Universidade Estadual do Sudoeste da Bahia
Departamento de Ciências Exatas e Tecnológicas

Teoria Elementar de Galois

Vitória da Conquista - Bahia
2016

Kaique Ribeiro Prates Santos

Teoria Elementar de Galois

Monografia apresentada ao Departamento de Ciências Exatas e Tecnológicas da Universidade Estadual do Sudoeste da Bahia - Campus Vitória da Conquista-BA, para obtenção do Título de Licenciado em Matemática, sob orientação do Prof. Dr. Júlio César dos Reis.

Vitória da Conquista - Bahia
2016

Folha de aprovação

Kaique Ribeiro Prates Santos

Teoria Elementar de Galois

Monografia apresentada ao Colegiado do Curso de Matemática como requisito parcial para aprovação na disciplina Seminário de Pesquisa II do Curso de Licenciatura em Matemática.

Aprovado em _____/_____/ 2016.

BANCA EXAMINADORA

Dr. Júlio César dos Reis - UESB

Orientador

Dr. Sérgio da Silva Aguiar - UESB

2º Membro

Dr. Gonçalo Renildo Lima Cerqueira - UESB

3º Membro

Vitória da Conquista - Bahia
2016

À minha amada esposa, Fernanda.

Agradecimentos

Em primeiro lugar, agradeço à Deus, pela vida e pelo amor.

Agradeço à minha esposa, Fernanda Silveira, pelo apoio incondicional durante todo o curso de graduação.

Ao Prof. Dr. Júlio César dos Reis, pela paciência e por ter me dado a oportunidade de ser seu orientando.

Aos meus amigos, Otiliano Júnior e Lucas Caeiro, pelos bons momentos de conversa e risadas.

Aos professores do curso de graduação da UESB, pelos ensinamentos.

Aos meus colegas do curso de graduação da UESB, com os quais partilhei bons momentos.

Agradeço também à minha família pelo carinho, em especial, à minha avó, Edite Prates, e aos meus pais, Luelton e Lucineide Santos, pelo apoio e motivação.

Resumo

O trabalho tem como objetivo central o estudo da correspondência de Galois a partir de diagramas.

Basicamente, serão demonstrados alguns resultados da Teoria de Grupos e da Teoria de Corpos. Com base na teoria estudada, serão utilizados reticulados de grupos (que são diagramas de grupos onde é possível a visualização dos subgrupos e seus respectivos índices) para a comparação com os reticulados das extensões de corpos (que, de forma análoga, possibilita a visualização de subcorpos dentro de uma extensão de corpos e seus respectivos índices).

Fazendo uso apropriado do Teorema Fundamental da Teoria de Galois, o trabalho apresenta uma forma de determinar se uma extensão é ou não galoisiana e compara as estruturas de grupos com as extensões de corpos a partir dos diagramas.

Sumário

Introdução **7**

1 Teoria de Grupos **8**
1.1 Grupos 8
1.1.1 Geradores de um grupo 11
1.1.2 Subgrupos 11
1.1.3 Teorema de Lagrange e Subgrupos normais 14
1.2 Homomorfismos e Reticulados 17
1.2.1 Homomorfismos 17
1.2.2 Reticulados 21

2 Corpos, Extensões de Corpos e Polinômios **25**
2.1 Corpos 25
2.2 Polinômios e Extensões de corpos 30
2.2.1 Extensões normais 32
2.2.2 Extensões separáveis 33

3 Elementos da Teoria de Galois **36**
3.1 Automorfismos em extensões de corpos 36
3.2 A Correspondência de Galois 40
3.2.1 Extensões Galoisianas 41
3.2.2 O Teorema Fundamental 42
3.3 Comparação de estruturas 47

Considerações Finais **54**

A O Teorema de Cauchy **56**

B Grupos de Klein e extensões de corpos **58**

Introdução

Dado um polinômio irredutível $p(x)$ sobre um corpo $\mathbb{K}$, podemos utilizar as raízes de p para "formar" uma extensão de corpos algébrica $\mathbb{L}$ sobre $\mathbb{K}$. Consideraremos então automorfismos sobre $\mathbb{L}$ tais que a restrição dos mesmos ao corpo $\mathbb{K}$ seja o automorfismo identidade. Observando que tais automorfismos apenas permutam as raízes do polinômio p, pois os coeficientes estão em $\mathbb{K}$, determinaremos todos os possíveis automorfismos desta forma, ou seja, o Grupo de Galois do polinômio p. À partir daí, compararemos a estrutura existente no Grupo de Galois de p com a estrutura da extensão de corpos $\mathbb{L}$ sobre $\mathbb{K}$.

O trabalho apresenta uma forma "visual" de comparar as estruturas citadas, à partir de diagramas que contêm informações sobre as estruturas. Fazendo uso da Correspondência de Galois, mostraremos que não é coincidência os diagramas das estruturas terem formas similares, mesmo quando consideramos os graus das extensões e os índices dos subgrupos do Grupo de Galois. É importante ressaltar que a teoria aqui apresentada fundamenta aplicações importantes de outros temas da álgebra abstrata como a solubilidade por radicais de um polinômio.

Dentre os conhecimentos prévios considerados, neste trabalho, estão: conhecimentos básicos de álgebra linear e polinômios. O trabalho é dividido em três capítulos. No primeiro capítulo, serão apresentados resultados referentes à Teoria de Grupos, a discussão teórica é centrada em fornecer as ferramentas necessárias para a demonstração do Teorema fundamental da Teoria de Galois. Sempre que possível e conveniente são apresentados reticulados de grupos para que o leitor possa se "acostumar" com as informações fornecidas. A última sessão deste capítulo é dedicada aos diagramas e a utilização dos mesmos para determinar a ordem de subgrupos.

No segundo capítulo, é apresentada a teoria relacionada aos corpos e extensões de corpos. Também, neste capítulo, fazemos uso de diagramas para estudar as estruturas das extensões de corpos. O leitor será direcionado a ter uma noção intuitiva de que extensões de corpos e grupos podem ser "comparados".

No terceiro capítulo, são apresentados exemplos de extensões galoisianas, fazendo uso de exemplos previamente discutidos nos capítulos anteriores. Basicamente, o terceiro capítulo utiliza os resultados apresentados nos capítulos 1 e 2 para comparar extensões de corpos com certos grupos de automorfismos. Antes da demonstração do resultado principal, vários resultados são demonstrados e apresentados. A última sessão deste capítulo conclui a comparação à partir dos diagramas e mostra como encontrar extensões galoisianas fazendo uso do teorema principal.

Além disso, este trabalho possui dois apêndices.No primeiro, é demonstrado o Teorema de Cauchy. No segundo, é feita uma "generalização" para o grupo de Klein e uma comparação de grupos de Klein com Grupos de Galois de certos tipos de polinômios.

Capítulo 1

Teoria de Grupos

Nesta primeira seção, discutiremos as definições e propriedades relacionadas aos grupos. Os exemplos, dados no decorrer do texto como um todo, serão sempre relembrados com frequência para relacionar as estruturas algébricas estudadas.

1.1 Grupos

São estruturas algébricas de grande relevância para os resultados que se seguirão. Como veremos, um grupo é um conjunto em que há uma operação bem definida com as propriedades de *associatividade, elemento neutro e elemento inverso*. Em alguns trabalhos da literatura são considerados ainda estruturas que necessitam de apenas duas destas três propriedades, que são os monoides (onde não há necessidade da propriedade do elemento inverso).

Definição 1 (Grupos) *Seja $G \neq \emptyset$ um conjunto e $*$ uma operação definida em G. Dizemos que o par $(G, *)$ é um grupo se G, munido da operação $*$, possui as seguintes propriedades:*

(i) Associatividade: Dados $a, b, c \in G$ vale $(a * b) * c = a * (b * c)$.

(ii) Elemento Neutro: Existe $e \in G$ tal que $e * a = a * e = a, \forall a \in G$.

(iii) Inverso: Dado $a \in G, \exists a^{-1} \in G$ tal que $a * a^{-1} = a^{-1} * a = e$.

Observação 2 *Afim de facilitar a notação, diremos que $(G, *)$ é um grupo e denotaremos apenas por G quando não houver risco de confusão. A operação $*$ ficará subentendida.*

Também denotaremos $x * y$ por xy e o elemento neutro por e. Tratando-se de grupos, quando não houver risco de ambiguidade, denotaremos ainda $(xy)z = x(yz)$ por apenas xyz, uma vez que vale a associatividade.

A unicidade de (ii) pode ser provada da seguinte forma:
Suponha que $e, e' \in G$ sejam elementos neutros de G. Segue então que $e = e * e' = e' \Longrightarrow e = e'$.

Prova-se também a unicidade de (iii):

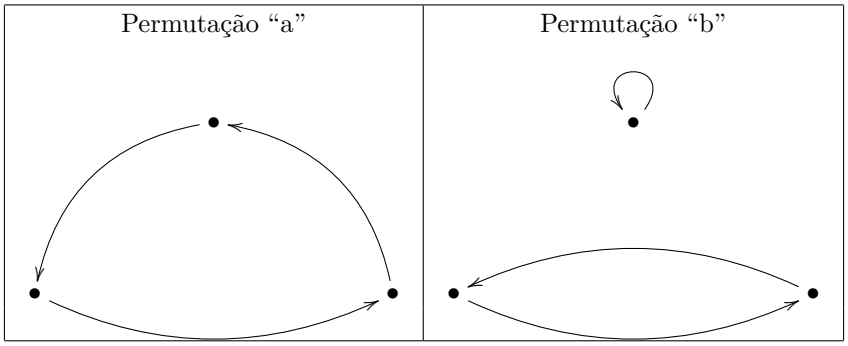
Dado $a \in G$, suponha que existem $b_1, b_2 \in G$ tais que ambos sejam elementos inversos do elemento a.
Daí, $b_1 = b_1 * e = b_1 * (a * b_2) = (b_1 * a) * b_2 = e * b_2 = b_2 \Longrightarrow b_1 = b_2$.

Observação 3 *Se, além dessas propriedades, G também cumprir:*
(iv) Comutatividade: $\forall a, b \in G$ é válida a igualdade $a * b = b * a$.
Diremos então que G é um grupo comutativo ou abeliano.

Para o nosso propósito, alguns grupos nos exemplos abaixo serão sempre relembrados no decorrer do texto. Esse fato se dará principalmente ao discutirmos grupos de automorfismos de extensões de corpos no Capítulo 3 deste trabalho.

Exemplo 4 (Permutações de 3 objetos) *O conjunto $S_3 = \{e, a, a^2, b, ab, a^2b\}$ é um grupo, onde $a^3 = b^2 = e$ (sendo que $ab = ba^2$), que são as permutações de 3 objetos.*

Observe que qualquer elemento de S_3 é obtido a partir de composições de a e b, como veremos mais adiante, a e b podem ser considerados geradores do grupo S_3. Além disso, podemos considerar que o elemento a representa uma permutação na qual nenhum dos três objetos fique fixo, ou seja todos os objetos são "trocados de lugar" e o elemento b representa uma permutação na qual apenas um objeto está fixo. A seguir uma ilustração da aplicação dos geradores de S_3 sobre objetos (pontos distintos).



Exemplo 5 (Grupo de Klein) *O conjunto $V_4 = \{e, a, b, ab\}$, onde $a^2 = b^2 = e$, é um grupo chamado de Grupo de Klein de ordem 4.*

Este é um grupo comutativo com apenas 4 elementos. Notamos que qualquer elemento de V_4 é inverso de si mesmo.

Exemplo 6 (Números inteiros) *O conjunto dos números inteiros $\mathbb{Z}$, munido da adição usual, é um grupo com uma infinidade de elementos.*

Um fato interessante deste grupo, é que qualquer elemento pode ser obtido de composições feitas com os elementos 1 e -1, ou seja, qualquer elemento é um múltiplo destes.

Exemplo 7 (Restos da divisão por $n \in \mathbb{N}$) *O conjunto $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\}$, munido da adição usual, é um grupo finito com n elementos.*

Exemplo 8 (Matrizes inversíveis de ordem n) *O conjunto das matrizes invertíveis $GL_n(\mathbb{R}) = \{M_{n\times n}(\mathbb{R}); detM \neq 0\}$, com coeficientes reais, munido da multiplicação usual de matrizes, é um grupo.*

Afim de simplificar a notação, denotaremos por M_n ao invés de $M_{n\times n}$ a matriz quadrada de ordem n. A matriz identidade de ordem n será denotada por I_n.

Exemplo 9 (Grupos diedrais) *O conjunto* $D_{2n} = \{e, r, r^2, ..., r^{n-1}, s, sr, sr^2, ..., sr^{n-1}\}$*, onde* $r^n = s^2$ *e* $rs = sr^{-1} = sr^{n-1}$*, é o grupo das simetrias no n-ágono regular.*

Este grupo representa movimentos rígidos feitos num polígono regular de n lados, evidentemente, por se tratar de simetrias, não representam translações, e sim rotações e reflexões.

Exemplo 10 (Permutação de n objetos) *No decorrer deste texto, denotaremos o grupo de permutações de n objetos por* S_n*.*

Observe ainda que S_3 (Exemplo 4) é um grupo de permutação. Mais ainda, de certa forma, $S_3 = D_6$. Discutiremos esta "equivalência" entre estes dois grupos quando falarmos de isomorfismos. Note que, quando $n = 3$, o n-ágono é na verdade um triângulo equilátero. Ou seja, S_3 pode ser visto como o grupo de simetrias no triângulo equilátero.

Exemplo 11 *O conjunto* $\mathbb{R}$*, munido da soma usual, é um grupo.*

Exemplo 12 *O conjunto* $\mathbb{R} - \{0\}$*, munido da multiplicação usual, é um grupo.*

Outro grupo multiplicativo, que está contido em $\mathbb{R} - \{0\}$, é $\mathbb{R}^*_+$.

Exemplo 13 *O conjunto* $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}; a, b \in \mathbb{Q}\}$ *é um grupo aditivo, com a adição usual.*

Exemplo 14 (Quatérnios) *O conjunto* $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$*, munido da multiplicação (Veja a tábua de multiplicação de* Q_8*, tabela 1.1, logo abaixo), é um grupo.*

Quando o número de elementos de G for um número natural n, diremos que G é um grupo finito e, quando G possuir uma infinidade de elementos, diremos que G é um grupo infinito.
Para grupos finitos podemos fazer a tábua da operação, onde muitas vezes podemos perceber várias propriedades do grupo. Por exemplo, se a tábua for simétrica em relação à sua diagonal principal o grupo envolvido é abeliano. Abaixo segue a tábua de Q_8, a operação foi realizada multiplicando-se a linha pela coluna:

$\cdot$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	k	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Tabela 1.1: Tábua de Q_8

Os produtos dos elementos que comutam entre si aparecerão de forma simétrica em relação à diagonal principal. Afim de que o grupo seja abeliano, toda a tábua precisa ser simétrica em relação à diagonal principal. Além disso, como a diagonal principal está praticamente preenchida por -1, temos que qualquer elemento $-1, 1 \neq a \in Q_8$ é tal que $a^2 = -1$. Evidentemente, a coluna e a linha do elemento neutro serão sempre iguais à linha e à coluna de elementos que foram usados na operação.

1.1.1 Geradores de um grupo

Diremos que um grupo G é gerado pelos elementos $\alpha_1, \alpha_2, ..., \alpha_n$, se qualquer elemento de G puder ser escrito como um número finito de operações entre os elementos $\alpha_1, \alpha_2, ..., \alpha_n$, e escreveremos $G =< \alpha_1, \alpha_2, ..., \alpha_n >$.
Ainda, se o número de elementos de G for n, escreveremos então $|G| = n$, onde $|G|$ denotará o número de elementos de G.

Definição 15 (Ordem de um grupo) *Seja G um grupo finito, ou seja, $|G| = n$. Definimos então como ordem de G o número de elementos de G.*

Observe que se o grupo G possui ordem infinita, então o conjunto G possui infinitos elementos. Nem sempre estaremos interessados em estudar apenas a ordem do grupo G como um todo. Por isso, a observação abaixo também define a ordem de um elemento de G.

Observação 16 (Ordem de um elemento) *Se $x \in G$, onde G é um grupo. Denotaremos por $| < x > |$ a ordem do elemento x.*

Essa observação diz apenas que para calcular a ordem de um elemento x é preciso saber quantos elementos de G podem ser representados por várias composições de x consigo mesmo, ou seja, quantos elementos o elemento x gera. A ordem de x é portanto o menor inteiro positivo n tal que $x^n = e$. Podemos denotar a ordem de um elemento simplesmente por $|x|$ ao invés de $| < x > |$.
Agora temos condições de definir grupos cíclicos.

Definição 17 (Grupos Cíclicos) *Seja G um grupo onde qualquer elemento $a \in G$ pode ser escrito como uma potência de um elemento $e \neq \alpha \in G$, isto é, $\forall\ a \in G, \exists\ n \in \mathbb{Z}; \alpha^n = a$ então G é cíclico.*

Observe que $\alpha \neq 1$ é necessário. Além disso, podemos definir $\alpha^{-n} = (\alpha^n)^{-1}$ e $\alpha^0 = 1$, para que todas as potências de α fiquem bem definidas. É fácil ver que se G é cíclico, então $G =< \alpha >$, para algum $1 \neq \alpha \in G$.

A seguir temos alguns exemplos de grupos e seus respectivos geradores.

1. $\mathbb{Z} =< 1 >$ é cíclico.
2. $V_4 =< a, b >$.
3. $S_3 =< a, b >$.
4. $D_{2n} =< r, s >$.
5. $Q_8 =< i, j, k >$.
6. $Z_n =< \overline{1} >$ é cíclico.

1.1.2 Subgrupos

Várias estruturas algébricas se repetem, no sentido de conter ou estarem contidas em outras estruturas com os mesmos padrões. Veremos a seguir que existem grupos contidos em outros grupos. A esses grupos "menores" chamaremos de subgrupos. Evidentemente, cada subgrupo é munido da operação do grupo no qual está contido e, por consequência, "herda" as propriedades necessárias para ser um grupo. Além disso, a operação restrita ao subgrupo tem a propriedade de fechamento, e isto caracteriza o respectivo subgrupo.

Definição 18 (Subgrupos) *Seja G um grupo e $H \subset G$ um conjunto não vazio. Diremos que H é um subgrupo de G e denotaremos por $H \leq G$ se H, munido da operação de G, for um grupo. Isto é, possui as seguintes propriedades:*

i) $e \in H$ *(O elemento neutro pertence a H).*

ii) $\forall\ x, y \in H,\ xy \in H$ *(Fechamento).*

iii) Dado $x \in H,\ \exists\ x^{-1} \in H;\ xx^{-1} = x^{-1}x = e$ *(Elemento inverso para cada elemento de H).*

Observação 19 *O elemento neutro de G é o mesmo de H, pois, caso não fosse, G possuiria dois elementos neutros, o que já provamos ser impossível. O mesmo ocorre com os inversos de cada elemento de H, são os mesmos no grupo G.*

Exemplo 20 (Matrizes quadradas de determinante igual a 1)
O conjunto $SL_n(\mathbb{R}) = \{M_n(\mathbb{R}); detM = 1\}$, das matrizes quadradas de ordem n com coeficientes reais e determinante igual a 1, é um subgrupo do grupo $GL_n(\mathbb{R}) = \{M_n(\mathbb{R}); detM \neq 0\}$.

Prova: $(SL_n \leq GL_n)$

A prova se dá mostrando que cada uma das propriedades de subgrupo é satisfeita por SL_n. Para isso, será considerado o fato de que $det(AB) = detA \cdot detB$, quando $A, B \in GL_n$, a demonstração deste fato foge aos objetivos deste trabalho e não será feita aqui.

i) Existe I_n , tal que, $\forall\ M \in SL_n, I_nM = MI_n = M$, e, além disso, $detI_n = 1$, ou seja, $I_n \in SL_n$.

ii) Dadas duas matrizes $A, B \in SL_n$ temos que $det(AB) = detA \cdot detB = 1$, e, claramente AB é uma matriz quadrada de ordem $n \times n$, ou seja, $A, B \in SL_n \Longrightarrow AB \in SL_n$.

iii) $\forall\ A \in SL_n$ (Como A é inversível, pois $detA = 1$), $\exists\ A^{-1} \in GL_n$ tal que $AA^{-1} = A^{-1}A = I$.
Só resta provar que $detA^{-1} = 1$.
De fato, $1 = detI = det(AA^{-1}) = detA \cdot detA^{-1}$. Agora, $A \in SL_n \Longrightarrow detA = 1$ e daí segue que $detA^{-1} = 1$.
Ou seja, $A^{-1} \in SL_n$. ■

Exemplo 21 (Subgrupos de Q_8) *Em Q_8 (Exemplo 14) é fácil ver que $< -1 > \leq Q_8$, $< i > \leq Q_8$, $< j > \leq Q_8$ e $< k > \leq Q_8$. Note ainda que $< -1 > \leq < a > \leq Q_8$ e $< a > = < -a > = \{1, -1, a, -a\}$ quando $a \in \{i, j, k\}$.*

Uma forma interessante para estudar grupos e seus respectivos subgrupos é desenhar os ***reticulados*** dos grupos. Trata-se de um diagrama que informa os subgrupos contidos dentro do grupo e compara os mesmos. O diagrama mostra ainda os geradores dos respectivos subgrupos. Voltaremos a falar mais sobre os reticulados quando houver mais resultados para serem discutidos utilizando-se os mesmos. Na seção 1.2, desenhamos vários reticulados de diversos grupos e exploramos algumas informações do grupo a partir dos respectivos reticulados. A seguir temos o reticulado do grupo Q_8:

$$\begin{tikzcd}
 & Q_8 & \\
< i > \arrow[ur] & < j > \arrow[u] & < k > \arrow[ul] \\
 & < -1 > \arrow[ul] \arrow[u] \arrow[ur] & \\
 & < 1 > \arrow[u] &
\end{tikzcd}$$

Todas as informações dadas no Exemplo 21 podem ser "lidas" no diagrama.
As setas partem de subgrupos e apontam para seus respectivos grupos. Observe ainda que podemos ver notoriamente as propriedades da relação $\leq$. Por exemplo, não existe uma flecha de $< -1 >$ para Q_8, mas podemos usar a transitividade : se $< -1 > \leq < i > \leq Q_8$, então $< -1 > \leq Q_8$.

Exemplo 22 (Retas no plano) *O conjunto $L = \{f : \mathbb{R} \longrightarrow \mathbb{R}; f(x) = x + b, b \in \mathbb{R}\}$ das retas em $\mathbb{R}^2$ com coeficiente angular igual a 1 é um subgrupo do grupo $(G, \circ)$ das retas em $\mathbb{R}^2$, onde $G = \{f : \mathbb{R} \longrightarrow \mathbb{R}; f(x) = ax + b, a, b \in \mathbb{R}\}$ e $\circ$ é a composição de funções.*

Exemplo 23 (Múltiplos de números inteiros) *No grupo aditivo $\mathbb{Z}$, cada conjunto da forma $m\mathbb{Z}$, onde $m \in \mathbb{Z}$, é um subgrupo.*

Alguns subgrupos podem ser encontrados de forma mais natural, genérica, como é o caso dos exemplos que veremos a seguir.

Exemplo 24 (Subgrupos triviais) *Dado um grupo G, dizemos que G e $\{e\}$ são os subgrupos triviais de G. Qualquer outro subgrupo será chamado de subgrupo próprio de G.*

Exemplo 25 (Centro de um grupo) *Seja G um grupo. Então, o conjunto $Z(G) = \{a \in G;\ ax = xa,\ \forall\ x \in G\}$, denominado de centro do grupo G é um subgrupo de G.*

Prova: $(Z(G) \leq G)$

i) Claramente, $e \in Z(G)$, pois, dado $a \in Z(G)$, temos que $a = ae = ea$.

ii) Dados $a, b \in Z(G)$ e $x \in G$ temos:

$$(ab)x = a(bx) = a(xb) = (ax)b = (xa)b \Longrightarrow (ab)x = x(ab) \Longrightarrow ab \in Z(G).$$

iii) Agora, dado $a \in Z(G)$, mostraremos que $a^{-1} \in Z(G)$. De fato, a^{-1} existe, pois G é grupo. Temos ainda que $\exists\ y \in G$ tal que $a^{-1}x = y, \forall\ x \in G$. Logo,

$$x = ay \Longrightarrow x = ya, pois\ a \in Z(G) \Longrightarrow xa^{-1} = y = a^{-1}x.$$

Ou seja, $a^{-1}x = xa^{-1}, \forall\ x \in G \Longrightarrow a^{-1} \in Z(G)$.

Segue então de i),ii) e iii) que $Z(G) \leq G$. ■

Este é um subgrupo especialmente interessante, pois seus elementos comutam com todos os elementos de G. Observe que G é abeliano $\Longleftrightarrow G = Z(G)$.

Exemplo 26 (Centralizadores) *Seja G um grupo. Dizemos que $C_G(x) = \{a \in G;\ ax = xa\}$ é o centralizador de x em G. Observe que x é fixo e que, naturalmente, $Z(G) \leq C_G(x)$. Pois, um elemento que comuta com todo o grupo G certamente comuta com o elemento $x \in G$.*
A prova de $C_G(x) \leq G$ é feita de forma análoga à que foi feita para $Z(G) \leq G$.

Exemplo 27 (Interseção de subgrupos) *Seja G um grupo e $H_1, H_2, ..., H_n \leq G$. Afirmamos que $\bigcap_{i=1}^{n} H_i \leq G$.*

De fato, $e \in H_i, \forall i$, operar dois elementos no conjunto $\bigcap_{i=1}^{n} H_i$ resulta em outro elemento do mesmo conjunto pois cada H_i é subgrupo, além disso, se $a \in H_i, \forall i$, então $a^{-1} \in H_i, \forall i$. Segue então que $\bigcap_{i=1}^{n} H_i \leq G$.

Exemplo 28 (Comutador de um grupo) *Definimos como comutador de um grupo G o conjunto $G' =< \{a \in G; a = xyx^{-1}y^{-1}, \forall\ x, y \in G\} >$. G' é um subgrupo de G, além disso, G é abeliano se, e somente se, $G' = \{e\}$.*

Exemplo 29 (Subgrupos de V_4) *Como visto no Exemplo 5, $V_4 = \{e, a, b, ab\}$.*

Os subgrupos de V_4 podem ser visualizados a seguir em seu reticulado.

$$\begin{tikzcd}
 & V_4 & \\
< a > \arrow[ur] & < ab > \arrow[u] & < b > \arrow[ul] \\
 & \{e\} \arrow[ul] \arrow[u] \arrow[ur] &
\end{tikzcd}$$

1.1.3 Teorema de Lagrange e Subgrupos normais

Discutiremos a seguir muitas definições que serão reutilizadas na Teoria de Galois. Como veremos no Capítulo 3, existe um relação entre subgrupos normais de automorfismos de uma extensão de corpo e a própria extensão de corpo. Agora, seja G um grupo e H um subgrupo de G. Sejam ainda $x, y \in G$, podemos definir a relação congruência módulo H em G da seguinte forma:

$$x \equiv y\ (modH) \Longleftrightarrow x = hy, \text{ para algum } h \in H.$$

É equivalente dizer que $x \in Hy$. O conjunto Hy será denominado classe lateral à esquerda de y. Além disso, congruência módulo H é uma relação de equivalência:

i) $x \equiv x\ (modH)$, pois $x = ex$, com $e \in H$ (Reflexiva).

ii) Suponha que $x \equiv y\ (modH)$. Ou seja, $\exists\ h \in H$ tal que $x = hy$. Agora, $H \leq G \Longrightarrow h^{-1} \in H$.
Daí segue que $h^{-1}x = h^{-1}hy \Longrightarrow y = h^{-1}x \Longrightarrow y \equiv x\ (modH)$ (Simétrica).

iii) Finalmente, se $x \equiv y\ (modH)$ e $y \equiv w\ (modH)$, então $x = h_1 y$ e $y = h_2 w$ para $w \in G$ e $h_1, h_2 \in H$. Segue que $x = h_1 h_2 w = h_3 w \Longrightarrow x \equiv w\ (modH)$ (Transitiva).

Assim, a relação descrita particiona o grupo G. O conjunto dessas "partes" será denotado por G/H. Observe ainda que a parte de G que possui o elemento e é o próprio H. Outro fato interessante é que de forma análoga podemos calcular as classes laterais à direita e, se $H = \{e, h_1, h_2, ..., h_n\}$, então $xH = \{x, xh_1, xh_2, ..., xh_n\}$ e $Hx = \{x, h_1x, h_2x, ..., h_nx\}$.
O próximo teorema explica por que a teoria a ser desenvolvida não difere se utilizarmos Hx ou xH.

Teorema 30 (Cardinalidade das classes laterais) *Seja $H \leq G$, então $|H| = |Hx| = |xH|$, $\forall\ x \in G$.*

Prova:

Primeiro vamos mostrar que $|xH| = |yH|$, $\forall\ x, y \in G$.
Defina a função $\phi\ : xH \longrightarrow yH$ onde $xh \longmapsto yh$. Claramente ϕ é sobrejetora pois $\phi^{-1}(yh) = xh$.
Temos ainda que ϕ é injetiva:

$$\phi(xh_1) = \phi(xh_2) \Longrightarrow yh_1 = yh_2 \Longrightarrow h_1 = h_2 \Longrightarrow xh_1 = xh_2.$$

Portanto, ϕ é uma bijeção e $|xH| = |yH|$.Agora, como x é qualquer elemento de G, podemos fazer $x = e$ e teremos $|H| = |yH|$.
É imediato que, analogamente, $|H| = |Hy|$. Ou seja, $|H| = |xH| = |Hx|$, $\forall\ x \in G$. ■

O teorema acima é de fundamental importância para provar o Teorema de Lagrange, como veremos a seguir.

Teorema 31 (Teorema de Lagrange) *Seja $H \leq G$ onde $|G| = n$. Então $|G| = |G/H||H|$ e, consequentemente, $|H|$ divide $|G|$.*

Prova:
Como mencionado anteriormente, a relação congruência módulo H particiona o conjunto G:

$$G = H \cup x_1H \cup x_2H \cup ... \cup x_{k-1}H, \text{ onde } G/H = \{H, x_1H, x_2H..., x_{k-1}H\} \text{ e } x_i \in G, \forall\ i.$$

Agora, cada xH é disjunto dos demais. Logo, $|G| = |H| + |x_1H| + |x_2H| + ... + |x_{k-1}H|$.
Pelo **Teorema 30**, $|H| = |x_iH|, \forall\ i \in \{1, 2, ..., k-1\}$. E daí,

$$|G| = \underbrace{|H| + |H| + ... + |H|}_{k\ vezes} \Longrightarrow |G| = k|H|.$$

Como $|G/H| = k$, segue imediatamente que $|G| = |G/H||H|$.■

O resultado acima é fundamental para a construção dos reticulados uma vez que a ordem de todo subgrupo de G é um divisor da ordem do grupo G. A procura por subgrupos não precisa ser feita de modo aleatório, basta analisar os divisores da ordem do grupo.
O número G/H será definido como índice de H em G e se trata da ordem do conjunto quociente G/H.
Como vimos, o conjunto quociente pode ajudar a coletar informações a respeito do grupo independentemente do subgrupo escolhido. Contudo, podemos escolher "convenientemente" o subgrupo para que o quociente tenha uma operação bem definida, que não dependa da escolha dos representantes da classe, com as propriedades de grupo e mais: $xH = Hx$, para todo $x \in G$.

Definição 32 (Subgrupos normais) *Seja $H \leq G$. Se para todo $x \in G$ temos a igualdade $xHx^{-1} = H$, então H é um subgrupo normal de G e escreveremos então $H \trianglelefteq G$.*

Particionando G por um subgrupo normal H, podemos escrever então $xH = \bar{x}$ e definir uma operação $\star$ em G/H que é "herdada" da operação do grupo G e ainda possui a seguinte propriedade: $xH \star yH = xyH$.
Como se trata de uma operação proveniente da operação do grupo G, denotaremos $xH \star yH$ apenas por $xHyH$.

Observação 33 *Observe que se G é abeliano, então todo subgrupo de G é normal.*

Exemplo 34 (Grupos normais em $\mathbb{Z}$) *Os subgrupos em $\mathbb{Z}$ são da forma $n\mathbb{Z}$, onde $\mathbb{Z}$ é abeliano.*

Pela **Observação 33**, todo subgrupo de $\mathbb{Z}$ é normal.
Temos ainda, $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$.

Observação 35 *Observe que, no **Exemplo 34**, vimos que é possível calcular $|G/H|$, em alguns casos, mesmo que G não seja finito.*

Exemplo 36 (Subgrupos normais em um grupo genérico G) *Dado um grupo G. Temos:*

- $Z(G) \trianglelefteq G$;
- $G' \trianglelefteq G$;
- $G \trianglelefteq G$;
- $\{e\} \trianglelefteq G$;

Exemplo 37 (Matrizes de determinante igual a 1) *No grupo GL_n, temos $SL_n \trianglelefteq GL_n$.*

Pode-se mostrar este fato facilmente, observando que se $A \in GL_n$ e $B \in SL_n$, então

$$det(ABA^{-1}) = detA \cdot detB \cdot detA^{-1} \overset{B \in SL_n}{\Longrightarrow} det(ABA^{-1}) = detA \cdot detA^{-1} = 1 \Longrightarrow ABA^{-1} \in SL_n.$$

Exemplo 38 (Normalidade em Q_8) *Em Q_8, temos que $< -1 >, < i >, < j >$ e $< k >$ são normais. Observe que $|Q_8/ < i > | = |Q_8/ < j > | = |Q_8/ < k > | = 2$ e $|Q_8/ < -1 > | = 4$.*

Observação 39 *Um fato interessante é que se $|G/H| = 2$ então $H \trianglelefteq G$. De fato, se $|G/H| = 2$, então $G/H = \{H, xH\}$, para algum $x \in G$. Esse resultado pode ser entendido observando-se que as classes laterais à esquerda serão sempre H e Hx e à direita H e xH, e como são disjuntas, necessariamente devemos ter $xH = Hx$, e, portanto, $G/H = \{H, xH\}$.*

A **Observação 39** é uma ferramenta útil para procurar subgrupos normais, uma vez que se $|G|$ for par, e existir $H \leq G$ tal que $|H| = 2$, então $H \trianglelefteq G$.
É fato que tal subgrupo H sempre irá existir. A razão disso é mostrada no ***Teorema de Cauchy***, que afirma o seguinte: "Se p é um número primo dividindo $|G|$, então existe um subgrupo $H \leq G$ tal que $|H| = p$."
A prova deste resultado pode ser encontrada no apêndice deste trabalho e é feita com base no exercício 9 da página 96 de [1].
Observe ainda que quando $|G|$ for um número primo p, pelo **Teorema de Lagrange**, qualquer subgrupo H existente em G deve ser tal que $|H|$ divide $p = |G|$, ou seja, H só pode ser um subgrupo trivial e, sendo assim, qualquer subgrupo gerado por um elemento $e \neq x \in G$ terá ordem $|x| = p$. Concluímos então que se $x^p = e$, $\forall\ e \neq x \in G$, então G é cíclico.

1.2 Homomorfismos e Reticulados

Pensando em estruturas algébricas buscamos funções que preservem algumas propriedades do seu domínio na sua imagem. Os homomorfismos são funções que conseguem ser "regulares" para as operações definidas nos grupos. A seguir, definiremos tais objetos e veremos o quão importante é o papel dos mesmos na *Teoria de Galois* (Capítulo 3).

1.2.1 Homomorfismos

Definição 40 (Homomorfismos) *Sejam $(G, *)$ e $(H, \star)$ grupos. A função*

$$\begin{array}{rccc} \phi & : & G & \longrightarrow & H \\ & & g & \longmapsto & \phi(g) = h \end{array}$$

com a propriedade $\phi(g_1 * g_2) = \phi(g_1) \star \phi(g_2)$ é chamada de homomorfismo de G em H.

Podemos ler a **Definição 40** da seguinte forma: "É a mesma coisa operar g_1 e g_2 em G e depois aplicar a ϕ ou aplicar a ϕ em g_1 e g_2 para depois operar as imagens destes em H." O Diagrama abaixo ilustra este fato.

$$\begin{tikzcd}
g_1 \arrow[r, "\phi"] \arrow[d, "*g_2"] & \phi(g_1) \arrow[d, "\star\phi(g_2)"] \\
g_1 * g_2 \arrow[r, "\phi"] & \phi(g_1 * g_2) = \phi(g_1) \star \phi(g_2) \\
g_2 \arrow[r, "\phi"] \arrow[u, "g_1*"] & \phi(g_2) \arrow[u, "\phi(g_1)\star"']
\end{tikzcd}$$

Podemos observar que quando há homomorfismo de um grupo para outro, estes grupos estão intimamente relacionados no que diz respeito as operações, por exemplo: $\phi(e_G) = e_H$, onde e_G e e_H denotam os elementos neutros de G e H, respectivamente, e $(\phi(x))^{-1} = \phi(x^{-1})$, o que mostra que tais funções se comportam de modo bem especifico em relação ao neutro e aos inversos das operações.
A seguir, a definição de núcleo de um homomorfismo, que nos ajudará a descobrir propriedades dos dois grupos e do próprio homomorfismo.

Definição 41 (Núcleo de um homomorfismo) *Sejam G e H grupos e ϕ um homomorfismo de G em H. O núcleo de ϕ, denotado por $Ker(\phi)$, é dado por:*

$$Ker(\phi) = \{x \in G \mid \phi(x) = e_H\}, \text{ onde } e_H \text{ é o elemento neutro de } H.$$

Observação 42 *É fato que os elementos do núcleo fazem parte de um subgrupo de G. Além disso, temos que $Ker(\phi) \trianglelefteq G$.*

Exemplo 43 (Projeção canônica) *Sejam G e $H \trianglelefteq G$. A função projeção canônica*

$$\begin{array}{rccc} \pi & : & G & \longrightarrow & G/H \\ & & g & \longmapsto & \pi(g) = \overline{g} \end{array}$$

é um homomorfismo.

Observe que $\pi(xy) = \overline{xy} = xyH = xHyH \Longrightarrow \pi(xy) = \pi(x)\pi(y)$.
Além disso, $Ker(\pi) = \{x \in G \mid \pi(x) = \overline{e}\} \Longleftrightarrow Ker(\pi) = \{x \in G \mid xH = H\} \Longleftrightarrow Ker(\pi) = H$.
O que nos diz que qualquer subgrupo normal H de G é o núcleo de um homomorfismo de G em G/H.

Exemplo 44 (Função Logaritmo Natural) *A função logaritmo, definida no grupo multiplicativo dos reais positivos $\mathbb{R}_+^*$ com valores no grupo aditivo dos reais $\mathbb{R}$, é um homomorfismo:*

$$\begin{array}{rccc} \ln : & \mathbb{R}_+ & \longrightarrow & \mathbb{R} \\ & ab & \longmapsto & \ln(ab) = \ln(a) + \ln(b) \end{array}$$

Obviamente o exemplo acima pode ser generalizado para qualquer outro logaritmo.
Agora, quando o homomorfismo for bijetor poderemos relacionar os grupos que estão no domínio e contradomínio. Por exemplo, se existe um homomorfismo bijetor entre dois grupos, então ambos serão representados pelo "mesmo reticulado". Assim, podemos de certa forma diminuir os estudos de grupos, pois, quando houver um homomorfismo bijetor, já saberemos o comportamento dos grupos.

Definição 45 (Isomorfismo) *Sejam G e H grupos. Seja ainda $\phi : G \longrightarrow H$ um homomorfismo bijetor. Diremos então que ϕ é um isomorfismo e que os grupos G e H são isomorfos, escreveremos então $G \cong H$.*

Naturalmente, se $G \cong H$, então $H \cong G$. Neste sentido, os grupos G e H são equivalentes, significa que os elementos dos grupos que estão relacionados pelo isomorfismo tem as mesmas propriedades algébricas e a mesma ordem. Voltando para o Exemplo 4, podemos perceber uma equivalência entre D_6 e S_3, onde a e b são equivalentes a r e s, respectivamente.

Observação 46 (Identificando um homomorfismo injetor) *Podemos saber se um homomorfismo é injetor apenas olhando para o seu núcleo: $\phi : G \longrightarrow H$ é injetor $\Longleftrightarrow Ker(\phi) = \{e_G\}$.*

A observação anterior pode ser demonstrada facilmente observando os seguintes fatos:

i) A ida ($\Longrightarrow$) é óbvia.

ii) Para provar a volta ($\Longleftarrow$), suponha que $Ker(\phi) = \{e_G\}$ e $\phi(x) = \phi(y)$. Segue imediatamente que $\phi(xy^{-1}) = e_H \overset{xy^{-1} \in Ker(\phi)}{\Longrightarrow} xy^{-1} = e_G \Longrightarrow x = y$, ou seja, ϕ é injetora.

Exemplo 47 (Função Logaritmo Natural) *Observe que a função* ln *possui inversa e é um homomorfismo. Portanto,*

$$(\mathbb{R}_+^*, \times) \cong (\mathbb{R}, +)$$

Exemplo 48 (Grupos de ordem ≤ 5) *Com o isomorfismo, temos agora ferramentas para dizer quando os grupos se comportam de forma similar. Por exemplo:*

i) Qualquer grupo de ordem 2 é isomorfo a $\mathbb{Z}_2$;

ii) Qualquer grupo de ordem 3 é isomorfo a $\mathbb{Z}_3$;

iii) Qualquer grupo de ordem 4 é isomorfo a $\mathbb{Z}_4$ ou V_4;

iv) Qualquer grupo de ordem 5 é isomorfo a $\mathbb{Z}_5$;

Esse processo pode ser feito comparar grupos e seus respectivos comportamentos. Por exemplo, se $|G| = 8$, então G é isomorfo a $\mathbb{Z}_8$, V_8, $\mathbb{Z}_4 \times \mathbb{Z}_2$, D_8 ou Q_8. Nos três primeiros casos, temos grupos abelianos e nos dois últimos grupos não-abelianos, a prova deste fato pode ser encontrada em [2] e não será feita aqui.
Certamente é um processo que fica mais difícil conforme a ordem do grupo for maior.
Se ϕ é um isomorfismo de G em G então diremos que ϕ é um automorfismo sobre G. O conjunto dos automorfismos sobre G será denotado por $Aut\ G$.
Observe que $(Aut\ G, \circ)$ é um grupo. Este grupo será fundamental para as discussões que se seguirão neste trabalho, uma vez que, no Capítulo 3, necessitaremos de automorfismos em extensões de corpos para desenvolver as demonstrações que são o foco de estudo deste trabalho.

O resultado a seguir é bem discutido nas diversas literaturas citadas na bibliografia deste trabalho. Trata-se de um teorema que relaciona dois grupos apenas pelo fato de existir homomorfismo entre eles.

Teorema 49 (Teorema dos isomorfismos) *Seja $f\ : (G, *) \longrightarrow (G', \star)$ um homomorfismo de grupos. Então,*

i) a função induzida

$$\begin{array}{rccc} \overline{f} : & G/Ker(f) & \longrightarrow & f(G) \\ & gKer(f) & \longmapsto & f(g) \end{array}$$

é um isomorfismo.

ii) Existe uma bijeção que associa subgrupos de G que contêm $Ker(f)$ e subgrupos de $f(G)$. Além disso, essas bijeções levam subgrupos normais em subgrupos normais.

$$\begin{array}{ccc} \{Subgrupos\ de\ G\ que\ contêm\ Kerf\} & \overset{1-1}{\longleftrightarrow} & \{Subgrupos\ de\ f(G)\} \\ H & \longmapsto & f(H) \\ f^{-1}(H') & \longleftarrow & H' \\ H \trianglelefteq G & \Longrightarrow & f(H) \trianglelefteq f(G) \\ f^{-1}(H') \trianglelefteq G & \Longleftarrow & H' \trianglelefteq f(G) \end{array}$$

Demonstração:

i) Se $f\ :\ G \longrightarrow G'$ é um homomorfismo de grupos, sabemos que $Kerf \trianglelefteq G$. Nesse caso, $G/Kerf$ é um grupo com a operação induzida da operação de G. A função $\overline{f}$ está bem definida, ou seja, independe dos representantes das classes em $G/Kerf$. De fato, se $gKerf = \tilde{g}Kerf$, então $g = \tilde{g}k$, para algum $k \in Kerf$.
Agora, $f(g) = \overline{f}(g) = \overline{f}(\tilde{g}k) \Longrightarrow \overline{f}(g) = f(\tilde{g}k) = f(\tilde{g})f(k) = f(\tilde{g}) \star e_{G'} \Longrightarrow f(g) = f(\tilde{g})$. Segue que $\overline{f}(g) = \overline{f}(\tilde{g})$. Claramente, $\overline{f}$ é sobrejetora, pois seu contradomínio foi definido de forma a ser igual à sua imagem. Se $\overline{f}(gKerf) = \overline{f}(hKerf)$, então $f(gKerf) = f(hKerf)$. Daí,

$$f(g) = f(h) \Longrightarrow gh^{-1} \in Kerf \Longrightarrow \exists\ k \in Kerf \mid g = hk,$$

ou seja, $gKerf = hKerf \Longrightarrow \overline{f}$ é injetiva.
Logo, $\overline{f}$ é um isomorfismo.

ii) Observando que : $f^{-1}(f(H)) = HKerf$ (a pré-imagem da imagem de H é a composição de H e $Kerf$) para qualquer $H \leq G$ temos que se $H \supseteq Kerf$, então $f^{-1}(f(H)) = H$.

Da mesma forma, $f(f^{-1}(H')) = H' \cap f(G)$ (a imagem da pré-imagem de um subgrupo H' de G' é a parte deste subgrupo que está na imagem de G), para qualquer $H' \leq G'$.
Quando $H' \subseteq f(G)$, então $f(f^{-1}(H')) = H'$. Ou seja, temos duas funções, uma inversa da outra, que associam subgrupos de G que contêm o núcleo de f a subgrupos da imagem de G por f.
Vamos mostrar agora que essas aplicações associam subgrupos normais a subgrupos normais.
Primeiramente, suponha que $H \trianglelefteq G$. Devemos mostrar que $g'f(H)(g')^{-1} = f(H)$, $\forall\ g' \in f(G)$. De fato,

$$g'f(H)(g')^{-1} \overset{g' \in f(G)}{=} f(g)f(H)f(g^{-1}) \overset{f\ \text{é}\ homomorfismo}{=} f(gHg^{-1}) \overset{H \trianglelefteq G}{=} f(H).$$

Da mesma forma, se $H' \trianglelefteq f(G)$, temos:
Dados $a \in f^{-1}(H')$ e $g \in G$,

$$f(gag^{-1}) = f(g)f(a)f(g^{-1}) \overset{H' \trianglelefteq f(G)}{\Longrightarrow} f(gag^{-1}) \in H' \Longrightarrow gag^{-1} \in f^{-1}H'.$$

Ou seja, $H' \trianglelefteq f(G) \Longrightarrow f^{-1}(H') \trianglelefteq G$. ■

Exemplo 50 (Inteiros e raízes n-ésimas da unidade) *Considere a função*

$$\begin{array}{rccc} \psi : & (\mathbb{Z}, +) & \longrightarrow & (\mathbb{U}_n, \cdot) \\ & z & \longmapsto & e^{2\pi z\imath/n} \end{array}.$$

Note que ψ é um homomorfismo e $Ker\ \psi = n\mathbb{Z}$. Pelo ***Teorema 49****, $(\mathbb{Z}_n, +) \cong (\mathbb{U}_n, \cdot)$.*

Exemplo 51 (Reais e números complexos no círculo unitário) *Considere a função*

$$\begin{array}{rccc} \omega : & (\mathbb{R}, +) & \longrightarrow & (\mathbb{S}^1, \cdot) \\ & r & \longmapsto & e^{2\pi r\imath} \end{array}.$$

Observamos que ω é um homomorfismo, e seu núcleo é $Ker\ \omega = \mathbb{Z}$. Ou seja, $\mathbb{R}/\mathbb{Z} \cong \mathbb{S}^1$.

Nos exemplos **50** e **51** temos homomorfismos em que a imagem é um número complexo de "tamanho" igual a 1. Observe ainda que o quociente $\mathbb{R}/\mathbb{Z}$ faz com que olhemos apenas para o intervalo $[0, 1)$ da reta real. Ou seja, através da função ω, cada intervalo da reta real é levado no círculo unitário.

Exemplo 52 (Espaços vetoriais e transformações lineares) *Na álgebra linear, as transformações lineares são exemplos de homomorfismos entre espaços vetoriais.*

Observação 53 (A relação $\cong$) *É importante observar que $\cong$ define uma relação de equivalência.*

i) Evidentemente, $\exists\ Id : G \longrightarrow G$; $Id(g) = g \Longrightarrow G \cong G$ (Reflexiva).

ii) Se $G \cong H$, então existe uma função $\phi : G \longrightarrow H$ que é um isomorfismo. Logo, $\phi^{-1} : H \longrightarrow G$ é também um isomorfismo $\Longrightarrow H \cong G$ (Simétrica).

iii) Se $G \cong H$ e $H \cong F$ é por que existem funções $\psi : G \longrightarrow H$ e $\omega : H \longrightarrow F$ que são isomorfismos. Logo, existe $\phi = \psi \circ \omega : G \longrightarrow F$ que também é isomorfismo, ou seja, $G \cong F$ (Transitiva).

A **Observação 53** resume grande parte do que foi dito nesta seção. Observe que, quando dizemos que um grupo G é isomorfo a um grupo H, todas as propriedades que G possui como grupo, ou seja, seus subgrupos, a ordem dos seus elementos, os inversos dos seus elementos, são mantidas em H. Obviamente, essas considerações se devem ao fato de que as imagens dos elementos de g são obtidas pelo isomorfismo. Então, por exemplo, se $|x| = n$, com $x \in G$, então $|\phi(x) = n|$, com $\phi(x) \in H$.

1.2.2 Reticulados

Esta seção é dedicada à discussão e comparação de diversos reticulados de grupos que serão utilizados no Capítulo 3 para estudo e tratamento da teoria.
Os resultados aqui discutidos são consequências das informações contidas nas seções anteriores.

O reticulado de um grupo é um diagrama contendo informações sobre o grupo e seus geradores, seus subgrupos e respectivos geradores. Algumas referências sobre o tema chamam também de diamante de um grupo.
Podemos enriquecer as informações de um reticulado colocando os índices de um subgrupo sobre as respectivas setas. Além disso, se existe uma seta partindo de A para B, então $A \leq B$.
Um fato interessante, é que grupos isomorfos possuem reticulados "idênticos". Ou seja, olhando o reticulado de grupos isomorfos fica claro quais são os subgrupos destes que são isomorfos e é possível também comparar os elementos com suas respectivas imagens no que diz respeito à ordem e subgrupos nos quais estão presentes.

Exemplo 54 (Reticulados de $\mathbb{Z}_n$)

$$\begin{tikzcd}
\mathbb{Z}_2 & \mathbb{Z}_3 & \mathbb{Z}_4 & \mathbb{Z}_5 & & \mathbb{Z}_6 & \cdots \\
< \overline{0} > \arrow[u, "2"] & < \overline{0} > \arrow[u, "3"] & < \overline{2} > \arrow[u, "2"] & < \overline{0} > \arrow[u, "5"] & < \overline{2} > \arrow[ur, "2"] & & \\
 & & < \overline{0} > \arrow[u, "2"] & & & < \overline{3} > \arrow[uul, "3"] & \\
 & & & & < \overline{0} > \arrow[uul, "3"] \arrow[ur, "2"] & &
\end{tikzcd}$$

Como $\mathbb{Z}_n$ é abeliano, qualquer subgrupo é normal. Logo, $\mathbb{Z}_4/ < \overline{2} > \cong \mathbb{Z}_2$, $\mathbb{Z}_6/ < \overline{3} > \cong \mathbb{Z}_3$, $\mathbb{Z}_6/ < \overline{2} > \cong \mathbb{Z}_2$.

O processo de construção do reticulado pode ser feito para qualquer n. Evidentemente, quando n for um número primo, $\mathbb{Z}_n$ será cíclico e não terá subgrupos próprios.

Exemplo 55 (Reticulados de grupos de ordem 8)

$$\begin{tikzcd}
\mathbb{Z}_8 \\
< \overline{2} > \arrow[u, "2"] \\
< \overline{4} > \arrow[u, "2"] \\
< \overline{0} > \arrow[u, "2"]
\end{tikzcd}$$

*(**Restos da divisão por 8**) Este é o único grupo de ordem 8 que é cíclico. Evidentemente, qualquer outro grupo de ordem 8 e cíclico seria isomorfo ao mesmo.*

$$\begin{tikzcd}
 & Q_8 & \\
< i > \arrow[ur, "2"] & < j > \arrow[u, "2"] & < k > \arrow[ul, "2"] \\
 & < -1 > \arrow[ul, "2"] \arrow[u, "2"] \arrow[ur, "2"] & \\
 & < 1 > \arrow[u, "2"] &
\end{tikzcd}$$

*(**Os Quatérnios**)Trata-se de um grupo de ordem 8 que não é abeliano.*

$$\begin{tikzcd}
 & & D_8 & & \\
 & < s, r^2 > \arrow[ur, "2"] & < r > \arrow[u, "2"] & < rs, r^2 > \arrow[ul, "2"] & \\
< s > \arrow[ur, "2"] & < r^2 s > \arrow[u, "2"] & < r^2 > \arrow[ul, "2"] \arrow[u, "2"] \arrow[ur, "2"] & < rs > \arrow[u, "2"] & < r^3 s > \arrow[ul, "2"] \\
 & & < 1 > \arrow[ull, "2"] \arrow[ul, "2"] \arrow[u, "2"] \arrow[ur, "2"] \arrow[urr, "2"] \arrow[urrr, "2"] & &
\end{tikzcd}$$

***(Simetrias no quadrado)** Este é um grupo diedral que representa as rotações e reflexões no*

quadrado. Como vimos no exemplo 9, $rs = sr^{-1}$, ou seja, D_8 não é abeliano.

$$\begin{tikzcd}
 & & \mathbb{Z}_4 \times \mathbb{Z}_2 & & \\
 & < (0,1),(2,0) > \arrow[ur, "2"] & < (1,0) > \arrow[u, "2"] & < (1,1) > \arrow[ul, "2"'] & \\
 & < (0,1) > \arrow[u, "2"] & < (2,1) > \arrow[ul, "2"] \arrow[ull, "2"] & < (2,0) > \arrow[u, "2"'] \arrow[ull, "2"] \arrow[ul, "2"] & \\
 & & < (0,0) > \arrow[ul, "2"] \arrow[u, "2"] \arrow[ur, "2"'] & &
\end{tikzcd}$$

(Produto cartesiano de $\mathbb{Z}_4$ e $\mathbb{Z}_2$) *Note que por se tratar de um produto cartesiano de dois grupos abelianos, o grupo $\mathbb{Z}_4 \times \mathbb{Z}_2$ também é abeliano, visto que a operação é feita coordenada a coordenada.*

$$\begin{tikzcd}
 & & & < 1 > \arrow[dl] \arrow[d] \arrow[dr] & & & \\
< a > \arrow[d] \arrow[dr] & < b > \arrow[dl] \arrow[dr] & < c > \arrow[d] \arrow[dl] & < ab > \arrow[dl] \arrow[dr] & < ac > \arrow[d] \arrow[dl] & < bc > \arrow[dl] \arrow[dr] & < abc > \arrow[dl] \arrow[dr] \\
< a,b > \arrow[dr] & < a,c > \arrow[d] & < b,c > \arrow[dl] & < a,bc > \arrow[d] & < b,ac > \arrow[dr] & < c,ab > \arrow[d] & < ab,ac > \arrow[dl] \\
 & & & V_8 & & &
\end{tikzcd}$$

(Grupo de Klein de ordem 8) *Os índices dos subgrupos foram omitidos pois este grupo possui uma grande quantidade de subgrupos. Entretanto, é fácil ver que qualquer índice possível nas setas é igual a dois. Claramente, este grupo tem propriedades que lembram V_4 do exemplo 5, pois, cada elemento diferente do neutro possui ordem 2 e trata-se de um grupo abeliano.*

Qualquer outro grupo de ordem 8 terá um reticulado similar a um destes. Note que, com exceção do grupo $\mathbb{Z}_8$, todos os outros grupos tem a estrutura do grupo V_4 dentro do próprio reticulado.

$$\begin{tikzcd}
 & V_4 & \\
< a > \arrow[ur, "2"] & < ab > \arrow[u, "2"] & < b > \arrow[ul, "2"'] \\
 & \{e\} \arrow[ul, "2"] \arrow[u, "2"] \arrow[ur, "2"'] &
\end{tikzcd}$$

$V_4 \cong \mathbb{Z}_4 \times \mathbb{Z}_2 / < (2,0) > \cong V_8 / < a > \cong Q_8 / < -1 >$ e $V_4 \cong D_8 / < r^2 >$.

Exemplo 56 (Reticulado de S_3)

$$\begin{tikzcd}
 & S_3 & & & \\
< \sigma > \arrow[ur, "2"] & & & & \\
 & & < \tau > \arrow[ul, "3"] & < \tau\sigma > \arrow[ull, "3"] & < \tau\sigma^2 > \arrow[ulll, "3"] \\
< 1 > \arrow[uu, "3"] \arrow[ur, "2"] \arrow[urr, "2"] \arrow[urrr, "2"] & & & &
\end{tikzcd}$$

Observe que o único subgrupo normal de S_3 é $< \sigma >$. Aqui, lembrando do Exemplo 4, $a = \sigma$, $b = \tau$ e $1 = e$.

Agora, uma curiosidade interessante dos reticulados com os índices dos subgrupos é que ele nos dá a ordem de cada subgrupo, basta apenas multiplicar os índices das setas partindo por um "caminho". Por exemplo, $|S_3| = |S_3/ < \sigma > || < \sigma > |$, onde $| < \sigma > | = | < \sigma > / < 1 > || < 1 > |$ e o "caminho" escolhido no diagrama foi o seguinte:

$$S_3 \xleftarrow[2]{} < \sigma > \xleftarrow[3]{} < 1 > \text{ , onde } |S_3| = 6 = 2 \cdot 3.$$

Devemos seguir então uma cadeia ascendente de subgrupos, partindo de $< 1 >$ até chegar ao subgrupo desejado, a multiplicação dos índices encontrados no caminho será a ordem do subgrupo.

Teorema 57 (Ordem de um subgrupo via reticulados) *Sejam $H \leq G$ e $< 1 >= H_0 \leq H_1 \leq H_2 ... \leq H_k = H$ uma cadeia de subgrupos do subgrupo H de G.*
Então, $|H| = |H_k/H_{k-1}||H_{k-1}/H_{k-2}|...|H_2/H_1||H_1|$.

Demonstração:

Vamos mostrar por indução sobre k fazendo sempre uso do **Teorema de Lagrange**.

i) Evidentemente, para $k = 1$ a igualdade é válida, pois a cadeia será $< 1 >= H_0 \leq H_1 = H$.

ii) Suponha que a igualdade seja válida para uma cadeia com k subgrupos próprios, ou seja, $|H| = |H_k/H_{k-1}||H_{k-1}/H_{k-2}|...|H_2/H_1||H_1|$.

iii) Agora, dada uma cadeia com $k + 1$ subgrupos próprios :

$$< 1 >= H_0 \leq H_1 \leq H_2 ... \leq H_k \leq H_{k+1} = H$$

Pelo *Teorema de Lagrange*, $|H| = |H/H_k||H_k|$. Da hipótese de indução em *ii)*, $|H_k| = |H_k/H_{k-1}||H_{k-1}/H_{k-2}|...|H_2/H_1||H_1|$. Daí,

$$|H| = |H/H_k||H_k/H_{k-1}||H_{k-1}/H_{k-2}|...|H_2/H_1||H_1|, \text{ como queríamos demonstrar. } \blacksquare$$

O resultado nada mais é do que uma utilização do **Teorema de Lagrange** várias vezes. Evidentemente, foi feito com subgrupos próprios por que não contabilizamos o subgrupo formado por 1, todavia, o resultado é válido também para calcular a ordem do grupo G.

Capítulo 2

Corpos, Extensões de Corpos e Polinômios

Na próxima sessão, definiremos estruturas algébricas que necessitam de mais propriedades, do que os grupos, para serem validadas. Alguns resultados discutidos no capítulo anterior serão utilizados ao longo da discussão teórica. Além disso, resultados envolvendo anéis, cálculos de raízes de polinômios, domínios de integridade e álgebra linear básica serão utilizados sem as demonstrações, uma vez que fogem ao objetivo deste trabalho.

2.1 Corpos

Definição 58 (Corpos) *Seja $K \neq \emptyset$, munido das operações $*$ e $\star$, onde valem :*

i) Associatividade: $\forall a, b, c \in K$ temos : $(a * b) * c = a * (b * c)$ e $(a \star b) \star c = a \star (b \star c)$.

ii) Elemento neutro: $\exists e_*, e_\star \in K$ tais que, dado $a \in K$, $a * e_* = e_* * a = a$ e $a \star e_\star = e_\star \star a = a$.

iii) Inverso em $(K, *)$: Dado $a \in K$, $\exists -a \in K$ tal que $a * (-a) = (-a) * a = e_*$.

iv) Inverso em $(K - \{e_*\}, \star)$: Dado $a \in K - \{e_*\}$, $\exists a^{-1} \in K - \{e_*\}$ tal que $a \star a^{-1} = a^{-1} \star a = e_\star$.

v) Comutatividade: $\forall a, b \in K, a * b = b * a$ e $a \star b = b \star a$.

vi) Distributividade: $\forall a, b, c \in K$ valem as igualdades: $a \star (b * c) = (a \star b) * (a \star c)$ e $(a * b) \star c = (a \star c) * (b \star c)$.

Nessas condições, dizemos que $(K, *, \star)$ é um corpo. Denotaremos apenas por K quando não houver risco de confusão e as operações $*$ e $\star$ ficaram subentendidas. Afim de simplificar a notação, denotaremos também $a \star b = ab$, $e_* = 0$ e $e_\star = 1$.

Observe que $(K, *)$ é um grupo abeliano e $(K - 0, \star)$ é um grupo abeliano. Assim, muitas propriedades conhecidas dos grupos podem ser analisadas de forma análoga para os corpos. Os homomorfismos de corpos funcionam da mesma maneira que os de grupo, entretanto eles o fazem para mais de uma operação. Sendo assim, usaremos os resultados e as definições apresentadas no capítulo anterior de forma inteiramente análoga.

Observação 59 *Seja K um corpo. Dado $a \in K$ então $a0 = 0$.*

Demonstração:

Se $a = 0$ nada há para demonstrar. Seja então $a \in K - \{0\}$. Temos:

$$a0 = a(0 * 0) = (a0) * (a0) \Longrightarrow (a0) * (-(a0)) = [(a0) * (a0)] * (-(a0))$$

Agora, 0 é o elemento neutro de $*$. Daí segue que $0 = (a0) * [(a0) * (-(a0))] = (a0) * 0 \Longrightarrow 0 = a0$. ■

Esta observação mostra que todo corpo é um *Domínio de Integridade.*

Observação 60 *Seja K um corpo. Se $0, 1 \in K$ são os elementos neutros das respectivas operações $*$ e $\star$, então $0 \neq 1$.*

Demonstração:

Suponha por absurdo que $0 = 1$. Dado $0 \neq a \in K$, $a = a1 = a0$.
Ou seja, pela **Observação 59**, $a1 = a = a0 = 0$. Segue imediatamente que $\forall\ a \in K, a = 0$ o que é um absurdo! ■

Exemplo 61 (Corpos mais conhecidos) *Os conjuntos a seguir, munidos das operações usuais, são corpos:*

i) O conjunto $\mathbb{R}$;

ii) O conjunto $\mathbb{C}$;

iii) O conjunto $\mathbb{Q}$;

Todos estes corpos possuem infinitos elementos.

Exemplo 62 (Os Corpos $\mathbb{Z}_p$) *Quando p é um número primo, $\mathbb{Z}_p$ é um corpo com p elementos.*

Exemplo 63 (Corpos contendo os racionais) *O conjunto $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ é um corpo.*

Observe que os elementos de $\mathbb{Q}(\sqrt{2})$ são feitos à partir da combinação linear de 1 e $\sqrt{2}$. Da mesma maneira, podemos construir $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{6})$ e assim por diante.
Também podemos construir o corpo $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a, b, c \in \mathbb{Q}\}$ através de combinações lineares entre 1, $\sqrt[3]{2}$, $(\sqrt[3]{2})^2$. Evidentemente poderíamos repetir este processo para outros números e outros radicais e todos os corpos gerados conteriam os racionais.

Quando F for um corpo contido em um corpo K, diremos que F é um subcorpo de K. Nos exemplos anteriores, $\mathbb{Q}$ é subcorpo de $\mathbb{R}$ e dos outros corpos formados a partir dos radicais de números racionais.

Definição 64 (Extensão de um corpo) *Seja K um corpo contendo um subcorpo F. Diremos então que K é uma extensão de corpos (ou simplesmente uma extensão) de F, e denotaremos por K/F. Também podemos representar pelo reticulado:*

$$\begin{array}{c} K \\ | \\ F \end{array}$$

Algumas vezes, F também poderá ser chamado de corpo base.
É importante caracterizar as informações invariantes aos corpos para poder conhecer as propriedades dos mesmos, independente da escolha do corpo. Uma dessas informações é a característica de um corpo.

Definição 65 (Característica de um corpo) *A característica de um corpo K, denotada por $ch(K)$, é o menor inteiro positivo n tal que $n \cdot 1 = \underbrace{1 * 1 * ... * 1}_{n\ vezes} = 0$ se o número n existir, caso contrário, é definida como zero.*

Note que a característica é um inteiro positivo e não um elemento de K. O leitor deve diferenciar o elemento neutro da operação $*$ (o elemento 0) do número da característica do corpo quando for zero.

Observação 66 *A característica de um corpo só pode ser um número primo p ou zero. De fato, se $ch(K) = n = ab$, então $ab \cdot 1 = (a \cdot 1)(b \cdot 1) = 0$, mas K é um corpo :*

$$a \cdot 1 = 0 \text{ ou } b \cdot 1 = 0, \text{ com } a, b \text{ dividindo } n.$$

Portanto, necessariamente a característica de um corpo é p, com p primo, ou igual a zero.
Além disso, $\forall\ a \in K$, $p \cdot a = \underbrace{a * a * ...a * a}_{p\ vezes} = a \star (p \cdot 1) = 0$.

Observe que a operação $\cdot$ é uma operação definida em $\mathbb{N} \times K \longrightarrow K$, onde $(n, a) \longmapsto n \cdot a = \underbrace{a * a * ...a * a}_{n\ vezes}$. Valem também $a \cdot 1 * b \cdot 1 = (a + b) \cdot 1$ e $(a \cdot 1) \star (b \cdot 1) = ab \cdot 1$.
Podemos definir essa operação de modo a usar números inteiros negativos da seguinte maneira, $(-n) \cdot 1 = -(n \cdot 1)$, onde n é um inteiro positivo.

A função

$$\begin{array}{rccc} \phi : & \mathbb{Z} & \longrightarrow & K \\ & n & \longmapsto & n \cdot 1 \end{array}$$

define um homomorfismo de $\mathbb{Z}$ em K. O núcleo de ϕ é formado pelos múltiplos de $ch(K)$, ou seja, $Ker(\phi) = ch(K)\mathbb{Z}$.
É fato que o núcleo dependerá da característica de K. Se $ch(K) = p$ primo, então tomando o quociente pelo núcleo, pelo **Teorema dos isomorfismos**, teremos uma função injetiva de $\mathbb{Z}_p$ em $\phi(\mathbb{Z}) \subseteq K$. O que nos diz que, desde que K seja um corpo, existe uma cópia de $\mathbb{Z}_p$ $(ch(K) = p)$ em K, a menos de isomorfismos.

A próxima observação é de notável importância para o desenvolvimento da teoria, entretanto sua prova foge aos objetivos deste trabalho e não será feita aqui.

Observação 67 *Se $\psi : K \longrightarrow F$ é um homomorfismo de corpos, então ψ é a função identicamente nula ou é injetiva (a imagem é uma cópia de K).*

A importância da **Observação 67** se dá pelo fato de que homomorfismos de corpos se comportam de maneira mais restrita do que homomorfismo de grupos.

Se K/F é uma extensão de corpos, então podemos ver o corpo K como um F-espaço vetorial. Estamos em condição de definir dimensão de uma extensão de corpos.

Definição 68 (Grau ou Índice de uma extensão de corpos) *O grau, ou índice, de uma extensão de corpos K/F é denotado por $[K : F]$ e é igual à dimensão de K sobre F.*
A extensão é dita finita se $[K : F] = dim_F K$ é finito e infinita em caso contrário.

Exemplo 69 (Graus de extensões sobre $\mathbb{Q}$) *Os índices a seguir são de extensões finitas sobre os racionais:*

i) $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$;

ii) $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$;

iii) $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$;

iv) $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$;

Notamos que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6};\ a, b, c, d \in \mathbb{Q}\}$ e, consequentemente, $dim_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}, \sqrt{3}) = 4$. Observe que $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{6})$ também é uma extensão de corpos e tem índice 2 (como veremos mais adiante).

Exemplo 70 (Os números complexos) *O leitor provavelmente desconfia que queremos olhar os números complexos como uma extensão dos números reais. De fato, $\mathbb{C} = \{a + b\imath \mid a, b \in \mathbb{R}\}$ e, consequentemente, $[\mathbb{C} : \mathbb{R}] = 2$.*

Com as impossibilidades de achar as raízes de determinados polinômios com coeficientes em um corpo, o desenvolvimento de extensões deste corpo que possuem as raízes dos dados polinômios se fez necessário. Por exemplo, o polinômio $p(x) = x^2 + 1$ é um polinômio com coeficientes reais e, entretanto, sabemos que suas raízes são imaginárias (complexas). O que nos motiva a estabelecer condições para que tal extensão exista e responder outras questões, como a unicidade e quando que podemos ter tais extensões, formadas a partir de raízes de polinômios, em outros corpos.
Basicamente, se $\imath$ é uma raiz de $p(x) = x^2 + 1$, então, observe que, $\mathbb{R}(\imath) = \mathbb{C}$.

De forma inteiramente análoga à de grupos e subgrupos, podemos fazer os reticulados das extensões de corpos. O teorema a seguir é uma consequência de que se K/F é uma extensão de corpos, então K é um $F-$espaço vetorial.

Teorema 71 (Graus de extensões finitas) *Sejam $F \subseteq K \subseteq L$ corpos finitos. Então,*

$$[L : F] = [L : K][K : F].$$

Demonstração:
Sejam $[L : K] = m$ e $[K : F] = n$, onde L/K e K/F são extensões de corpos. Obviamente, L/F também é uma extensão de corpos, vamos mostrar que vale $[L : F] = mn$.
(i) K é um $F-$espaço vetorial de dimensão $n \Longrightarrow$ existe uma base $\alpha = \{\alpha_1, \alpha_2, ..., \alpha_n\}$ de K com n elementos.
(ii) L é um $K-$espaço vetorial de dimensão $m \Longrightarrow$ existe uma base $\beta = \{\beta_1, \beta_2, ..., \beta_m\}$ de L com m elementos.

Agora, seja $l \in L$. De (i) temos: $\exists\ a_i \in K \mid l = \displaystyle\sum_{i=1}^{m} a_i\beta_i$.
Cada a_i é um elemento de K e pode ser escrito como combinação linear da base α:

$$\text{(iii) } a_i = b_{i1}\alpha_1 + b_{i2}\alpha_2 + ... + b_{in}\alpha_n \Longrightarrow a_i = \sum_{j=1}^{n} b_{ij}\alpha_j, \text{ para todo } i.$$

O item (iii) nos permite escrever o elemento genérico l como combinação linear de mn elementos:

$$l = \sum_{i=1}^{m} a_i\beta_i \Longrightarrow l = \sum_{i=1}^{m}\sum_{j=1}^{n} b_{ij}\alpha_j\beta_i \Longrightarrow l = \sum_{\substack{i=1\\j=1}}^{\substack{i=n\\j=m}} b_{ij}\alpha_j\beta_i.$$

Cada elemento $\alpha_j\beta_i$ é um elemento que não pertence a F e pertence à L. Observe ainda que os escalares b_{ij} são todos do corpo F. Sendo assim, só nos resta mostrar que o conjunto $\alpha\beta = \{\alpha_j\beta_i \mid i = 1, 2, ..., m \text{ e } j = 1, 2, ..., m\}$ é L.I.

De fato, seja $\sum_{\substack{i=1\\j=1}}^{\substack{i=n\\j=m}} b_{ij}\alpha_j\beta_i = 0$, vamos mostrar que $b_{ij} = 0, \forall\ i, j$.

Como a base β é evidentemente L.I., então temos que $\sum_{j=1}^{n} b_{ij}\alpha_j = 0$.

Lembramos que $\sum_{j=1}^{n} b_{ij}\alpha_j$ é um elemento de K. Agora, α é uma base de K, ou seja, $\sum_{j=1}^{n} b_{ij}\alpha_j = 0 \Longrightarrow b_{ij} = 0, \forall\ i, j$.

Dessa forma, $\sum_{\substack{i=1\\j=1}}^{\substack{i=n\\j=m}} b_{ij}\alpha_j\beta_i = 0 \Longrightarrow b_{ij} = 0, \forall\ i, j$. E, consequentemente, $\alpha\beta$ é uma base de L/F. ■

O teorema anterior é de importância inestimável para as discussões teóricas que se seguirão neste trabalho. Podemos notar que há uma espécie de conexão entre este teorema e o **Teorema de Lagrange**, demonstrado no **Capítulo 1**. A seguir, seguem alguns diagramas que servirão de objetos para comparar extensões de corpos e grupos.

Exemplo 72 (A extensão $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$)

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt{2}, \sqrt{3}) & \\
\mathbb{Q}(\sqrt{2}) \arrow[ur, "2"] & \mathbb{Q}(\sqrt{6}) \arrow[u, "2"] & \mathbb{Q}(\sqrt{3}) \arrow[ul, "2"'] \\
 & \mathbb{Q} \arrow[ul, "2"] \arrow[u, "2"] \arrow[ur, "2"'] &
\end{tikzcd}$$

O leitor pode notar a semelhança do diagrama acima com o do grupo V_4, no **Exemplo 29**. Discutiremos essa semelhança mais a fundo no próximo capítulo.
Observe que, naturalmente, $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ e $(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$. Podemos escrever um elemento genérico de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $\mathbb{Q}(\sqrt{2})$ fazendo $g = a + b\sqrt{2} + \sqrt{3}(c + d\sqrt{2})$, o que mostra que

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2.$$

Da mesma forma, chegamos à conclusão de que $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})] = 2$.
A prova da inclusão inversa $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \supseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$, e, consequentemente, $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, é feita no Exemplo 86.

Exemplo 73 (A extensão $\mathbb{Q}(\sqrt[4]{2}, \imath)/\mathbb{Q}$)

$$\begin{tikzcd}
 & & \mathbb{Q} \arrow[dl, "2"'] \arrow[d, "2"] \arrow[dr, "2"] & & \\
 & \mathbb{Q}(\sqrt{2}) \arrow[dl, "2"'] \arrow[d, "2"] \arrow[dr, "2"] & \mathbb{Q}(\imath) \arrow[d, "2"] & \mathbb{Q}(\sqrt{-2}) \arrow[dl, "2"'] \arrow[d, "2"] \arrow[dr, "2"] & \\
\mathbb{Q}(\imath\sqrt[4]{2}) \arrow[drr, "2"] & \mathbb{Q}(\sqrt[4]{2}) \arrow[dr, "2"] & \mathbb{Q}(\sqrt{2}, \imath) \arrow[d, "2"] & \mathbb{Q}((1+\imath)\sqrt[4]{2}) \arrow[dl, "2"'] & \mathbb{Q}((1-\imath)\sqrt[4]{2}) \arrow[dll, "2"'] \\
 & & \mathbb{Q}(\sqrt[4]{2}, \imath) & &
\end{tikzcd}$$

Este diagrama é muito similar ao reticulado do grupo D_8, no **Exemplo 55**. Observe que todas os índices são iguais a 2, o que difere os dois reticulados é apenas o sentido das setas e os objetos que são comparados.

2.2 Polinômios e Extensões de corpos

Uma grande motivação para se estudar polinômios é que suas raízes podem estar ou não no corpo ou anel dos seus coeficientes. Quando não estão, podemos utilizar o conjunto gerado pelas raízes como uma extensão de corpos, como veremos mais adiante.

Definição 74 (Polinômios em um corpo K) *Seja K um corpo e $a_i \in K, \forall\, i \in \mathbb{N}$. Definimos então $p(x) = \sum_{i=0}^{n} a_i x^i$ como um polinômio com coeficientes em K.*

O grau do polinômio é definido como a maior potência n de x tal que $a_n \neq 0$ e será denotado por ∂p.

Se K/F é uma extensão de corpos, então dizemos que $\alpha \in K$ é algébrico sobre F se α é raiz de algum polinômio (não nulo) sobre F. Se α não é algébrico sobre F então diremos que é transcendente.
Além disso, a extensão K/F é dita algébrica se todo elemento de K for algébrico sobre F.
Note que, com a exceção de $\mathbb{R}$, todas as outras extensões sobre $\mathbb{Q}$, dos exemplos deste trabalho, são algébricas sobre $\mathbb{Q}$. Note ainda que $\mathbb{C}/\mathbb{R}$ é uma extensão algébrica.

Definição 75 (Polinômios mônicos) *Um polinômio $p(x) = \sum_{i=0}^{n} a_i x^i$ é dito mônico quando $a_n = 1$.*

Polinômios mônicos são de suma importância pois, além de simplificar as contas, qualquer polinômio não mônico, sobre um corpo, é gerado por um polinômio mônico.

Exemplo 76 (Alguns polinômios mônicos) *Os polinômios a seguir são mônicos.*

i) $p(x) = x^2 + 1$;

ii) $p(x) = x^2 - 2$;

iii) $p(x) = x^4 - 10x^2 + 1$;

iv) $p(x) = x^2 - 3$;

Observação 77 *Seja K/F uma extensão de corpos. Para cada $\alpha \in K$ algébrico sobre F, existe um único polinômio mônico sobre K tal que α é raiz.*

A prova da observação anterior se deve ao fato de que K é um corpo e que podemos efetuar a divisão euclidiana em $F[x]$ (conjunto dos polinômios com coeficientes em F). Entretanto, por fugir um pouco do objetivo, a demonstração não será feita aqui.
O polinômio encontrado na **Observação 77** será chamado de polinômio minimal de α e será denotado por $p_\alpha(x)$.
Como dito anteriormente, podemos usar as raízes de um polinômio que não estão no corpo dos coeficientes para "fazer" uma extensão de corpos. Observe que se α é raiz de um polinômio $p(x)$ então, $p_\alpha(x)$ divide $p(x)$. Agora, como sabemos, α pode não pertencer ao corpo base, o que nos sugere que $p_\alpha(x)$ é um polinômio com coeficientes na extensão. Se para todo elemento do corpo base não houver um polinômio que possa dividir $p(x)$ (além de $p(x)$ e polinômios constantes), então diremos que $p(x)$ é *irredutível* sobre o corpo base.

Diremos que p divide d, e denotaremos por $p \mid d$, quando dados p e d, elementos de um corpo K ou polinômios em $K[x]$, existe um q (elemento de K ou de $K[x]$, respectivamente) tal que $d = pq$. Caso contrário, diremos que p não divide d e denotaremos por $p \nmid d$. A seguir, um resultado que nos ajudará a encontrar polinômios irredutíveis sobre $\mathbb{Q}$.

Teorema 78 (Critério de Eisenstein) *Seja $f(x) = \sum_{i=0}^{n} a_i x^i$ um polinômio em $\mathbb{Z}[x]$. Suponha que exista um número inteiro p, primo, tal que:*

i) $p \nmid a_n$;

ii) $p \mid a_0, a_1, a_2, ..., a_{n-1}$;

iii) $p^2 \nmid a_0$;

Então $f(x)$ é irredutível sobre $\mathbb{Q}$.

Exemplo 79 *O polinômio $p(x) = x^2 + 1$ é irredutível sobre $\mathbb{R}$.*

Exemplo 80 *Os polinômios $p(x) = x^2 - 2$ e $q(x) = x^2 - 3$ são irredutíveis sobre $\mathbb{Q}$.*

Exemplo 81 *O polinômio $p(x) = x^2 - 3$ é irredutível sobre $\mathbb{Q}(\sqrt{2})$.*

Exemplo 82 *O polinômio $p(x) = x^3 + x + 1$ é irredutível sobre $\mathbb{Z}_2$.*

Observe que se um polinômio não é irredutível, isto é, redutível, então podemos decompô-lo no corpo base sem precisar de coeficientes de qualquer extensão.

2.2.1 Extensões normais

Quando temos polinômios com coeficientes em um corpo, uma pergunta natural a ser feita pode ser: "Aonde podemos encontrar as raízes deste polinômio?". Como vimos, polinômios irredutíveis possuem raízes em alguma extensão.

Definição 83 (Corpo de decomposição de um polinômio) *A extensão K/F é dita corpo de decomposição de um polinômio $f(x) \in F[x]$ se f é completamente fatorado (ou seja, pode ser escrito como produto de polinômios de grau 1) em $K[x]$, e, além disso, K/F é a menor extensão com essa propriedade.*

Basicamente, o corpo de decomposição de um polinômio é uma extensão que contêm todas as raízes e qualquer extensão própria desta não contêm todas as raízes do polinômio.
Por exemplo, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ é o corpo de decomposição de $p(x) = (x^2 - 2)(x^2 - 3)$, entretanto, $\mathbb{Q}(\sqrt{2})$, que é apenas uma extensão própria não possui todas as raízes de p.

Observação 84 *Se K/F é uma extensão algébrica e corpo de decomposição de uma coleção de polinômios $f(x) \in F[x]$, então K/F é dita extensão normal.*

Exemplo 85 (Números complexos) *A extensão $\mathbb{C}/\mathbb{R}$ é uma extensão normal. Observe ainda que $\mathbb{C} = \mathbb{R}(\imath)$.*

O exemplo acima nos diz basicamente que $\mathbb{C}$ é o corpo de decomposição de $p(x) = x^2 + 1$. É importante observar que $\mathbb{C} = \mathbb{R}(1 + \imath)$. Ou seja, a extensão $\mathbb{C}/\mathbb{R}$ possui todas as combinações lineares de números reais com as raízes de p, sendo assim, mudar o gerador não alterará a extensão desde que o novo gerador seja combinação linear dos outros.
Basicamente, podemos ter mais de 1 polinômio com a mesma extensão normal do que outro.

Exemplo 86 (Extensão sobre $\mathbb{Q}$) *Vamos mostrar que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.*

Observe que $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ é o corpo de decomposição de $p(x) = (x^2 - 2)(x^2 - 3)$. Olhando agora para o polinômio

$$q(x) = [x - (\sqrt{2} + \sqrt{3})][x + (\sqrt{2} + \sqrt{3})][x - (\sqrt{2} - \sqrt{3})][x + (\sqrt{2} - \sqrt{3})] = x^4 - 10x^2 + 1$$

temos, por **Eisenstein**, que $q(x)$ é irredutível sobre $\mathbb{Q}$. Ou seja, p e q tem o mesmo corpo de decomposição. Como $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ e $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{6})] = 2$, basta mostrar então que $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}(\sqrt{6})] = 2$. E, de fato, o polinômio $q_1(x) = [x-(\sqrt{2}+\sqrt{3})][x+(\sqrt{2}+\sqrt{3})] = x^2 - 5 - 2\sqrt{6}$ é irredutível sobre $\mathbb{Q}(\sqrt{6})$ e suas raízes pertencem a extensão $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \supset \mathbb{Q}(\sqrt{6})$, e como $\sqrt{6} = \frac{(\sqrt{2}+\sqrt{3})^2-5}{2}$, temos que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Exemplo 87 (Extensões com radicais e $\imath$) *O polinômio $m(x) = x^3 - 2$ pode ser completamente fatorado no corpo $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, onde ζ_3 é uma raiz terça da unidade.*

Um resultado que ajuda a visualizar este fato é o ***Teorema Fundamental da Álgebra***, que diz que qualquer polinômio de grau n, sobre os complexos, possui exatamente n raízes (observando-se também a questão da multiplicidade de uma raiz). De fato, m possui três raízes: $\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2}$, onde $\zeta_3 = \frac{1+\imath\sqrt{3}}{2}$ é uma raiz terça da unidade. A importância deste exemplo reside na observação de que $\mathbb{Q}(\sqrt[3]{2})$ não é o corpo de decomposição de m. Também, notamos que $[\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}] = 6$, pois

$$\mathbb{Q}(\sqrt[3]{2}, \zeta_3) = \{a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 + d\zeta_3 + e\zeta_3\sqrt[3]{2} + f\zeta_3\sqrt[3]{2}^2 \mid a, b, c, d, e, f \in \mathbb{Q}\}$$

.

Observe que $\zeta_3^2 = 1 - \zeta_3$ não aparece como gerador por ser combinação linear dos geradores.

Logo mais, o reticulado que representa a extensão de corpos do exemplo anterior.

$$\begin{tikzcd}
 & \mathbb{Q} \arrow[dl, "2"'] \arrow[dr, "3"] \arrow[drr, "3"] \arrow[drrr, "3"] & & & \\
\mathbb{Q}(\zeta_3) \arrow[dr, "3"'] & & \mathbb{Q}(\sqrt[3]{2}) \arrow[dl, "2"] & \mathbb{Q}(\zeta_3\sqrt[3]{2}) \arrow[dll, "2"] & \mathbb{Q}(\zeta_3^2\sqrt[3]{2}) \arrow[dlll, "2"] \\
 & \mathbb{Q}(\sqrt[3]{2}, \zeta_3) & & &
\end{tikzcd}$$

Novamente, podemos ver a semelhança entre um reticulado de extensões de corpos e um reticulado de grupos. Neste caso, o reticulado mostrado no **Exemplo 56**, *de* S_3, tem o mesmo formato do que este, o que muda é apenas o conteúdo do reticulado. Até mesmo os índices dos grupos "coincidem" com os graus das extensões.

2.2.2 Extensões separáveis

Nesta sessão, definiremos e discutiremos alguns resultados sobre *Extensões Separáveis*. A discussão teórica agora é voltada para saber qual a multiplicidade das raízes de polinômios em uma extensão de corpos. Tal análise nem sempre é considerada tão natural quanto a da sessão passada, mas é de igual importância para a discussão dos resultados principais.
Utilizaremos recursos como a derivada de um polinômio, que aparece frequentemente no cálculo. Entretanto, a definição dada a seguir não é feita com base em pontos de acumulação, ou seja, sequer temos uma topologia definida, trata-se apenas de uma fórmula.

Definição 88 (Derivada de um polinômio) *Seja* $f(x) = \sum_{i=0}^{n} a_i x^i \in F[x]$ *um polinômio. A derivada de* f *é definida por*

$$D_x f(x) = \sum_{i=1}^{n} i a_i x^{i-1} \in F[x].$$

São válidas as regras de derivação usuais do cálculo que podem ser provadas de forma direta e não requerem a utilização de limites.No decorrer do trabalho, poderemos também usar a notação f' para a derivada de f. Por enquanto, apenas definimos a derivada, seu uso se dará mais adiante nesta mesma sessão, visto que mais algumas definições se fazem necessárias.

Exemplo 89 (Derivadas em $\mathbb{Q}$ e $\mathbb{Z}_2$) *Polinômios sobre* $\mathbb{Q}$*:*

i) $p(x) = x^2 + 1$*, cuja derivada é* $p'(x) = 2x$*;*

ii) $p(x) = x^2 - 2$*, cuja derivada é* $p'(x) = 2x$*;*

iii) $p(x) = x^4 - 10x^2 + 1$*, cuja derivada é* $p'(x) = 4x^3 - 20x$*;*

iv) $p(x) = x^2 - 3$, *cuja derivada é* $p'(x) = 2x$;

Polinômios sobre $\mathbb{Z}_2$:

i) $p(x) = x^2 + 1$, *cuja derivada é* $p'(x) = 2x = 0$;

ii) $p(x) = x^2 - 2$, *cuja derivada é* $p'(x) = 2x = 0$;

iii) $p(x) = x^4 - 10x^2 + 1$, *cuja derivada é* $p'(x) = 4x^3 - 20x = 0$;

iv) $p(x) = x^3 - 3$, *cuja derivada é* $p'(x) = 3x^2 = x^2$;

De maneira geral, a derivada de qualquer polinômio da forma x^p, no corpo $\mathbb{Z}_p$, é o polinômio identicamente nulo.

Definição 90 (Polinômios Separáveis) *Um polinômio* $p(x) \in F[x]$ *é dito separável se todas as suas raízes são distintas.*

Observe que não especificamos o corpo de decomposição do polinômio, isso se deve ao fato de que a definição dada independe da normalidade da extensão.
Caso o polinômio não seja separável, dizemos que o mesmo é inseparável.

Definição 91 (Extensão Separável) *Seja* K/F *uma extensão de corpos. Dizemos que o corpo* K *é separável sobre* F *se todo elemento de* K *for raiz de um polinômio separável* $p(x) \in F[x]$.

De forma equivalente, K/F é separável se, $\forall\ \alpha \in K$, temos que $p_\alpha(x) \in F[x]$ é separável.
Quando uma extensão não é separável, diremos que a mesma é inseparável.

A ideia aqui é utilizar a derivada de um polinômio para determinar se o mesmo é separável ou não. Para isso, utilizaremos o máximo divisor comum (M.D.C.) de polinômios que será denotado por $(p(x), q(x))$, onde p e q são polinômios com coeficientes em algum corpo F. Podemos caracterizar um polinômio separável da seguinte maneira.

Teorema 92 (Caracterização de polinômios separáveis) *Um polinômio* $p(x)$ *é separável se, e somente se, é relativamente primo à sua derivada. Ou seja,*

$$(p(x), p'(x)) = 1$$

Demonstração:

($\Longrightarrow$) Seja $p(x) = (x-\alpha)^n g(x)$ um polinômio com coeficientes no seu corpo de decomposição K. Observe que o número n é a multiplicidade da raiz α. Agora, analisando a derivada de p temos:

$$p'(x) = [(x-\alpha)^n g(x)]' \Longrightarrow p'(x) = n(x-\alpha)^{n-1}g(x) + (x-\alpha)^n g'(x)$$

Note que se $n > 1$, podemos reescrever a igualdade acima e considerar a multiplicidade de α em p'.

$$p'(x) = (x-\alpha)[n(x-\alpha)^{n-2}g(x) + (x-\alpha)^{n-1}g'(x)]$$

Ou seja, α também é raiz de p', e, consequentemente, $p_\alpha(x)$ divide p' e p. Portanto, se α tem multiplicidade maior do que 1, p e p' não são primos entre si.

($\Longleftarrow$) Para mostrar a volta, suponhamos que $p(x) = (x-\alpha)g(x)$ e $p'(x) = (x-\alpha)g_1(x)$. Vamos mostrar que α é uma raiz de p com multiplicidade maior do que 1. Temos:

$$p'(x) = g(x) + (x-\alpha)g'(x) = (x-\alpha)g_1(x)$$

Agora, α é raiz de p', portanto, $g(\alpha) = 0 \Longrightarrow g(x) = (x-\alpha)h(x)$. Substituindo em p :

$$p(x) = (x-\alpha)^2 h(x)$$

O que mostra que α possui multiplicidade maior ou igual a 2, como queríamos demonstrar. ■

Exemplo 93 (Polinômios separáveis)

i) Todos os polinômios do Exemplo 89, com derivada diferente de zero, são separáveis;

ii) O polinômio $x^8 - 2$ é separável sobre $\mathbb{Q}$;

ii) O polinômio $(x^2-2)(x^2-3)$ é separável sobre $\mathbb{Q}$;

Mais um bom motivo para analisar corpos de característica igual a 0 é apresentado no teorema a seguir. A sua demonstração é feita basicamente usando o **Teorema 92**.

Teorema 94 (Polinômios irredutíveis em corpos de característica igual a 0) *Seja $p(x) \in F[x]$ um polinômio irredutível. Se F é um corpo de característica 0, então $p(x)$ é separável. Em particular, qualquer polinômio irredutível sobre $\mathbb{Q}$ é separável. Além disso, qualquer polinômio que é produto de polinômios irredutíveis e distintos em $F[x]$ é separável.*

Demonstração:

Se p é irredutível sobre F, então, a menos de constantes, apenas $p(x)$ e 1 podem dividir p, logo $(p(x), p'(x)) = 1$.
A segunda parte do teorema segue do fato de que polinômios irredutíveis e distintos não possuem raízes em comum, e, portanto, a derivada do produto dos mesmos é relativamente prima ao produto. ■

Agora temos uma garantia de que polinômios irredutíveis sobre $\mathbb{Q}$ são separáveis. Além disso, o produto de polinômios irredutíveis também é separável. A seguir, veremos alguns exemplos de polinômios e extensões separáveis e não separáveis também.

Exemplo 95 (O corpo $\mathbb{Z}_2$) *O polinômio $f(x) = x^2 + 1$ não é separável sobre $\mathbb{Z}_2$. Observe que a derivada de f é igual a zero.*

Em geral, qualquer polinômio da forma $x^p + 1$ sobre um corpo de característica p não é separável, uma vez que a sua derivada é igual a 0.

Exemplo 96 (Números complexos) *O polinômio $f(x) = x^2 + 1$ é separável sobre $\mathbb{C}/\mathbb{R}$. Observe que podemos escrevê-lo na forma $(x+\imath)(x-\imath)$.*

Basicamente, $\mathbb{C}/\mathbb{R}$ é uma extensão separável.

Capítulo 3

Elementos da Teoria de Galois

Este capítulo é destinado à discussão dos resultados que são o foco deste trabalho. Aqui procuraremos deixar bem claro as relações existentes entre os diagramas de extensões de corpos e os reticulados de grupos. A teoria básica aqui discutida é consequência das discussões dos capítulos anteriores.

3.1 Automorfismos em extensões de corpos

Nesta primeira sessão, faremos algumas definições básicas e discutiremos o comportamento de tipos específicos de automorfismos.

Definição 97 (Automorfismos em corpos) *Seja K/F uma extensão de corpos. A função $\phi : K \longrightarrow K$ é dita um automorfismo se é um homomorfismo bijetor sobre K. O conjunto de automorfismos de K será denotado por $Aut(K)$.*

Basicamente, vamos dar especial atenção a automorfismos sobre K que restritos ao subcorpo F são a identidade. Ou seja, automorfismos que não alteram os elementos do corpo F. A esse conjunto de automorfismos denotaremos por $Aut(K/F)$.
Agora, devido à restrições, o conjunto $Aut(K/F)$ possui características notáveis.

i) O conjunto $Aut(K/F)$ é um grupo com a operação composição;

ii) Seja $f(x) = \sum_{i=0}^{n} a_i x^i \in F[x]$ e $\sigma \in Aut(K/F)$. Observe que como cada a_i pertence ao corpo F: $\sigma(f(x)) = f(\sigma(x))$. Agora, como as raízes de f não são indeterminadas e sim números, quando K for o corpo de decomposição de f, então σ apenas permuta as raízes de f. Uma forma de ver isso é que, pelas relações de Girard, os coeficientes de f podem ser escritos através de relações entre as raízes. Por exemplo, se f for de grau 2 e mônico, então:

$$a_0 = u_1 u_2$$
$$-a_1 = u_1 + u_2$$

Onde os u_i's são as raízes de f.
Assim, cada a_i pode ser escrito como polinômios simétricos nas raízes de f. Ou seja, aplicar σ apenas permuta as raízes:

$$f(x) = \prod_{i=1}^{n}(x - u_i) \Longrightarrow \sigma(f(x)) = \prod_{i=1}^{n}(\sigma(x) - \sigma(u_i))$$

Pelo produtório, podemos ver que o novo polinômio terá o mesmo grau e as mesmas raízes que f. A observação a seguir demonstra o que discutimos.

Observação 98 *Seja K/F uma extensão de corpos onde $\theta \in K$ é algébrico sobre F. Então, para qualquer automorfismo $\alpha \in Aut(K/F)$, $\alpha(\theta)$ é uma raiz do polinômio mínimo de θ sobre F.*

Demonstração:

Suponha que θ é raiz de um polinômio:

$$\sum_{i=0}^{n} a_i\theta^i = 0, \text{ onde } a_i \in F, \ \forall\ i = 1, 2..., n$$

Agora, usando o fato de que α é um automorfismo sobre K, temos:

$$\alpha(\sum_{i=0}^{n} a_i\theta^i) = \alpha(0) \Longrightarrow \sum_{i=0}^{n} \alpha(a_i)\alpha(\theta)^i = 0$$

Como $\alpha(a_i) = a_i$, então $\sum_{i=0}^{n} a_i\alpha(\theta)^i = 0$. Agora, isso significa que $\alpha(\theta)$ também é raiz do mesmo polinômio, como queríamos demonstrar. ■

Agora, é válido ressaltar que nem todas as permutações são aceitas, por exemplo, se considerarmos a extensão $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$, que é corpo de decomposição do polinômio $p(x) = (x^2-2)(x^2-3)$, uma boa pergunta é:

"Será que existe algum automorfismo σ que permuta $\sqrt{2}$ e $\sqrt{3}$ sem modificar o corpo base?"

A resposta é não. Para mostrar, basta supor que exista tal automorfismo. No corpo base, $\sigma(2) = 2$, agora, $\sigma(2) = \sigma(\sqrt{2}\sqrt{2}) = \sigma(\sqrt{2})\sigma(\sqrt{2}) = \sqrt{3}\sqrt{3} = 3$.
Ou seja, σ não é a identidade quando restrito ao corpo base.

Em geral, descobrir quais os tipos de permutações permitidas não é uma tarefa fácil. Notamos que, para o polinômio p, as permutações permitidas entre suas raízes podem ser as seguintes:

$$Id : \left\{ \begin{array}{ccc} \sqrt{2} & \longmapsto & \sqrt{2} \\ \sqrt{3} & \longmapsto & \sqrt{3} \end{array} \right. ; \quad \sigma : \left\{ \begin{array}{ccc} \sqrt{2} & \longmapsto & -\sqrt{2} \\ \sqrt{3} & \longmapsto & \sqrt{3} \end{array} \right. ; \quad \beta : \left\{ \begin{array}{ccc} \sqrt{2} & \longmapsto & \sqrt{2} \\ \sqrt{3} & \longmapsto & -\sqrt{3} \end{array} \right. ; \quad \sigma \circ \beta : \left\{ \begin{array}{ccc} \sqrt{2} & \longmapsto & -\sqrt{2} \\ \sqrt{3} & \longmapsto & -\sqrt{3} \end{array} \right.$$

Observe que, neste caso, $Aut(K/F) \cong V_4$ que é o grupo de Klein de ordem 4. Como pode ser facilmente comprovado, o grupo é comutativo e qualquer elemento que não seja a identidade é de ordem 2, e é gerado por σ e β. O leitor já deve estar familiarizado com os reticulados de V_4 e da extensão $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$, abaixo temos ambos:

$$\begin{tikzcd}
 & \{Id\} \arrow[dl, "2"'] \arrow[d, "2"'] \arrow[dr, "2"] & \\
< \beta > \arrow[dr, "2"'] & < \sigma\beta > \arrow[d, "2"'] & < \sigma > \arrow[dl, "2"] \\
 & V_4 &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \mathbb{Q}(\sqrt{2},\sqrt{3}) & \\
\mathbb{Q}(\sqrt{2}) \arrow[ur, "2"] & \mathbb{Q}(\sqrt{6}) \arrow[u, "2"] & \mathbb{Q}(\sqrt{3}) \arrow[ul, "2"'] \\
 & \mathbb{Q} \arrow[ul, "2"] \arrow[u, "2"] \arrow[ur, "2"'] &
\end{tikzcd}$$

Agora, observe que o automorfismo σ "fixa" o corpo $\mathbb{Q}(\sqrt{3})$. Mais ainda, os subgrupos de V_4 tem seus respectivos "corpos fixos" na extensão de corpos dada. Obviamente, a única permutação que fixa o corpo $\mathbb{Q}(\sqrt{2},\sqrt{3})$ é a identidade e quanto maior o corpo, menos permutações poderemos fazer, ou seja, as setas nos diagramas estão em sentidos opostos se compararmos os subgrupos que fixam os corpos.

O interessante é que a composição fixa exatamente o corpo $\mathbb{Q}(\sqrt{6})$ que é a multiplicação de $\sqrt{2}$ e $\sqrt{3}$, de fato, se $x \in \mathbb{Q}(\sqrt{6})$, então

$$\psi(x) = (\sigma \circ \beta)(x) = \psi(a + b\sqrt{6}) = a + b\psi(\sqrt{2}\sqrt{3}), \text{ logo}$$
$$\psi(x) = a + b(-\sqrt{2})(-\sqrt{3}) \Longrightarrow \psi(x) = x$$

Por certo, a simetria deste reticulado dificulta um pouco a visualização, não fica tão clara a posição dos subgrupos em relação aos corpos fixados. No exemplo a seguir essa relação fica mais clara.

Exemplo 99 (A extensão $\mathbb{Q}(\sqrt[3]{2},\zeta_3)/\mathbb{Q}$) *Conforme vimos no Exemplo 87, essa é uma extensão de grau* 6 *e suas raízes são formadas considerando-se as raízes terças da unidade.*

Olhando para os automorfismos desta extensão, procuramos saber o que acontece com as raízes de $m(x) = x^3 - 2$. Observe que não necessariamente devemos olhar apenas para os geradores, mas podemos saber o que acontece com as raízes através dos geradores:

$$\phi : \begin{cases} \sqrt[3]{2} & \longmapsto & \zeta_3^i\sqrt[3]{2} \\ \imath & \longmapsto & \imath \end{cases} ; \quad \gamma : \begin{cases} \sqrt[3]{2} & \longmapsto & \sqrt[3]{2} \\ \imath & \longmapsto & -\imath \end{cases}, \quad \text{onde } i \in \{0,1,2\} \text{ e } \zeta_3^3 = 1.$$

Agora, vamos descobrir o que acontece com $\zeta_3 = \frac{-1+\imath\sqrt{3}}{2}$:

$$\phi(\zeta_3) = \zeta_3$$
$$\gamma(\zeta_3) = \frac{-1-\imath\sqrt{3}}{2} = \zeta_3^2$$

Podemos acrescentar então as raízes terças da unidade:

$$\phi : \begin{cases} \sqrt[3]{2} & \longmapsto & \zeta_3^i\sqrt[3]{2} \\ \imath & \longmapsto & \imath \\ \zeta_3 & \longmapsto & \zeta_3 \end{cases} ; \quad \gamma : \begin{cases} \sqrt[3]{2} & \longmapsto & \sqrt[3]{2} \\ \imath & \longmapsto & -\imath \\ \zeta_3 & \longmapsto & \zeta_3^2 \end{cases}$$

Note que $\phi^3 = Id$ e $\gamma^2 = Id$, ainda $\phi^2\gamma = \gamma\phi$. Considerando as raízes no plano complexo, ϕ é uma rotação de $\frac{2\pi}{3}$ no triângulo formado pelas raízes, no sentido anti-horário e γ é uma reflexão sobre o eixo real, ou seja, a conjugação. Com todas essas características, percebemos claramente que $Aut(\mathbb{Q}(\sqrt[3]{2},\zeta_3)/\mathbb{Q}) \cong S_3 \cong D_6$, que corresponde aos movimentos rígidos, ou permutações, dos vértices de um triângulo (Exemplo 4 do Capítulo 1).

Novamente, compararemos a extensão de corpos e o grupo de automorfismos pelos reticulados.

$$\begin{tikzcd}
 & S_3 & & & \\
< \phi > \arrow[ur, "2"] & & & & \\
 & < \gamma > \arrow[uul, "3"] & < \gamma\phi > \arrow[uul, "3"] & < \gamma\phi^2 > \arrow[uul, "3"] & \\
< 1 > \arrow[uul, "3"] \arrow[ur, "2"] \arrow[urr, "2"] \arrow[urrr, "2"] & & & &
\end{tikzcd}$$

$$\begin{tikzcd}
 & \mathbb{Q} \arrow[dl, "2"'] \arrow[ddr, "3"] \arrow[ddrr, "3"] \arrow[ddrrr, "3"] & & & \\
\mathbb{Q}(\zeta_3) \arrow[ddr, "3"'] & & & & \\
 & \mathbb{Q}(\sqrt[3]{2}) \arrow[dl, "2"] & \mathbb{Q}(\zeta_3\sqrt[3]{2}) \arrow[dll, "2"] & \mathbb{Q}(\zeta_3^2\sqrt[3]{2}) \arrow[dlll, "2"] & \\
\mathbb{Q}(\sqrt[3]{2}, \zeta_3) & & & &
\end{tikzcd}$$

Vamos utilizar o formato de um elemento $x \in \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ para ver os corpos fixados pelos automorfismos, como os subcorpos são gerados pelas raízes, também necessitaremos de outros formatos para descobrir o que acontece com os geradores de cada subcorpo próprio, os elementos sublinhados são exatamente os que foram fixados pelo respectivo automorfismo:

i) $\phi(x) = \phi(a+b\sqrt[3]{2}+c\sqrt[3]{2}^2+d\zeta_3+e\zeta_3\sqrt[3]{2}+f\zeta_3\sqrt[3]{2}^2) = \underline{a}+b\zeta_3\sqrt[3]{2}+c\zeta_3^2\sqrt[3]{2}^2+\underline{d\zeta_3}+e\zeta_3^2\sqrt[3]{2}+f\sqrt[3]{2}^2$;

ii) $\gamma(x) = \underline{a + b\sqrt[3]{2} + c\sqrt[3]{2}^2} + d\zeta_3^2 + e\zeta_3^2\sqrt[3]{2} + f\zeta_3^2\sqrt[3]{2}^2$;

iii) $\gamma(\phi(x)) = \underline{a} + b\zeta_3^2\sqrt[3]{2} + c\zeta_3\sqrt[3]{2}^2 + d\zeta_3^2 + \underline{e\zeta_3\sqrt[3]{2}} + f\sqrt[3]{2}^2$;

iv) $\phi^2(x) = \underline{a} + b\zeta_3^2\sqrt[3]{2} + c\zeta_3\sqrt[3]{2}^2 + \underline{d\zeta_3} + e\sqrt[3]{2} + f\zeta_3^2\sqrt[3]{2}^2$;

v) $\gamma(\phi^2(x)) = \underline{a} + b\zeta_3\sqrt[3]{2} + c\zeta_3^2\sqrt[3]{2}^2 + d\zeta_3^2 + e\sqrt[3]{2} + \underline{f\zeta_3\sqrt[3]{2}^2}$;

vi) $\phi(a + b\zeta_3\sqrt[3]{2} + c\zeta_3^2\sqrt[3]{2}^2) = \underline{a} + b\zeta_3^2\sqrt[3]{2} + c\zeta_3\sqrt[3]{2}^2$;

vii) $\gamma(a + b\zeta_3\sqrt[3]{2} + c\zeta_3^2\sqrt[3]{2}^2) = \underline{a} + b\zeta_3^2\sqrt[3]{2} + c\zeta_3\sqrt[3]{2}^2$;

viii) $\gamma(\phi(a + b\zeta_3\sqrt[3]{2} + c\zeta_3^2\sqrt[3]{2}^2)) = \underline{a + b\zeta_3\sqrt[3]{2} + c\zeta_3^2\sqrt[3]{2}^2}$;

ix) $\gamma(\phi^2(a + b\zeta_3^2\sqrt[3]{2} + c\zeta_3\sqrt[3]{2}^2)) = \underline{a + b\zeta_3^2\sqrt[3]{2} + c\zeta_3\sqrt[3]{2}^2}$;

Necessariamente, se um automorfismo σ fixa um corpo, então qualquer automorfismo do tipo σ^n também fixará o corpo. Além disso, se dois automorfismos fixam um corpo, a composição dos mesmos também o fará. Sendo assim, basta olharmos para os geradores dos subgrupos e não precisamos nos preocupar em calcular para todos os elementos gerados.

Observamos então que, se um automorfismo fixa um corpo, evidentemente ele fixará os geradores. A volta também é válida, pois qualquer elemento do corpo é obtido a partir de combinações lineares. Sendo assim, os itens *vi*), *vii*), *viii*) e *ix*) podem ser deduzidos a partir dos itens anteriores. Agora, o cálculo feito, mostra que, de fato, existem subcorpos que são fixados.

Para discutir melhor o que foi feito, faremos uma comparação entre os automorfismos e os corpos fixados nos itens acima.

Subgrupos de S_3	Corpos fixados
$< 1 >$	$\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$
$< \phi >$	$\mathbb{Q}(\zeta_3)$
$< \gamma >$	$\mathbb{Q}(\sqrt[3]{2})$
$< \gamma\phi >$	$\mathbb{Q}(\zeta_3 \sqrt[3]{2})$
$< \gamma\phi^2 >$	$\mathbb{Q}(\zeta_3^2 \sqrt[3]{2})$
S_3	$\mathbb{Q}$

Tabela 3.1: Subgrupos de S_3 e corpos fixados da extensão $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$

É importante perceber que, nos reticulados, os subgrupos e seus respectivos corpos fixados estão em "posições" similares e que determinadas composições em subcorpos são fixadas por, respectivamente, determinadas composições de elementos em S_3. A observação a seguir resume parte do que foi discutido nesta sessão.

Observação 100 (Subgrupos de automorfismos) *Seja K/F uma extensão de corpos e $Aut(K)$ o grupo de automorfismos sobre K. Então, o conjunto H de automorfismos que fixam um subcorpo $F \subseteq E \subseteq K$ é um subgrupo de $Aut(K)$.*

Demonstração:

i) Dado $a \in E$, $\exists\, 1_K \in Aut(K)$, tal que $1_K(b) = b$, $\forall\, b \in K$, em particular, $1_K(a) = a$, $\forall\, a \in E$. Logo, $1_K \in H$.

ii) Dados $\alpha, \beta \in H$, temos $(\alpha \circ \beta)(a) = \alpha(\beta(a)) = \alpha(a) = a$, $\forall\, a \in E$. Logo, $\alpha \circ \beta \in H$.

iii) Se $\alpha \in H$, automorfismo sobre o corpo K, sabemos que existe α^{-1}, que é a função inversa de α e também um automorfismo sobre K. Vamos mostrar que $\alpha^{-1} \in H$. Observe que $\alpha(a) = a$, $\forall\, a \in E$, o que nos diz que $\alpha^{-1}(a) = a$ e, consequentemente, $\alpha^{-1} \in H$. ■

3.2 A Correspondência de Galois

Vamos discutir agora as relações existentes entre os automorfismos que fixam um corpo dentro de uma extensão e os subcorpos existentes na extensão.

Observação 101 *Seja $H \leq Aut(K)$ um subgrupo do grupo de automorfismos sobre K. Então a coleção F de elementos de K fixados por todos os elementos de H é um subcorpo de K.*

Demonstração:

Seja $h \in H$ e $a, b \in F$. Por definição, $h(a) = a$ e $h(b) = b$, então $h(a+b) = h(a)+h(b) = a+b$ e $h(ab) = h(a)h(b) = ab$. Além disso, $h(a^{-1}) = h(a)^{-1} = a^{-1}$.

Evidentemente, como H é automorfismo, H fixa a unidade e o elemento zero. Portanto, F é um corpo. ■

Observe que em nenhum momento foi utilizado o fato de H ser um subgrupo. E, de fato, a observação anterior vale para qualquer subconjunto de $Aut(K)$.
Se $G = Aut(K/F)$ e $H \leq G$, denotaremos então o corpo fixo de H em K, por apenas K_H.Assim, no Exemplo 99, temos:

- $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)_{<\phi>} = \mathbb{Q}(\zeta_3)$;
- $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)_{<1>} = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$;
- $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)_{S_3} = \mathbb{Q}$;

O próximo resultado é relativamente intuitivo observando-se os reticulados dos grupos de automorfismos e das extensões de corpos.

Teorema 102 (Relação de inclusão inversa) *Sejam $F_1 \subseteq K$ e $F_2 \subseteq K$ uma extensão de corpos e $H_1 \leq H_2 \leq Aut(K)$ subgrupos de automorfismos de K. Temos então:*

i) Se $F_1 \subseteq F_2$, então $Aut(K/F_2) \leq Aut(K/F_1)$;

ii) Se F_1 é o corpo fixo de H_1 e F_2 é o corpo fixo de H_2, então $F_2 \subseteq F_1$;

Demonstração:

Para mostrar o item i), observe que qualquer automorfismo que fixa F_2 também fixa F_1, pois F_1 é um subconjunto de F_2. Logo, $Aut(K/F_2) \leq Aut(K/F_1)$.
Para mostrar o item ii), dado um elemento de $x \in F_2$ e $h_1 \in H_1$, temos que $h_1(x) = x$, pois h_1 também é elemento de H_2. Ou seja, x é um elemento do corpo fixo de H_1, que é, precisamente, F_1. ■

O **Teorema 102** pode ser entendido como "Quanto mais automorfismos menor é o corpo fixo". Podemos observar este fato também olhando para os geradores de um corpo, quanto maior o número de geradores fixados menor é o subgrupo de automorfismos, pois mais restrições são impostas para fixar os elementos do corpo base.

3.2.1 Extensões Galoisianas

No Capítulo 2, falamos sobre extensões normais e extensões separáveis. Vimos que é possível "montar" extensões de corpos à partir de raízes de polinômios irredutíveis sobre o corpo base. Além disso, mostramos que qualquer polinômio irredutível com coeficientes em um corpo de característica zero é separável.
Discutiremos agora sobre extensões que são normais e separáveis. Ou seja, além de possuir as raízes de uma determinada coleção de polinômios, qualquer elemento da extensão é raiz de multiplicidade 1 de algum polinômio com coeficientes no corpo base.

Definição 103 (Extensões Galoisianas) *Seja K/F uma extensão de corpos onde K é o corpo de decomposição de alguma coleção de polinômios separáveis $p(x) \in F[x]$. Dizemos então que K/F é uma extensão galoisiana.*

Equivalentemente, K/F é uma extensão normal e separável. Se K/F é de Galois, denotaremos o conjunto de automorfismos $Aut(K/F)$ por $Gal(K/F)$ e diremos que o mesmo é o grupo de Galois de K/F.

Exemplo 104 (Extensões galoisianas em $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$) *Observamos que as únicas extensões de Galois em $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$ são $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$ e $\mathbb{Q}(\zeta_3)/\mathbb{Q}$.*

Observe que o polinômio $p(x) = x^2 + 3$ é irredutível sobre $\mathbb{Q}$, por **Eisenstein**. Agora, $\mathbb{Q}(\zeta_3)$ é o corpo de decomposição de p, pois $\imath\sqrt{3} = 2\zeta_3 - 1$. Como p é separável, temos que $\mathbb{Q}(\zeta_3)/\mathbb{Q}$ é de Galois.
É importante ressaltar que $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ não é galoisiana, uma vez que $\mathbb{Q}(\sqrt[3]{2})$ não é o corpo de decomposição de $x^3 - 2$.

Exemplo 105 (Extensões galoisianas em $\mathbb{Q}(\sqrt[4]{2}, \imath)/\mathbb{Q}$) *Vamos utilizar polinômios irredutíveis para verificar algumas extensões galoisianas em $\mathbb{Q}(\sqrt[4]{2}, \imath)/\mathbb{Q}$.*

Polinômios irredutíveis	Corpos de decomposição	Corpo base
$x^2 - 2$	$\mathbb{Q}(\sqrt{2})$	$\mathbb{Q}$
$x^2 + 1$	$\mathbb{Q}(\imath)$	$\mathbb{Q}$
$x^2 + 2$	$\mathbb{Q}(\imath\sqrt{2})$	$\mathbb{Q}$
$(x^2 - 2)(x^2 + 1)$	$\mathbb{Q}(\sqrt{2}, \imath)$	$\mathbb{Q}$
$x^4 - 2$	$\mathbb{Q}(\sqrt[4]{2}, \imath)$	$\mathbb{Q}$
$x^2 - \sqrt{2}$	$\mathbb{Q}(\sqrt[4]{2})$	$\mathbb{Q}(\sqrt{2})$

Observe que $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ não é uma extensão galoisiana, entretanto $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ e $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ são extensões galoisianas. Este exemplo mostra que uma extensão galoisiana de outra extensão galoisiana não necessariamente é galoisiana. Note ainda que esta análise é feita olhando-se para o corpo base e as raízes presentes na extensão.
Adiante mostraremos um método mais fácil de achar extensões galoisianas e voltaremos a falar da extensão $\mathbb{Q}(\sqrt[4]{2}, \imath)/\mathbb{Q}$.

3.2.2 O Teorema Fundamental

Na sessão anterior vimos que os automorfismos que fixam corpos dentro de extensões de corpos se comportam de uma certa maneira. A seguir, exploraremos este fato e iremos mostrar o teorema fundamental e resultados que auxiliam na prova do mesmo.
O teorema a seguir é interessante pois, além de relacionar o conteúdo trabalhado até aqui com a álgebra linear, nos informa ainda mais sobre o comportamento de automorfismos.

Teorema 106 (Independência Linear de automorfismos) *Seja $\sigma = \{\sigma_1, \sigma_2, ..., \sigma_n\}$ um conjunto de automorfismos distintos de K, então σ é um conjunto linearmente independente(L.I.).*

Demonstração:
Suponha que σ é um conjunto linearmente dependente (L.D.), ou seja, a combinação linear

$$a_1\sigma_1 + a_2\sigma_2 + ... + a_n\sigma_n = 0 \qquad (1)$$

admite solução não trivial. Agora, podemos escolher então um número mínimo m de coeficientes que são não nulos. Podemos supor, renumerando se necessário, que estes coeficientes são $a_1, a_2, ..., a_m$. Temos ainda que

$$a_1\sigma_1 + a_2\sigma_2 + ... + a_m\sigma_m = 0. \qquad (2)$$

Agora, como cada σ_i é um automorfismo de K, temos que, $\forall\ k \in K$:

$$a_1\sigma_1(k) + a_2\sigma_2(k) + ... + a_m\sigma_m(k) = 0. \qquad (3)$$

Tome $k_0 \in K$ de forma que $\sigma_1(k_0) \neq \sigma_m(k_0)$, o que é possível pois $\sigma_1 \neq \sigma_m$. Como k_0k é um elemento de K, podemos substitui-lo na equação (3), o que nos da

$$a_1\sigma_1(k_0k) + a_2\sigma_2(k_0k) + ... + a_m\sigma_m(k_0k) = 0. \qquad (4)$$

Usando o fato de que σ é um conjunto de automorfismos de K, a equação (4) pode ser reescrita da seguinte forma:

$$a_1\sigma_1(k_0)\sigma_1(k) + a_2\sigma_2(k_0)\sigma_2(k) + ... + a_m\sigma_m(k_0)\sigma_m(k) = 0. \qquad (4')$$

Equivalentemente, multiplicando a equação (3) por $\sigma_m(k_0)$ tem-se:

$$a_1\sigma_m(k_0)\sigma_1(k) + a_2\sigma_m(k_0)\sigma_2(k) + ... + a_m\sigma_m(k_0)\sigma_m(k) = 0. \qquad (3')$$

Fazendo $(3') - (4')$ vem:

$$[\sigma_m(k_0) - \sigma_1(k_0)]a_1\sigma(k) + [\sigma_m(k_0) - \sigma_2(k_0)]a_2\sigma(k) + ... + [\sigma_m(k_0) - \sigma_{m-1}(k_0)]a_{m-1}\sigma(k) = 0,$$

que é uma equação em qualquer $k \in K$. Mas, o primeiro coeficiente, $[\sigma_m(k_0) - \sigma_1(k_0)]a_1$, é diferente de zero. Logo, temos uma relação com menos coeficientes não nulos, o que contraria a minimalidade de m. Portanto, uma contradição. ■

Em particular, o grupo $Aut(K/F)$ é um conjunto L.I.. Vamos utilizar este resultado para provar a relação fundamental entre a ordem de subgrupos de $Aut(K/F)$ e a dimensão de extensões de corpos.

Teorema 107 (Ordem de automorfismos e graus de extensões de corpos) *Seja $G = \{\sigma_1 = 1, \sigma_2, ..., \sigma_n\}$, o subgrupo de automorfismos de um corpo K e seja F o corpo fixo de G. Temos então: $[K : F] = |G| = n$.*

Demonstração:

Primeiro vamos mostrar que n não pode ser maior do que $[K : F]$.
Suponha que $n > [K : F] = m$ e seja $\Omega = \{\omega_1, \omega_2, ..., \omega_m\}$ uma base de K sobre o corpo F. Então, o sistema

$$\begin{cases} \sigma_1(\omega_1)x_1 + \sigma_2(\omega_1)x_2 + \cdots + \sigma_n(\omega_1)x_n = 0 \\ \vdots \\ \sigma_1(\omega_m)x_1 + \sigma_2(\omega_m)x_2 + \cdots + \sigma_n(\omega_m)x_n = 0 \end{cases} \qquad (*)$$

Tem m equações e n indeterminadas, portanto, admite solução não trivial $\beta_1, \beta_2, ..., \beta_n$ em K, pois assumimos que existem mais indeterminadas do que equações.
Sejam $a_1, a_2, ..., a_m \in F$ escalares não nulos. Por hipótese, F é o corpo fixo de G, portanto vale $\sigma_i(a_j) = a_j,\ \forall\ i = 1, 2, ..., n$ e $\forall\ j = 1, 2, ..., m$. Agora, multiplicando cada $j-$ésima equação por a_j, utilizando as propriedades de automorfismos e o fato de que $(*)$ possui solução não trivial, podemos reescrever o sistema $(*)$ da seguinte forma:

$$\begin{cases} \sigma_1(a_1\omega_1)\beta_1 + \sigma_2(a_1\omega_1)\beta_2 + \cdots + \sigma_n(a_1\omega_1)\beta_n = 0 \\ \vdots \\ \sigma_1(a_m\omega_m)\beta_1 + \sigma_2(a_m\omega_m)\beta_2 + \cdots + \sigma_n(a_m\omega_m)\beta_n = 0 \end{cases} \qquad (**)$$

Somando as equações de $(**)$ temos:

$$\sigma_1(a_1\omega_1 + a_2\omega_2 + \cdots + a_m\omega_m)\beta_1 + \cdots + \sigma_n(a_1\omega_1 + a_2\omega_2 + \cdots + a_m\omega_m)\beta_n = 0 \qquad (\star)$$

Agora, Ω é uma base de K sobre F e, consequentemente, todo elemento $\alpha \in K$ é da forma $a_1\omega_1 + a_2\omega_2 + \cdots + a_m\omega_m$. Logo, também podemos interpretar a equação $(\star)$ como sendo

$$\sigma_1(\alpha)\beta_1 + \sigma_2(\alpha)\beta_2 + \cdots + \sigma_n(\alpha)\beta_n = 0 \qquad (\star\star)$$

Finalmente, em $(\star\star)$ temos uma combinação linear dos automorfismos que admite solução não trivial, o que nos diz que G é um conjunto L.D., contradizendo o **Teorema 106**.

Vamos mostrar que n não pode ser menor do que $[K : F]$.
Suponha agora que $n < [K : F]$. Então existem pelo menos $n + 1$ elementos de $K - F$ que são linearmente independentes, digamos $\alpha_1, \alpha_2, ..., \alpha_{n+1}$ satisfazendo o sistema:

$$\begin{cases} \sigma_1(\alpha_1)x_1 + \sigma_1(\alpha_2)x_2 + \cdots + \sigma_1(\alpha_{n+1})x_{n+1} = 0 \\ \vdots \\ \sigma_n(\alpha_1)x_1 + \sigma_n(\alpha_2)x_2 + \cdots + \sigma_n(\alpha_{n+1})x_{n+1} = 0 \end{cases} \qquad (\diamond)$$

Agora, $(\diamond)$ possue n equações e $n+1$ indeterminadas $x_1, x_2, ..., x_{n+1}$ possue solução não trivial $\beta_1, \beta_2, ..., \beta_{n+1}$ em K. Observe que não podemos ter todos os β_i's em F, pois $\sigma_1 = 1$ e na primeira equação teríamos uma combinação linear nula dos α_i's com solução não trivial, o que contraria a independência linear destes. Logo, pelo menos um β_i não é elemento de F.
Dentre todos β_i's, que são solução de $(\diamond)$, escolha um número mínimo r de β_i's não nulos. Renumerando, se necessário, podemos supor que $\beta_1, \beta_2, ..., \beta_r$ são não nulos. Já sabemos que pelo menos um dos elementos $\beta_1, \beta_2, ..., \beta_{r-1}, \beta_r$ não pertence a F, o que mostra em particular que $r > 1$.
Agora, vamos dividir cada equação de $(\diamond)$ por β_r. Para simplificar as contas, vamos assumir que $\beta_r = 1$. Temos então

$$\begin{cases} \sigma_1(\alpha_1)\beta_1 + \sigma_1(\alpha_2)\beta_2 + \cdots + \sigma_1(\alpha_{r-1})\beta_{r-1} + \sigma_1(\alpha_r) = 0 \\ \vdots \\ \sigma_n(\alpha_1)\beta_1 + \sigma_n(\alpha_2)\beta_2 + \cdots + \sigma_n(\alpha_{r-1})\beta_{r-1} + \sigma_n(\alpha_r) = 0 \end{cases} \qquad (\diamond\diamond)$$

Assumindo que $\beta_1 \notin F$, então temos que $\sigma_{k_0}(\beta_1) \neq \beta_1$, para algum automorfismo σ_{k_0}, com $k_0 \in \{1, 2, ..., n\}$. Se aplicarmos σ_{k_0} a cada equação de $(\diamond\diamond)$ teremos então

$$\sigma_{k_0}\sigma_j(\alpha_1)\sigma_{k_0}(\beta_1) + \cdots + \sigma_{k_0}\sigma_j(\alpha_{r-1})\sigma_{k_0}(\beta_{r-1}) + \sigma_{k_0}\sigma_j(\alpha_r) = 0 \qquad (\diamond\diamond\diamond)$$

para cada $j-$ésima linha, com $j = 1, 2, ..., n$. Agora, cada aplicação da forma $\sigma_{k_0}\sigma_j$ é um elemento de G. Então, se colocarmos $\sigma_{k_0}\sigma_j = \sigma_i$, teremos que ambos os índices j e i percorrerão o conjunto $\{1, 2, ..., n\}$. Ou seja, as equações são as mesmas obtidas no sistema $(\diamond\diamond)$, com a diferença de que ao invés de combinações de β_i's, temos agora combinações de $\sigma_{k_0}(\beta_i)$'s. Assim, podemos escrevê-las como

$$\sigma_i(\alpha_1)\sigma_{k_0}(\beta_1) + \cdots + \sigma_i(\alpha_{r-1})\sigma_{k_0}(\beta_{r-1}) + \sigma_i(\alpha_r) = 0 \qquad (\triangle)$$

.

Fazendo agora a subtração de cada equação de $(\diamond\diamond)$ pelas equações de $(\triangle)$, temos

$$\sigma_i(\alpha_1)[\beta_1 - \sigma_{k_0}(\beta_1)] + \cdots + \sigma_i(\alpha_{r-1})[\beta_{r-1} - \sigma_{k_0}(\beta_{r-1})] = 0 \qquad (\triangle\triangle)$$

para cada $i = 1, 2, ..., n$. Mas, a solução de $(\triangle\triangle)$ é uma solução do sistema $(\diamond)$ com $x_1 = \beta_1 - \sigma_{k_0}(\beta_1) \neq 0$, pela escolha de k_0. Ou seja, temos então uma solução não trivial que tem um número menor do que r de x_i's não nulos. O que contradiz a minimalidade de r e completa a demonstração. ■

O leitor deve se lembrar que no **Exemplo 99**, $[\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}] = 6 = |S_3|$, onde $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ é o corpo de decomposição do polinômio irredutível (sobre $\mathbb{Q}$) $m(x) = x^3 - 2$ e S_3 é isomorfo ao grupo de automorfismos de $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ tendo $\mathbb{Q}$ como corpo fixo. Ou seja, o **Exemplo 99** ilustra claramente uma aplicação do teorema anterior.

Observação 108 *Se K/F é uma extensão finita, então temos a relação: $|Aut(K/F)| \leq [K : F]$, com a igualdade sendo válida apenas se F for o corpo fixo de $Aut(K/F)$.*

Se F_0 for o corpo fixo de $Aut(K/F)$, teríamos $F \subseteq F_0 \subseteq K$ e, pelo **Teorema 107**, $[K : F_0] = |Aut(K/F)|$. Agora, usando o **Teorema 71** obtemos $[K : F] = [K : F_0][F_0 : F] = |Aut(K/F)|[F_0 : F]$, o que confirma a observação feita.
Note que o corpo fixo F_0 é, na verdade, o "maior" subcorpo de K que é fixado pelos automorfismos de $Aut(K/F)$. E como vimos no Teorema 102, podem existir elementos que fixem F e não fixem F_0.
Uma outra forma de interpretar essa observação é a seguinte: K/F é de Galois se, e somente se, F é o corpo fixo de $Aut(K/F)$. Ou seja, se F é o maior corpo que é fixado por todos os automorfismos de $Aut(K/F)$.

Observação 109 *Seja G um subgrupo finito de automorfismos de K e seja F o corpo fixo de G. Então todo automorfismo de K que fixa F está contido em G.*

Ora, por definição, $G \leq Aut(K/F)$. Agora, usando o **Teorema 107** temos $|G| = [K : F]$ e, pela **Observação 108**, $|Aut(K/F)| \leq [K : F]$, assim concluímos que

$$[K : F] = |G| \leq |Aut(K/F)| \leq [K : F] \Longrightarrow G = Aut(K/F)$$

o que demonstra a **Observação 109**.
Ou seja, se $G = Aut(K/F)$ então K/F é de Galois, com grupo de Galois sendo igual a G, isto é, $G = Gal(K/F)$.

Observação 110 *Sejam $G_1, G_2 \leq Aut(K/F)$, onde $G_1 \neq G_2$. Então os corpos fixos de G_1 e G_2 também são diferentes.*

Através desta observação, podemos concluir que distintos subgrupos de $Aut(K/F)$ estão relacionados a distintos subcorpos de K. Como $Aut(K/F)$ é um grupo de automorfismos, sabemos que a imagem sempre será um corpo, assim, para cada subgrupo sempre conseguiremos um único subcorpo fixado.
Finalmente, podemos resumir os resultados aqui apresentados observando características de extensões K/F Galoisianas:

① Corpos de decomposição de polinômios separáveis;

② Corpos onde F é precisamente o corpo fixo de $Aut(K/F)$;

③ Corpos para os quais vale a relação $[K : F] = |Aut(K/F)|$;

④ Extensões finitas, normais e separáveis;

O ***Teorema Fundamental*** reune todos os resultados desta sessão e ainda nos permite encontrar extensões galoisianas com mais facilidade. As demonstrações feitas nesta sessão são baseadas em [1].

Teorema 111 (Teorema Fundamental da Teoria de Galois) *Seja K/F uma extensão de Galois com grupo de Galois $G = Gal(K/F)$, então existe uma bijeção que associa subcorpos E de K que contêm F a subgrupos H de G. Ou seja, dado $F \subseteq E \subseteq K$ existe $H \leq G$ tal que H fixa E e dado $H \leq G$ existe um corpo $F \subseteq E \subseteq K$ que é fixo por H. Cada subcorpo estará associado ao subgrupo de automorfismos que fixa o respectivo corpo. Além dessa correspondência, valem também:*

(a) A inclusão inversa: Se E_1 e E_2 correspondem, respectivamente, a H_1 e H_2, então $E_1 \subseteq E_2$ se, e somente se, $H_2 \leq H_1$;

(b) Temos as igualdades: $[K : E] = |H|$ e $[E : F] = |G/H|$;

(c) K/E é de Galois, com $Gal(K/E) = H$;

(d) E/F é de Galois se, e somente se, $H \trianglelefteq G$. Se este for o caso, temos ainda que $Gal(E/F) \cong G/H$;

(e) Se vale a correspondência entre E_1, E_2 e H_1, H_2 ,respectivamente, então $E_1 \cap E_2$ corresponde a $< H_1, H_2 >$, gerado por H_1 e H_2 e o corpo E_1E_2 corresponde a $H_1 \cap H_2$;

Demonstração:

Dado $H \leq G$, podemos obter um único subcorpo $F \subseteq E \subseteq K$ que é fixo por H, pela **Observação 110**. Assim, $E = K_H$.
Agora, se K é normal e separável (de Galois) sobre F, temos que K é o corpo de decomposição de alguma coleção de polinômios separáveis $f(x) \in F[x]$. Usando o fato de que $F \subseteq E$ temos que $f(x) \in E[x]$ e, consequentemente, K é o corpo de decomposição de uma coleção de polinômios separáveis em $E[x]$, ou seja, K/E é de Galois. Pelas **Observações 108 e 109**, E é o corpo fixo de $Aut(K/E) \leq G$.
Mostramos então que vale a correspondência:

$$\begin{array}{ccc} F \subseteq K_H \subseteq K & \longleftarrow & H \leq G \\ F \subseteq E \subseteq K & \longrightarrow & Aut(K/E) \leq G \end{array}$$

Temos então duas funções, onde uma é o inverso da outra, sendo ambas injetivas. Portanto, mostramos que a correspondência é uma bijeção.

Nós demonstramos no **Teorema 102** que vale o item *(a)*.

Para mostrar o item *(b)*, lembramos que se $E = K_H$ então, usando o **Teorema 107**, temos que $[K : E] = |H|$. Fazendo uso agora do **Teorema de Lagrange** e do **Teorema 71** observamos que:

$$|G| = |G/H||H| \text{ e } [K : F] = [K : E][E : F] \Longrightarrow \frac{|G|}{|H|} = \frac{[K : F]}{[K : E]} \Longrightarrow |G/H| = [E : F]$$

A **Observação 109** nos dá a demonstração do item *(c)* de forma imediata.

Para mostrar o item *(d)*, observamos que dado $\sigma \in G$ e $E = K_H \subseteq K$ temos $\sigma(E) = K_{\sigma H \sigma^{-1}}$, ou seja, o grupo que fixa o corpo $\sigma(E)$ é precisamente $\sigma H \sigma^{-1}$.

Claramente, se $a = \sigma(b) \in \sigma(E)$ e $\beta \in H$, $\sigma \circ \beta \circ \sigma^{-1}(\sigma(b)) = \sigma \circ \beta(b) = \sigma(b) = a$.
Cada automorfismo $\sigma \in G$ sobre K induz uma função $\lambda : E \longrightarrow \lambda(E) \subseteq K$, basta tomar $\lambda = \sigma|_E$. Sendo assim, cada λ é um monomorfismo (homomorfismo injetor) de E em $\sigma(E)$. Se dois monomorfismos $\sigma_1, \sigma_2 \in G$ tem o mesmo conjunto imagem $\sigma_1(E) = \sigma_2(E)$, então, obviamente $\sigma_1^{-1}\sigma_2 \in H$, ou seja, $\sigma_1 \cong \sigma_2(modH)$. Como consequência, existe uma bijeção entre os corpos $\sigma(E)$ e as classes laterais σH de H em G e H divide G em $|G/H|$ elementos que são monomorfismos de E em $\sigma(E)$. Usando o item *(c)* temos $|Mon(E/F)| = |G/H| = [E : F]$, onde $Mon(E/F)$ denota o conjunto de monomorfismos de E em algum corpo $\sigma(E)$.
Como E/F é de Galois se, e somente se, $|Aut(K/F)| = [E : F]|$, então cada monomorfismo é na verdade um automorfismo sobre E, observando o fato de que $Aut(E/F) \subseteq Mon(E/F)$. Ou seja, E/F é de Galois se, e somente se, $\sigma(E) = E$ para qualquer $\sigma \in G$. Agora, observando que existe uma bijeção natural entre subgrupos e seus respectivos subcorpos fixados, como foi demonstrado, teremos que $\sigma(E) = E$ se, e somente se, $H = \sigma H \sigma^{-1}$, para qualquer $\sigma \in G$.
Nós identificamos monomorfismos de E sobre F com classes laterais de H, além disso, quando H é normal em G esses monomorfismos são automorfismos. Consequentemente, se H é normal, podemos identificar o grupo G/H com o grupo $Gal(E/F)$, uma vez que E/F é de Galois. Sendo assim, $G/H \cong Gal(E/F)$. Assim, item *(d)* está demonstrado.

Considerando a correspondência entre E_1 e H_1 e E_2 e H_2, observamos que qualquer elemento de E_1E_2 é fixado por $H_1 \cap H_2$. Além disso, se $\sigma \in H_1 \cap H_2$ então σ fixa E_1 e E_2 e, consequentemente, fixa o corpo E_1E_2. Mostramos então que E_1E_2 tem correspondência com $H_1 \cap H_2$.
Agora, dado $\sigma \in < H_1 \cup H_2 >$, observe que $\sigma(a) = a$, para qualquer $a \in E_1 \cap E_2$. Além disso, se $a \in E_1 \cap E_2$, então qualquer elemento $\beta \in H_1$ fixa a e qualquer elemento $\gamma \in H_2$ fixa a também. Como $< H_1, H_2 >=< H_1 \cup H_2 >$, o item *(e)* está provado. ■

3.3 Comparação de estruturas

Nesta sessão, faremos uso das ferramentas fornecidas no ***Teorema Fundamental***. Esclareceremos através de exemplos algumas alternativas para o uso deste teorema.

O item *(e)* do **Teorema 111** compara os reticulados das extensões com os subgrupos de automorfismos que fixam o corpo base, observe que, usando a relação de inclusão inversa (item *(a)*), o item *(e)* nos diz que a "composição" de subcorpos está em correspondência com a "intersecção" dos subgrupos e a "intersecção" de subcorpos está relacionada com a "composição" de subgrupos, ou seja, os reticulados de ambos estão relacionados tendo um a mesma forma que o outro só que de "cabeça para baixo". Valendo a correspondência entre $E_1, E_2 \subseteq K$ e $H_1, H_2 \leq G$, respectivamente, temos:

$$\begin{tikzcd}
 & E_1E_2 & \\
E_1 \arrow[ur] & & E_2 \arrow[ul] \\
 & E_1 \cap E_2 \arrow[ul] \arrow[ur] &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & H_1 \cap H_2 \arrow[dl] \arrow[dr] & \\
H_1 \arrow[dr] & & H_2 \arrow[dl] \\
 & < H_1, H_2 > &
\end{tikzcd}$$

Podemos ilustrar mais informações dadas pelo teorema à partir dos reticulados. Por exemplo, com o item *(b)* fazemos a comparação entre os índices e graus das extensões que são os mesmos nos reticulados de grupos de automorfismos e extensões de corpos.

$$\begin{tikzcd}
K \arrow[r, leftrightarrow, dotted] & Id \arrow[d, "|H|"] \\
E \arrow[u, "{[K:E]}"] \arrow[r, leftrightarrow, dotted] & H \arrow[d, "|G/H|"] \\
F \arrow[u, "{[E:F]}"] \arrow[r, leftrightarrow, dotted] & G
\end{tikzcd}$$

Exemplo 112 ***(Grupo de Galois da extensão*** $\mathbb{Q}(\sqrt[4]{2}, \imath)/\mathbb{Q}$***)***

No **Exemplo 105** falamos sobre esta extensão e comentamos sobre uma forma mais fácil de achar extensões galoisianas, sem precisar utilizar polinômios irredutíveis, vamos somente usar o item *(d)* do **Teorema 111**.

Observe que estamos falando do corpo de decomposição do polinômio $p(x) = x^4 - 2$, cujas raízes são $\pm\sqrt[4]{2}, \pm\imath\sqrt[4]{2}$. Note ainda que

$$\mathbb{Q}(\sqrt[4]{2}, \imath) = \mathbb{Q}(\imath\sqrt[4]{2}) = \{a+b\sqrt[4]{2}+c\sqrt{2}+d\sqrt[4]{2^3}+e\imath+f\imath\sqrt[4]{2}+g\imath\sqrt{2}+h\imath\sqrt[4]{2^3}; a,b,c,d,e,f,g,h \in \mathbb{Q}\}.$$

Claramente, $[\mathbb{Q}(\sqrt[4]{2}, \imath) : \mathbb{Q}] = 8$, portanto, $|Gal(\mathbb{Q}(\sqrt[4]{2}, \imath)/\mathbb{Q})| = 8$ então, $Gal(\mathbb{Q}(\sqrt[4]{2}, \imath)/\mathbb{Q})$ é isomorfo a algum grupo do **Exemplo 55**.

Vamos considerar então as permutações, das raízes, que são "permitidas" para que o corpo base continue fixo:

$$\sigma : \left\{ \begin{array}{ccc} \sqrt[4]{2} & \longmapsto & \imath\sqrt[4]{2} \\ \imath & \longmapsto & \imath \end{array} \right. , \quad \tau : \left\{ \begin{array}{ccc} \sqrt[4]{2} & \longmapsto & \sqrt[4]{2} \\ \imath & \longmapsto & -\imath \end{array} \right.$$

Evidentemente, é mais viável procurar automorfismos "permitidos" olhando para os geradores e não para as raízes. Entretanto, o que interessa realmente é o que acontece com as raízes.

$$\begin{tikzcd}
 & \sigma & & \tau & \\
 & \imath\sqrt[4]{2} \arrow[dl, bend right] & & \imath\sqrt[4]{2} \arrow[d, bend right] & \\
-\sqrt[4]{2} \arrow[dr, bend right] & & \sqrt[4]{2} \arrow[ul, bend right] \arrow[loop right, "-\sqrt[4]{2}"] & & \sqrt[4]{2} \arrow[loop right] \\
 & -\imath\sqrt[4]{2} \arrow[ur, bend right] & & -\imath\sqrt[4]{2} \arrow[u, bend right] &
\end{tikzcd}$$

Note que, claramente, $\sigma^4 = \tau^2 = 1 = Id$ e $\sigma\tau = \tau\sigma^3$. Ou seja, só podemos ter $Gal(\mathbb{Q}(\sqrt[4]{2}, \imath)/\mathbb{Q}) \cong D_8$.
Notoriamente, não pode haver nenhum automorfismo que "troca" os geradores da extensão, pois o corpo base não continuaria fixo. Assim sendo, as únicas possibilidades para a imagem de $\imath$ são $\imath$ ou $-\imath$ e de $\sqrt[4]{2}$ é $\imath^n\sqrt[4]{2}$, onde $n \in \mathbb{Z}$. Agora, todas as possibilidades para $\sqrt[4]{2}$ são esgotadas para composições de σ consigo mesmo, e as únicas possibilidades para $\imath$ são a identidade (Id) e a conjugação(τ).

Vamos utilizar os reticulados para analisar quais os corpos fixos e seus respectivos subgrupos de automorfismos fixadores.

$$
\begin{tikzcd}
 & & D_8 & & \\
 & < \tau, \sigma^2 > \arrow[ur, "2"] & < \sigma > \arrow[u, "2"] & < \sigma\tau, \sigma^2 > \arrow[ul, "2"'] & \\
< \tau > \arrow[ur, "2"] & < \sigma^2\tau > \arrow[u, "2"] & < \sigma^2 > \arrow[ul, "2"'] \arrow[u, "2"] \arrow[ur, "2"] & < \sigma\tau > \arrow[u, "2"] & < \sigma^3\tau > \arrow[ul, "2"'] \\
 & & < 1 > \arrow[ul, "2"] \arrow[ul, "2"'] \arrow[u, "2"] \arrow[ur, "2"] \arrow[ur, "2"'] \arrow[urr, "2"'] & &
\end{tikzcd}
$$

$$
\begin{tikzcd}
 & & \mathbb{Q} \arrow[dl, "2"] \arrow[d, "2"] \arrow[dr, "2"] & & \\
 & \mathbb{Q}(\sqrt{2}) \arrow[dl, "2"] \arrow[d, "2"] \arrow[dr, "2"] & \mathbb{Q}(\imath) \arrow[d, "2"] & \mathbb{Q}(\imath\sqrt{2}) \arrow[dl, "2"'] \arrow[d, "2"] \arrow[dr, "2"] & \\
\mathbb{Q}(\sqrt[4]{2}) \arrow[drr, "2"] & \mathbb{Q}(\imath\sqrt[4]{2}) \arrow[dr, "2"] & \mathbb{Q}(\imath, \sqrt{2}) \arrow[d, "2"] & \mathbb{Q}((1+\imath)\sqrt[4]{2}) \arrow[dl, "2"'] & \mathbb{Q}((1-\imath)\sqrt[4]{2}) \arrow[dll, "2"'] \\
 & & \mathbb{Q}(\sqrt[4]{2}, \imath) & &
\end{tikzcd}
$$

Agora, para saber qual subcorpo é uma extensão de Galois sobre $\mathbb{Q}$, basta usar o item *(d)*. Isto pode ser feito de várias formas, podemos procurar por subgrupos normais em D_8 e também usar o fato de que $\lambda(E) = E$ para todo $\lambda \in D_8$, ou seja, E é invariante por qualquer automorfismo de D_8, o que não quer dizer necessariamente que a restrição de tal automorfismo a E seja a identidade (sabemos que este papel é cumprido pelo subgrupo de D_8 que fixa E).
Como D_8 é gerado apenas por dois automorfismos, é suficiente mostrar que a imagem de cada gerador dos subcorpos é ainda um elemento do subcorpo para os dois automorfismos (σ e τ).

- ☞ $\sigma(\sqrt{2}) = -\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ e $\tau(\sqrt{2}) = \sqrt{2} \in \mathbb{Q}(\sqrt{2})$;
- ☞ $\sigma(\imath) = \imath \in \mathbb{Q}(\imath)$ e $\tau(\imath) = -\imath \in \mathbb{Q}(\imath)$;
- ☞ $\sigma(\imath\sqrt{2}) = -\imath\sqrt{2} \in \mathbb{Q}(\imath\sqrt{2})$ e $\tau(\imath\sqrt{2}) = -\imath\sqrt{2} \in \mathbb{Q}(\imath\sqrt{2})$;
- ☞ $\sigma(\sqrt[4]{2}) = \imath\sqrt[4]{2} \notin \mathbb{Q}(\sqrt[4]{2})$;
- ☞ $\sigma(\imath\sqrt[4]{2}) = -\sqrt[4]{2} \notin \mathbb{Q}(\imath\sqrt[4]{2})$;
- ☞ Como visto acima $\mathbb{Q}(\imath)$, $\mathbb{Q}(\sqrt{2})$ e $\mathbb{Q}(\imath\sqrt{2})$ são invariantes, assim $\mathbb{Q}(\imath, \sqrt{2})$ também é invariante;
- ☞ $\sigma((1+\imath)\sqrt[4]{2}) = (-1+\imath)\sqrt[4]{2} \notin \mathbb{Q}((1+\imath)\sqrt[4]{2})$;
- ☞ $\sigma((1-\imath)\sqrt[4]{2}) = (1+\imath)\sqrt[4]{2} \notin \mathbb{Q}((1-\imath)\sqrt[4]{2})$;

Observe que $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\imath)$, $\mathbb{Q}(\imath\sqrt{2})$ e $\mathbb{Q}(\imath\sqrt{2})$ são as extensões de Galois encontradas, consequentemente, seus respectivos subgrupos fixadores são normais em D_8.
Notamos ainda que $D_8/ < \sigma^2 > \cong V_4$ onde todos os subgrupos são normais. Ainda, as extensões

quadráticas (de grau igual a 2) são de Galois, assim como a extensão "biquadrática" $\mathbb{Q}(\imath, \sqrt{2})$. Uma possível interpretação para o "efeito" dos automorfismos sobre as raízes é que σ caracteriza uma rotação no sentido antihorário e τ é uma reflexão sobre o eixo real. Ou seja, as combinações dos automorfismos são precisamente os movimentos rígidos do grupo diedral de ordem 8 (simetrias nos vértices de um quadrado). De fato, as raízes se comportam como vértices de um quadrado.
As reflexões sobre os eixos que contêm os pontos médios dos lados do "quadrado" são dadas precisamente pelas composições de $\sigma\tau$ e $\sigma^3\tau$, esses pontos médios são múltiplos escalares de $(1+\imath)\sqrt[4]{2}$ e $(1-\imath)\sqrt[4]{2}$, que estão sobre as retas $y = x$ e $y = -x$ no $\mathbb{R}^2$.
Algumas vezes o comportamento dos automorfismos sobre as raízes da unidade estabelecer alguma relação algébrica entre raízes complexas e radicais de números racionais, como é o caso do exemplo a seguir.

Exemplo 113 (O corpo de decomposição de $p(x) = x^8 - 2$)

As raízes de p são da forma $\zeta_8^n \sqrt[8]{2}$, onde n varia de 0 a 7 e $\zeta_8 = \frac{\sqrt{2}}{2} + \imath\frac{\sqrt{2}}{2}$. Agora, vamos procurar automorfismos que são "permitidos", lembrando que agora vale a relação

$$\zeta_8 = \frac{(1+\imath)}{2}\sqrt[8]{2^4}$$

Sem dificuldades, percebemos que $[\mathbb{Q}(\sqrt[8]{2}) : \mathbb{Q}] = 8$ e, como $\imath$ gera uma extensão quadrática, $\mathbb{Q}(\sqrt[8]{2}, \zeta_8)/\mathbb{Q}$ é de grau 16. Usando o fato de que $\mathbb{Q}(\sqrt[8]{2}, \zeta_8) = \mathbb{Q}(\sqrt[8]{2}, \imath)$ (que são geradores mais "convenientes" para procurarmos automorfismos) temos que:

$$\sigma : \left\{ \begin{array}{ccc} \sqrt[8]{2} & \longmapsto & \zeta_8\sqrt[8]{2} \\ \imath & \longmapsto & \imath \end{array} \right. , \quad \tau : \left\{ \begin{array}{ccc} \sqrt[8]{2} & \longmapsto & \sqrt[8]{2} \\ \imath & \longmapsto & -\imath \end{array} \right.$$

Agora, $\imath$ apesar de ser um gerador "conveniente" não da as informações completas sobre o que acontece com as raízes. Vamos aplicar os automorfismos em ζ_8 então:

$$\sigma(\zeta_8) = \frac{(1+\imath)}{2}\zeta_8^4\sqrt[8]{2^4} = -\frac{(1+\imath)}{2}\sqrt[8]{2^4} = -\zeta_8 = \zeta_8^5;$$

$$\tau(\zeta_8) = \frac{(1-\imath)}{2}\sqrt[8]{2^4} = \zeta_8^7;$$

Observe que este σ é bem diferente da rotação do exemplo anterior.

$$\sigma$$

$$\begin{tikzcd}
 & \zeta_8^2\sqrt[8]{4} \arrow[d, bend right] & \\
\zeta_8^3\sqrt[8]{2} \arrow[rrr, bend left] \arrow[ddrr, bend left] & & \zeta_8\sqrt[8]{2} \arrow[ddll, bend right] \\
\zeta_8^4\sqrt[8]{2} \arrow[d, bend left] & & \zeta_8^0\sqrt[8]{2} \arrow[u, bend left] \\
\zeta_8^5\sqrt[8]{2} \arrow[uurr, bend left] & & \zeta_8^7\sqrt[8]{2} \arrow[uull, bend right] \\
 & \zeta_8^6\sqrt[8]{2} \arrow[u, bend left] \arrow[uurr, bend right] &
\end{tikzcd}$$

Como sabemos, o automorfismo τ é a conjugação.

$$\tau$$

$$\begin{tikzcd}
 & \zeta_8^2\sqrt[8]{4} \arrow[dd, bend right] & \\
\zeta_8^3\sqrt[8]{2} \arrow[d, bend right] & & \zeta_8\sqrt[8]{2} \arrow[d, bend right] \\
\zeta_8^4\sqrt[8]{2} \arrow[loop left] & & \zeta_8^0\sqrt[8]{2} \arrow[loop right] \\
\zeta_8^5\sqrt[8]{2} \arrow[u, bend right] & & \zeta_8^7\sqrt[8]{2} \arrow[u, bend right] \\
 & \zeta_8^6\sqrt[8]{2} \arrow[uu, bend right] &
\end{tikzcd}$$

Além disso, temos ainda a igualdade $\tau\sigma^3 = \sigma\tau$. Observe que esta igualdade caracteriza um grupo "quase diedral" que é gerado por σ e τ. O fato de que $\sqrt[8]{2^4} = \sqrt{2} = \zeta_8 + \zeta_8^7$ nos revela que a imagem dos geradores tem que respeitar essa relação algébrica, sendo que $\sqrt{2}^2 = 2 \in \mathbb{Q}$, o que sugere uma certa cautela ao procurar automorfismos visto que estes tem que fixar o corpo base. A seguir, o diagrama da extensão de corpos $\mathbb{Q}(\imath, \sqrt[8]{2})/\mathbb{Q}$. Observe que o diagrama da extensão $\mathbb{Q}(\imath, \sqrt[4]{2})/\mathbb{Q}$ está "dentro" do mesmo. O procedimento para procurar extensões galoisianas será o mesmo do utilizado anteriormente.

$$
\begin{tikzcd}
 & & \mathbb{Q}((1-\imath)\sqrt[4]{2}) \arrow[ddrr] & & \\
 & \mathbb{Q}(\imath\sqrt{2}) \arrow[ur] \arrow[dr] \arrow[ddr] & & & \\
 & & \mathbb{Q}((1+\imath)\sqrt[4]{2}) \arrow[dr] & & \\
\mathbb{Q} \arrow[uur] \arrow[r] \arrow[ddr] & \mathbb{Q}(\imath) \arrow[r] & \mathbb{Q}(\imath, \sqrt{2}) \arrow[r] & \mathbb{Q}(\sqrt[4]{2}, \imath) \arrow[r] & \mathbb{Q}(\imath, \sqrt[8]{2}) \\
 & & & \mathbb{Q}(\sqrt[8]{2}) \arrow[ur] & \\
 & & \mathbb{Q}(\sqrt[4]{2}) \arrow[uur] \arrow[ur] \arrow[dr] & & \\
 & & & \mathbb{Q}(\zeta_8^2\sqrt[8]{2}) \arrow[uur] & \\
 & \mathbb{Q}(\sqrt{2}) \arrow[uur] \arrow[uuurr] \arrow[dr] & & & \\
 & & & \mathbb{Q}(\zeta_8^3\sqrt[8]{2}) \arrow[uuurr] & \\
 & & \mathbb{Q}(\imath\sqrt[4]{2}) \arrow[uuurr] \arrow[ur] \arrow[dr] & & \\
 & & & \mathbb{Q}(\zeta_8\sqrt[8]{2}) \arrow[uuurr] &
\end{tikzcd}
$$

Vamos aplicar σ e τ aos geradores dos subcorpos:

- ☞ $\sigma(\sqrt{2}) = -\sqrt{2},\ \tau(\sqrt{2}) = \sqrt{2} \in \mathbb{Q}(\sqrt{2})$;
- ☞ $\sigma(\imath) = \imath,\ \tau(\imath) = -\imath \in \mathbb{Q}(\imath)$;
- ☞ $\sigma(\imath\sqrt{2}) = -\imath\sqrt{2},\ \tau(\imath\sqrt{2}) = -\imath\sqrt{2} \in \mathbb{Q}(\imath\sqrt{2})$;
- ☞ $\sigma(\imath\sqrt[4]{2}) = -\sqrt[4]{2},\ \notin \mathbb{Q}(\imath\sqrt[4]{2})$;
- ☞ $\sigma(\sqrt[4]{2}) = \imath\sqrt[4]{2},\ \notin \mathbb{Q}(\sqrt[4]{2})$;
- ☞ $\mathbb{Q}(\imath, \sqrt{2})$ é de Galois sobre $\mathbb{Q}$ pois seus as imagens de seus geradores ainda pertence à $\mathbb{Q}(\imath, \sqrt{2})$;
- ☞ $\sigma((1+\imath)\sqrt[4]{2}) = (-1+\imath)\sqrt[4]{2},\ \notin \mathbb{Q}((1+\imath)\sqrt[4]{2})$;
- ☞ $\sigma((1-\imath)\sqrt[4]{2}) = (1-\imath)\sqrt[4]{2},\ \notin \mathbb{Q}((1-\imath)\sqrt[4]{2})$;
- ☞ $\tau(\zeta_8\sqrt[8]{2}) = \zeta_8^7\sqrt[8]{2} \notin \mathbb{Q}(\zeta_8\sqrt[8]{2})$;
- ☞ $\tau(\zeta_8^3\sqrt[8]{2}) = \zeta_8^5\sqrt[8]{2} \notin \mathbb{Q}(\zeta_8^3\sqrt[8]{2})$;
- ☞ $\sigma(\zeta_8^2\sqrt[8]{2}) = \zeta_8^3\sqrt[8]{2} \notin \mathbb{Q}(\zeta_8^2\sqrt[8]{2})$;
- ☞ $\sigma(\sqrt[8]{2}) = \zeta_8\sqrt[8]{2} \notin \mathbb{Q}(\sqrt[8]{2})$;
- ☞ $\sigma(\sqrt[4]{2}) = \zeta_8^2\sqrt[8]{2},\ \sigma(\imath) = \imath,\ \tau(\sqrt[4]{2}) = \sqrt[4]{2},\ \tau(\imath) = -\imath \in \mathbb{Q}(\sqrt[4]{2}, \imath)$;

Então, são galoisianas: $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\imath)$, $\mathbb{Q}(\imath\sqrt{2})$, $\mathbb{Q}(\imath, \sqrt{2})$ e $\mathbb{Q}(\sqrt[4]{2}, \imath)$. Observe que todas são corpos de decomposição de polinômios separáveis.

Considerações Finais

Concluímos o trabalho observando que dada uma extensão de corpos normal, que foi "montada" a partir das raízes de um polinômio irredutível e separável, o grupo formado pelas permutações das raízes que não alteram o corpo base é justamente o Grupo de Galois da extensão.

Além disso, tais permutações formam um conjunto linearmente independente como funções e o grupo gerado por essas permutações possue ordem igual ao grau da extensão de corpos. Para cada permutação teremos um subcorpo da extensão correspondente e, reciprocamente, para cada subcorpo, teremos um subgrupo de permutações correspondente.

Como foi demonstrado, devido à correspondência, os reticulados das estruturas terão a mesma forma, onde as únicas diferenças são a inclusão inversa (sentido das setas dos diagramas) e o conteúdo dos diagramas, um é um diagrama de grupos e o outro de corpos.

Observamos também que, dada uma extensão galoisiana, um subcorpo desta extensão será uma extensão galoisiana se, e somente se, for invariante para qualquer permutação entre as raízes. Usamos este fato para encontrar extensões galoisianas nos exemplos dados. Note que utilizar os geradores dos subgrupos e das extensões de corpos para encontrar as extensões invariantes torna as contas muito mais simples.

O leitor interessado em outros exemplos e mais diagramas pode consultar [1], que é a referência principal deste trabalho.

Referências Bibliográficas

[1] Dummit, D.S.; Foote, R.M., *Abstract Algebra*, 3ª edição, John Wiley & Sons, Inc., 2004.

[2] Gonçalves, A., *Introdução à Álgebra*, Projeto Euclides.

[3] Domingues, H. H.; Iezzi, G., *Álgebra Moderna*, 4ª edição, Atual Editora,1934.

[4] Garcia, A.; Iequain, Y., *Elementos de Álgebra*, Projeto Euclides,2001.

[5] Herstein, I. N., *Topics in Algebra*, 2ª edição, John Wiley & Sons, Inc.,1975.

Apêndice A

O Teorema de Cauchy

Este apêndice apresenta uma demonstração para o ***Teorema de Cauchy***. A demonstração aqui feita é baseada no exercício número 9 de [1], como dito anteriormente.

Teorema 114 (Teorema de Cauchy) *Dado um grupo G de ordem finita e p um número primo dividindo a ordem de G, existe então um elemento $x \in G$, diferente de 1, tal que $x^p = 1$, onde 1 é o elemento neutro de G.*

Demonstração:

Por hipótese, $|G| = pk$, onde p é um número primo e $k \in \mathbb{Z}_+$. Considere agora o conjunto $S = \{(x_1, x_2, ..., x_p)|\ x_1x_2x_3 \cdots x_p = 1 \text{ e } x_i \in G,\ \forall\ i \in \{1, 2, ..., p\}\}$.

Vamos mostrar que o conjunto S possui ordem $|G|^{p-1}$.
De fato, observando que $S \subset A = \{(x_1, x_2, ..., x_p)|\ x_i \in G,\ \forall\ i \in \{1, 2, ..., p\}\}$ e que $|A| = |G|^p$, notamos que existem $|G|$ possibilidades para o produto $x_1x_2 \cdots x_p = y \in G$, onde y é um elemento associado ao produto dos x_i de alguma $p-$upla. Agora, o conjunto o conjunto S restringe essas possibilidades a apenas um elemento, que é o elemento neutro 1. Ora, os elementos de G são regulares para a operação, sendo assim, todos os elementos possuem a mesma quantidade $|G|$ de $p-$uplas associadas. Logo,

$$|S| = \frac{|A|}{|G|} \Longrightarrow |S| = |G|^{p-1}$$

Defina agora em S a relação $\alpha \cong \beta$ se os elementos da $p-$upla β são os mesmos da $p-$upla α a menos de uma permutação cíclica. Observe que, se $\alpha = (x_1, x_2, ..., x_p)$ é um elemento de S, então o elemento $\beta = (x_p, x_1, x_2, ..., x_{p-1})$ é também um elemento de S, pois $x_1x_2 \cdots x_p = 1$ acarreta $x_1x_2 \cdots x_{p-1} = (x_p)^{-1}$, e daí temos que $x_px_1x_2 \cdots x_{p-1} = 1$. Assim, para cada permutação cíclica, a nova $p-$upla ainda é um elemento de S.

Vamos mostrar agora que a relação $\cong$ define uma relação de equivalência em S. Sejam $\alpha, \beta, \gamma \in S$.

- Claramente, $\alpha \cong \alpha\ \forall\ \alpha \in S$, pois a identidade é uma permutação cíclica;
- Como, o inverso de uma permutação cíclica é ainda uma permutação cíclica, então, se $\alpha \cong \beta$ teremos $\beta \cong \alpha$;

- Agora, usando o fato de que a composição de duas permutações cíclicas é também uma permutação cíclica, teremos que se $\alpha \cong \beta$ e $\beta \cong \gamma$ então $\alpha \cong \gamma$;

Mostraremos agora que uma classe de equivalência contêm apenas um elemento α se, e somente se, $\alpha = (x, x, ..., x) \in S$, onde $x^p = 1$.

Para mostrar a ida, suponha que a classe $\overline{\alpha}$ seja unitária. Assim, qualquer permutação cíclica σ aplicada em α tem como imagem o próprio α, ora, mas isto significa que na $p-$upla α todos os x_i's são iguais.
Para mostrar a volta, observe que $\alpha = (x, x, ..., x)$ é invariante para toda permutação cíclica, sendo assim, $\overline{\alpha} = \{\alpha\}$.

Vamos mostrar agora que qualquer classe de equivalência possui ordem 1 ou p.
Note que, como p é primo, nenhuma permutação cíclica diferente da identidade pode associar o elemento α consigo mesmo, pois a quantidade de coordenadas da $p-$upla α é p. Dada uma permutação cíclica σ, observe que sempre teremos $\sigma^p(\alpha) = \alpha$. Agora, considerando $\alpha \neq (x, x, ..., x)$, notamos que a ordem da classe $\overline{\alpha}$ não pode ser um número k' entre 1 e p, pois isso implicaria que $\sigma^k(\alpha) = \sigma^p(\alpha)$ e daí teríamos que $\sigma^{p-k'}(\alpha) = \alpha$, donde concluiríamos que as coordenadas da $p-$upla α são todas iguais. De forma análoga deduzimos que $\overline{\alpha}$ não possui ordem maior do que p.

Como $\cong$ é uma relação de equivalência sobre S, a ordem de S será a soma de todos os elementos que as classes de equivalência possuem. Agora, sabemos que as únicas classes de equivalência são aquelas de ordem 1 ou p. Consequentemente,

$$|S| = q + pd,$$

onde q denota o número de classes com 1 elemento e d o número de classes com p elementos.

Como q é o número de classes com 1 elemento, q também é o número de elementos $x \in G$ tais que $x^p = 1$. Agora, se q for maior do que 1, então, claramente, existe algum $x \neq 1$ tal que $x^p = 1$.

Ora, $|S| = |G|^{p-1} = (pk)^{p-1}$ e $|S| = q + pd$. Então, $q = -pd + (pk)^{p-1}$, e daí segue que $p|q$, e como $q > 0$ pois existe pelo menos o elemento $(1, 1, 1, ...1)$ cuja classe de equivalência possui ordem 1, então $q > 1$ pois p é primo e divide q. Sendo assim, existe um elemento $x \in G$, diferente de 1, tal que $x^p = 1$. E assim o teorema está demonstrado. ■

Apêndice B

Grupos de Klein e extensões de corpos

Este apêndice é destinado à apresentação de Grupos de Galois associados a polinômios do tipo $p(x) = \prod_{i=1}^{n}(x^2 - \theta_i^2)$, onde θ_i^2 é um número racional primo e $\theta_i^2 \neq \theta_j^2$ para $i \neq j$.

Primeiro, iniciaremos com uma breve discussão à respeito do grupo V_4 (Grupo de Klein) e como "estendê-lo" sem perder as propriedades algébricas. Observe que cada elemento de V_4, que é diferente do neutro, possui ordem 2. Além disso, V_4 é um grupo comutativo.

Definição 115 (Grupo de Klein de ordem 2^n) *Diremos que V_{2^n} é um grupo de Klein quando for abeliano e quando seus elementos, que são diferentes do neutro, possuírem ordem 2.*

Exemplo 116 (Grupo de Klein de ordem 8) *O grupo V_8, apresentado no **Exemplo 55**, é um grupo de Klein.*

Exemplo 117 (Grupo de Klein de ordem 2) *O grupo $\mathbb{Z}_2 \cong V_2$ é um grupo de Klein.*

Podemos estabelecer uma relação entre a ordem de um grupo de Klein e o seu número de geradores. O próximo teorema esclarece essa relação.

Teorema 118 (Ordem de um grupo de Klein) *Seja V_m um grupo de Klein. Se n é o número de geradores de V_m, então $m = 2^n$.*

Demonstração:

Vamos mostrar por indução sobre n.
Para $n = 1$ a igualdade é óbvia, pois $V_m = \{1, a\}$, onde a é o gerador de $V_m = V_2$. Consequentemente, $m = 2^1$.
Suponha que a igualdade seja válida para k geradores. Ou seja, se V é um grupo de Klein com k geradores, então $V = V_{2^k}$.
Agora, seja G um grupo de Klein com $k+1$ geradores, vamos mostrar que $|G| = |V_{2^{k+1}}| = 2^{k+1}$.
Primeiro, observe que $V_{2^k} \leq G$, onde $V_{2^k} =< \alpha_1, \alpha_2, ..., \alpha_k >$ e $G =< \alpha_1, \alpha_2, ..., \alpha_k, \alpha_{k+1} >$.
Agora, como G é abeliano, $V_{2^k} \trianglelefteq G$ e $G/V_{2^k} = \{V_{2^k}, \alpha_{k+1}V_{2^k}\}$. Pelo **Teorema 30**, segue que

$|V_{2^k}| = |\alpha_{k+1}V_{2^k}| = 2^k$, e daí temos que $|G| = 2^k + 2^k$ donde concluímos que $|G| = 2^{k+1}$ e, consequentemente, $G = V_{2^{k+1}}$. ■

Uma outra forma de mostrar o teorema anterior é tomando os possíveis produtos de i geradores de G (sendo G um grupo de Klein com n geradores). Usando o fato de que G é comutativo e que todo produto com i termos em G não pode ter elementos repetidos, visto que $\alpha^2 = 1$, $\forall\ \alpha \in G$, temos então que o número de produtos de i termos de G é dado justamente pela combinação dos n geradores tomados i a i. Ou seja, o número de elementos gerados pelos n geradores, considerando um produto de i geradores é o número $\frac{n!}{(n-i)!i!}$.

Assim, $|G| = \displaystyle\sum_{i=0}^{n} \frac{n!}{(n-i)!i!} = 2^n$.

Como visto na página 36 deste trabalho, $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \cong V_4$ é o Grupo de Galois associado ao polinômio $p(x) = (x^2 - 2)(x^2 - 3)$.

Fazendo $\theta_1^2 = 2$ e $\theta_2^2 = 3$, se σ é um automorfismo do Grupo de Galois de p, então $\sigma(\theta_i) = \pm\theta_i$ para todo i.

Teorema 119 *Seja* $p(x) = \displaystyle\prod_{i=1}^{n}(x^2 - \theta_i^2)$, *onde* θ_i^2 *é um número racional primo e* $M.D.C.(\theta_i, \theta_j) = 1$ *quando* $i \neq j$. *O Grupo de Galois associado a* p *é o grupo* V_{2^n}.

Demonstração:

Primeiro, seja G o grupo de Galois associado a p. Observe que qualquer automorfismo σ de G é tal que $\sigma(\theta_i) = \pm\theta_i$. Vamos mostrar que G é abeliano, com todos os seus elementos que são diferentes da unidade tendo ordem 2 e que possui n geradores.

Seja $\sigma_i \in G$ tal que $\sigma_i(\theta_i) = -\theta_i$ e $\sigma_i(\theta_j) = \theta_j$, para todo $i \neq j$. Vamos mostrar que $G =< \sigma_1, \sigma_2, ..., \sigma_n >$.
Claramente, $\sigma_i^2 = Id$, para todo i. Agora,

$$\sigma_i \circ \sigma_j : \begin{cases} \theta_i \overset{\sigma_j}{\longmapsto} \theta_i \overset{\sigma_i}{\longmapsto} -\theta_i \\ \theta_j \overset{\sigma_j}{\longmapsto} -\theta_j \overset{\sigma_i}{\longmapsto} -\theta_j \\ \theta_k \overset{\sigma_j}{\longmapsto} \theta_k \overset{\sigma_i}{\longmapsto} \theta_k \end{cases}, \quad \sigma_j \circ \sigma_i : \begin{cases} \theta_i \overset{\sigma_i}{\longmapsto} -\theta_i \overset{\sigma_j}{\longmapsto} -\theta_i \\ \theta_j \overset{\sigma_i}{\longmapsto} \theta_j \overset{\sigma_j}{\longmapsto} -\theta_j \\ \theta_k \overset{\sigma_i}{\longmapsto} \theta_k \overset{\sigma_j}{\longmapsto} \theta_k \end{cases},$$

para todo $i \neq j$, $j \neq k$ e $k \neq i$. Ou seja, as permutações σ_i comutam entre si.
Além disso, observe que a composição destas permutações geram todas as outras possíveis permutações. Basicamente, G é gerado pelos σ_i's. Sendo assim, $G \cong V_{2^n}$.■

Exemplo 120 (O Grupo de Galois do polinômio $p(x) = (x^2 - 2)(x^2 - 3)(x^2 - 5)$**)** *Observe que, neste caso,* $\theta_1 = \sqrt{2}$, $\theta_2 = \sqrt{3}$ *e* $\theta_3 = \sqrt{5}$.

A extensão $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}$ é o corpo de decomposição de p. Observe que,

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{5} + e\sqrt{6} + f\sqrt{10} + g\sqrt{15} + h\sqrt{30} \mid a, b, c, d, e, f, g, h \in \mathbb{Q}\}$$

.

Utilizando a correspondência de Galois, sabemos que o grupo de Galois G associado possui ordem 8. Além disso, as únicas permutações possíveis são as do tipo $\sigma(\theta_i) = \pm\theta_i$. Consequentemente, $G \cong V_8$ (veja o reticulado de V_8 no **Exemplo 55**).

Basicamente, cada θ_i possui a sua "conjugação". Assim, para cada parcela no produto do polinômio o número de permutações é duplicado. Observe que se o polinômio p for escrito como o produto de n parcelas do tipo $(x^2 - \theta_i^2)$ (com θ_i primo racional e primo com θ_j para $i \neq j$) então o Grupo de Galois associado a p será o V_{2^n}.