Algebraische Strukturen

Einige Ergebnisse der elementaren Zahlentheorie lauten:

Kleiner Fermatscher Satz: *Sei p eine Primzahl, die a nicht teilt, dann gilt: p teilt $a^{p-1}-1$.*
Satz von Wilson: *Jede Primzahl p teilt $(p-1)!+1$.* *Beispiel: 13 teilt 12! + 1 (=479001601)*
Satz von Lagrange: *Jede natürliche Zahl ist die Summe von vier Quadraten, Nullen sind zulässig.*
Noch unbewiesen ist die Goldbachsche Vermutung: *Jede gerade Zahl größer als 2 ist die Summe zweier Primzahlen.*

Carl Friedrich Gauss (1777-1855) konnte die Zahlentheorie wesentlich vereinfachen, indem er auf den Teilerresten eine Addition und Multiplikation betrachtete. Die Menge der Teilerreste für $p = 5$ lautet: $\mathcal{M} = \{0,\ 1,\ 2,\ 3,\ 4\}$. Die Verknüpfungen sind durch die Tabellen gegeben.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Aufg. Finde heraus, was diesen Definitionen zugrunde liegt.

Die Teilerreste bilden mit diesen Verknüpfungen einen sogenannten endlichen Körper.

Definition eines Körpers

In einer Menge $\mathcal{M}$ seien zwei Verknüpfungen, die wir Addition und Multiplikation nennen, erklärt, d.h. jedem Paar von Elementen $a,\ b \in \mathcal{M}$ ist eine Summe $a+b$ und ein Produkt $a \cdot b$ zugeordnet.
$\mathcal{M}$ bildet mit diesen Verknüpfungen einen Körper, falls für beliebige Elemente $a,\ b,\ c \in \mathcal{M}$ gilt:

Assoziativität:	$(a+b)+c$	$=$	$a+(b+c)$	$a\cdot(b\cdot c)$	$=$	$(a\cdot b)\cdot c$	
Kommutativität:	$a+b$	$=$	$b+a$	$a\cdot b$	$=$	$b\cdot a$	
neutrales Element:	$a+0$	$=$	a	$a\cdot 1$	$=$	a	
inverses Element:	$a+(-a)$	$=$	0	$a\cdot a^{-1}$	$=$	1	*für* $a \neq 0$
Distributivität	$a\cdot(b+c)$	$=$	$a\cdot b + a\cdot c$				

Aus diesen Körperaxionen können alle bekannten Rechenregeln, wie z. B. $(-a)\cdot(-b) = a\cdot b$ hergeleitet werden.

Seitdem im 19. Jahrhundert erkannt wurde, dass in verschiedenen Teilgebieten der Mathematik gleichartige Gesetzmäßigkeiten zu finden sind, untersuchte man die gemeinsamen zugrundeliegenden Strukturen. So erfolgt die Addition von Vektoren nach den gleichen Rechenregeln wie die Addition der Teilerreste oder die Verkettung von Permutationen. In der Algebra werden diese Strukturen anhand von Gruppen und Körpern untersucht. Wesentliches haben hierzu *Emmy Noether (1882-1935)* und *Ernst Steinitz (1871-1928)* beigetragen.

Definition einer Gruppe
Eine Menge $\mathcal{G}$ heißt Gruppe, wenn eine Verknüpfung $\circ$ definiert ist, die folgende Bedingungen erfüllt:

Die Verknüpfung ist assoziativ:	$(a\circ b)\circ c$	$=$	$a\circ(b\circ c)$
Es gibt ein neutrales Element e:	$a\circ e$	$=$	a
Zu jedem Element $a \in \mathcal{G}$ gibt es ein inverses Element $\overline{a}$:	$a\circ\overline{a}$	$=$	e