Curriculum for Algebra 2010-Aalborg University

Pensum/curriculum
The curriculum for the exam consists of the contents of the lectures excepting RSA. Namely, the following pages from [Lau] Niels Lauritzen, "Concrete abstract algebra", Cambridge University Press, 2003. ISBN: 978-0-521-53410-9.

(line -x means line x counting from the bottom of the page)
Chapter 1:

- Pages 1–24 (line -9)
- Page 26, Corollary 1.9.2 (Fermat's little theorem)

Chapter 2:

- Pages 50–Pages 77 (line 11)
- Pages 77 (line -7)–86 (line 9)
- Page 86, Lemma 2.9.28

Chapter 3:

- Pages 111–Pages 124 (line 2)
- Pages 125 (line -14)–133 (line 9)

Chapter 4:

- Pages 143–Pages 145
- Pages 147 (line -6)–159 (line -15)
- Pages 161–167 (line 2)

Appendix A:

- Section A.2.2 (page 227)

  We have also used some definitions and results from pages 223-227.

Errata
Be aware of the errata in the book that can be found at Course's web page, please. Unfortunately, I cannot guarantee that there are no errata in my slides.

Further comments

- Page 115, line 5: We can find in the slides (lection 12th) an equivalent definition of ideal: An ideal I of a ring R is a subset $I \subset R$ such that:

1. $0 \in I$
2. If $x, y \in I$, then $x + y \in I$
3. If $x \in I$ and $\lambda \in R$, then $x\lambda \in I$.

- Page 124, line 2: Consider also the following: Every element $\frac{a}{s} \in Q$, with $a \in R$ and $s \in R \setminus \{0\}$, can be written in the following way

$$\frac{a}{s} = \frac{a}{1} \cdot \frac{1}{s} = \frac{a}{1} \cdot \left(\frac{1}{s}\right)^{-1} = i(a) \cdot (i(s))^{-1}$$

  and this is why Q is called the field of fractions of R.

- Page 126, line -9: According to the book, the fact that $r = s$ is a consequence of the definition of *unique factorization into irreducible elements* (by applying Prop. 3.1.3). However, the usual definition is: x has a *unique factorization into irreducible elements* if for any other factorization

$$x = q_1 \cdots q_s,$$

  $r = s$ and for every $i = 1, \ldots, s$, $p_i | q_j$ for some j, that is, $pi = uq_j$, with u unit (and one says that p_i and q_j are related).

- Page 127, line 15: Consider the following proof for Proposition 3.5.3 (you can find it in the slides, lection 16th).

  Proof: ($\Longleftarrow$) The proof is the same as the unique factorization for integers (Theorem 1.8.5)

  Proof: ($\Longrightarrow$) Suppose that $x \in R$ is a non-zero element with two factorizations

$$x = p_1 \cdots p_r = q_1 \cdots q_s$$

  into irreducible elements. If an irreducible factor associated with a p_j appears on the right hand side for some q_j, we divide both sides by p_j. Therefore, we can assume from the beginning that the left and right hand side of the above equation have no associated irreducible elements in common and that $r \geq 1$ and $s \geq 1$. Now, since p_1 is a prime element, it follows that $p_1 | q_j$ for some j. However, this can only happen if p_1 and q_j are associated, contradiction.

- Page 157, line 5: Consider the following correction for the proof of Proposition 4.4.3 (i): Let $\mathbb{C}_n = \{\xi \in \mathbb{C} : \xi^n = 1\}$ the set of nth roots of unity. Since $\mathbb{C}_n$ has n elements that are roots of $X^n - 1$ and $X^n - 1$ is monic and its degree is n, we have that $X^n - 1 = \prod_{\xi \in \mathbb{C}_n} (X - \xi)$, by Theorem 4.3.5. Now consider lines 5–11 to conclude the proof.

Exam

An exam question from the following list will be chosen randomly. The student will have 30 minutes for preparing the question. Then, a 30 minutes (including grading) oral exam takes place. During the presentation some questions may be asked.

Exam questions

1. Greatest common divisor, the Euclidean algorithm and extended Euclidean algorithm in $\mathbb{Z}$.
2. The Chinese remainder theorem. Euler φ-function.
3. Greatest common divisor, prime numbers and unique factorization in $\mathbb{Z}$.
4. Groups, subgroups and cosets.
5. Normal subgroups and quotient groups.
6. Group homomorphisms and isomorphism theorem for groups.
7. Cyclic groups.
8. Symmetric group: simple transpositions and sign of a permutation as a group homomorphism.
9. Ideals and Quotient rings.
10. Ring homomorphisms.
11. Unique factorization into irreducible elements in a principal ideal domain.
12. Polynomials: division with remainder and roots.
13. Ideals and polynomials, irreducible polynomials and polynomial ring modulo an ideal.

Best regards,

Diego Ruano