1 Grundlagen

1.1 Primzahlen

1.2 Algebraische Strukturen

Definiert durch die Zahlentheorie und als zentraler Untersuchungsgegenstand des mathematischen Teilgebietes der universellen Algebra, liefern algebraische Strukturen die Basis zur Realisierung komplexer symmetrischer und asymmetrischer Kryptosysteme, weshalb wir im folgenden Kapitel die Eigenschaften relevanter algebraischer Strukturen näher betrachten wollen. Darüber hinaus möchten wir Ihnen auch einige Werkzeuge zum Rechnen in der jeweiligen algebraischen Struktur an die Hand geben, welche zur späteren Realisierung von Kryptosystemen benötigt werden.

Unter einer sehr allgemeinen Betrachtung ist eine mathematische Struktur eine Liste nichtleerer Mengen, genannt Trägermengen, mit Elementen aus den Trägermengen, genannt Konstanten, und mengentheoretischer Konstruktionen über den Trägermengen. Diese sind konkret Funktionen über den Trägermengen. Im Weiteren beschränken wir uns auf den Fall einer einzigen Trägermenge, wodurch die Strukturen als homogen bezeichnet werden können.

Definition: Homogene algebraische Struktur Eine homogene algebraische Struktur ist ein Tupel $(M, c_1, \ldots, c_m, f_1, \ldots, f_n)$ mit $m, n \in \mathbb{N}$ und $n \geq 1$. Dabei ist M eine nichtleere Menge, genannt **Trägermenge**, alle c_i sind Elemente aus M, genannt die **Konstanten**, und alle f_i sind s_i-stellige Funktionen $f_i : M \to M$ im Fall $s = 1$ und $f_i : M^{s_i} \to M$ im Fall $s_i > 1$, genannt die (inneren) **Operationen**. Die lineare Liste$(0, \ldots, 0, s_1, \ldots, s_n)$ mit m Nullen heißt **Typ** oder die **Signatur**.

1.2.1 Monoid

1.2.2 Gruppe

1.2.3 Ring

1.2.4 Körper