Abstrakt algebra med konkrete anvendelser 2
Aalborg Universitet (2013)
Spørgsmål (og pensum) til den mundtlige eksamen

1. Monomiale ordninger, polynomiers division i flere variable og Gröbner baser. Regning med Gröbner baser vha. computer
   Baggrund: Afsnit 21.2, 21.3, 21.4 i [GG] (også Afsnit 5.1-5.4 i [Lau]). Maple/Singular/Sage hjælp

2. Gröbner baser, Buchbergers algoritme og anvendelser.
   Baggrund: Afsnit 21.4, 21.5, 21.6 i [GG] (også Afsnit 5.4, 5.6, 5.7, 5.8, 5.9 i [Lau])

3. Endelige legemer og deres konstruktion. Berlekamps algoritme. Regning med endelige legemer vha. computer.
   Baggrund: Afsnit 4.6, 4.9 i [Lau] og Afsnit 2.1 og 2.2 i [JH]. Maple/Singular/Sage hjælp

4. Cyklotomiske polynomier, eksistens og entydighed af endelige legemer.
   Baggrund: Afsnit 4.4, 4.5 (ikke 4.5.1, 4.5.2, 4.5.3) og 4.8 i [Lau]

5. Reed-Solomon koder og deres dekodning (og lidt om list dekodning).
   Baggrund: Kapitel 5 og lidt af Kapitel 12 i [JH]

6. Cykliske koder (og BCH koder).
   Baggrund: Afsnit 2.3 og Kapitel 6 i [JH]

7. Offentlig-nøgle kryptografi (Knapsack, ElGamal, McEliece) og Secret Sharing.
   Baggrund: Afsnit 8.1, 8.4, 8.5, 8.6 i [MOV], Afsnit 4.5.2 i [Lau] og Afsnit 5.3 i [GG]

Grundbøger:

- [GG] Joachim von zur Gathen, Jürgen Gerhard "Modern Computer Algebra", 3rd Edition, Cambridge University Press, June 2013. ISBN: 9781107039032.
- [Lau] Niels Lauritzen "Concrete abstract algebra", Cambridge University Press, 2003, ISBN: 978-0-521-53410-9
- [JH] Jørn Justesen og Tom Høholdt, "A Course In Error-Correcting Codes". EMS Textbooks in Mathematics, 2004. ISBN 978-3-03719-001-2.
- [MOV] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, "Handbook of Applied Cryptography", CRC Press.