

1 Grupos simples e solúveis

Como já discutimos, classificar grupos finitos G de uma dada ordem n é uma tarefa hercúlea. Além dos teoremas de Sylow, uma possível abordagem é a seguinte, encontrar os subgrupos normais $N \triangleleft G$, não triviais, para estudar os grupos quocientes G/N que possuirão uma ordem menor que a ordem de G , e assim tentar obter alguma informação sobre G . Fica claro então que grupos que **NÃO** possuem subgrupos normais, merecem uma atenção especial. Nesse sentido definimos:

Definição 1. Seja G um grupo. Dizemos que G é **simples**, se os únicos subgrupos normais de G são $\{e_G\}$ e G .

Exemplo 1. O grupo cíclico $\mathbb{Z}_p$ para p primo é simples. De fato, é possível mostrar que todo grupo abeliano finito simples é isomorfo a $\mathbb{Z}_p$ para algum p primo.

Para que possamos dar exemplos de grupos simples não abelianos, precisaremos voltar nossa atenção novamente para os grupos de permutação.

Lembre que na primeira sessão você provou que:

Corolário 1. *Todo elemento $\alpha \in S_n$ pode ser escrito como produto de transposições.*

Precisaremos do seguinte lema

Lema 1. *Seja S_n o grupo das permutações de n elementos, com $n \geq 2$. Se Id por ser escrita como produto de r transposições, então r é par.*

Demonstração. Procederemos por indução em r . Como a identidade não pode ser uma transposição, então $r \geq 2$. Se $r = 2$ estamos prontos. Suponha $r \geq 3$. Com $Id = \sigma_1 \sigma_2 \cdots \sigma_{r-1} \sigma_r$, onde cada σ_i é uma transposição.

Podemos ver que $\sigma_{r-1} \sigma_r$ deve satisfazer uma das seguintes possibilidades:

1. $(ab)(ab) = Id$
2. $(bc)(ab) = (ac)(bc)$

$$3. (cd)(ab) = (ab)(cd)$$

$$4. (ac)(ab) = (ab)(bc)$$

Perceba que se ocorre a possibilidade 1, então Id pode ser escrita como produto de $r - 2$ transposições e aplicamos a hipótese de indução, assim, Id poderá ser escrita como produto de um número par de transposições.

Se ocorre uma das 3 últimas possibilidades, perceba que podemos trocar $\sigma_{r-1}\sigma_r$ por uma das 3 possibilidades dentre as igualdades da esquerda, e com isso, teríamos deslocado o elemento a da transposição da direita para a transposição da esquerda. Sempre que repetirmos esse procedimento, o elemento a estará uma transposição mais a esquerda. Como existe apenas um número finito de vezes que podemos fazer isso, acabamos com duas possibilidades:

a) $\sigma_1\sigma_2 = (ax)(ax) = id$, e assim Id será escrita como o produto de $r - 2$ transposições e podemos aplicar a hipótese de indução.

b) $\sigma_1 = (ax)$ e $\sigma_2 \neq (ax)$. Note que esse caso não pode ocorrer, uma vez que se a aparece apenas uma vez, então Id não fixaria ele, o que é um absurdo.

Com isso concluímos nosso resultado. $\square$

Além disso temos o seguinte.

Teorema 1. *Se uma permutação σ pode ser escrita como um número par de transposições, e se $\sigma = \tau_1\tau_2 \cdots \tau_r$, é outra decomposição de σ em transposições, então r é par. Analogamente se σ for escrito como um número ímpar de transposições.*

Demonstração. Suponha que $\sigma = \tau_1\tau_2 \cdots \tau_r = \sigma_1 \cdots \sigma_s$, com s par. Então, como $(\sigma_1 \cdots \sigma_s)^{-1} = \sigma_s \cdots \sigma_1$ (cheque!!) temos que

$$Id = (\sigma_1 \cdots \sigma_s)^{-1}(\sigma_1 \cdots \sigma_s) = \sigma_s \cdots \sigma_1 \tau_1 \tau_2 \cdots \tau_r,$$

temos pelo lema anterior que r é par. $\square$

O teorema anterior nos permite fazer a seguinte definição.

Definição 2. Uma permutação em S_n é dita par, se pode ser escrita como um produto de um número par de transposições. A permutação é dita ímpar se for escrita como um número ímpar de transposições. O conjunto das transposições pares de S_n é um subgrupo, dito **grupo alternado** em n elementos, e denotado por A_n .

Os grupos alternados são importantes, pois eles nos dão os primeiros exemplos não abelianos de grupos simples. De fato, temos o seguinte Teorema;

Teorema 2. A_n é simples para $n \geq 5$.

Demonstração. Veja o Exercício 3. □

Outro importante resultado sobre os grupos alternados A_n , é que eles são normais em S_n .

Teorema 3. Para todo $n \geq 2$, temos que $A_n \triangleleft S_n$, e $|A_n| = \frac{n!}{2}$.

Demonstração. Defina $\pi : S_n \rightarrow \mathbb{Z}_2$ como $\pi(\sigma) = 1$ se σ é ímpar, e $\pi(\sigma) = 0$ se σ é par.

Afirmção 1: π é homomorfismo.

De fato, Sejam σ_1, σ_2 permutações pares, e τ_1 e τ_2 permutações ímpares. Note que $\pi(\tau_1\tau_2) = 1 = \pi(\tau_1)\pi(\tau_2)$, $\pi(\sigma_1\sigma_2) = 1 = \pi(\sigma_1)\pi(\sigma_2)$ e por fim, $\pi(\tau_1\sigma_1) = 0 = \pi(\tau_1)\pi(\sigma_2)$. Assim π é homomorfismo.

Afirmção 2: π é epimorfismo.

Temos que $\pi(Id) = 0$, pelo Lema 1, e que se $n \geq 2$, existe $(ab) \in S_n$, e que $\pi((ab)) = 1$.

Note que $\ker \pi \simeq A_n$, e assim A_n é normal em S_n , e mais ainda, pelo Teorema do isomorfismo segue que $S_n/A_n \simeq \mathbb{Z}_2$, e assim $(S_n : A_n) = |S_n/A_n| = |\mathbb{Z}_2| = 2$, e logo $|A_n| = \frac{n!}{2}$ pelo Teorema de Lagrange. □

Veremos agora como podemos utilizar o conceito de grupos simples para estudar qualquer grupo, e em particular, como usaremos eles para avançar no nosso problema de classificação de grupos finitos.

Definição 3. Seja G um grupo. Uma sequência de subgrupos

$$H^\bullet : \{e\} \leq H_1 \leq H_2 \leq \cdots \leq H_n = G,$$

é dita **série subnormal** se $H_i \triangleleft H_{i+1}$. Se, adicionalmente, $H_i \triangleleft G$ para todo i , então a série é dita **normal**. Por fim, diremos que n é o **comprimento** da série. Os grupos H_i/H_{i+1} são ditos **fatores da série**, ou **grupos fatores**.

Exemplo 2. As séries

$$\{0\} \leq \langle 15 \rangle \leq \langle 3 \rangle \leq \mathbb{Z}_{60},$$

$$\{0\} \leq \langle 20 \rangle \leq \langle 4 \rangle \leq \mathbb{Z}_{60},$$

são normais.

Um refinamento de uma composição em série, é a inclusão de certos subgrupos na série original. O refinamento é dito **próprio** quando algum dos novos grupos na série, for distinto dos já existentes.

Diremos que duas séries subnormais $K^\bullet$, e $H^\bullet$ com grupos fatores $\{\overline{K_1}, \overline{K_2}, \dots, \overline{K_n}\}$, e $\{\overline{H_1}, \overline{H_2}, \dots, \overline{H_m}\}$ são **isomorfas** ou **equivalentes**, se $n = m$ e se existe $\sigma \in S_n$ tal que $\overline{H} \simeq \overline{K}_{\sigma(i)}$. Para todo i .

Exemplo 3. As séries

$$\{0\} \leq \langle 15 \rangle \leq \langle 3 \rangle \leq \mathbb{Z}_{60},$$

$$\{0\} \leq \langle 20 \rangle \leq \langle 4 \rangle \leq \mathbb{Z}_{60},$$

são isomorfas.

Seja G um grupo, e $H^\bullet : \{e\} \leq H_1 \leq H_2 \leq \cdots \leq H_n = G$, uma série subnormal. $H^\bullet$ é dita uma **composição em série** se todos os grupos fatores H_{i+1}/H_i forem simples.

Exemplo 4. O grupo $\mathbb{Z}_{60}$ possui a seguinte composição em série:

$$\{0\} \leq \langle 30 \rangle \leq \langle 15 \rangle \leq \langle 3 \rangle \leq \mathbb{Z}_{60}.$$

Exemplo 5. O grupo S_n possui a seguinte composição em série:

$$\{Id\} \leq A_n \leq S_n.$$

De fato, $S_n/A_n \simeq \mathbb{Z}_2$ e $A_n = A_n/\{Id\}$, que são simples.

É imediato verificar o seguinte lema é verdadeiro

Lema 2. *Sejam G um grupo e $H^\bullet$ uma série de composição de G . Então $H^\bullet$ não admite refinamento próprio.*

Antes de prosseguirmos, considere o seguinte exemplo.

Exemplo 6. Considere as séries subnormais:

$$H^\bullet : \langle 0 \rangle \leq \langle 14 \rangle \leq \langle 7 \rangle \leq \langle 1 \rangle = \mathbb{Z}_{42}, \quad (1)$$

$$H^{\bullet\bullet} : \langle 0 \rangle \leq \langle 14 \rangle \leq \langle 1 \rangle = \mathbb{Z}_{42}, \quad (2)$$

$$H^{\bullet\bullet\bullet} : \langle 0 \rangle \leq \langle 7 \rangle \leq \langle 1 \rangle = \mathbb{Z}_{42}. \quad (3)$$

$$K^\bullet : \langle 0 \rangle \leq \langle 6 \rangle \leq \langle 3 \rangle \leq \langle 1 \rangle = \mathbb{Z}_{42}, \quad (4)$$

$$K^{\bullet\bullet} : \langle 0 \rangle \leq \langle 6 \rangle \leq \langle 1 \rangle = \mathbb{Z}_{42}, \quad (5)$$

Note que $H^\bullet$ é uma série de composição para G , uma vez que seus grupos fatores são $H_3/H_2 \simeq \mathbb{Z}_7$, $H_2/H_1 \simeq \mathbb{Z}_2$ e $H_1/H_0 \simeq \mathbb{Z}_3$, que são grupos cíclicos de ordem prima, e portanto simples.

Ademais, $H^\bullet$ é refinamento de $H^{\bullet\bullet}$ e $H^{\bullet\bullet\bullet}$.

Além disso, $K^\bullet$ é uma série de composição para G , uma vez que seus grupos fatores são $K_3/K_2 \simeq \mathbb{Z}_3$, $K_2/K_1 \simeq \mathbb{Z}_2$ e $K_1/K_0 \simeq \mathbb{Z}_7$. E também temos que $K^\bullet$ é refinamento de $K^{\bullet\bullet}$.

Note também que $K^{\bullet\bullet}$, $H^{\bullet\bullet}$ e $H^{\bullet\bullet\bullet}$ não são equivalentes, mas seus refinamentos o são. Por fim perceba que não podemos refinar mais $H^\bullet$ e $K^\bullet$, pois essas já são séries de composição para G .

O exemplo anterior, nos mostra que é possível encontrar séries subnormais não equivalente para um grupo, mas dá a entender que quando refinamos essas séries, no “máximo” possível, os refinamentos serão equivalentes. Esse resultado é surpreendentemente verdadeiro para qualquer grupo, como mostrará o Teorema de Jordan-Holder. Para que possamos demonstrá-lo, precisaremos dos seguintes resultados intermediários.

Lema 3. *Sejam G um grupo e H, K subgrupos de G . Se HK for subgrupo de G então $HK = KH$.*

Lema 4 (Zassenhaus). *Sejam G um grupo, e H, H_1, K, K_1 subgrupos com $H_1 \triangleleft H$ e $K_1 \triangleleft K$. Então*

1. $H_1(H \cap K_1) \triangleleft H_1(H \cap K)$
2. $K_1(H_1 \cap K) \triangleleft K_1(H \cap K)$
3. $H_1(H \cap K)/H_1(H \cap K_1) \simeq K_1(H \cap K)/K_1(H_1 \cap K)$

Demonstração. Começaremos pelo item 1; Como $H_1 \triangleleft H$ e como $H \cap K_1$ é subgrupo de H , segue que $H_1(H \cap K_1)$ é um subgrupo de H e portanto é um subgrupo de G . O mesmo vale para $H_1(H \cap K), K_1(H_1 \cap K), K_1(H \cap K)$. Vamos provar que $H_1(H \cap K_1) \triangleleft H_1(H \cap K)$. Dados $x \in H_1$ e $y \in H \cap K$, temos:

$$xyH_1(H \cap K_1)(xy)^{-1} = x[yH_1(H \cap K_1)y^{-1}]x^{-1} = x[(yH_1y^{-1})(y(H \cap K_1)y^{-1})]x^{-1},$$

Como $H_1 \triangleleft H$ e $y \in H$, temos $yH_1y^{-1} = H_1$, e como $K_1 \triangleleft K$, e $y \in H \cap K$, temos $(y(H \cap K_1)y^{-1}) = H \cap K_1$. Assim:

$$xyH_1(H \cap K_1)(xy)^{-1} = xH_1(H \cap K_1)x^{-1},$$

Mas como $x \in H_1$ e pelo Lema 3 temos $H_1(H \cap K_1) = (H \cap K_1)H_1$, segue que

$$xyH_1(H \cap K_1)(xy)^{-1} = H_1(H \cap K_1)$$

Assim segue o resultado. A demonstração do item 2 é análoga.

Vamos agora ao item 3). Sejam $A := H_1(H \cap K_1)$ e $B = H \cap K$.

Afirmção 1: $H_1(H \cap K) = AB$.

Afirmção 2: $(H \cap K_1)(H_1 \cap K) = A \cap B$.

Ambas seguem diretamente mostrando as duas inclusões.

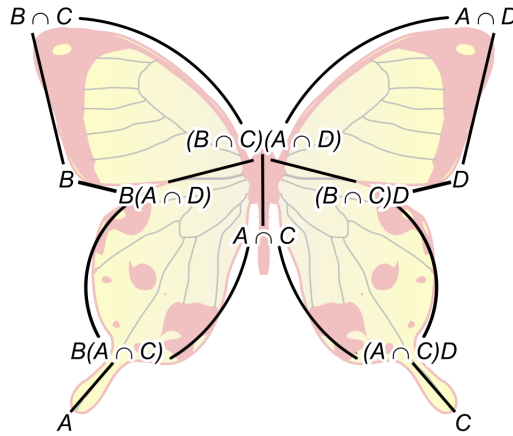
Afirmção 3: $A \triangleleft AB$. De fato, isso é precisamente o item 1.

Assim, pelo segundo teorema do isomorfismo temos $AB/A \simeq B/A \cap B$. Ou seja $H_1(H \cap K)/H_1(H \cap K_1) \simeq H \cap K/(H \cap K_1)(H_1 \cap K)$.

Afirmção 4: $K_1(H \cap K)/K_1(H_1 \cap K) \simeq H \cap K/(H \cap K_1)(H_1 \cap K)$. De fato, basta replicar as afirmações 1-3 para este caso.

Assim temos o nosso resultado. $\square$

O Lema de Zassenhaus também é conhecido como Lema da borboleta, por causa do seguinte diagrama:



Teorema 4 (Schreier). *Duas séries subnormais de um grupo G possuem refinamentos que são equivalentes.*

Demonstração. sejam $H^\bullet : \{e\} \leq H_1 \leq H_2 \leq \dots \leq H_n = G$, e $K^\bullet : \{e\} \leq K_1 \leq K_2 \leq \dots \leq K_m = G$, duas séries subnormais para G .

Para cada $0 \leq i \leq n - 1$, temos a cadeia de subgrupos:

$$H_i = H_i(H_{i+1} \cap K_0) \subseteq H_i(H_{i+1} \cap K_1) \subseteq \dots \subseteq H_i(H_{i+1} \cap K_m) = H_{i+1}.$$

Repetindo o procedimento para cada $0 \leq i \leq n-1$, e denotando $H_{i,j} = H_i(H_{i+1} \cap K_j)$, temos a seguinte cadeia de grupos:

$$\{e\} = H_{0,0} \subseteq H_{0,1} \subset \cdots H_{0,m-1} \subseteq H_{1,0} \subseteq H_{1,1} \subseteq H_{n-1,m-1} \subseteq H_{n-1,m} = G,$$

onde teremos uma sequência de $nm+1$ grupos não necessariamente distintos. Pelo Lema de Zassenhaus, vemos que de fato essa é uma série subnormal que é o refinamento da série $H^\bullet$. Analogamente, fazendo $K_{j,i} = K_j(K_{j+1} \cap H_i)$, para $0 \leq j \leq m-1$ e $0 \leq i \leq n-1$, temos

$$\{e\} = K_{0,0} \subseteq K_{0,1} \subset \cdots K_{0,n-1} \subseteq K_{1,0} \subseteq K_{1,1} \subseteq K_{m-1,n-1} \subseteq K_{m-1,n} = G,$$

Agora, veja que, pela parte 2) do Lema de Zassenhaus, temos que

$$H_{i+1}(H_i \cap K_j)/H_{i+1}(H_i \cap K_{j+1}) \simeq K_{j+1}(H_i \cap K_j)/K_{j+1}(H_{i+1} \cap K_j),$$

isto é,

$$H_{i,j+1}/H_{i,j} \simeq K_{j,i+1}/K_{j,i}, \tag{6}$$

para $0 \leq j \leq m-1$ e $0 \leq i \leq n-1$. Mas os grupos da esquerda da equação 6 são os grupos fatores da série subnormal $\{H_{i,j}\}$ e os grupos da direita da equação 6 são os grupos fatores da série subnormal $\{K_{j,i}\}$. Assim, segue que ambas são equivalentes. $\square$

Teorema 5 (Jordan-Holder). *Seja G um grupo. Então quaisquer duas composições em série de G são isomorfas.*

Demonstração. Sejam $H^\bullet$ e $K^\bullet$ duas composições em série de G . Pelo Teorema de Schreier vemos que $H^\bullet$ e $K^\bullet$ possuem refinamentos equivalentes, mas pelo Lema 2, vemos que uma composição em série não possui refinamento próprio, assim, $H^\bullet$ e $K^\bullet$ são eles mesmos equivalentes. $\square$

O teorema acima nos diz que sempre que um grupo possuir uma com-

posição em série, podemos associar a ele uma sequência de grupos simples. Veremos a seguir que todo grupo finito possui uma composição em série.

Teorema 6. *Seja G um grupo finito, então G possui uma composição em série.*

Demonstração. Procederemos por indução em $|G|$. $|G| = 1$, não há o que provar. Suponha então que $|G| = n$, que todo grupo de ordem até $n - 1$ possui composição em série. Se G é simples, $\{e_G \leq G\}$ é uma composição em série. Se G não é simples, seja $N \triangleleft G$. Considere S o conjunto de todos os subgrupos próprios normais de G , ordenado parcialmente pela inclusão. Como G é finito, ele possui um número finito de subgrupos, assim, S também é finito. Deste modo, tome em S um elemento M tal que, se $K \triangleleft G$ e $M \subset K$, então $K = G$. Segue do teorema da correspondência, que G/M é um grupo simples, e como M é subgrupo próprio de G , segue que $|M| < |G|$. Assim pela hipótese de indução temos que M admite uma composição em série $\{e\} \leq H_1 \leq \dots \leq H_n = M$, de modo que $\{e\} \leq H_1 \leq \dots \leq H_n = M \leq G$ é uma composição em série para G .

□

O teorema acima, junto com o Teorema de Jordan Holder nos diz que a todo grupo finito está associado uma sequência de grupos simples. Ou seja, os grupos simples estão para teoria de grupos, assim como os números primos estão para teoria dos números. Por isso, a atenção dos algebristas interessados no estudo de grupos se voltou por muito tempo para os grupos simples. Acontece que o estudo da classificação de grupos finitos simples, se provou uma tarefa extremamente difícil, e só foi concluído em 2004, após a contribuição de inúmeros matemáticos, sendo considerado por alguns como um dos maiores feitos recentes da matemática. Para se ter uma ideia da dificuldade da classificação dos grupos simples, é possível mostrar que cada grupo simples deve ser isomorfo a um $\mathbb{Z}_p$ para p primo, ou A_n para algum n , ou alguns exemplos clássicos de grupos de matrizes sobre corpos finitos, alguns exemplos excepcionais de tipo de Lie, ou um dos grupos esporádicos. Esse curso cobrirá apenas os dois primeiros tipos de grupos simples. Para se ter uma

ideia do tamanho do problema, um dos grupos esporádicos, conhecido como grupo monstro, possui ordem $2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$ que é igual à

808.017.424.794.512.875.886.459.904.961.710.757.005.754.368.000.000.000,

aproximadamente $8 \cdot 10^{53}$. Descrever sua tabela de multiplicação explicitamente necessita de mais de 4,5 GB de dados!

Uma outra classe importante de grupo que será muito útil no problema que motiva o nosso curso, ou seja, decidir se existem fórmulas por meio de radicais para as raízes de um dado polômio são os grupos solúveis.

Definição 4. Um grupo G é **solúvel** se possui uma série subnormal, tal que todo grupo fator é abeliano.

Lembre-se que dado G um grupo, definimos $G' = [G, G]$, $G^{(0)} = G$ e $G^{(i+1)} = [G^{(i)}, G^{(i)}]$. É possível usar grupos derivados dar uma descrição algorítmica de grupos solúveis, da seguinte maneira:

Teorema 7. *Seja G um grupo. Então G é solúvel se, e somente se, existe n natural tal que $G^{(n)} = \{e_G\}$.*

Para que possamos provar este resultado, precisamos da seguinte proposição que é de fácil verificação, e será deixado como exercício ao leitor:

Proposição 1. *Sejam G um grupo e G' o seu grupo derivado. Então:*

- G/G' é abeliano.
- G' é o menor subgrupo normal de G com essa propriedade, ou seja, se $H \triangleleft G$ com G/H abeliano, então $G' \subseteq H$

Demonstração. Suponha que G é solúvel, e considere uma série subnormal $H^\bullet : \{e\} \leq H_1 \leq H_2 \leq \dots \leq H_n = G$, com os grupos fatores abelianos. Como H_n/H_{n-1} é abeliano, segue na proposição anterior que $G' \subset H_{n-1}$. Como H_{n-1}/H_{n-2} é abeliano, segue também que $H'_{n-1} \subset H_{n-2}$,

mas como $G' \subseteq H_{n-1}$, segue que $G'' = G^{(2)} \subseteq H'_{n-1} \subseteq H_{n-2}$. Repetindo o procedimento, vemos que $G^{(n)} \subseteq \{e\}$, de onde segue o resultado. Por outro lado, suponha que exista n tal que $G^{(n)} = \{e\}$. Assim a série $H^\bullet : \{e\} \leq G^{(n)} \leq G^{(n-1)} \leq \dots \leq G^{(1)} = G' \subseteq G$, é uma série subnormal, que possui todos os grupos fatores abelianos. $\square$

Exemplo 7. Todo grupo abeliano é solúvel.

Exemplo 8. Todo p -grupo é solúvel.

É possível mostrar que todo grupo de ordem $p^a q^b$ é solúvel. Este resultado é conhecido como Teorema pq de Burnside.

O Teorema 7 nos ajuda a demonstrar o seguinte resultado importante.

Teorema 8. *Sejam G um grupo e H é um subgrupo de G , se G é solúvel então H é solúvel, e mais, se $H \triangleleft G$, então G é solúvel se, e somente se H e G/H são solúveis.*

Crédito da imagem do Lema da Borboleta: Claudio Rocchini, Wikipedia.

2 Exercícios

1. Mostre que todo grupo abeliano finito simples é isomorfo a $\mathbb{Z}_p$ para algum p primo.
2. Prove que A_n é um grupo, e calcule sua ordem.
3. Nesse exercício provaremos que A_n é simples para $n \geq 5$.
 - a) Prove que se $n \geq 3$, então A_n é gerado por 3-ciclos. (Sugestão: Mostre que o produto de duas transposições pode ser escrito como o produto de 3-ciclos, use as possibilidades expostas no Lema 1)
 - b) Seja $N \triangleleft A_n$. Se $n \geq 3$ e N contém um 3-ciclo, então $N = A_n$
 - c) Para $n \geq 5$, então todo subgrupo normal não trivial de A_n contém um 3-ciclo(**).
 - d) conclua que A_n é simples para $n \geq 5$.

4. Prove que se G é um grupo simples de ordem menor que 60, então G é cíclico. Por quê o resultado não é válido para $|G| = 60$?
5. Sejam G um grupo, e H, K subgrupos de G tais que $H \triangleleft G$ e $K \triangleleft K$. Então $K \triangleleft G$?
6. Dê exemplo de uma série subnormal que não é normal.
7. Prove que $\mathbb{Z}$ não admite uma composição em série.
8. O que dá errado no Teorema da existência de composição de séries para grupos finitos, se tentarmos repetir o mesmo argumento para grupos de ordem infinita?
9. Prove que A_4 e S_4 são solúveis.
10. Prove o Teorema 8.
11. Prove que todo grupo de ordem menor que 60 é solúvel. (**) (Dica: divida a prova em vários passos, cobrindo números da forma $p^n q$, com $p \not\equiv 1 \pmod{q}$, $2^n 3^m$, e o que você sabe sobre quais grupos são abelianos. Por fim trabalhe com os números restantes).
12. Prove que S_n não é solúvel para $n \geq 4$.

3 Exercícios Complementares

1. Seja G um grupo. Prove que o conjunto dos automorfismos de G , denotado por $\text{Aut}(G)$ com a operação de composição de funções define um grupo.
2. Nesse exercício iremos discutir a noção de **produto semidireto** de grupos. Sejam N e H grupos, e considere um homomorfismo $\varphi : H \rightarrow \text{Aut}(N)$. Considere o produto o grupo G cujos elementos são os elementos de $N \times H$, com a seguinte operação:

$$(n_1, h_1) * (n_2, h_2) = (n_1 \varphi(h_1)(n_2), h_1 h_2)$$

- . Denotaremos G por $N \rtimes_{\varphi} H$. Prove que
- a) $H \rtimes_{\varphi} N$ é de fato grupo, e exiba seu elemento neutro, e o elemento inverso de (n, h) .
 - b) Prove que $N \times \{e_H\} \triangleleft N \rtimes_{\varphi} H$ e que $\{e_N\} \times H \leq N \rtimes_{\varphi} H$, onde e_N e e_H denotam os elementos neutros de N e H respectivamente.
 - c) Prove que se $\varphi = id_{\text{Aut}(N)}$, então $N \rtimes_{\varphi} H \simeq N \times H$, o produto direto convencional.
3. Sejam G um grupo e H, K subgrupos de G . Se HK for subgrupo de G então $HK = KH$.
 4. Seja G um grupo de ordem 280. Mostre que G não é um grupo simples.