Prof. Dr. H. Brenner **Osnabrück SS 2011**

Körper- und Galoistheorie

Vorlesung 4

In dieser und der nächsten Vorlesung werden wir uns mit Gruppentheorie, insbesondere mit Restklassenbildung, beschäftigen. Zum einen ist die Restklassenbildung für uns wichtig, um zu einem Ideal $I \subseteq K[X]$ den Restklassenring $K[X]/I$ zu konstruieren. Diese Konstuktion ist entscheidend, um die dritte zu Beginn der letzten Vorlesung gestellte Frage beantworten zu können. Zum andern treten Gruppen als Galoisgruppen von Körpererweiterungen auf, und die Korrespondenz zwischen Untergruppen der Galoisgruppe und Zwischenkörpern ist der Hauptgegenstand der Galoistheorie. Um unser hauptsächliches Interesse, die Körper- und Galoistheorie, nicht zu lange aus dem Blick zu verlieren, werden wir uns hier bei den ohnehin einfachen Beweisen kurz halten. Ähnliche Argumente sind von der linearen Algebra bekannt.

Gruppenhomomorphismen

DEFINITION 4.1. Seien $(G, \circ, e_G)$ und $(H, \circ, e_H)$ Gruppen. Eine Abbildung

$$\psi : G \longrightarrow H$$

heißt *Gruppenhomomorphismus*, wenn die Gleichheit

$$\psi(g \circ g') \ = \ \psi(g) \circ \psi(g')$$

für alle $g, g' \in G$ gilt.

Die Menge der Gruppenhomomorphismen von G nach H wird mit

$$\operatorname{Hom}(G, H)$$

bezeichnet. Aus der linearen Algebra sind vermutlich die linearen Abbildungen zwischen Vektorräumen bekannt, welche insbesondere Gruppenhomomorphismen sind, darüber hinaus aber auch noch mit der skalaren Multiplikation verträglich sind. Die folgenden beiden Lemmata folgen direkt aus der Definition.

LEMMA 4.2. *Es seien G und H Gruppen und $\varphi : G \to H$ sei ein Gruppenhomomorphismus. Dann ist $\varphi(e_G) = e_H$ und $(\varphi(g))^{-1} = \varphi(g^{-1})$ für jedes $g \in G$.*

Beweis. Siehe Aufgabe 4.1. □

LEMMA 4.3. *Es seien F, G, H Gruppen. Dann gelten folgende Eigenschaften.*

(1) *Die Identität* $\mathrm{id} : G \to G$ *ist ein Gruppenhomomorphismus.*

(2) *Sind $\varphi : F \to G$ und $\psi : G \to H$ Gruppenhomomorphismen, so ist auch die Hintereinanderschaltung $\psi \circ \varphi : F \to H$ ein Gruppenhomomorphismus.*
(3) *Ist $F \subseteq G$ eine Untergruppe, so ist die Inklusion $F \hookrightarrow G$ ein Gruppenhomomorphismus.*
(4) *Sei $\{e\}$ die triviale Gruppe. Dann ist die Abbildung $\{e\} \to G$, die e auf e_G schickt, ein Gruppenhomomorphismus. Ebenso ist die (konstante) Abbildung $G \to \{e\}$ ein Gruppenhomomorphismus.*

Beweis. Das ist trivial. □

LEMMA 4.4. *Sei G eine Gruppe. Dann entsprechen sich eindeutig Gruppenelemente $g \in G$ und Gruppenhomomorphismen φ von $\mathbb{Z}$ nach G über die Korrespondenz*

$$g \longmapsto (n \mapsto g^n) \text{ und } \varphi \longmapsto \varphi(1)\,.$$

Beweis. Siehe Aufgabe 4.2. □

Man kann den Inhalt dieses Lemmas auch kurz durch $G \cong \mathrm{Hom}\,(\mathbb{Z}, G)$ ausdrücken. Die Gruppenhomomorphismen von einer Gruppe G nach $\mathbb{Z}$ sind schwieriger zu charakterisieren. Die Gruppenhomomorphismen von $\mathbb{Z}$ nach $\mathbb{Z}$ sind die Multiplikationen mit einer festen ganzen Zahl a, also

$$\mathbb{Z} \longrightarrow \mathbb{Z},\ x \longmapsto ax.$$

Gruppenisomorphismen

DEFINITION 4.5. Seien G und H Gruppen. Einen bijektiven Gruppenhomomorphismus

$$\varphi : G \longrightarrow H$$

nennt man einen *Isomorphismus* (oder eine *Isomorphie*). Die beiden Gruppen heißen *isomorph*, wenn es einen Isomorphismus zwischen ihnen gibt.

LEMMA 4.6. *Seien G und H Gruppen und sei*

$$\varphi : G \longrightarrow H$$

ein Gruppenisomorphismus. Dann ist auch die Umkehrabbildung

$$\varphi^{-1} : H \longrightarrow G,\ h \longmapsto \varphi^{-1}(h),$$

ein Gruppenisomorphismus.

Beweis. Siehe Aufgabe 4.3. □

Isomorphe Gruppen sind bezüglich ihrer gruppentheoretischen Eigenschaften als gleich anzusehen. Isomorphismen einer Gruppe auf sich selbst nennt man auch *Automorphismen*. Wichtige Beispiele für Automorphismen sind die sogenannten inneren Automorphismen, siehe die nächste Vorlesung.

Der Kern eines Gruppenhomomorphismus

DEFINITION 4.7. Seien G und H Gruppen und sei

$$\varphi : G \longrightarrow H$$

ein Gruppenhomomorphismus. Dann nennt man das Urbild des neutralen Elementes den *Kern* von φ, geschrieben

$$\text{kern } \varphi = \varphi^{-1}(e_H) = \{g \in G | \, \varphi(g) = e_H\} \, .$$

LEMMA 4.8. *Seien G und H Gruppen und sei*

$$\varphi : G \longrightarrow H$$

ein Gruppenhomomorphismus. Dann ist der Kern von φ eine Untergruppe von G.

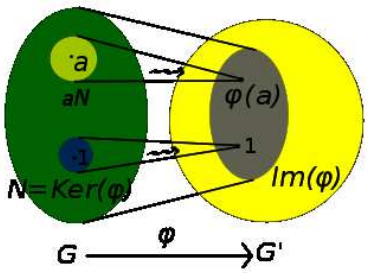
Beweis. Wegen $\varphi(e_G) = e_H$ ist $e_G \in \ker \varphi$. Seien $g, g' \in \ker \varphi$. Dann ist

$$\varphi(gg') = \varphi(g)\varphi(g') = e_H e_H = e_H$$

und daher ist auch $gg' \in \ker \varphi$. Der Kern ist also ein Untermonoid. Sei nun $g \in \ker \varphi$ und betrachte das inverse Element g^{-1}. Es ist

$$\varphi(g^{-1}) = (\varphi(g))^{-1} = e_H^{-1} = e_H \, ,$$

also auch $g^{-1} \in \ker \varphi$. □



LEMMA 4.9. *Seien G und H Gruppen. Ein Gruppenhomomorphismus $\varphi : G \to H$ ist genau dann injektiv, wenn der Kern von φ trivial ist.*

Beweis. Wenn φ injektiv ist, so darf auf jedes Element $h \in H$ höchstens ein Element aus G gehen. Da e_G auf e_H geschickt wird, darf kein weiteres Element auf e_H gehen, d.h. $\ker \varphi = \{e_G\}$. Sei umgekehrt dies der Fall und sei angenommen, dass $g, \tilde{g} \in G$ beide auf $h \in H$ geschickt werden. Dann ist

$$\varphi(g\tilde{g}^{-1}) = \varphi(g)\varphi(\tilde{g})^{-1} = hh^{-1} = e_H$$

und damit ist $g\tilde{g}^{-1} \in \ker \varphi$, also $g\tilde{g}^{-1} = e_G$ nach Voraussetzung und damit $g = \tilde{g}$. □

Nebenklassen

DEFINITION 4.10. Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Wir setzen $x \sim_H y$ (und sagen, dass x und y äquivalent sind) wenn $x^{-1}y \in H$.

Dies ist in der Tat eine Äquivalenzrelation: Aus $x^{-1}x = e_G \in H$ folgt, dass diese Relation reflexiv ist. Aus $x^{-1}y \in H$ folgt sofort $y^{-1}x = (x^{-1}y)^{-1} \in H$ und aus $x^{-1}y \in H$ und $y^{-1}z \in H$ folgt $x^{-1}z \in H$.

DEFINITION 4.11. Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Dann heißt zu jedem $x \in G$ die Teilmenge

$$xH = \{xh |\, h \in H\}$$

die *Linksnebenklasse von* x in G bzgl. H. Jede Teilmenge von dieser Form heißt *Linksnebenklasse*. Entsprechend heißt eine Menge der Form

$$Hy = \{hy |\, h \in H\}$$

Rechtsnebenklasse (zu y).

Die Äquivalenzklassen zu der oben definierten Äquivalenzrelation sind wegen

$$\begin{aligned}
[x] &= \{y \in G |\, x \sim y\} \\
&= \{y \in G |\, x^{-1}y \in H\} \\
&= \{y \in G |\, \text{es gibt } h \in H \text{ mit } x^{-1}y = h\} \\
&= \{y \in G |\, \text{es gibt } h \in H \text{ mit } y = xh\} \\
&= xH
\end{aligned}$$

genau die Linksnebenklassen. Die Linksnebenklassen bilden somit eine disjunkte Zerlegung (eine *Partition*) von G. Dies gilt ebenso für die Rechtsnebenklassen. Im kommutativen Fall muss man nicht zwischen Links- und Rechtsnebenklassen unterscheiden.

LEMMA 4.12. *Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Es seien $x, y \in G$ zwei Elemente. Dann sind folgende Aussagen äquivalent.*

(1) $x \in yH$
(2) $y \in xH$
(3) $y^{-1}x \in H$
(4) $x^{-1}y \in H$
(5) $xH \cap yH \neq \emptyset$
(6) $x \sim_H y$.
(7) $xH = yH$.

Beweis. Die Äquivalenz von (1) und (3) (und die von (2) und (4)) folgt aus Multiplikation mit y^{-1} bzw. mit y. Die Äquivalenz von (3) und (4) folgt durch Übergang zum Inversen. Aus (1) folgt (5) wegen $1 \in H$. Wenn (5) erfüllt ist, so bedeutet das $xh_1 = yh_2$ mit $h_1, h_2 \in H$. Damit ist $x = yh_2h_1^{-1}$ und (1) ist erfüllt. (4) und (6) sind nach Definition äquivalent. Da die Nebenklassen Äquivalenzklassen sind, ergibt sich die Äquivalenz von (5) und (7). □

Gruppenordnung und Elementordnung

DEFINITION 4.13. Zu einer endlichen Gruppe G bezeichnet man die Anzahl ihrer Elemente als *Gruppenordnung* oder als die *Ordnung der Gruppe*, geschrieben

$$\operatorname{ord}(G) = \#(G).$$

DEFINITION 4.14. Sei G eine Gruppe und $g \in G$ ein Element. Dann nennt man die kleinste positive Zahl n mit $g^n = e_G$ die *Ordnung* von g. Man schreibt hierfür $\operatorname{ord}(g)$. Wenn alle positiven Potenzen von g vom neutralen Element verschieden sind, so setzt man $\operatorname{ord}(g) = \infty$.

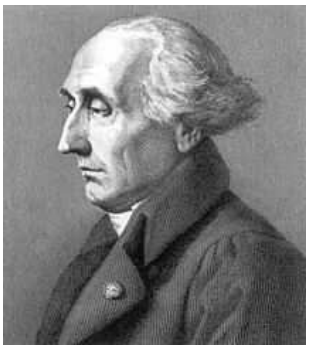
LEMMA 4.15. *Sei G eine endliche Gruppe. Dann besitzt jedes Element $g \in G$ eine endliche Ordnung. Die Potenzen*

$$g^0 = e_G,\ g^1 = g,\ g^2, \ldots, g^{\operatorname{ord}(g)-1}$$

sind alle verschieden.

Beweis. Siehe Aufgabe 4.8. □

Der Satz von Lagrange



Joseph-Louis Lagrange (1736 Turin - 1813 Paris)

SATZ 4.16. *Sei G eine endliche Gruppe und $H \subseteq G$ eine Untergruppe von G. Dann ist ihre Kardinalität $\#(H)$ ein Teiler von $\#(G)$.*

Beweis. Betrachte die Linksnebenklassen $gH := \{gh \,|\, h \in H\}$ für sämtliche $g \in G$. Es ist $h \mapsto gh$ eine Bijektion zwischen H und gH, so dass alle Nebenklassen gleich groß sind (und zwar $\#(H)$ Elemente haben). Die Nebenklassen bilden (als Äquivalenzklassen) zusammen eine Zerlegung von G, so dass $\#(G)$ ein Vielfaches von $\#(H)$ sein muss. □

KOROLLAR 4.17. *Sei G eine endliche Gruppe und sei $g \in G$ ein Element. Dann teilt die Ordnung von g die Gruppenordnung.*

Beweis. Sei H die von g erzeugte Untergruppe. Nach Lemma 4.15 ist $\operatorname{ord}(g) = \operatorname{ord}(H)$. Daher teilt diese Zahl nach Satz 4.16 die Gruppenordnung von G. □

DEFINITION 4.18. Zu einer Untergruppe $H \subseteq G$ heißt die Anzahl der (Links- oder Rechts)Nebenklassen der *Index* von H in G, geschrieben

$$\operatorname{ind}_G H\,.$$

In der vorstehenden Definition ist Anzahl im allgemeinen als die *Mächtigkeit* einer Menge zu verstehen. Der Index wird aber hauptsächlich dann verwendet, wenn er endlich ist, wenn es also nur endlich viele Nebenklassen gibt. Das ist bei endlichem G automatisch der Fall, kann aber auch bei unendlichem G der Fall sein, wie schon die Beispiele $\mathbb{Z}n \subseteq \mathbb{Z}$, $n \geq 1$, zeigen. Wenn G eine endliche Gruppe ist und $H \subseteq G$ eine Untergruppe, so gilt aufgrund des Satzes von Lagrange die einfache *Indexformel*

$$\#(G) = \#(H) \cdot \operatorname{ind}_G H\,.$$

Abbildungsverzeichnis