Teorema Bezout: se $(n,m)=d$ então existe $a,b \in \mathbb{Z}$ tal que $mdc(n,m) = an + bm$.

Subgrupo Normal: $G \to N \trianglelefteq G$ é um subgrupo normal, N é normal se:

$$aN = Na \quad \forall a \in G$$

$$G/N = \{\bar{a}\}, \quad a \sim b \Leftrightarrow a \in bN \text{ ou } ab^{-1} \in N$$

Homomorfismo natural: $\varphi: G \to G/N$

pega todos os elementos e $\to$ $a \to aN$
manda p/ sua classe

A ordem de um grupo é dado por: $(G, *)$ é denotado por $|G|$ é o número de elementos do conjunto G. (1) Dizemos que G é um grupo finito, se e somente se, o conjunto G é um conjunto finito:

$$|G| = n$$

Caso contrário, dizemos que G tem ordem infinita, se:

$$|G| = \infty, \ G \text{ é dito grupo infinito.}$$

A ordem de um grupo é sua cardinalidade, a ordem de um elemento "a" é o menor inteiro positivo "n", $(n \in \mathbb{Z})$ tal que:

$$a^n = 1 = e \quad \text{(se existe valor existe)}$$

Se este valor não existe, o elemento tem ordem infinita.

Dado um grupo G onde todos os elementos $\neq e$ têm ordem 2, então G é abeliano.

Dados $a, b \in G$, temos que mostrar:
$$a \cdot b = b \cdot a$$

Sabemos que todo elemento de G que $\neq e$ tem ordem 2.
$$\therefore x \in G, \ x \neq e \to x^2 = e$$

Agora se $x = e \to x^2 = e$

$$(ab)^2 = e$$

$$a\,abab\cdot b = a\,e\cdot b$$

$$\underbrace{a^2}_{e}\,\underbrace{b^2}_{e} = a\,e\,b$$

$$ba = ab.$$

Portanto G é Abeliano.

Subgrupos: A subconjunto H de um grupo G é um subgrupo de G se H é ele mesmo um grupo sob as operações em G.

Cada grupo G tem dois subgrupos: G (ele mesmo) e o $\{e\}$ elemento identidade. Sendo $\{e\}$ um subgrupo trivial.

Temos que H é um subconjunto não vazio de um grupo G. Se H é fechado sob a operação em G, então H é um subgrupo de G!

Centro de um grupo. Se G é um grupo, então o centro do G é o subconjunto denotado por $Z(G)$ e definido por:

$$Z(G) = \{a \in G \mid ag = ga \ \forall g \in G\}$$

Em outras palavras, um elemento de G esta em $Z(G)$ se e somente se ele comuta com todos os elementos de G.
Se G é um grupo abeliano, então:
$Z(G) = G$ porque todos os elementos comuta com cada um.
Quando G é não abeliano, então $Z(G)$ não está p/ todo G.

Grupos cíclicos: Um importante tipo de subgrupos pode ser construído como sequências. Se G é um grupo e $a \in G$, temos $\langle a \rangle$ denota o conjunto de todas as potências de a:

$$\langle a \rangle = \{\ldots, a^{-3}, a^{-2}, \ldots, a^{2}, \ldots\} = \{a^{n} \mid n \in \mathbb{Z}\}$$

Teorema: Se G é um grupo e $a \in G$, então $\langle a \rangle = \{a^{n} \mid n \in \mathbb{Z}\}$ é um subgrupo de G.

O grupo $\langle a \rangle$ é chamado de subgrupo cíclico gerador por a. Se o subgrupo $\langle a \rangle$ esta no interior do grupo G, dizemos que G é um grupo cíclico. Note que cada grupo cíclico é abeliano desde que:

$$a^{i} \cdot a^{j} = a^{i+j} = a^{j} a^{i}$$

Exemplo: $\langle G, * \rangle$ grupo, $a \in G$

① Define-se: $a^n = \underbrace{a * a * \ldots\ldots * a}_{n \text{ vezes}}$

$\langle \mathbb{Z}, + \rangle$ $a = 4$
$a^2 = 4^2 = 4 + 4 = 8$

$\langle \mathbb{Z}_6, + \rangle$ $a^2 = 4^2 = 4 + 4 = 8 = \underline{\underline{2}} \pmod 6$

$\langle \mathbb{Z}_7, \cdot \rangle$ $a^2 = 5^2 = 25 = 4 \pmod 7$

$\langle \mathbb{Z}_8, + \rangle$ $a = 2$
$2^1 = 2$
$2^2 = 4$
$2^3 = 2^2 + 2 = 6$
$2^4 = 2^3 + 2 = 8 = 0 \pmod 8$
$2^5 = 2^4 + 2 = 0 + 2 = 2$ → começa a repetir

$2^n = \{2, 4, 6, 0\}$
$H = \{2, 4, 6, 0\}$
$H \leq \mathbb{Z}_8$

H é um subgrupo gerado por 2: $H = \langle 2 \rangle$

① __Definição:__ Sejam $\underline{G}$ um grupo e $\underline{a \in G}$. Denomina-se __subgrupo gerado por $\underline{a}$__, o conjunto de todas as potências inteiras de $\underline{a}$, isto é:

$$\langle a \rangle = \{\ldots\ldots, a^{-2}, a^{-1}, a^0, a, a^2, \ldots\}$$

↳ $a^0 = e_G$ $\forall a$ e $\forall G$

↳ subgrupo gerado por $\underline{a}$ (gerador do subgrupo)

$\langle \mathbb{Z}_{10}, + \rangle$ $a = 5$
$a^2 = 5 + 5 = 10 = 0 \pmod{10}$
$a^3 = 15 = 5 \pmod{10}$ → começa a repetir

$\langle 5 \rangle = \{5, 0\}$

Agora o subgrupo gerado por 2: $\langle 2 \rangle$

$2^1 = 2$

$2^2 = 4$

$2^3 = 6$

$2^4 = 8$

$2^5 = 10 = 0 \pmod{10}$

$\langle 2 \rangle = \{2, 4, 6, 8, 0\}$

• $\langle 4 \rangle$. $4^1 = 4$

$4^2 = 8$

$4^3 = 12 = 2 \pmod{10}$

$4^4 = 16 = 6 \pmod{10}$

$4^5 = 20 = 0 \pmod{10}$

$\langle 4 \rangle = \{4, 8, 2, 6, 0\}$

$\langle 4 \rangle = \langle 2 \rangle$

• $\langle 8 \rangle$

$8^1 = 8$

$8^2 = 16 = 6 \pmod{10}$

$8^3 = 24 = 4 \pmod{10}$

$8^4 = 32 = 2 \pmod{10}$

$40 = 8^5 = 0 \pmod{10}$

$\langle 6 \rangle$

$6^1 = 6$

$6^2 = 12 = 2 \pmod{10}$

$6^3 = 18 = 8 \pmod{10}$

$6^4 = 24 = 4 \pmod{10}$

$30 = 6^5 = 0 \pmod{10}$

$\langle 8 \rangle = \{8, 6, 4, 2, 0\} = \langle 6 \rangle = \{6, 2, 8, 4, 0\}$

$\langle 8 \rangle = \langle 6 \rangle = \langle 4 \rangle = \langle 2 \rangle$

Agora: $\langle 3 \rangle$.

$3^1 = 3$

$3^2 = 6$

$3^3 = 9$

$3^4 = 12 = 2 \pmod{10}$

$3^5 = 15 = 5 \pmod{10}$

$3^6 = 18 = 8 \pmod{10}$

$3^7 = 21 = 1 \pmod{10}$

$3^8 = 24 = 4 \pmod{10}$

$3^9 = 27 = 7 \pmod{10}$

$3^{10} = 30 = 0 \pmod{10}$

$\langle 3 \rangle = \{3, 6, 9, 2, 5, 8, 1, 4, 7, 0\} = \mathbb{Z}_{10}$

$\langle 3 \rangle$ é gerador de $\mathbb{Z}_{10}$.

Seja $\underline{G}$ um grupo; diz-se que $\underline{G}$ é um grupo $\underline{\text{cíclico}}$ se existe um elemento $\underline{a \in G}$ tal que o grupo $\underline{G}$ coincide com o subgrupo gerado pelo elemento $\underline{a}$.

Temos que: G é um grupo cíclico $\longrightarrow \exists\, a \in G$ tal que $G = \langle a \rangle = \{x = a^n \mid n \in \mathbb{Z}\}$

$\underline{\text{Proposição}}$: Se $\underline{a \in G}$ é um gerador do grupo cíclico $\underline{G}$, então seu simétrico a' é também gerador de $\underline{G}$.

$\underline{\text{Ex1}}$: Quais são os geradores do grupo $\langle \mathbb{Z}_8, + \rangle$?

$\langle 2 \rangle = \{\underbrace{2, 4, 6}_{\text{simétrico}}, 0\} \neq \mathbb{Z}_8$ $\quad 2 \neq -2 = (6-8)$

Pela proposição se um dado elemento é gerador seu simétrico também é.

$\langle 6 \rangle = \{6, 4, 2, 0\}$, $\langle 6 \rangle = \langle 2 \rangle$
$\langle 6 \rangle \neq \mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$

Agora o 4: $\langle 4 \rangle = \{4, 0\} \neq \mathbb{Z}_8$

Agora o 7 que é simétrico do 1: $1 \neq -1 = (7-8)$

$\langle 1 \rangle = \{1, 2, 3, 4, 5, 6, 7, 0\} = \mathbb{Z}_8 = \langle 7 \rangle$

O $\mathbb{Z}_8$ é um grupo cíclico gerado pelos elementos 1 e 7, 5 e 3.

Temos que 5 é simétrico a 3, então $\langle 5 \rangle = \langle 3 \rangle$
$\langle 5 \rangle = \langle 3 \rangle = \mathbb{Z}_8 = \{5, 2, 7, 4, 1, 6, 3, 0\} = \langle 5 \rangle$

Proposição: Todo grupo cíclico é abeliano.

Demo: G grupo cíclico $\rightarrow \exists a \in G \,/\, G = \langle a \rangle = \{x = a^n \,/\, n \in \mathbb{Z}\}$.

Sejam $x, y \in G = \langle a \rangle$, vamos mostrar que $x * y = y * x$.

$x, y \in G \rightarrow \exists m, n \in \mathbb{Z}$ tais que $x = a^m$ e $y = a^n$.

Temos que $x * y = a^m * a^n = a^{m+n} = a^{n+m} = a^n * a^m = y * x$

Determinando Subgrupos: Seja $\langle G, * \rangle$ uma estrutura algébrica. Diz-se que G é um grupo se para a operação $*$ vale:

i) $(a * b) * c = a * (b * c)$, $\forall a, b, c \in G$,

ii) $\exists e \in G$, $\forall a \in G$ vale $a * e = a = e * a$, (e é denominado elemento neutro do grupo).

iii) $\forall a \in G$, $\exists a^{-1} \in G$, $a * a^{-1} = e = a^{-1} * a$.
(a^{-1} é denominado simétrico do elemento a.)

iv) a operação entre os elementos é fechado dentro do grupo, ou seja: $a, b \in G \Rightarrow a * b \in G$,

Subgrupo: Seja $\langle G, * \rangle$ um grupo. Um subgrupo de G é uma estrutura algébrica $\langle H, * \rangle$ que satisfaz as seguintes condições:

i) H é um subconjunto não vazio de G.
ii) $*$ é associativa em H.
iii) $*$ admite elemento neutro em H.
iv) Todo elemento de H admite simétrico com relação à operação $*$ em H.
v) $*$ é fechado em H.

Assim para termos um subgrupo de um grupo G, na verdade, é necessário encontrar um grupo dentro do grupo G.

Indica-se por $H < G$

Todo grupo G tal que $|G| \geq 2$ tem, pelo menos dois subgrupos: ele próprio e o conjunto formado pelo elemento neutro de G. Esses são chamados <u>subgrupos triviais</u>.

$H = \{e_G\}$ é subgrupo de G

Condições: i) $H \subset G$ e $H \neq \emptyset$
ii) $*$ é associativa em H
iii) $*$ admite elemento neutro em H
iv) $e_G \in H$ e seu simétrico também pertence a H
v) $*$ é fechado em H

<u>Subgrupos não triviais</u>: todo grupo, ex: G, admite pelo menos 2 subgrupos chamados triviais:

G e $H = \{e_G\}$

O principal interesse é com os outros subgrupos se existirem.

São os subgrupos próprios ou não-triviais.

Ex: Dado $\langle \mathbb{Z}_6, + \rangle$, $H = \{0, 2, 3\}$ é subgrupo?

$\langle \mathbb{Z}_6, + \rangle = \{0, 1, 2, 3, 4, 5\}$

$H \subset \langle \mathbb{Z}_6 + \rangle$ onde $H = \{0, 2, 3\}$

i) $H \neq \emptyset$
ii) $0+2 \in H$, $0+3 \in H$, $2+3 \notin H$
iii) $0 \in H$, o elemento neutro
iv) 2, 3 admite simétrico
v) é fechado em +

Então H não é subgrupo $(2+3=5 \notin H)$.

<u>Caracterização de Subgrupos</u>:

<u>Proposição</u>: Sejam G um grupo e H um subgrupo de G. O elemento neutro de H é o elemento neutro de G.

<u>Proposição</u>: Sejam G um grupo e H um subgrupo de G. O simétrico de h em H coincide com o simétrico de h em G.

<u>Proposição</u>: Sejam G um grupo e H um subgrupo não vazio de G. H é um subgrupo de G se:

i) $h_1 h_2 \in H$, $\forall h_1, h_2 \in H$
ii) $h^{-1} \in H$, $\forall h \in H$

A verificação de H ser não vazio é feita verificando se o elemento neutro do grupo G está em H.

Não é necessário verificar a associatividade, pois, os elementos de H são de G, para os quais está garantida a associatividade.

Ex: $H = \{0, 2, 4, 6, 8, 10\}$ é subgrupo de $\mathbb{Z}_{12}$.

$\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$, temos que:

$$H \subseteq \mathbb{Z}_{12}$$

i) $0 \in H$ e $0 \in \mathbb{Z}_{12}$, elemento neutro
ii) Os simétricos de H coincide com alguns simétricos de $\mathbb{Z}_{12}$

Ser simétrico indica que a soma deles será zero, que é o elemento neutro do grupo.

$0^{-1} = 0 \in H$
$2^{-1} = 10 \in H$
$4^{-1} = 8 \in H$
$6^{-1} = 6 \in H$

A soma é 12, $\mathbb{Z}_{12}$.

iii) Compondo os elementos de H, o resultado também será de H;

$2+2 = 4 \in H$	$4+4 = 8 \in H$
$0+2 = 2 \in H$	$4+6 = 10 \in H$
$2+4 = 6 \in H$	$4+8 = 0 \in H$
$0+4 = 4 \in H$	$4+10 = 2 \in H$
$2+6 = 8 \in H$	$6+6 = 0 \in H$
$2+8 = 10 \in H$	$6+8 = 2 \in H$
$2+10 = 0 \in H$	$6+10 = 4 \in H$
⋮	⋮

De fato pertence a H. Assim H é subgrupo de $\mathbb{Z}_{12}$.

Mostre que $12\mathbb{Z}$ é subgrupo de $6\mathbb{Z}$.

As condições a verificar são as mesmas, mas sendo os conjuntos infinitos devemos trabalhar com a caracterização dos seus elementos.

i) O elemento neutro de $6\mathbb{Z}$, o zero, deve pertencer a $12\mathbb{Z}$.

$$0 \in 6\mathbb{Z} \to 0 = 6.0 \to 2.0 = 2.(6.0) \to$$
$$2.0 = 12.0 \to 0 \in 12\mathbb{Z}$$

ii) Cada elemento de $12\mathbb{Z}$, tem seu simétrico também em $12\mathbb{Z}$.

$$x \in 12\mathbb{Z} \to x = 12.m, \; m \in \mathbb{Z}$$
$$\to -x = 12(-m), \; m \in \mathbb{Z}$$
$$\to -x \in 12\mathbb{Z}$$

iii) Compondo os elementos de $12\mathbb{Z}$, o resultado também é de $12\mathbb{Z}$;

Sejam $x, y \in 12\mathbb{Z} \to x = 12.m$ e $y = 12.n$, com m e $n \in \mathbb{Z}$. Logo,

$$x + y = 12.m + 12.n = 12(m+n)$$

$\therefore x + y \in 12\mathbb{Z}$

Como 6 e 12 são múltiplos, temos que $12\mathbb{Z}$ é subgrupo de $6\mathbb{Z}$.

• Verifique se $3\mathbb{Z}$ é subgrupo de $6\mathbb{Z}$.

$3\mathbb{Z}$ não é subgrupo de $6\mathbb{Z}$, isto porque $3\mathbb{Z}$ não é subconjunto de $6\mathbb{Z}$.
E $6\mathbb{Z}$ é subconjunto de $3\mathbb{Z}$, assim basta mostrar que existe $a \in 3\mathbb{Z}$ e $a \notin 6\mathbb{Z}$.

Portanto, tomamos 3, é elemento de $3\mathbb{Z}$. Mas não é elemento de $6\mathbb{Z}$.

$3.1 \in \mathbb{Z}$ e $3.1 \in \mathbb{Z}_6$.