Gruppen, Ringe, Körper

Gruppe $(G,*)$, abelsch

Menge G mit Abbildung
$*: G\times G \to G$, $(a,b)\mapsto a*b$
(„Verknüpfung") mit:

(a) $\forall a,b,c\in G$:
$a*(b*c)=(a*b)*c$
„Assoziativität"

(b) Es gibt $e_G\in G$ („neutrales El.") → e_G eindeutig
mit $\forall a\in G: e_G*a=a=a*e_G$

(c) $\forall a\in G\ \exists a'\in G: a'*a=e_G=a*a'$ → a' eindeutig
(„inverses Element")

(d) für „abelsch":
$\forall a,b\in G: a*b=b*a$

$G=R$
$*=+$

Ring $(R,+,\cdot)$

Menge R mit Verknüpfungen
$+: R\times R\to R$, $(a,b)\mapsto a+b$ „Addition"
$\cdot: R\times R\to R$, $(a,b)\mapsto a\cdot b$ „Multipl."
mit:

(a) $(R,+)$ ist abelsche Gruppe
neutrales Element $0=0_R$
inverses Element zu a: $-a$

(b) Multiplikation „$\cdot$" ist assoziativ
$\forall a,b,c\in R: (a\cdot b)\cdot c = a\cdot(b\cdot c)$

(c) Distributivgesetze:
$\forall a,b,c\in R: a\cdot(b+c)=a\cdot b+a\cdot c$
$(b+c)\cdot a = b\cdot a+c\cdot a$

Satz: $\forall a,b\in R$:
$0_R\cdot a=0_R=a\cdot 0_R$
$a\cdot(-b)=-a\cdot b=(-a)\cdot b$

Satz: Kürzungsregel
$\forall a,b,c\in G$:
$a*b=a*c\Rightarrow b=c$

$(R,+,\cdot)$ kommutativer Ring

$\forall a,b\in R: a\cdot b=b\cdot a$

$(R,+,\cdot)$ Ring mit 1

Es gibt $1_R\in R$ mit
$\forall a\in R: 1_R\cdot a=a=a\cdot 1_R$

$(R,+,\cdot)$ kommutativer Ring mit 1

+ inverse Elemente Multiplikation

$(R,+,\cdot)$ nullteilerfrei

$\forall a,b\in R$:
$a\cdot b=0_R\Rightarrow a=0_R$ oder $b=0_R$

Genau dann, wenn m Primzahl

$(R,+,\cdot)$ Körper

$(R,+)$ abelsche Gruppe
(neutrales Element 0_R)
$(R\setminus\{0_R\},\cdot)$ abelsche Gruppe
(neutrales Element 1_R)
inverses El. zu a: a^{-1}
Es gelten die Distributivgesetze

Füge Eigenschaften für Multiplikation hinzu

Beispiel

$m\in\mathbb{N}$, $m>1$

$(F_m,+_m,\cdot_m)$

$F_m=\{0,\dots,m-1\}$

Für $a\in\mathbb{Z}$ seien $q,r\in\mathbb{Z}$ die eindeutig bestimmten Zahlen mit
$a=q\cdot m+r$, $0\le r<m$
Definiere $r_m(a):=r$.

$a+_m b := r_m(a+b)$
$a\cdot_m b := r_m(a\cdot b)$

Regeln:
$r_m(a\cdot b)=r_m(r_m(a)\cdot b)=r_m(a\cdot r_m(b))$
$r_m(a+b)=r_m(r_m(a)+b)=r_m(a+r_m(b))$