Abstract Algebra I

Discrete Algebraic Structures

Thomas J. Friese

January 9, 2025

Recap of RSA

- ◇ find distinct prime numbers p and q
- ◇ $n := pq \to \varphi(n) = (p-1)(q-1)$
- ◇ choose $e \in \{2, \dots, \varphi(n) - 1\}$ coprime with $\varphi(n)$
- ◇ calculate d inverse of e modulo $\varphi(n)$ with euclids algorithm
- ◇ encrypt: $a \mapsto [a]_n^e$
- ◇ decrypt: $[m] \mapsto [m]_n^d$

$\to$ apply fermats theorem where possible

Cayley tables

$\times$	a	b	c
a	$a \times a$	$a \times b$	$a \times c$
b	$b \times a$	$b \times b$	$b \times c$
c	$c \times a$	$c \times b$	$c \times c$

Groups and Monoids

Associativity: $\forall a, b, c \in A : a \circ (b \circ c) = (a \circ b) \circ c$

Commutativity: $\forall a, b \in A$: $a \circ b = b \circ a$

Neutral element $\exists e_A \in A$ such that $\forall a \in A$: $e_A \circ a = a \circ e_A = a$

Inverse $\forall a \in A \; \exists b \in A$ such that $a \circ b = b \circ a = e_A$

$(A, \circ)$ is

$\rightarrow$ **monoid** if associative and has neutral element

$\rightarrow$ **group** if monoid and has inverse