Algebra, písemka

17. května 2024

Úlohy 1 – 3: 45 minut; celá písemka 150 minut

Informace

Všechny své odpovědi (např. v 4, 5, 6) samozřejmě zdůvodněte.

V početních příkladech 4, 5, 6 můžete používat tvrzení z přednášky, **pokud je zformulujete**.

V důkazech 7, 8, 9 můžete používat předcházející tvrzení z přednášky, **pokud je zformulujete**. („Tvrzení“ samozřejmě zahrnují i lemmata, věty, atd.)

Z maxima 90 bodů na známku 1, 2, resp. 3 stačí 79, 68, resp. 57 bodů.

1. (10 bodů) Popište, jak funguje kryptosystém RSA pro šifrování s veřejným klíčem (včetně volby klíčů atd.).

2. (10 bodů) a) Definujte pojmy euklidovská norma, euklidovský obor, ireducibilní rozklad, jednoznačný ireducibilní rozklad, gaussovský obor.

   b) Jaký platí vztah mezi euklidovskými a gaussovskými obory? *(Svou odpověď nemusíte zdůvodňovat.)*

3. (10 bodů)

   a) Definujte faktorokruh (včetně operací na něm). *Můžete uvést kteroukoli ze dvou definic z přednášky.*

   Uveďte příklad faktorokruhu (podle vámi zvolené definice), který

   b) je těleso;

   c) není obor.

   Své odpovědi nemusíte zdůvodňovat.

4. (10 bodů) V celých číslech $\mathbb{Z}$ spočtěte $\mathrm{NSD}(74, 232)$ a (nějaké) příslušné Bézoutovy koeficienty.

5. (10 bodů) Dokažte, že polynom

   $$\frac{2}{3}x^7 + 3x^5 - 2x^4 + 5x^2 + 9x + 7 \in \mathbb{Q}[x]$$

   je ireducibilní v $\mathbb{Q}[x]$.

6. (10 bodů)

   a) Zformulujte Burnsideovu větu.

   b) Uvažujme rovnostranný trojúhelník o straně 3 rozdělený na 9 rovnostranných trojúhelníků o straně 1. Každý z těchto malých trojúhelníků obarvíme jednou ze 4 barev. Určete celkový počet možných obarvení až na otočení a zrcadlení (čili dvě obarvení považujeme za stejná, pokud se liší otočením nebo zrcadlením velkého trojúhelníka).

   Svou odpověď nemusíte vyčíslovat (např. $\frac{8^5-3\cdot 17}{5^2+111^3}$ *by stačilo jako odpověď).*

7. (10 bodů) Definujte algebraické rozšíření těles. Zformulujte a dokažte větu o tom, že každé rozšíření těles konečného stupně je algebraické.

8. (10 bodů) Zformulujte a dokažte 2. větu o izomorfismu pro grupy. *Úloha se týká pouze příslušného izomorfismu, nikoli popisu všech podgrup ve faktorgrupě.*

9. (10 bodů) Zformulujte a dokažte základní větu algebry.