Discrete Mathematics in Computer Science

M. Helmert, G. Röger
S. Eriksson
University of Basel
Computer Science
Fall Term 2021

Exercise Sheet 6

Due: Thursday, November 4, 2021

Exercise 6.1 (2 marks)

Why are the following tuples not groups?

(a) $(\mathbb{Z}, -)$

(b) $(\{0, 1\}, \max)$

Exercise 6.2 (2 marks)

Let $G = (S, \cdot)$ be a group. Show that for every $x \in S$, the inverse of x is unique, meaning there are no y and y' with $y \neq y'$, $x \cdot y = e$ and $x \cdot y' = e$.

Exercise 6.3 (2 marks)

Show that $S = \{\begin{pmatrix}1 & 2\end{pmatrix}, \begin{pmatrix}2 & 3 & 1\end{pmatrix}\}$ is a generating set of S_3 by showing how each permutation can be represented as a combination of S.
Hint: S_3 is the symmetric group of $\{1, 2, 3\}$.

Exercise 6.4 (1 mark)

Prove or disprove the following statement: For $c \neq 0$ we have that if $ac \mid bc$ then $a \mid b$.

Exercise 6.5 (3 marks)

For each of the following equivalences, use the operations from slide 19 of chapter B11 (handout version) or Fermat's Little Theorem to compute the *smallest* $x \in \mathbb{N}_0$ that satisfies the equivalence. Justify your answer.

(a) $(3a)^3 - 2 \equiv x \pmod 6$ with $a \equiv 1 \pmod 6$

(b) $a \equiv x \pmod 5$ with $\sqrt{a} - 3 \equiv 1 \pmod 5$

(c) $5^{602} \equiv x \pmod 7$

Do not compute 5^{602} explicitly!

Submission rules:
Upload a single PDF file (ending .pdf) generated using LaTeX. Put the names of all group members on top of the first page. Use page numbers or put your names on each page. Make sure your PDF has size A4 (fits the page size if printed on A4).