LMU Mathematisches Institut

§8 Gruppen und Körper

(8.1) Definition: Eine *Gruppe* G ist eine Menge zusammen mit einer Verknüpfung, die jedem Paar (a,b) von Elementen aus G ein weiteres Element a?b aus G zuordnet, so dass die folgenden drei Axiome erfüllt sind:

1º (a?b)?c = a?(b?c) für alle a,b,c aus G. („*Assoziativgesetz*“)
2º Es gibt n aus G mit a?n = a . (n heißt *neutrales Element*.)
3º Zu jedem a aus G existiert a* aus G mit a?a* = n . (a* heißt *inverses Element* oder *Inverse* zu a.)

Die Gruppe heißt *abelsch*, wenn außerdem
4º a?b = b?a für alle a,b aus G.

LMU Mathematisches Institut

(8.2) Beispiele:
1º **Z,** die Menge der ganzen Zahlen, mit + anstelle von ? : n = 0 und a* = -a**.**
2º Man beachte: **N** mit + ist keine Gruppe, weil es zu positiven ganzen Zahlen a keine Inverse –a in **N** gibt.
3º Analog zu 1º: **Q, R, C** mit + ist abelsche Gruppe.
4º $\mathbf{R}_+$ mit der Multiplikation ist ebenfalls eine abelsche Gruppe: n = 1 und $a^* = a^{-1}$. Ebenso: **R \{0} .**
5º Weitere Beispiele sind alle T aus **§**7, also die Translationen zu einem Translationsraum (A,T,t).
6º Eine zweielementige Gruppe (die Gruppe zum Modell 1 in Beispiel 7.3.1):
G = {0,1} mit 0+0 = 1+1 = 0 und 0+1 = 1+0 = 1 .
Die „gleiche“ (vgl. Isomorphismus in 8.8) Gruppe:
H = {n,w} mit n+n = w+w = n und n+w = w+n = w .

(8.3) Bemerkungen, Notationen:

1º Die Verknüpfung einer Gruppe heißt auch *Gruppen-operation* oder (*Gruppen-*) *Multiplikation*. Sie wird meist kurz ab Statt a?b geschrieben. Die grundlegenden Axiome haben dann die Form: (ab)c = a(bc) , an = na = a , a*a = aa* = n .

Das neutrale Element schreibt man auch als 1 und nennt es *Einselement*. Die Inverse schreibt man auch als a^{-1}.
Im abelschen Fall schreibt man auch a+b anstelle von a?b und man spricht von einer *abelschen additiven Gruppe.* Das neutrale Element n wird dann meist als 0 geschrieben und dann auch als Null (-element) bezeichnet, a* wird als –a geschrieben und a-b als Abkürzung von a+(-b) .

Jede Gruppe G besitzt ein neutrales Element, ist daher nicht leer.

2º Das Assoziativgesetz (ab)c = a(bc) erlaubt die Definition abc := (ab)c = a(bc) unabhängig von der Klammerung.

Analog hat man für 4 Elemente den klammerfreien Ausdruck abcd . Entsprechend für beliebig (aber endlich) viele Elemente (Induktion!)

3º *Potenzen*: $a^0 := e$, $a^{(n+1)} := aa^n$ (rekursive Definition für natürliche Zahlen n). Und $a^{-n} := (a^n)^{-1}$. Dann gelten die Regeln:
$a^n a^m = a^{n+m}$, $(a^n)^m = a^{nm}$.

4º Allgemeiner lassen sich endliche Summen oder Produkte mit beliebigen Gruppenelementen bilden:

$$\prod_{i=n} a_i \quad \text{oder} \quad \sum_{i=n} a_i \ .$$

5º In einer Gruppe G gilt immer: n?a = a und a*?a = n für alle Gruppenelemente a .

(8.4) Äquivalenzsatz für Gruppen: Es sei auf der nichtleeren Menge G eine Verknüpfung gegeben, die dem Assoziativgesetz genügt: (ab)c = a(bc) . Behauptung:

G ist genau dann eine Gruppe, wenn für alle a, b aus G die Gleichungen $ax = b$ und $ya = b$ stets Lösungen in G haben.

(8.5) Folgerungen: G sei Gruppe mit dem neutralen Element e . Dann gilt für alle a,b,c aus G:

1° (*Kürzungsregel*) Aus $ab = ac$ folgt $b = c$ und aus $ab = cb$ folgt $a = c$.

2° $ax = b$ und $ya = b$ sind eindeutig lösbar.

3° Die Inverse a^{-1} zu a ist eindeutig bestimmt.

4° e ist eindeutig bestimmt.

(8.6) Beispiel: Sei M einen Menge. Die Menge S(M) der bijektiven Abbildungen von M nach M bildet mit der Komposition „?“ als Verknüpfung und der Identität id als neutralem Element eine Gruppe. S(M) ist nicht abelsch, wenn M drei verschieden Elemente enthält.

S(M) mit dieser Verknüpfung nennt man die Gruppe der *Permutationen* von M .
Im Falle der Menge $M = \{1,2,3, \dots , n\}$ schreibt man die Elemente p von $S(M) =: S_n$ in der Form

oder

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ p(1) & p(2) & p(3) & \dots & p(n) \end{pmatrix}$$

$$\begin{pmatrix} a^1 & a^2 & a^3 & \dots & a^n \\ p(a^1) & p(a^2) & p(a^3) & \dots & p(a^n) \end{pmatrix}$$

Spezielle Permutationen auf $M = \{1,2,3, \dots , n\}$ sind die *zyklischen* Permutationen, das sind per Definition die p_k, $k = 0,1,2, \dots n$, mit

$p_k(j) := j+k$ für $j = 1, 2, \dots , n-k$, und
$p_k(j) := j+k-n$ für $j = n-k+1, n-k+2, \dots , n$.

Es gilt: $p_k ? p_m = p_{k+m}$ für $k+m < n$, und
$p_k ? p_m = p_{k+m-n}$ für $k+m > n-1$.

Also ist die Komposition von Abbildungen eine Verknüpfung auf der Menge $E_{(n)} := \{p_k : k = 0,1,2, \ldots n-1\}$ der zyklischen Permutationen von n Elementen:

$$\circ : E_{(n)} \times E_{(n)} \to E_{(n)}$$

Das Assoziativgesetz gilt für die Komposition, p_0 ist das neutrale Element und zu p_k ist p_{n-k} die Inverse. Damit ist $E_{(n)}$ eine Gruppe, und sogar eine abelsche Gruppe.

Besonderheiten: Die Regeln $p_k ? p_m = p_{k+m}$, bzw. $p_k ? p_m = p_{k+m-n}$ zeigen (in multiplikativer Schreibweise mit $p_0 = 1$, vgl. 8.3.3°):

$(p_1)^k = p_k$, und
$(p_k)^n = 1$

Also: p_1 „erzeugt“ die Gruppe $E_{(n)}$ (vgl. 9.3).

Und: p_k erfüllt die Gleichung $(p_k)^n = 1$, kann also als *n-te Wurzel der Einheit* aufgefasst werden. Daher:

(8.7) Beispiel: Die Menge $E_{(n)}$ der „n-ten Einheitswurzeln“ bildet eine abelsche Gruppe bezüglich der Komposition. (Es handelt sich um eine zyklische Gruppe, vgl. 9.3).

Andere Realisierungen von $E_{(n)}$:

- Als die n komplexen Zahlen auf dem Einheitskreis:
  $e_k := \exp(2p\,ik/n)$
- Als die n Drehungen r_k in der Ebene, die ein regelmäßiges n-Eck in sich überführen.

(8.8) Definition: (Homomorphismus) Ein *Homomorphismus* zwischen den Gruppen G und H ist eine Abbildung

mit $f(ab) = f(a)f(b)$ für alle a,b aus G .

Ein Homomorphismus f ist *Isomorphismus*, wenn f bijektiv ist und die Umkehrabbildung auch ein Homomorphismus ist.

Beispiele: f(a) := 2a ; g(a) := exp(a) für a aus **R** . f und g sind Isomorphismen von **R** nach **R** bzw. von **R** nach $\mathbf{R}_+$.

(8.9) Lemma: Für einen Homomorphismus f von Gruppen gilt:

1º f(e) ist das neutrale Element von H, wenn e das neutrale Element von G ist.

2º $f(a^{-1})$ ist die Inverse zu f(a) für alle a aus G: $[f(a)]^{-1} = f(a^{-1})$

3º Sei $f : G \to H$ ein bijektiver Homomorphismus von Gruppen, dann ist f ein Isomorphismus.

(8.10) Definition: (Untergruppen) Eine Teilmenge U einer Gruppe G ist eine Untergruppe, wenn U bezüglich der restringierten Verknüpfung $(a,b) \mapsto ab$, a,b aus U, eine Gruppe ist.

(8.11) Lemma: Eine nichtleere Teilmenge U einer Gruppe G ist genau dann eine Untergruppe, wenn gilt: Für alle a,b aus U sind auch ab und a^{-1} Elemente aus U .

(8.12) Lemma: Für einen Homomorphismus sei
Ker f := {a : f(a) = e} = f^{-1}(e),
Im f := {f(a): a aus G} = f(G) .
Es gilt:

1º Im f ist Untergruppe von H .
2º Ker f ist Untergruppe von G .
3º f ist genau dann injektiv, wenn Ker f = {e} gilt.

Für den *Kern* Ker f eines Homomorphismus gilt außerdem: Für alle u aus Ker f und alle a aus G ist $a^{-1}ua$ wieder eine Element von Ker f. Ker f ist also ein Normalteiler:

(8.13) Definition: Eine Untergruppe U einer Gruppe G ist ein *Normalteiler* von G, wenn für alle u aus U und alle a aus G $a^{-1}ua$ wieder eine Element von U ist.

(8.14) Definition: Ein *Körper* K ist eine additive abelsche Gruppe, zu der es eine Multiplikation $K \times K \to K$ gibt mit den folgenden Eigenschaften:

1° K\{0} ist eine abelsche Gruppe bezüglich der Multiplikation.

2° a(b+c) = ab + ac für alle a,b,c aus K .

(8.15) Beispiele: 1° **R** und **Q** . **Z** ist aber nicht Körper.

2° Die zweielementige Gruppe aus 8.2.6° : G = {0,1} mit 0+0 = 1+1 = 0, 0+1 =1+0 = 1 und 0·0 = 0·1 = 1·0 = 0, 1·1 = 1 .

3° Der Körper mit 3 Elementen.

4° Der Körper mit 4 Elementen.

5° Der Körper **C** der *komplexen Zahlen*:

C ist die Menge der reellen Zahlenpaare $\mathbf{R}^2$ mit der Addition:

(x,y) + (v,w) := (x+v,y+w) ,

Multiplikation:

(x,y)(v,w) := (xv-yw,xw+yv) ,

Für x,y,v,w aus **R** .

C mit diesen Verknüpfungen ist ein Körper.

Es gilt in **C** :

0 := (0,0) ist die Null in **C**

1 := (1,0) ist das Einselement in **C** ,

Die Inverse zu (x,y) aus **C**{0} ist

$$\left(\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2} \right)$$

Notation in **C** :

i := (0,1) erfüllt die Gleichung $i^2 + 1 = 0$,

x + iy := (x,y) ,

Re (x,y) = Re (x+iy) := x

Im (x,y) = Im (x+iy) := y.

Multiplikation mit der Notation x + iy :

(x + iy)(v + iw) = xv-yw + i(xw+yv) .

Im übrigen sind 1, i, -1, -i die 4-ten Einheitswurzeln (vgl. 8.7).

(8.16) Definition: Unterkörper, Homomorphismus, Isomorphismus analog zu Gruppen.

Ein Homomorphismus $f : K \to K'$ zwischen Körpern erfüllt also

f(a+b) = f(a) + f(b) und

f(ab) = f(a)f(b)

für alle a und b aus K. Insbesondere: f(0) = 0 und f(1) = 1.