Charakteristik eines Körpers

Sei K ein beliebiger kommutativer Körper.

„Multiplikation“ ganzer Zahlen mit Körperelementen

Man definiert rekursiv eine Operation $\mathbb{Z}\times K\to K$, die man auch als Multiplikation bezeichnet: Zunächst definiert man $1\cdot x:=x$, dann für natürliche Zahlen $(n+1)\cdot x:=n\cdot x+x$, anschließend $0\cdot x:=0$, und schließlich für negative ganze Zahlen $n\cdot x:=-\big((-n)\cdot x\big)$.

Ist $n>0$, so ergibt sich der Wert $n\cdot x$ durch die n-fache Addition in K von x zu sich selbst.

Man beachte, daß jetzt z.B. der Ausdruck $1\cdot x$ verschieden interpretiert werden kann: einerseits als Multiplikation des Körperelements 1 mit dem Körperelement x, andererseits als die oben definierte Multiplikation der natürlichen Zahl 1 mit dem Körperelement x: das Ergebnis ist in beiden Fällen dasselbe. Im Ausdruck $-\big((-n)\cdot x\big)$ haben wir es beim inneren Minus mit der Inversenbildung in $\mathbb{Z}$ und beim äußeren mit der additiven Inversenbildung in K zu tun. Genauso beachte man, daß mit 1+1 jetzt einerseits eine natürliche bzw. ganze Zahl, andererseits ein Körperelement gemeint sein kann, welches letztere man dann auch gern 2 nennt. Dabei können sich irritierende aber durchaus widerspruchsfreie Gleichungen ergeben, z.B. 2=0 in $\mathbb{Z}_2$.

Man kann jetzt (i.w. durch Induktion) folgende Eigenschaften der obigen Multiplikation beweisen:

A $\forall\, n,m\in\mathbb{Z},\, x\in K:\ (n+m)\cdot x=n\cdot x+m\cdot x$
B $\forall\, n\in\mathbb{Z},\, x,\, y\in K:\ n\cdot(x+y)=n\cdot x+n\cdot y$
C $\forall\, n\in\mathbb{Z},\, x\in K:\ n\cdot(-x)=-(n\cdot x)$
D $\forall\, n,m\in\mathbb{Z},\, x\in K:\ (n\cdot m)\cdot x=n\cdot(m\cdot x)$
E $\forall\, n\in\mathbb{Z},\, x,\, y\in K:\ n\cdot(x\cdot y)=(n\cdot x)\cdot y$

Zur Übung hier der Beweis von C:
Man zeige zunächst $0=n\cdot 0$ und hat dann $0=n\cdot 0=n\cdot(x+(-x))=n\cdot x+n\cdot(-x)$ (wegen B); also ist $n\cdot(-x)$ das additiv Inverse von $n\cdot x$ und damit $n\cdot(-x)=-(n\cdot x)$.

und von D: Wir zeigen zunächst $\forall\, n\in\mathbb{N}\big(\forall\, m\in\mathbb{N}(\forall\, x\in K:\ (n\cdot m)\cdot x=n\cdot(m\cdot x))\big)$.

Dazu ist nachzuweisen, daß
1. $\forall\, m\in\mathbb{N}(\forall\, x\in K:\ (1\cdot m)\cdot x=1\cdot(m\cdot x))$
2. $\forall\, m\in\mathbb{N}(\forall\, x\in K:\ (n\cdot m)\cdot x=n\cdot(m\cdot x))\quad\Rightarrow\quad\forall\, m\in\mathbb{N}(\forall\, x\in K:\ ((n+1)\cdot m)\cdot x=(n+1)\cdot(m\cdot x))$.

ad 1.
Offenbar gilt für beliebige $m\in\mathbb{N},\, x\in K:\ (1\cdot m)\cdot x=m\cdot x=1\cdot(m\cdot x)$.

ad 2.
Es gilt für $n,\, m\in\mathbb{N},\, x\in K$:
$((n+1)\cdot m)\cdot x=(n\cdot m+m)\cdot x=(n\cdot m)\cdot x+m\cdot x=n\cdot(m\cdot x)+m\cdot x=(n+1)\cdot(m\cdot x)$
Dabei haben wir für die erste Gleichung das Distributivgesetz in $\mathbb{Z}$ benutzt, für die zweite die Formel A, für die dritte die Induktionsvoraussetzung und für die letzte die Definition unserer Operation $\mathbb{Z}\times K\to K$.

Als nächstes betrachtet man den Fall, daß mindestens einer der beteiligten „Faktoren“ n, m gleich Null ist, und dann, daß einer oder beide negativ sind; sind z.B. n, $m<0$, so hat man:
$(n\cdot m)\cdot x=((-n)\cdot(-m))\cdot x=(-n)\cdot((-m)\cdot x)=-(n\cdot((-m)\cdot x))=-(n\cdot(-(m\cdot x)))=-(-(n\cdot(m\cdot x)))=n\cdot(m\cdot x)$

Die erste Gleichung benutzt nur eine Eigenschaft der Multiplikation in $\mathbb{Z}$, die zweite das bereits bewiesene „Assoziativgesetz“ bei positiven ganzen Zahlen, die dritte folgt mit der Definition der „Multiplikation“ mit einer negativen Zahl, die vierte ebenfalls, die fünfte benutzt die oben bewiesene Eigenschaft C, und die letzte ist eine Eigenschaft der Körperaddition.

Im Körper $\mathbb{Z}_3$ gilt: 1+1+1=0 . Genauso muß bei jedem anderen endlichen Körper durch vielfache Addition der 1 zu sich selbst irgendwann Null herauskommen: Setzt man $x_1:=1$ und $x_{n+1}:=x_n+1$, so muß in der so definierten unendlichen Folge von Körperelementen irgendwann eine Wiederholung auftreten, d.h. es muß Zahlen $n, m\in\mathbb{N}$, $n<m$ geben mit $x_n = x_m$. Offenbar ist $x_k=k\cdot 1$; man hat demnach $x_n=n\cdot 1$ und $x_m=m\cdot 1$. Es ergibt sich also $0=x_m-x_n=m\cdot 1-n\cdot 1=(m-n)\cdot 1=x_{m-n}$.

In den Restklassenkörpern $\mathbb{Z}_p$ gilt $p\cdot 1=0$, und damit auch $\forall\, x\in\mathbb{Z}_p:\ p\cdot x=0$

Die **Charakteristik** eines Körpers[1] **char *K*** ist die kleinste natürliche Zahl, für die gilt: $n\cdot 1=0$. Falls es keine solche Zahl gibt, falls also $\forall\, n\in\mathbb{N}:\ n\cdot 1\neq 0$, so sagt man, der Körper habe die Charakteristik 0[2]. Damit haben $\mathbb{Q}\subset\mathbb{R}\subset\mathbb{C}$ die Charakteristik 0, während die Körper $\mathbb{Z}_p$ die Charakteristik p besitzen. Es ist leicht zu zeigen, daß die Charakteristik eines Körpers gleich 0 oder eine Primzahl sein muß[3].

In einem Körper der Charakteristik 2 gilt für jedes $x\in K: x=-x$, weil ja $x+x=(1+1)x=0x=0$. In einem solchen Körper folgt also aus $x=-x$ nicht, daß $x=0$. In allen anderen Körpern ist $1+1\neq 0$ und daher folgt dann aus $x=-x$ daß $0=x+(-x)=x+x=(1+1)x$, und wegen der Nullteilerfreiheit im Körper muß $x=0$ sein.

Körper der Charakteristik 2 spielen insbesondere in Informatik-nahen Gebieten eine große Rolle. Wir kennen bisher nur $\mathbb{Z}_2$ als solchen. Man kann zeigen, daß es zu jeder natürlichen Zahl n einen Körper mit 2^n Elemente gibt. Dieses Ergebnis kann man so auffassen, daß es auf dem Vektorraum $\mathbb{Z}_2^n$ auch eine Multiplikation gibt, die diesen Raum zu einem Körper macht.

Für Vektorräume zeigt man analog:

Ist V ein Vektorraum über einem Körper der Charakterisik 2, so gilt:
$\forall\, x\in V:\ x=-x$ bzw. $\forall\, x\in V:\ x+x=0$.

Ist V ein Vektorraum über einem Körper mit Charakterisik ungleich 2, so gilt:
$\forall\, x\in V:\ x=-x\ \Rightarrow\ x=0$.

---

1 Genauso hätten wir die Charakteristik von Ringen definieren können.

2 Eigentlich müßte man in diesem Fall setzen char $K=\infty$. Es hat sich aber die Bezeichnung char $K=0$ eingebürgert.

3 Wäre n=char K und $n=m\cdot k$ mit $1<m,k<n$, so hätte man $0=n\cdot 1=(m\cdot k)\cdot 1=m\cdot(k\cdot 1)=(m\cdot 1)(k\cdot 1)$. (Man sollte sich klarmachen, daß man so rechnen darf.) Wegen der Nullteilerfreiheit des Körpers K müßte dann bereits $m\cdot 1=0$ oder $m\cdot 1=0$ gelten, was der Minimalität von n widerspricht.