# Resumo de Álgebra Avançada

## 1 Aula 1 - Conceitos iniciais de grupo

**Definição 1.1.** Um **grupo** é um conjunto $G$ com uma operação $\cdot : G \times G \to G$, $(g, h) \mapsto g \cdot h = gh$, chamada **produto** (ou multiplicação) que satisfaz:

i) Para todo $a, b, c \in G$, vale $(ab)c = a(bc)$ (associatividade).

ii) Existe $e \in G$ tal que, para todo $g \in G$, temos que $eg = ge = g$ (existência de um elemento neutro).

iii) Para todo $a \in G$, existe $b \in G$ tal que $ab = ba = e$ (existência de um inverso).

**Lema 1.1.** O elemento neutro é único

**Lema 1.2.** O inverso é único.

**Lema 1.3.** Sejam $f, g \in G$. Então as equações $fx = g$ e $xf = g$ possuem única solução.

**Lema 1.4.** Se $f, g \in G$, então $(fg)^{-1} = g^{-1}f^{-1}$. Em particular, se $g_1, \ldots, g_n \in G$, então $(g_1 \ldots g_n)^{-1} = g_n^{-1} \ldots g_1^{-1}$.

**Definição 1.2.** Um grupo $G$ é **abeliano** (ou comutativo), se para todo $a, b \in G$, ocorre $ab = ba$.

## 2 Aula 2 - Subgrupo gerado

**Definição 2.1.** Sejam $n \in \mathbb{Z}$ e $g \in G$. Definimos $g^n = (g^{n-1})g$, $g^0 = e$ e $g^{-n} = (g^n)^{-1}$.

**Lema 2.1.** $g^{-n} = (g^{-1})^n$.

**Definição 2.2.** Dizemos que $H \subseteq G$, com $H \neq \emptyset$, é um **subgrupo de** $G$, se $H$ é grupo com o mesmo produto de $G$. Notação: $H \leq G$.

**Lema 2.2.** $H \subseteq G$, com $H \neq \emptyset$ é subgrupo de $G$, se, e somente se,

i) para todo $h_1, h_2 \in H$, $h_1h_2 \in H$.

ii) para todo $h \in H$, $h^{-1} \in H$.

**Definição 2.3.** Seja $g \in G$. Definimos $\langle g \rangle = \{g^z \mid z \in \mathbb{Z}\}$ e o denominamos por **subgrupo de** $G$ **gerado por** $g$.

**Lema 2.3.** $\langle g \rangle$ é subgrupo de $G$.

**Lema 2.4.** Considere $G = (\mathbb{Z}, +)$. Se $H$ é subgrupo de $G$, então existe $n \in \mathbb{Z}_{\geq 0}$ tal que $H = n\mathbb{Z} = \langle n \rangle = \{nz \mid z \in \mathbb{Z}\}$.

**Definição 2.4.** Dado um grupo $G$, denotamos $|G|$ ou $o(G)$ como sendo a cardinalidade de $G$. Dizemos que $G$ é finito, se $|G| < \infty$ e que é infinito se $|G| = \infty$.

**Definição 2.5.** Sejam um grupo $G$ e $g \in G$. Definimos a **ordem de** $g$ como sendo $|\langle g \rangle|$. Notação: $|g|$ ou $o(g)$.

**Lema 2.5.** Seja $g \in G$ tal que $|g| = n$. Então valem as seguintes propriedades:

i) $g^n = e$.

ii) $\langle g \rangle = \{g^0 = e, g, g^2, \ldots, g^{n-1}\}$.

iii) se $z \in \mathbb{Z}$ é tal que $g^z = e$, então $n \mid z$.

# 3 Aula 3 - Teorema de Lagrange

**Definição 3.1.** Seja $H \leq G$. Uma **classe lateral à direita de $H$ em** $G$ é um subconjunto $Hg = \{hg \mid h \in H\}$, para algum $g \in G$. Analogamente, defini-se uma classe lateral à esquerda.

**Lema 3.1.** Sejam $H \leq G$ e $g_1, g_2 \in G$. Então $Hg_1 = Hg_2$ ou $Hg_1 \cap Hg_2 = \emptyset$.

**Corolário 3.1.** Sejam $H \leq G$ e $g_1, g_2 \in G$. Então $Hg_1 = Hg_2 \Leftrightarrow g_2 \in Hg_1$ e $g_1 \in Hg_2$.

**Proposição 3.1.** Seja $H \leq G$. Então

a) $G$ é união disjunta das classes laterais à direita.

a) $G$ é união disjunta das classes laterais à esquerda.

**Lema 3.2.** Seja $H \leq G$. Defina $X_1 = \{$ classes laterais à direita de $H$ em $G$ $\}$ e $X_2 = \{$ classes laterais à esquerda de $H$ em $G$ $\}$. Então existe uma bijeção $\varphi : X_1 \to X_2$.

**Definição 3.2.** Seja $H \leq G$. Uma **transversal à direita de $H$ em** $G$ é um subconjunto $T$ de $G$ tal que $G = \bigcup_{s \in S} Hs$.

**Definição 3.3.** Seja $H \leq G$. O **índice de $H$ em** $G$, denotado por $[G : H]$, é $|T| = |S|$, para alguma transversal à direita $T$ ou alguma transversal à esquerda $S$.

**Teorema 3.1** (Lagrange)**.** Seja $H \leq G$. Então $o(G) = o(H)[G : H]$.

**Corolário 3.2.** Se $o(G) < \infty$ e $H \leq G$, então $o(H) \mid o(G)$.

**Corolário 3.3.** Se $o(G) < \infty$ e $g \in G$, então $o(g) \mid o(G)$.

**Corolário 3.4.** Se $p \in \mathbb{Z}_{>0}$ é primo e $|G| = p$, então $G$ é cíclico, ou seja, existe $g \in G$ tal que $G = \langle g \rangle$.

**Proposição 3.2.** Sejam $H \leq G$ e $K \leq H$. Então $[G : K] = [G : H][H : K]$.

**Lema 3.3** (Euler)**.** Sejam $n \in \mathbb{N}$, com $n \geq 2$, e $a \in \mathbb{Z}$, tal que $\text{mdc}(a, n) = 1$. Então $a^{\varphi(n)} \equiv 1 \pmod{n}$, onde $\varphi(n) = \#\{1 \leq r \leq n \mid \text{mdc}(r, n) = 1\}$.

# 4 Aula 4 - Grupos quociente e comutador

**Definição 4.1.** Sejam $H \leq G$ e $g_1, g_2 \in G$. Definimos o produto de classes como sendo $g_1 H g_2 H = (g_1 g_2)H$.

**Proposição 4.1.** Seja $H \leq G$. Então são equivalentes:

a) O produto das classes é bem definido.

b) $gH = Hg$, para todo $g \in G$

**Definição 4.2.** Um subgrupo $H$ de $G$ é **normal**, se $Hg = gH$ (ou, equivalentemente, $g^{-1}Hg = H$). Notação: $H \lhd G$.

**Lema 4.1.** Se $H \leq G$ tal que $[G : H] = 2$, então $H \lhd G$.

**Definição 4.3.** Definimos o **centro de** $G$ por $\mathcal{Z}(G) = \{g \in G \mid \forall\, h \in G, gh = hg\}$.

**Lema 4.2.** $\mathcal{Z}(G) \lhd G$.

**Teorema 4.1.** Seja $H \lhd G$. Defina $G/H = \{gH \mid g \in G\}$. Então $G/H$ é grupo com a operação induzida de $G$, isto é, $(g_1H)(g_2H) = (g_1g_2)H$.

**Definição 4.4.** Chamamos $G/H$ de **grupo quociente de $G$ por $H$**.

**Definição 4.5.** Seja $\emptyset \neq S \subseteq G$. Definimos $\langle S \rangle = \{g_1g_2 \dots g_k \mid k \geq 1 \text{ e } g_i \in S \cup S^{-1}\}$, onde $S^{-1} = \{s^{-1} \mid s \in S\}$.

**Teorema 4.2.** $\langle S \rangle$ é o menor subgrupo de $G$ que contém $S$, isto é, se $S \subseteq H \leq G$, então $\langle S \rangle \subseteq H$.

**Definição 4.6.** Sejam $g, h \in G$. O **comutador de $g$ e $h$** é $[g, h] = g^{-1}h^{-1}gh$.

**Definição 4.7.** Seja $S = \{[g, h] \mid g, h \in G\}$. Definimos o **comutador de $G$** (ou subgrupo derivado de $G$) por $G' = \langle S \rangle$ (às vezes, denotado também por $[G, G]$).

**Teorema 4.3.**

a) $G' \lhd G$.

b) $G/G'$ é abeliano.

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

# 5 Aula 5 - Homomorfismo

**Definição 5.1.** Uma função (de conjuntos) $\varphi : G \to H$ é um **homomorfismo**, se $\varphi(ab) = \varphi(a)\varphi(b)$, para todo $a, b \in G$.

**Lema 5.1.** Seja $\varphi : G \to H$ um homomorfismo. Então:

i) $\varphi(1_G) = 1_H$.

ii) $\varphi(g^{-1}) = \varphi(g)^{-1}$, para todo $g \in G$.

iii) $\ker \varphi = \{g \in G \mid \varphi(g) = 1_H\} \lhd G$.

iv) $\operatorname{Im} \varphi = \{h \in H \mid \exists\, g \in G, \varphi(g) = h\} \leq H$.

**Definição 5.2.** Seja $\varphi : G \to H$ um homomorfismo. Então:

i) $\varphi$ é **monomorfismo**, se $\varphi$ é injetora.

ii) $\varphi$ é **epimorfismo**, se $\operatorname{Im} \varphi = H$.

iii) $\varphi$ é **isomorfismo**, se $\varphi$ é bijetora.

**Lema 5.2.** Seja $\varphi : G \to H$ um homomorfismo. Então:

i) $\varphi$ é monomorfismo $\Leftrightarrow \ker \varphi = \{1_G\}$.

ii) $\varphi$ é isomorfismo $\Leftrightarrow$ existe $\theta : H \to G$ homomorfismo tal que $\theta \circ \varphi = \mathrm{id}_G$ e $\varphi \circ \theta = \mathrm{id}_H$.

**Lema 5.3.** Seja $\varphi : G \to H$ um homomorfismo. Então:

a) Se $A \leq G$, então $\varphi(A) \leq H$. Além disso, $\varphi^{-1}(\varphi(A)) = A \ker \varphi = \{ah \mid a \in G, h \in \ker \varphi\}$.

b) Se $B \leq H$, então $\varphi^{-1}(B) \leq G$. Além disso, $\varphi(\varphi^{-1}(B)) = B \cap \operatorname{Im} \varphi$.

**Teorema 5.1** (Isomorfismo)**.** Sejam $\varphi : G \to H$ um homomorfismo e $N = \ker \varphi$. Então:

1. $\varphi$ induz um isomorfismo entre $G/N$ e $\operatorname{Im} \varphi$ com a função $\theta : G/N \to \operatorname{Im} \varphi$, $gN \mapsto \varphi(g)$.
2. Existe uma bijeção entre { subgrupos de $G$ que contêm $N$ } e { subgrupos de $\operatorname{Im} \varphi$ }, fazendo $N \leq K \leq G \mapsto \varphi(K)$ e $\varphi^{-1}(C) \hookleftarrow C \leq \operatorname{Im} \varphi$
3. $K \lhd G \Leftrightarrow \varphi(K) \lhd \operatorname{Im} \varphi$.

**Corolário 5.1.** Sejam $A \leq G$ e $\varphi : G \to H$ um homomorfismo. Então $A \cap \ker \varphi \lhd A$ e $A/A \cap \ker \varphi \cong \varphi(A)$.

**Lema 5.4.** Se $N \lhd G$ e $K \leq G$. Então:

i) $NK = KN$ e é subgrupo de $G$.

ii) Se $K \lhd G$, então $NK \lhd G$.

**Corolário 5.2.** Se $N \lhd G$ e $K \leq G$, então $K/N \cap K \cong KN/N$.

# 6 Aula 6 - Subgrupo característico e produto direto

**Corolário 6.1.** Se $K \leq H \leq G$, $K \lhd G$ e $H \lhd G$, então $G/H \cong \left(G/K\right)/\left(H/K\right)$.

**Definição 6.1.** $\operatorname{Aut}(G) = \{\varphi : G \to G \mid \varphi \text{ é isomorfismo } \}$.

**Lema 6.1.** $\operatorname{Aut}(G)$ sobre a composição de funções é grupo.

**Definição 6.2.** Dado $g \in G$, definimos $I_g : G \to G$, $h \mapsto ghg^{-1}$.

**Lema 6.2.**

1. $I_g \in \operatorname{Aut}(G)$.
2. $I_{g_1 g_2} = I_{g_1} \circ I_{g_2}$.
3. $I_{g^{-1}} = (I_g)^{-1}$.
4. Se $\sigma \in \operatorname{Aut}(G)$, então $\sigma I_g \sigma^{-1} = I_{\sigma(g)}$.

**Lema 6.3.** $\operatorname{Inn}(G) = \{I_g \mid g \in G\} \lhd \operatorname{Aut}(G)$.

**Definição 6.3.** Seja $H \leq G$ tal que $\varphi(H) \subset H$, para todo $\varphi \in \operatorname{Aut}(G)$. Então $H$ é chamado de **subgrupo característico de** $G$ e é denotado por $H \lhd_{char} G$.

**Lema 6.4.** Se $H \lhd_{char} G$, então $H \lhd G$.

**Lema 6.5.** Se $T \subseteq G$ e $\varphi \in \operatorname{Aut}(G)$, então $\varphi(\langle T \rangle) = \langle \varphi(T) \rangle$.

**Lema 6.6.** Se $M \lhd_{char} H \lhd G$, então $M \lhd G$.

**Definição 6.4.** Sejam $G_1, \ldots, G_k$ grupos. Considere o produto cartesiano $G_1 \times \cdots \times G_k$ e defina $(g_1, \ldots, g_k)(h_1, \ldots, h_k) = (g_1 h_1, \ldots, g_k h_k)$, com $g_i h_i$ usando o produto de $G_i$.

**Lema 6.7.** $G = G_1 \times \cdots \times G_k$ com a multiplicação acima é grupo.

**Lema 6.8.**

1. $H_i = \{(1_{G_1}, \ldots, 1_{G_{i-1}}, g, 1_{G_{i+1}}, \ldots, 1_{G_k}) \mid g \in G_i\} \lhd G$
2. Se $h_i \in H_i$, $h_j \in H_j$ e $i \neq j$, então $h_i h_j = h_j h_i$.
3. $G = H_1 \ldots H_k$.
4. $H_i \cong G_i$, para todo $i = 1, \ldots, k$.

**Lema 6.9.** Sejam $G$ grupo e $H_i \leq G$, com $i = 1, \ldots, k$ tais que

i) $h_i h_j = h_j h_i$, para todo $h_i \in H_i$, $h_j \in H_j$ e $i \neq j$.

ii) para todo $g \in G$, existem únicos $h_i \in H_i$ tais que $g = h_1 \ldots h_k$.

Então $G \cong H_1 \times \cdots \times H_k$.

**Teorema 6.1** (Chinês do Resto)**.** Sejam $m_1, \ldots, m_k \in \mathbb{Z}_{>0}$ tais que $\text{mdc}(m_i, m_j) = 1$, se $i \neq j$. Se $m = m_1 \ldots m_k$, então $\mathbb{Z}_m \cong \mathbb{Z}/m_1\mathbb{Z} \times \ldots \mathbb{Z}/m_k\mathbb{Z} \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$

**Lema 6.10.** Se $G$ é cíclico, então existe $\varphi : \mathbb{Z} \to G$ epimorfismo.

**Corolário 6.2.** Se $G$ é cíclico, com $|G| = \infty$, então $G \cong \mathbb{Z}$.

**Corolário 6.3.** Se $G$ é cíclico, com $|G| < \infty$, então $G \cong \mathbb{Z}/m\mathbb{Z}$, com $m > 0$.

# 7 Aula 7 - Grupo de permutação

**Lema 7.1.** Seja $G$ um grupo cíclico de ordem finita.

a) Se $H \leq G$, então $o(H) \mid o(G)$ e $H$ é cíclico.

b) Se $d \mid o(G)$, então existe $H \leq G$ tal que $o(H) = d$.

**Lema 7.2.** Sejam $G = \mathbb{Z}/m\mathbb{Z}$ e $g = s + m\mathbb{Z}$, com $0 \leq 0 \leq m - 1$. Então $o(g) = o(G) \Leftrightarrow G = \langle g \rangle \Leftrightarrow \text{mdc}(s, m) = 1$.

**Definição 7.1.** Seja $X = \{1, \ldots, n\}$. Denotaremos o grupo de permutação dos elementos de $X$ por $S_n$, ou seja, $S_n = \{f : X \to X \mid f \text{ é bijetora } \}$ com a operação de composição de funções.

**Teorema 7.1** (Cayley)**.** Seja $G$ um grupo finito. Então existe um monomorfismo $\varphi : G \to S_n$, para algum $n$.

**Definição 7.2.** Um elementos $\mu \in S_k$ é chamado **ciclo**, se existem $i_1, \ldots, i_m$ $(m \geq 2)$ tal que $i_1 \xrightarrow{\mu} i_2 \xrightarrow{\mu} \ldots \xrightarrow{\mu} i_m \xrightarrow{\mu} i_1$ e $\mu(\ell) = \ell$, se $\ell \notin \{i_1, \ldots, i_m\}$.

**Definição 7.3.** Ciclos $\sigma_1, \sigma_2$ são **independentes** se $\text{supp}(\sigma_1) \cap \text{supp}(\sigma_2) = \emptyset$, onde $\text{supp}(\sigma) = \{i \mid \sigma(i) \neq i\}$.

**Teorema 7.2.** Se $g \in S_m$, então $g = \sigma_1 \ldots \sigma_j$, onde $\sigma_i$ são ciclos independentes. Além disso, essa decomposição é única.

**Lema 7.3.** Se $\sigma = (\alpha_1 \alpha_2 \ldots \alpha_k)$ é ciclo, então $|\sigma| = k$.

**Teorema 7.3.** Seja $\sigma \in S_n$, com $\sigma = \sigma_1 \ldots \sigma_m$, onde $\sigma_i$ são ciclos independentes. Então $|\sigma| = \text{mmc}(|\sigma_1|, \ldots, |\sigma_m|)$.

**Definição 7.4.** Uma **transposição** em $S_n$ é um ciclo de ordem 2, ou seja, $(ij)$, com $i \neq j$.

**Lema 7.4.**

1. $S_n = \langle\{(ij) \mid 1 \leq i < j \leq n\}\rangle$.
2. $S_n = \langle\{(1i) \mid 2 \leq i \leq n\}\rangle$.
3. $S_n = \langle\{(i(i+1)) \mid 1 \leq i \leq n-1\}\rangle$.

**Definição 7.5.** $A_n = \{g \in S_n \mid g = \mu_1 \dots \mu_s$, com $\mu_i$ transposições e 2 divide $s\}$ é chamado **subgrupo alternado** (ou subgrupo alternativo).

**Teorema 7.4.** $A_n \lhd S_n$.

# 8 Aula 8 - Simplicidade de $A_n$

**Lema 8.1.** Sejam $f \in \mathbb{Z}[X_1, \dots, X_n]$ e $\alpha, \beta \in S_n$. Então $((\alpha\beta)f) = (\alpha(\beta f))$, onde definimos $\sigma f(X_1, \dots, X_n) = f(X_{\sigma^{-1}(1)}, \dots, X_{\sigma^{-1}(n)})$, sendo $\sigma \in S_n$.

**Lema 8.2.** Sejam $f \in \mathbb{Z}[X_1, \dots, X_n]$, com $f = \prod_{1 \leq i < j \leq n}(X_j - X_i)$, e $\sigma$ um transposição. Então $\sigma f = -f$.

**Teorema 8.1.** Seja $g \in S_n$, com $g = \mu_1 \dots \mu_s = \nu_1 \dots \nu_t$, onde $\mu_i$ e $\nu_j$ são transposições. Então $2 \mid (s - t)$, isto é, a paridade da decomposição é única.

**Definição 8.1.** Seja $g \in S_n \setminus \{1\}$ tal que $g = g_1 \dots g_m$, com $g_i$ ciclos independentes e $|g_1| \leq |g_2| \leq \dots \leq |g_m|$. Dizemos que $g$ tem **tipo de decomposição** $(|g_1|, |g_2|, \dots, |g_m|)$.

**Definição 8.2.** Seja $G$ um grupo qualquer. Dizemos que $g$ e $g'$ são **conjugados**, se existe $h \in G$ tal que $g' = hgh^{-1}$.

**Teorema 8.2.** Seja $g = (i_{11} \dots i_{1\alpha_1})(i_{21} \dots i_{2\alpha_2}) \dots (i_{m1} \dots i_{m\alpha_m}) \in S_n$.

a) Se $\sigma \in S_n$, então $\sigma g \sigma^{-1} = t$, com $t = (\sigma(i_{11}) \dots \sigma(i_{1\alpha_1})) \dots (\sigma(i_{m1}) \dots \sigma(i_{m\alpha_m}))$

b) $g, g' \in S_n \setminus \{1\}$ têm o mesmo tipo de decomposição $\Leftrightarrow$ existe $\sigma \in S_n$ tal que $g' = \sigma g \sigma^{-1}$.

c) Se $g, g' \in S_n \setminus \{1\}$ têm o mesmo tipo de decomposição e $|\operatorname{supp}(g)| \leq n - 2$, então $\sigma \in A_n$ tal que $g' = \sigma g \sigma^{-1}$.

**Definição 8.3.** $G$ é **simples**, se os únicos subgrupos normais dele são $\{1\}$ e o próprio $G$.

**Lema 8.3.**

a) $A_n = \langle\{(ijk) \mid i \neq j \neq k \neq i\}\rangle$.

b) Fixados $a \neq b$, $A_n = \langle\{(abk) \mid a \neq k \neq b\}\rangle$.

**Teorema 8.3.** Se $n \geq 5$, então $A_n$ é simples.

**Corolário 8.1.** Seja $n \geq 5$. Então

a) Se $M \lhd S_n$, então $M = \{1\}$, $M = A_n$ ou $M = S_n$.

b) $S_n' = A_n$, $A_n' = A_n$, $\mathcal{Z}(S_n) = \{1\}$ e $\mathcal{Z}(A_n) = \{1\}$.

# 9 Aula 9 - Ações e subgrupos de Sylow

**Definição 9.1.** Se $G$ é um grupo finito abeliano, então denotamos:

- produto por $+$
- elemento neutro por $0$
- $g^z$ passa a ser $zg$ e $G \times H$ vira $G \oplus H$.

**Definição 9.2.** $G(p) = \{g \in G \mid |g| \in \{p^0, p^1, p^2, \dots\}\}$

**Teorema 9.1.** Se $G \neq 0$ é grupo abeliano e finito, então $G \cong \oplus_{G(p)\neq\{0\}} G(p)$ .

**Definição 9.3.** Sejam $G$ um grupo qualquer e $X$ um conjunto. Dizemos que $G$ **age em** $X$ **a esquerda**, $X \curvearrowleft G$, se existe uma aplicação $G \times X \to X$, $(g, x) \mapsto g \cdot x$ (ou, só $gx$) tal que

- $1_G x = x, \forall\, x \in X$
- $(g_1 g_2)x = g_1(g_2 x)$

**Definição 9.4.** Se $X_1 \curvearrowleft G$ e $X_2 \curvearrowleft G$, dizemos que $f : X_1 \to X_2$ é um **morfismo**, se para todo $x \in x_1$ e todo $g \in G$, $f(gx) = gf(x)$. Se $f$ é bijetora, dizemos que $f$ é um **isomorfismo** de $G$-conjuntos.

**Definição 9.5.** Seja $X \curvearrowleft G$. Para cada $x \in X$, definimos $G_x = \{g \in G \mid gx = x\}$, chamado **estabilizador de** $x$ **em** $G$. Definimos também a $G$**-órbita de** $x$ por $Gx = \{gx \mid g \in G\}$.

**Lema 9.1.** Se $X \curvearrowleft G$ e $x \in X$, então $Gx = Gy$, para todo $y \in Gx$.

**Corolário 9.1.** Se $X \curvearrowleft G$ e $x, y \in X$, então $Gx = Gy$ ou $Gx \cap Gy = \emptyset$.

**Corolário 9.2.** Se $X \curvearrowleft G$, então $X = \bigsqcup Gx$.

**Lema 9.2.** Se $X \curvearrowleft G$ e $x \in X$, então $Gx \cong \{gGx\}_{g\in G}$.

**Corolário 9.3.** $[G : G_x] = |Gx|$.

**Proposição 9.1.** Se $G$ é grupo tal que $|G| = p^m$, com $p$ primo, então $\mathcal{Z}(G) \neq \{1\}$.

**Definição 9.6.** Seja $G$ um grupo finito. Dizemos que $P \leq G$ é um $p$**-subgrupos de Sylow**, se $|P| = p^m$ e $p^{m+1} \nmid |G|$ (note que $p^m \mid G$).

**Teorema 9.2.** Se $p$ é primo e $p \mid |G|$, então existe $p$-subgrupo de Sylow em $G$.

# 10 Aula 10 - Teorema de Sylow

**Teorema 10.1** (Teorema de Sylow)**.** Sejam $G$ um grupo finito, $p$ um primo tal que $p \mid |G|$ e $H \leq G$ tal que $|H|$ = potência de $p$.

1. Existe $P \in \mathrm{Syl}_p(G)$ tal que $H \leq P$.
2. Se $P_1, P_2 \in \mathrm{Syl}_p(G)$, então existe $g \in G$ tal que $P_1 = gP_2g^{-1}$.
3. Seja $\eta_p = |\mathrm{Syl}_p(G)|$. Então $\eta_p \equiv 1 \pmod p$ e $\eta_p \mid |G|$.

# 11 Aula 11 - Primeira Prova

Foi realizada a primeira prova.

# 12 Aula 12 - Conceitos Iniciais de Anéis

**Definição 12.1.** $R \neq \varnothing$ conjunto tal que $(R, +)$ é grupo abeliano e $(R, \cdot)$ satisfaz:

i) $a(bc) = (ab)c$

ii) $a(b + c) = ab + ac$ e $(a + b)c = ac + bc$

para todo $a, b, c \in R$ é dito **anel**. A operação $+$ é dita **adição** (ou soma) e $\cdot$, **multiplicação** (ou produto). Se $ab = ba$, para todo $a, b \in R$, então $R$ é dito **anel comutativo**. Se existe $1_R \in R$ tal que $1_R a = a1_R = a, \forall\, a \in R$, então $R$ é dito **anel com identidade**.

**Teorema 12.1.** Para todo $a, b, a_i, b_j \in R$ e todo $n \in \mathbb{Z}_{>0}$, valem:

- $0a = a0 = 0$;
- $(-a)b = a(-b) = -(ab)$;
- $(-a)(-b) = ab$;
- $(na)b = a(nb) = n(ab)$;
- $\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j$.

**Definição 12.2.** $a \in R\setminus\{0\}$ é dito **divisor de zero a esquerda** (direita), se existe $b \in R\setminus\{0\}$ tal que $ab = 0$ ($ba = 0$). Se $a$ é divisor de zero a esquerda e a direita, então $a$ é **divisor de zero**.

**Definição 12.3.** Seja $R$ é um anel com identidade $1_R$. $a$ é **invertível a esquerda** (direita), se existe $c \in R$ tal que $ca = 1_R$ ($ac = 1_R$). Se $a$ é invertível tanto a esquerda, quanto a direita, dizemos que $a$ é **unidade** (ou invertível).

**Definição 12.4.** Se $R$ é comutativo com identidade $1_R \in R \setminus \{0\}$ e não tem divisores de zero, então $R$ é um **domínio de integridade** (DI).

**Definição 12.5.** Um anel $D$ com identidade $1_D \in D \setminus \{0\}$ tal que todo $a \in D \setminus \{0\}$ é unidade é dito **anel de divisão** (AD).

**Definição 12.6.** $F$ é um **corpo** se $F$ é anel de divisão comutativo.

**Definição 12.7.** Sejam $G$ um grupo e $R$ um anel. Defina $R(G) = \{\sum_{g\in G} r_g g \mid r_g \in R\}$, denotado também por $\langle g \mid g \in G\rangle_R$. Defina a adição e a multiplicação como sendo $(\sum_{g\in G} r_g g) + (\sum_{h\in G} s_h h) = (\sum_{g\in G}(r_g + s_g)g)$ e $(\sum_{g\in G} r_g g) \cdot (\sum_{h\in G} s_h h) = \sum_{g\in G}\sum_{h\in G}(r_g s_h)(gh)$. Assim, $R(G)$ é um anel chamado de **anel de grupo de $G$ sobre $R$**.

**Definição 12.8.** Sejam $R, S$ anéis. Uma função $f : R \to S$ é um **homomorfismo** (de anéis), se para todo $a, b \in R$, $f(a + b) = f(a) + f(b)$ e $f(ab) = f(a)f(b)$.

Mono, epi, iso e automorfismo são definidas analogamente ao caso de grupo.

Definimos o núcleo de $f$ como sendo $\ker f = \{a \in R \mid f(a) = 0_S\}$ (note que são os elementos de $R$ que são levados na identidade da soma e não do produto).

**Definição 12.9.** Se existe $n \in \mathbb{Z}_{>0}$ tal que $nr = 0, \forall\, r \in R$, então a **característica de** $R$, $\text{char}(R)$, é definida como sendo o menor $n$ satisfazendo $nr = 0, \forall\, r \in R$. Se tal $n$ não existe, então definimos $\text{char}(R)$ como sendo zero.

**Teorema 12.2.** Se $R$ é anel com identidade $1_R$ e $\text{char}(R) = n > 0$, então

a) $\varphi : \mathbb{Z} \to R$, $m \mapsto mr$ é homomorfismo e $\ker \varphi = \langle n \rangle = n\mathbb{Z}$;

b) $n$ é o menor inteiro positivo tal que $n1_R = 0$;

c) se $R$ não tem divisores de zero, então $n$ é primo.

**Teorema 12.3.** Todo anel $R$ pode ser mergulhado em um anel com identidade $S$. Além disso, $S$ pode ser escolhido com $\text{char}(S) = 0$ ou $\text{char}(S) = \text{char}(R)$.

**Definição 12.10.** $\varnothing \neq S \subseteq R$ é um **subanel de** $R$, se $S$ é um anel com respeito as operações de $R$. Um subanel $I \subseteq R$ é um **ideal a esquerda** (direita), se dados $r \in R, i \in I$, $ri \in I$ ($ir \in I$). Denotamos por $I \lhd_\ell R$ ($I \lhd_r R$). Se $I$ é ideal a esquerda e a direita, dizemos que $I$ é **ideal**, denotado por $I \lhd R$.

# 13 Aula 13 - Teorema de Isomorfismo e Ideais Primos e Maximais

**Teorema 13.1.** $\varnothing \neq I \subseteq R$ é ideal a esquerda se, e somente se,

- $a - b \in I, \forall\, a, b \in I$;
- $ra \in I, \forall\, r \in R, a \in I$.

Vale também para $\lhd_r$ e $\lhd$.

**Corolário 13.1.** $\{A_i \lhd_\ell R\}_{i \in I} \Rightarrow \cap_{i \in I} A_i \lhd_\ell R$. Vale também para $\lhd_r$ e $\lhd$.

**Definição 13.1.** Seja $X \subseteq R$. Definimos $\cap\{A_i \mid A_i \lhd_\ell, X \subseteq A_i\}$ é o **ideal a esquerda gerado por** $X$. Vale também para $\lhd_r$ e $\lhd$.

Observações:

1. O ideal bilateral gerado por $X$ é denotado por $(X)$.
2. Se $X = \{x\}$, então $(X) = (x)$ e é chamado **ideal principal gerado por** $x$.
3. $R$ é chamado **anel de ideal principal**, se todo ideal de $R$ é principal. Se $R$ for um domínio, então dizemos **domínio de ideal principal**.

**Teorema 13.2.** Se $X \subseteq R$ e $a \in R$, então

1. $(a) = \{ra + as + na + \sum_{i=1}^{m} r_i a s_i \mid r, s, r_i, s_i \in R, n \in \mathbb{Z}\}$.
2. Se $1_R \in R$, então $(a) = \{\sum_{i=1}^{m} r_i a s_i \mid r_i, s_i \in R\}$.
3. Se $a \in C(R)$, então $(a) = \{ra + na \mid r \in R, n \in \mathbb{Z}\}$.
4. $Ra = \{ra \mid r \in R\}$ é ideal a esquerda e $aR = \{ar \mid r \in R\}$ é ideal a direita.
5. Se $1_R \in R$ e $ar = ra$, então $aR = Ra$.
6. Se $1_R \in R$ e $xr = rx$, para todo $x \in X$ e $r \in R$, então $(X) = \{\sum_{i=1}^{m} r_i x_i \mid r_i \in R, x_i \in X\}$

**Definição 13.2.** Sejam $A, A_1, \ldots, A_n, B \subseteq R$. Então

1. $A_1 + \cdots + A_n = \{\sum a_i \mid a_i \in A_i\}$.
2. $AB = \{\sum ab \mid a \in A, b \in B\}$.
3. Se $A$ (ou $B$) é fechado com relação a soma e $B = \{b\}$ (ou $A = \{a\}$), então $AB = Ab = \{ab \mid a \in A\}$ (ou $AB = aB = \{ab \mid b \in B\}$).
4. $A_1 \ldots A_n = \{\sum a_1 \ldots a_n \mid a_i \in A_i\}$.

**Teorema 13.3.** ${}^{R}\!/_{I}$ é anel com multiplicação $(a + I)(b + I) = ab + I$, para todo $a, b \in R$.

**Teorema 13.4.** Se $f : R \to S$ é homomorfismo, então $\ker f \lhd R$. Além disso, se $I \lhd R$, então $I = \ker \pi$, onde $\pi : R \to {}^{R}\!/_{I}$, $r \mapsto r + I$.

**Teorema 13.5.** Se $f : R \to S$ é homomorfismo, então ${}^{R}\!/_{\ker f} \cong \operatorname{Im} f$.

**Teorema 13.6.** Sejam $I, J \lhd R$. Então

- ${}^{(I+J)}\!/_{J} \cong {}^{I}\!/_{I \cap J}$
- Se $I \subseteq J$, então ${}^{J}\!/_{I} \lhd {}^{R}\!/_{I}$ e ${}^{R}\!/_{J} \cong {}^{R}\!/_{I}\big/{}_{J}\!/_{I}$.

**Teorema 13.7.** Se $I \lhd R$, então existe uma bijeção entre $\{J \lhd R \text{ tal que } I \subseteq J\}$ e $\{K \lhd {}^{R}\!/_{I}\}$, fazendo $J \mapsto \pi(J)$ e $\pi^{-1}(K) \hookleftarrow K$.

**Definição 13.3.** Um ideal $P \lhd R$ é **primo**, se $P \neq R$ e se dados $A, B \lhd R$ tais que $AB \subseteq P$, então $A \subseteq P$ ou $B \subseteq P$.

**Teorema 13.8.**

1. Se $P \lhd R$ e $P \neq R$ é tal que para todo $a, b \in R$, temos que $a \in P$ ou $b \in P$, sempre que $ab \in P$, então $P$ é primo.
2. Se $P$ é primo e $R$ é comutativo, então $a \in P$ ou $b \in P$, sempre que $ab \in P$.

**Teorema 13.9.** Seja $R$ comutativo com $1_R \in R$. Então $P$ é primo se, e somente se, ${}^{R}\!/_{P}$ é domínio.

**Definição 13.4.** $M \lhd R$ é **maximal**, se $M \neq R$ e se $M \lhd I \lhd R$, então $I = M$ ou $I = R$.

**Teorema 13.10.** Se $R \neq 0$ e $1_R \in R$, então todo ideal $I$ de $R$ está contido em um ideal maximal de $R$.

**Corolário 13.2.** Se $R \neq 0$ e $1_R \in R$, então $R$ admite um ideal maximal.

**Teorema 13.11.** Seja $R$ comutativo tal que $R^2 = R$. Então se $M \lhd R$ é maximal, então $M$ é primo.

**Corolário 13.3.** Seja $R$ comutativo tal que $1_R \in R$. Então se $M \lhd R$ é maximal, então $M$ é primo.

**Teorema 13.12.** Seja $M \lhd R$ e $1_R \in R$.

1. $R$ comutativo e $M$ maximal $\Rightarrow$ ${}^{R}\!/_{M}$ é corpo.

2. $R/M$ anel de divisão $\Rightarrow$ $M$ é maximal.

**Corolário 13.4.** Seja $R$ comutativo tal que $1_R \in R$. Então são equivalentes:

1. $R$ é corpo.
2. $R$ não possui ideais não triviais.
3. (0) é ideal maximal.
4. Se $\varphi : R \to S$ é homomorfismo não nulo, então $\varphi$ é monomorfismo.

**Definição 13.5.** Se $\{R_i\}_{i\in I}$ é família não vazia de anéis, então $\prod_{i\in I} R_i = \{(r_i)_{r_i\in R_i}\}$ é anel soma e produto definidos coordenada a coordenada através das operações dos anéis $R_i$.

**Teorema 13.13.** Seja $A_1, \ldots, A_n \lhd R$ tais que:

- $A_1 + \cdots + A_n = R$
- $A_i \cap (A_1 + \cdots + A_{i-1} + A_{i+1} + \cdots + A_n) = 0$

Então $R \cong A_1 \times \cdots \times A_n = \prod_{i=1}^n A_i$.

# 14 Aula 14 - Fatoração em Anéis Comutativos

**Teorema 14.1** (Teorema do Resto Chinês)**.** Sejam $A_1, \ldots, A_n \lhd R$ tais que $R^2 + A_i = R$, $\forall\, i = 1.\ldots, n$, e $A_i + A_j = R$, $\forall\, i \neq j$. Se $b_1, \ldots, b_n \in R$, então $\exists\, b \in R$ tal que $b \equiv b_i \,(\mathrm{mod}\ A_i)$, $\forall\, i = 1.\ldots, n$. Também $b$ é único $(\mathrm{mod} \cap_{i=1}^n) A_i$, isto é, se $c \equiv b_i \,(\mathrm{mod}\, A_i)$, $\forall\, i = 1.\ldots, n$, então $c \equiv b \,(\mathrm{mod}\ \cap_{i=1}^n A_i)$.

**Corolário 14.1.** Se $A_1, \ldots, A_n \lhd R$, então existe monomorfismo $\theta : R/\cap_{i=1}^n A_i \to R/A_1 \times \cdots \times R/A_n$, $r + \cap_{i=1}^n A_i \mapsto (r + A_1, \ldots, r + A_n)$. Além disso, se $R^2 + A_i = R$, $\forall\, i$ e $A_i + A_j = R$, $\forall\, i \neq j$, então $\theta$ é isomorfismo.

**Definição 14.1.**

1. $a \in R$ **divide** $b \in R$, se $b = ax$, para algum $x \in R$. Notação: $a \mid b$. Se $a \mid b$ e $b \mid a$, então $a$ e $b$ são **associados**.
2. Se $1_R \in R$, então $c \in R$ é **irredutível**, se
   i) $c \neq 0$ e $c$ não é unidade;
   ii) $c = ab \Rightarrow a$ unidade ou $b$ unidade.
3. Se $p \in R$ é **primo**, se
   i) $p$ não é unidade;
   ii) $p \mid ab \Rightarrow p \mid a$ ou $p \mid b$.

**Teorema 14.2.** Sejam $R$ um domínio integral e $p, c \in R$. Então:

1. $p$ é primo $\Leftrightarrow$ $(p) \lhd_{\text{primo}} R$;
2. $c$ é irredutível $\Leftrightarrow$ $(c)$ é maximal em $S = \{(r) \lhd R \mid (r) \neq R\}$, isto é, se $(c) \subseteq (r)$, então $(c) = (r)$;
3. primo $\Rightarrow$ irredutível;

4. se $R$ é domínio de ideal principal, então $p$ primo $\Leftrightarrow$ $p$ irredutível;

5. associado de primo é primo e associado de irredutível é irredutível;

6. $c$ irredutível e $a \mid c \Rightarrow a$ e $c$ são associados.

**Definição 14.2.** Seja $R$ um domínio integral. Dizemos que ele é um **domínio de fatoração única** (DFU), se:

i) $\forall\, a \in R \setminus \{0\}$ não unidade, temos que $a = c_1 \dots c_n$, com $c_i$ irredutível, $\forall\, i$.

ii) se $a = c_1 \dots c_n$ e $a = d_1 \dots d_m$, então $n = m$ e existe $\sigma \in S_n$ tal que $c_i$ e $d_{\sigma(i)}$ são associados, $\forall\, i$.

**Lema 14.1.** Se $R$ é anel de ideal principal e $(a_1) \subseteq (a_2) \subseteq \dots$ uma cadeia, então $\exists\, n \in \mathbb{Z}_{>0}$ tal que $(a_i) = (a_n)$, $\forall\, i \geq n$.

**Teorema 14.3.** Todo DIP é DFU.

**Definição 14.3.** $R$ comutativo é um **anel euclidiano**, se existe uma função $\varphi : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ tal que:

- $\forall\, a, b \in R$, com $ab \neq 0$, temos $\varphi(a) \leq \varphi(ab)$;

- $\forall\, a, b \in R$, $\exists\, q, r \in R$ tal que $a = qb + r$, onde $r = 0$ ou $\varphi(r) < \varphi(b)$.

**Teorema 14.4.** Se $R$ é anel euclidiano, então $R$ é anel de ideal principal com $1_r \in R$. Em particular, se $R$ é domínio euclidiano, então $R$ é DFU.

# 15 Aula 15 - Anel de Polinômios

Para anéis de polinômios, vamos sempre considerar $1_R \in R$.

**Definição 15.1.** Seja $\varnothing \neq X \subseteq R$ (R comutativo). Dizemos que $d \in R$ é **máximo divisor comum** de $X$, se

a) $d \mid x, \forall\, x \in X$;

b) se $c \mid x, \forall\, x \in X$, então $c$ e $d$ são associados.

**Definição 15.2.** Se $1_R$ é o mdc de $X$, então os elementos de $X$ são ditos **relativamente primos**.

**Teorema 15.1.** Sejam $a_1, a_2, \dots, a_n \in R$, onde $1_r \in R$.

1. $d = \text{mdc}(a_1, \dots, a_n) = r_1 a_1 + \dots + r_n a_n \Leftrightarrow (d) = (a_1) + \dots + (a_n)$.

2. Se $R$ é anel de ideal principal, então $\text{mdc}(a_1, \dots, a_n)$ existe e é da forma $r_1 a_1 + \dots + r_n a_n$.

3. Se $R$ é domínio de fatoração única, então $\text{mdc}(a_1, \dots, a_n)$ existe.

**Definição 15.3.** Se $R \subseteq S$ são anéis, então $x \in S$ é uma **indeterminada** sobre $R$, se $\forall\, n > 0$ $a_0 + a_1 x + \dots + a_n x_n = 0 \Leftrightarrow a_i = 0, \forall\, i$, com $a_i \in R$.

**Lema 15.1.** Dado um anel $R$ existe um anel $S$ satisfazendo:

a) $R \subseteq S$ é subanel;

b) $\exists\, x \in S$ indeterminada sobre $R$;

c) $xr = rx, \forall\, r \in R$.

**Definição 15.4.** Sejam $R \subseteq S$ como lema. Então $R[x] = \{a_0 + a_1x + \cdots + a_nx^n \mid n \geq 0, a_i \in R\}$ é subanel de $S$, chamado **anel de polinômio** sobre $R$. Em particular, $f(x) \in R[x] \Rightarrow f(x) = \sum_{i=0}^{n} a_i x^i$.

**Definição 15.5.** Seja $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$. Então

1. Se $a_n \neq 0$, então o **grau de** $f(x)$ é $\deg(f(x)) = n$.
2. $a_n$ é o **coeficiente líder** de $f(x)$.
3. $a_0$ é o **coeficiente constante** de $f(x)$.
4. Se $a_n = 1_R$, então $f(x)$ é **mônico**.

**Lema 15.2.** Sejam $f(x), g(x) \in R[x]$.

a) $\deg\big(f(x) + g(x)\big) \leq \max\Big(\deg\big(f(x)\big), \deg\big(g(x)\big)\Big)$

b) $\deg\big(f(x)g(x)\big) \leq \deg\big(f(x)\big) + \deg\big(g(x)\big)$

c) Se $R$ é domínio, então $\deg\big(f(x)g(x)\big) = \deg\big(f(x)\big) + \deg\big(g(x)\big)$

d) Se $R$ é domínio, então $R[x]$ é domínio

e) Se $R$ é domínio, então as unidades de $R[x]$ são as unidades de $R$

f) Se o coeficiente líder de $f(x)$ ou $g(x)$ é unidade, então $f(x)g(x) \neq 0$ e $\deg\big(f(x)g(x)\big) = \deg\big(f(x)\big) + \deg\big(g(x)\big)$.

**Teorema 15.2** (Algoritmo da Divisão)**.** Sejam $f(x), g(x) \in R[x]$, com $f(x) \neq 0$. Suponha que o coeficiente líder de $f(x)$ seja unidade em $R$. Então existem únicos $q(x), r(x) \in R[x]$ tais que $g(x) = q(x)f(x) + r(x)$, com $r(x) = 0$ ou $\deg\big(r(x)\big) < \deg\big(f(x)\big)$.

**Corolário 15.1.** Se $F$ é corpo, então $F[x]$ é domínio euclidiano (com função euclidiana igual a deg). Em particular, $F[x]$ é DFU.

**Teorema 15.3.** Seja $f(x) \in R[x]$. Então $\forall\, a \in R$, o resto da divisão de $f(x)$ por $(x - a)$ é $f(a)$.

**Definição 15.6.** $a \in R$ é **raiz** de $f(x) \in R[x]$, se $f(a) = 0$.

**Teorema 15.4.** Seja $f(x) \in R[x]$. $a \in R$ é raiz de $f(x) \Leftrightarrow (x - a) \mid f(x)$.

**Definição 15.7.** Seja $a \in R$. Dizemos que $a$ tem **multiplicidade** $m \geq 0$ como raiz de $f(x)$, se $f(x) = (x - a)^m q(x)$ e $q(a) \neq 0$.

**Teorema 15.5.** Seja $R$ domínio integral e $f(x) \in R[x]$. Se $\deg\big(f(x)\big) = n$, então $f(x)$ possui, no máximo, $n$ raízes distintas.

**Teorema 15.6.** Seja $R$ domínio integral. Defina $X = \{(r, u) \mid r, u \in R,\ u \neq 0\}$ com a relação de equivalência $(r, u) \equiv (s, v) \Leftrightarrow rv = su$. Defina por $r/u$ a classe de equivalência de $(r, u)$ e considere $Q = \{r/u \mid r, u \in R,\ u \neq 0\}$. Defina $r/u + s/v = (rv + su)/uv$ e $r/u \cdot s/v = rs/uv$. Então $(Q, +, \cdot)$ é corpo.

# 16 Aula 16 - Lema de Gauss

**Proposição 16.1.** Sejam $D$ DFU, $F$ o corpo de frações de $D$ e $f(x) = \sum_{i=0}^{n} a_i x^i \in D[x]$. Se $u = \frac{c}{d} \in F$, $(c, d) = 1_D$ e $f(u) = 0$, então $c \mid a_0$ e $d \mid a_n$.

**Definição 16.1.** Sejam $D$ domínio integral e $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in D[x]$. A **derivada formal** de $f(x)$ é o polinômio $f'(x) = a_1 x + 2a_2 x + \cdots + n a_n x^{n-1}$.

**Lema 16.1.** Se $c \in D$, então:

a) $(cf(x))' = cf'(x)$;

b) $(f(x) + g(x))' = f'(x) + g'(x)$;

c) $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$;

d) $(f^n(x))' = nf^{n-1}(x)f'(x)$.

**Teorema 16.1.** Sejam $D \subseteq E$ domínios integrais, $f(x) \in d[x]$ e $c \in E$.

1. $c$ é raiz com multiplicidade maior do que 1 $\Leftrightarrow$ $f(c) = 0$ e $f'(c) = 0$;
2. Se $D$ é corpo e $(f(x), f'(x)) = 1_{D[x]}$, então $f(x)$ não possui raiz com multiplicidade maior do que 1 em $E$;
3. Se $D$ é corpo, $f(x)$ é irredutível em $D[x]$ e $E$ contém uma raiz de $f(x)$, então $f(x)$ não possui raízes com multiplicidade maior do que 1 em $E$ $\Leftrightarrow$ $f'(x) = 0$.

**Definição 16.2.** Seja $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in D[x]$. O **conteúdo** de $f(x)$, denotado por $\text{cont}(f(x))$, é qualquer $\text{mdc}(a_0, \ldots, a_n)$.

**Definição 16.3.** Se $\text{cont}(f(x))$ é unidade em $D$, dizemos que $f(x)$ é **primitivo**.

**Lema 16.2** (Lema de Gauss)**.** Se $D$ é DFU e $f(x), g(x) \in D[x]$, então $\text{cont}(f(x)g(x)) = \text{cont}(f(x))\,\text{cont}(g(x))$. Em particular, se $f(x)$ e $g(x)$ são primitivos, então $f(x)g(x)$ é primitivo.

**Lema 16.3.** Sejam $D$ DFU, $F$ corpo de frações de $D$ e $f(x), g(x) \in D[x]$ primitivos. Então $f(x)$ e $g(x)$ são associados em $D[x]$ $\Leftrightarrow$ $f(x)$ e $g(x)$ são associados em $F[x]$.

**Teorema 16.2.** Sejam $D$ DFU, $F$ corpo de frações de $D$ e $f(x) \in D[x]$ primitivo, com $\deg(f(x)) > 0$. Então $f(x)$ é irredutível em $D[x]$ $\Leftrightarrow$ $f(x)$ é irredutível em $F[x]$.

**Teorema 16.3.** $D$ é DFU $\Rightarrow$ $D[x]$ é DFU.

# 17 Aula 17 - R-módulos Noetheriano

**Definição 17.1.** Um grupo abeliano $(M, +)$ é um $R$**-módulo à esquerda**, se existe uma ação de $R$ em $M$, $R \times M \to M$, $(r, m) \mapsto rm$ tal que $\forall\, m, n \in M$ e $\forall\, r, s \in R$, vale

i) $r(m + n) = rm + rn$

ii) $(r + s)m = rm + sm$

iii) $r(sx) = (rs)x$

iv) $1_r m = m$

**Definição 17.2.** Sejam $M, N$ $R$-módulos. Dizemos que $f : M \to N$ é **homomorfismo de $R$-módulos**, se $f$ é homomorfismo de grupos abelianos e $f(rm) = rf(m)$, $\forall\, r \in R, m \in M$.

**Definição 17.3.** Seja $N$ um subgrupo de $M$ tal que $R$ age em $N$ via restrição. Chamamos $N$ de **submódulo de** $M$. Notação: $N \leq M$ (ou $M \geq N$).

**Definição 17.4.** Sejam $N \leq M$. Sabemos que $M/N$ é grupo abeliano. Defina $M/N$ como $R$-módulo, fazendo a ação ser $r(m + N) = rm + N$, para todo $m \in M$.

**Proposição 17.1.** Sejam $N \leq M$. Qualquer homomorfismo $f : M \to L$ tal que $N \subseteq \ker(f)$ induz homomorfismo $\overline{f} : M/N \to L$, $m + N \mapsto f(m)$. Além disso,

- $\overline{f}$ é epimorfismo $\Leftrightarrow$ $f$ é epimorfismo.
- $\overline{f}$ é monomorfismo $\Leftrightarrow$ $N = \ker(f)$.

**Teorema 17.1** (Isomorfismo)**.** Se $f : M \to N$ é homomorfismo, então $f(M) \cong M/\ker(f)$ (iso de $R$-módulos).

**Proposição 17.2** (Correspondência)**.** Existe bijeção $\{N \leq K \leq M\} \leftrightarrow \{L \leq M/N\}$.

**Definição 17.5.** $N \leq M$ é **maximal** (próprio), se $N \neq M$ e $N \leq L \leq M \Rightarrow L = M$ ou $L = M$. Se $M \neq \{0\}$ não possui submódulos próprios não nulos, dizemos que $M$ é **simples**.

**Lema 17.1.** $N \leq M$ é maximal $\Leftrightarrow$ $M/N$ é simples.

**Definição 17.6.** Seja $\{M_i\}_{i \in I}$ uma família de $R$-módulos. O **produto direto** de $M_i$, denotado por $\prod_{i \in I} M_i = \{(a_i)_{i \in I} \mid a_i \in M_i\}$ é um $R$-módulo com $(a_i)_{i \in I} + (b_i)_{i \in I} = (a_i + b_i)_{i \in I}$ e $r(a_i)_{i \in I} = (ra_i)_{i \in I}$. A **soma direta** (externa) de $M_i$, denotada por $\oplus_{i \in I} M_i$ é o submódulo de $\prod_{i \in I} M_i$, cujos elementos são da forma $(a_i)_{i \in I}$, com $a_i \neq 0$, somente para finitos índices.

**Definição 17.7.** Dizemos que $M$ satisfaz a **condição de cadeia ascendente (descendente)**, CCA (CCD), se toda cadeia ascendente (descendente) de submódulos estabiliza, isto é, se $M_1 \leq M_2 \leq M_3 \leq \dots$ ($M_1 \geq M_2 \geq M_3 \geq \dots$) é cadeia de submódulos, então existe $n > 0$ tal que $M_n = M_{n+1} = \dots$.

**Proposição 17.3** (Noeth)**.** As seguintes condições são equivalentes:

1. $M$ satisfaz CCA.
2. toda família não vazia de submódulos de $M$ admite elemento maximal (com relação a inclusão).

**Proposição 17.4** (Artin)**.** As seguintes condições são equivalentes:

1. $M$ satisfaz CCD.
2. toda família não vazia de submódulos de $M$ admite elemento simples (com relação a inclusão).

**Definição 17.8.** Um $R$-módulo satisfazendo uma das condições da proposição de Noeth (Artin) é chamado **noetheriano** (**artiniano**).

**Definição 17.9.**

1. Se $N_1, N_2 \leq M$, então $N_1 + N_2 = \{x + y \mid x \in N_1, y \in N_2\}$ é submódulo.

2. Seja $S \subseteq M$. Dizemos que $S$ **gera** $M$ se todo elemento $x \in M$ é da forma $\sum_{i=1}^{n} r_i x_i$, $r_i \in R, x_i \in S$. Se $S$ é finito e gera $M$, então $M$ é **finitamente gerado**. $M$ é **cíclico** se é gerado por um só elemento.

**Proposição 17.5.** $M$ é noetheriano $\Leftrightarrow$ todo submódulo de $M$ é finitamente gerado.

**Definição 17.10.** Um anel $R$ é **noetheriano** (**artiniano**) à esquerda se $R$ é noetheriano (artiniano) como $R$-módulo à esquerda ($R \times R \to R, (r, s) \mapsto rs$).

**Proposição 17.6.** Sejam $N \leq M$. Então $M$ é noetheriano (artiniano) $\Leftrightarrow$ $N$ e $M/N$ são noetheriano (artiniano).

# 18 Aula 18 - Base de Hilbert

**Corolário 18.1.** Se $M_1, \ldots, M_n$ são noetherianos (artinianos), então $M_1 \oplus \cdots \oplus M_n$ é noetheriano (artiniano).

**Definição 18.1.** Uma **série de comprimento** $n$ **de** $M$ é uma sequência de submódulos $M = M_0 \supsetneqq M_1 \supsetneqq M_2 \supsetneqq \cdots \supsetneqq M_{n-1} \supsetneqq M_n = 0$. Uma série de comprimento $n$ é uma **série de composição** se os fatores $M_i/M_{i+1}$ são simples, $\forall\, i = 0, \ldots, n-1$. Duas séries são equivalentes se elas têm o mesmo comprimento e os fatores são isomorfos a menos de reordenação.

**Teorema 18.1** (Jordan-Hölder)**.** Se um módulo $M$ admite uma série de composição, então quaisquer duas séries de composição são equivalentes. Além disso, qualquer cadeia de submódulos pode ser refinada para uma série de composição.

**Teorema 18.2.** Um módulo $M$ admite uma série de composição $\Leftrightarrow$ $M$ é noetheriano e artiniano.

**Teorema 18.3** (Base de Hilbert)**.** Se $R$ é noetheriano, então $R[x_1, \ldots, x_n]$ é noetheriano.

**Definição 18.2.** $f : M \times N \to L$ é $R$**-bilinear** se:

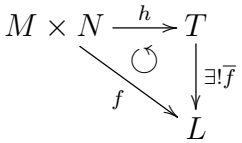
i) $f(x + x', y) = f(x, y) + f(x', y)$

ii) $f(x, y + y') = f(x, y) + f(x, y')$

iii) $f(rx, y) = f(x, ry) = rf(x, y)$

para todo $x, x' \in M, y, y' \in N, r \in R$.

**Definição 18.3.** O **produto tensorial de** $M$ **e** $N$ é um $R$-módulo $T$ unido de uma aplicação $R$-bilinear $h : M \times N \to T$ satisfazendo a seguinte propriedade universal: se $L$ é um $R$-módulo e $f : M \times N \to L$ é $R$-bilinear, então $\exists! \overline{f} : T \to L$ $R$-homomorfismo tal que $f = \overline{f} \circ h$, ou seja, tal que o diagrama abaixo comuta.




**Lema 18.1.** Se o produto tensorial existe, então ele é único a menos de isomorfismo.

# 19 Aula 19 - Propriedades do produto tensorial

**Definição 19.1.** Seja $X$ um conjunto. O $R$**-módulo livre com base** $X$ é $F = \{\varphi : X \to R \mid \varphi(x) \neq 0 \text{ para finitos } x \in X\}$, onde $(\varphi_1 + \varphi_2)(x) = \varphi_1(x) + \varphi_2(x)$ e $(r\varphi)(x) = r\varphi(x)$, $\forall\, \varphi_1, \varphi_2 \in F, x \in X, r \in R$. Pensamos nos elementos como $R$-combinações lineares finitas de elementos de $X$.

$$\varphi \in F \leftrightarrow \sum_{x \in X} \varphi(x)x$$

**Teorema 19.1.** Sejam $M$ e $N$ $R$-módulos. Considere o $R$-módulo livre $F$ com base $M \times N$ e tome $G$ o submódulo de $F$ gerado pelos elementos da forma $(x + x', y) - (x, y) - (x', y)$, $(x, y+y') - (x, y) - (x, y')$, $(rx, y) - r(x, y)$ e $(x, ry) - r(x, y)$, para todo $x, x' \in M, y, y' \in N, y \in N$. Defina $M \otimes N = {}^{F}\!/_{G}$ e denote $(x, y) + G = x \otimes y$, para todo $x \in M, y \in N$. Então o $R$-módulo $M \otimes N$ junto com o mapa $f : M \times N \to M \otimes N, (x, y) \mapsto x \otimes y$ é o produto tensorial de $M$ e $N$.

**Definição 19.2.** Os elementos do produto tensorial são chamados tensores e os tensores da forma $x \otimes y$ são chamados tensores simples.

**Proposição 19.1.** $M \otimes N \cong N \otimes M$.

**Proposição 19.2.** $(M \otimes N) \otimes L \cong M \otimes (N \otimes L)$.

**Proposição 19.3.** $M \otimes (N \oplus L) \cong (M \otimes N) \oplus (M \otimes L)$.

**Proposição 19.4.** $R \otimes_R M \cong M$.

# 20 Aula 20 - Conceitos Iniciais de Extensão de Corpos

**Proposição 20.1.** Se $M$ é gerado por um conjunto $X$ e $N$ é gerado por um conjunto $Y$, então $M \otimes N$ é gerado por $\{x \otimes y \mid x \in X, y \in Y\}$.

**Proposição 20.2.** Se $M, N$ são $R$-módulos livres com base $X$ e $Y$, respectivamente, então $M \otimes N$ é $R$-módulo livre com base $\{x \otimes y \mid x \in X, y \in Y\}$.

**Corolário 20.1.** Se $V$ e $W$ são espaços vetoriais finitos sobre um corpo $K$, então $V \otimes W$ também é dimensão finita e $\dim(V \otimes W) = \dim(V)\dim(W)$.

**Corolário 20.2.** $R^m \otimes_R R^n \cong R^{mn}$.

**Definição 20.1.** Suponha $f_1 : M_1 \to N_1$ e $f_2 : M_2 \to N_2$ homomorfismo. Defina $M_1 \times M_2 \to N_1 \otimes N_2, (x, y) \mapsto f_1(x) \otimes f_2(y)$ que é $R$-bilinear. Então $\exists!$ homomorfismo $f : M_1 \otimes M_2 \to N_1 \otimes N_2, x \otimes y \mapsto f_1(x) \otimes f_2(y)$. Então $f$ é dito **produto tensorial de** $f_1$ **e** $f_2$ e é denotado por $f_1 \otimes f_2$.

**Definição 20.2.** Suponha (por facilidade que):

- $M$ é $R$-módulo com base $w_1, w_2$;
- $N$ é $R$-módulo com base $x_1, x_2$;
- $P$ é $R$-módulo com base $y_1, y_2$;
- $Q$ é $R$-módulo com base $z_1, z_2$;

Considere $f : M \to N$, $g : P \to Q$ homomorfismos com matrizes $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ e $B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$, respectivamente (nas bases fixadas). Então $f \otimes g : M \otimes P \to N \otimes Q$ tem matriz $\begin{pmatrix} a_{11}B & a_{12}B \\ a_{21}B & a_{22}B \end{pmatrix}$ na base $\{w_1 \otimes y_1, w_1 \otimes y_2, w_2 \otimes y_1, w_2 \otimes y_2\}$. Essa matriz, denotada por $A \otimes B$ é chamada **produto de Kronecker** das matrizes $A$ e $B$.

**Definição 20.3.** Sejam $F, K$ corpos. $K$ é uma **extensão de** $F$, se $F \subseteq K$ é subcorpo.

**Definição 20.4.** Seja $K \supseteq F$ extensão de corpo. O **grau de** $K$ **sobre** $F$ é definido por $[K : F] = \dim_F K$. Dizemos que $K \supseteq F$ é extensão finita de $F$, se $[K : F] < \infty$.

**Teorema 20.1.** Sejam $L \supseteq K \supseteq F$ tais que $[L : K] < \infty$ e $[K : F] < \infty$. Então $[L : F] = [L : K][K : F]$.

**Corolário 20.3.** Se $L \supseteq K \supseteq F$ são extensões finitas, então $[L : K] \mid [L : F]$ e $[K : F] \mid [L : F]$.

**Definição 20.5.** $a \in K$ é **algébrico** sobre $F$, se existe $f(x) \in F[x]$ não nulo tal que $f(a) = 0$.

**Teorema 20.2.** $a \in K$ é algébrico se, e somente se, $F(a)$ é uma extensão finita de $F$.

**Definição 20.6.** $a$ é **algébrico de grau** $n$ **sobre** $F$, se o polinômio mônico de grau mínimo que se anula em $a$ em $F[x]$ tem grau $n$.

**Corolário 20.4.** Se $a \in K$ é algébrico de grau $n$ sobre $F$, então $[F(a) : F] = n$.

**Teorema 20.3.** $L = \{a \in K \mid a \text{ é algébrico sobre } F\}$ é subcorpo de $K$.

# 21 Aula 21 - Corpo de fatoração

**Corolário 21.1.** Se $a, b \in K$ são algébricos (em $F$) de grau $n$ e $m$, respectivamente, então $a + b$, $ab$, $\frac{a}{b} (b \neq 0)$ são algébricos com grau menor do que ou igual a $mn$.

**Definição 21.1.** Uma extensão $K \supseteq F$ é uma **extensão algébrica** se todo $a \in K$ é algébrico sobre $F$.

**Teorema 21.1.** Se $L \supseteq K$ é algébrica, $K \supseteq F$ é algébrica, então $L \supseteq F$ é algébrica.

**Teorema 21.2.** Se $p(x) \in F[x]$ é irredutível e $\deg(p(x)) = n \geq 1$, então existe extensão $E$ de $F$ tal que $[E : F] = n$ e $p(x)$ admite raiz.

**Corolário 21.2.** Se $f(x) \in F[x]$, então existe extensão finita $E \supseteq F$ com uma raiz de $f(x)$ e, além disso, $[E : F] \leq \deg(f(x))$.

**Teorema 21.3.** Seja $f(x) \in F[x]$ com $\deg(f(x)) = n \geq 1$. Então existe extensão $E \supseteq F$ com $[E : F] \leq n!$ onde vivem todas as raízes de $f(x)$.

**Definição 21.2.** Seja $f(x) \in F[x]$. Uma extensão finita $E \supseteq F$ com grau mínimo tal que $f(x)$ se fatora como produto de fatores lineares em $E[x]$ é chamada de um **corpo de fatoração de** $f(x)$.

Suponha $F \cong_\tau F'$ e denote $\tau(\alpha) = \alpha'$, $\forall\, \alpha \in F$. Isso induz um isomorfismo $F[x] \cong_\tau F'[t]$, onde $\tau(f(x)) = \tau(a_0 + a_1x + \cdots + a_nx^n) = a_0' + a_1't + \cdots + a_n't^n = f'(t)$. Note que fatoração de $f(x) \Leftrightarrow$ fatoração de $f'(t)$; em particular, $f(x)$ irredutível $\Leftrightarrow$ $f'(t)$ irredutível. Como $\tau(f(x)) = f'(t)$, então $\tau((f(x))) = (f'(t))$. Daí, $\tau$ também induz isomorfismo ${}^{F[x]}\!/_{(f(x))} \cong_\tau {}^{F'[t]}\!/_{(f'(t))}$, onde $g(x) + (f(x)) \mapsto g'(t) + (g'(t))$; em particular $x + (f(x)) \mapsto t + (f'(t))$ e $\alpha + (f(x)) \mapsto \alpha + (f'(t))$. Observe que $F \hookrightarrow F[x]$, logo $F \hookrightarrow {}^{F[x]}\!/_{(f(x))}$, portanto, $\tau(\alpha) = \alpha'$ em ${}^{F[x]}\!/_{(f(x))}$, $\forall\, \alpha \in F$.

**Teorema 21.4.** Se $p(x)$ é irredutível em $F[x]$ e $v$ é uma raiz de $p(x)$, então $F(v) \cong F'(w)$, onde $w$ é uma raiz de $f'(t)$. Além disso, tal isomorfismo pode ser escolhido de modo que $\tau(\alpha) = \alpha'$, $\forall\, \alpha \in F$ e $\tau(v) = w$.

**Corolário 21.3.** Se $p(x) \in F[x]$ é irredutível e $a, b$ são duas raízes quaisquer de $p(x)$, então $F(a) \cong F(b)$ por um isomorfismo que leva $a$ em $b$ e deixa fixo os elementos de $F$.

**Teorema 21.5.** Sejam $E$ e $E'$ corpos de fatoração de $f(x) \in F[x]$ e $f'(t) \in F'[t]$. Então $E \cong_\phi E'$, onde $\phi(\alpha) = \alpha'$, $\forall\, \alpha \in F$. Em particular, quaisquer corpos de fatoração de $f(x)$ são isomorfos por isomorfismo que deixa os elementos de $F$ fixados.

# 22 Aula 22 - Corpo fixado

De agora em diante, todo corpo tem característica 0.

**Definição 22.1.** $K \supseteq F$ é uma **extensão simples de** $F$ se $K = F(\alpha)$ para algum $\alpha \in K$.

**Teorema 22.1.** Se $a, b$ são algébricos sobre $F$, então existe $c \in F(a, b)$ tal que $F(c) = F(a, b)$.

**Corolário 22.1.** Se $\alpha_1, \ldots, \alpha_n$ são algébricos sobre $F$, então existe $c \in F(\alpha_1, \ldots, \alpha_n)$ tal que $F(\alpha_1, \ldots, \alpha_n) = F(c)$. Em particular, qualquer extensão finita é simples.

**Teorema 22.2.** Se $\sigma_1, \ldots, \sigma_n \in \mathrm{Aut}(K)$, com $\sigma_i \neq \sigma_j$, se $i \neq j$, então $\nexists\, a_1, \ldots, a_n \in K$ não todos nulos tais que $a_1\sigma_1 + \cdots + a_n\sigma_n = 0$ (isto é, $a_1\sigma_1(u) + \cdots + a_n\sigma_n(u) = 0$, para todo $u \in K$).

**Definição 22.2.** Seja $G \leq \mathrm{Aut}(K)$. O **corpo fixado por** $G$ é $\{a \in K \mid \sigma(a) = a, \forall\, \sigma \in G\}$.

**Definição 22.3.** Seja $K \supseteq F$. Então $G(K : F) = \{\sigma \in \mathrm{Aut}(K) \mid \sigma(a) = a, \forall\, a \in F\}$.

**Teorema 22.3.** Seja $K \supseteq F$ extensão finita. Então $|G(K : F)| \leq [K : F]$.

# 23 Aula 23 - Segunda prova

Foi realizada a segunda prova.

# 24 Aula 24 - Funções Racionais Simétricas

**Definição 24.1.** O subcorpo $S$ de $F(x_1, \ldots, x_n)$ que é fixado pelos elementos de $S_n$, isto é, $\sigma(f(x)) = f(x)$, $\forall\, \sigma \in S_n$ é chamado **corpo de funções racionais simétricas**. Definimos as funções elementares simétricas: $a_0 = 0$, $a_1 = \sum_{i=1}^n x_i$, $a_2 = \sum_{i<j}^n x_ix_j$, $\ldots$, $x_n = \prod_{i=1}^n x_i$.

**Teorema 24.1.** Se $S \subseteq F(x_1, \ldots, x_n)$ é o corpo das funções racionais simétricas, então:

1. $[F(x_1, \ldots, x_n) : S] = n!$.
2. $G(F(x_1, \ldots, x_n) : S) = S_n$.
3. Se $a_1, \ldots, a_n \in F(x_1, \ldots, x_n)$ são funções simétricas elementares, então $S = F(a_1, \ldots, a_n)$.
4. $F(x_1, \ldots, x_n)$ é o corpo de fatoração do polinômio $p(t) = (t - x_1) \ldots (t - x_n) = \sum_{i=0}^{n} (-1)^i a_i t^{n-1} \in S[t]$.

**Definição 24.2.** $K \supseteq F$ é **extensão normal de** $F$, se:

1. $[K : F]$ é finita.
2. O subcorpo de $K$ fixado pelo grupo $G(K : F)$ é $F$.

**Teorema 24.2.** Sejam $E \supset F$ extensão normal, $H \leq G(E : F)$ e $E_H = \{x \in E \mid \sigma(x) = x, \forall\, \sigma \in H\}$. Então:

1. $[E : E_H] = |H|$.
2. $H = G(E : E_H)$.

Em particular, $[E : F] = |G(E : F)|$.

**Lema 24.1.** Seja $K \supseteq F$ corpo de fatoração de $f(x) \in F[x]$ e seja $p(x) \in F[x]$ fator irredutível de $f(x)$. Se as raízes de $p(x)$ são $\alpha_1, \ldots, \alpha_r$, então existem $\sigma_i \in G(K : F)$ tais que $\sigma_i(\alpha_1) = \alpha_i$, $\forall\, i = 1, \ldots, r$.

**Teorema 24.3.** $K \supseteq F$ é extensão normal de $F$ se, e somente se, $K$ é corpo de fatoração de algum polinômio $f(x) \in F[x]$.

# 25 Aula 25 - Teorema Fundamental da Teoria de Galois

**Definição 25.1.** Seja $K \supseteq F$ o corpo de fatoração de algum polinômio $f(x) \in F[x]$. O **grupo de Galois de** $f(x)$ é $G(K, F)$.

**Lema 25.1.** Sejam $f(x) \in F[x]$, $E \supseteq F$ corpo de fatoração de $f(x)$ e $G(E, F)$ o grupo de Galois de $f(x)$. Então $T \supseteq F$ é normal $\Leftrightarrow$ $\sigma(T) = T$, $\forall\, \sigma \in G(E, F)$.

**Teorema 25.1** (Teorema Fundamental da Teoria de Galois)**.** Sejam $f(x) \in F[x]$, $E \supseteq F$ corpo de fatoração de $f(x)$ e $G(E, F)$ o grupo de Galois de $f(x)$. Para cada subcorpo $T$ tal que $E \supseteq T \supseteq F$ considere $G(E, T) \leq G(E, F)$ e para cada subgrupo $H \leq G(E, F)$ considere $E_H = \{x \in E \mid \sigma(x) = x, \forall\, \sigma \in H\}$ (note que $E \supseteq E_H \supseteq F$). Sejam $A = \{T \text{ corpo} \mid E \supseteq T \supseteq F\}$ e $B = \{H \text{ grupo} \mid H \leq G(E, F)\}$. Considere as aplicações:

$$\begin{array}{lll} \varphi : A \to B & & \psi : B \to A \\ \quad T \mapsto G(E, T) & & \quad H \mapsto E_H \end{array}$$

Então

1. $\psi(\varphi(T)) = T$, ou seja, $E_{G(E,T)} = T$.
2. $\varphi(\psi(H)) = H$, ou seja, $G(E, E_H) = H$.
3. $[E : T] = |G(E, T)|$ e $[T : F] = [G(E, F) : G(E, T)]$.
4. $T \supseteq F$ é normal $\Leftrightarrow$ $G(E, T) \lhd G(E, F)$.
5. $T \supseteq F$ é normal $\Rightarrow$ $G(T, F) \cong {}^{G(E,F)}\!/_{G(E,T)}$.

# 26 Aula 26 - Solubilidade por radicais

**Definição 26.1.** $G$ é **solúvel** se existe uma cadeia finita de subconjuntos $G = N_0 \geq N_1 \geq \cdots \geq N_k = \{1_G\}$, onde $N_i \lhd N_{i-1}$ e $^{N_{i-1}}\!/_{N_i}$ é abeliano.

**Lema 26.1.** Defina $G^{(1)} = G'$, $G^{(k)} = (G^{(k-1)})'$. Então $G^{(k)} \lhd G$, $\forall\, k$, e $^{G^{(k-1)}}\!/_{G^{(k)}}$ é abeliano.

**Lema 26.2.** $G$ é solúvel $\Leftrightarrow$ $G^{(k)} = \{1_G\}$ para algum $k \geq 0$.

**Corolário 26.1.** Seja $f : G \to H$ homomorfismo. Se $G$ é solúvel, então $f(G)$ é solúvel.

**Corolário 26.2.** $S_n$, $n \geq 5$, não é solúvel.

**Definição 26.2.** Um polinômio $p(x) \in F[x]$ é **solúvel por radicais** se existem corpos $F = F_0 \subseteq F_1 = F_0(w_1) \subseteq F_2 = F_1(w_2) \subseteq \cdots \subseteq F_k = F_{k-1}(w_k)$, onde $w_i^{r_i} \in F_{i-1}$, $\forall\, i = 1, \ldots, k$, e todas as raízes de $p(x)$ estão em $F_k$.

**Lema 26.3.** Se $F$ tem todas as $n$-ésimas raízes da identidade (para algum $n$) e se $a$ é um elemento não nulo de $F$, então:

1. $K = F(u)$ é corpo de fatoração de $x^n - a \in F[x]$, onde $u$ é raiz qualquer de $x^n - a$.
2. O grupo de Galois, $G(K, F)$, é abeliano.

**Teorema 26.1.** Seja $F$ corpo que contém todas as raízes da identidade. Se $p(x) \in F[x]$ é solúvel por radicais, então o grupo de Galois de $p(x)$ é solúvel. (Observação: o teorema mais geral é: $p(x) \in F[x]$ é solúvel por radicais $\Leftrightarrow$ o grupo de Galois de $p(x)$ é solúvel).

**Teorema 26.2.** Um polinômio geral $p(x)$ com grau $\deg(p(x)) \geq 5$ não é solúvel por radical.

# 27 Aula 27 - Terceira Prova

Foi realizada a terceira prova.