Matemática Discreta
Os inteiros
T. Praciano-Pereira

Lista numero 03
tarcisio.praciano@gmail.com
Dep. de Computação

alun@:

9 de abril de 2013 **Univ. Estadual Vale do Aca**

Documento escrito com LaTeX - sis. op. Debian/Gnu/Linux
http://www.matem-discreta.sobralmatematica.org/

Se entregar em papel, por favor, prenda esta *folha de rosto* na sua solução desta lista, deixando-a em branco. Ela será usada na correção.

Exercícios 1 *Assunto: Os inteiros objetivo: Entender a estrutura algébrica dos inteiros*

palavras chave: *anel dos inteiros, estrutura algébrica, grupo, inteiros módulo n, monoide*

1. *Operação*

   (a) *(V)[ ](F)[ ] A operação "/", de dividir, é uma operação definida no conjunto dos inteiros.*

   (b) *(V)[ ](F)[ ] A operação "*", de multiplicar, é uma operação definida no conjunto dos inteiros e goza das propriedades,* comutativa, associativa, distributividade *e* existencia do elemento neutro.

   (c) *(V)[ ](F)[ ] A operação "*", de multiplicar, é uma operação definida no conjunto dos inteiros e goza das propriedades,* comutativa, associativa, existencia do elemento neutro *e todo elemento de* $\mathbf{Z}$ *possui um inverso multiplicativo.*

   (d) *(V)[ ](F)[ ] A operação "+", de somar, é uma operação definida no conjunto dos inteiros e goza das propriedades,* comutativa, associativa, distributividade *e* existencia do elemento neutro.

   (e) *(V)[ ](F)[ ] A operação "+", de somar, é uma operação definida no conjunto dos inteiros e goza das propriedades,* comutativa, associativa, existencia do elemento neutro *e todo elemento de* $\mathbf{Z}$ *possui um inverso aditivo.*

2. *Operações*

   Nos itens desta questão, experimente com $p = 6$ *ou* $p = 4$ *mas procure abstrair-se dos valores particulares.*

   (a) *(V)[ ](F)[ ] A soma e a multiplicação são operações definidas em* $\mathbf{Z}$ *que é fechado para ambas operações.*

   (b) *(V)[ ](F)[ ] A multiplicação é distributiva relativamente à adição, em* $\mathbf{Z}$*.*

   (c) *(V)[ ](F)[ ] Defina* $\mathbf{Z}_p$ *como o conjunto dos restos na divisão (inteira) por p. Os elementos de* $\mathbf{Z}_p$ *são representados pelos símbolos* $\{0, 1, 2, \ldots, p\}$*.*

   (d) *(V)[ ](F)[ ] Defina* $\mathbf{Z}_p$ *como o conjunto dos restos na divisão (inteira) por p. Os elementos de* $\mathbf{Z}_p$ *são representados pelos símbolos* $\{0, 1, 2, \ldots, p-1\}$*. Uma adição,* $\oplus$*, pode ser definida em* $\mathbf{Z}_p$*:*

   $$x, y \in \mathbf{Z}_p; x \oplus y = \text{ resto de } x + y \text{ na divisão por } p \qquad (1)$$

   Esta adição, em $\mathbf{Z}_p$ *é comutativa, associativa, tem elemento neutro, e todo elemento tem um inverso aditivo relativamente a* $\oplus$*.*

   (e) *(V)[ ](F)[ ] Sendo* $\mathbf{Z}_p$ *o conjunto dos restos na divisão (inteira) por p com seus elementos de* $\mathbf{Z}_p$ *representados pelos símbolos* $\{0, 1, 2, \ldots, p-1\}$*, Um produto,* $\otimes$*, pode ser definida em* $\mathbf{Z}_p$*:*

   $$x, y \in \mathbf{Z}_p; x \otimes y = \text{ resto de } x * y \text{ na divisão por } p \qquad (2)$$

   Este produto, em $\mathbf{Z}_p$ *é comutativo, associativo, tem elemento neutro, e todo elemento tem um inverso relativamente a* $\otimes$*.*

3. *Nos referimos ao par* $(\mathbf{Z}, +)$ *como uma estrutura algébrica e se forem dados dois elementos arbitrários de* $\mathbf{Z}$*,* x, y *então* $x + y \in \mathbf{Z}$ *o que signfica que* $+$ *é uma operação binária definida em* $\mathbf{Z}$ *e que* $\mathbf{Z}$ *é fechado para esta operação.*

   Considerando o conjunto $\mathbf{Z}_p$ *dos restos na divisão por p, e com a "adição de restos"* $\oplus$ *como já foi definida na questão dois. É um exemplo de operação binária definida no conjunto. De forma semelhante podemos definir um "produto de restos"* $\oplus$ *que é também um exemplo de operação binária definida neste conjunto.*

   Estrutura algébrica

   (a) *(V)[ ](F)[ ] O produto é uma operação binária definida em* $\mathbf{Z}$ *que é fechado para o produto.*

   (b) *(V)[ ](F)[ ] A divisão é uma operação binária definida em* $\mathbf{Z}$ *que é fechado para a divisão.*

   (c) *(V)[ ](F)[ ] O produto de restos,* $\otimes$ *é uma operação binária definida em* $\mathbf{Z}_5$ *que é fechado para esta operação.*

(d) (V)[ ](F)[ ] *A adição de restos,* $\oplus$ *é uma operação binária definida em* $\mathbf{Z}_5$ *que é fechado para esta operação.*

(e) (V)[ ](F)[ ] *Considerando a estrutura algébrica* $(\mathbf{Z}_5, \oplus)$ *todo elemento tem inverso relativamente a operação* $\oplus$*. E seria uma frase incorreta dizer "*todo elemento tem inverso*" sem mencionar a operação.*

4. *Considere o conjunto dos restos na divisão por 4 e as estruturas algébricas* $(\mathbf{Z}_4, \oplus)$, $(\mathbf{Z}_4, \otimes)$, *que já foram mencionadas nas questões anteriores.*

   Estrutura algébrica

   (a) (V)[ ](F)[ ] *A operação binária* $\oplus$*, definida em* $\mathbf{Z}_4$*, é comutativa, asssociativa e distributiva.*

   (b) (V)[ ](F)[ ] *A operação binária* $\oplus$*, definida em* $\mathbf{Z}_4$*, é comutativa, asssociativa, Existe um elemento neutro relativamente a* $\oplus$ *em* $(\mathbf{Z}_4, \oplus)$*, e todo elemento* $x \in \mathbf{Z}_4$ *tem um único inverso relativamente a* $\oplus$ *em* $(\mathbf{Z}_4, \oplus)$*.*

   (c) (V)[ ](F)[ ] *A operação binária* $\otimes$*, definida em* $\mathbf{Z}_4$*, é comutativa, asssociativa, existe um elemento neutro relativamente a* $\otimes$ *em* $(\mathbf{Z}_4, \otimes)$*, e todo elemento* $x \in \mathbf{Z}_4$ *tem um único inverso relativamente a* $\otimes$ *em* $(\mathbf{Z}_4, \otimes)$*.*

   (d) (V)[ ](F)[ ] *Como as duas operações binárias* $\otimes, \oplus$ *estão definidas em* $\mathbf{Z}_4$ *então podemos considerar a estrutura algébrica* $(\mathbf{Z}_4, \oplus, \otimes)$ *e valem as propriedades:*

      i. $\oplus$ *é comutativa, asssociativa, existe um elemento neutro relativamente a* $\oplus$ *em* $(\mathbf{Z}_4, \oplus)$ *e todo elemento* $x \in \mathbf{Z}_4$ *tem um único inverso relativamente a* $\oplus$ *em* $(\mathbf{Z}_4, \oplus)$*.*

      ii. $\otimes$ *é comutativa, asssociativa, existe um elemento neutro relativamente a* $\otimes$ *em* $(\mathbf{Z}_4, \otimes)$ *e todo elemento* $x \in \mathbf{Z}_4$ *tem um único inverso relativamente a* $\otimes$ *em* $(\mathbf{Z}_4, \otimes)$*.*

      iii. $\otimes$ *é distributiva relativamente a* $\oplus$*.*

   (e) (V)[ ](F)[ ] *Como as duas operações binárias* $\otimes, \oplus$ *estão definidas em* $\mathbf{Z}_4$ *então podemos considerar a estrutura algébrica* $(\mathbf{Z}_4, \oplus, \otimes)$ *e valem as propriedades:*

      i. $\oplus$ *é comutativa, asssociativa, existe um elemento neutro relativamente a* $\oplus$ *em* $(\mathbf{Z}_4, \oplus)$ *e todo elemento* $x \in \mathbf{Z}_4$ *tem um único inverso relativamente a* $\oplus$ *em* $(\mathbf{Z}_4, \oplus)$*.*

      ii. $\otimes$ *é comutativa, asssociativa, existe um elemento neutro relativamente a* $\otimes$ *em* $(\mathbf{Z}_4, \otimes)$*, mas nem todo elemento* $x \in \mathbf{Z}_4$ *tem um inverso relativamente a* $\otimes$ *em* $(\mathbf{Z}_4, \otimes)$*.*

      iii. $\otimes$ *é distributiva relativamente a* $\oplus$*.*

   Compare $(\mathbf{Z}_4, \oplus, \otimes)$ *com* $(\mathbf{Z}, +, \cdot)$ *escreva algumas linhas sobre esta comparação.*

Experimente montar um sistema de funções `LISP`*, um programa, que gere a tabela operatória para cada uma das operações* $\oplus$ *e* $\otimes$ *para o conjunto* $\mathbf{Z}_4$ *dos restos na divisão por 4. Sugestão, as funções deve ser*

`(ovezes x y)` *ou* `(omais x y)` *...*

5. *Considere o conjunto* $\mathbf{Z}_5$ *dos restos na divisão por 4 e as estrutura algébricas* $(\mathbf{Z}_5, \oplus)$, $(\mathbf{Z}_5, \otimes)$, *que já foram mencionadas nas questões anteriores. Esta questão parece ser uma repetição enfadonha da anterior e é um erro pensar assim!*

   Estrutura algébrica

   (a) (V)[ ](F)[ ] *A operação binária* $\oplus$*, definida em* $\mathbf{Z}_5$*, é comutativa, asssociativa e distributiva.*

   (b) (V)[ ](F)[ ] *A operação binária* $\oplus$*, definida em* $\mathbf{Z}_5$*, é comutativa, asssociativa, Existe um elemento neutro relativamente a* $\oplus$ *em* $(\mathbf{Z}_5, \oplus)$*, e todo elemento* $x \in \mathbf{Z}_5$ *tem um único inverso relativamente a* $\oplus$ *em* $(\mathbf{Z}_5, \oplus)$*.*

   (c) (V)[ ](F)[ ] *A operação binária* $\otimes$*, definida em* $\mathbf{Z}_5$*, é comutativa, asssociativa, existe um elemento neutro relativamente a* $\otimes$ *em* $(\mathbf{Z}_5, \otimes)$*, e todo elemento* $x \in \mathbf{Z}_5$ *tem um único inverso relativamente a* $\otimes$ *em* $(\mathbf{Z}_5, \otimes)$*.*

   (d) (V)[ ](F)[ ] *Como as duas operações binárias* $\otimes, \oplus$ *estão definidas em* $\mathbf{Z}_5$ *então podemos considerar a estrutura algébrica* $(\mathbf{Z}_5, \oplus, \otimes)$ *e valem as propriedades:*

      i. $\oplus$ *é comutativa, asssociativa, existe um elemento neutro relativamente a* $\oplus$ *em* $(\mathbf{Z}_5, \oplus)$ *e todo elemento* $x \in \mathbf{Z}_5$ *tem um único inverso relativamente a* $\oplus$ *em* $(\mathbf{Z}_5, \oplus)$*.*

      ii. $\otimes$ *é comutativa, asssociativa, existe um elemento neutro relativamente a* $\otimes$ *em* $(\mathbf{Z}_5, \otimes)$ *e todo elemento* $x \in \mathbf{Z}_5$ *tem um único inverso relativamente a* $\otimes$ *em* $(\mathbf{Z}_5, \otimes)$*.*

      iii. $\otimes$ *é distributiva relativamente a* $\oplus$*.*

   (e) (V)[ ](F)[ ] *Como as duas operações binárias* $\otimes, \oplus$ *estão definidas em* $\mathbf{Z}_5$ *então podemos considerar a estrutura algébrica* $(\mathbf{Z}_5, \oplus, \otimes)$ *e valem as propriedades:*

      i. $\oplus$ *é comutativa, asssociativa, existe um elemento neutro relativamente a* $\oplus$ *em* $(\mathbf{Z}_5, \oplus)$ *e todo elemento* $x \in \mathbf{Z}_5$ *tem um único inverso relativamente a* $\oplus$ *em* $(\mathbf{Z}_5, \oplus)$*.*

      ii. $\otimes$ *é comutativa, asssociativa, existe um elemento neutro relativamente a* $\otimes$ *em* $(\mathbf{Z}_5, \otimes)$*, mas nem todo elemento* $x \in \mathbf{Z}_5$ *tem um inverso relativamente a* $\otimes$ *em* $(\mathbf{Z}_5, \otimes)$*.*

      iii. $\otimes$ *é distributiva relativamente a* $\oplus$*.*

Compare $(\mathbf{Z}_5, \oplus, \otimes)$ *com* $(\mathbf{Z}, +, \cdot)$ *escreva algumas linhas sobre esta comparação.*

Experimente montar um sistema de funções `LISP`*, um programa, que gere a tabela operatória para cada uma das operações* $\oplus$ *e* $\otimes$ *para o conjunto* $\mathbf{Z}_5$ *dos restos na divisão por 4. Sugestão, as funções deve ser*

`(ovezes x y)` *ou* `(omais x y)` *...*

6. *Considere o conjunto* $\mathbf{Z}_6$ *dos restos na divisão por 4 e as estrutura algébricas* $(\mathbf{Z}_6, \oplus)$, $(\mathbf{Z}_6, \otimes)$*, que já foram mencionadas nas questões anteriores. Esta questão parece ser uma repetição enfadonha das anteriores e é um erro pensar assim!*

   Estrutura algébrica

   (a) *(V)[ ](F)[ ] A operação binária* $\oplus$*, definida em* $\mathbf{Z}_6$*, é comutativa, asssociativa e distributiva.*

   (b) *(V)[ ](F)[ ] A operação binária* $\oplus$*, definida em* $\mathbf{Z}_6$*, é comutativa, asssociativa, Existe um elemento neutro relativamente a* $\oplus$ *em* $(\mathbf{Z}_6, \oplus)$*, e todo elemento* $x \in \mathbf{Z}_6$ *tem um único inverso relativamente a* $\oplus$ *em* $(\mathbf{Z}_6, \oplus)$*.*

   (c) *(V)[ ](F)[ ] A operação binária* $\otimes$*, definida em* $\mathbf{Z}_6$*, é comutativa, asssociativa, existe um elemento neutro relativamente a* $\otimes$ *em* $(\mathbf{Z}_6, \otimes)$*, e todo elemento* $x \in \mathbf{Z}_6$ *tem um único inverso relativamente a* $\otimes$ *em* $(\mathbf{Z}_6, \otimes)$*.*

   (d) *(V)[ ](F)[ ] Como as duas operações binárias* $\otimes, \oplus$ *estão definidas em* $\mathbf{Z}_6$ *então podemos considerar a estrutura algébrica* $(\mathbf{Z}_6, \oplus, \otimes)$ *e valem as propriedades:*

      i. $\oplus$ *é comutativa, asssociativa, existe um elemento neutro relativamente a* $\oplus$ *em* $(\mathbf{Z}_6, \oplus)$ *e todo elemento* $x \in \mathbf{Z}_6$ *tem um único inverso relativamente a* $\oplus$ *em* $(\mathbf{Z}_6, \oplus)$*.*

      ii. $\otimes$ *é comutativa, asssociativa, existe um elemento neutro relativamente a* $\otimes$ *em* $(\mathbf{Z}_6, \otimes)$ *e todo elemento* $x \in \mathbf{Z}_6$ *tem um único inverso relativamente a* $\otimes$ *em* $(\mathbf{Z}_6, \otimes)$*.*

      iii. $\otimes$ *é distributiva relativamente a* $\oplus$*.*

   (e) *(V)[ ](F)[ ] Como as duas operações binárias* $\otimes, \oplus$ *estão definidas em* $\mathbf{Z}_6$ *então podemos considerar a estrutura algébrica* $(\mathbf{Z}_6, \oplus, \otimes)$ *e valem as propriedades:*

      i. $\oplus$ *é comutativa, asssociativa, existe um elemento neutro relativamente a* $\oplus$ *em* $(\mathbf{Z}_6, \oplus)$ *e todo elemento* $x \in \mathbf{Z}_6$ *tem um único inverso relativamente a* $\oplus$ *em* $(\mathbf{Z}_6, \oplus)$*.*

      ii. $\otimes$ *é comutativa, asssociativa, existe um elemento neutro relativamente a* $\otimes$ *em* $(\mathbf{Z}_6, \otimes)$*, mas nem todo elemento* $x \in \mathbf{Z}_6$ *tem um inverso relativamente a* $\otimes$ *em* $(\mathbf{Z}_6, \otimes)$*.*

      iii. $\otimes$ *é distributiva relativamente a* $\oplus$*.*

Compare $(\mathbf{Z}_6, \oplus, \otimes)$ *com* $(\mathbf{Z}, +, \cdot)$*,* $(\mathbf{Z}_5, \oplus, \otimes)$ *com* $(\mathbf{Z}, +, \cdot)$*,* $(\mathbf{Z}_4, \oplus, \otimes)$ *com* $(\mathbf{Z}, +, \cdot)$*, escreva algumas linhas sobre esta comparação. O que torna diferente uma destas estruturas das outras duas.*

Experimente montar um sistema de funções `LISP`*, um programa, que gere a tabela operatória para cada uma das operações* $\oplus$ *e* $\otimes$ *para o conjunto* $\mathbf{Z}_6$ *dos restos na divisão por 4. Sugestão, as funções deve ser*

`(ovezes x y)` *ou* `(omais x y)` *...*

7. $(\mathbf{Z}_6, \oplus)$ $(\mathbf{Z}_5, \oplus)$ $(\mathbf{Z}_4, \oplus)$ *e* $(\mathbf{Z}, +)$ *são a mesma estrutura, têm as mesma propriedades, satisfazem ao mesmo padrão, como uma* classe *em* programação orientada a objeto. *Esta estrutura se chama "*grupo*", ou seja* $(\mathbf{Z}_6, \oplus)$ $(\mathbf{Z}_5, \oplus)$ $(\mathbf{Z}_4, \oplus)$ *e* $(\mathbf{Z}, +)$ *são exemplos de grupo (instâncias desta estrutura, numa linguagem usada em computação). Nesta questão vou explorar um exemplo ligeiramente diferente dos anteriores.*

   Considere o conjunto das matrizes da forma

$$T = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \tag{3}$$

   Este conjunto é costumeiramente designado por $\mathcal{M}_{2,2}$ *indicando a dimensão das matrizes envolvidas:* 2×2*.*

   Estrutura Algébrica

   (a) *(V)[ ](F)[ ]* $\mathcal{M}_{2,2}$ *é fechado para o produto de matrizes.*

   (b) *(V)[ ](F)[ ] Se "o" designar o produto de matrizes, então* $(\mathcal{M}_{2,2}, o)$ *é uma estrutura associativa.*

   (c) *(V)[ ](F)[ ] Se* $T = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ *e* $S = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ *então* $SoT = ToS$*.*

   Você pode usar `octave`*, um programa para Álgebra Linear Computacional livremente distribuido sob GPL, então*

```
T = [1,0;1,1];  S = [1,1;0,1];

e o produto se calcula com

S*T
```

   (d) *(V)[ ](F)[ ] Se* $T = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ *e* $S = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ *então* $SoT \neq ToS$*.*
   Este exemplo **prova** *que o produto de matrizes não é comutativo.*

   (e) *(V)[ ](F)[ ] Para qualquer matriz* T *de* $\mathcal{M}_{2,2}$ *existe uma outra matriz* $S = T^{-1}$ *tal que* $SoT = ToS = I$ *em que* I *é a matriz identidade.*

8. *Ainda trabalhando com* $\mathcal{M}_{2,2}$*, o conjunto das matrizes de dimensão* 2×2*.*

   Estrutura Algébrica

(a) (V)[ ](F)[ ] *Para a matriz* T *de* $\mathcal{M}_{2,2}$ *tenha uma inversa* $S = T^{-1}$ *tal que* $SoT = ToS = I$ *em que* I *é a matriz identidade é* preciso *que* $\det(T) = 1$

(b) (V)[ ](F)[ ] *Para a matriz* T *de* $\mathcal{M}_{2,2}$ *tenha uma inversa* $S = T^{-1}$ *tal que* $SoT = ToS = I$ *em que* I *é a matriz identidade é* suficiente *que* $\det(T) = 1$

(c) (V)[ ](F)[ ] *Para a matriz* T *de* $\mathcal{M}_{2,2}$ *tenha uma inversa* $S = T^{-1}$ *tal que* $SoT = ToS = I$ *em que* I *é a matriz identidade é* suficiente *que* $\det(T) \neq 0$

(d) (V)[ ](F)[ ] *Os itens 8b e 8c definem dois conjuntos* $\mathcal{U}$*, das matrizes cujo determinante é exatamente 1,* $\mathcal{S}$ *das matrizes cujo determinante é diferente de zero, então* $\mathcal{U} \subset \mathcal{S}$

(e) (V)[ ](F)[ ] *Os itens 8b e 8c definem dois conjuntos* $\mathcal{U}$*, das matrizes cujo determinante é exatamente 1,* $\mathcal{S}$ *das matrizes cujo determinante é diferente de zero, então* $\mathcal{U} \supset \mathcal{S}$

9. *Ainda trabalhando com* $\mathcal{M}_{2,2}$*, o conjunto das matrizes de dimensão* 2×2*. Com a notação introduzida no item 8d definindo os conjuntos* $\mathcal{U}, \mathcal{S}$*.*

   Estrutura Algébrica

   (a) (V)[ ](F)[ ] $(\mathcal{U}, o)$ *e* $(\mathcal{S}, o)$ *são estruturas associativas.*

   (b) (V)[ ](F)[ ] $(\mathcal{U}, o)$ *e* $(\mathcal{S}, o)$ *são estruturas comutativas.*

   (c) (V)[ ](F)[ ] $(\mathcal{U}, o)$ *e* $(\mathcal{S}, o)$ *são fechados para o produto de matrizes "o".*

   (d) (V)[ ](F)[ ] *Todo elemento de* $M \in \mathcal{U}$ *tem um inverso* $N \in \mathcal{U}$*, relativamente ao produto de matrizes "o".*

   (e) (V)[ ](F)[ ] *Todo elemento de* $M \in \mathcal{S}$ *tem um inverso* $N \in \mathcal{S}$*, relativamente ao produto de matrizes "o".*

   $\mathcal{U}$ *e* $\mathcal{S}$ *são dois exemplos de grupos não comutativos porque o produto de matrizes não é comutativo.*

   Um caso particular (um subconjunto de $\mathcal{U}$*) é muito importante em* Computação Gráfica plana *e tem a forma* $T = \begin{bmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{bmatrix}$ *verifique que o determinante é 1. São as matrizes de rotação, elas produzem uma rotação de* θ *quando aplicadas a qualquer objeto geométrico.*

10. **Notação:** *Considere um conjunto formado de quatro objetos:*

    $S = \{a, b, c, d\}$

    Uma função injetiva definida de S *em* S *é também, necessariamente, bijetiva e se chama uma permutação de* S*. Por exemplo, todas as linhas das tabelas de* $(\mathbf{Z}_p, \oplus)$ *são permutações do conjunto* $\mathbf{Z}_p$*.*

    (abc) *é a função* $a \mapsto b; b \mapsto c; c \mapsto a$ *é um três cíclo.*

(acb) *é a função* $a \mapsto c; c \mapsto b; b \mapsto a$ *é diferente de* (abc)*.*

(ab) *é a função* $a \mapsto b; b \mapsto a; c \mapsto c;$ *é um dois cíclo.*

(ac) *é a função* $a \mapsto c; c \mapsto a; b \mapsto b;$

I *é a identidade.*

Há 4! funções que permutam os elementos de S *e esta notação se chama "de ciclos" porque ela identifica as sub-permutações que são circulares.*

Eu tentei fazer um programa em LISP para simular esta operações e até agora falhei.

O nome do conjunto destas permutações é **Notação:** $\mathrm{sim}(4)$ *e a operação de composição de funções produz de duas permutações outra permutação.* **Notação:** *vou usar o símbolo "o" para representar a composição de permutações ou simples justaposição delas.*

Aplicação: *em encriptação (o caso mais elementar usado pelos alemães na WWII e quebrado pelo grupo de matemáticos trabalhando para o exército inglês, entre os quais, matemáticos, estava Alan Turing).*

Estrutura Algébrica

(a) (V)[ ](F)[ ] $(abc)(acb) = I$

(b) (V)[ ](F)[ ] $(ab)(ab) = I$

(c) (V)[ ](F)[ ] $(abc)(bac) = I \Rightarrow (acb) = (bac)$

(d) (V)[ ](F)[ ] *Qualquer dois-ciclo é o seu próprio inverso.*

(e) (V)[ ](F)[ ] *O produto de permutações não é comutativo, assim*

```
(sim(4), o)
```

é um exemplo de grupo não comutativo com 24 elementos.