MB104 – 2. demonstrovaná cvičení
Algebraické struktury

Masarykova univerzita
Fakulta informatiky

23.2. 2009

Příklad 1. *Rozhodněte o následujících množinách a operacích, jaké tvoří struktury (grupoid, pologrupa, grupa). Určete zda existují levé (pravé) neutrální prvky a zda ja daná operace komutativní.*

1. *Podmnožiny množiny přirozených čísel spolu s operací průnik,*
2. *přirozená čísla spolu s binární operací největší společný dělitel,*
3. *množina všech invertibilních matic* 3×3 *nad* $\mathbb{R}$ *spolu se sčítáním,*
4. *množina všech matic* 3×3 *nad* $\mathbb{R}$ *spolu s násobením matic,*
5. *množina všech matic* 3×3 *spolu se sčítáním matic,*
6. *množina všech invertibilních matic* 3×3 *nad* $\mathbb{Z}_2$ *s násobením matic,*
7. *množina* $(\mathbb{Z}_9, +)$,
8. *množina* $(\mathbb{Z}_9, \cdot)$,

Svá tvrzení zdůvodněte (proč je něco např. pouze grupoid a není pologrupa . . .). U posledního příkladu sestavte tabulku dané operace.

1. Pologrupa s neutrálním prvkem (monoid).

1. Pologrupa s neutrálním prvkem (monoid).
2. Pologrupa.

1. Pologrupa s neutrálním prvkem (monoid).
2. Pologrupa.
3. Monoid.

1. Pologrupa s neutrálním prvkem (monoid).
2. Pologrupa.
3. Monoid.
4. Grupa.

1. Pologrupa s neutrálním prvkem (monoid).
2. Pologrupa.
3. Monoid.
4. Grupa.
5. Grupa.

1. Pologrupa s neutrálním prvkem (monoid).
2. Pologrupa.
3. Monoid.
4. Grupa.
5. Grupa.
6. Grupa.

1. Pologrupa s neutrálním prvkem (monoid).
2. Pologrupa.
3. Monoid.
4. Grupa.
5. Grupa.
6. Grupa.
7. Pologrupa.

Příklad 2. *Určete grupu*

- *rotačních*
- *všech*

symetrií krychle (popište všechny symetrie). Jsou tyto grupy komutativní?

Příklad 3. *Rozložte na součin transpozic následující permutaci:*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 6 & 8 & 7 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

Spočtěte σ^{2009}.

Určete počet všech trojprvkových grupoidů (až na isomorfismus, tj. přejmenování prvků)

Určete počet všech trojprvkových grupoidů (až na isomorfismus, tj. přejmenování prvků)
Určete počet všech trojprvkových grup (až na isomorfismus, tj. přejmenování prvků)

Nalezněte všechny podgrupy grupy symetrií tetraedru.

Eulerova funkce φ

Pro dané přirozené číslo n udává počet čísel menších než n, která jsou s n nesoudělná.

Eulerova funkce φ

Pro dané přirozené číslo n udává počet čísel menších než n, která jsou s n nesoudělná.

Eulerova věta

Pro libovolná nesoudělná kladná celá (a, m) platí

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

Bezoutova rovnost. Pro libovolná celá čísla a, b existují celá čísla u, v taková, že

$$au + bv = (a, b),$$

kde (a, b) je největší společný dělitel čísel (a, b).

Bezoutova rovnost. Pro libovolná celá čísla a, b existují celá čísla u, v taková, že

$$au + bv = (a, b),$$

kde (a, b) je největší společný dělitel čísel (a, b).

Příklad *Určete inverzi prvku* 17 *v grupě invertibilních prvků* $\mathbb{Z}_{35}$.

RSA algoritmus.