Matemática Discreta
grupos finitos
T. Praciano-Pereira

Lista numero 04
tarcisio.praciano@gmail.com
Dep. de Computação

alun@:

16 de abril de 2013 — **Univ. Estadual Vale do Acaraú**

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 *Grupos finitos objetivo: Encriptar dados com permutações*
palavras chave: *grupos finitos, permutações*

1. *grupos finitos*

   Faça a tabela de adição do conjunto dos restos na divisão por 5. Este é o conjunto $\mathbf{Z}_5$ *e as opções abaixo dizem respeito às estruturas* $(\mathbf{Z}_5, +)(\mathbf{Z}_5, *)$

   (a) *(V)[ ](F)[ ] Em cada linha da tabela de adição de* $(\mathbf{Z}_5, +)$ *há uma cópia exata do conjunto* $\mathbf{Z}_5$.

   (b) *(V)[ ](F)[ ] Cada linha da tabela de adição de* $(\mathbf{Z}_5, +)$ *é uma permutação do conjunto* $\mathbf{Z}_5$.

   (c) *(V)[ ](F)[ ] Se você quiser enviar uma cópia enctriptada de* $\mathbf{Z}_5$ *basta enviar uma linha e, separadamente, como chave, o elemento que foi adicionado gerando esta linha. Obviamente isto somente teria utilidade prática para* $\mathbf{Z}_n$ *com n grande.*

   (d) *(V)[ ](F)[ ] Na tabela operatória da multiplicação de* $(\mathbf{Z}_5, *)$ *cada linha da tabela é uma permutação do conjunto* $\mathbf{Z}_5$.

   (e) *(V)[ ](F)[ ] Na tabela operatória da multiplicação de* $(\mathbf{Z}_5, *)$ *cada linha da tabela é uma permutação do conjunto* $\mathbf{Z}_5$ *se o zero for excluído da tabela.*

2. *grupos finitos*

   Continuando com as tabelas operatóriws de $\mathbf{Z}_5$*, adição e multiplicação.*

   (a) *(V)[ ](F)[ ] A solução de* $7x + 4 = 9$ *é* $x = 10$.

(b) (V)[ ](F)[ ] *A equação no item anterior está mal posta porque não existe o elemento* $10 \in \mathbf{Z}_5$.

(c) (V)[ ](F)[ ] *A soluçãode* $3x + 4 = 2$ *é* $x = 0$.

(d) (V)[ ](F)[ ] *A soluçãode* $3x + 4 = 2$ *é* $x = 1$.

(e) (V)[ ](F)[ ] *Para resolver a equaçã* $3x + 4 = 2$, *posso resolver como se fosse em* $\mathbf{Z}$ *e depois "rebater" a solução de volta para* $\mathbf{Z}_5$

3. *Continuando com as tabelas operatóriws de* $\mathbf{Z}_5$, *adição e multiplicação.*

   grupos finitos

   (a) (V)[ ](F)[ ] *Como a equação* $3x+4 = 1$ *não tem solução em* $\mathbf{Z}$ *então ela não tem solução em* $\mathbf{Z}_5$.

   (b) (V)[ ](F)[ ] *A equação* $3x + 4 = 1$ *não tem solução em* $\mathbf{Z}$ *mas ela tem solução em* $\mathbf{Z}_5$.

   (c) (V)[ ](F)[ ] *A equação* $3x + 4 = 1$ *tem por solução em* $\mathbf{Z}_5; x = 0$.

   (d) (V)[ ](F)[ ] *Não é possível resolver a equação* $3x + 4 = 1$ *em* $\mathbf{Z}$ *e rebater a solução para* $\mathbf{Z}_5$.

   (e) (V)[ ](F)[ ] *A equação* $3x + 4 = 1$ *tem por solução em* $\mathbf{Z}_5; x = 3$.

4. *grupos finitos*

   Continuando agora com as tabelas operatóriws de $\mathbf{Z}_7$, *adição e multiplicação.*

   (a) (V)[ ](F)[ ] *A solução de* $3x + 4 = 1$ *é* $x = 1$.

   (b) (V)[ ](F)[ ] *A solução de* $3x + 4 = 1$ *é* $x = 2$.

   (c) (V)[ ](F)[ ] *A solução de* $3x + 4 = 1$ *é* $x = 0$.

   (d) (V)[ ](F)[ ] *A solução de* $3x + 4 = 1$ *é* $x = -1$.

   (e) (V)[ ](F)[ ] *A solução de* $3x + 4 = 1$ *é* $x = 7$.

5. *O grupo* $(sim(3), o)$

   Continuando agora com a tabela operatória, agora de sim(3).

   Considere que sim(3) é o conjunto das permutações dos três elementos $\{a, b, c\}$.

   Você pode fazer esta tabela usando os ciclos (abc), (ab) há um total de $6 = 3!$ *ciclos, elementos do conjunto sim(3) que com a operação composição é um grupo. Vamos verificar isto nas opções abaixo.*

   (abc) signfica: $a \mapsto b; b \mapsto c; c \mapsto a;$ *e*

   (ab) signfica: $a \mapsto b; b \mapsto a; c \mapsto c;$ *sendo o elemento c um elemento fixo.*

   I é a função identidade.

   $sim(3) = \{I, (ab), (ac), (bc), (abc), (acb)\}$

(a) (V)[ ](F)[ ] $(abc)(abc) = (ab)$

(b) (V)[ ](F)[ ] $(abc)(abc) = (ba)$

(c) (V)[ ](F)[ ] $(abc)(abc) = (ac)$

(d) (V)[ ](F)[ ] $(ac)(ac) = I$

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

6. *O grupo* $(sim(3), o)$

   Continuando agora com a tabela operatória de sim(3) definido na questão 5.

   (a) (V)[ ](F)[ ] *O inverso de (abc) é (bca)*

   (b) (V)[ ](F)[ ] *O inverso de (abc) é (acb)*

   (c) (V)[ ](F)[ ] *O inverso de todo dois-ciclo é ele mesmo.*

   (d) (V)[ ](F)[ ] *Se você enviar a chave (abc) quem a receber sabe que os dados são* $\{I, (ab), (ac), (bc), (abc), (acb)\}$

   (e) (V)[ ](F)[ ] *Se você enviar a chave (abc) quem a receber sabe que os dados são* $\{(abc), (bc), (ab), (ac), (ac), (bc)\}$ *mas depende da ordem da multiplicação que precisa ser combinada.*

7. *O grupo* $(sim(3), o)$

   (a) (V)[ ](F)[ ] *Todo elemento de* $sim(3)$ *tem um inverso relativamente à operação de composição "o".*

   (b) (V)[ ](F)[ ] *A composição é uma operação binária comutativa.*

   (c) (V)[ ](F)[ ] $(sim(3), o)$ *é um exemplo de grupo não comutativo.*

   (d) (V)[ ](F)[ ] *Os elementos* $I, (ab)$ *formam um subgrupo do grupo* $(sim(3), o)$*, quer dizer, este subconjunto é fechado para a operação "o" e todo elemento tem inverso.*

   (e) (V)[ ](F)[ ] *Todos os dois cíclos de* $sim(3)$ *junto com a identidade I formam um subgrupo.*

8. *(abc) e (acb) são os dois três-cíclos do grupo* $(sim(3), o)$*.*

   (a) (V)[ ](F)[ ] *O subconjunto* $\{I, (abc), (acb)\}$ *é fechado para operação "o" e como* $(abc)^{-1} = (acb)$ *então este subconjunto é um grupo de* $(sim(3), o)$*.*

   (b) (V)[ ](F)[ ] *As potências*[1] *de (abc) são*

   $$I, (abc), (acb)$$

[1] Potência é a iteração da operação do grupo.

(c) (V)[ ](F)[ ] *A solução da equação* $(ab)x = (abc)$ *é* (bc).

(d) (V)[ ](F)[ ] *A solução da equação* $(ab)x = (abc)$ *é* (bc).

(e) (V)[ ](F)[ ] *A solução da equação* $(ab)x = (abc)$ *é* (ac).

9. *Este exemplo somente mostra o que é possível fazer, à mão. Os alemães na WWII criaaram uma máquina de enctriptação que permutava as letras do alfabeto. Bastava saber qual era a chave para decodificar o texto.*

   O grupo $(sim(3), o)$

   (a) (V)[ ](F)[ ] *Toda linha da tabela de* $(sim(3), o)$ *representa uma permutação dos elementos de* $sim(3)$.

   (b) (V)[ ](F)[ ] *Se a chave for* (ab) *a permutação será*

   $$\{(ab), I, (acb), (abc), (ac), (bc)\}$$

   (c) (V)[ ](F)[ ] *Se a chave for* (ab) *a permutação será*

   $$\{(ab), I, (abc), (acb), (ac), (bc), \}$$

   (d) (V)[ ](F)[ ] *Se a chave for* (abc) *a permutação será*

   $$\{(abc), (bc), (abc), (ac), (cb), I\}$$

   (e) (V)[ ](F)[ ] *Se a chave for* (abc) *a permutação será*

   $$\{(abc), (bc), (abc), (ac), (acb), I\}$$

10. *O grupo* $sim(4)$ *das permutaçõe de quatro elementos terá* $24 = 4!$ *elementos e já mostra muito mais interessante, entretanto trabalhoso para estudar manualmente. Há um início de trabalho para automatizar este processo nos meus programas em LISP. O objetivo aqui é estimular o trabalho teórico (fazer o programa).*

    $sim(4) = \{I, (abcd), (abdc), (acbd), (acdb), (adbc), (adcb), \ldots\}$

    O grupo $(sim(3), o)$

    (a) (V)[ ](F)[ ] *Os dois-ciclos de* $sim(4)$ *são* $\{(ac), (ab), (ad), (bc), (bd), (cd)\}$

    (b) (V)[ ](F)[ ] *Os três-ciclos de* $sim(4)$ *são*

    $$\{(abc), (acb), (abd), (adb), (acd), (adc), (bcd), (bdc)\}$$

    (c) (V)[ ](F)[ ] *Os quatro-ciclos de* $sim(4)$ *são*

    $$\{(abcd), (abdc), (acbd), (acdb), (adbc), (adcb)\}$$

(d) *(V)[ ](F)[ ]* *As potências de* $(abcd)$ *são*

$$\{I, (abcd), (ac)(bd), (adc)\}$$

e é um subgrupo de $sim(4)$

(e) *(V)[ ](F)[ ]* *As potências de* (abc) *são*

$$\{I, (abc), (acb)\}$$

e é um subgrupo de $sim(4)$