Algebra, písemka 1 (předtermín)

1. června 2021
150 minut

Informace

Všechny své odpovědi (např. v 3b, 4, 5, 6) samozřejmě zdůvodněte.

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

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

Z maxima 90 bodů na známku 1, 2, resp. 3 bude určitě stačit 79, 68, resp. 57 bodů, možná i trochu méně: přesné hranice určím podle obtížnosti písemky.

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

2. (10 bodů)

   a) Definujte pojmy ideál, hlavní ideál a obor hlavních ideálů.

   b) Uveďte příklad oboru, který *není* oborem hlavních ideálů. *(Svou odpověď nemusíte zdůvodňovat.)*

3. (10 bodů)

   a) Definujte minimální polynom prvku a nad tělesem T.

   b) Najděte minimální polynom prvku $\sqrt{5}$ nad $\mathbb{Q}$.

4. (10 bodů) Najděte ireducibilní rozklad prvku $12 - 6i$ v oboru $\mathbb{Z}[i]$. *(Dokažte, že jednotlivé faktory jsou opravdu ireducibilní!)*

5. (10 bodů) Najděte všechny grupové homomorfismy ze $\mathbb{Z}_{10}$ do $\mathbb{Z}_{12}$. Pro každý z nich určete jeho jádro a obraz.

6. (10 bodů)

   a) Zformulujte Burnsideovu větu.

   b) Určete počet obarvení vrcholů pravidelného 6-úhelníka 4 barvami až na otočení (čili dvě obarvení považujeme za stejná, pokud se liší otočením 6-úhelníka).

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

7. (10 bodů) Definujte rozkladové třídy podle podgrupy. Zformulujte a dokažte lemma o disjunkci rozkladových tříd.

8. (10 bodů) Dokažte, že Galoisova grupa polynomu je izomorfní podgrupě symetrické grupy S_n pro nějaké $n \in \mathbb{N}$ *(napřed zformulujte, co přesně dokazujete).*

9. (10 bodů) Zformulujte a dokažte čínskou zbytkovou větu pro polynomy.