL(n,\mathbb{F}) = \{A \in GL(n,\mathbb{F}) \mid \det A = 1\}$. Seja $P(V) = \{\langle v\rangle \mid v \in V \setminus \{0\}\}$. Note que $GL(n,\mathbb{F})$ e $SL(n,\mathbb{F})$ agem primitivamente em $P(V)$. O núcleo da ação $P(V) \curvearrowleft GL(n,\mathbb{F})$ é $Z = \{\lambda I \mid \lambda \in \mathbb{F}^*\}$ e o núcleo da ação $P(V) \curvearrowleft SL(n,\mathbb{F})$ é $Z \cap SL(n,\mathbb{F}) = \{\lambda I \mid \lambda^n = 1\}$. Dessa forma, definimos o **grupo linear geral projetivo** como

$$PGL(n,\mathbb{F}) = {}^{GL(n,\mathbb{F})}\!/_{Z}$$

Definimos também o **grupo linear especial projetivo** como

$$PSL(n,\mathbb{F}) = {}^{SL(n,\mathbb{F})}\!/_{Z \cap SL(n,\mathbb{F})}.$$

Lema 15.1 (Lema de Iwasawa)**.** Assuma que $\Omega \curvearrowleft G$ primitivamente e que:

1. G é perfeito, isto é, $G' = G$;

2. G_α contém um subgrupo normal abeliano A tal que $\langle A^g \mid g \in G\rangle = G$.

Suponha também que K é o núcleo da ação de G em Ω. Então G/K é simples.

Exercício 15.1.

1. Prove que o núcleo da ação $P(V) \curvearrowleft GL(n,\mathbb{F})$, Z, é o centro do grupo $GL(n,\mathbb{F})$, $\mathcal{Z}(G(n,\mathbb{F}))$ e que o núcleo da ação $P(V) \curvearrowleft SL(n,\mathbb{F})$, $Z \cap SL(n,\mathbb{F})$ é $Z\,SL(n,\mathbb{F})$.

2. Prove que se $n = 1$, então $PSL(1,\mathbb{F}) = 1$ e que $PSL(2,2)$ e $PSL(2,3)$ são solúveis.

3. Prove que

   (a) $\begin{pmatrix} 1 & 0 \\ v & I \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & A \end{pmatrix} = \begin{pmatrix} a & 0 \\ av & A \end{pmatrix}$

   (b) $\begin{pmatrix} 1 & 0 \\ v_1 & I \end{pmatrix}\begin{pmatrix} 1 & 0 \\ v_2 & I \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ v_1+v_2 & I \end{pmatrix}$

   (c) $\begin{pmatrix} a & 0 \\ 0 & A \end{pmatrix}\begin{pmatrix} b & 0 \\ 0 & B \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & AB \end{pmatrix}$

   (d) $\begin{pmatrix} a & 0 \\ 0 & A \end{pmatrix}\begin{pmatrix} 1 & 0 \\ v & I \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ a^{-1}Av & I \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & A \end{pmatrix}$

Aula 16 - Simplicidade de $PSL(n,\mathbb{F})$

Teorema 16.1. Se $n \geq 2$ e $(|n|,|\mathbb{F}|) \neq (2,2)$ ou $(2,3)$, então $PSL(n,\mathbb{F})$ é simples.

Aula 17 - Grupos clássicos

Definição 17.1. Sejam $\mathbb{F}$ um corpo com $\operatorname{char}\mathbb{F} \neq 2$, $V = \mathbb{F}^n$ espaço vetorial e $\sigma \in \operatorname{Aut}\mathbb{F}$. Considere a função $(\cdot,\cdot) : V \times V \to \mathbb{F}$.

1. $(\cdot,\cdot)$ é dita **forma σ-sesquilinear** se $\forall\, \alpha,\beta \in \mathbb{F}$ e $\forall\, u,v, \in V$, vale

   (a) $(\alpha u + \beta v, w) = \alpha(u,w) + \beta(v,w)$.

   (b) $(u, \alpha v + \beta w) = \alpha\sigma(u,v) + \beta\sigma(u,w)$.

2. $(\cdot,\cdot)$ é dita **forma σ-hermitiana** se $\forall\, u,v, \in V$, vale $(u,v) = (v,u)\sigma$.

3. $(\cdot,\cdot)$ é dita **forma bilinear** se ela é id-sesquilinear.

4. $(\cdot,\cdot)$ é dita **forma simplética** se $\forall\, v \in V$, vale $(v,v) = 0$.

5. $(\cdot,\cdot)$ é dita **forma simétrica** se $\forall\, u, v \in V$, vale $(u,v) = (v,u)$.

6. $(\cdot,\cdot)$ é dita **forma antissimétrica** se $\forall\, u, v \in V$, vale $(u,v) = -(v,u)$.

7. $(\cdot,\cdot)$ é dita **forma não degenerada** se $0 = \{v \in V \mid (v,u) = 0, \forall\, u \in V\} = \{v \in V \mid (u,v) = 0, \forall\, u \in V\}$.

Observação 17.1.

- $(\cdot,\cdot)$ simplética $\Rightarrow$ $(\cdot,\cdot)$ antissimétrica.
- Se $\operatorname{char}\mathbb{F} \neq 2$, então $(\cdot,\cdot)$ antissimétrica $\Rightarrow$ $(\cdot,\cdot)$ simplética.

Observação 17.2. Assuma que $(\cdot,\cdot)$ é forma σ-hermitiana não nula e seja $c \in \mathbb{F}$ tal que $c = (u,v)$, para algum $u, v \in V$. Então

$$c\sigma^2 = (u,v)\sigma\sigma = (v,u)\sigma = (u,v) = c$$

Logo $\sigma^2 = \mathrm{id}$. Daí, $\sigma = \mathrm{id}$ ou $|\sigma| = 2$.

Exemplo 17.1. Exemplos de forma σ-hermitiana.

1. $\mathbb{F} = \mathbb{C}$, σ conjugação complexa, isto é, $\sigma(\alpha) = \overline{\alpha}$ e $(\cdot,\cdot)$ o produto interno em $\mathbb{C}$, ou seja, $((\alpha_1,\ldots,\alpha_n),(\beta_1,\ldots,\beta_n)) = \alpha_1\overline{\beta_1} + \cdots + \alpha_n\overline{\beta_n}$.
2. Considere uma extensão de Galois $|\mathbb{F} : \mathbb{K}| = 2$ e tome $\sigma \in \mathrm{Gal}(\mathbb{F} : \mathbb{K}) \setminus \{\mathrm{id}\}$.
3. $\mathbb{F} = \mathbb{F}_q$ com $q = q_0^2$. Tome $\sigma : \mathbb{F}_q \to \mathbb{F}_q$, $x \mapsto x^{q_0}$.

Definição 17.2. Seja $(\cdot,\cdot) : V \times V \to \mathbb{F}$, com $V = \mathbb{F}^n$. Se $(\cdot,\cdot)$ satisfaz uma das seguintes condições abaixo, ela é dita **forma clássica**.

1. Ser forma nula, isto é, $(u,v) = 0$, $\forall\, u, v \in V$.
2. Ser simplética não degenerada.
3. Ser σ-hermitiana não degenerada com $|\sigma| = 2$.
4. Ser simétrica não degenerada.

Exemplo 17.2. Exemplos de formas clássicas.

1. Seja $V = \mathbb{F}^n$. Considere $A = (a_{ij})_{n\times n}$ a matriz nula. Então $(v,u) = vAu^t$.
2. Seja $V = \mathbb{F}^n$. Considere $A = (a_{ij})_{n\times n}$ invertível e antissimétrica (isto é, $A^t = -A$). Então $(v,u) = vAu^t$.
3. Seja $V = \mathbb{F}^n$. Considere $A = (a_{ij})_{n\times n}$ invertível tal que $A^t = A\sigma$, com $\sigma \in \operatorname{Aut}\mathbb{F}$ com $|\sigma| = 2$. Então $(v,u) = vA(u\sigma)^t$.

4. Seja $V = \mathbb{F}^n$. Considere $A = (a_{ij})_{n\times n}$ invertível e simétrica (isto é, $A^t = A$). Então $(v, u) = vAu^t$.

Definição 17.3. Seja $(\cdot,\cdot) : V \times V \to \mathbb{F}$, com $V = \mathbb{F}^n$ uma forma clássica. Dizemos que $g \in GL(n, \mathbb{F})$ é **isometria** se $(ug, vg) = (u, v), \forall\, u, v \in V$. Se $g \in SL(n, \mathbb{F})$, então dizemos que g é **isometria especial**. Definimos também os seguintes conjuntos.

- $G(n, \mathbb{F}) = \{g \in GL(n, \mathbb{F}) \mid g \text{ é isometria}\}$.
- $S(n, \mathbb{F}) = G(n, \mathbb{F}) \cap SL(n, \mathbb{F})$.
- $Z = \{\lambda I \mid \lambda \in \mathbb{F}^*\} = Z(GL(n, \mathbb{F}))$.
- $PG(n, \mathbb{F}) = {}^{G(n,\mathbb{F})}\!/_{Z \cap G(n,\mathbb{F})}$.
- $PS(n, \mathbb{F}) = {}^{S(n,\mathbb{F})}\!/_{Z \cap S(n,\mathbb{F})}$.

Particularmente, definimos

1. Para a forma nula:
   - $G(n, \mathbb{F}) = GL(n, \mathbb{F})$.
   - $S(n, \mathbb{F}) = SL(n, \mathbb{F})$.
   - $PG(n, \mathbb{F}) = PGL(n, \mathbb{F})$.
   - $PS(n, \mathbb{F}) = PSL(n, \mathbb{F})$.
2. Para a forma simplética não degenerada:
   - $G(n, \mathbb{F}) = S(n, \mathbb{F}) = S_p(n, \mathbb{F})$.
   - $PG(n, \mathbb{F}) = PS(n, \mathbb{F}) = PS_p(n, \mathbb{F})$.

   Tais grupos são ditos **grupos simpléticos**.
3. Para a forma σ-hermitiana não degenerada:
   - $G(n, \mathbb{F}) = GU(n, \mathbb{F})$.
   - $S(n, \mathbb{F}) = SU(n, \mathbb{F})$.
   - $PG(n, \mathbb{F}) = PGU(n, \mathbb{F})$.
   - $PS(n, \mathbb{F}) = PSU(n, \mathbb{F})$.

   Tais grupos são ditos **grupos unitários**.
4. Para a forma simétrica não degenerada:
   - $G(n, \mathbb{F}) = GO(n, \mathbb{F})$.

- $S(n, \mathbb{F}) = SO(n, \mathbb{F})$.
- $PG(n, \mathbb{F}) = PGO(n, \mathbb{F})$.
- $PS(n, \mathbb{F}) = PSO(n, \mathbb{F})$.

Tais grupos são ditos **grupos ortogonais**.

Observação 17.3. Se $\mathbb{F} = \mathbb{F}_q$, então escrevemos $GL(n, \mathbb{F})$ como $GL(n, q)$. O mesmo se faz com todos os grupos acima.

Teorema 17.1.

1. $PSL(n, q)$ é simples, se $n \geq 2$ e $(n, q) \neq (2, 2), (2, 3)$.
2. $PS_p(n, q)$ é simples, se $n \geq 2$ e $(n, q) \neq (2, 2), (2, 3), (4, 2)$.
3. $PSU(n, q)$ é simples, se $n \geq 2$ e $(n, q) \neq (2, 4), (2, 9), (3, 4)$.
4. Defina $P\Omega(n, q) = PSO(n, q)'$. Se $n \geq 5$ e q ímpar, então $P\Omega(n, q)$ é simples.

Aula 18 - Grupos livres

Definição 18.1. Sejam X, Y conjuntos disjuntos, onde existe uma bijeção $\varphi : X \to Y$. Denotamos Y por X^{-1} e $\varphi(x) = x^{-1}$. Denotamos também $\varphi^{-1}(x^{-1}) = (x^{-1})^{-1}$, ou seja, $(x^{-1})^{-1} = x$. Se $x_1, x_2, \ldots, x_k \in X \cup X^{-1}$, então a expressão $x_1 x_2 \ldots x_k$ é dita **palavra em X**. Se uma palavra $x_1 x_2 \ldots x_k$ não possui uma subpalavra da forma xx^{-1} ou $x^{-1}x$, com $x \in X$, então ela é dita **palavra reduzida em X**. Seja F_X o conjunto das palavras reduzidas em X. Considere $w_1, w_2 \in F_X$, com $w_1 = x_1 x_2 \ldots x_m x_{m+1} \ldots x_{m+k}$ e $w_2 = y_k y_{k-1} \ldots y_1 y_{k+1} \ldots y_{k+l}$, onde $x_i, y_j \in X \cup X^{-1}$, $y_i = x_{m+i}^{-1}$, $\forall\, i \in \{1, \ldots, k\}$, e $y_{k+1} \neq x_m^{-1}$. Assim, definimos uma operação, $\cdot$, em F_X fazendo $w_1 \cdot w_2 = x_1 \ldots x_m y_{k+1} \ldots y_{k+l}$.

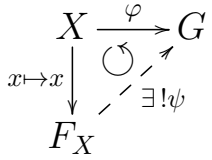
Teorema 18.1. $(F_X, \cdot)$ é um grupo.

Definição 18.2. F_X é o **grupo livre em X**.

Observação 18.1.

- $F_\varnothing = 1$.
- Se $|X| \geq 1$, então F_X é infinito.
- Se $|X| \geq 2$, então F_X é não abeliano.

Teorema 18.2 (Propriedade universal)**.** Sejam X um conjunto, G um grupo e $\varphi : X \to G$ um mapa. Então existe um único homomorfismo $\psi : F_X \to G$ tal que $\psi|_X = \varphi$.



Corolário 18.1. Assuma que G é um grupo gerado por $X \subseteq G$. Então existe um homomorfismo sobrejetivo $\psi : F_X \to G$, logo, $G \cong {}^{F_X}\!/_{\ker \psi}$, ou seja, todo grupo é quociente de algum grupo livre.

Definição 18.3. Seja X um conjunto e considere $Y \subseteq F_X$. Denote por $\langle Y \rangle^{F_X}$ o menor subgrupo normal de F_X que contém Y. Seja $G = {}^{F_X}\!/_{\langle Y \rangle^{F_X}}$. A expressão $\langle X \mid Y \rangle$ é uma **apresentação para o grupo G**.

Exemplo 18.1. $\langle a, b \mid a^n, b^2, abab \rangle$ é uma apresentação para D_n.

Aula 19 - Representações lineares

Definição 19.1. Sejam G um grupo e V um $\mathbb{F}$-espaço vetorial de dimensão finita. Um **representação linear de G** é um homomorfismo de G para $GL(V)$. Um $\mathbb{F}$-espaço vetorial V é dito um **G-módulo**, se está dado um mapa $V \times G \to V$, $(v, g) \mapsto vg$ tal que, para todo $\alpha, \beta \in \mathbb{F}, v, w \in V, g \in G$:

i) $v1 = v$;

ii) $(vg)h = v(gh)$;

iii) $(\alpha v + \beta w)g = \alpha(vg) + \beta(wg)$.

Observação 19.1. Existe uma correspondência biunívoca entre representação linear e G-módulo.

Definição 19.2. Uma representação $\varphi : G \to GL(V)$ é **fiel**, se $\ker \varphi = 1$.

Observação 19.2. Dada $\varphi : G \to GL(V)$ uma representação de G e fixada B uma base de V, então, uma vez que $GL(V) \cong GL(n\mathbb{F})$, podemos considerar o homomorfismo de G para $GL(n, \mathbb{F})$, que leva $g \in G$ na matriz da aplicação $g\varphi$.

Exemplo 19.1.

1. Se $G \leq S_n$, $V = \langle e_1, \ldots, e_n \rangle$ espaço vetorial sobre $\mathbb{F}$, então V é um G-módulo pela ação $e_i g = e_{ig}$, chamado **módulo permutacional**. A representação correspondente é dita **representação permutacional**. Tal representação é fiel

2. Se $G = D_n = \langle a, b \mid a^n, b^2, baba \rangle$, $V = \mathbb{R}^2$, então $\varphi : G \to GL(V)$ tal que $a \mapsto \text{Rot}(\frac{2\pi}{n})$, $b \mapsto \text{Ref}(\pi)$ é uma representação linear. Tal representação é fiel. Vendo como matriz, $a \mapsto \begin{pmatrix} \cos\frac{2\pi}{n} & \text{sen}\,\frac{2\pi}{n} \\ -\text{sen}\,\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix}$ e $b \mapsto \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$

3. Se G é um grupo qualquer e V um espaço vetorial arbitrário, então $\varphi : G \to GL(V)$, $g \mapsto \text{id}$, é representação linear de G. Se $|G| \geq 2$, então tal representação não é fiel.

Definição 19.3. Sejam V_1, V_2 G-módulos sobre $\mathbb{F}$. Uma aplicação linear $\varphi : V_1 \to V_1$ é dita **homomorfismo de G-módulo** (ou G-homomorfismo), se $(v\varphi)g = (vg)\varphi$, para todo $v \in V_1, g \in G$.

Definição 19.4. Sejam V um G-módulo e $U \leq V$ um subespaço. Dizemos que U é um **G-submódulo**, $U \leq_G V$, se $ug \in U$, $\forall\, u \in U, g \in G$.

Exemplo 19.2.

1. $\{0\}$ e V são G-módulos.

2. Sejam $G = S_n$ e $V = \langle e_1, \ldots, e_n \rangle$, então $U = \langle e_1 + \cdots + e_3 \rangle$ e $W = \{\alpha_1 e_1 + \cdots + \alpha_n e_n \mid \sum_{i=1}^n \alpha_i = 0\}$ são G-submódulos e $\dim U = 1$ e $\dim W = n - 1$. Se $\text{char}\,\mathbb{F} = 0$, então $V = U \oplus W$. Além disso, eles são os únicos G-submódulos.

Exercício 19.1.

1. Se $\varphi : V_1 \to V_2$ é G-homomorfismo, então $\ker\varphi \leq_G V_1$ e $\text{Im}\,\varphi \leq_G V_2$.

Aula 20 - Teorema de Maschke

Definição 20.1. Um G-módulo V é **simples** ou **irredutível**, se $\{0\}$ e V são todos os submódulos de V.

Exemplo 20.1.

a) $\mathbb{F}$ é um G módulo redutível.

b) A representação permutacional é redutível.

Definição 20.2. Um G-módulo V é **completamente redutível**, se $V \cong V_1 \oplus \cdots \oplus V_k$, onde V_i são G-módulos simples.

Exemplo 20.2. Sejam $G = C_2 = \langle g \rangle$, $V = \mathbb{F}_2^2 = \langle e_1, e_2 \rangle$. Então V é redutível, mas não é completamente redutível.

Definição 20.3. Sejam G um grupo e $\mathbb{F}$ um corpo. Definimos a **álgebra de grupo** como sendo $\mathbb{F}G = \{\sum \alpha_g g \mid \alpha_g \in \mathbb{F},\, g \in G\}$, onde $(\sum \alpha_g g)(\sum \beta_h h) = \sum \alpha_g \beta_h gh$. Note que $\mathbb{F}G$ é um espaço vetorial com base G.

Observação 20.1.

- Existe uma correspondência biunívoca entre representação de G e representação de $\mathbb{F}G$.
- Os G-submódulos de $\mathbb{F}G$ são ideais à direita. Além disso, se $U \subseteq \mathbb{F}G$ é ideal à direita, então $\mathbb{F}G/U$ é G-submódulo.
- Se V é G-módulo e $U \leq_G V$, então V/U é um G-módulo.

Teorema 20.1 (Teorema de Maschke)**.** Seja G um grupo finito e $\mathbb{F}$ um corpo. As sequintes afirmações são equivalentes.

1. Todo $\mathbb{F}G$-módulo de dimensão finita é completamente redutível.
2. $\operatorname{char}\mathbb{F} \nmid |G|$.

Aula 21 - Lema de Schur

Teorema 21.1 (Lema de Schur)**.** Sejam V, U G-módulos simples e seja $\alpha : V \to U$ um G-homomorfismo (α é transformação linear tal que $(v\alpha)g = (vg)\alpha$, $\forall g \in G, v \in V$). Então $\alpha = 0$ ou α é invertível (bijeção).

Corolário 21.1. Sejam G um grupo e V um G-módulo simples de dimensão finita sobre $\mathbb{F}$ algebricamente fechado. Seja $\alpha \in \operatorname{End}(V)$. Então $\alpha = \lambda \operatorname{id}$, onde $\lambda \in \mathbb{F}$. Em particular, $\operatorname{End}(V) \cong \mathbb{F}$.

Corolário 21.2. Sejam V um G-módulo simples de dimensão finita e seja $\rho : G \to GL(V)$ sua representação correspondente. Então $\mathcal{Z}(G)\rho \leq \{\lambda \operatorname{id} \mid \lambda \in \mathbb{F}^*\}$. Em outros termos, se $g \in \mathcal{Z}(G)$, então existe $\lambda_g \in \mathbb{F}^*$ tal que $vg = \lambda_g v$.

Corolário 21.3. Se G é abeliano e V é um G-módulo simples de dimensão finita sobre $\mathbb{F}$ algebricamente fechado, então $\dim V = 1$.

Exemplo 21.1. Considere $G = C_4 = \langle g \rangle$, $V = \mathbb{R}^2$ e $vg = v \operatorname{Rot}(\frac{\pi}{2})$ (ou seja, $g \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$). Então V é simples e $\dim V = 2$.

Exemplo 21.2. Sejam $\xi \neq 1$ tal que $\xi^5 = 1$ e $\mathbb{F}$ um corpo tal que $\xi \in \mathbb{F}$. Sejam

$$A = \begin{pmatrix} \xi & 0 & 0 & 0 \\ 0 & \xi^3 & 0 & 0 \\ 0 & 0 & \xi^4 & 0 \\ 0 & 0 & 0 & \xi^2 \end{pmatrix} \quad \text{e} \quad B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Então $A^B = B^{-1}AB = A^2$, ou seja, $\langle B \rangle$ normaliza $\langle A \rangle$. Assim, podemos considerar $G = \langle A \rangle \langle B \rangle = \{A^i B^j \mid i = 0, \ldots, 4 \text{ e } j = 0, \ldots, 3\}$. Note que $|G| = 20$. Sejam $N = \langle A \rangle \trianglelefteq G$ e $V = \mathbb{F}^4$. Então V é um G-módulo irredutível. Porém, V como N-módulo é redutível, com $V = V_1 \oplus V_2 \oplus V_3 \oplus V_4$, onde $V_i = \langle e_i \rangle$ e e_i é a i-ésima base canônica de $\mathbb{F}^4$. Além disso, B induz uma permutação no conjunto $X = \{V_1, V_2, V_3, V_4\}$.

Aula 22 - Teorema de Clifford

Definição 22.1. Sejam G um grupo e V um G-módulo. A cadeia de G-módulos $V = V_0 > V_1 > V_2 > \cdots > V_k > V_{k+1} = 0$ é dita **série de composição** se V_i / V_{i+1} é simples, para todo i.

Teorema 22.1 (Jordan-Hölder)**.** Seja V G-módulo de dimensão finita simples. Então existe uma série de composição em V. Além disso, se $V = V_0 > V_1 > V_2 > \cdots > V_k > V_{k+1} = 0$ e $U = U_0 > U_1 > U_2 > \cdots > U_m > U_{m+1} = 0$ são séries de composição, então $k = m$ e existe $\pi \in S_k$ tal que $V_i / V_{i+1} \cong U_{i\pi} / U_{i\pi+1}$.

Observação 22.1. Se $\operatorname{char} \mathbb{F} \nmid |G|$ e $V = V_0 > V_1 > V_2 > \cdots > V_k > V_{k+1} = 0$ é série de composição, então, por Maschke, $V \cong U_0 \oplus \cdots \oplus U_k$, onde $U_i = V_i / V_{i+1}$.

Teorema 22.2 (Clifford)**.** Sejam V um G-módulo simples de dimensão finita, $N \trianglelefteq G$ e $U \leq_N V$ simples. Então

1. $V = \sum_{g \in G} Ug$ e V é N-completamente redutível.
2. Sejam $I_1, I_2, \ldots, I_k$ tipos de isomorfismos de N-módulos simples de V e considere, para todo i, $V_i = \sum W$, onde $W \leq_N V$ e $W \cong I_i$. Então $V \cong V_1 \oplus \cdots \oplus V_k$
3. G age transitivamente em $\{V_1, \ldots, V_k\}$.
4. G_{V_i} é irredutível em V_i.

Aula 23 - Caracter de uma representação

Definição 23.1. Sejam V um espaço vetorial e $T \in \mathrm{End}(V)$. Dizemos que T é **diagonalizável**, se existe uma base B de V tal que $[T]_B$ é diagonal.

Observação 23.1. As seguintes afirmações são equivalentes.

1. T é diagonalizável.
2. V possui uma base formada por autovetores de T.
3. Se $\mathbb{F}$ é algebricamente fechado, então os blocos de Jordan têm dimensão 1.
4. As raízes do polinômio minimal de T são distintas, sobre o fecho algébrico.

Lema 23.1. Seja X uma matriz complexa de ordem finita n. Então X é diagonalizável e os autovetores de X são n-ésima raízes da unidade.

Definição 23.2. Seja $\rho : G \to GL(V)$. Fixada uma base B de V, definimos o **caracter de $\boldsymbol{\rho}$** como sendo a função $\chi = \chi_\rho : G \to \mathbb{F}$, $g \mapsto \mathrm{tr}[g\rho]_B$.

Observação 23.2. Se B' é outra base de V, então $[g\rho]_B$ e $[g\rho]_{B'}$ são conjugadas. Daí χ independe da base.

Lema 23.2. Sejam $\mathbb{F}$ corpo, $\rho : G \to GL(V)$ representação e χ caracter de ρ. Então:

1. $\chi(1) = \dim V$.
2. χ é constante nas classes de conjugação de G.
3. Se $\mathbb{F} = \mathbb{C}$, então $\chi(g^{-1}) = \overline{\chi(g)}$.

Exemplo 23.1. Sejam $G = C_3 = \langle g \rangle$ e $\mathbb{F} = \mathbb{C}$. Então as representações irredutíveis de G são $\rho_j : G \to GL(V)$, $g \mapsto \xi^j$, onde $\xi = e^{\frac{i2\pi}{3}}$, com $j = 1, 2, 3$. Segue a tabela de caracteres.

	1	g	g^2
χ_1	1	ξ	ξ^2
χ_2	1	ξ^2	ξ
χ_3	1	1	1

Exercício 23.1. Se A e B são matrizes $n \times n$, então $\mathrm{tr}\, AB = \mathrm{tr}\, BA$. Em particular, se B é invertível, então $\mathrm{tr}\, B^{-1}AB = \mathrm{tr}\, BB^{-1}A = \mathrm{tr}\, A$. Além disso, $\mathrm{tr}\, A = \sum \lambda_i$, onde λ_i são autovalores com multiplicidade geométrica.

Aula 24 - Relações de ortogonalidade

Definição 24.1. Seja V um $\mathbb{C}$-espaço vetorial. Uma aplicação $V \times V \to \mathbb{C}$, $(u, v) \mapsto \langle u, v\rangle$ é dita **produto interno** se satisfaz

1. $\langle u + v, w\rangle = \langle u, w\rangle + \langle v, w\rangle$.
2. $\langle \lambda u, w\rangle = \lambda\langle u, w\rangle$.
3. $\langle u, w\rangle = \overline{\langle w, u\rangle}$.
4. $\langle u, u\rangle \in \mathbb{R}_{\geq 0}$.
5. $\langle u, u\rangle = 0 \Leftrightarrow u = 0$.

Observação 24.1. Seja $V \times V \to \mathbb{C}$, $(u, v) \mapsto \langle u, v\rangle$, um produto interno. Então

- $\langle u, \lambda w\rangle = \overline{\lambda}\langle u, w\rangle$.
- $\langle u, v + w\rangle = \langle u, v\rangle + \langle u, w\rangle$.
- Se $\dim V < \infty$, existe $b_1, \ldots, b_n$ base ortonormal de V, isto é, $\langle b_i, b_j\rangle = \delta_{ij}$. Além disso, se $v \in V$, então $v = \alpha_1 v_1 + \cdots + \alpha_n v_n$, onde $\alpha_i = \langle v, b_i\rangle$.

Exemplo 24.1. Seja $V = \mathcal{F}(X, \mathbb{C})$ o conjunto de todas as funções $f : X \to \mathbb{C}$, com X sendo um conjunto finito qualquer. Note que V é um $\mathbb{C}$-espaço vetorial isomorfo a $\mathbb{C}^{|X|}$. Nesse espaço vetorial, podemos definir o seguinte produto interno.

$$\langle f, g\rangle = \frac{1}{|X|}\sum_{x\in X} f(x)g(x)$$

Lema 24.1. Sejam $\rho : G \to GL(n, \mathbb{F})$ e $\sigma : G \to GL(m, \mathbb{F})$ representações irredutíveis do grupo finito G. Sejam $i, j \in \{1, \ldots, n\}$ e $r, s \in \{1, \ldots, m\}$.

1. Se ρ e σ são equivalentes, então $\sum_{g\in G}(g\rho)_{ij}(g^{-1\sigma})_{rs} = 0$.
2. Se $\mathbb{F}$ é algebricamente fechado, com $\operatorname{char}\mathbb{F} \nmid |G|$, então $\sum_{g\in G}(g\rho)_{ij}(g^{-1\rho})_{rs} = \frac{|G|}{n}\delta_{is}\delta_{jr}$.

Aula 25 - Relações de ortogonalidade - parte II

Corolário 25.1 (Relações de ortogonalidade)**.** Sejam ρ e σ representações irredutíveis de G (grupo finito) que não são equivalentes. Sejam χ e ψ os caracteres correspondentes. Então

1. $\sum_{g\in G}(g\chi)(g^{-1}\psi) = 0$.

2. $\sum_{g\in G}(g\chi)(g^{-1}\chi) = |G|$.

Observação 25.1. Note que

1. $\sum_{g\in G}(g\chi)(g^{-1}\psi) = 0 \Leftrightarrow \langle\chi,\psi\rangle = 0$.
2. $\sum_{g\in G}(g\chi)(g^{-1}\chi) = |G| \Leftrightarrow \langle\chi,\chi\rangle = 1$.

Observação 25.2.

1. Sejam $\rho, \sigma : G \to GL(V)$ representações de G e χ e ψ seus caracteres, respectivamente. Se ρ é equivalente a σ, então $\chi = \psi$. Caso contrário, $\chi \neq \psi$.
2. Seja V um G-módulo sobre $\mathbb{C}$. Por Maschke, $V = V_1 \oplus \cdots \oplus V_k$, onde V_i são simples. Sejam $\chi, \chi_1, \ldots, \chi_k$ os caracteres correspondentes a $V, V_1, \ldots, V_k$, respectivamente. Então $\chi = \chi_1 + \cdots + \chi_k$.
3. Se $\chi_1, \ldots, \chi_k$ são caracteres irredutíveis de G, grupo finito, e χ é um caractere (não necessariamante irredutível), então $\chi = \alpha_1\chi_1 + \cdots + \alpha_k\chi_k$, com $\alpha_i \in \mathbb{N}\cup\{0\}$. Note que $\alpha_i = \langle\chi,\chi_i\rangle$ e também que $\langle\chi,\chi\rangle = \alpha_1^2 + \cdots + \alpha_k^2 = 1 \Leftrightarrow \chi$ é irredutível.

Exemplo 25.1. Tabela de A_4. Nela $\xi = e^{\frac{i2\pi}{3}}$

	1	(12)(34)	(123)	(132)
χ_1	1	1	1	1
χ_2	1	1	ξ	$\overline{\xi}$
χ_3	1	1	$\overline{\xi}$	ξ
χ_4	3	-1	0	0

Teorema 25.1. Se G é um grupo finito, $\rho_1, \ldots, \rho_k$ são representações irredutíveis de G sobre $\mathbb{C}$ (a menos de equivalência) e d_i é a dimensão de ρ_i, então $|G| = \sum_{i=1}^{k} d_i^2$.

Aula 26 - Relações de ortogonalidade - parte III

Definição 26.1. Sejam $W = \{f : G \to \mathbb{C} \mid (x^{-1}gx)f = (g)f,\ \forall g, x \in G\}$, $f \in W$ e $\sigma : G \to GL(V)$. Defina $\sigma_f = \sum_{g\in G}(gf)(g\sigma)$.

Lema 26.1. Se σ é irredutível co caracter χ, então $\sigma_f = \sum_{g\in G}(gf)(g\sigma)$.

Teorema 26.1. Sejam G um grupo finito e $W = \{f : G \to \mathbb{C} \mid (x^{-1}gx)f = (g)f,\ \forall g, x \in G\}$. Então os caracter irredutíveis de G formam uma base ortonormal de W. (Esse enunciado também foi apresentado na aula 24).

Teorema 26.2.

1. $\dim W =$ número de classes de conjugação.

2. O número de classes de equivalências de representações irredutíveis é igual ao número de classes de conjugação.

3. Se $\chi_1, \ldots, \chi_k$ são caracteres irredutíveis, então

$$\langle \chi_i, \chi_j \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_i(g)\overline{\chi_j(g)} = \begin{cases} 0, & \chi_i \neq \chi_j \\ 1, & \chi_i = \chi_j \end{cases}$$

(Ver as notas da aula 24).

Corolário 26.1 (Ortogonalidade das colunas)**.** Sejam $g, h \in G$ pertencentes a classes distintas de conjugação. Assuma que $\chi_1, \ldots, \chi_k$ são caracteres irredutíveis.

1. $\sum_{i=1}^{k} (g\chi_i)\overline{g\chi_i} = |C_G(g)|$
2. $\sum_{i=1}^{k} (g\chi_i)\overline{h\chi_i} = 0$

Exemplo 26.1. Tabela de S_4.

Classes	1	(12)	(12)(34)	(123)	(1234)
#classe	1	6	3	8	6
$\#C_G(g)$	24	4	8	3	4
χ_1	1	1	1	1	1
χ_2	1	-1	1	1	-1
χ_3	3	1	-1	0	-1
χ_4	3	-1	-1	0	1
χ_5	2	0	2	-1	0

Exercício 26.1. Sejam V um $\mathbb{C}$-espaço com produto interno e $v_1, \ldots, v_k$ um sistema ortonormal. Se $\{v \in V \mid \langle v, v_i \rangle = 0, \forall i\} = \{0\}$, então $v_1, \ldots, v_k$ é base de V.