Teoretické otázky (pokrývají víceméně úplný seznam důkazů, které je třeba umět)

Uveďte postup řešení polynomiální rovnice $x^3 + bx + c = 0$ v $\mathbb{C}$.

Uveďte postup řešení polynomiální rovnice $x^4 + bx^2 + cx + d = 0$ v $\mathbb{C}$.

Formulujte a dokažte kritérium existence racionálního kořene.

Dokažte, že existuje transcendentní číslo. Bez důkazu použijte fakt, že množina reálných čísel je nespočetná.

Dokažte, že množina reálných čísel je nespočetná.

Formulujte a dokažte Základní větu aritmetiky. Bez důkazu můžete použít Bézoutovu rovnost pro celá čísla.

Formulujte rozšířený Eukleidův algoritmus (počítající NSD i Bézoutovy koeficienty) pro celá čísla a dokažte jeho správnost.

Formulujte a dokažte Eulerovu větu.

Formulujte a dokažte Čínskou větu o zbytcích.

Formulujte a dokažte vzorec na výpočet Eulerovy funkce.

Definujte komutativní okruh s jednotkou a dokažte přímo z definice, že $a \cdot (-b) = -(a \cdot b)$.

Definujte obor integrity a dokažte přímo z definice, že pokud $ac = bc$ a $c \neq 0$, pak $a = b$.

Dokažte, že konečný obor integrity je nutně tělesem.

Definujte polynom nad daným oborem integrity, definujte základní operace na polynomech a dokažte, že polynomy s těmito operacemi tvoří obor integrity.

Definujte podílové těleso a dokažte, že je definice korektní. Nemusíte ověřovat axiomy těles.

Definujte podílové těleso a ověřte, že jde skutečně o těleso. Nemusíte ověřovat, že je definice korektní.

Dokažte, že $a \parallel b$ právě tehdy, když $a = bq$ pro nějaký invertibilní prvek q.

Formulujte a dokažte větu o tom, jak v gaussovských oborech vypadají dělitelé prvku s daným ireducibilním rozkladem.

Dokažte, že v gaussovských oborech existují NSD všech dvojic prvků. Bez důkazu použijte větu o tom, jak v gaussovských oborech vypadají dělitelé prvku s daným ireducibilním rozkladem.

Dokažte, že v gaussovských oborech, pro každý ireducibilní prvek p, platí: jestliže $p \mid ab$, pak $p \mid a$ nebo $p \mid b$. Bez důkazu použijte větu o tom, jak v gaussovských oborech vypadají dělitelé prvku s daným ireducibilním rozkladem.

Dokažte, že v gaussovských oborech neexistují nekonečné klesající řetězce vlastních dělitelů Bez důkazu použijte větu o tom, jak v gaussovských oborech vypadají dělitelé prvku s daným ireducibilním rozkladem.

Dokažte, že pokud v daném oboru neexistují nekonečné klesající řetězce vlastních dělitelů, pak lze každý prvek rozložit na součin ireducibilních prvků.

Dokažte, že pokud v daném oboru existují NSD všech dvojic prvků, pak má každý prvek nejvýše jeden ireducibilní rozklad.

Formulujte rozšířený Eukleidův algoritmus (počítající NSD i Bézoutovy koeficienty) v eukleidovských oborech a dokažte jeho správnost.

Dokažte, že eukleidovské obory jsou gaussovské. Bez důkazu použijte Eukleidův algoritmus. Formulujte všechny věty, které používáte.

Definujte normu ν na oboru $\mathbb{Z}[\sqrt{s}]$ a dokažte, že $\nu(uv) = \nu(u)\nu(v)$ a že $\nu(u) = 1$ právě tehdy když $u \parallel 1$.

Definujte normu ν na oboru $\mathbb{Z}[i]$ a dokažte, že je tato norma eukleidovská.

Formulujte a dokažte Gaussovo lemma. Vysvětlete použité pojmy.

Formulujte a dokažte, jak spolu souvisí ireducibilita v $\mathbf{R}[x]$ a v $\mathbf{Q}[x]$, kde $\mathbf{Q}$ je podílové těleso oboru $\mathbf{R}$. Gaussovo lemma použijte bez důkazu.

Formulujte a dokažte, jak počítat NSD v oboru $\mathbf{R}[x]$ za pomocí NSD v oborech $\mathbf{R}$ a $\mathbf{Q}[x]$, kde $\mathbf{Q}$ je podílové těleso oboru $\mathbf{R}$. Gaussovo lemma použijte bez důkazu.

Dokažte, že obor polynomů nad gaussovským oborem je gaussovský. Bez důkazu použijte fakt, že v takovém oboru existují NSD všech dvojic polynomů. Formulujte všechny věty, které používáte.

Formulujte a dokažte větu o tom, že $f(a) = 0$ právě tehdy, když $x - a \mid f$.

Formulujte a dokažte větu o počtu kořenů daného polynomu.

Definujte grupu a dokažte přímo z definice, že v grupách platí $(a * b)' = b' * a'$.

Definujte grupu a dokažte přímo z definice, že v grupách platí $(a')' = a$.

Definujte grupu $\mathbb{Z}_n^*$ a ukažte dvě metody výpočtu inverzních prvků v této grupě.

Formulujte a dokažte větu o tom, jak vypadají prvky podgrupy generované danou množinou.

Definujte řád prvku a a dokažte, že je roven nejmenšímu n takovému, že $n \times a = e$, pokud takové existuje.

Dokažte, že podgrupy cyklických grup jsou cyklické.

Dokažte větu o počtu generátorů cyklických grup.

Sečtěte řadu $\sum_{d|n} \varphi(d)$. Bez důkazu můžete využít vlastnosti cyklických grup.

Formulujte a dokažte větu o cykličnosti multiplikativních grup těles.

Popište Diffie-Hellmanův protokol.

Dokažte Lagrangeovu větu, včetně pomocných lemmat.

Dokažte lemma o vztahu mezi velikostmi G, G_x a $[x]$. Bez důkazu můžete použít Lagrangeovu větu.

Dokažte Burnsideovu větu. Bez důkazu můžete použít vztah mezi velikostmi G, G_x a $[x]$ (tento vztah formulujte).