Zkoušený dostane dvě otázky, na které si písemně připraví odpovědi. Jedna otázka se bude týkat Gröbnerových bazí druhá ireducibilních rozkladů polynomů. V závorce jsou uvedena čísla tvrzení z přednášky, na něž otázka míří.

1. Gröbnerovy báze

1.1. Terminující, normální a konvergentní relace. Uspořádání na termech a polynomech a relace přepisování. Zformulujte a dokažte charakterizaci náležení rozdílu polynomů do ideálu s (Gröbnerovou) bází a napište a vysvětlete Buchbergerův algoritmus A. (2.1, 2.2)

1.2. Vyslovte, vysvětlete a dokažte tvrzení o ekvivalenci konvergentních, konfluentních, lokálně konfluentních a slabě lokálně konfluentních relacích. (3.2)

1.3. Kritické páry a s-polynomy. Zformulujte a dokažte Buchbergerovu větu a napište Buchbergerův algoritmus B. (2.5, 3.3)

1.4. Redukovaná Gröbnerova báze. Napište a vysvětlete algoritmus pro redukci Gröbnerovy báze. Dokažte existenci a jednoznačnost redukované normované Gröbnerova báze. (4.2, 4.4)

1.5. Napište a vysvětlete algoritmy rovnosti ideálů, nalezení báze průniku dvou ideálů a náležení radikálů (5.3, 5.5)

2. Faktorizace polynomů

2.1. Zformulujte a vysvětlete algoritmus bezčtvercového rozkladu polynomů. (6.4 a 6.5)

2.2. Zformulujte algoritmus bezčtvercového rozkladu polynomů nad konečným tělesem a odhadněte jeho časovou složitost. (6.7)

2.3. Napište Berlekampův algoritmus pro rozklad bezčtvercových polynomů nad konečnými tělesy a dokažte jeho korektnost. (7.3)

2.4. Zformulujte a vysvětlete algoritmus Henselova zdvihání. (8.3)

2.5. Zformulujte a vysvětlete algoritmus kombinace faktorů podle Zassenhause. Jak najít ireducibilní rozklad polynomů nad celými čísly? (9.3)