Foundations of Mathematics, Lecture 7

András Kornai

BMETE91AM35 Fall 2023-24

Groups

- All groups are defined as structures $\langle G, \cdot, ^{-1}, e \rangle$ (signature $=$ arity of operations 2,1,0)
- G is an arbitrary set
- We also need *group axioms*
- $\cdot$ is associative $\forall a, b, c \in G : (ab)c = a(bc)$
- e behaves as unit $\forall a \in G : ae = ea = a$
- $^{-1}$ behaves as inverse of $\cdot$ $\forall a \in G : aa^{-1} = a^{-1}a = e$
- Commutativity is *not* an axiom, typically $ab \neq ba$
- Commutative groups often written additively, using $+$ instead of $\cdot$ for the binary operation, $-$ instead of $^{-1}$ for the unary operation, and 0 instead of e for the nullary operation (distinguished constant)

Rings

- All rings are defined as structures $\langle R, +, \cdot, -, 0, 1\rangle$ (signature = arity of operations 2,2,1,0,0)
- We also need *ring axioms*
- $\langle R, +, -, 0\rangle$ is a commutative group
- $\langle R, \cdot, 1\rangle$ is a semigroup (no inverse, no commutativity, but assoc)
- Distributivity $a(b + c) = ab + ac; (a + b)c = ac + bc$

The ring Z_3

- Has three elements: $R = \{-1, 0, 1\}$
- Has addition defined by addition table

+	-1	0	1
-1	1	-1	0
0	-1	0	1
1	0	1	-1

- Mult by mult table

·	-1	0	1
-1	1	0	-1
0	0	0	0
1	-1	0	1

- Need to check associativity, distributivity!

Automata

- Finite state automata
- Turing machines

Finite automata

- $\mathcal{A} = \langle \Sigma, O, S, T, G, i \rangle$, where
- Σ is a finite alphabet called the *input alphabet*
- O is a finite alphabet called the *output alphabet*
- S is a finite set of *states*, with $i \in S$ *initial state*
- T is the *transition function* (possibly partial) $S \times \Sigma \to S$
- G is the *output function* (possibly partial) $S \to O$
- This is "Moore-style", we also have "Mealy style" and other styles

Homework

W7.1 Create a division table for Z_3 (do not attempt to divide by 0)

W7.2 Solve the equation $x^{17} - x^{16} + x^{15} - x^{14} + \ldots - 1 = 0$ in Z_3

W7.3 Count the number of non-equivalent polynomials of degree 17 ($p \equiv q$ is defined by $\forall x p(x) = q(x)$)

W7.4 Write a finite automaton that accepts all and only those strings that correspond to finite decimal numbers whose (a) integer part does not begin with 0, (b) has at most one decimal point in the string, (c) does not end with a string of 0s