Jméno:

Tvrzení a definice pečlivě formulujte včetně všech předpokladů. Pište text stejně formálně, jako je psán ve skriptech (tj. formálněji než na tabuli). Odpovědi na otázky zdůvodněte. Pokud používáte nějaké netriviální tvrzení z přednášky, uveďte explicitně odkaz (často budete vyzváni, abyste všechna použitá tvrzení zformulovali). Časový limit je 120 minut.

1. (6 bodů) Napište Viètovy vztahy pro polynom třetího stupně. Zformulujte tvrzení včetně značení.

2. (10 bodů) Spočtěte $3^{3^{3^3}} \mod 33$. Připomínám, že $a^{b^c} = a^{(b^c)}$.

3. (6 bodů) Rozhodněte, zda je polynom 2 ireducibilní v oboru (a) $\mathbb{Z}_5[x]$, (b) $\mathbb{Z}[x]$, (c) $\mathbb{Z}[\sqrt{2}][x]$, (d) $\mathbb{Q}(i)[x]$. Stručně zdůvodněte!

4. (10 bodů) Spočtěte $\mathrm{NSD}(1+13i, 17-6i)$ v oboru $\mathbb{Z}[i]$.

Jméno:

5. (14 bodů) Napište nějaké těleso s 81 prvky a dokažte, že to je opravdu těleso, včetně popisu výpočtu inverzního prvku. Využít můžete cokoliv z teorie eukleidovských oborů.

6. (19 bodů) Buď $a \in \mathbb{C}$.

(a) Definujte pojem ideálu v oboru $\mathbb{Q}[x]$ a dokažte, že množina všech polynomů z $\mathbb{Q}[x]$, které mají kořen a, tvoří ideál v oboru $\mathbb{Q}[x]$.

(b) Pomocí bodu (a) dokažte následující tvrzení: existuje polynom $f_a \in \mathbb{Q}[x]$ takový, že polynom $g \in \mathbb{Q}[x]$ má kořen a právě tehdy, když $f_a \mid g$ v $\mathbb{Q}[x]$. Formulujte všechny věty, které v důkazu používáte.

(c) Dokažte, že polynom f_a z bodu (b) musí být ireducibilní v $\mathbb{Q}[x]$.

(d) Z bodu (b) plyne, že kdykoliv mají dva polynomy $f, g \in \mathbb{Q}[x]$ společný komplexní kořen, pak jsou soudělné. Platí i opačné tvrzení, tj. jestliže jsou polynomy $f, g \in \mathbb{Q}[x]$ soudělné, pak mají společný komplexní kořen? Dokažte, nebo uveďte protipříklad.